Guarding Vision Client Software

User Manual

Legal Information

User Manual

About this Manual

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.
Please use this user manual under the guidance of professionals.

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 OUR COMPANY 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 OUR COMPANY, 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 OUR COMPANY 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. OUR COMPANY SHALL NOT TAKE ANY RESPONSIBILITES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER ATTACK, HACKER ATTACK, VIRUS INSPECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, OUR COMPANY WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
SURVEILLANCE LAWS VARY BY JURISDICTION. PLEASE CHECK ALL RELEVANT LAWS IN YOUR JURISDICTION BEFORE USING THIS PRODUCT IN ORDER TO ENSURE THAT YOUR USE CONFORMS THE APPLICABLE LAW. OUR COMPANY SHALL NOT BE LIABLE IN THE EVENT THAT THIS PRODUCT IS USED WITH ILLEGITIMATE PURPOSES.
IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATER PREVAILS.

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
⚠️ **Danger**	Indicates a hazardous situation which, if not avoided, will or could result in death or serious injury.
⚠️ **Caution**	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
📖 **Note**	Provides additional information to emphasize or supplement important points of the main text.

Contents

Chapter 1 Overview

Guarding Vision Client Software is a versatile security management software for the DVRs, NVRs, IP cameras, encoders, decoders, security control panels, video intercom devices, access control devices, etc.

1.1 Introduction

The software 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 functions, configurations and operation steps of the client 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

The followings are the recommended running environment for installing the client software.

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

2 GB or Above

Video Card

RADEON X700 Series or Above

GPU

256 MB or Above

⊡**Note**

- For high stability and good performance, the 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 the operating systems with the version after Windows XP.

1.3 Customize Displayed Modules on Control Panel

For the first time running the software, you can customize the modules displayed on the Operation and Control area of the control panel.

Perform this task when you need to customize the modules displayed on control panel.

Steps
1. Click **Modules Customization** on the control panel to open Modules Customization page.
2. Check the module(s) to display them on the control panel according to the actual needs.
3. Click **OK**.

⊡**Note**

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

1.4 Summary of Changes

The followings are the changes between this version and the previous version.

- Add queue management and face recognition check-in function in Statistics.
- Add access control device parameters configuration.
- Provide IPC default password setting for activating IPC using NVR device.
- Add two-way audio function in Access Control module.
- Add unlocking two doors when two door stations are connected.

Chapter 2 User Registration and Login

You should register a super user and then you can login the client with the super user account as administrator.
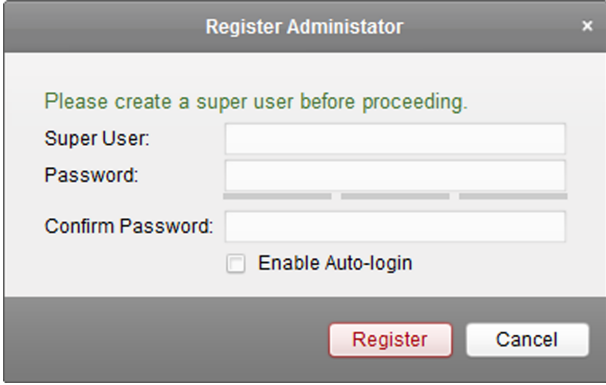
2.1 Register a User

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

Perform the following steps to register a super user for login.

Steps
1. After installing the client, double click to run the software.

Figure 2-1 Register a User

2. Create a user name and password for the super user.

⎥**i**⎥**Note**

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

---

3. Confirm the password.
4. **Optional:** Check the **Enable Auto-login** checkbox to log into the software automatically.
5. Click **Register** to register the super user.

   You can log into the software as super user.

What to do next
Log into the client. Refer to *Login* for details.

2.2 Login

You can log in to the client software to perform the operations, such as live view, playback, and so on.

Perform this task if you want to log in to the client software.

Steps
1. Run the client software to open Login dialog.
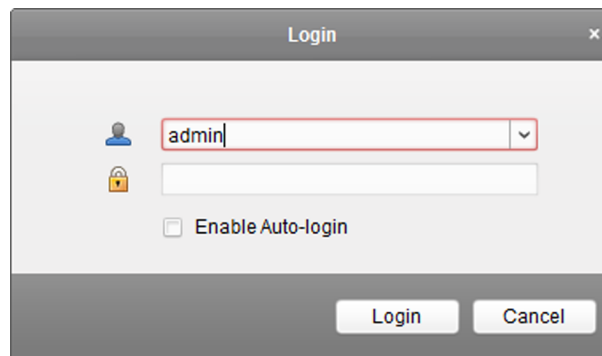
Figure 2-2 Login

2. Input the user name and password you registered.
3. **Optional:** Check **Enable Auto-login** checkbox to log in to the software automatically for next running.
4. Click **Login** to log in to the client software.

   After logging in to 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 Resource Management

You can manage devices on the client, including adding, editing, and deleting the devices. You can also perform operations such as checking device's online users and checking devices' QR codes.

3.1 Add Device

After running the client, 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.

After adding device(s), you can select a device and click **Remote Configuration** to configure further parameters of the selected device if needed. You can also

Note
- 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 details about the settings, refer to the user manual of the devices.

After adding access control devices and CVR, you can 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 Activate Devices

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

Perform this task to activate device.

Steps
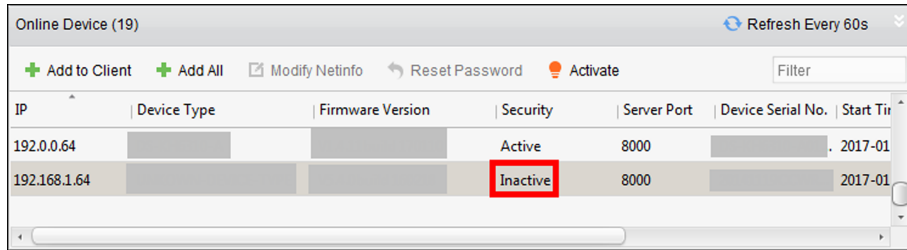
Note
This function should be supported by the device.

1. Enter the Device Management page.

2. Check the device status (shown on **Security** column) and select an inactive device on the **Device for Management** or **Online Device** area.

Figure 3-1 Online Device

3. Click **Activate** to open the Activation dialog.
4. Create a password in the password field, and confirm the password.

⚠ **Caution**

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: 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.

---

5. **Optional:** For the NVR device connecting with the inactive network camera(s), create a password in **IPC default password** field for activating the network camera(s) via NVR.
6. **Optional:** Enable Cloud P2P service when activating the device if the device supports.
   1) Check **Enable Cloud P2P** to open the Note dialog.
   2) Create a verification code.
   3) Confirm the verification code.
   4) Click **Terms of Service** and **Privacy Policy** to read the requirements.
   5) Click **OK** to enable the Cloud P2P service.
7. Click **OK** to activate the device.

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

3.1.2 Add Online Device

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

Add Single Online Device

You can add single online device to the client software.

Perform this task to add single online device to the client software.

Steps
1. Enter the Device Management module.
2. Click **Device** tab and select **Device** as the device type to display the **Online Device** area.

Figure 3-2 Online Device

3. Select an online device from the **Online Device** area.

> 🛈**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 **Activate Devices** .

4. Click **Add to Client** to open the device adding window.
5. 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

   The default value is 8000.

   User Name

   By default, the user name is admin.

   Password

   Input the device password.

> ⚠**Caution**
>
> The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: 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.

6. **Optional:** Check **Synchronize Device Time** to synchronize the device time with the PC running the client after adding the device to the client.
7. **Optional:** Check **Export to Group** to create a group by the device name.

☐**i**Note

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

8. **Optional:** Add the offline devices.
   1) Check **Add Offline Device**.
   2) Input the required information, including the device channel number and alarm input number.
   3) Click **Add**.

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

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

Add Multiple Online Devices

You can add multiple online devices to the client software.

Perform this task if you need to add multiple online devices to the client software.

Steps
1. Enter the Device Management module.
2. Click **Device** tab and select **Device** as the device type to display the **Online Device** area.
3. Click and hold **Ctrl** key to select multiple devices.

☐**i**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 **Activate Devices** .

4. Click **Add to Client** to open the device adding window.
5. Input the required information.

   User Name

   By default, the user name is admin.

   Password

   Input the device password.

⚠ **Caution**

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: 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.

6. **Optional:** Check **Synchronize Device Time** to synchronize the time of the devices with the PC running the client after adding the devices to the client.
7. **Optional:** Check **Export to Group** to create a group by the device name.

📖 **Note**

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

8. Click **Add** to add the devices.

Add All Online Devices

You can add all online devices to the client software.

Perform this task if you need to add all online devices to the client software.

Steps
1. Enter the Device Management page.
2. Click **Device** tab and select **Device** as the device type to display the **Online Device** area.
3. Click **Add All** to open the device adding window.

📖 **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 ***Activate Devices*** .

4. Input the user name and password.

   User Name

   By default, the user name is admin.

   Password

   Input the device password.

⚠ **Caution**

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least

three kinds of following categories: 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.

5. **Optional:** Check **Synchronize Device Time** to synchronize the time of the devices with the PC running the client after adding the devices to the client.
6. **Optional:** Check **Export to Group** to create a group by the device name.

⌷[i]**Note**

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

7. Click **Add** to add the devices.

3.1.3 Add Device by IP Address or Domain Name

You can add device by IP address or domain name.

Perform this task if you need to add device by IP address or domain name.

Steps
1. Open the Device Management module.
2. Click **Device** tab and select **Device** as the device type.
3. Click **Add** to open the Add window.
4. Select **IP/Domain** as the adding mode.
5. Input the required information, including nickname, IP address, port number, user name, and password.

   Address

   Input the device IP addresss 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.

⚠**Caution**

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at

least three kinds of following categories: 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.

6. **Optional:** Check **Synchronize Device Time** to synchronize the device time with the PC running the client after adding the device to the client.
7. **Optional:** Check **Export to Group** to create a group by the device name.

   ⌐i̚**Note**

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

8. **Optional:** Add the offline devices.
   1) Check **Add Offline Device**.
   2) Input the required information, including the device channel number and alarm input number.
   3) Click **Add**.

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

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

3.1.4 Add Devices by IP Segment

If you want to add devices of which the IP addresses are within an IP segment, you can specify the start IP address and end IP address, user name, password, and other parameters to add them.

Perform this task when you need to add devices to the client by IP segment.

Steps
1. Enter the Device Management module.
2. Click **Device** tab and select **Device** as the device type.
3. Click **Add** to open the Add window.
4. Select **IP Segment** as the adding mode.
5. 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

By default, the user name is admin.

Password

Input the device password.

⚠️**Caution**

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: 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.

6. **Optional:** Check **Synchronize Device Time** to synchronize the device time with the PC running the client after adding the device to the client.
7. **Optional:** Check **Export to Group** to create a group by the device name.

ℹ️**Note**

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

8. **Optional:** Add offline devices to the client.
   1) Check **Add Offline Device**.
   2) Input the required information, including the device channel number and alarm input number.
   3) Click **Add**.

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

3.1.5 Add Device by Cloud P2P

You can add the devices to the client via Cloud P2P domain.

Before You Start
Add the devices to Cloud P2P account first.

Perform this task when you need to add device by Cloud P2P domain.

Steps
1. Log in to the Cloud P2P account.
2. Open the Device Management module.
3. Click **Device** tab and select **Device** as the device type.
4. Click **Add** to open the Add window.
5. Select **Cloud P2P** as the adding mode.

The device(s) under the Cloud P2P account will be displayed.

6. Select the device(s).
7. Input the device user name and password.

> ☐**i** **Note**
>
> By default, the device user name is admin and the password is created when you activate the device.

8. **Optional:** Check **Synchronize Device Time** to synchronize the device time with the PC running the client after adding the device to the client.
9. **Optional:** Check **Export to Group** to create a group by the device name.

> ☐**i** **Note**
>
> By default, you can import all the channels of the device to the corresponding group.

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

3.1.6 Add Device by EHome Account

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 *Set Network Parameters* .

Perform this task if you need to add devices by EHome account.

Steps
1. Enter the Device Management module.
2. Click **Device** tab and select **Device** as the device type.
3. Click **Add** to open the Add window.
4. Select **EHome** as the adding mode.
5. Input the required information.

   Account

   Input the account name registered on EHome protocol.

6. **Optional:** Check **Synchronize Device Time** to synchronize the device time with the PC running the client after adding the device to the client.
7. **Optional:** Check **Export to Group** to create a group by the device name.
8. **Optional:** Add the offline devices.
   1) Check **Add Offline Device**.
   2) Input the required information, including the device channel number and alarm input number.
   3) Click **Add**.

> **ℹ Note**
>
> When the offline device comes online, the software will connect it automatically.

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

3.1.7 Add Device by Serial Port

You can add access control device connected via serial port.

Perform this task when you need to add access control device by serial port.

Steps
1. Open the Device Management module.
2. Click **Device** tab and select **Device** as the device type.
3. Click **Add** to open the Add window.
4. Select **Serial Port** as the adding mode.
5. Input the required information.

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.

6. Optional: Check **Synchronize Device Time** to synchronize the device time with the PC running the client after adding the device to the client.

7. Optional: Check **Export to Group** to create a group by the device name.

> **ℹ Note**
>
> By default, you can import all the channels of the device to the corresponding group.

8. Optional: Add offline devices to the client.
1) Check **Add Offline Device**.
2) Input the required information, including the device channel number and alarm input number.
3) Click **Add**.

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

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

3.1.8 Add Device by IP Server

You can add device by IP server.

Perform the following steps to add device by IP server.

Steps
1. Open the Device Management module.
2. Click **Device** tab and select **Device** as the device type.
3. Click **Add** to open the Add window.
4. Select **IP Server** as the adding mode.
5. Input the required information.

   Server Address

   Input the IP address of the PC that installs the IP Server.

   User Name

   Input the device user name. By default, the user name is admin.

   Password

   Input the device password.

   ⚠️**Caution**

   The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: 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.

   ---

6. **Optional:** Check **Synchronize Device Time** to synchronize the device time with the PC running the client after adding the device to the client.
7. **Optional:** Check **Export to Group** to create a group by the device name.

   📖**Note**

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

   ---

8. **Optional:** Add the offline devices
   1) Check **Add Offline Device**.
   2) Input the required information, including the device channel number and alarm input number.
   3) Click **Add**.

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

3.1.9 Add Device by HiDDNS

You can add device by HiDDNS.

Perform this task to add the device by HiDDNS.

Steps
1. Open the Device Management module.
2. Click **Device** tab and select **Device** as the device type.
3. Click **Add** to open the Add window.
4. Select **HiDDNS** as the adding mode.
5. Input the required information.

   Server Address

   http://www.hiddns.com

   Device Domain Name

   Input the device domain name registered on HiDDNS server.

   User Name

   Input the device user name.

   Password

   Input the device password.

   ⚠️**Caution**

   The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: 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.

6. **Optional:** Check **Synchronize Device Time** to synchronize the device time with the PC running the client after adding the device to the client.
7. **Optional:** Check **Export to Group** to create a group by the device name.

   ⓘ**Note**

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

8. **Optional:** Add offline devices.
   1) Check **Add Offline Device**.
   2) Input the required information, including the device channel number and alarm input number.
   3) Click **Add**.

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

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

3.2 Edit Device's Network Information

After activating device, you can edit the network information for the online device.

Before You Start

Activate the device if the device status is inactivated.

Perform this task if you want to edit the network information of activated online device.

Steps

1. Enter Device Management page.
2. Select an activated device in **Online Device** area.
3. Click **Modify Netinfo** to open the Modify Network Parameter window.

> [i]**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.

4. Change the device IP address to the same subnet with your computer.
   - Edit the IP address manually.
   - Check **DHCP**.
5. Input the password created when you activate the device.
6. Click **OK** to complete the network settings.

3.3 Restore/Reset Device Password

If you forgot the password of the detected online devices, you can restore the device's default password or reset the device's password through the client .

3.3.1 Reset Device Password

If you forgot the password of the detected online devices, you can reset the device password through the client.

Perform this task if you want to reset the device password.

Steps

1. Enter the Device Management module.

   All the online devices in the same subnet will display in the Online Device list.

2. Select the device from the list and click **Reset Password**.
3. Reset the device password.

- If the window with Export button, password, and confirm password field pops up, click
  Export to save the device file on your PC and then send the file to our technical support.

[i] **Note**

For the following operations for resetting the password, contact our technical support.

- If the window with **Export** and **Generate** buttons, password and confirm password field pops
  up, click **Generate** to pop up the QR Code window and click **Download** to save the QR code
  to your PC. You can also take a photo of the QR code to save it to your phone. Send the
  picture to our technical support.

[i] **Note**

For the following operations for resetting the password, contact our technical support.

- If the window with safe mode selectable pops up, select the Safe Mode according to actual
  needs.

[i] **Note**

For the following operations for resetting the password, contact our technical support.

⚠ **Caution**

The password strength of the device can be automatically checked. We highly recommend you
change the password of your own choosing (using a minimum of 8 characters, including at least
three kinds of following categories: 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.

3.3.2 Restore Device's Default Password

For some old version device, if you forgot the password of the detected online devices, you can
restore the device's default password through the client.

Perform this task if you want to restore the device password to the default one for the old version
device.

Steps
1. Enter the Device Management module.

   All the online devices in the same subnet will display in the Online Device list.

2. Select the device from the list and click **Reset Password**.
3. Restore the device password.
   - 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.

⌷**i**⌷**Note**

For getting the security code, contact our technical support.

- If the window with **Import** and **Export** buttons pops up, click **Export** to save the device file on your PC and send the file to our technical support.

⌷**i**⌷**Note**

For the following operations for resetting the password, contact our technical support.

What to do next

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.

⚠**Caution**

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: 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.

3.4 Check Device's Online Users

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.

Perform this task if you need to check the device's online users.

Steps

⌷**i**⌷**Note**

This function should be supported by the device.

1. Enter the Device Management page.
2. Click **Device → Device** to display the device list
3. Select an added and online device.
4. Click **Online Users** to open the Online User window.
5. View the information of the users that log into the device.
6. Click **OK** to close the window.

3.5 Check Device's QR Code

The client can generate the QR code of the added devices. 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.

Perform this task to check device's QR code.

Steps
1. Open the Device Management page.
2. Click **Device → Device** to display the device list.
3. View a single device's QR code.
   - Double-click a device in the device list or select a device and click **Modify**to show the device information and QR code.
   - Select a device and click **QR Code** to open the QR code window.
4. **Optional:** Hold **Ctrl** key and select multiple devices, and click **QR Code** to pop up the QR code window of multiple devices.

What to do next
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 user manual of the mobile client software.

3.6 Import Devices in a Batch

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

Perform this task to import devices in a batch.

Steps
1. Enter the Device Management page
2. Click **Device → Device → Add** to open the adding device window.
3. Select **Batch Import** as the adding mode.
4. Click **Export Template** and then save the pre-defined template (CSV file) on your PC.
5. 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 Cloud P2P.

   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.hiddns.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.

⚠️**Caution**

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: 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.

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.

Cloud P2P Account

If you set *6* as the adding mode, input the Cloud P2P account.

Cloud P2P Password

If you set *6* as the adding mode, input the Cloud P2P account password.

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

3.7 Upgrade Device Firmware Version

When there is a new firmware version for the added network camera, you can upgrade the firmware version via the client.

Perform this task if you need to upgrade the added device's firmware version.

Steps
1. Enter the Device Management interface and click **Device** tab.
2. On the Device for Management panel, if there is a new firmware version available, the status in the Firmware Upgrade column of the device will turn to **Upgradeable**.

Figure 3-3 Upgrade Device Firmware Version

⎿**Note**

Status in the Firmware Upgrade column: **None** (no upgrade server added in the client), **Network Disconnected** (cannot connect to the upgrade server), **Upgradeable** (a new firmware version available), **Not Upgradeable** (no firmware version available), **Waiting** (wait for upgrade), **Upgraded**, and **Upgrading Failed**.

---

3. **Optional:** Move the cursor to the to view the current version, latest version, and upgrade content of the firmware version.
4. Select the upgradeable device and click **Upgrade** to start upgrading the device firmware.

   The upgrade progress will show. When the upgrade is completed, the status in the Firmware Upgrade column of the device will turn to **Upgraded**.

Chapter 4 Group Management

The resources added should be organized into groups for convenient management, such as encoding channels, alarm inputs, alarm outputs, zones, access control points, and lane controllers. You can get the live view, play back the video files, and do some other operations of the device through the group.

4.1 Add Group

You can add group to organize the added device for convenient management.

Perform this task if you need to add group for managing device.

Steps
1. Click **Device Management → Group** to enter the group management page.
2. Click to open the Add Group dialog.
3. Set the group name.
   - Create a group name as you want in the **Group Name** field.
   - Check **Create Group by Device Name** to create the new group by the name of the selected device.
4. Click **OK** to add the new group to the group list.

4.2 Import Resources to Group

You can import the device resources (such as encoding channels, alarm input, alarm outputs, etc.) to the added group in a batch.

Before You Start
Add a group for managing devices. Refer to *Add Group* .

Perform this task if you want to import the device resources to group. Here we take importing the device's encoding channels to group as an example.

Steps

 Note

Up to 256 encoding channels can be added to one group.

1. Click **Device Management → Group** to enter the group management page.
2. Click **Import**.
3. Click **Encoding Channel** tab to enter Import Encoding Channel page.
4. Select the thumbnails/names of the cameras in the thumbnail/list view.

> **ⓘ Note**
>
> You can click ▦ or ▤ to switch the camera display mode to thumbnail view or to list view.

5. Select a group from the group list.

> **ⓘ Note**
>
> You can click ⊕ to add a new group if there is no required group in the list.

6. Import encoding channels to group.
- Click **Import** to import the selected encoding channels to the selected group.
- Click **Import All** to import all the encoding channels to the selected group.
- Click 🗂 to create a new group named as device name and directly import the corresponding encoding channels to group.

4.3 Edit Channel Parameters

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.

Before You Start

Import the channels to group. Refer to *Import Resources to Group* .

Perform the following steps to edit the parameters of the channels imported to group. Here we take modifying the encoding channel's parameters as an example.

Steps

> **ⓘ Note**
>
> For modifying the camera(s) of Cloud P2P device, refer to *Edit Camera Parameters* .

1. Click **Device Management → Group** to enter the group management page.

All the added groups are displayed on the left.

2. Click **Encoding Channel** in the group.

The encoding channels imported to the group will display.

3. Open the Modify Camera dialog.
- Double click the encoding channel.
- Select the encoding channel and click **Modify**.

4. Edit the camera information, including the camera name, the 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

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.

Note

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.

4.4 Remove Channel from Group

You can remove the added channels from the group.

Perform the following steps to remove the added channels from the group. Here we take encoding channel as an example.

Steps

1. Click **Device Management → Group** to enter the group management page.

    All the added groups are displayed on the left.

2. Click **Encoding Channel** in the group.

    The encoding channels imported to the group will display.

3. Select the encoding channel and click **Delete** to remove the camera from the group.

4. **Optional:** Remove all the encoding channels from the group.
    1) Click **Import**.

        All the groups and the encoding channels in the groups will display.
    2) Move the mouse to the group.
    3) Click ✖ near the group name to remove all the cameras from the group.

4.5 Delete Group

You can delete the group if needed.

Perform the following steps to delete the group.

Steps

1. Click **Device Management → Group** to enter the group management page.
2. Delete the group.
    - Select the group and click 🗑 .
    - Move the mouse to the group and click ✖ .

    The selected group and the resource in it will be deleted.

Chapter 5 Live View

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.

The following icons show different statuses of the camera.

	The camera is online and works properly.
	The camera is in live view.
	The camera is in recording status.
	The camera is offline.
	Event (e.g., motion detection) is detected for the camera. The group icon will turn to .
	The camera is offline, the client can still get the live video via the stream media server if the stream media server is configured. For configuring the stream media server of the camera, refer to *Forward Video Stream through Stream Media Server* .

5.1 Start and Stop Live View

You can start the live view of one camera or all cameras in a group. You can also start the live view in default or custom view mode.

5.1.1 Start Live View for One Camera

You can start the live view of only one camera.

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

Perform this task if you want to start the live view of one camera.

Steps
1. Open the Main View page.
2. **Optional:** Click in live view toolbar to select the window division mode for live view.
3. **Optional:** Click to set the view scale of the live view window. You can set it as **Full Screen**, **4:3**, **16:9**, or **Original Resolution**.

Note

You can also set the view scale for both live view and playback window in System Configuration. For details, refer to *Set Image Parameters* .

4. Do one of the following operations to start the live view of one camera.
   - Drag a camera in the group from camera list to a display window to start the live view.
   - Double-click the camera name after selecting a display window to start the live view.

Note

For Cloud P2P device, if the live view or video file(s) of its camera(s) is encrypted, you should input the stream key.

5. **Optional:** Drag the video of the camera in live view to another window to change the display window for live view.
6. **Optional:** Right click on the camera name in the camera list to switch the stream type according to actual needs.

Note

You can click **All Stream Types** to select the frequently used stream types to display on the right-click menu.
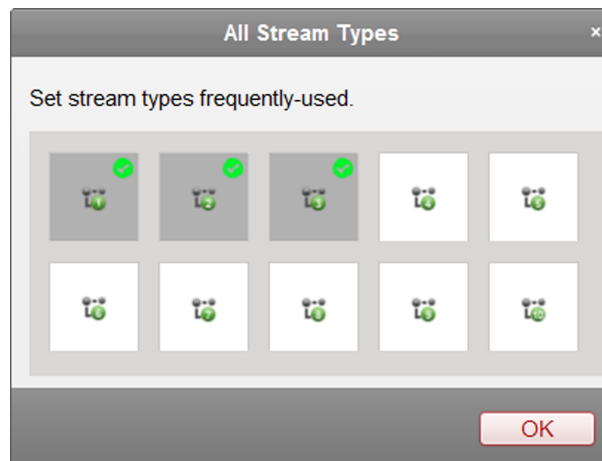
Figure 5-1 Select Frequently Used Stream Types

5.1.2 Start Live View for Camera Group

You can start the live view for all cameras in one group synchronously.

Before You Start

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

Perform this task when you want to start live view for camera group.

Steps
1. Open the Main View page.
2. **Optional:** Click ▣ ◄ⁿ Original Resolu... ▾ ⊙ to set the view scale of the live view window. You can set it as **Full Screen**, **4:3**, **16:9**, or **Original Resolution**.

> ⓘ**Note**
>
> You can also set the view scale for both live view and playback window in System Configuration. For details, refer to *Set Image Parameters* .

3. Perform one of the following operations to start the live view of all cameras in a group.
   - Drag a camera group from camera list to the display window to start the live view.
   - 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.

4. **Optional:** Right click on the group name in the camera list to switch the stream type for the cameras in the group.

> ⓘ**Note**
>
> Before switching to the sixth, seventh, eighth, ninth, and tenth stream, you should set these stream type in the device's web configuration page. For details, refer to the user manual of the device.

5.1.3 Start Live View in Default View Mode

The video of the added cameras can display in different view modes. Four frequently-used default view modes are selectable: 1-Window, 4-Windows, 9-Windows, and 16-Windows.

Perform this task when you want to start live view in default view mode.

Steps
1. Open the Main View page.
2. Click ➕ to expand the default view list in the View panel.
3. Select the default view mode.

   The video of the added cameras displays in a sequence in the selected view.
4. **Optional:** Click ▣ ◄ⁿ Original Resolu... ▾ ⊙ to set the view scale of the live view window. You can set it as **Full Screen**, **4:3**, **16:9**, or **Original Resolution**.

> ⓘ**Note**
>
> You can also set the view scale for both live view and playback window in System Configuration. For details, refer to *Set Image Parameters* .

5. **Optional:** Perform the following operation(s) after starting live view in default mode.

| Start Instant Playback | Move the cursor over the view and click ◀ to start the instant playback of the view, see *Instant Playback* for details. |
| Start Auto-Switch | Move the cursor over the view and click ⟳ to start switching automatically of the view, see details in ***Auto-Switch in Live View*** . |

5.1.4 Add Custom View

You can customize the view mode for live view.

Perform this task when you want to add custom view for live view.

Steps
1. Open the Main View page.
2. Click ✚ in the View panel to create a new view.
3. Input a name for the view as desired.
4. Click **Add** to add the view.
5. **Optional:** Click ▦ in the live view toolbar to set window division mode for the new view.

> 📖**Note**
> By default, the new view is in 4-window division.

6. Perform one of the following operations to save the new view settings.
   - Click ▤ to directly save the view.
   - Click ▥ to save the view as another custom view.
7. **Optional:** Perform the following operations after adding the custom view.

| Edit View Name | Move the cursor over the new view and click ✎ to edit the view name. |
| Delete View | Move the cursor over the new view and click ✖ to delete the view. |
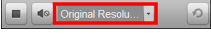
5.1.5 Start Live View in Custom View Mode

You can display the video of added cameras in custom view mode.

Before You Start
Customize view modes and add them to the client software, see ***Add Custom View*** for details.

Perform this task when you want to start live view in custom view mode.

Steps
1. Open the Main View page.
2. **Optional:** Click ▣ ◀ Original Resolu... ⟳ to set the view scale of the live view window. You can set it as **Full Screen**, **4:3**, **16:9**, or **Original Resolution**.

📖**Note**

You can also set the view scale for both live view and playback window in System Configuration. For details, refer to *Set Image Parameters* .

---

3. Click ➕ to expand the custom view list in the View panel.
4. Select a custom view.
5. Perform one of the following operations to start live view in custom view mode.
   - Drag camera or camera group to display window to start live view in the selected custom view mode.
   - Double-click camera name or camera group name to start live view in the selected custom view mode.
6. **Optional:** Move the cursor over the view and click ◀ to start instant playback of the view.

5.1.6 Stop Live View

After starting the live view, you can stop it as desired.

Before You Start
Start the live view.

Perform this task when you want to stop the live view.

Steps
1. Select a live view display window on Main View page.
2. Perform one of the following operations to stop the live view.
   - Move the cursor over the display window and click ✖ appeared at the upper-right corner to stop the live view of this display window.
   - Right-click on the display window to open right-click menu and click **Stop Live View** on the menu to stop live view.
   - Click ◼ in live view toolbar to stop all the live view.

5.2 Auto-Switch in Live View

You can auto-switch cameras or views in live view.

When auto-switching in live view, three modes are available:

- Auto-Switch All Cameras in Default View
- Auto-Switch Cameras in a Group
- Auto-Switch Custom Views

5.2.1 Auto-Switch All Cameras in Default View

The video of all the cameras in the camera list can switch automatically in the selected default view.

Perform this task when you need to auto-switch all cameras in default view.

Steps
1. Open the Main View page.
2. Click ⌄ in the toolbar and select or customize the switching interval.
3. Select a default view to click 🔄 on the selected view node.

   All cameras in the camera list start auto-switching in the selected default view.

4. **Optional:** Perform the following operation(s) after starting auto-switching all cameras in the default view.

Pause/Resume Auto-Switch	Click 🔄 / 🔄 to pause/resume auto-switching all cameras in default view.
View Previous/Next Video	Click ← / → to view the live video of previous or next camera.

5.2.2 Auto-Switch Cameras in a Group

The video stream of the cameras from the same group can switch automatically in a selected display window.

Perform this task when you need to auto-switch cameras in a group.

Steps
1. Open the Main View page.
2. Select a display window for auto-switch.
3. Click ⌄ in the toolbar to select or customize the switching interval.
4. Select a group and click 🔄 on the group node.

   The cameras in the selected group starts auto-switch in the display window.

   ⓘ**Note**

   The audio is off by default after auto-switch starts.

5. **Optional:** Perform the following operation(s) after starting auto-switching cameras in a group.

Pause/Resume Auto-Switch	Click 🔄 / 🔄 to pause/resume auto-switching cameras in a group.
View Previous/Next Video	Click ← / → to view the live video of previous or next camera.

5.2.3 Auto-Switch Custom Views

The configured custom views can switch one by one automatically.

Before You Start
Add the custom views, see **Add Custom View** for details.

Perform this task when you need to auto-switch custom views.

Steps
1. Open the Main View page.
2. Click ⌄ in the toolbar and select the switching interval.
3. Click ↻ on the Custom View node.

   All configured custom views starts auto-switching.

4. **Optional:** Perform the following operation(s) after starting auto-switching custom views.

Pause/Resume Auto-Switch	Click ↻ / ⊞ to pause/resume auto-switching custom views.
View Previous/Next Video	Click ← / → to view the live video of previous or next camera.

5.3 PTZ Control

The software provides PTZ control for cameras with pan/tilt/zoom functionality. During the PTZ control, you can set preset, patrol, and pattern, and you can also open a new window for controlling the PTZ.

⌷**Note**
Cloud P2P device only supports the PTZ movement to the directions of up, down, left, and right.

The following icons are available on the PTZ control panel.

Icon	Name	Description
⊡	Manual Tracking	For speed dome with auto-tracking function, enable the auto-tracking (via right-click menu) for it and click the icon to manually track the target by clicking on the video.
≡	Menu	For analog speed dome, click the icon to display its local menu. For detailed operation of the menu, refer to user manual of the speed dome.
⟳	One-Touch Patrol	For speed dome with one-touch patrol function, click the icon and the speed dome starts patrol from the predefined preset No.1 to preset No.32 in order after

Icon	Name	Description
		a period of inactivity (park time). For setting the park time, refer to user manual of the speed dome.
	One-Touch Park	For the speed dome with one-touch park function, click the icon and the speed dome saves 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 park time, refer to user manual of the speed dome.

5.3.1 Configure Preset

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

Perform this task when you need to add a preset for the PTZ camera.

Steps
1. Open the Main View page and start the live view of the PTZ camera.
2. Click ⌃ to expand the PTZ Control panel.
3. Click **Preset** to enter the PTZ preset configuration panel.
4. Click the direction buttons and other buttons on the PTZ control panel to steer the camera to the desired view.
5. Select a PTZ preset number from the preset list and click 🖉 to open a dialog.
6. Input the name of the preset in the dialog.
7. Click **OK**.
8. **Optional:** Perform the following operation(s) after setting the preset

Call Preset	Double-click the configured preset in the list, or select the preset and click ▶ to call the preset. You can also press the number key (e.g., **4**) on keyboard to call the preset 1 to 9, and press **[**, number keys (e.g., **124**), and **]** on keyboard to call the other preset.
Edit Preset	Select the configured preset from the list and click 🖉 to edit it.
Delete Preset	Select the configured preset from the list and click ✖ to delete it.

5.3.2 Configure 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

Add two or more presets for one PTZ camera.

Perform this task when you need to add a patrol for the PTZ camera.

Steps

![i]**Note**

For Cloud P2P device, the patrol function is not supported.

1. Open the Main View page and start the live view of PTZ camera.
2. Click ![icon] to expand the PTZ Control panel.
3. Click **Patrol** to enter the PTZ patrol configuration panel.
4. Select a path No. from the drop-down list.
5. Click ![icon] to open Add Patrol No. dialog.
6. Set the dwell time and patrol speed for the preset in the dialog.
7. Click **OK**.
8. Repeat step 5, 6, and 7 to add other presets to the patrol.
9. **Optional:** Perform the following operation(s) after setting the patrol.

Call Patrol	Click ![icon] to call the patrol.
Stop Calling Patrol	Click ![icon] to stop calling the patrol.
Edit Preset in Patrol	Select a preset in the patrol path and click ![icon] to edit the preset.
Remove Preset from Patrol	Select a preset in the patrol path and click ![icon] to remove the preset from the patrol.

5.3.3 Configure Pattern

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

Perform this task when you need to add a pattern for the PTZ camera.

Steps

![i]**Note**

For Cloud P2P device, the pattern function is not supported.

1. Open the Main View page and start the live view of the PTZ camera.
2. Click ![icon] to expand the PTZ Control panel.
3. Click **Pattern** to enter the PTZ pattern configuration panel.
4. Click ![icon] to start the recording of this pattern path.
5. Use the direction buttons to control the PTZ movement.
6. Click ![icon] to stop recording and save the recorded pattern.
7. **Optional:** Perform the following operation(s) after setting the pattern.

Call Pattern	Click ![icon] to call the pattern.

Stop Calling Pattern	Click ⬛ to stop calling the pattern.
Delete Pattern	Select one pattern and click ✖ to delete the pattern.
Delete All Patterns	Click 🗑 to delete all patterns.

5.4 Manually Record and Capture

During live view, you can record videos and capture pictures manually, and then view the recorded video files and captured pictures in the local PC.

5.4.1 Manually Record Video

Manual recording function allows to record the live video on the Main View page manually, and you can store the video files in the local PC.

Perform this task when you need to record videos manually.

Steps

🛈**Note**

The manual recording is not supported by the Cloud P2P device during live view.

1. Open the Main View page.
2. Start the live view
3. Perform one of the following operations to start manual recording.
   - Move the cursor to the display window in live view to show the toolbar and click ⭕ on the toolbar.
   - Right-click on the display window and click **Start Recording** on the right-click menu.

   The icon ⭕ turns to 🔴. An indicator 🔴 appears in the upper-right corner of the display window.
4. Click 🔴 to stop the manual recording.

   The recorded video file is automatically saved to the local PC, and a small window with the saving path information appears in the lower-right corner of desktop.

   🛈**Note**

   The saving path of the recorded video files can be set on the System Configuration page. See **Set File Saving Path** for details.

5.4.2 View Local Videos

You can view the recorded video files stored in your local PC.

Before You Start

Record the live video.

Perform this task when you need to view the local video files.

Steps

1. Click **File → Open Video File** in the upper-left corner to open the Video Files page.
2. Select the camera to be searched from the Camera Group list.
3. Click ⬚ 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 displays in thumbnail format on the page.

5. **Optional:** Perform the following operation(s) after the search.

Delete Video File	Select the video file, and click **Delete** to delete the video file.
Send Email	Select the video file, and click **Send Email** to send an email notification with the selected video file attached.
	⬚**Note**
	To send an email notification, the email settings need to be configured before proceeding. For details, refer to *Set Email Parameters* .
Save Local Video	Select the video file, and click **Save as** to save a new copy of the video file.
Playback	Double-click the video file to start the local playback.

5.4.3 Capture Pictures

You can capture pictures during the live view.

Perform this task when you need to capture pictures during the live view.

Steps

1. Open Main View page and start the live view of a camera.
2. Perform one of the following operations to capture pictures.
   - Move the cursor to the display window in live view to show the toolbar and click ⬚ on the toolbar.
   - Right-click the display window and click **Capture** on the right-click menu.

   The captured picture is automatically saved to the local PC, and a small window with the picture preview and saving path information appears in the lower-right corner of desktop.

⌐**i**⌐**Note**

The saving path of the captured pictures can be set on the System Configuration page. For details, refer to **Set File Saving Path** .

5.4.4 View Captured Pictures

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

Before You Start
Capture pictures in the live view.

Perform this task when you need to view the captured pictures.

Steps
1. Click **File → Open Image File** in the upper-left corner to open the Captured Images page.
2. Select the camera to be searched from the Camera Group list.
3. Click 📅 to specify the start time and end time for the search.
4. Click **Search**.

   The pictures captured between the start time and end time display in thumbnail format on the page.
5. **Optional:** Perform the following operation(s) after the search.

Enlarge Picture	Double-click the picture thumbnail to enlarge it for a better view.
Print Picture	Select the captured picture, and click **Print** to print the selected picture.
Delete Picture	Select the captured picture, and click **Delete** to delete the selected picture.
Send Email	Select the captured picture, and click **Send Email** to send an email notification with the selected picture attached.
Save Picture	Select the captured picture, and click **Save as** to save a new copy of the selected picture.

5.5 Instant Playback

Instant playback shows a piece of the video which is remarkable, or which is unclear on the first sight. So you can play the video files instantly on the Main View page and get an immediate review if needed.

Before You Start
Record the video files and store them on the storage devices, such as the SD/SDHC cards and HDDs on the DVRs, NVRs, network cameras, etc., or on the storage servers.

Perform this task when you need to start the instant playback.

Steps

1. Open Main View page and start the live view.
2. Perform one of the following operations to show the pre-play durations' list of instant playback.
   - Move the cursor to the display window to show the toolbar and click ⏴ .
   - Right-click the display window and select **Switch to Instant Playback** on the right-click menu.
   - Move the cursor to default view or custom view node on the View panel and click ◀ .

   The list with pre-play durations of 30s, 1 min, 3 min, 5 min, 8 min, and 10 min displays.
3. Select a time period from the appeared list to start the instant playback.

   Example

   If you select 3 min, and the current time of the live view is 09:30:00, then the instant playback will start from 09:27:00.

   During the instant playback, an indicator 🔄 appears in the upper-right corner of the display window.
4. **Optional:** Click ⏴ again to stop the instant playback and go back for the live view.

5.6 Customize Window Division

The client software provides multiple kinds of predefined window divisions. You can also set custom the window division as desired.

Perform this task when you need to customize the window division.

Steps

📖 **Note**

Up to 5 window divisions can be customized.

---

1. Open the Main View or Remote Playback page.
2. Click 🖼 on the live view or playback toolbar.
3. Select **Edit** to open the custom window division page.
4. Click **Add** to open the Add Custom Window Division dialog.
5. Set a name for the new window division as desired and click **OK**.
6. Select the window division as 3×3, 4×4, 5×5, or 6×6.

   📖 **Note**

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

---

7. **Optional:** Drag your mouse to select the adjacent windows, and click **Joint** to joint them as a whole window.
8. Click **Save**.

What to do next
Click ✖ to go back to the Main View or Remote Playback page.

5.7 Live View for Fisheye Camera

For fisheye cameras, you can start the live view in fisheye mode, set presets and patrols, and perform PTZ control.

5.7.1 Perform Live View in Fisheye Mode

You can play the live videos of the camera in fisheye expansion mode.

Perform this task when you need to start live view in fisheye mode for fisheye camera.

Steps
1. Open the Main View page and start the live view of fisheye camera.
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. Select the expanding mode for live view 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 produce curvilinear images of a large area, while distort the perspective and angles of objects in the image.

   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. **Optional:** Perform the following operation(s) after starting live view in fisheye mode.

Capture	Right-click on the window and select **Capture** to capture the picture in the live view process.
Enter Full Screen	Right-click on a playing window and switch the selected window to full-screen mode.

5.7.2 PTZ Control in Fisheye Mode

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

Note

The PTZ panel varies according to different devices.

The following functions are available on the PTZ control panel.

- Select a PTZ window, and click the direction buttons to adjust view angle. Or drag the No. label in the fisheye or panorama window to change the view angle of the PTZ window.
- Select a PTZ window, click ⟳ to start auto-scan, and click it again to stop auto-scan.
- Drag the slider on ━━━━━━━ + to adjust the speed for PTZ movement.
- Click + or ━ , or scroll the mouse wheel to zoom in or zoom out the selected PTZ window.

Configure Preset

In fisheye mode, you can configure the preset which is a user-defined monitor position/point and simply call the preset No. to change the monitor scene to the defined position.

Perform this task when you need to configure preset in fisheye mode.

Steps

Note

Only the specific fisheye cameras support configuring the preset, and up to 256 presets can be configured in fisheye mode.

1. Open Main View page and start the live view of fisheye camera.
2. Right-click on the video and select **Fisheye Expansion** to enter the Fisheye Expansion window.
3. Click **Preset** tab to enter the preset configuration panel.
4. Select a PTZ window and adjust the scene to the place you want to mark as a preset.
5. Click 📝 to open Add Preset window.
6. Input the preset name.
7. Click **OK**.
8. **Optional:** Perform the following operation(s) after configuring the preset.

Call Preset	Select the preset and click ▶ to call the configured preset.
Delete Preset	Select the preset and click ✖ to delete the configured preset.

Configure Patrol

In fisheye mode, you can configure the patrol, which 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
Configure two or more presets.

Perform this task when you need to configure the patrol in fisheye mode.

Steps

___

ⓘ**Note**

Only the specific fisheye cameras support configuring the patrol, and up to 32 patrols can be configured in fisheye mode.

___

1. Open Main View page and start the live view of fisheye camera.
2. Right-click on the video and select **Fisheye Expansion** to enter the Fisheye Expansion window.
3. Click **Patrol** tab to enter the patrol configuration panel.
4. Select a path No. from the drop-down list.
5. Click ➕ to open Add Patrol No. window.
6. Set the dwell time and patrol speed for the preset.

   ___

   ⓘ**Note**

   The dwell time ranges from 1s to 120s and the patrol speed ranges from 1 to 40.

   ___

7. Click **OK**.
8. Repeat step 5, 6, and 7 to add other presets to the patrol.
9. **Optional:** Perform the following operation(s) after configuring the patrol.

Edit Preset in Patrol	Select a preset in the patrol path and click 🖉 to edit the preset.
Remove Preset from Patrol	Select a preset in the patrol path and click 🗑 to remove the preset from the patrol.
Call Patrol	Click ▶ to call the patrol.
Stop Calling Patrol	Click ⏹ to stop calling the patrol.

5.8 Perform Master-Slave Linkage

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

Note

- 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 box or bullet camera.

5.8.1 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, including setting VCA detection rule, linking to a speed dome, and calibrating camera and speed dome.

Set Intrusion Detection Rule

You should set the VCA detection rule for the bullet or box camera, and when the VCA event is triggered, the client can trigger speed dome to track the target. Here we take intrusion detection as an example.

Perform this task to set the intrusion detection rule for the bullet or box camera.

Steps
1. Open Device Management page and select a box or bullet camera.
2. Click **Remote Configuration → VCA Config → Rule → Rule Settings** to enter rule settings page.
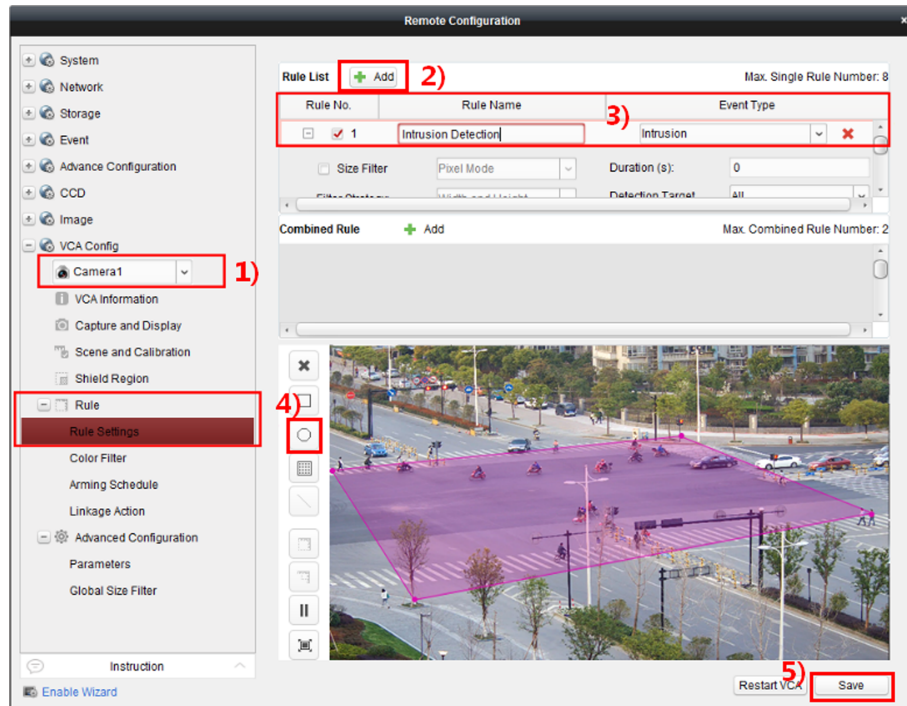
Figure 5-2 Rule Settings

3. Click **Add** in Rule List panel to add a rule.
4. Select **Intrusion** as the event type.
5. Click ⃝ to draw a detection region on the live video.
6. Click **Save**.

Link Speed Dome

When configuring the master-slave tracking for the box or bullet camera, you can link the camera to a speed dome and set the PTZ position for the speed dome for tracking.

Perform this task to link the box or bullet camera to a speed dome for master-slave tracking.

Steps
1. Open Device Management page and select a box or bullet camera.
2. Click **Remote Configuration → Advanced Configuration → Master-Slave Tracking** to enter master-slave tracking settings page.
3. Click **Login** on the display window to open the speed dome login window.
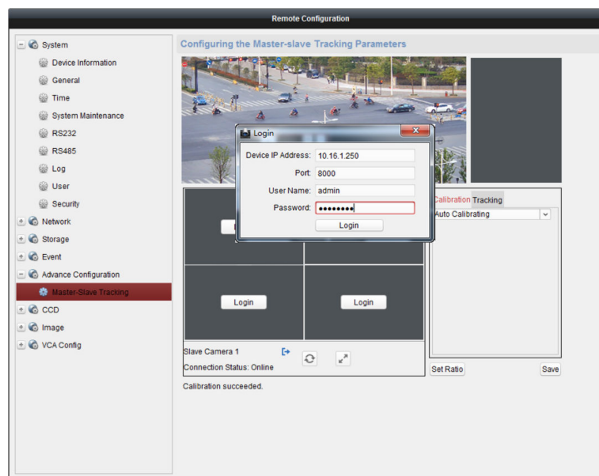
Figure 5-3 Speed Dome Login Window

4. Input the speed dome's IP address, port No., user name, and password.
5. Click **Login** to log in to the speed dome.
6. Click **PTZ** and use the direction arrows to adjust the speed dome to a horizontal position.

What to do next
Calibrate the box or bullet camera and the linked speed dome, see ***Calibrate Camera and Speed Dome Automatically*** or ***Calibrate Camera and Speed Dome Manually*** for details.

Calibrate Camera and Speed Dome Automatically

When setting the bullet or box camera's master-slave tracking rule, you should calibrate the camera and the speed dome. Two calibration modes, including auto and manual, are available, here we introduce the auto calibration.

Before You Start

Link the camera to a speed dome, see *Link Speed Dome* for details.

Perform this task to calibrate the camera and the speed dome automatically.

Steps
1. Open Device Management page and select a box or bullet camera.
2. Click **Remote Configuration → Advanced Configuration → Master-Slave Tracking** to enter master-slave tracking settings page.
3. Select the calibration mode as **Auto Calibrating** in the lower-right corner of Calibration panel.
4. Move and zoom in/out the view of speed dome to make sure the live views of dome and camera are mostly same.
5. Click **Save**.

Calibrate Camera and Speed Dome Manually

When setting the bullet or box camera's master-slave tracking rule, you should calibrate the camera and the speed dome. Two calibration modes, including auto and manual, are available, here we introduce the manual calibration.

Before You Start

Link the camera to a speed dome, see *Link Speed Dome* for details.

Perform this task to calibrate the camera and the speed dome manually.

Steps
1. Open Device Management page and select a box or bullet camera.
2. Click **Remote Configuration → Advanced Configuration → Master-Slave Tracking** to enter master-slave tracking settings page.
3. Select the calibration mode as **Manual Calibrating** in the lower-right corner of Calibration panel.
4. Select site 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.
5. Repeat step 4 to add other manual calibration sites.
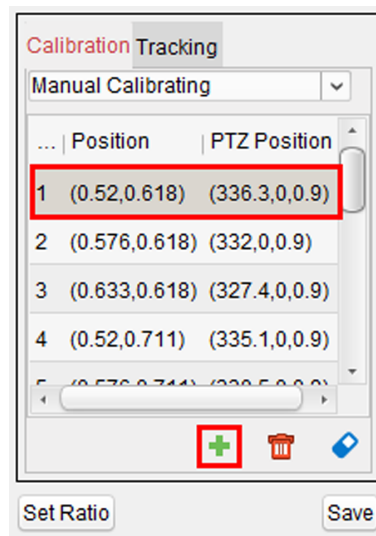
Figure 5-4 Calibration Sites

6. Adjust the distances among the four calibration sites evenly in the live view page.
7. Select the calibration site No. 1.

   The digital zoom view of site No. 1 appears at the right.

8. Move and zoom in or out the view of speed dome to make sure the live views of speed dome and the digital zoom view of selected site are mostly same.
9. Click ⊕ to save the current site position information.
10. Repeat step 7, 8, and 9 to set other sites' position.
11. Click **Save**.

5.8.2 Enable Master-Slave Tracking

During live view, you can enable the master-slave tracking to locate or track the target appeared in the view of bullet or box camera with a speed dome.

Before You Start
Configure the master-slave tracking rules for the box or bullet camera.

Perform this task when you need to enable the master-slave tracking for box or bullet camera.

Steps
1. Enter the Main View page and start the live view of box or bullet camera.
2. Right-click on the live view window and click **Enable Master-Slave Tracking**.

   When the configured VCA rule is triggered by target, the linked speed dome performs the automatic master-slave tracking and the target frame turns from green into red.

5.9 Live View for Thermal Camera

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

5.9.1 View Fire Source Information during Live View

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

Before You Start

Configure the alarm rules for the thermal device, see the user manual of the device for details.

Perform this task when you need to view the fire source information during live view.

Steps

1. Enter Main View page and start the live view of a thermal camera.

> ⓘ**Note**
>
> For starting and stopping live view, refer to *Start Live View for One Camera* and *Stop Live View* .

2. Right-click on the live view image and select **File Source Information** in the right-click menu to show the list of information types.

3. Select a information type in the list to display the information.

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.
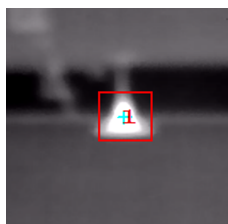
Figure 5-5 Fire Source Information on Live View Image

5.9.2 Show Temperature Information on Live View Image

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, see the user manual of the device for details.

Perform this task when you need to show the temperature information on the live view image.

Steps
1. Enter Main View page and start the live view of a thermal camera.

   ⚓**Note**

   For starting and stopping live view, refer to *Start Live View for One Camera* and *Stop Live View* .

2. Adjust the scene to the area configured with temperature measurement rule.
3. Right-click on the live view image and select **Show Temperature Information** in the right-click menu.

   The temperature displays on the live view image.
4. Click on the image to view the detailed temperature information.
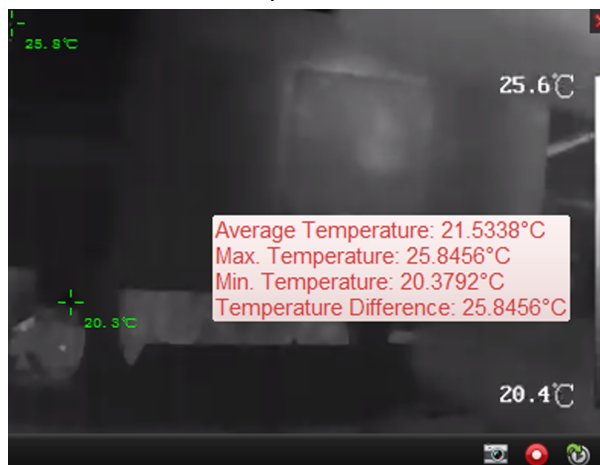
Figure 5-6 Temperature Information on Live View Image

5. **Optional:** Right-click on the live view image and select **Hide Temperature Information** to hide the temperature information.

5.9.3 Manually Measure Temperature

During the live view of thermal camera, you can draw points or frames on the live view image to get the temperature of point or region.

ℹ️**Note**

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

Manually Measure Temperature on Points

During the live view of thermal camera, you can draw points on the live view image to measure the temperature on different points.

Perform this task when you need to measure temperature on points manually.

Steps

1. Enter Main View page and start the live view of a thermal camera.

   ℹ️**Note**

   For starting and stopping live view, refer to *Start Live View for One Camera* and *Stop Live View* .

2. Perform one of the following operations to select the temperature measurement type.
   - Right-click on the live view inage and select **Manual Temperature Measurement → By Point** .
   - Click 🖼 on the live view toolbar and select **By Point**.
3. Click on the live view image to draw the points.

Figure 5-7 Temperature Measurement on Points

The temperatures of the configured points show on the image beside the points.

4. **Optional:** Perform the following operation(s) after measuring temperature on points manually.

Delete Point	Click **Cancel** and click a drawn point on the live view image to delete.
Hide Temperature	Right-click on the live view image and select **Disable Manual Temperature Display** on the right-click menu.

Manually Measure Temperature in Area

During the live view of thermal camera, you can draw frames on the live view image to measure the temperature in different areas.

Perform this task when you need to measure temperature in area manually.

Steps
1. Enter Main View page and start the live view of a thermal camera.

   $\boxed{i}$**Note**

   For starting and stopping live view, refer to ***Start Live View for One Camera*** and ***Stop Live View*** .

2. Perform one of the following operations to select the temperature measurement type.
   - Right-click on the live view inage and select **Manual Temperature Measurement → By Frame** .
   - Click ![icon] on the live view toolbar and select **By Frame**.
3. Click on the live view image to draw the area frames.
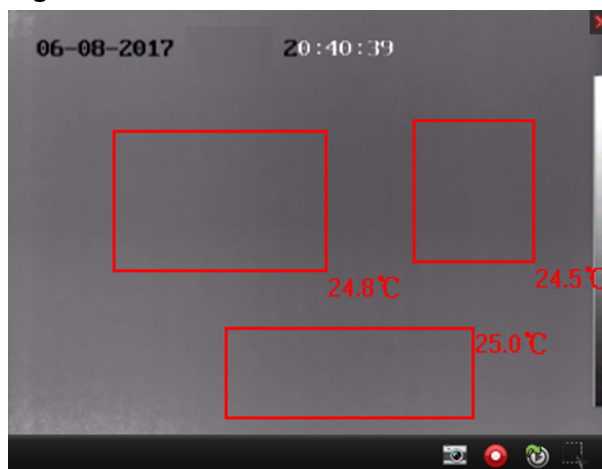
Figure 5-8 Temperature Measurement in Areas

The average temperatures of the drawn areas show on the live view image beside the areas.
4. **Optional:** Perform the following operation(s) after measuring temperature in areas manually.

Delete Point	Click **Cancel** and click a drawn area on the live view image to delete.
Hide Temperature	Right-click on the live view image and select **Disable Manual Temperature Display** on the right-click menu.

5.10 More Functions

There are some more functions supported in the live view, including auxiliary screen preview, digital zoom, channel-zero, two-way audio, camera status, and synchronization.

Auxiliary Screen Preview

Display the live video on different auxiliary screens for the convenient preview of multiple monitoring scenes.

⌷**Note**

Up to 3 auxiliary screens are supported.

Digital Zoom

Drag the mouse to draw a rectangle area in the lower-right/upper-left direction to zoom in or out the drawn area. Or use the mouse wheel to zoom in or out the view in digital zoom mode.

Channel-Zero

For the channel-zero of the device, 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 a channel to start two-way audio.

⌷**Note**

- The two-way audio can be used for only one camera at one time.
- Cloud P2P 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 checking. 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 6 Remote Storage Configuration

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

6.1 Store Picture and Video on DVR, NVR, or Network Camera

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 and picture files. You can set a recording schedule or capture schedule for the channels of the local devices.

Before You Start
The newly installed storage devices should 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.

Perform this task when you need to store the picture and video files on the encoding device such as DVR, NVR, or network camera.

Steps

📖**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.

---

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

Figure 6-1 Enable Local Recording or Capture

4. Select the recording or capture schedule template from the drop-down list.
   All-day Template

     All-day continuous recording.

   Weekday Template

     Working-hours continuous recording from 8:00 AM to 8:00 PM.

   Event Template

All-day event triggered recording.

Template 01 to 08

Fixed templates for specific schedules. You can edit the templates if needed.

Custom

Customize a template as you want.

⌊i⌋**Note**

If you need to edit or customize the template, refer to *Configure Recording Schedule Template* or *Configure Capture Schedule Template* .

5. Click **Advanced Settings** of Recording Schedule to set the recording advanced parameters.

⌊i⌋**Note**

The displayed items vary according to the devices.

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 Video 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 Recording

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.

⌊i⌋**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 *Normal Playback* for stream switch during playback.

6. Click **Advanced Settings** of Capture Schedule to set the capture advanced parameters.

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.

7. **Optional:** Click **Copy to...** to copy the recording schedule settings to other channels.
8. Click **Save** to save the settings.

6.2 Store Picture and Video on Storage Device

You can store the video files and pictures of the added encoding devices on storage device.

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 Guarding Vision Storage Server, CVR (Center Video Recorder), or other NVR.

Here we take the settings of Guarding Vision Storage Server as an example.

Note

The Guarding Vision Storage Server application software needs to be installed and it is packed in the client installation package. After running the installation package, select **Storage Server** to enable the installation of Guarding Vision Storage Server.

6.2.1 Activate Storage Server

If it is the first running the Guarding Vision Storage Server, you are required to active the storage server.

Perform this task when you need to activate storage server.

Steps

1. Click 📠 on the desktop to run the Guarding Vision Storage Server.
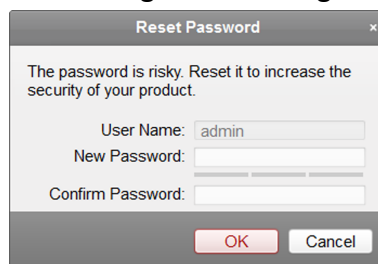
Figure 6-2 Reset Password for Storage Server

📖ℹ️**Note**

- If the storage server port (value: 8000) is occupied by other service, a dialog will pop up. You should change the port No. to other value to ensure the proper running of the storage server.
- You can also record the video files on the Guarding Vision Storage Server installed on another PC.

2. Input the **New Password** and **Confirm Password**.

⚠️**Caution**

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: 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.

3. Click **OK** to change the password.

After changing the password, the storage server will run automatically.

6.2.2 Add Storage Server to Client

You can add storage server to the client for storing the video files and pictures of the added encoding devices.

Perform this task when you need to add storage server.

Steps
1. Open the Device Management page.
2. Click **Device**.
3. Click **Device** to display the device list.
4. Add Guarding Vision Storage Server.
- You can add online storage server. For details, refer to ***Add Single Online Device*** .
- You can add storage server via IP address or domain name. For details, refer to ***Add Device by IP Address or Domain Name***

6.2.3 Format Storage Server's HDD

You should format the HDDs of the storage server for the video file and picture storage.

Perform this task to format storage server's HDD.

Steps

ⓘ**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.

1. Open the Device Management page.
2. Click **Device**.
3. Select the added storage server from the list.
4. Click **Remote Configuration**.
5. Click **Storage → General** to enter the HDD Formatting window.
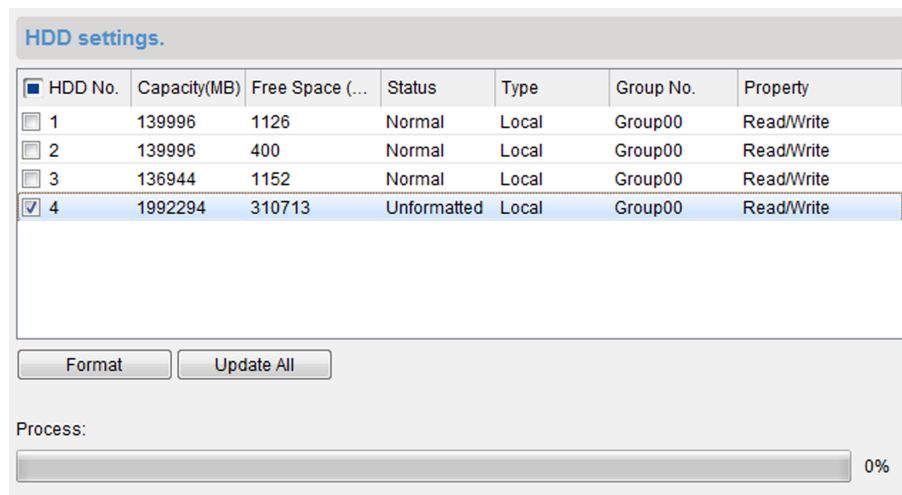
Figure 6-3 HDD Formatting

6. 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**.

6.2.4 Configure Storage Settings

When the storage server is available, you can set the recording schedule or capture schedule for the cameras.

Before You Start

The newly installed storage devices need to be formatted.

Perform this task when you need to configure storage settings.

Steps

1. Click **Storage Schedule** on the control panel to open the Storage Schedule page.
2. Select the camera in the Camera Group list.
3. Select a 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 **Recording Schedule** or **Picture Storage** to enable storing the video files or alarm pictures of the camera when event occurs.
5. **Optional:** For the network cameras with the function of heat map or people counting, check **Additional Information Storage** and click **VCA Config** to set the VCA rule for the camera.

Note

For detailed configuration about setting the VCA rule, refer to user manual of the camera.

You can upload the heat map, people counting data, and road traffic data to the storage server.

6. Select the schedule template for recording or capture from the drop-down list.

Note

If you need to edit or customize the template, refer to *Configure Recording Schedule Template* or *Configure Capture Schedule Template* .

---

7. **Optional:** For Recording Schedule, click **Advanced Settings** to set the pre-record time, post-record time, video stream, and other parameters.

Note

The Guarding Vision Storage Server only supports main-stream.

---

8. Click **Set Quota** to set the corresponding quota ratio for record, picture, and additional information.

   Example

   If you set **Record Quota** as 60%, up to 60% of the storage space can be used for storing the video files.

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

6.3 Configure Recording Schedule Template

You can edit the recording schedule template, or customize a recording schedule template.

Perform this task if you need to configure the recording schedule template.

Steps
1. Enter the Storage Schedule module.
2. Open the template settings window.
   - Select **Template 01** to **Template 08** from the dropdown list and click **Edit**.
   - Select **Custom**from the drop-down list.
3. Drag on the time-line to set the time periods for the selected template when the cursor turns to
   .

Continuous

Normal and continuous recording. The schedule time bar is marked with ▭ .

Event Recording

The recording is triggered by event. The schedule time bar is marked with ▭ .

Command

The recording triggered by command. The schedule time bar is marked with ▭ .

> ⓘ**Note**
>
> Command triggered recordding is only available for the ATM transactions when the ATM DVR is added to the client.

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

4. **Optional:** After setting the time periods, you can do one or more of the following:

Move	Drag a time period to move it when the cursors turns to 🖐 .
Lengthen or Shorten	Select a time period and then lengthen or shorten it when the cursor turns to ⟷ .
Delete	Select the configured schedule time period and click ✖ to delete it.
Delete All	Click 🗑 to delete all the configured time periods.
Copy to	Select one date and click 📋 to copy the date's time period settings to the other dates.

5. **Optional:** For template 01 to 08, you can edit the template name as you want.
6. Click **OK** to save the settings.

> ⓘ**Note**
>
> If you select **Custom** to customize a template, you can click **Save as Schedule Template**, and then the custom template can be saved as template 01 to 08.

6.4 Configure Capture Schedule Template

You can edit the capture schedule template, or customize a capture schedule template.

Perform this task if you need to configure the capture schedule template.

Steps
1. Enter the Storage Schedule module.
2. Open the template settings window.
   - Select **Template 01** to **Template 08** from the dropdown list and click **Edit**.
   - Select **Custom** from the dropdown list.

3. Drag on the time-line to set time periods for the selected template when the cursor turns to .

Continuous Capture

Normal and continuous capture. The schedule time bar is marked with ▬▬▬ .

Event Capture

The capture is triggered by event. The schedule time bar is marked with ▬▬▬ .

4. Optional: After setting the time period, you can do one or more of the followings

Move	When the cursor turns to , you can move the time period you just edited. You can also edit the displayed time point to set the accurate time period.
Lengthen or Shorten	When the cursor turns to , you can lengthen or shorten the selected time period.
Delete	Select a time period and click to delete it.
Delete All	Click to delete all the configured time periods.
Copy to	Select one date and click to copy the date's time period settings to the other dates.

5. Optional: For template 01 to 08, you can edit the template name as you want.

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

> 📖 **Note**
>
> If you select **Custom** to customize a template, you can click **Save as Schedule Template**, and then the custom template can be saved as template 01 to 08.

Chapter 7 Remote Playback

You can search the video files stored in the local device or the storage server by camera or triggering event, and then play them remotely.

Note

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 *Set Live View and Playback Parameters* .

7.1 Normal Playback

You can search video files by camera or group for normal playback.

Figure 7-1 Normal Playback Toolbar

Icon	Name	Description
	Single Frame (Reverse)	Play the video files frame by frame (reversely). You can also scroll down the mouse wheel to play the video file frame by frame (reversely).
	Event Playback	Search the video files recorded based on event, such as motion detection, video loss or video tampering.
	ATM Playback	Search the video files of ATM devices.
	POS Playback	Search the video files which contain POS information.
	VCA Playback	Set VCA rule for 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.
	Download	Download the video files of the camera and store them to local 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.

Icon	Name	Description
2016/05/31 10:39:37	Accurate Positioning	Set the accurate time point to play the video file.
11/30 12/01	Date	The day that has video files will be marked with .

Note

The Cloud P2P device only supports normal playback and it also does not support the functions of reverse playback, slow forward or fast forward, and adding tag.
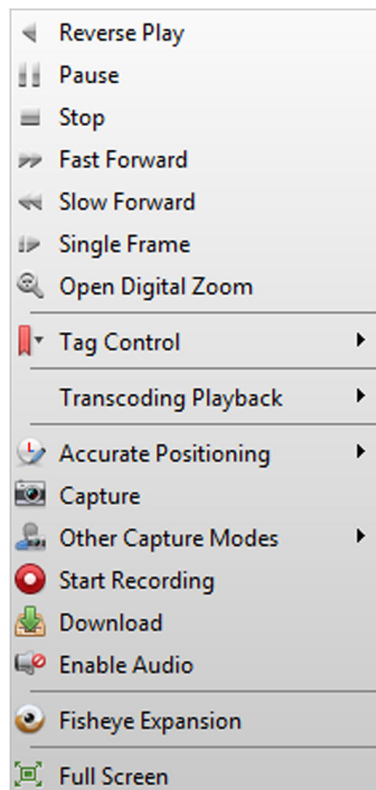
Figure 7-2 Right-Click Menu of Normal Playback Display Window

Icon	Name	Description
	Show/Hide Temperature Information	Enable or disable the temperature information overlay of playback image.

Icon	Name	Description
		ⓘ**Note** The temperature information overlay is only supported by thermal camera.
	Tag Control	Add default (the default tag name is TAG) or custom tag (the tag name is customized) for the video file to mark the important video point. You can also edit the tag or go to the tag position conveniently.
	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.
	Fisheye Expansion	Enter the fisheye playback mode. For details, refer to *Fisheye Playback* .

7.1.1 Switch Video Stream for Playback

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

Before You Start
Set the video stream for recording as **Dual-Stream**.

ⓘ**Note**

For details, refer to *Store Picture and Video on DVR, NVR, or Network Camera* .

Perform this task if you want to switch video stream for playback.

Steps

ⓘ**Note**

This function should be supported by device.

1. Open Group Management page.

ⓘ**Note**

See *Group Management* for details.

2. Open Modify Camera window.

ⓘNote

Refer to *Edit Channel Parameters* for details.

3. Select the video stream as **Main Stream** or **Sub-Stream** in the **Video Stream** field.
4. Click **OK**.

7.1.2 Search Video Files

You can search the video files by date, and you can also input keyword to filter the matched results for normal playback.

Perform this task if you need to search video files for normal playback.

Steps
1. Open the Remote Playback page.
2. **Optional:** Click 📅 to set the start date and end date of searching time period.

ⓘNote

In the calendar, the date which has video files recorded by schedule will be marked with ◢ , and the date which has video files recorded based on event will be marked with ◢ .

3. Start the playback of camera(s) to search the video files of the selected camera(s). You can do one of the followings to start the playback.

ⓘNote

Up to 16 cameras can be searched simultaneously.

- **-** Drag the camera or group to a display window.
- **-** Select a display window and double-click the camera or group to start.

The matched video files of the selected group or camera will display on the right of the Remote Playback page in chronological order. And by default, the first video file will play automatically.

4. **Optional:** Input keyword in the **Filter** field to filter the results.

7.1.3 Play Video Files

After searching the video files for the normal playback, you can play the video via file list or timeline.

Perform this task if you need to play the video files.

Steps
1. Open the Remote Playback page.
2. Search the video files.
3. Play video via file list or timeline.

- Select the video file from the search result list, and click ▶ on the video file or double-click the video file to play the video in the playback display window.
- Click on the timeline to positioning the desired video segment of specified time for normal playback.

ⓘNote

- The timeline indicates the time duration for the video files, and the video files of different types are color coded.
- You can use mouse wheel or click ⊞ / ⊟ to scale up or scale down the timeline bar.

7.2 Alarm Input Playback

When the alarm input is triggered and the linked video can be searched for alarm input playback. This function requires the support of the connected device.

For the description of the alarm input playback toolbar and right-click menu of display window, refer to **Normal Playback** .

ⓘNote

Some icons may be not available for alarm input playback.

7.2.1 Search Video Files

You can search the video files by date, and you can also input keyword to filter the matched results for alarm input playback.

Perform this task when you need to search video files for alarm input playback.

Steps
1. Open the Remote Playback page.
2. Click ⌄ to show the Alarm Input panel at the left.
3. **Optional:** Click 📅 to set the start date and end date of searching time period.
4. Start the playback of alarm input(s) to search the video files of the selected alarm input(s). You can do one of the followings to start the playback.
   - Drag the alarm input to a display window.
   - Select a display window and double-click the alarm input to start.

   The matched video files of the selected alarm input will display on the right of the Remote Playback page in chronological order. And by default, the first video file will play automatically.

5. **Optional:** Input keyword in the **Filter** field to filter the results.

7.2.2 Play Video Files

After searching the video files for the alarm input playback, you can play the video via file list or timeline.

Perform this task when you want to play the video files of alarm input.

Steps
1. Open the Remote Playback page.
2. Click ⌄ to show the Alarm Input panel at the left.
3. Search the video files of the alarm input.

> **Note**
>
> See **Search Video Files** for details about searching video files of the alarm input.

4. Play video via file list or timeline.
   - Select the video file from the search result list, and click ▶ on video file, or double-click the video file to play the video in the playback display window.
   - Click on the timeline to positioning the desired video segment of specified time for alarm input playback.

> **Note**
>
> • The timeline indicates the time duration for the video files, and the video files of different types are color coded.
> • You can use mouse wheel or click ⊞ / ⊟ to scale up or scale down the timeline bar.

7.3 Event Playback

The recorded video files 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. This function requires the support of the connected device.

For the description of the event playback toolbar and right-click menu of display window, refer to **Normal Playback** .

> **Note**
>
> Some icons may be not available for event playback.

7.3.1 Search Video Files

You can search the video files by date and by event type. And you can also input keyword to filter the matched results for event playback.

Perform this task when you want to search video files for event playback.

Steps
1. Open the Remote Playback page.
2. Select the camera and start the normal playback.

> **⟦ℹ⟧Note**
>
> For details about starting normal playback, refer to *Play Video Files* .

3. Click ▣ to enable event playback.

   By default, the video files recorded based on motion detection will be searched.
4. **Optional:** Click ▦ to set the start date and end date of searching time period.

> **⟦ℹ⟧Note**
>
> In the calendar, the date which has video files recorded by schedule will be marked with ◢ , and the date which has video files recorded based on event will be marked with ◢ .

5. Select the event type from the drop-down list to start searching.

   The matched video files will display on the right of the Remote Playback page in chronological order. And by default, the first video file will play automatically.
6. **Optional:** Input keyword in the **Filter** field to filter the results.

7.3.2 Play Video Files

After searching the video files for the event playback, you can play the video via file list or timeline.

Before You Start
Start the normal playback of the cameras.

Perform this task when you want to play the video files recorded based on event.

Steps
1. Open the Remote Playback page.
2. Click ▣ on Remote Playback page to enable event playback.
3. Search the video files recorded based on event.
4. Play the video file.
   - Select the video file from the search result list, and click ▶ on the video file, or double-click the video file to play the video in the playback display window.
   - Click on the timeline to positioning the desired video segment of specified time for event playback.

> **⟦ℹ⟧Note**
>
> • The timeline indicates the time duration for the video files, and the video files of different types are color coded.
> • You can use mouse wheel or click ⊞ / ⊟ to scale up or scale down the timeline bar.

7.4 ATM Playback

You can search the video files of ATM DVR for ATM playback. This function requires the support of the connected device which is configured with transaction rule.

For the description of the ATM playback toolbar and right-click menu of display window, refer to **Normal Playback** .

ⓘNote
Some icons may be not available for ATM playback.

7.4.1 Search Video Files

You can search the video files of ATM DVR by card number, by transaction type, by transaction amount, by file type, or by date. And you can also input keyword to filter the matched results for ATM playback.

Perform this task when you want to search video files for ATM playback.

Steps
1. Open the Remote Playback page.
2. Select the camera of ATM DVR and start the normal playback.

   ⓘNote
   For details about starting normal playback, refer to **Play Video Files** .

3. Click 🔳 to enable ATM playback.
4. Set the search conditions.

   by Card Number

   Input the card number contained in the ATM information.

   by Transaction Type and Amount

   Select transaction type for search, and input the related transaction amount.

   by File Type

   Select the type of video files for search.

   by Date

   Click 📅 to set the start date and end date of searching time period.

5. Click **Search** to start searching.

   The matched video files of selected ATM DVR will display on the right of the Remote Playback page in chronological order. By default, the first video file will play automatically.

6. **Optional:** Input keyword in the **Filter** field to filter the results.

7.4.2 Play Video Files

After searching the video files of the cameras connected with ATM DVR, you can play the video via file list or timeline.

Before You Start
Start the normal playback of cameras connected with ATM DVR.

Perform this task when you want to play the video files of cameras connected with ATM DVR.

Steps
1. Open the Remote Playback page.
2. Click ![ATM icon] on Remote Playback page to enable ATM playback.
3. Search the video files of cameras connected with ATM DVR.
4. Play the video file.
   - Select the video file from the search result list, and click ![play icon] on the video file, or double-click the video file to play the video in the playback display window.
   - Click on the timeline to positioning the desired video segment of specified time for ATM playback.

![Note icon]**Note**

- The timeline indicates the time duration for the video files, and the video files of different types are color coded.
- You can use mouse wheel or click ![+] / ![−] to scale up or scale down the timeline bar.

7.5 POS Playback

You can search the video files which contain POS information for POS playback. This function requires the support of the connected device which is configured with POS text overlay.

For the description of the POS playback toolbar and right-click menu of display window, refer to **Normal Playback** .

![Note icon]**Note**

Some icons may be not available for POS playback.

7.5.1 Search Video Files

You can search the video files which contain POS information by keywords or by date.

Perform this task when you want to search video files for POS playback.

Steps
1. Open the Remote Playback page.

2. Select the camera and start the normal playback.

> 🗏**Note**
>
> For details about starting normal playback, refer to *Play Video Files* .

3. Click 🗏 to enable POS playback.
4. Set the search conditions.

by Keywords

Input the card number contained in the ATM information.

> 🗏**Note**
>
> Up to three keywords can be inputted for once. And each two keywords should be separated with a comma.

by Filter

For more than one keyword, 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.

by Case Sensitive

Check **Case Sensitive** to search the POS information by case-sensitive keywords.

by Date

Click 🗓 to set the start date and end date of searching time period.

5. Click **Search** to start searching.

The video files contain POS information will display on the right of the Remote Playback page in chronological order. And by default, the first video file will play automatically.

6. Optional: Input keyword in the **Filter** field to filter the results.

7.5.2 Play Video Files

After searching the video files which contain POS information, you can play the video via file list or timeline.

Before You Start

Start the normal playback of cameras configured with POS information overlay.

Perform this task when you want to play the video files which contain POS information.

Steps
1. Open the Remote Playback page.
2. Click 🗏 on Remote Playback page to enable POS playback.
3. Search the video files which contain POS information.
4. Play video via file list or timeline.

- Select the video file from the search result list, and click ▶ on the video file, or double-click the video file to play the video in the playback display window.
- Click on the timeline to positioning the desired video segment of specified time for POS playback.

ⓘNote

- The timeline indicates the time duration for the video files, and the video files of different types are color coded.
- You can use mouse wheel or click ⊞ / ⊟ to scale up or scale down the timeline bar.

7.6 VCA Playback

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.

Perform this task when you need to set VCA rule and find the video that VCA event occurs.

Steps

ⓘ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.

1. Open the Remote Playback page.
2. Select the camera and start the normal playback.

ⓘNote

Refer to *Play Video Files* for details.

3. Click 🔲 to enter the VCA playback interface.
4. Select the VCA Type, draw the detection region and set the sensitivity.

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.

Set Detection Region for Motion	Click 🔳 , and then click and move on the playback window to set the grid rectangle as the detection region.

Set All the Area as Detection Region for Motion	Click ▣ to set all the area shot by the camera as the detection region.
Set Vertex of Detection Region for Intrusion	Click ✛ , and then click on the playback window to set the vertex for the detection region.
Set Detection Line for Line Crossing	Click ✛ , and then drag on the playback window to set the detection line.
Delete Drawn Region or Line	Click ✖ .

Note

For Intrusion and Line Crossing, you can click **Advanced Attributes** and 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.

5. **Optional:** Click 📅 to set the start date and end date of searching time period.
6. Click **Search**.

   The VCA events occurred in the defined area will be red marked on the timeline.

   Note

   • By default, the playback speed of concerned video will be 1X, and the playback speed of unconcerned video will be 8X.
   • 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 **Set Live View and Playback Parameters** for details.

7. Play the video files after searching.

   Note

   • Refer to **Play Video Files** for the description of the playback control toolbar and right-click menu.
   • Some icons may not available for VCA playback.

7.7 Synchronous Playback

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

Perform this task when you need to play the video files in synchronization.

Steps

Note

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

1. Open the Remote Playback page.
2. Start normal playback of at least two cameras.

📖**Note**

Refer to *Play Video Files* for details.

---

3. Click ⇥ in the toolbar to enable the synchronous playback.

   The camera under playback will start synchronous playback.
4. Click ⇤ to disable the synchronous playback.

7.8 Fisheye Playback

You can play the video files of a fisheye camera in fisheye expansion mode.

Perform this task when you need to play video files of fisheye camera in fisheye expansion mode.

Steps

📖**Note**

For other playback control instruction, refer to *Normal Playback* . Some icons may not be available for fisheye playback.

---

1. Open the Remote Playback page.
2. Select a fisheye camera to start playback.

📖**Note**

For detailed configuration about playback and playback control, refer to *Normal Playback* .

---

3. Right-click on the video file and select **Fisheye Expansion** to enter the Fisheye Expansion mode.

📖**Note**

The mounting type in playback of fisheye expansion is set according to the mounting type in live view. For details, refer to *Perform Live View in Fisheye Mode*

---

4. Select the expanding mode for playback as you 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.

⌊i⌋**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. **Optional:** Right-click on a playing window and you can switch the selected window to full-screen mode.

⌊i⌋**Note**

You can press **Esc** key on the keyboard or right-click on the window and select **Quit Full Screen** to exit the full-screen mode.

Chapter 8 Download Video Files

During playback, you can download the video files of one camera or multiple cameras to the local PC by file, by date, or by tag.

ⓘ**Note**

You cannot download the video files of Cloud P2P device.

8.1 Download by File

During playback, you can download the video files of the camera to the local PC by file.

Perform the following steps to download the video files by file.

Steps
1. Enter Playback page and select a camera to start playback.

   ⓘ**Note**

   For details about starting playback, refer to **Remote Playback** .

2. Click 🔽 on the toolbar to open Video File Downloading page.

   The video files of the selected camera displays on the page.

3. Check the video file(s).

   The total size of the selected file(s) is calculated and shown at the bottom.

4. Click **Download** to start downloading the selected file(s) to the local PC.

5. **Optional:** Input the flow and click **Set** to control the downloading speed.

   ⓘ**Note**

   The flow should be between 0 Kbps and 32,768 Kbps.

6. **Optional:** Click **Stop** to stop downloading manually.

8.2 Download by Date

During playback, you can download the video files of the camera to the local PC by date.

Perform the following steps to download the video files by date.

Steps
1. Enter Remote Playback page and select a camera to start playback.

⌊**i**⌋**Note**

For details about starting playback, refer to ***Remote Playback*** .

2. Click 📥 on the toolbar to open File Download page.
3. Click **Download by Date** tab in the File Download page.
4. Check the duration(s) to enable and click 📅 to set the start and end time.

   The total size of the videos in the configured duration(s) is calculated and shown at the bottom.
5. Click **Download** to start downloading the video file(s) of the configured duration(s) to the local PC.

⌊**i**⌋**Note**

The progress bar shows the downloading process.

6. **Optional:** Input the flow and click **Set** to control the downloading speed.

⌊**i**⌋**Note**

The flow should be between 0 Kbps and 32,768 Kbps.

7. **Optional:** Click **Stop** to stop downloading manually.

⌊**i**⌋**Note**

When downloading video file of one time duration, you can set to merge the downloaded video files in the configured time duration. For merging downloaded video files, refer to ***Set Live View and Playback Parameters*** .

8.3 Download by Tag

During playback, you can download the video files of the camera to the local PC by tag.

Perform the following steps to download the video files by tag.

Steps
1. Enter Remote Playback page and select a camera to start playback.

⌊**i**⌋**Note**

For details about starting playback, refer to ***Remote Playback*** .

2. Click 📥 on the toolbar to open File Download page.
3. Click **Download by Tag** tab on the File Download page.

   All added tags displays on the page.
4. Check the tag(s) to select the video file(s) in the time period of 30 seconds before and after the tag time.

   The total size of the selected video file(s) is calculated and shown at the bottom.

5. Click **Download** to start downloading the selected file(s) to the local PC.

6. **Optional:** Input the flow and click **Set** to control the downloading speed.

> 🛈**Note**
>
> The flow should be between 0 Kbps and 32,768 Kbps.

7. **Optional:** Click **Stop** to stop downloading manually.

8.4 Download for Multiple Cameras

During the playback of multiple cameras, you can download the video files of multiple cameras by date simultaneously.

Perform the following steps to download the video files of multiple cameras by date simultaneously.

Steps

1. Enter Playback page and select multiple cameras to start playback.

> 🛈**Note**
>
> For details about starting playback, refer to *Remote Playback* .

2. Click 📷 to open the Download for Multiple Cameras page.

3. Check the cameras to enable the corresponding video duration settings.

4. Set the start time and end time of video duration for each camera.

5. **Optional:** Check **Download Player** to download the player.

6. Click **Download** to start downloading the video files of the configured duration(s) to the local PC.

The progress bar shows the downloading process.

7. **Optional:** Input the flow and click **Set** to control the downloading speed.

> 🛈**Note**
>
> The flow should be between 0 Kbps and 32,768 Kbps.

8. **Optional:** Click **Stop** to stop downloading manually.

> 🛈**Note**
>
> Up to 16 cameras' video files can be downloaded simultaneously.

Chapter 9 Event and Alarm

You can configure the alarm of the added resources and set the linkage actions so that when the alarm is triggered, you can view the alarm details.

9.1 Alarm Configuration

You can add event detections for the added resources, such as camera, alarm input, device, access control, and trigger the linkage actions when the event occurs. For example, when motion is detected, an audible warning appears or video recording starts.

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

9.1.1 Configure Motion Detection Alarm

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

Perform this task when you need to configure the motion detection alarm.

Steps

Note
The configuration varies according to different devices, see the user manual of the devices for details.

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 **Enable** to enable the motion detection.
4. Check **Enable Dynamic Analysis** to mark the detected objects with green rectangles in live view and playback.
5. Select the arming schedule template from the Arming Schedule field.

   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

Customize template as desired, see ***Configure Arming Schedule*** for details.

6. **Optional:** Select **Normal** or **Expert** as the configuration type for some cameras.

[i]**Note**

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.

7. Select the triggered camera.

[i]**Note**

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 ***Remote Storage Configuration*** .

The image or video from the triggered camera pops up or displays on the video wall when motion detection alarm occurs.

8. Draw a defined area for the arming region.
   - Drag the mouse to draw.
   - Click [icon] to set the whole video area as detection area.

   [i]**Note**

   You can click [icon] to clear all the detection area.

9. Drag the slider on the sensitivity bar to adjust the motion detection sensitivity.

[i]**Note**

The larger the value is, the more sensitive the detection is.

10. Check the linkage action(s) for the alarm.

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 ***Set Alarm Sound*** .

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.

[i]**Note**

You should set the triggered camera first, see step 7 in this task for details.

Alarm Triggered Video Wall Display

Display the video of the triggered camera on the video wall when alarm is triggered.

[i]**Note**

You should set the triggered camera first, see step 7 in this task for details.

11. Click **Copy to...** to copy the alarm parameters to other channels
12. Click **Save**.

9.1.2 Configure Video Tampering Alarm

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

Perform this task when you need to configure the video tampering alarm.

Steps

[i]**Note**

The configuration varies according to different devices, see the user manual of the devices for details.

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 **Enable** to enable the video tampering detection.
4. Select the arming schedule template from the **Arming Schedule** field.

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

Customize template as desired, see *Configure Arming Schedule* for details.

5. Select the triggered camera.

> 📖 **Note**
>
> 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 ***Remote Storage Configuration*** .

The image or video from the triggered camera pops up or displays on the video wall when video tampering alarm occurs.

6. Draw a defined area for the arming region.
- Drag the mouse to draw.
- Click 🔲 to set the whole video area as the detection area.

> 📖 **Note**
>
> Click 🔲 to clear the detection area.

7. Drag the slider on the sensitivity bar to adjust the tampering alarm sensitivity.
8. Check the linkage action(s) for the alarm.

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 ***Set Alarm Sound*** .

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, see step 5 in this task for details.

Alarm Triggered Video Wall Display

Display the video of the triggered camera on the video wall when alarm is triggered.

> 📖 **Note**
>
> You should set the triggered camera first, see step 5 in this task for details.

9. Optional: Click **Copy to...** to copy the alarm parameters to other cameras.
10. Click **Save**.

9.1.3 Configure Video Loss Alarm

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

Perform this task when you need to configure video loss alarm.

Steps

⎙**Note**

The configuration varies according to different devices, see the user manual of the devices for details.

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 **Enable** to enable the video loss alarm.
4. Select the arming schedule template from the **Arming Schedule** field.

   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

   Customize template as desired, see *Configure Arming Schedule* for details.
5. Select the triggered camera.

   ⎙**Note**

   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 .

   The image or video from the triggered camera pops up or displays on the video wall when the video loss alarm occurs.
6. Check the linkage action(s) for the alarm.

   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 *Set Alarm Sound* .

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, see step 5 in this task for details.

Alarm Triggered Video Wall Display

Display the video of the triggered camera on the video wall when alarm is triggered.

☐ⓘ**Note**

You should set the triggered camera first, see step 5 in this task for details.

7. **Optional:** Click **Copy to...** to copy the alarm parameters to other cameras.
8. Click **Save**.

9.1.4 Configure Audio Exception Alarm

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

Perform this task when you need to configure the audio exception alarm.

Steps

☐ⓘ**Note**

The audio exception alarm requires the support of the connected device.

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. Perform the following operation(s) to enable the related function of audio detection alarm.

Audio Input Detection	Check **Audio Input Detection** to detect the exceptions of audio input condition.
Sudden Increase of Sound Intensity	Check **Sudden Increase of Sound Intensity** to detect the sudden increase of the sound intensity, and it consists the settings of sensitivity and sound intensity threshold. ☐ⓘ**Note** **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]. The sound in the environment can be filtered, the louder the environment sound, the higher the value should be. You can adjust it according to the real environment.

Sudden Decrease of Sound Intensity	Check **Sudden Decrease of Sound Intensity** to detect the sudden decrease of the sound intensity, by which you can find the abnormal silent. For example, the electric generator makes loud noise when it's working, so it should be paid attention to if the noise drops down suddenly.

4. Select the arming schedule template the **Arming Schedule** field.

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

Customize template as desired, see **Configure Arming Schedule** for details.

5. Select the triggered camera.

$\boxed{\mathbf{i}}$**Note**

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 **Remote Storage Configuration** .

The image or video from the triggered camera pops up or displays on the video wall when audio exception alarm occurs.

6. Check the linkage action(s) for the alarm.

Alarm Output

Enable the alarm output function. Select the alarm output port and the external device connected to the port can be controlled.

Recording

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 **Set Alarm Sound** .

E-mail 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.

⌷**i**⌷**Note**

You should set the triggered camera first, see step 5 in this task for details.

Alarm Triggered Video Wall Display

Display the video of the triggered camera on the video wall when alarm is triggered.

⌷**i**⌷**Note**

You should set the triggered camera first, see step 5 in this task for details.

7. **Optional:** Click **Copy to...** to copy the alarm parameters to other cameras.
8. Click **Save**.

9.1.5 Configure Face Detection Alarm

Face detection helps to detect the human faces within the monitoring area automatically. And a series of linkage actions will be triggered if any object is detected.

Perform this task when you need to configure the face detection alarm.

Steps

⌷**i**⌷**Note**

The face detection function requires the support of the connected device.

1. Enter 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 **Enable** to enable the face detection alarm.
4. Select the arming schedule template from the **Arming Schedule** field.

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

Customize template as desired, see **_Configure Arming Schedule_** for details.

5. Select the triggered camera.

ⓘ**Note**

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 **_Remote Storage Configuration_** .

The image or video from the triggered camera pops up or displays on the video wall when face detection alarm occurs.

6. Set the sensitivity for face detection.

7. **Optional:** Check **Enable Dynamic Analysis for Face Detection** to mark the detected faces with rectangle in the live view.

8. Check the linkage action(s) for the alarm.

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 **_Set Alarm Sound_** .

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**

Set the triggered camera first, see step 5 in this task for details.

Alarm Triggered Video Wall Display

Display the video of the triggered camera on the video wall when alarm is triggered.

ⓘ**Note**

Set the triggered camera first, see step 5 in this task for details.

9. **Optional:** Click **Copy to...** to copy the alarm parameters to other cameras.

10. Click **Save**.

9.1.6 Configure Line Crossing Detection Alarm

Line crossing detection can be used for detecting people, vehicles and objects crossing a predefined virtual line. The crossing direction can be set as bidirectional, from left to right, or from right to left. And a series of linkage actions will be triggered if any object is detected.

Perform this task when you need to configure the line crossing detection alarm.

Steps

[i]**Note**

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

1. Enter 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 **Enable** to enable the line crossing detection alarm.

   [i]**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 **Arming Schedule** field.

   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

   Customize template as desired, see *Configure Arming Schedule* for details.

5. Select the triggered camera.

   [i]**Note**

   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 *Remote Storage Configuration* .

   The image or video from the triggered camera pops up or displays on the video wall when line crossing detection alarm occurs.

6. Configure the arming line.
   1) 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.

---

2) Select the virtual line direction as A<->B, A ->B, or 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.

3) Click 🔲 and draw a virtual line on the preview window.

ⓘ Note

- If you want to draw another virtual line, you must select another virtual line ID for it.
- Up to 4 lines can be drawn.

---

4) **Optional:** Click 🔍 and drag the virtual line to adjust its position
5) **Optional:** Click 🔲 to delete the selected virtual line.

7. Set the sensitivity between 1 and 100.
8. Check the linkage action(s) for the alarm.

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 *Set Alarm Sound* .

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**

Set the triggered camera first, see step 5 in this task for details.

Alarm Triggered Video Wall Display

Display the video of the triggered camera on the video wall when alarm is triggered.

⎘**Note**

Set the triggered camera first, see step 5 in this task for details.

9. **Optional:** Click **Copy to...** to copy the alarm parameters to other cameras.
10. Click **Save**.

9.1.7 Configure Alarm Input Alarm

When a device's alarm input receives a signal from an external alarm device, such as smoke detector, doorbell, etc., the client software can trigger linkage actions for notification.

Before You Start
Add the alarm inputs to the client and group the alarm inputs for management.

Perform this task when you need to configure the alarm input alarm.

Steps
1. Enter the Event Management page and click **Alarm Input** tab.
2. Select the alarm input channel to be configured.
3. Check **Enable** to enable the alarm input alarm.
4. Create a name for the alarm.
5. Set the alarm status according to the alarm input device.
6. Select the arming schedule template from the **Arming Schedule** field.

   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

   Customize template as desired, see *Configure Arming Schedule* for details.
7. Select the triggered camera.

⃞ℹ️**Note**

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 ***Remote Storage Configuration*** .

The image or video from the triggered camera pops up or displays on the video wall when alarm input alarm occurs.

8. Check the linkage action(s) for the alarm.

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 ***Set Alarm Sound*** .

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.

⃞ℹ️**Note**

Set the triggered camera first, see step 7 in this task for details.

Alarm Triggered Video Wall Display

Display the video of the triggered camera on the video wall when alarm is triggered.

⃞ℹ️**Note**

Set the triggered camera first, see step 7 in this task for details.

9. **Optional:** Click **Copy to...** to copy the alarm parameters to other alarm inputs.
10. Click **Save**.

9.1.8 Configure Device Exception Alarm

When the enabled type of device exception occurs, such as HDD full, HDD exception, illegal login, device offline, and so on, the linkage actions will be triggered for notification. You can set the linkage actions as desired.

Perform this task when you need to configure the device exception alarm.

Steps

1. Enter the Event Management page and click **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 **Enable** to enable the device exception alarm.
5. Check the linkage action(s) for the alarm.

   Alarm Output

   Enable the alarm output function. Select the alarm output port and the external device connected to the port can be controlled.

   ⌐**i**⌐**Note**

   Alarm Output is not available for device offline exception.

   Audible Warming

   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 *Set Alarm Sound* .

   Email Linkage

   Send an email notification of the alarm information to one or more receivers.

6. **Optional:** Click **Copy to...** to copy the alarm parameters to other devices.
7. Click **Save**.

9.1.9 Configure Arming Schedule

The client provides two default arming schedule templates: All-day template and weekday template. It also provides 9 pre-defined templates. You can set the time periods in each day of the week and save the settings as pre-defined arming schedule.

Perform this task when you need to configure the pre-defined arming schedule.

Steps

1. Open the Event Management page and click **Camera Event** tab.
2. Select the camera to be configured and select a event type.
3. Check **Enable** to enable detecting the selected event type.
4. Click **Edit** to enter the Templates Management page.
5. Drag the cursor on the timeline to set the time periods.

   ⌐**i**⌐**Note**

   Up to 8 time periods can be set for each day.

6. **Optional:** Perform the following operation(s) to manage the time periods.

Move	Move the cursor on a time period and when the cursor turns to ![icon], drag to move the time period.
Lengthen or Shorten	Move the cursor to one end of a time period, and when the cursor turns to ![icon], drag to lengthen or shorten the time period.
Delete	Select a time period, and then click ![icon] to delete it
Delete All	Click ![icon] to delete all time periods.
Copy to Other Dates	Select a time period, and then click ![icon] to copy the time periods settings to other dates.

7. Click **OK**.

9.1.10 Configure Custom Arming Schedule

You can set custom arming schedule as desired.

Perform this task when you need to configure custom arming schedule.

Steps
1. Open the Event Management page and click **Camera Event** tab.
2. Select the camera to be configured and select an event type.
3. Check **Enable** to enable detecting the selected event type.
4. Select **Custom** from the **Arming Schedule** field to open the Custom Schedule page.
5. Drag the cursor on the timeline to set the time periods.

> **Note**
> Up to 8 time periods can be set for each day.

6. **Optional:** Perform the following operation(s) to manage the time periods.

Move	Move the cursor on a time period and when the cursor turns to ![icon], drag to move the time period.
Lengthen or Shorten	Move the cursor to one end of a time period, and when the cursor turns to ![icon], drag to lengthen or shorten the time period.
Delete	Select a time period, and then click ![icon] to delete it
Delete All	Click ![icon] to delete all time periods.
Copy to Other Dates	Select a time period, and then click ![icon] to copy the time periods settings to other dates.

7. Click **Save as Schedule Template**.

   The custom template is saved as template 01, 02, 03... or 09.

8. Click **OK**.

9.2 View Alarm and Event Information

The received recent alarms of all the added and armed devices, and the exceptions of the client can be displayed in the alarm event center. And you can view their information and manage them.

9.2.1 Enable Receiving Alarms from Devices

Before the client can receive the alarm information from the device, you need to arm the device first.

Perform this task when you need to enable receiving alarms from devices.

Steps
1. Click **Tool → Device Arming Control** open Device Arming Control page.

   All the added devices display on this page.
2. Check device(s) to arm the selected device(s).

   The icon 🔔 in Arming Status column turns to 🔔 , and the alarms of armed device(s) are automatically uploaded to the client when the alarm is triggered.

9.2.2 View Alarm Information

Different alarm types, including motion detection, video/audio exception, alarm input, device exception, VCA alarm, CID alarm, access control alarm, and other alarms, can display in the alarm and event center.

Before You Start
Configure the alarms in Event Management, see the configuration of different alarms (e.g., *Configure Motion Detection Alarm*) for details.

Perform this task when you need to view the received alarm information.

Steps
1. Enter the Alarm Event page.
   - Click ⌃ in the lower-right corner of the client software to show the Alarms and Events panel, and then click ▭ .
   - Click **Alarm Event** on the Control Panel.
2. Click **Alarm** tab.

   ⓘ**Note**

   When the alarm occurs, the icon ⚠ in the upper-left corner twinkles to call attention.

   The received alarm information, including alarm time, source, details, and content displays on the page.
3. **Optional:** Check different alarm type(s) to filter the display of alarms.

4. Double click the alarm information to view the alarm details.

5. Optional: Perform the following operation(s) after displaying the desired alarm information.

View Live Video of Triggered Camera	For alarm configured with triggered camera, click ▶ in the Live View column to view the live video and alarm picture of the triggered camera. See *View Pop-up Alarm Information* for details.
Send Email Notification	Click ✉ in Send Email column to send an email notification of the alarm to one or more receivers. ⊡**Note** Configure the email settings first, see *Set Email Parameters* for details.
Display Alarm Video on Video Wall	Click ⊞ in Live View column to display the video of the alarm triggered camera on the Video Wall. You can enter the Video Wall page to check the alarm triggered video on the screen (which is set as the alarm window). The physical video wall also displays the video. ⊡**Note** Add the decoding device and configure the video wall first, see the topics of *Video Wall* for details.
Write Alarm Note	Click the Note column and input the description for the alarm.
Clear Alarm	Click 🔔, or right-click on an alarm and select **Clear**.
Enable/Disable Audible Warning	For alarm configured with audible warning, click 🔇 or 🔊 to enable or disable the audible warning for the alarm. ⊡**Note** For configure audible warning for alarm, refer to the configuration of different alarms (e.g., *Configure Motion Detection Alarm*).

9.2.3 View Event Information

The exceptions of the client software, such as the live view failure, device disconnection, can display in the alarm and event center.

Perform this task to view the event information of the client.

Steps

1. Enter the Alarm Event page.
   - Click ⌃ in the lower-right corner of the client software to show the Alarms and Events panel, and then click ▭ .
   - Click **Alarm Event** on the Control Panel.

2. Click **Event** tab.

The received event information, including occurred time and details display on the page.

3. **Optional:** Clear the event information.
   - Click ![icon] .
   - Right-click on an event information and then click **Clear**.

9.2.4 View Pop-up Alarm Information

For the alarm configured with pop-up image, the alarm videos and pictures can display on a pop-up window when the corresponding alarm is triggered.

Before You Start
Configure the alarm linkage action as Alarm Triggered Pop-up Image, see the configuration of different alarms (e.g., *Configure Motion Detection Alarm*) for details.

Perform this task when you need to view the pop-up alarm information.

Steps
1. Enter the Alarm Event page.
   - Click ![icon] in the lower-right corner of the client software to show the Alarms and Events panel, and then click ![icon] .
   - Click **Alarm Event** on the Control Panel.
2. Click **Alarm** tab.
3. Click ![icon] to enable alarm triggered pop-up function.
4. Trigger the alarm.

   An alarm window, showing the alarm video, alarm picture, and alarm details, will pop up.
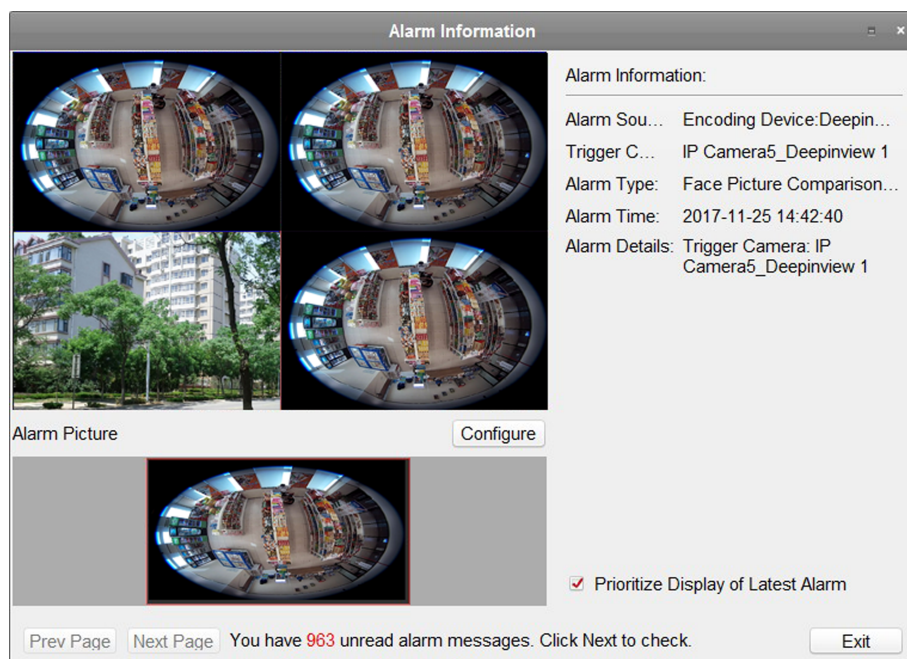
Figure 9-1 Alarm Pop-up Window

5. Perform the following operation(s) after popping up the image.

View Alarm Video	By default, the alarm video displays in 4-window division mode.
	⊡**ⅈ**⌷**Note**
	For thermal camera and target capture camera, both the live video will display at the same time.
View Alarm Picture	For the alarm triggered camera configured with picture storage on the storage server, the alarm picture will display on the field below the alarm video. You can also directly click **Configure** to set the parameters.
	⊡**ⅈ**⌷**Note**
	For configuring picture storage, refer to ***Store Picture and Video on Storage Device*** .
Display Latest Alarms	Check **Prioritize Display of Latest Alarm** to replace the earliest alarm by the latest alarm, so the latest alarm window displays. Otherwise, the current alarm information displays.
View Previous or Next Alarm	Click **Prev Page** or **Next Page** to view the previous or next alarm information.

9.2.5 Acknowledge Fire Source Detection Alarm

When the thermal device detects fire source during scanning, the fire source detection alarm will be triggered and the device stops 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
- Configure the fire source detection alarm on the client, see the configuration of different alarms (e.g., ***Configure Motion Detection Alarm***) for details.
- Configure the fire source acknowledgment mode on the device, see the user manual of the device for details.

Perform this task when you need to acknowledge the fire source detection alarm.

Steps
1. Trigger a fire source detection alarm.
2. Perform one of the following operations to view alarm details.
  - Enter Alarm Event page and click the fire source detection alarm to open the details window.
  - Configure the pop-up image linkage for fire source detection alarm, and then the alarm window will pop up automatically when the alarm is triggered.

Note

For configuring alarm pop-up image linkage, refer to the configuration of different alarms (e.g., *Configure Motion Detection Alarm*).
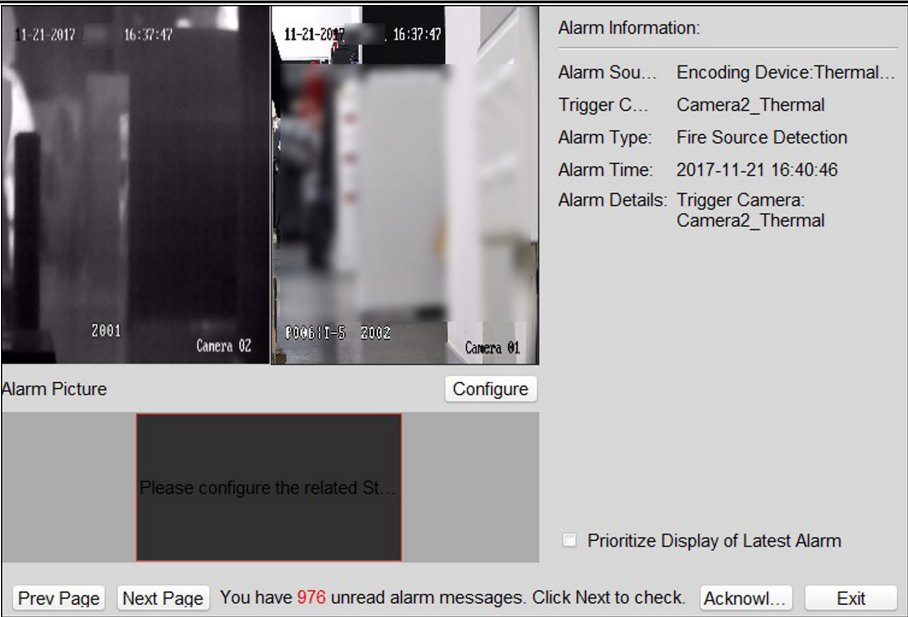
Figure 9-2 Alarm Details Window

3. Click **Acknowledge**.

Note

If the acknowledgment mode is configured as Auto, the device will continue to scan automatically when the alarm is not acknowledged in the configured acknowledgment duration. For setting the acknowledgment duration, refer to the user manual of the device.

For manual acknowledgment mode, the device continues to scan according to the configured path.

Chapter 10 Map Management

The E-map function gives a visual overview of the locations and distributions of the installed cameras, alarm input devices, alarm output 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.

10.1 Add Map

You should add a map as the parent map for the hot spots and hot regions.

Perform this task when you need to add a map.

Steps

---

[i]**Note**

Only one map can be added to one group.

---

1. Open the E-map page.
2. Select a group for which you want to add a map.

   ---

   [i]**Note**

   For details about setting the group, refer to *Group Management* .

   ---

3. Click 🗺 in the map display area to open the map adding window.
4. Input a descriptive name of the added map as desired.
5. Click ⋯ and select a map picture from the local path.

   ---

   [i]**Note**

   The picture format of the map can only be PNG, JPG or BMP.

   ---

6. Click **OK**.
7. **Optional:** Perform the following tasks after adding the map.

Zoom in/out	Use the mouse wheel or click + or − to zoom in or zoom out on the map.
Adjust Map Area	Drag the yellow window in the lower-right corner or use the direction buttons and zoom bar to adjust the map area for view.

10.2 Manage Hot Spot

The cameras, alarm inputs, and alarm outputs can be added on the map and are called the hot spots. The hot spots show the locations of the cameras, alarm inputs, and alarm outputs, and you

can also get the live view and alarm information of the surveillance scenarios through the hot spots.

☐**i**☐**Note**

- For details about managing and previewing the zone hot spot, refer to ***Display Zone on Map*** .
- For details about managing and previewing the access control point hot spot, refer to .

10.2.1 Add Camera as Hot Spot

You can add cameras to the map as hot spots.

Perform this task when you want to add cameras as hot spot on the map.

Steps
1. Enter the E-map page.
2. Click **Edit** on the E-map toolbar to enter the map editing mode.
3. Click 🔧 on the toolbar to open the Add Hot Spot window.
4. Check the checkboxes to select the cameras to be added.
5. **Optional:** Edit hot spot name, select the name color and select the hot spot icon by double-clicking the corresponding field.
6. Click **OK** to save the settings.

☐**i**☐**Note**

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

The camera icons are added on the map as hot spots and the icons of the added cameras in the group list change from 🔴 to 🟢 .

10.2.2 Add Alarm Input as Hot Spot

You can add the alarm inputs to the map as hot spots.

Perform the following steps to add alarm input as hot spot on the map.

Steps
1. Enter the E-map module.
2. Click **Edit** on the E-map toolbar to enter the map editing mode.
3. Click 🔧 on the toolbar to open the Add Hot Spot window.
4. Check the checkboxes to select the alarm inputs to be added.
5. **Optional:** Edit hot spot name, select the name color and select the hot spot icon by double-clicking the corresponding field.
6. Click **OK**.

📖**Note**

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

The alarm input icons are added on the map as hot spots and the icons of the added alarm inputs in the group list change from 🔔 to 🔔 .

10.2.3 Add Alarm Output as Hot Spot

You can add the alarm outputs to the map as hot spots.

Perform the following steps to add alarm output as hot spot on the map.

Steps
1. Enter the E-map module.
2. Click **Edit** on the E-map toolbar to enter the map editing mode.
3. Click 🖼 on the toolbar to open the Add Hot Spot window.
4. Check the checkboxes to select the alarm outputs to be added.
5. **Optional:** Edit the hot spot name, select the name color, and select the hot spot icon by double-clicking the corresponding field.
6. Click **OK**.

📖**Note**

You can also drag the alarm output icons from the alarm output list to the map directly to add the hot spot.

The alarm output are added on the map as hot spots and the icons of the added alarm outputs in the group list change from 🔔 to 🔔 .

10.2.4 Edit Hot Spot

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

Perform the following steps to edit hot spot parameters.

Steps
1. Enter the E-map module.
2. Click **Edit** at the lower left corner to enter the map editing mode.
3. Open the Modify Hot Spot window.
   - Select the hot spot icon on the map and then click 🖉 on the E-map toolbar to open the Modify Hot Spot window.
   - Right-click the hot spot icon on the map and select **Modify** in the right-click menu to open the Modify Hot Spot window.

- Double-click the hot spot icon on the map to open the Modify Hot Spot window.
4. Edit the hot spot name in the text field, select the hot spot color, the icon, and the linked zone.
5. Click **OK**.
6. **Optional:** Delete the hot spot.
   - Select the hot spot icon and click on the toolbar to delete the hot spot.
   - Right-click the hot spot icon and select **Delete** to delete the hot spot.

10.2.5 Preview Hot Spot

You can view the live view of the camera hot spot and the triggered alarm information of the hot spot on the map.

Perform the following steps to view the live view of the camera hot spot and the triggered alarm information of the hot spot on the map.

Steps
1. Enter the E-map module.
2. Click **Exit Editing Mode** on the E-map toolbar to enter the map preview mode.
3. Get the live view of the camera.
   - Double-click the camera hot spot on the map.
   - Right-click the camera hot spot on the map and click **Live View**.
4. **Optional:** For camera hot spot, if there is any alarm triggered, will appear and twinkle near the hot spot (it will twinkle for 10s). You can do the following operations:

View Alarm Information	Click to view the alarm information, including the alarm type and the triggering time.
View Instant Playback	Right-click the camera hot spot on the map and click **Live View** to view the 30s instant playback.

Note

- For DeepinMind device, the alarm picture will display near the hot spot if there is any alarm triggered. You can click and double click the alarm to view the alarm details and play back the alarm recorded video.
- To display the alarm information on the map, you should select the **Alarm on E-map** as the alarm linkage action. For details, refer to *Alarm Configuration* .
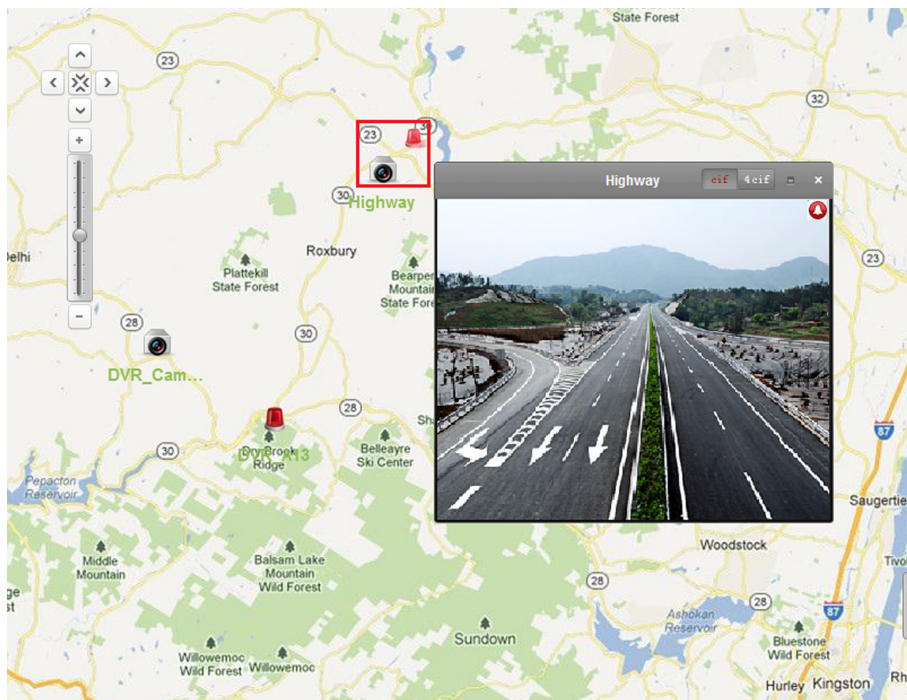
Figure 10-1 Preview Camera Hot Spot

5. **Optional:** For alarm output hot spot, if it is triggered, 🔔 will appear and twinkle near the hot spot (it will twinkle for 10s). Right-click the alarm output hot spot on the map and click **Close** or **Open** to control the alarm output status.

10.3 Manage Hot Region

The hot region function links a map to another map.

You can manage the hot region, such as adding, editing, or deleting hot region. You can also preview the hot region.

10.3.1 Add Hot Region

You can add a map to another map as a hot region and 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.

Before You Start
At least two maps should be added. Refer to **Add Map** for details about adding maps.

Perform this task when you need to add hot region.

Steps

ⓘ**Note**

A map can only be added as the hot region for once.

1. Enter the E-map page.
2. Click **Edit** on the E-map toolbar to enter the map editing mode.
3. Select an added map as the parent map.
4. Click on the toolbar to open the Add Hot Region window.
5. Check the checkbox to select the child map.
6. **Optional:** Edit the hot region name, and select the hot region color and icon by double-clicking the corresponding field.
7. Click **OK**.

   The child map icons are added on the parent map as the hot regions.

10.3.2 Edit Hot Region

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

Perform this task when you need to edit hot region.

Steps
1. Enter the E-map module.
2. Click **Edit** on the E-map toolbar to enter the map editing mode.
3. Open the Modify Hot Region window.
   - Select the hot region icon on the parent map and click on the toolbar.
   - Right-click the hot region icon and select **Modify**.
   - Double-click the hot region icon.
4. Edit the hot region name and select color, icon, and the linked child map as desired.
5. Click **OK**.
6. **Optional:** Delete the hot region.
   -
     Select the hot region icon and click on the toolbar.
   - Right-click the hot region icon and click **Delete**.

10.3.3 Preview Hot Region

You can view the hot spots on the hot region.

Perform this task when you need to preview hot region.

Steps
1. Enter the E-map page.

ℹ️Note

If you are in the editing map mode, click **Exit Editing Mode** on the E-map toolbar to enter the map preview mode.

You can view the hot spots on the hot region.

2. Click the hot region icon to enter the linked child map.
3. **Optional:** Click 🗺️ on the toolbar to go back to the parent map.
4. **Optional:** Click 🔔 on the toolbar to clear the alarm information.

Chapter 11 Cloud P2P

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

11.1 Register a Cloud P2P Account

The client software supports registering a Cloud P2P account to manage devices which supports Cloud P2P service.

Perform this task when you want to register a Cloud P2P account via the client software.

Steps
1. Enter the Device Management page.
2. Click **Device → Cloud P2P Device** to enter the Welcome to Cloud P2P page.
3. Select the region where the Cloud P2P account registered.
4. Click **Login** to open the Login page.
5. Click **Register** to open Register Account window.

Figure 11-1 Register Cloud P2P Account

🛈**Note**

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

---

6. Input required information, including user name, password, confirm password, and phone number/email address.

⚠**Caution**

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least

---

three kinds of following categories: 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.

7. Click **Send Message** to get verification code.

The system will send verification code to your phone or email.

8. Input the received verification code in the **Verification Code** text field.

9. Click **Register** to finish the registration.

11.2 Log in to Cloud P2P Account

You can log in to Cloud P2P account via the client software.

Before You Start

Register a Cloud P2P account.

$\boxed{\text{i}}$**Note**

For details, refer to ***Register a Cloud P2P Account*** .

Perform this task when you want to log in to the registered Cloud P2P account via client software.

Steps
1. Enter the Deivce Management page.
2. Click **Device → Cloud P2P Device** to enter the Welcome to Cloud P2P page.
3. Click **Login** to enter Login page.
4. Input user name/phone number, and password.
5. Click **Login** to log into your account.
6. **Optional:** Click **Logout** to log out of your account.

11.3 Device Management

You can add the Cloud P2P device to the Cloud P2P account, and delete the added device(s) from the account. You can also do remote configuration and group management to the devices of the Cloud P2P account.

11.3.1 Add Device toCloud P2P Account

You can add the Cloud P2P device to the Cloud P2P account via two ways, i.e., adding manually or adding via online device.

[i] Note

You can add 256 devices (1024 cameras) to one Cloud P2P account at most.
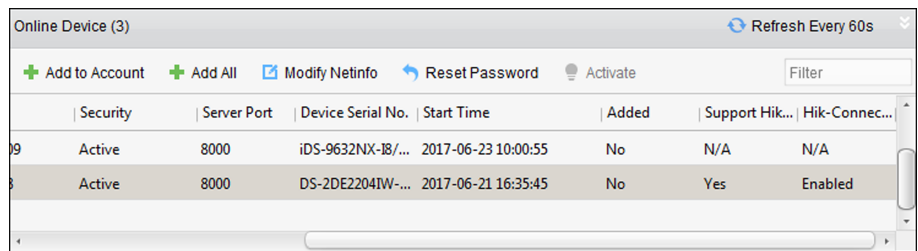
Add Online Device

You can add online Cloud P2P device(s) in the same local subnet with the PC running the client to the Cloud P2P account.

Perform this task if you need to add online device(s) to the Cloud P2P account.

Steps
1. Enter the Device Management page.
2. Click **Device → Cloud P2P Device** and log into your Cloud P2P account.

   The active online devices in the same local subnet with the client software will be displayed on the Online Device area. You can click **Refresh Every 60s** to refresh the information of the online devices.
3. Select the device(s) which support Cloud P2P service on the online device list.

Figure 11-2 Online Device List

[i] Note

For the inactive device, you need to create the password and enable the Cloud P2P service for it before you can add the device properly. For details, refer to *Activate Devices* .

4. Click **Add to Account** to open the device adding dialog box.
5. 5. Input the verification code.

   The verification code is created when you enabling the Cloud P2P service. For details, refer to *Activate Devices* .
6. Click **OK** to add the device.
7. **Optional:** Select device from the Device Management page and click **Delete** to remove the device from the Cloud P2P account.

What to do next
After adding the device to the Cloud P2P account, you should add the device by Cloud P2P if you want to add the device to the local client software. For details, refer to *Add Device by Cloud P2P* .

Manually Add Device

You can add Cloud P2P device to the Cloud P2P account manually by inputting the serial No. and verification code.

Perform this task if you need to add a device manually.

Steps

[i]**Note**

- Only the device that supports the Cloud P2P service can be added.
- One device can only be added to one Cloud P2P account.

1. Enter the Device Management page.
2. Click **Device → Cloud P2P Device** and then log into your Cloud P2P account.
3. Click **Add Device** to open the Add Device window.
4. Input the serial No. and verification code of the device.

   Serial No.

   Marked on the label of you device.

   Verification Code

   Created when you enabling the Cloud P2P service. For details, refer to *Activate Devices* .

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

   The successfully added device will be displayed on the Device Management page.

What to do next
After adding the device to the Cloud P2P account, you should add the device by Cloud P2P if you want to add the device to the client. For details, refer to *Add Device by Cloud P2P* .

11.3.2 Edit Camera Parameters

After adding a Cloud P2P device to the local client software, you can edit the camera parameters and set stream key.

Before You Start
Add a Cloud P2P device to the local client software.

[i]**Note**

See *Manually Add Device* or *Add Online Device* for details.

Perform this task when you need to edit camera which is added to Cloud P2P account.

Steps
1. Enter Device Management page.
2. Click **Group** tab.

3. Select camera in the resource list.

4. Click **Modify** to pop up Modify Camera dialog.

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

Rotate

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

Stream Key

For Cloud P2P device, the stream key is the same with the verification code, which is created when you enable the Cloud P2P service.

If the live view or video file(s) of the Cloud P2P 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.

Note

You can set whether to encrypt the live view or video file(s) of the Cloud P2P device on the Cloud P2P mobile client software. For details, refer to the *User Manual of the Cloud P2P Mobile Client Software*.

---

6. **Optional:** Click **Copy to** to copy the configured parameters to other camera(s).

7. Click **OK** to edit the camera.

Chapter 12 Forward Video Stream through Stream Media Server

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.

[i]**Note**

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

12.1 Import Certificate to Stream Media Server

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.

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**.
2. Copy the certificate to the PC which has installed with stream media server.
3. Click [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 [icon] on the task bar and click **Display**.
    2) Click **Configuration** to enter the Configuration window.
    3) In the security certificate field, click **Import** and select the certificate file you export from client in Step 1.
    4) Click **OK**.
5. Restart the stream media server to take effect.

[i]**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.

12.2 Add Stream Media Server

You can add the stream media server by IP address or by IP segment to the client.

If you add the stream media server by IP address, you can add one stream media server to the client each time and you can add multiple stream media servers to the client each time.

12.2.1 Add Stream Media Server by IP Address

You can add stream media server by IP address one by one.

Perform the following steps to add stream media server by IP address.

Steps

Note

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

1. Click ▨ on the desktop to run the stream media server.

   Note

   - You can also forward the video through the stream media server installed on other PC.
   - If the stream media server port (value: 554) is occupied by other service, a dialog box will pop up. You should change the port No. to other value to ensure the proper running of the stream media server.

2. In the client software, enter the Device Management page and click **Device**.
3. Add a new device type in the Device tab.
   1) Click **Add New Device Type**.
   2) Select **Stream Media Server**.
   3) Click **OK**.
4. Click **Stream Media Server** on the list and then click **Add** to open the Add window.
5. Select **IP Address** as the adding mode.
6. Input the nickname and IP address of the stream media server.

   Note

   The default port value is 554.

7. Click**Add**.

   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 ⚠ to view exception message and follow the provided steps to keep certificates consistent.

12.2.2 Add Stream Media Servers by IP Segment

You can add multiple stream media servers by IP segment in a batch.

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

Steps

ⁱNote

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

1. Click 🖳 on the desktop to run the stream media server.

   ⁱNote

   - You can also forward the video through the stream media server installed on other PC.
   - If the stream media server port (value: 554) is occupied by other service, a dialog box will pop up. You should change the port No. to other value to ensure the proper running of the stream media server.

2. In the client software, enter the Device Management page and click**Device**.
3. Add a new device type in the Device tab.
   1) Click**Add New Device Type**.
   2) Select **Stream Media Server**.
   3) Click **OK**.
4. Click **Stream Media Server** on the list and then click **Add** to open the Add window.
5. Select **IP Segment** as the adding mode.
6. Input the start IP and end IP address.

   ⁱNote

   The default port value is 554.

7. Click **Add**.

   ⁱNote

   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 ⚠ to view exception message and follow the provided steps to keep certificates consistent.

   The steam media server of which the IP address is between the start IP and end IP will be added to the client.

12.3 Add Cameras to Stream Media Server to Forward Video Stream

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

Perform the following steps to add cameras to stream media server to forward video stream.

Steps
1. Enter the Device Management page.
2. Click **Device** to enter the Device tab.
3. Select **Stream Media Server** on the Device Type panel.
4. Select the stream media server from the Device Management list.
5. Click **Configure** to enter the Stream Media Server Settings page.
6. Select the cameras of which the video stream is to be forwarded via the stream media server.
7. Click **OK**.
8. Go the Main View page and start the live view of the cameras again.

   On the stream media server control panel, check the channel number of the video stream forwarded through or sent from the stream media server.

$\boxed{i}$**Note**

- 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 13 Video Wall

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.

13.1 Manage Encoding Device

The encoding device needs to be added to the client for decoding and displaying on the Video Wall.

13.1.1 Add Encoding Device

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.

Perform this task if you need to add encoding device in Video Wall page.

Steps
1. Enter the Video Wall module.
2. In the Camera area, click ➕ to open the adding device window.
3. Select the adding mode and configure the corresponding parameters for the device.
   - For **IP/Domain** mode, refer to *Add Device by IP Address or Domain Name* .
   - For **IP Segment** mode, refer to *Add Devices by IP Segment* .
   - For **IP Server** mode, refer to *Add Device by IP Server* .
   - For **HiDDNS** mode, refer to *Add Device by HiDDNS* .

13.1.2 Add Third-Party Encoding Device

You can add third-party encoding devices to the client.

Adding third-party encoding devices by IP address or domain or by IP segment is supported.

Add Third-Party Encoding Device by IP Address or Domain Name

You can add third-party encoding device to the client by IP address or domain name for decoding and displaying on the video wall.

Perform this task if you need to add third-party encoding device to the client.

Steps
1. Click **Device Management** on the control panel to enter the Device Management module.
2. Click **Device → Add New Device Type** and select **Third-Party Encoding Device**.
3. Click **Third-party Encoding Device** to enter the third-party encoding device management page.

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

5. Select the adding mode as **IP/Domain**.

6. Input the required information.

Channel Number

The amount of the channels.

Start From

Add the encoding device's channel from the start channel No.

Example

If you input 4 in **Start From** text field, it means that the starting channel No. is 4.

7. Optional: Check **Export to Group** to create a group by the device name.

⬚**i**|**Note**

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

---

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

Add Third-Party Encoding Device by IP Segment

If you want add third-party encoding devices of which the IP addresses are within an IP segment for decoding and displaying on the video wall, you can specify the start IP address and end IP address, user name, password, and other parameters to add them.

Perform this task if you need to add multiple third-party encoding device to the client by IP segment.

Steps

1. Click **Device Management** on the control panel to enter the Device Management module.

2. Click **Device → Add New Device Type** and select **Third-party Encoding Device**.

The Third-party Encoding Device will display in the Device Type panel on the left.

3. Click **Third-party Encoding Device → Add** to to open the adding device window.

4. Select **IP Segment** as the adding mode.

5. Input the required information.

Start IP

Input the start IP address.

End IP

Input the end IP address in the same network segment with the start IP.

Channel Number

The amount of the channels.

Start From

Add the encoding device's channel from the start channel No.

6. **Optional:** Check **Export to Group** to create a group by the device name.

⌈i⌋**Note**

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

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

   The devices which the IP address is between the start IP and end IP will be added to the device list.

13.2 Manage Decoding Device

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

13.2.1 Add Decoding Device

You should add the decoding device to decode the video of the encoding device and display the decoded video on the Video Wall. If you do not add the decoding devices in the Device Management page, you can add them in Video Wall page.

Perform this task if you need to add decoding device in Video Wall page.

Steps

1. Enter the Video Wall module.
2. Click **Enter Video Wall Config** to enter the decoding device and video wall configuration interface.
3. In the Decoding Output area, click ➕ to activate the Quick Adding of Decoding Device window.
4. Select the adding mode and configure the corresponding parameters for the device.
   - For **IP/Domain** mode, refer to *Add Device by IP Address or Domain Name* .
   - For **IP Segment** mode, refer to *Add Devices by IP Segment* .

13.2.2 Edit Output of Decoding Device

You can edit the decoding output of the added decoding device.

Before You Start

Add decoding device to the client. For details, refer to *Add Decoding Device* .

Perform this task when you need to edit the decoding device's decoding output.

Steps

⌈i⌋**Note**

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

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

1. Enter the Video Wall module.
2. Click **Enter Video Wall Config** to enter the decoding device and video wall configuration interface.
3. In the Decoding Output area, click ⊕ before the decoding device to list the outputs of it.
4. Open the Modify Decoding Output window.
   - Double-click a decoding output.
   - Right-click a decoding output in the video wall area and select **Decoding Output Configuration**.
5. Set the display format and resolution.

   ⓘ**Note**

   For HDMI and VGA outputs, you can edit configure the resolution; for BNC output, you can configure the video standard.

6. **Optional:** You can check **Batch Configuration** and select other outputs to copy the settings to.
7. Click **OK** to save the settings.

13.3 Configure Video Wall Settings

After adding the encoding device and decoding device to the client, you need to configure the parameters of video wall for video display.

13.3.1 Add Video Wall

You should add a virtual video wall on the client and set the video wall's window division according to actual needs before linking the decoding output to the video wall and performing further operations such as displaying live view on video wall, etc.

Perform this task when you need to add a video wall on the client.

Steps

ⓘ**Note**

Up to 4 video walls can be added to the client.

1. Enter the Video Wall module.

2. Click **Enter Video Wall Config** to enter the decoding device and video wall configuration interface.

The client pre-defines a default video wall with the window division of 4*4. You can edit it if needed.

3. Open the Add Video Wall window.
  - Right- click the video wall and select **Add Video Wall**.
  - Click ⊕ .
4. Create a video wall name as you want.
5. Set the video wall's row and column.
  - Drag on the frames to set the row and column.
  - Input the row and column in the fields.

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

6. Select the video wall's proportion.
7. Click **Add**.
8. After adding the video wall, you can edit or delete it if you want.

Edit Video Wall	Right-click the video wall and select **Modify Video Wall** to edit the video wall's name, row number, column number, and proportion.
Delete Video Wall	Right-click the video wall and select **Delete Video Wall**, or click ☒ on the video wall tab to delete it.

13.3.2 Link Decoding Output with Video Wall

You should link the decoding output of the added decoding device to the window of the created video wall.

Before You Start

- Add the decoding device to the client. Refer to **Add Device** for detailed configuration about adding decoding device.
- Add a video wall to the client. Refer to **Add Video Wall** for details.

Perform this task if you need to link the decoding output with the video wall.

Steps
1. Enter the Video Wall module.
2. Click **Enter Video Wall Config** to enter the decoding device and video wall configuration interface.

The decoding output of the added decoding device will display on the left and the added video wall will display on the right.

3. Drag the decoding output on the left-side list to the display window of video wall, to configure the one-to-one correspondence.

⌊ⁱ⌋**Note**

You can also press and hold the **Ctrl** or **Shift** key to select multiple outputs and then drag them to the video wall for configuring linkage in batch.

4. **Optional:** You can click ✖ in the upper-right corner of the display window to cancel the linkage.

13.4 Display Video on Video Wall

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

After enabling decoding and displaying, the captured pictures of videos from encoding devices will display on the windows of Video Wall page. And the real-time video will also display on the physical video wall.

⌊ⁱ⌋**Note**

For some kinds of decoder, the video stream from signal source (which refers to the video signal (e.g., PC) connected to decoder via local APIs) can also display on the video wall. Refer to the user manual of device for details.

13.4.1 Decode and Display

After adding decoding device and video wall, you can start decoding the video stream from encoding devices and display the video on Video Wall.

Before You Start

Add encoding and decoding devices, and link decoding output with video wall.

Perform this task when you want to enable decoding video stream and displaying video on video wall.

Steps

1. Enter the Video Wall module.
2. Click **Back to Operation Page** to go back to the Video Wall Operation interface.
3. Perform one of the following operations to start decoding and displaying.
   - Drag a camera from the camera list at the left panel to a decoding window, or select a decoding window and then double-click a camera.
   - Hold the **Ctrl** or **Shift** key on the keyboard and click to select multiple cameras,and then drag the selected cameras to the video wall.
4. **Optional:** Perform one of the following operations to save the settings for scene.

📖**Note**

Up to 8 scenes can be set for a video wall. Each scene can be configured with different settings and window divisions.

- Click 📇 on the video wall toolbar to save the settings for the current scene.
- Click ▪ (beside 📇) and select a scene to save the settings for.

5. **Optional:** Click ▶ in the Scene panel to enable the scene.

6. **Optional:** Get live video of camera in preview window.
   1) Click ◂ at the lower-right corner of video wall to open the preview window.
   2) Select a playing window or directly drag a camera to the preview window.
   3) **Optional:** Double-click the preview window to view the live video in full screen mode.

7. **Optional:** Expand PTZ panel at left to realize PTZ control for the camera.

📖**Note**

The camera should support PTZ control.

---

8. **Optional:** Right-click on the playing window to manage the decoding and display via right-click menu.

📖**Note**

The menu differs depending on the devices.

Start/Pause Successive Decoding

Start/Pause the auto-switch decoding. This function is only supported by decoder.

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.

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.

13.4.2 Perform Windowing and Roaming

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.

Before You Start

The decoding output has linked to the video wall.

Perform this task if you need to set windowing and roaming.

Steps

ⓘ**Note**

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

1. Click **Enter Video Wall Config** to enter the decoding device and video wall configuration interface.
2. Start decoding and displaying. Refer to **Decode and Display** for details.
3. Drag a screen which links to a decoding output to open a window.

ⓘ**Note**

- If you want to open a window on the opened window, drag the window and hold the **Ctrl** key to create one.
- At least one camera should be selected before opening window.
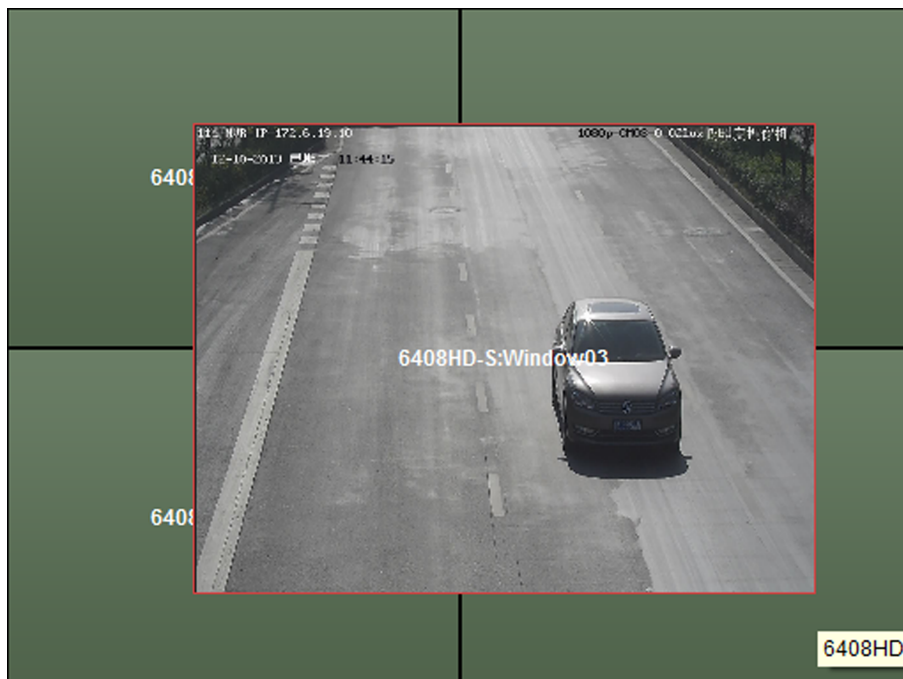
The window will be displayed within a screen or span multiple screens.

4. Optional: Adjust the open window.

   1) When the cursor becomes ![icon], move the window to adjust its position.

     ![Note icon]**Note**

     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.
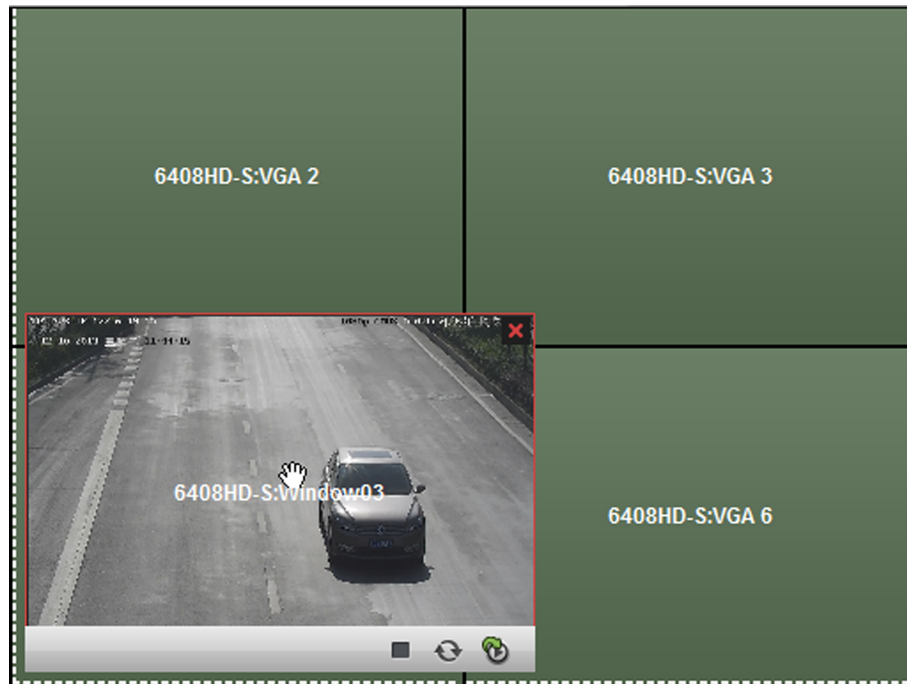
Figure 13-2 Move Window

   2) When the cursor becomes directional arrow, adjust the window size.

     ![Note icon]**Note**

     You can also hold the **Shift** key to scale the window in proportion.

   3) 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. Set the window division.

   1) Select a window and click ![icon] to set the window division for it.

   2) Click ![icon] to save the settings for it.

6. Optional: You can do one or more of the following.

Disable Roaming Function	Right-click on window and select **Lock** in the right-click menu, and the icon ![lock] shows on the top-right corner of the window. In this way, the window cannot be moved and resized.

📖**Note**

For the locked window, you can click-and-drag to create a new window on it.

Recover Roaming Function	Right-click on the window and select **Unlock** in the right-click menu.
Stop Decoding of Window	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. The window and it will be closed.
Close All Roaming Windows	Click 🔳 to close all the roaming windows.
Display the Latest Captured Picture	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.
Digital Zoom	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. --- 📖**Note** You can check the effect on the physical video wall. ---
Get a Preview of Video	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. --- 📖**Note** You can also double-click the preview window to get a full-screen view. ---

13.4.3 Display Playback on Video Wall

You can play the recorded video files on the video wall.

Before You Start
Add encoding devices stored with video files and decoders, and link decoding output with video wall.

Perform this task when you want to display playback on video wall.

Steps

☐ **Note**

Playback function is only supported by decoder.

1. Enter Video Wall module.
2. Drag a camera from the camera list on the left panel to a display window of video wall.
3. Go to the playback mode.
   - Move the cursor to the display window and click ⟳ appeared at the upper-right corner.
   - Right-click on the display window and select **Go to Playback** on the right-click menu.

   For cameras with video files of current day, playback will start automatically. Otherwise, you can perform the following step to search video files for playback.
4. **Optional:** Set time period or other search conditions and click **Search** at the left of playback mode page to search video files.

   The searched video files will start playback automatically.
5. **Optional:** Control the playback.
   - Move the cursor to the playback window to show icons on the window. You can realize the functions of pausing playback, stopping playback, capturing, starting recording, going back to live view mode, and adjusting playback speed via the appeared icons.
   - Right-click on the display window to control playback via the right-click menu, such as **Pause**, **Stop**, **Fast Forward**, **Slow Forward**, **Capture**, **Start Recording**, and **Full-Screen**.

   ☐ **Note**

   The saving path for the captured pictures and recorded files can be configured on System Configuration page. Refer to **Set File Saving Path** for details.

13.4.4 Configure Auto-Switch Decoding

The auto-switch 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.

Before You Start
Add encoding devices and decoders, and link decoding output with video wall.

Perform this task when you want to set auto-switch decoding for the video wall.

Steps

☐ **Note**

The auto-switch decoding is only supported by decoder.

1. Enter Video Wall Operation page.
2. Click ☐ beside ⟳ on the video wall toolbar to set switching interval for auto-switch decoding.
3. Drag a camera from the camera list on the left panel to a display window of video wall.

4. Move the cursor to a camera group node and click ⟳ appeared beside the node to start auto-switch decoding.

The display window of decoding output under auto-switch decoding will be marked with ⟳ at the upper-right corner.

Chapter 14 Security Control Panel

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

⬚ⁱNote

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 **_Account Management_** .

14.1 Configure Client Linkage for Zone Event

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

Perform this task when you need to configure the linkages for the security control panel zone's event.

Steps

⬚ⁱNote

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

1. Click **Event Management → Zone Event** .
2. Select a zone from the list.
3. Create a name for the zone.
4. Select the zone type.
5. Select the relay and siren to be linked.
6. Check the checkboxes to configure the client linkage.

   Audible Warning

   The client software gives an audible warning when alarm is triggered. You can select the alarm sound for audible warning.

   ⬚ⁱNote

   For setting the alarm sound, refer to **_Set Alarm Sound_** .

   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.

⬚ⁱNote

You should set the triggered camera first.

Alarm Triggered Video Wall Display

Display the video on the Video Wall when alarm is triggered.

⬚ⁱNote

You should set the triggered camera first.

7. Select the camera(s) to be triggered for displaying image or displaying video on the video wall when the alarm is triggered.

⬚ⁱNote

- To capture the picture of the triggered camera when the event occurs, you should set the capture schedule and the storage in Storage Schedule. For details, refer to *Remote Storage Configuration* .
- Up to 4 cameras can be set as the triggered cameras.

8. Optional: Click **Copy to...** to copy the event settings to other zones.
9. Click **Save**.

14.2 Remotely Control Security Control Panel

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.

14.2.1 Remotely Control Partitions

You can remotely control the security control panel's partitions such as away arming, stay arming, instant arming, disarming, clearing alarm, group bypass, and recovering group bypass.

Perform this task when you need to remotely control the partitions on the client software.

Steps
1. Click **Security Control Panel** on the control panel to enter the Security Control Panel module.
2. Optional: Click ☰ or ⚏ to at the upper right corner of the page to switch the display mode between the tile or list mode.
3. Optional: Click **Modify** to edit the partition name as you want and change the partition display status as show or hide.
4. In tile mode, click **Operation** to open the Partition Operation window. You can control the partitions in batch.
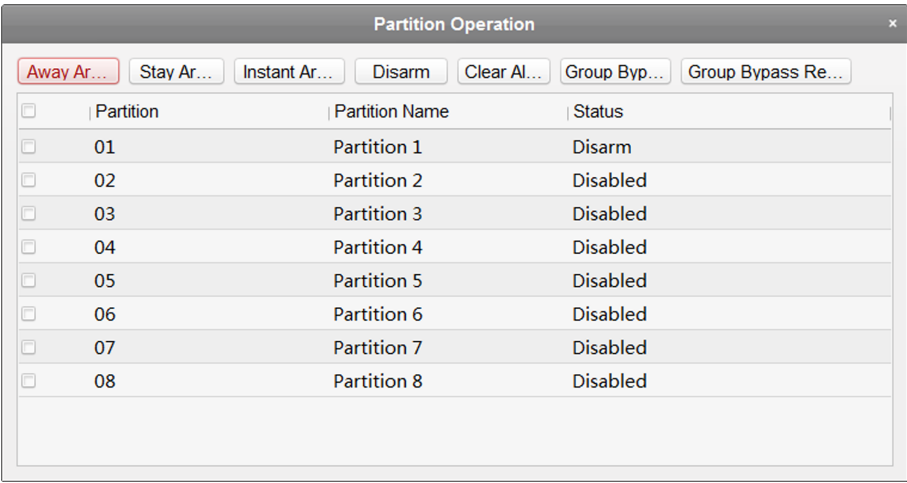
Figure 14-1 Partition Operation Window

5. Select the partition(s) to operate.
6. 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).
7. Display the partition's zone status if the partition is in alarm status.
   - For tile mode, hover the cursor over the 🔔 to display the partition's zone status.
   - For list mode, hover the cursor over the ⚠ to display the partition's zone status.

> **i Note**
> For the details about the triggered zone alarm, refer to **Handle Alarms** .

14.2.2 Remotely Control Zones

You can remotely control the security control panel's zones including bypass, or recover bypass.

Perform this task when you need to remotely control the zones on the client software.

Steps
1. Click **Security Control Panel** on the control panel.
2. **Optional:** Click ☰ or ⊞ to at the upper right corner of the page to switch the display mode between the tile or list mode.
3. Click 📑 open the Zone Operation window.

   You can view the all linked zones of the partition in this window and check the zone status.

4. Select the zone(s) for operation.
5. Click **Arm**, **Disarm**, **Bypass**, or **Bypass Recovery** to control the selected zones.
6. **Optional:** 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 *Configure Client Linkage for Zone Event* .

14.3 Display Zone on Map

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.

Perform this task if yo need to manage the security control panel's zones on the E-map.

Steps

Note

For detailed operations of E-map, refer to *Map Management*

1. Enter the E-map module.
2. Add zone on the E-map as hot spot.
   1) Click **Edit** on the toolbar to enter the map editing mode.
   2) Click on the E-map Toolbar to open the Add Hot Spot window. Or directly drag the zone icons from the group list on the left panel to the map.
   3) Select the zone(s) to be added.
   4) Click **OK**.

   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 .
3. Preview the added hot spots.
   1) Click **Exit Editing Mode** on the toolbar to enter the map preview mode.
   2) **Optional:** 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.

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 *Configure Client Linkage for Zone Event* .
- You can also check the zone alarm information in the Real-time Alarm module. For details, refer to *Handle Alarms* .

14.4 Handle Alarms

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.

14.4.1 View Real-Time Alarm

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.

Perform this task if you need to view the real-time triggered alarm information of the added security control panel.

Steps

1. 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.

2. **Optional:** Check **Alarm**, **Exception**, **Restore**, or **Operation** to show the alarms in corresponding type(s).

   $\boxed{i}$**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 ▮ .
   - The number after the alarm type indicates the alarm quantity of this type.

3. Acknowledge alarm.
   - Click 🖊 in the **Operation** column to acknowledge the selected alarm.
   - Click **Acknowledge in Batch** to acknowledge all the real-time triggered alarms.

   The acknowledged alarm will disappear from the list.

4. **Optional:** Click 👁 in the **Operation** column to view the live view of the triggered cameras.

   $\boxed{i}$**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 ***Configure Client Linkage for Zone Event*** .

5. **Optional:** Click 🗺 in the Operation column to check the zone as hot spot on the map.

   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 ***Display Zone on Map*** .

6. **Optional:** Subscribe the alarm types to receive desired alarms.
   1) Click **Subscribe** to open the Subscribe window.
   2) Click **Alarm**, **Exception**, **Restore**, or **Operation** to select the major alarm type(s).
   3) Check the checkbox(es) to select the minor alarm type(s).

4) Click **OK** to save the selections.

14.4.2 Search History Alarm

You can search the history alarms by time and filter the searching results by alarm type. You can also handle the matched alarms.

Perform this task if you need to search the security control panel's history alarms.

Steps

[i]**Note**

For details about operating the alarms, refer to ***View Real-Time Alarm*** .

1. Open the Real-time Alarm page.
2. In the Real-time Alarm module, click **History Alarm** tab to enter the History Alarm page.
3. Click 📅 to set the start time and end time of a time period.
4. Click **Search** button and the matched alarms will display on this page.
5. **Optional:** Filter the searching results by alarm type.
   1) Click **Filter** button to pop up the Filter dialog.
   2) Click **Alarm**, **Exception**, **Restore**, or **Operation** tab to select the major alarm type(s).

   [i]**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.
6. **Optional:** For the found alarms, click 🖊 or click **Acknowledge in Batch** to acknowledge the unacknowledged alarms

   The acknowledged alarm items will turn to gray.
7. **Optional:** Click 👁 and 🧍 to check the linked live view of the alarms and view the linked hot spots on the E-map.

   [i]**Note**

   For details about operating the alarms, refer to ***View Real-Time Alarm*** .

14.4.3 Handle Panic Alarm

For the panic alarm station, when the panic alarm is triggered, you can handle the alarm via the client. When the user calls the center from panic alarm station, the panic alarm will be triggered.

Perform this task when you need to handle the panic alarm triggered from panic alarm station.

Steps

1. Enter the Real-time Alarm module.
2. Click ![icon] on the pop-up Panic Alarm window to answer the call.
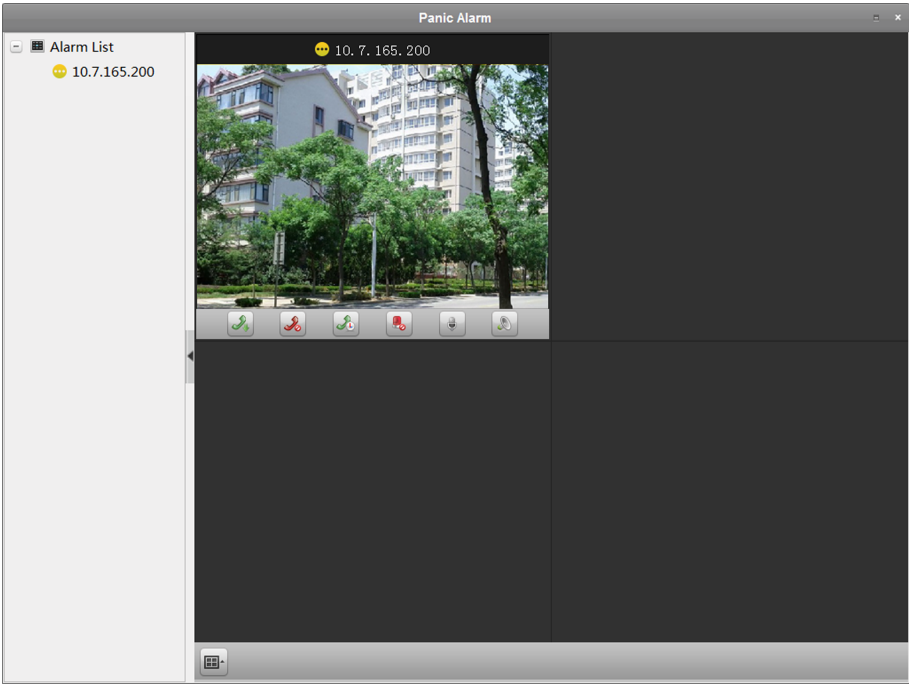
Figure 14-2 Handle Panic Alarm

3. **Optional:** Right-click on the live view window to open the right-click menu, and then perform the following operations.

Capture a Picture	Click ![icon] to capture a picture.
Start/Stop Recording	Click ![icon] / ![icon] to start or stop recording. ⓘ**Note** The video file is stored in the PC.
PTZ Control	If the zone is linked to the speed dome, click ![icon] to enable PTZ control function on the display window. Click ![icon] again to disable the function. ⓘ**Note** For setting the triggered camera, refer to *Configure Client Linkage for Zone Event* .

Chapter 15 Pyronix Control Panel

Pyronix control 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 *Display Zone on Map* .

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

---

[i]**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 *Account Management* .

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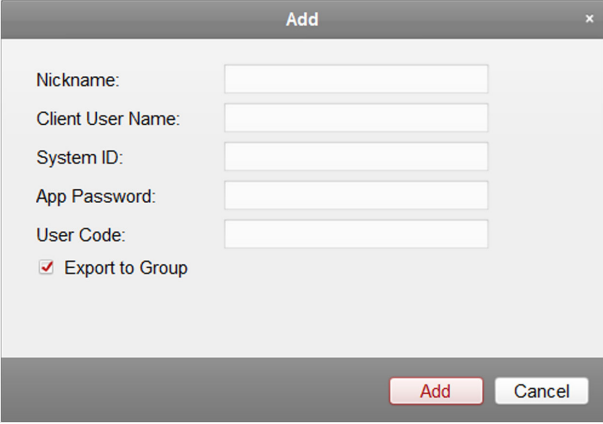
You can add the Pyronix control panel to the client in Device Management module. The device can be managed and controlled via the client once it is authorized by the device administrator on the PyronixCloud service.

Perform the following task to add Pyronix control panel to the client.

Steps
1. Open the Device Management page.
2. Display the Pyronic control panel tab on the device type panel.
   1) Click **Device → Add New Device Type** .
   2) Check **Pyronix Control Panel** and click **OK**.

   The Pyronix control panel will display in the device type panel.
3. Click **Pyronix Control Panel** tab to enter the Pyronix control panel management page.
4. Click **Add**.

Figure 15-1 Add Pyronix Control Panel

5. Input the required information for adding a Pyronix control panel on the dialog.

Client User Name

Set the user name which is used for applying the permission from PyronixCloud.

⌊**i**⌉**Note**

See *Authorize Client via PyronicCloud* for details.

System ID

The system ID of the Pyronix control panel. It is a unique serial number for each control panel.

⌊**i**⌉**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.

⌊**i**⌉**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.

⌊**i**⌉**Note**

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

6. **Optional:** Check **Export to Group** 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.

7. Click **Add** to add the Pyronix control panel.

8. **Optional:** Perform the following operations after adding a Pyronix control panel.

Modify	Select the device and click **Modify** to edit the device parameters.
Delete	Select the device and click **Delete** to delete the device.

   > ⓘ**Note**
   >
   > 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

Contact the administrator to authorize the client via the PyronixCloud. For details, refer to *Authorize Client via PyronicCloud* .

15.2 Authorize Client via PyronicCloud

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 the client software.

> ⓘ**Note**
>
> For one computer, you should ask for authorization if it is the first time to add the Pyronix control panel.

15.2.1 Create PyronixCloud Account

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

Perform the following steps to create a PyronixCloud account.

Steps

1. Go to *http://www.pyronixcloud.com* via PC to register an account.

Figure 15-2 Create PyronixCloud 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 log into PyronixCloud and connect your device.

3. Return to PyronixClound home page and log in.

15.2.2 Connect Device to PyronixCloud

You should connect device to PyronixCloud before you can authorize the client via PyronixCloud.

Perform the following steps to connect device to PyronixCloud.

Steps
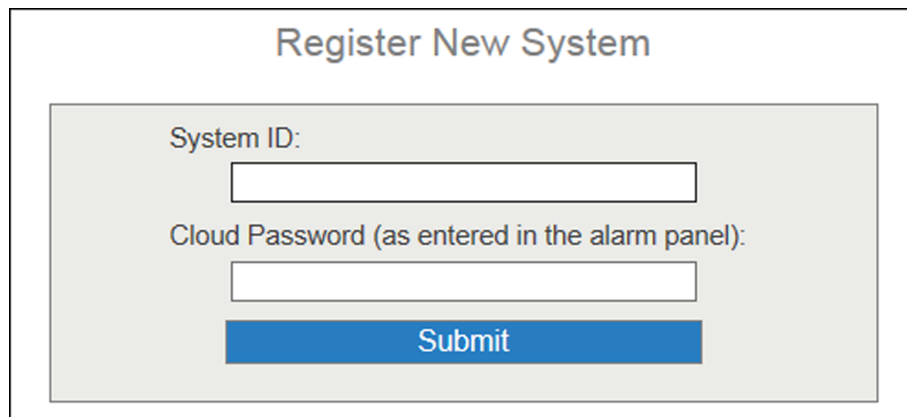
1. Go to ***http://www.pyronixcloud.com*** and log in to your PyronixCloud account.

> 📖**Note**
>
> If you don't have a PyronixCloud account, create one first. See ***Create PyronixCloud Account*** for details.

Figure 15-3 Connect Device to PyronixCloud

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

i **Note**

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.

3. Input the cloud password that you entered in the Pyronix device.

i **Note**

The cloud password should be set via the device. For details, refer to the specified device user manual.

4. Click **Submit**.
5. Input a system reference to set a different name for the device.
6. Click **Submit** to compete the operation.

i **Note**

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.

15.2.3 Authorize Client

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.

Perform the following steps to authorize the client software.

Steps

1. Register a PyronixCloud account and connect the Pyronix control panel to PyronixCloud.

   ![Note icon]**Note**

   See ***Create PyronixCloud Account*** and ***Connect Device to PyronixCloud*** for details.

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

   ![Note icon]**Note**

   The user name in the User column is the client user name you input when adding the Pyronix control panel. See ***Add Pyronix Control Panel*** for details.

3. Click ![On icon] next to the selected user.
4. Click **Save Now** to save the settings.

   The icon will turn to ![On icon] .

   Then you can access the device via the client successfully.

User	Last Connected	Permission	Notifications
1111	28/03/2017 13:49:58	On Off	✅ Enabled

   Figure 15-4 Authorize Client via PyronixCloud

15.3 Configure Client Linkage for Pyronix Control Panel Event

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.

Perform the following steps if you need to configure linkage actions for Pyronix control panel event.

Steps

1. Open the Event Management page.
2. Click **Pyronix Control Panel Event**.

   The added Pyronix control panel is displayed in the list on the left.

3. Click ![+ icon] to unfold the zone list and select ![icon] to configure its zone event linkage.

   ![Note icon]**Note**

   You can also click ![icon] to configure device event linkage for Pyronix control panel.

4. In the Trigger Camera field, select the camera to be triggered for showing image when the alarm is triggered.

⌐ⁱ⌐**Note**

- 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 **_Remote Storage Configuration_** .
- Up to one camera can be set as the triggered camera.

5. Check **Trigger Client Action** to activate the client linkage actions.

   You can check the detailed actions as the client linkage. See the detailed actions below for details:

   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 **_Set Alarm Sound_** .

   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.

   ⌐ⁱ⌐**Note**

   You should set the triggered camera first.

   Alarm on E-map

   Display the zone's alarm information on the E-map.

   ⌐ⁱ⌐**Note**

   This linkage is only available for device event.

6. **Optional:** Click **Copy to...** to copy the event settings to other zones.
7. Click **Save** to save the settings.

15.4 Remotely Control Pyronix Control Panel

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.

15.4.1 Remotely Control Partition

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

Perform this task if you need to remotely control partition.

Steps

1. Click **Pyronix Control Panel** on the Control Panel to enter the Pyronix Control Panel page.

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

   ⓘ**Note**
   - The device name will turn gray if it is offline.
   - If the partition is in fault status, an ⚠ will display near the partition name. You can hover ⚠ to view the fault details if the partition is in fault status.

2. **Optional:** Click **Modify** to edit the partition name as you want and change the partition display status as **Show** or **Hide**.
3. Click on the switch of each partition to arm or disarm the partition.
4. **Optional:** Hover over the 📄 to view the last operation.

15.4.2 Remotely Control Zone

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.

Perform this task when you need to remotely control the zone of Pyronix control panel.

Steps

1. Click **Pyronix Control Panel** on the Control Panel to enter the Pyronix Control Panel module.
2. Click **Zone** to open the Zone Control window.

   The zones will be displayed.

   You can view the zone details including zone No., name, and its location.

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

3. Perform bypass control.

Bypass	Select the zone and click **Bypass**to bypass the zone.
Recover	Select the zone and click **Bypass Recovery** to recover the bypass.

15.4.3 Remotely Control Connected Alarm Output

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

Perform the following steps to remotely control connected alarm output.

Steps

1. Click **Pyronix Control Panel** on the Control Panel to enter the Pyronix Control Panel module.
2. Click **Output** to open the Alarm Output Control window.

   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.

3. Perform alarm output control.
- Select the alarm output and click **Open** to turn on the alarm output.

> ⓘ**Note**
>
> The countdown will start in pulse time. When the countdown finishes, the output status will turn to **Off** automatically.

- Select the alarm output and click **Close** to turn off the alarm output.

Chapter 16 Access Control

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 **Account Management** .

16.1 Select Application Scenario

For the first time entering the Access Control module, you are required to select the access control's application scenario as residence or non-residence according to the actual needs.

Perform this task if you need to select the access control's application scenario when entering the Access Control module for the first time.

Steps

Note

Once the scene is configured, you cannot change it.

1. Enter the Access Control module.

   The Select Scene window will pop up.
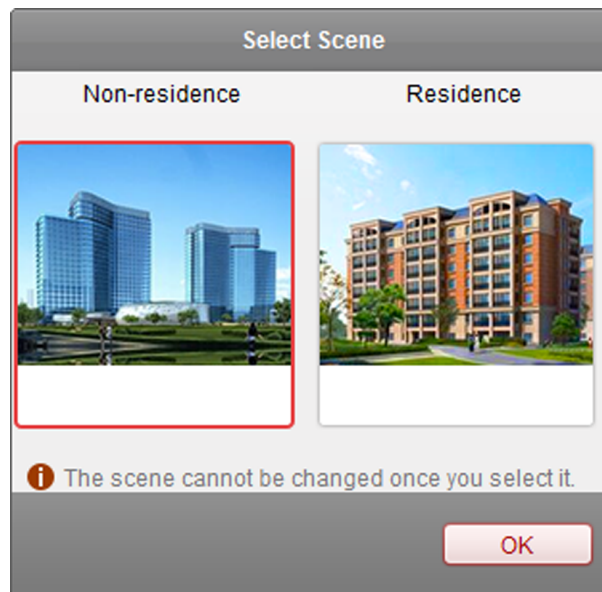
Figure 16-1 Select Access Control Application Scenario

2. Select the scene as residence or non-residence according to the actual needs.

ⓘNote

If you select **Residence** mode, you cannot configure person's attendance rule when adding person.

3. Click **OK**.

16.2 Configure Device Parameters

After adding the access control device, you can set its parameters such as network parameters, capture parameters, RS-485 parameters, Wiegand parameters, etc.

16.2.1 Set Network Parameters

After adding the access control device, you can set the device log uploading mode, and create EHome account via wired or wireless network.

Set Log Uploading Mode

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

Perform this task when you need to set the access control device's log uploading mode.

Steps
1. Click **Access Control → Device Management** to enter the Device Management page.

2. Select the device in the device list and click **Modify**.

3. Click **Network Settings → Uploading Mode** to enter the Uploading Mode page.

4. Select the center group from the drop-down list.

5. Check **Enable** to enable to set the oploading mode.

6. Select the uploading mode from the drop-down list.
   - Enable **N1** or **G1** for the main channel and the backup channel.
   - Select **Close** to disable the main channel or the backup channel

> ℹ️ **Note**
>
> The main channel and the backup channel cannot enable N1 or G1 at the same time.

7. Click **Save**.

Create EHome Account in Wire Communication Mode

You can set the account for EHome protocol in wire communication mode. Then you can add devices via EHome protocol.

Perform this task when you need to create EHome account in wire communication mode for access control device.

Steps

> ℹ️ **Note**
>
> This function should be supported by the device

1. Click **Access Control → Device Management** to enter the Device Management page.

2. Select the device in the device list and click **Modify**.

3. Click **Network Settings → Network Center** to enter the Network Center page.

4. Select the center group from the drop-down list.

5. Select the **Address Type** as **IP Address** or **Domain Name**.

6. Input IP address or domain name according to the address type.

7. Input the port number for the protocol.

> ℹ️ **Note**
>
> The port number of the wireless network and wired network should be consistent with the port number of EHome.

8. Select the **Protocol Type** as **EHome**.

9. Set an account name for the network center.

10. Click **Save**.

Create EHome Account in Wireless Communication Mode

You can set the account for EHome protocol in wireless communication mode. Then you can add devices via EHome protocol.

Perform this task when you need to create EHome account in wireless communication mode for access control device.

Steps

ⓘ**Note**

This function should be supported by the device

1. Click **Access Control → Device Management** to enter the Device Management page.
2. Select the device in the device list and click **Modify**.
3. Click **Network Settings → Wireless Communication Center** to enter the Wireless Communication Center page.
4. Select the **APN Name** as **CMNET** or **UNINET**.
5. Input the SIM Card No.
6. Select the center group from the drop-down list.
7. Input the IP address and port number.

   ⓘ**Note**

   • By default, the port number for EHome is 7660.
   • The port number of the wireless network and wired network should be consistent with the port number of EHome.

8. Select the **Protocol Type** as **EHome**.
9. Set an account name for the network center.
10. Click **Save**.

16.2.2 Set Device Capture Parameters

You can configure the device capture parameters, including manual capture and linked capture.

ⓘ**Note**

• 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 *Remote Storage Configuration* .

Set Triggered Capture Parameters

You can set the triggered capture parameters for the device with capture function.

Before You Start

Before setting the capture setting, you should configure the storage server for picture storage. For details, refer to *Remote Storage Configuration* .

Perform this task when you need to set triggered capture parameters.

Steps

⚠**Note**

This function should be supported by the device

1. Click **Access Control → Device Management** to enter the Device Management page.
2. Select the device in the device list and click **Modify**.
3. Click **Capture Settings → Linked Capture** to enter the Linked Capture page.
4. Set the picture size and quality.
5. Set the capture times once triggered.
6. Set the capture interval according to the capture times.
7. Click **Save**.

Set Manual Capture Parameters

You can set the manual capture parameters for the device with capture function.

Before You Start

Before setting the capture setting, you should configure the storage server for picture storage. For details, refer to *Remote Storage Configuration* .

Perform this task when you need to set manual capture parameters.

Steps

⚠**Note**

This function should be supported by the device

1. Click **Access Control → Device Management** to enter the Device Management page.
2. Select the device in the device list and click **Modify**.
3. Click **Capture Settings → Manual Capture** to enter the Manual Capture page.
4. Select the resolution of the captured pictures from the drop-down list.
5. Select the picture quality as **High**, **Medium**, or **Low**.
6. Click **Save**.
7. **Optional:** Click **Restore Default Value** to restore the parameters to default settings.

16.2.3 Set RS-485 Parameters

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

Perform this task when you need to set the access control device's RS-485 parameters.

Steps

[i]**Note**

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

1. Click **Access Control → Device Management** to enter the Device Management page.
2. Select the device in the device list and click **Modify**.
3. Click **RS-485 Settings** to enter the RS-485 settings page.
4. Select the serial port number from the dropdown list to set the RS-485 parameters.
5. Set the baud rate, data bit, the stop bit, parity type, communication mode, working mode, and connection mode in the dropdown list.
6. Click **Save**.
   - The configured parameters will be applied to the device automatically.
   - After changing the working mode, the device will reboot automatically.

16.2.4 Set Weigand Parameters

You can set the access control device's Wiegand channel and the communication mode.

Perform this task when you need to set access control device's Weigand parameters.

Steps

[i]**Note**

This function should be supported by the device

1. Click **Access Control → Device Management** to enter the Device Management page.
2. Select the device in the device list and click **Modify**.
3. Click **Wiegand Settings** to enter the Wiegand Settings page.
4. Select the Wiegand channel No. and the communication mode from the drop-down list.

   [i]**Note**

   If you set **Communication Direction** as **Send**, you are required to set the **Wiegand Mode** as **Wiegand 26** or **Wiegand 34**.

5. Click **Save**.
   - The configured parameters will be applied to the device automatically.
   - After changing the communication direction, the device will reboot automatically.

16.2.5 Authenticate M1 Card Encryption

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.

Before You Start
Use the specified card enrollment station to issue card. See *Issue a General Card to Person* for details.

Perform this task when you need to enble M1 card encryption function.

📖 **Note**

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

Steps
1. Click **Access Control → Device Management** to enter the access control device management page.
2. Select the device in the device list, and click **Modify** to pop up Modify window.
3. Click **M1 Card Encryption** tab to enter the M1 Card Encryption page.
4. Check **Enable** checkbox to enable the M1 card encryption function.
5. Set the sector ID.

   The sector ID ranges from 1 to 100.

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

16.3 Manage Organization

You can manage the organization as desired, such as adding, editing, or deleting the organization.

Perform this task when you need to manage organization.

Steps
1. Click **Access Control → Person and Card** to enter the person and card management page.
2. Click **Add** to pop up Add Organization window.
3. Create a name for the organization.
4. Click **OK**.

   📖 **Note**

   Up to 10 levels of organizations can be added.

   ---

5. **Optional:** After adding the organization, you can do one or more of the following operations.

Edit Organization	Select the added organization and click **Modify** to modify its name.
Delete Organization	Select the added organization and click **Delete** to delete it.

> **Note**
> - 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.

16.4 Manage Person Information

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.

16.4.1 Add Single Person

You can add person to the client software one by one and input the person information such as basic information, detailed information, access control permission, linked card, linked face picture, linked fingerprint, and attendance rule.

Configure Person's Basic Information

You can add person to the client software one by one and configure the person's basic information such as name, gender, phone number, etc.

Perform this task when you need to configure the person's basic information when adding person.

Steps
1. Enter **Access Control → Person and Card** .
2. Select an organization in the organization list to add the person.
3. Click **Add** to open the adding person window.

   The Person No. will be generated automatically and is not editable.
4. Input the basic information including person name, gender, phone No., birthday details, and email address.
5. **Optional:** Set the person's picture.
   - Click **Upload Picture** to select the person picture from the local PC to upload it to the client.
   - Click **Take Photo** to take the person's photo with the PC camera.
6. Confirm to add the person.
   - Click **OK** to add the person and close the Add Person window.
   - Click **Save and Continue** to add the person and continue to add other persons .

Configure Person's Detailed Information

When adding person, you can configure the detailed information for the person, such as person's ID type, ID No., country, etc., according to actual needs.

Perform this task when you need to configure the person's detailed information.

Steps
1. Enter **Access Control → Person and Card** .
2. Select an organization in the organization list to add the person and click **Add**.

> **Note**
>
> Input the person's basic iformation first. For details about configuring person's basic information, refer to *Configure Person's Basic Information* .

3. Click **Details** tab.
4. Input the detailed information of the person, including person's ID type, ID No., country, etc., according to actual needs.

   Linked Device

   bind the indoor station to the person.

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

5. Confirm to add the person.
   - Click **OK** to add the person and close the Add Person window.
   - Click **Save and Continue** to add the person and continue to add other persons .

Assign Permission to Person

When adding person, you can assign the permissions (including operation permissions of access control device and access control permissions) to the person.

Perform this task when you need to assign access control permission to the person.

Steps

> **Note**
>
> For setting the access control permission, refer to *Assign Permission to Person* .

1. Enter **Access Control → Person and Card** .
2. Select an organization in the organization list to add the person.
3. Click **Add**.
4. Input person's basic information.

📖**i**Note

For details about configuring person's basic information, refer to ***Configure Person's Basic Information*** .

---

5. Click **Permission** tab.
6. In the Permission(s) to Select list, check the permission(s) checkbox(es) and click **>** to add to the Selected Permission(s) list.
7. Confirm to add the person.
  - Click **OK** to add the person and close the Add Person window.
  - Click **Save and Continue** to add the person and continue to add other persons .

Issue a General Card to Person

When adding person, you can issue a general card with a unique card number to the person.

Perform this task when you need to issue a general card to the person.

Steps
1. Enter **Access Control → Person and Card** .
2. Select an organization in the organization list to add the person and click **Add**.

📖**i**Note

Input the person's basic information first. For details about configuring person's basic information, refer to ***Configure Person's Basic Information*** .

---

3. Click **Credential → Card** tab to enter the card credential settings page.
4. Click **Add** and select **General Card** tab to enter the general card configuration page.
5. Set card parameters.
  1) Select a card type for the general 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.

2) **Optional:** In the Remark field, input the remark information for the card if needed.

ⓘ**Note**

Up to 32 characters are allowed in the Remark field.

3) In the Card Password field, create a password (4 to 8 digits) for the card itself.

ⓘ**Note**

The password will be required when the card holder swiping the card to enter or exit the door if the card reader authentication mode requires password. For details, refer to ***Configure Card Reader Authentication Mode and Schedule*** .

4) Set the effective time and expiry time of the card.

6. Select the reading card mode and input the card number.

- Access Controller Reader

   a. Place the card on the reader of the Access Controller.

   b. Click **Read** to get the card number.

- Card Enrollment Station

   a. Connect the card enrollment station with the PC running the client.

   b. Click **Set Card Enrollment Station** to set the card enrollment station's parameters.

   c. 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.

   d. Set the serial port number, the baud rate, the timeout value, the buzzing, or the card number type.

   e. Optional: If the card is M1 card, and if you need to enable the M1 Card Encryption function, you should check **Enable** 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.

   f. Click **Save**.

g. Place the card on the card enrollment station.

h. click **Read**to get the card No.

- Manually Input

a. Input the card number manually.

b. Click **Enter** to input the card number.

7. Click **OK**.

The card(s) will be issued to the person.

8. Optional: You can do one or more of the followings after issuing to person.

Generate QR Code	Click **QR Code** to generate the card QR code for QR code authentication.
	ⓘ**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.
Link Fingerprint	Click **Link Fingerprint** to link the card with the person's fingerprint.
	The person can place the finger on the scanner instead of swiping card when passing the door.
Link Face Picture	Click **Link Face Picture** to link the card with the face picture.
	The person can pass the door by scanning the face via the device instead of swiping card when passing the door.

9. Confirm to add the person.

- Click **OK** to add the person and close the Add Person window.
- Click **Save and Continue** to add the person and continue to add other persons .

Uploading Person's Face Picture

When adding person, you can collect the person's face picture via uploading the face picture stored in local PC.

Perform this task when you need to collect the person's face picture via uploading face picture.

Steps

1. Enter **Access Control → Person and Card** .

2. Select an organization in the organization list to add the person and click **Add**.

ⓘ**Note**

Input the person's basic information first. For details about configuring person's basic information, refer to ***Configure Person's Basic Information*** .

3. Click **Credential → Face Picture** tab to enter the card credential settings page.

4. Select the collection mode as **Local Uploading**.

5. **Optional:** Check **Verify by Device** and select the device for recognizing the face using the device.
6. Click **Upload Picture** to upload the local face picture.
7. **Optional:** Collect face picture.
   1) Click **Collect** to capture the face picture.
   2) **Optional:** Click **Re-Collect** to collect the captured picture again
8. **Optional:** Click **Delete** to delete the uploaded picture or captured picture.
9. Confirm to add the person.
   - Click **OK** to add the person and close the Add Person window.
   - Click **Save and Continue** to add the person and continue to add other persons .

Collect Person's Face Picture Locally

When adding person, you can collect the person's face picture via the face picture scanner connected to the PC running the client.

Perform this task when you need to collect the person's face picture via face picture scanner.

Steps
1. Enter **Access Control → Person and Card** .
2. Select an organization in the organization list to add the person and click **Add**.

   ⓘ**Note**

   Input the person's basic information first. For details about configuring person's basic information, refer to ***Configure Person's Basic Information*** .

3. Click **Credential → Face Picture** tab to enter the card credential settings page.
4. Select the collection mode as **Local Collection**.
5. Connect the face picture scanner to the PC running the client.

   ⓘ**Note**

   You can click **Initialize** to initialize the face picture scanner.

6. Collect face picture.
   1) Click **Collect** to capture the face picture.
   2) **Optional:** Click **Re-Collect** the captured picture again
   3) **Optional:** Click **Delete** to delete the captured picture.
7. Confirm to add the person.
   - Click **OK** to add the person and close the Add Person window.
   - Click **Save and Continue** to add the person and continue to add other persons .

Collect Person's Face Picture Remotely

When adding person, you can collect the person's face picture via access control terminal which supports face recognition function.

Perform this task when you need to collect the person's face picture via access control terminal.

Steps
1. Enter **Access Control → Person and Card** .
2. Select an organization in the organization list to add the person and click **Add**.

> **ⓘ Note**
>
> Input the person's basic information first. For details about configuring person's basic information, refer to **Configure Person's Basic Information** .

3. Click **Credential → Face Picture** tab to enter the card credential settings page.
4. Select the collection mode as **Remote Collection**.
5. Click **Select Device** to select the access control terminal which supports face recognition function.
6. Collect face picture.
   1) Click **Collect** to capture the face picture.
   2) **Optional:** Click **Re-Collect** the captured picture again
   3) **Optional:** Click **Delete** to delete the captured picture.
7. Confirm to add the person.
   - Click **OK** to add the person and close the Add Person window.
   - Click **Save and Continue** to add the person and continue to add other persons .

Collect Person's Fingerprint Locally

When adding person, you can collect the person's fingerprint information via the fingerprint machine connected to the PC running the client.

Perform this task when you need to collect the person's fingerprint via the fingerprint machine connected to the PC running the client.

Steps
1. Enter **Access Control → Person and Card** .
2. Select an organization in the organization list to add the person and click **Add**.

> **ⓘ Note**
>
> Input the person's basic information first. For details about configuring person's basic information, refer to **Configure Person's Basic Information** .

3. Click **Credential → Fingerprint** tab to enter the card credential settings page.
4. Select the collection mode as **Local Collection**.

5. Connect the fingerprint machine to the PC and set its parameters.

   1) Click **Set Fingerprint Machine** to open the setting fingerprint machine window.

   2) Select the device type.

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

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

> 🛈**Note**
>
> - 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 collection is over.

   4) Click **Save**.

6. Collect the fingerprint.

   1) Click **Start**.

   2) Select a fingerprint on the hand picture to start collecting.

   3) Lift and rest the corresponding fingerprint on the fingerprint scanner twice to collect the fingerprint.

> 🛈**Note**
>
> When the same fingerprints of one person are collected, the prompt with repeat ID appears. When the similar fingerprints are collected for different person, the prompt with repeat ID and person name appears.

7. Confirm to add the person.

   - Click **OK** to add the person and close the Add Person window.

   - Click **Save and Continue** to add the person and continue to add other persons .

Collect Person's Fingerprint Remotely

When adding person, you can collect the person's fingerprint information via the remote access control device's fingerprint module.

Perform this task when you need to collect the person's fingerprint via the fingerprint module of the access control device.

Steps

1. Enter **Access Control → Person and Card** .

2. Select an organization in the organization list to add the person and click **Add**.

⌐**i**¬**Note**

Input the person's basic information first. For details about configuring person's basic information, refer to *Configure Person's Basic Information* .

3. Click **Credential → Fingerprint** tab to enter the card credential settings page.
4. Select the collection mode as **Remote Collection**.
5. Click **Select Device** and select an access control device to collect the fingerprint.

⌐**i**¬**Note**

The function should be supported by the device.

6. Collect the fingerprint.
    1) Select a fingerprint on the hand picture to start collecting.
    2) Lift and rest the corresponding fingerprint on the device's fingerprint module to collect the fingerprint.

⌐**i**¬**Note**

When the same fingerprints of one person are collected, the prompt with repeat ID appears. When the similar fingerprints are collected for different person, the prompt with repeat ID and person name appears.

7. Confirm to add the person.
    - Click **OK** to add the person and close the Add Person window.
    - Click **Save and Continue** to add the person and continue to add other persons .

Configure Person's Attendance Rule

When adding person, you can configure the person's attendance rule if the application scenario is non-residence mode and the person joins in the time and attendance.

Perform this task when you need to configure the person's attendance rule when adding person.

Steps

⌐**i**¬**Note**

For details about attendance settings and application, refer to *Time and Attendance* .

1. Enter **Access Control → Person and Card** .
2. Select an organization in the organization list to add the person and click **Add**.
3. Input person's basic information.

⌐**i**¬**Note**

For details about configuring person's basic information, refer to *Configure Person's Basic Information* .

4. Click **Attendance Rule** tab.

> ⓘ**Note**
>
> This tab page will display when you select **Non-Residence** mode as the application scene when running the software for the first time. For details, refer to *Select Application Scenario* .

5. If the person joins in the time and attendance, check **Time and Attendance** to enable this function for the person.

The person's card swiping records will be recorded and analyzed for time and attendance.

6. Set attendance rule for the person.

> ⓘ**Note**
>
> For details about Time and Attendance, click **More** to go to the Time and Attendance module.

7. Confirm to add the person.
- Click **OK** to add the person and close the Add Person window.
- Click **Save and Continue** to add the person and continue to add other persons .

16.4.2 Batch Import and Export Person Information

You can import the information and pictures of multiple persons to the client software in a batch. Meanwhile, you can also export the person information and pictures and save them in your PC.

Import Person Information

You can import the information of multiple persons (including identity information, fingerprint data, and fingerprint linked card number) to the client software in a batch by importing an Excel file from the local PC.

Perform this task when you need to import the person information to the client in a batch.

Steps
1. Enter **Access Control → Person and Card** .
2. Click **Import Person** and select **Person Information** as the content to import.
3. In the pop-up window, click **Download Template for Importing Person** to download the template first.
4. Input the person information in the downloaded template.

f1 to f10

The person's fingerprint data.

f1card to f10card

The fingerprint's linked card number. If it links to no card, leave it empty.

> **i** **Note**
>
> If the person has multiple cards, separate the card No. with semicolon.

5. Select the Excel file with person information.
6. Click **OK** to start importing.

> **i** **Note**
>
> If the person No. already exists in the client software's database, it will replace the person information automatically after importing.

Import Person Pictures

After adding the persons, you can import multiple person pictures in a batch by importing a ZIP file with pictures to the client software.

Perform this task when you need to import the persons' pictures to the client in a batch.

Steps
1. Name the person picture after the person name.

> **i** **Note**
>
> The picture should be in JPG format and smaller than 200 KB.

2. Compress the file which contains the person pictures to ZIP format.
3. Enter **Access Control → Person and Card** module.
4. Click **Import Person** and select **Person Pictures** as the content to import.
5. In the pop-up window, select the ZIP file.
6. Click **OK** to start importing.

> **i** **Note**
>
> By default, the imported person picture is linked with the person's first card.

The importing progress and result will show.

Export Person Information

You can export the added persons' information to the local PC in an Excel file.

Perform this task when you need to export the added person information in a batch.

Steps
1. Enter **Access Control → Person and Card** module.
2. Click **Export Person** and select **Person Information** as the content to export.
3. Select the path for saving the exported Excel file.

4. Select the items of person information to export.
5. Click **OK** to start exporting.

> **f1 to f10**
>
> The person's fingerprint data.
>
> **f1card to f10card**
>
> The fingerprint's linked card number. If it links to no card, leave it empty.

Export Person Pictures

You can export the pictures of the added persons and save it in your PC.

Perform this task if you want to export the added persons' pictures.

Steps
1. Enter **Access Control → Person and Card** module.
2. Click **Export Person** and select **Person Pictures** as the content to export.
3. Select the path for saving the exported ZIP file.
4. Click **OK** to start exporting.

> **⌕ⁱNote**
> • The exported file is in ZIP format.
> • The person picture is named after the person name.

16.4.3 Get 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.

Perform this task when you need to get the configured person informatio from the access control device.

Steps

> **⌕ⁱNote**
> • This function is only supported by the device the connection mothod of which is TCP/IP when adding the device.
> • 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.

1. Enter **Access Control → Person and Card** .
2. Select an organization to import the persons.

3. Click **Get Person** to open the selecting device window.

The added access control device will be displayed.

4. Start getting the person information.
- Select the device and then click **OK** to start getting the person information from the device.
- Double click the device name to start getting the person information.

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.

16.4.4 Issue Cards to Person in Batch

You can issue multiple cards to one person in batch.

Perform this task when you need to issue multiple cards to one person.

Steps
1. Enter **Access Control → Person and Card** .
2. Click **Issue Card in Batch**.

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

3. Set the parameters for the cards.
1) Select the card type according to actual needs.

> **⌷i Note**
>
> For details about the card type, refer to *Issue a General Card to Person* .

2) In the Card Password field, create a password (4 to 8 digits) for the card itself.

> **⌷i Note**
>
> The password will be required when the card holder swiping the card to enter or exit the door if the card reader authentication mode requires password. For details, refer to *Configure Card Reader Authentication Mode and Schedule* .

3) Input the card quantity issued for each person.

Example

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

4) Set the effective time and expiry time of the card.
4. In the Person(s) with No Card Issued list on the left, select the person to issue cards.
5. Select the reading card mode and input the card number.

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.

⌐**i**⌐**Note**

The Card Enrollment Station should connect with the PC running the client. You can click **Set Card Enrollment Station** to set the card enrollment station's parameters. For details, refer to *Issue a General Card to Person* .

Manually Input

Input the card No. manually and click **Enter** to input the card No.

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

6. Click **OK**.

16.4.5 Search Person Information

After adding the person information to the client, you can search the person by setting the search conditions.

It provides normal search and advanced search to search the person.

Normal Search

After adding the person information to the client, you can search the person by person name or card number.

Perform this task if you want to search the person information by person name or card number.

Steps
1. Enter **Access Control → Person and Card** module.
2. Set the search condition.
   - To search the person by person name, input the keyword of the person name in the search field.
   - To search the person by card number, input the keyword of the card number in the search field manually, or click **Read** to read the card number from certain card by card enrollment station.

⌐**i**⌐**Note**

Before reading by card enrollment station, you need to connect the card enrollment station with the PC running the client first. You can click **Read → Set Card Enrollment Station** to set its parameters. For details, refer to *Issue a General Card to Person* .

3. Click **Search**.

The search results will display in the person list.

Advanced Search

After adding the person information to the client, you can search the target person by setting more accurate search conditions, including card number, person name, person number, and gender.

Perform this task if you need to search the target person with more accurate search conditions.

Steps
1. Enter **Access Control → Person and Card** module.
2. Click **Advanced Search** to display the search conditions.
3. Set the search condition.

   Card No.

   Input the keyword of the card number, or click **Read** to read the card number from certain card by card enrollment station.

   ⓘ**Note**

   Before reading by card enrollment station, you need to connect the card enrollment station with the PC running the client first. You can click **Read → Set Card Enrollment Station** to set its parameters. For details, refer to *Issue a General Card to Person* .

   Person No.

   Input the keyword of the person number.

   Person Name

   Input the keyword of the person name.

   ⓘ**Note**

   The person name is case sensitive.

4. Click **Search**.

   The search results will display in the person list.

5. **Optional:** Click **Reset** to clear the search conditions.

16.4.6 Report Card Loss

If the person lost his/her card, you can report the card loss so that the related access control permission will be deleted.

Perform this task if you need to report the card loss for the person who lost his/her card.

Steps
1. Enter **Access Control → Person and Card** module.
2. **Optional:** Search the person you want to report card loss for.

> **ℹ Note**
>
> For searching the person, refer to ***Search Person Information*** .

3. Select the person and click **Modify** to open the Edit Person window.
4. Click **Credential → Card** tab to show the person's card information
5. Select the lost card and click **Report Card Loss**.

   The card status will turn to lost.

6. **Optional:** If the lost card is found, you can select the card and click **Cancel Card Loss** to cancel the loss.

   The card status will turn to normal.

7. **Optional:** If you have assigned access permission to the person, a window will pop up to notify you to apply the permission to the device again to take effect. You can click **Apply Now** or **Apply Later** to apply the permission changes to the device.

16.5 Configure Schedule and Template

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.

> **ℹ Note**
>
> For access control permission settings, refer to ***Assign Permission to Person*** .

16.5.1 Add Week Schedule

You can add custom week schedule to make the access control permission valid or invalid in the configured schedule of the week.

Perform this task when you want to add custom week schedule.

Steps
1. Click **Access Control → Schedule and Template → Week Schedule** to enter the Week Schedule Management page.

   > **ℹ Note**
   >
   > There are two default week schedules: Whole Week Schedule and Blank Schedule, and they cannot be edited or deleted.

   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.

2. Add a week schedule.
   1) Click **Add Week Schedule** to open the Add Week Schedule dialog.
   2) Input a desired name in the **Week Schedule Name** field.
   3) Click **OK** to add the week schedule.
3. Click the added week schedule in the left list to show its property on the right.
4. Select a day of the week and draw time periods on the timeline bar.

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

5. Optional: Perform one of the following operations to edit the drawn time periods.
   - Move the cursor to the time period and drag the time period on the timeline bar to the desired position when the cursor turns to 🖐 .
   - Click the time period and directly edit the start/end time in the appeared dialog.
   - Move the cursor to the ends of time period and drag to lengthen or shorten the time period when the cursor turns to ⬅➡ .
6. Optional: After setting the time schedule, you can do one or more of the following operations.

Delete Day Schedule	Select a day and click **Delete Duration** to delete the schedule of the selected day.
Clear Week Schedule	Click **Clear** to delete the whole week schedule.
Copy to Whole Week	Click **Copy to Week** to copy the schedule of this day to the whole week.

7. Click **Save** to saving the settings and finishing adding the week schedule.

16.5.2 Add Holiday Schdule

You can create a schedule for holidays and set the days in the holiday schedule, including start date, end date, and holiday duration in one day.

Perform this task when you need to add a holiday schedule to pre-define the holidays.

Steps
1. Click **Access Control → Schedule and Template → Week Schedule** to enter the Holiday Group Management page.
2. Add a holiday group.
   1) Click **Add Holiday Group** on the left to open the adding holiday group window.
   2) Create a name for the holiday group.
   3) Click **OK**.
3. Add a holiday period to the holiday group and configure the holiday duration.

Note

Up to 16 holiday periods can be added to one holiday group.

1) Click **Add Holiday**.
2) 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 to one holiday period.

3) **Optional:** 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.
4) **Optional:** When the cursor turns to ⟷ , you can lengthen or shorten the selected time bar.

4. Click **Save**.

16.5.3 Add Template

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

Perform this task if you want to add and configure template.

Steps

1. Click **Access Control → Schedule and Template → Template** to enter the Template Management page.

Note

There are two default templates: Whole Week Template and Blank Template, and they cannot be edited or deleted.

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.

2. Add a template.
   1) Click **Add Template** to open Add Template window.
   2) Input a name in the **Template Name** filed.
   3) Click **OK** to add the template.
3. Click the added template in the left list to show its property on the right.
4. Add a week schedule to apply to the template.
   1) Click **Week Schedule** tab on the right.
   2) In the Week Schedule field, select a configured week schedule.
   3) **Optional:** Click **Add Week Schedule** to add a new week schedule.

⌷**i**|**Note**

For details about adding a week schedule, refer to ***Add Week Schedule*** .

5. Add a holiday group schedule to apply to the template.

⌷**i**|**Note**

Up to four holiday groups can be added to one template.

1) Click **Holiday Group** tab.
2) Select a holiday group in the list.
3) **Optional:** Click **Add Holiday Group** to add a new holiday group schedule.

   ⌷**i**|**Note**

   For details about adding a holiday group, refer to ***Add Holiday Schdule*** .

4) Click **Add** to add the selected holiday group schedule to the right list.
5) **Optional:** Select a selected holiday group on the right list and click **Delete** to remove the selected one.

6. Click **Save** to save the settings and finish adding the template.

16.6 Manage Permission

After adding the person and configuring the person's credentials, you can create the access permissions to define the access level of which person(s) can get access to which door(s).

16.6.1 Assign Permission to Person

You can assign permission to persons so that person can enter or exist the access control points (doors) according to the assigned permission.

Perform this task if you need to assign access permissions to persons.

Steps
- You can add up to 4 permissions to one access control point of one device.
- You can add up to 128 permissions in total.
- When the permission settings are changed, you need to apply the permissions to the devices again to take effect. The permission changes include changes of schedule and template, permission settings, person's permission settings, and related person details (including card number, fingerprint, face picture, linkage between card number and fingerprint, linkage between card number and fingerprint, card password, card effective period, etc).

1. Click **Access Control → Permission** to enter the Permission Management interface.
2. Click **Add** to open the adding permission window.
3. In the **Permission Name** text field, create a name for the permission as you want.
4. Select a schedule template for the permission.

Note

You should configure the template before permission settings. You can click **Add Template** to add the template. Refer to *Configure Schedule and Template* for details.

---

5. In the Person list, select person(s) to assign the permission and click **>** to add to the Selected Person list.
6. In the Access Control Point/Device list, select door(s) or door station(s) for the selected persons to access and click **>** to add to the selected list.
7. Click **OK**.

   The selected persons will have the permission to enter/exit the selected doors/door stations with their linked card(s) or fingerprints.

8. After adding the access permissions, you need to apply them 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.

   Note

   You can also click **Apply Changes** to apply the changed part of the selected permission(s) to the device(s).

16.6.2 Search Assigned Permission

After adding the access permissions, you can search the existing permissions by setting the search conditions.

Perform this task if you need to search the assigned access permission.

Steps
1. Click **Access Control → Permission** to enter the Permission Management interface.
2. Click **Advanced Search** to open the search window.
3. Set the search condition.

   Person No.

   Input the keyword of the person number.

   Person Name

   Input the keyword of the person name.

   Note

   The person name is case sensitive.

   Card No.

Input the keyword of the card number.

Permission Name

The permission name is case sensitive.

4. Click **Search**.

The search results will display below.

5. Click **Reset** to clear the search conditions.

16.7 Configure Advanced Functions

After configuring the person, template, and access 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-passback, etc.

⌐ⁱ⌐**Note**

The advanced functions should be supported by the device.

16.7.1 Configure Access Control Parameters

After adding the access control device, you can configure the parameters of access control points (door or floor), alarm inputs, alarm outputs, and card readers.

Configure Access Control Device Parameters

After adding the access control device, you can configure its parameters, including overlaying user information on picture, uploading pictures after capturing, saving captured pictures, etc.

Perform this task when you want to configure device parameters for the access control device.

Steps
1. Click **Access Control → Advanced Function → Access Control Parameters** to enter Parameter Settings page.
2. Select an access controller to show its parameters on the right.
3. Check the checkbox to enable the corresponding functions.

⌐ⁱ⌐**Note**

The displayed parameters may vary for different access control devices.

RS-485 Card Reader Communication Redundancy

You should check the checkbox if you wire the RS-485 card reader to the access control device redundantly.

Display Detected Face Pictures

Display face picture when authenticating.

Display Card No.

Display the card information when authenticating.

Display User Information

Display the user information when authenticating.

Overlay User Information on Picture

Display the user information on the captured picture.

Enable Voice Prompt

If check the checkbox, the voice prompt is enabled in the device. You can hear the voice prompt when operating in the device.

Upload Pictures after Capturing

Upload the pictures captured by linked camera to the system automatically.

Save Captured Pictures

If you check the checkbox, you can save the picture captured by linked camera to the device.

Press Key to Input Card No.

If you check the checkbox, you can input the card No. by pressing the key.

Enable 3G/4G

If you check the checkbox, the device can communicate in 3G/4G network.

4. Click **Save**.
5. **Optional:** Click **Copy to** and select the access control device to copy the parameters to other devices.

Configure Door (Floor) Parameters

After adding the access control device, you can configure its access control point (door or floor) parameters.

Perform this task when you want to configure door (floor) parameters for the access control device.

Steps
1. Click **Access Control** → **Advanced Function** → **Access Control Parameters** to enter Parameter Settings page.
2. Select an access controller and click ⊞ to show the doors or floors of the selected access control device.
3. Select a door or floor to show its parameters on the right.
4. Edit the door or floor parameters.

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 closed in a configured time period.

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

Create a dismiss code which can be used to stop the buzzer of the card reader (by entering the dismiss code on the keypad).

Elevator Control Delay Time

The time duration of the visitor using the elevator. It is only available for elevator controller.

⌊i⌋**Note**

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

5. Click **Save**.
6. **Optional:** Click **Copy to** and select the door/floor(s) to copy the parameters to other doors/floors.

⌊i⌋**Note**

The door or floor's status duration settings will be copied to the selected door/floor(s) as well.

Configure Duration Schedule for Door Status

You can configure the weekly duration schedule for access control device's access control point (door) to remain open or remain closed.

Perform this task when you need to configure the door status duration schedule.

Steps

1. Click **Access Control → Advanced Function → Access Control Parameters** to enter Parameter Settings page.
2. Select a door to show its parameters on the right.
3. Click **Status Duration Settings** to open the Status Duration window.
4. Select a door status brush as **Remain Open** or **Remain Closed**.
   - **Remain Open:** The door will keep unlocked during the configured time period. The brush is marked as [blue] .
   - **Remain Closed:** The door will keep locked during the configured duration. The brush is marked as [orange] .
5. Drag on the timeline to draw a color bar on the schedule to set the duration.
6. **Optional:** Select the schedule time bar and click **Copy to Whole Week** to copy the time bar settings to the other days in the week.
7. Click **Save** to save the status duration schedule.
8. Click **Save** to save the door parameters.

Configure Duration Schedule for Elevator Status

You can configure the weekly duration schedule for elevator's permission to certain floors as free or disabled.

Perform this task when you need to configure the elevator status duration schedule.

Steps

1. Click **Access Control → Advanced Function → Access Control Parameters** to enter Parameter Settings page.
2. Select a floor to show its parameters on the right.
3. Click **Status Duration Settings** to open the Status Duration window.
4. Select a status brush as **Free** or **Disabled**.
   - **Free:** The selected floor's button in the elevator will be valid all the time during the configured time period. The brush is marked as [blue] .
   - **Disabled:** The selected floor's button in the elevator will be invalid and you cannot go to the selected floor during the configured duration. The brush is marked as [orange] .
5. Drag on the timeline to draw a color bar on the schedule to set the duration.
6. **Optional:** Select the schedule time bar and click **Copy to Whole Week** to copy the time bar settings to the other days in the week.
7. Click **Save** to save the status duration schedule.
8. Click **Save** to save the floor parameters.

Configure Card Reader Parameters

After adding the access control device, you can configure its card reader parameters.

Perform this task when you want to configure card reader parameters for the access control device.

Steps

1. Click **Access Control → Advanced Function → Access Control Parameters** to enter Parameter Settings page.
2. Select an access controller and click ⊞ to show the card readers of the selected access controller.
3. Select a card reader to show its parameters on the right.
4. Edit the card reader parameters.

⌷**i**⌷**Note**

The displayed parameters may vary for different access control devices. There are part of parameters listed as follows. Refer to the user manual of the device for more details.

Nickname

Edit the card reader name as desired.

Enable Card Reader

Select **Yes** to enable the card reader for card swiping.

OK LED Polarity/Error LED Polarity/Buzzer Polarity

Set OK LED Polarity/Error LED Polarity/Buzzer LED Polarity of main board according to the card reader parameters. Generally, adopts the default settings.

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 5,999s. 0 represents continuous buzzing.

Card Reader Type/Card Reader Description

Get card reader type and description. They are read-only.

Fingerprint Recognition Level

Select the fingerprint recognition level in the drop-down list.

Score

The device will score the captured picture according to the yaw angle, pitch angle, and pupillary distance. If the score is less than the configured value, face recognition will be failed.

Face Recognition Timeout Value

If the recognition time is more than the configured time, the device will remind you.

Face Recognition Interval

The time interval between two continuous face recognitions when authenticating. By default, it is 2s.

1:1 Match Threshold

Set the matching threshold when authenticating via 1:1 matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate when authentication.

1:N Match Threshold

Set the matching security level when authenticating via 1:N matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate when authentication.

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.

Live Face Detection Security Level

After enabling Live Face Detection function, you can set the matching security level when performing live face authentication.

Application Mode

You can select indoor or others application modes according to actual environment.

5. Click **Save**.
6. **Optional:** Click **Copy to** and select the card reader(s) to copy the parameters to other card readers.

Configure Zone Parameters

After adding the access control device, you can configure the parameters for its zones.

Perform this task if you need to set the zone parameters of the access control device.

Steps

⌐i⌐**Note**

If the zone is armed, you cannot edit its parameters. Disarm it first.

1. Click **Access Control → Advanced Function → Access Control Parameters** to enter Parameter Settings page.
2. Select a device and click ⊞ to show the zones of the selected access control device.
3. Set the zone parameters.

   Link Relay

   The alarm output that will be triggered when the zone event is triggered.

4. Click **Save**.
5. **Optional:** Click the switch on the upper-right corner to arm or disarm the zone.

Configure Alarm Output Parameters

After adding the access control device, if the device links to alarm outputs, you can configure the parameters.

Perform this task if you need to set the alarm input parameters of the access control device.

Steps
1. Click **Access Control → Advanced Function → Access Control Parameters** to enter Parameter Settings page.
2. Select a device and click ⊞ to show the alarm outputs of the selected access control device.
3. Set the alarm output parameters.

   Output Delay

   The delay time for the alarm output to be triggered.

4. Click **Save**.
5. **Optional:** Set the switch on the upper right corner to **ON** to trigger the alarm output.

Configure Lane Controller Parameters

After adding the lane controller to the client, you can configure its parameters for passing through the lane.

Perform this task to set the parameters for the lane controller.

Steps

1. Click **Access Control → Advanced Function → Access Control Parameters** to enter Parameter Settings page.
2. In the device list on the left, click ⊞ to expand the door, select a lane controller and you can edit the lane controller's parameters on the right.
3. Edit the parameters.

    Passing Mode

    Select the controller which will control the barrier status of the device.

    - If select **According to Lane Controller's DIP Settings**, the device will follow the lane controller's DIP settings to control the barrier. The settings on the software will be invalid.
    - If select **According to Main Controller's Settings**, the device will follow the settings of the software to control the barrier. The DIP settings of the lane controller will be invalid.

    Enable Free Passing Authentication

    If check the checkbox, when both entrance and exit's barrier mode is Remain Open, the pedestrians should authenticate each time passing through the lane. Or an alarm will be triggered.

    Opening/Closing Door Speed

    Set the barrier's opening and closing speed. You can select from 1 to 10. The greater the value, the faster the speed.

    ⓘ**Note**

    The recommended value is 6.

    Alarm Audio Prompt Time Duration

    Set the alarm audio prompt playing duration.

    ⓘ**Note**

    0 refers to the alarm audio will be played until the alarm is ended.

    Temperature Unit

    Select the temperature unit that displayed in the device status.

4. Click **Save**.

16.7.2 Configure Card Reader Authentication Mode and Schedule

You can set the passing rules for the card reader of the access control device according to your actual needs.

Perform this task if you need to configure the card reader's authentication mode and schedule.

Steps

1. Click **Access Control → Advanced Function → Card Reader Authentication** to enter the card reader authentication configuration page.
2. Select a card reader on the left to configure.
3. Set card reader authentication mode.
   1) Click **Configuration**.
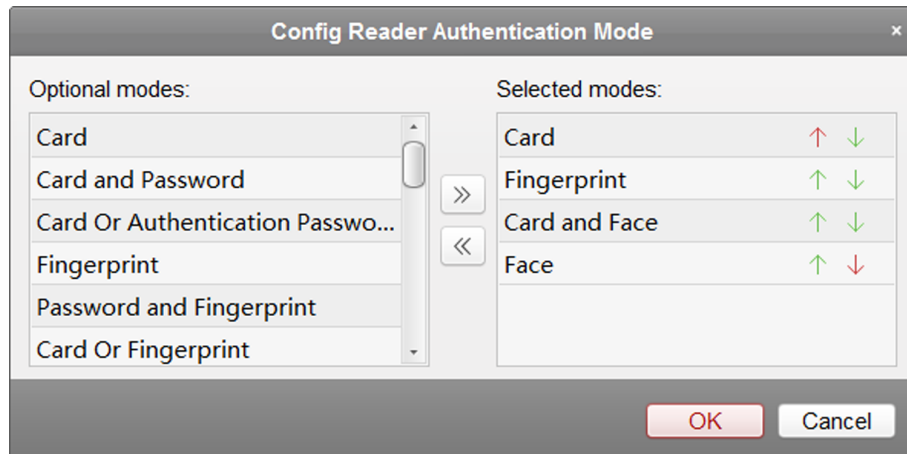
Figure 16-2 Select Card Reader Authentication Mode

> **Note**
> • Password refers to the card password set when issuing the card to the person. For details, refer to **Add Single Person** .
> • Authentication password refers to the password set to open the door. Refer to **Configure Authentication Password** .

   2) Select the modes and click » to add to the selected modes list.
   3) **Optional:** Click ↑ or ↓ to adjust the display order.
   4) Click **OK**.

   After selecting the modes, the selected modes will display as icons.
4. Click the icon to select a card reader authentication mode, and drag on the 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.
6. **Optional:** Select a configured day and click **Copy to Week** to copy the same settings to the whole week.
7. **Optional:** Click **Copy to** to copy the settings to other card readers.
8. Click **Save**.

16.7.3 Configure Multiple Authentication

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

Before You Start

Set the card permission and apply the permission settings to the access control device. For details, refer to *Assign Permission to Person* .

Perform this task when you want to set authentications for multiple cards of one access control point (door).

Steps

1. Click **Access Control → Advanced Function → Multiple Authentication** to enter the Multiple Authentication page.
2. Select an access control device in the list of Controller List panel.
3. Add a card group for the access control device.
   1) Click **Add** on the Set Card Group panel.
   2) Create a name for the group as desired.
   3) Specify the start time and end time of the effective period for the card group.
   4) Select card(s) to add to the card group.
   5) Click **OK**.
4. Select an access control point (door) of selected device on the Set Authentication Group panel.
5. Input the time interval for card swiping.
6. Add an authentication group for the selected access control point.
   1) Click **Add** on the Set Authentication Group panel.
   2) Select a configured template for the authentication group from the drop-down list.

   > 🛈**Note**

   For setting the template, refer to *Configure Schedule and Template* .

   3) Select the authentication type as **Local Authentication**, **Local Authentication and Remotely Open Door**, or **Local Authentication and Super Password** from the drop-down 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. When the person swipes the card on the device, a window will pop up. You can unlock the door via the client.
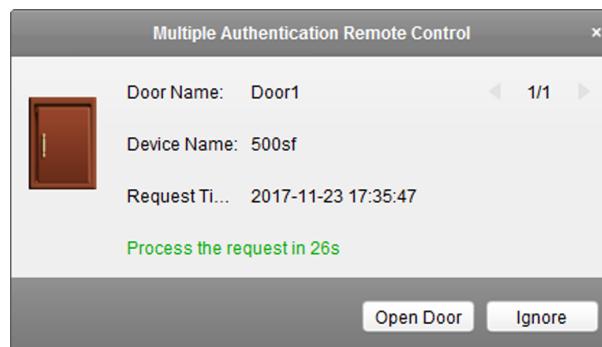
Figure 16-3 Remotely Open Door

Note

You can check **Offline Authentication** to enable the super password authentication when the access control device is disconnected with the client.

Local Authentication and Super Password

Authentication by the access control device and by the super password.

4) Select the added card group in the left list below and click ➕ to add the selected card group to the right list as the authentication group.
5) **Optional:** Click ⬆ or ⬇ to set the card swiping order.
6) Click the added authentication group in the right list to set card swiping times.

Note

- The card swiping times should be larger than 0 and smaller than the added card quantity in the card group.
- The maximum value of card swiping times is 16.

7) Click **OK**.

Note

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

7. Click **Save**.

16.7.4 Configure Opening Door with First Card

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.

Before You Start
Set the card permission and apply the permission setting to the access control device. For details, refer to ***Assign Permission to Person*** .

Perform this task when you want to configure opening door with first card.

Steps
1. Click **Access Control → Advanced Function → Open Door with First Card** to enter the Open Door with First Card page.
2. Select an access control device in the list of Controller List panel.

3. Select the first card mode as **Remain Open with First Card**, **Disable Remain Open with First Card**, or **First Card Authorization** from the drop-down list for each access control point of the selected device.

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. If you select this mode, you should set the remain open duration.

ⓘ**Note**

The remain open duration should be between 0 and 1440 minutes. By default, the remain open duration is 10 minutes.

Disable Remain Open with First Card

Disable the function of remaining open with first card.

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.

ⓘ**Note**

The **First Card Authorization** is effective only on the current day. The authorization will be expired after 24:00 on the current day.

ⓘ**Note**

You can swipe the first card again to disable the first card mode.

4. Click **Add** on the First Card List panel.
5. Select a card in the list and click **OK** to add the selected card as the first card of the doors.

   The added first card will list on the First Card List panel.

6. **Optional:** Select a first card from the list and click **Delete** to remove the card from the first card list.
7. Click **Save**.

16.7.5 Configure Anti-Passback

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.

Before You Start
Enable the anti-passing back function of the access control device.

Perform this task when you want to configure the anti-passing back for the access control device.

Steps

ℹ️**Note**

Either the anti-passing back or multi-door interlocking function can be configured for an access control device at the same time. For the configuration of multi-door interlocking, refer to *Configure Multi-door Interlocking* .

1. Click **Access Control → Advanced Function → Anti-Passback** to enter the anti-passing back configuration page.
2. Select an access control device in the list.
3. Select a card reader as the beginning of the path in the **First Card Reader** field.
4. Click the text field of the selected first card reader in the **Card Reader Afterward** column to open Select Card Reader dialog.
5. Select the afterward card readers for the first card reader.

   ℹ️**Note**

   Up to four afterward card readers can be added for one card reader.

6. Click **OK** in the dialog to save the selections.
7. Click **Save** at the upper-right corner of Anti-Passing Back page to save the settings and take effect.

Example

Set Card Swiping Path

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.

16.7.6 Configure Cross-Controller Anti-passing Back

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.

ℹ️**Note**

It should be supported by the device.

Configure Route Anti-passing Back Based on Card

The route anti-passing back depends on the card swiping route. You should set the first card reader and the card readers afterwards. It will judge the anti-passing back according to the entrance and exit records on the card.

Perform this task if you need to configure route anti-passing back and judge the anti-passing back according to the entrance and exit records on the card.

Steps

> **Note**
>
> It supports M1 card at present and the sector cannot be encrypted. For details about sector encryption, refers to ***Authenticate M1 Card Encryption*** .

1. Click **Access Control → Advanced Function → Cross-Controller Anti-passing Back** to enter the cross-controller anti-passing back configuration page.
2. Check **Enable Cross-Controller Anti-passing Back** to enable the function.
3. Select **Based on Card** as the anti-passing back mode.
4. Select **Route Anti-passing Back** as the rule.
5. Set the sector ID.
6. Click **Select Access Controller** to select a device for anti-passing back.

> **Note**
>
> Up to 64 devices with anti-passing back function can be added.

7. Set the first card reader and after card readers.
   1) In the Card Reader area, click the icon on the left of the card reader column to set it as the first card reader.

   Figure 16-4 Select First Card

   The icon will turn to 👤 .
   2) Click the card reader afterward input field to select the card readers afterward in the pop-up window.

   > **Note**
   >
   > • Up to 16 card readers afterward can be added for each card reader.
   > • The displayed card readers in the card reader afterward input field should be in authentication order.

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

Configure Route Anti-passing Back Based on Network

The route anti-passing back depends on the card swiping route. You should set the first card reader and the card readers afterwards. It will authenticate the anti-passing back according to the entrance and exit information stored on the card reader.

Perform this task if you need to configure route anti-passing back and authentice the anti-passing back recsult according to the entrance and exit information stored on the card reader.

Steps
1. Click **Access Control → Advanced Function → Cross-Controller Anti-passing Back** to enter the cross-controller anti-passing back configuration page.
2. Check **Enable Cross-Controller Anti-passing Back** to enable the function.
3. Select **Based on Network** as the anti-passing back mode.
4. Select **Route Anti-passing Back** as the rule.
5. Select a server in the drop-down list for judging the anti-passing back.

   ⌊i⌋Note

   - You can click **Delete Card Swiping Record** and select the card in the pop-up window to delete the card swiping information in all devices.
   - Up to 5000 cards' swiping records can be stored in the selected server.

6. Click **Select Access Controller** to select a device for anti-passing back.

   ⌊i⌋Note

   Up to 64 devices with anti-passing back function can be added.

7. Set the first card reader and after card readers.
   1) In the Card Reader area, click the icon on the left of the card reader column to set it as the first card reader.

   Figure 16-5 Select First Card

   The icon will turn to 🧍 .
   2) Click the card reader afterward input field to select the card readers afterward in the pop-up window.

- Up to 16 card readers afterward can be added for each card reader.
- The displayed card readers in the card reader afterward input field should be in authentication order.

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

8. Click **Save**.

Configure Entrance/Exit Anti-Passback Based on Card

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. It will judge the anti-passing back according to the entrance and exit records on the card.

Perform this task if you need to configure entrance/exit anti-passing back and judge the anti-passing back according to the entrance and exit records on the card.

Steps

ⓘ **Note**

It supports M1 card at present and the sector cannot be encrypted. For details about sector encryption, refers to *Authenticate M1 Card Encryption* .

1. Click **Access Control → Advanced Function → Cross-Controller Anti-passing Back** to enter the cross-controller anti-passing back configuration page.
2. Check **Enable Cross-Controller Anti-passing Back** to enable the function.
3. Select **Based on Card** as the anti-passing back mode.
4. Select **Entrance/Exit Anti-passing Back** as the rule.
5. Set the sector ID.
6. Click **Select Access Controller** to select a device for anti-passing back.

   ⓘ **Note**

   Up to 64 devices with anti-passing back function can be added.

7. 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.

   ⓘ **Note**

   Up to one entrance carder and one exit card reader should be checked.

8. Click **Save**.

Configure Entrance/Exit Anti-Passback Based on Network

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. It will authenticate the anti-passing back according to the entrance and exit information on the card reader.

Perform this task if you need to configure entrance/exit anti-passing back and judge the anti-passing back according to the entrance and exit information stored on the card reader.

Steps
1. Click **Access Control → Advanced Function → Cross-Controller Anti-passing Back** to enter the cross-controller anti-passing back configuration page.
2. Check **Enable Cross-Controller Anti-passing Back** to enable the function.
3. Select **Based on Network** as the anti-passing back mode.
4. Select **Entrance/Exit Anti-passing Back** as the rule.
5. Select a server in the drop-down list for judging the anti-passing back.

   ⓘ**Note**
   - You can click **Delete Card Swiping Record** and select the card in the pop-up window to delete the card swiping information in all devices.
   - Up to 5000 cards' swiping records can be stored in the selected server.

6. Click **Select Access Controller** to select a device for anti-passing back.

   ⓘ**Note**
   Up to 64 devices with anti-passing back function can be added.

7. 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.

   ⓘ**Note**
   Up to one entrance carder and one exit card reader should be checked.

8. Click **Save**.

16.7.7 Configure Multi-door Interlocking

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.

Perform this task when you want to realize interlocking between multiple doors.

Steps

ⓘNote

- 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. For the configuration of anti-passing back function, refer to *Configure Anti-Passback* .

---

1. Click **Access Control → Advanced Function → Multi-door Interlocking** to enter the Multi-door Interlocking page.
2. Select an access control device in the list of Controller List panel.
3. Click **Add** on the Multi-door Interlocking List panel to open Add Access Control Point to Interlock window.
4. Select access control point (s) from the list.

   ⓘNote

   Up to four doors can be added in one multi-door interlocking combination.

   ---

5. Click **OK** to add the selected access control point(s) for interlocking.

   The configured multi-door interlocking combination will list on the Multi-door Interlocking List panel.

6. **Optional:** Select an added multi-door interlocking combination from the list and click **Delete** to delete the combination.
7. Click **Save**.

16.7.8 Configure Authentication Password

You can input the authentication password on the card reader keypad to open the door after setting the authentication password.

Perform this task when you want to configure authentication password to open door.

ⓘNote

- The authentication password function should be supported by the access control device.
- 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.

Steps

1. Click **Access Control → Advanced Function → Authentication Password** to enter the authentication password configuration page.
2. Select an access control device in the list of Controller List panel.

   All the applied cards and persons will display on the Card List panel.

📖ℹ**Note**

For setting and applying the permissions to the device, refer to **Assign Permission to Person** .

---

3. Click the field of each card in the Password column to input the authentication password.

📖ℹ**Note**

The authentication password should contain 4 to 8 digits.

---

4. Click **Save** at the upper-right corner of Authentication Password page to save the settings.

   The authentication password function of the card will be enabled automatically. And you can set the card reader authentication mode of access control device as **Card or Authentication Password**. Refer to **Configure Card Reader Authentication Mode and Schedule** for details.

16.7.9 Configure Relay for Elevator Controller

For elevator controller, you can manage the relationship between the floor and the relay and configure the floor's relay type.

Configure Relationship between Relay and Floor

You can assign different kinds of relays to the target floors, so that you can control the elevator according to the relationship between the relay and the floor.

Before You Start
Add the elevator controller to the client.

Perform the following steps to assign the relays to the floors.

Steps

📖ℹ**Note**

- An elevator controller can link to up to 24 distributed elevator controllers. A distributed elevator controller can link up to 16 relays.
- By default, the relay total amount is the added floor number *3 (three types of relay).
- If you change the floor number in the door group management, all relays in the Relay Settings interface will restore to the default settings.

---

1. Click **Access Control → Advanced Function → Elevator Settings** to enter the Relay Settings page.
2. Select an elevator controller on the left.
3. Select an unconfigured relay in the Unconfigured Relay panel on the right.

   There are three types of relay available.

   Button Relay

Control the validity for buttons of each floor.

Note

▇▇▇ represents button relay.

Call Elevator Relay

Control to call the elevator to go to the specified floor.

Note

▇▇▇ represents the call elevator relay.

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.

Note

▇▇▇ represents the auto button relay.

Example

Take ▫ as an example. In the number 1-2, 1 represents the distributed elevator controller number, 2 represents the relay, and the icon ▇▇▇ represents the relay type. You can change the relay type. For details, refer to **Configure Relay Type** .

4. Configure the relationship between the relays and the floors.
- Drag the unconfigured relay from the Unconfigured Relay panel to the target floor in the Floor List panel.
- Drag the relay from the Floor List panel to the Unconfigured Relay panel.
- Drag the relay from one floor to another floor in the Floor List panel.

Note

If the target floor has already configured with a relay of the same type as the dragged one, it will replace the existed one of the same type.
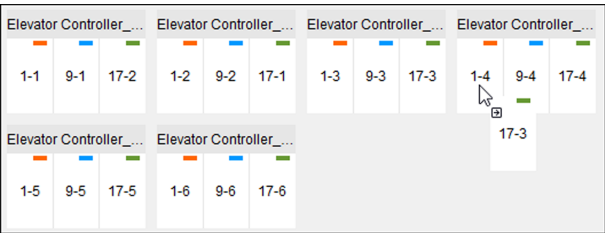
Figure 16-6 Replace Existed Relay Type

5. Click **Save** to apply the settings to the selected elevator controller.

Configure Relay Type

For some reasons, you should change relay types. You can change the button relay, call elevator relay, and auto button relay with each other.

Perform the following steps to change the relay type.

Steps
1. Click **Access Control → Advanced Function → Elevator Settings** to enter the Relay Settings page.
2. Select an elevator controller in the Controller List on the left of the page.
3. Click **Relay Type** to open the Relay Type Settings window.

---

i Note

- All relays in the Relay Type Settings window are unconfigured relays.
- Three types of relay are available: ▭ represents the button relay, ▭ represents the call elevator relay, and ▭ represents the auto button relay.

---

4. Drag the relay from one relay type panel to the target one.
5. Click **OK**.

16.7.10 Configure Custom Wiegand Rule

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

Before You Start
Wire the third party card readers to the device.

Perform this task to configure the custom Wiegand rule for the third party card readers.

Steps

---

i Note

- 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.
- For details about the custom Wiegand, see **Custom Wiegand Rule Descriptions** .

---

1. Click **Access Control → Advanced Function → Custom Wiegand** to enter the custom Wiegand configuration page.
2. Select a custom Wiegand on the left.
3. Check **Enable** to enable the custom Wiegand.
4. Create a Wiegand name.

Up to 32 characters are allowed in the custom Wiegand name.

5. Click **Select Device** to select the access control device for setting the custom wiegand.
6. Set the parity according to the property of the third party card reader.

ℹ️**Note**

- Up to 80 bits are allowed 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.

7. Set output transformation rule.
    1) Click **Set Rule** to open the Set Output Transformation Rules window.
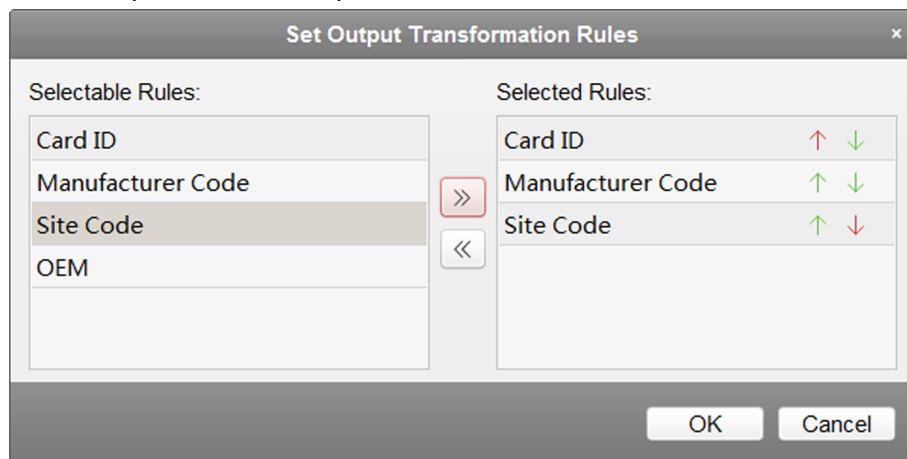
Figure 16-7 Set Output Transformation Rule

    2) Select rules on the left list.
    3) Click 》 to move the selected rules to the right list.
    4) **Optional:** Click ↓ or ↑ to change the rule order.
    5) Click **OK**.
    6) In the Custom Wiegand tab, set the rule's start bit, length, and the decimal digit.
8. Click **Save**.

16.7.11 Configure Person in Blacklist

You can manage the person information in the blacklist and apply the blacklist information to the access control device to take effect.

Add Person to Blacklist

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

Perform this task when you need to configure person information in blacklist for access control device.

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.

   $\boxed{i}$**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**.
7. **Optional:** Select the added person and click **Delete** to remove it from the blacklist.
8. Apply the person information in blacklist to the device to take effect.
   1) Select the person(s) to apply to the device.
   2) Click **Apply**.
   3) Select **Apply All** to start applying all the selected permission(s) to the access control device or door station.

      $\boxed{i}$**Note**

      You can also select **Apply Changes** to apply the changed part of the selected permission(s) to the device(s).

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

Manage Application Result of Person in Blacklist

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

Perform this task when you need to manage the person information application result of blacklist.

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.

16.8 Search Access Control Event

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

16.8.1 Search Local Access Control Event

You can search the access control event from the database of the client and export the events to local PC.

Perform this task when you want to search and export the local access control events.

Steps

1. Click **Access Control → Search → Access Control Event** to enter the searching access control event page.
2. Select the event source as **Local Event**.
3. Set the search conditions as deaired, such as device name, event type, occurred time, and so on.
4. Click **Search** to start searching the access control events.

   The matched access control events will display.

5. **Optional:** After searching the events, you can do one or more of the followings.

View Card Holder Details	For the access control event which is triggered by the card holder, click the event to view the card holder details, including person No., person name, organization, phone number, contact address and photo.
View Captured Picture	For events contain linked pictures, click **Capture** column to view the captured picture of the triggered camera when the alarm is triggered. ⓘ**Note** For setting the triggered camera, refer to ***Configure Client Linkage for Access Control Alarm*** .

View Linked Video	For events contain linked video, click **Playback** column to view the recorded video file of the triggered camera when the alarm is triggered.
	⬚**ℹ️**Note
	For setting the triggered camera, refer to ***Configure Client Linkage for Access Control Alarm*** .
Export Event	Click **Export** to export the search results to the local PC in CSV file.

16.8.2 Search Remote Access Control Event

You can search the access control event records stored on the access control device.

Perform this task when you need to search the access control events stored on the access control device.

Steps
1. Click **Access Control → Search → Access Control Event** to enter the searching remote access control event page.
2. Select the event source as **Remote Event**.
3. Set the search conditions as deaired.
4. **Optional:** Check **With Alarm Picture** to search the events with alarm pictures.
5. Click **Search**.
   The matched access control events will display.
6. **Optional:** Click **Export** to export the search results to the local PC in CSV file.

16.9 Configure Access Control Alarm Linkage

For the added access control device, you can configure the linkage actions such as client linkage, device linkage, or cross-device linkage.

16.9.1 Configure Client Linkage for Access Control Alarm

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

Perform this task when you need to configure the client linkage for the access control alarm.

Steps

ⓘNote

The linkage here refers to the linkage of the client software's own actions such as pop-up image, audible warning, email linkage, etc.

1. Click **Event Management → Access Control Event** .

   The added access control devices will display in the Access Control Device panel on the left.
2. 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.

   ⓘNote

   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 *Remote Storage Configuration* .

   The image or video from the triggered camera will pop up when the selected event occurs.
5. Set the client linkage actions.

   Audible Warning

   The client software gives an audible warning when alarm is triggered. You can select the alarm sound for audible warning.

   ⓘNote

   For setting the alarm sound, please refer to *Set Alarm Sound* .

   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**.

7. **Optional:** Click **Copy to** to copy the linkage settings to other access control device, alarm input, access control point, or card reader.

16.9.2 Configure Device Linkage for Access Control Alarm

You can set the access control device's linkage actions for the access control device's triggered alarm. When the alarm is triggered, it can trigger the alarm output, host buzzer, and other actions on the same device.

Perform this task when you need to configure the access control device linkage for the device's access control alarm.

Steps

🔖**Note**

It should be supported by the device.

1. Click **Event Management → Event Card Linkage** .
2. Select the access control device from the list on the left.
3. Click **Add** button to add a new linkage.
4. Select the event source as **Event Linkage**.
5. select the alarm type and detailed alarm to set the linkage.
6. In the Linkage Target panel, set the property switch to on to enable this action.

Host Buzzer

The audible warning of access control device 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 Buzzer

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.

Note

- 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.

Audio Play

The audio prompt will be triggered. And the select audio index related audio content will be played according to the configured play mode.

7. Click **Save**.
8. **Optional:** After adding the device linkage, you can do one or more of the following:

Edit Linkage Settings	Select the configured linkage settings in the device list and you can edit its event source parameters, including event source and linkage target.
Delete Linkage Settings	Select the configured linkage settings in the device list and click **Delete** to delete it.

16.9.3 Configure Device Linked Actions for Card Swiping

You can set the access control device's linkage actions for the specified card swiping. When you swipe the specified card, it can trigger the alarm output, host buzzer, and other actions on the same device.

Perform this task when you need to configure the access control device linkage for the card swiping action.

Steps

Note

It should be supported by the device.

1. Click **Event Management** → **Event Card Linkage** .
2. Select the access control device from the list on the left.
3. Click **Add** button to add a new linkage.
4. Select the event source as **Card Linkage**.
5. Input the card number or select the card from the dropdown list.
6. Select the card reader where the card swipes to trigger the linked actions.
7. In the Linkage Target panel, set the property switch to on to enable this action.

Host Buzzer

The audible warning of access control device will be triggered.

Capture

The real-time capture will be triggered.

Recording

The recording will be triggered.

⃞**i**⃞**Note**

The device should support recording.

Card Reader Buzzer

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.

⃞**i**⃞**Note**

The device should support zone function.

Access Control Point

The door status of open, close, remain open, and remain close will be triggered.

⃞**i**⃞**Note**

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

Audio Play

The audio prompt will be triggered. And the select audio index related audio content will be played according to the configured play mode.

8. Click **Save**.

   When the card (configured in Step 5) swipes on the card reader (configured in Step 6), it can trigger the linked actions (configured in step 7).

9. **Optional:** After adding the device linkage, you can do one or more of the following:

Delete Linkage Settings	Select the configured linkage settings in the device list and click **Delete** to delete it.
Edit Linkage Settings	Select the configured linkage settings in the device list and you can edit its event source parameters, including event source and linkage target.

16.9.4 Configure Device Linkage for Mobile Terminal's MAC Address

You can set the access control device's linkage actions for the specified MAC address of mobile terminal. When the access control device detects the specified MAC address, it can trigger the alarm output, host buzzer, and other actions on the same device.

Perform this task when you need to configure the access control device linkage for the MAC address

Steps

⌐i̱⌐Note

It should be supported by the device.

1. Click **Event Management → Event Card Linkage** .
2. Select the access control device from the list on the left.
3. Click **Add** button to add a new linkage.
4. Select the event source as **MAC Linkage**.
5. Input the MAC address to be triggered.

   ⌐i̱⌐Note

   MAC Address Format: AA:BB:CC:DD:EE:FF.

6. In the Linkage Target panel, set the property switch to on to enable this action.

   Host Buzzer

   The audible warning of access control device will be triggered.

   Capture

   The real-time capture will be triggered.

   Recording

   The recording will be triggered.

   ⌐i̱⌐Note

   The device should support recording.

   Card Reader Buzzer

   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.

$\boxed{i}$**Note**

The device should support zone function.

Access Control Point

The door status of open, close, remain open, and remain close will be triggered.

$\boxed{i}$**Note**

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

7. Click **Save** to save the settings.
8. **Optional:** After adding the device linkage, you can do one or more of the following:

Edit Linkage Settings	Select the configured linkage settings in the device list and you can edit its event source parameters, including event source and linkage target.
Delete Linkage Settings	Select the configured linkage settings in the device list and click **Delete** to delete it.

16.9.5 Configure Cross-Device Linkage

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

$\boxed{i}$**Note**

It should be supported by the device.

Configure Cross-Device Linkage for Access Control Event

When the access control event is triggered and detected, it can trigger linkage actions of other access control device, such as alarm output, opening door, etc. The event can be divided into four types: device event, alarm input, door event, and card reader event.

Perform this task when you need to configure other access control device's linkage actions for access control event.

Steps

$\boxed{i}$**Note**

The devices should support this function.

1. Click **Event Management** → **Cross-Device Linkage** to enter the cross-device linkage configuration interface.
2. Click **Add** to add a new cross-device linkage.
3. Select the linkage type as **Event Linkage**.

4. Set the event source.
1) Select the access control device as event source device.
2) Select the access control event type.

Device Event

Select the detailed event type from the dropdown list.

Alarm Input

Select the detailed event type as zone event or alarm input event and select the zone name or alarm input name from the dropdown list.

Door Event

Select the detailed event type and select the access control point from the dropdown list.

Card Reader Event

Select the detailed event type and select the card reader from the dropdown list.

5. Set the target access control device as linkage target.
1) Select the access control device from the dropdown list as the linkage target.
2) Set the switch to on to enable the linkage action.

Alarm Output

The alarm output pf the target device 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.

6. Click **Save**.

Configure Cross-Device Linkage for Card Swiping

When person swipes the specified card on the specified card reader, it can trigger linkage actions of other access control device, such as alarm output, opening door, etc.

Perform this task when you need to configure other access control device's linkage actions for card swiping.

Steps
1. Click **Event Management → Cross-Device Linkage** to enter the cross-device linkage configuration interface.
2. Click **Add** to add a new cross-device linkage.
3. Select the linkage type as **Card Linkage**.
4. Set the event source.
1) Select the card from the dropdown list.
2) Select the access control device as event source device.

3) Select the card reader for triggering.
5. Set the target access control device as linkage target.
    1) Select the access control device from the dropdown list as the linkage target.
    2) Set the switch to on to enable the linkage action.

    Alarm Output

    The alarm output pf the target device will be triggered for notification.

    Access Control Point

    The door status of open, close, remain open, and remain close will be triggered.

    ---
    [i] **Note**

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

    ---

6. Click **Save**.

16.10 Manage Access Control Point Status

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

16.10.1 Group Access Control Points

Before controlling the doors status and setting the status duration, you should organize the access control device's access control points into groups for convenient management.

Perform this task when you need to group the access control points for convenient management.

Steps

---
[i] **Note**
- You can also import the access control device's alarm inputs into groups.
- For video access control terminal, you can import its camera into groups.
- For other detailed operations, refer to *Group Management* .

---

1. Click **Device Management → Group** to enter the group management page.
2. Add a new group.
    1) Click [icon] to open the Add Group window.
    2) Create a group name.
    3) **Optional:** Check **Create Group by Device Name** to create the new group by the name of the selected device.
    4) Click **OK**.
3. Import the access control points to the group.
    1) Click **Import**.

2) Click **Access Control Point** tab.
3) Select the access control points in the list.
4) Select a group from the group list.
5) Click **Import** to import the selected access control points to the group.

16.10.2 Control Door Status

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

Perform this task when you need to control the door's status.

Steps
1. Click **Status Monitor → Door Status** to door status monitoring page.
2. Select an access control group on the left.

[i]**Note**

For managing the access control group, refer to **Group Access Control Points** .

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

3. Click ▮ on the Status Information panel to select a door.
4. Click the following buttons listed on the Status Information panel to control the door.

Open Door

Open the door once.

Close Door

Close the door once

Remain Open

Keep the door open

Remain Closed

Keep the door closed

Capture

Capture the picture manually

[i]**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 **Remote Storage Configuration** to configure the capture schedule.

16.10.3 Control Elevator Status

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

Before You Start
Before controlling the elevator status, you should distribute the relays to the target floors. For details, refer to *Configure Relationship between Relay and Floor* .

Perform this task when you need to control the elevator's status.

Steps

📖ℹ️**Note**
- 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.

---

1. Click **Status Monitor → Door Status** to door status monitoring page.
2. Select an access control group on the left.

   📖ℹ️**Note**
   For managing the access control group, refer to *Group Access Control Points* .

   The floors of the selected access control group will be displayed on the right of the interface.
3. Click 🟫 on the Status Information panel to select a floor.
4. Click the following buttons listed on the Status Information panel to control the door.

   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 before pressing the target floor button. And the elevator can go to the target floor.

   Free

      The selected floor's button in the elevator will be valid all the time.

   Disabled

      The selected floor's button in the elevator will be invalid and you cannot go to the target floor.

   Call Elevator (Visitor)

The elevator will go down to the first floor. The visitor can only press the target floor's button.

Call Elevator (Resident)

Call the elevator to the target floor.

16.10.4 Check Real-time Card Swiping Record

The logs of card swiping records of all access control devices will display in real time.

Perform this task when you need to check the real-time card swiping records.

Steps

1. Click **Status Monitor → Card Swiping Record** to enter the real-time card swiping record page.

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

2. **Optional:** Check **Auto-Select the Latest Record** and the latest card swiping record will be selected and displayed at the top of the record list.

3. **Optional:** Click the event to view the card holder details, including captured person pictures (captured picture and profile) person No., person name, organization, phone, contact address, etc.

   Authentication Result

   Card swiping result such as card No. not registered, succeeded, etc.

16.10.5 Check Real-time Access Control Alarm

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

Perform this task when you need to check the real-time access control alarms.

Steps

1. Click **Status Monitor → Access Control Alarm** to enter the real-time access control alarm page.

   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.

   ⓘ**Note**

   For configuring the access control point on E-map, refer to ***Display Access Control Point on E-map*** .

3. **Optional:** 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 *Configure Client Linkage for Access Control Alarm* .

4. **Optional:** Select the alarm that the client can receive when the alarm is triggered.
   1) Click **Subscribe**.
   2) Check the checkbox(es) to select the alarm(s), including device exception alarm, door event alarm, card reader alarm, and alarm input.
   3) Click **OK** to save the settings.

16.11 Control Door during Live View

During live view, you can control the camera's linked access control point (door) such as opening door, closing door, etc.

Perform this task when you need to control the camera's linked door to open or close during live view.

Steps
1. Enter **Live View** module and start live view of one camera.

   Note

   For details about starting live view, refer to *Start Live View for One Camera* for details.

2. Link the camera with an access control point.
   1) Right click on the live view window and select **Link to Access Control Point** to open the Set Linked Access Control Point window.
   2) Check **Enable** to enable the linkage.
   3) Select access control point from the drop-down list.
   4) Click **OK**.

   Note

   One camera can be linked to only one access control point; Different cameras can be linked to the same access control point.
3. Start the camera's live view again to make the settings effective.

   Four door control buttons will appear on the toolbar during live view.
4. Click ▣ ▣ ▣ ▣ to control the door to open, close, remain open, or remain closed.

16.12 Display Access Control Point on E-map

You can add the access control point on the E-map. 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.

Perform this task when you need to display the access control point on the e-map as hot spot.

Steps

ℹ️**Note**

- For Video Access Control Terminal, you can also add its camera to the E-map to view the live view of the camera.
- For detailed operations of E-map, refer to *Map Management* .

1. Enter **E-map** module.
2. Click **Edit** on the E-map toolbar to enter the map editing mode.
3. Click 🚪 on the toolbar to open the Add Hot Spot window.
4. Select the access control point to be added as hot spot.
5. **Optional:** Edit hot spot name, select the name color, and select the hot spot icon by double-clicking the corresponding field.
6. Click **OK**.

   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.

7. After adding the access control point on the map as hot spot, you can control the access control point and view triggered alarm.
   1) Click **Exit Editing Mode** on 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.
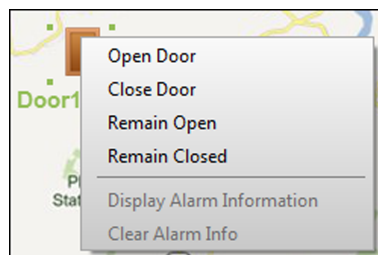
Figure 16-8 Control Access Control Point on Map

   3) **Optional:** 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 to check the alarm information, including alarm type and triggering time.

ℹ️**Note**

To display the alarm information on the map, you should set display on e-map as the alarm linkage action. For details, refer to *Configure Client Linkage for Access Control Alarm* .

16.13 Two-way Audio

After adding the device to the client software, you can call the client from the device or call the device from the client. You can get not only the live video but also the real-time audio.

16.13.1 Call Client from the Device

For the access control devices with the camera, you can call the client via the device. If the requirement is accepted, you can get the real-time audio and video from the client.

Before You Start

Add the device to the software and properly configure the corresponding settings. See ***Add Device*** for details about adding the device.

Perform this task if you need to receive the call from the access control device.

Steps

$\boxed{\mathbf{i}}$**Note**

This function should be supported by the device.

1. Tap **Call** on the device initial page.
2. Enter **0** in the pop-up window.
3. Tap **Call** to call the client.
4. Click **Answer** on the pop-up page of the client to answer the call.

   An incoming call dialog appears in the client software. You can start two-way audio between the device and the client.

   $\boxed{\mathbf{i}}$**Note**

   If the device is added by multiple clients and when the device is calling the client, only the first client added the device will show the call receiving window.

16.13.2 Call Device from Client

You can call the added access control device with the camera via the client and perform two-way audio.

Before You Start

Add the device to the software and properly configure the corresponding settings. See ***Add Device*** for details about adding the device.

Perform this task if you want to call the access control device via the client.

Steps

ⓘNote

This function should be supported by the device.

---

1. Enter the Main View page.
2. Start the live view of the device's camera.
3. Right-click the live view window to open the shortcut menu.
4. Click **Start Two-Way Audio**.

   The call will be answered automatically to start two-way audio between the device and the client.

Chapter 17 Time and Attendance

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.

17.1 Manage Shift Schedule

Shift work is an employment practice designed to make use of all 24 hours of the clock each day of the week. The practice typically sees the day divided into shifts, set periods of time during which different shifts perform their duties.

You can set department schedule, person schedule, and temporary schedule.

17.1.1 Add Time Period

You can add the time period for the shift schedule.

Perform this task when you need to add time period.

Steps
1. Enter Time and Attendance module and click **Shift Schedule Management** tab.
2. Click **Shift Settings → Time Period Settings** to enter Time Period Settings window.
3. Click **Add** to enter Add Time Period page.
4. Set the time period related parameters.

   Attend at Least

   Set the minimum attendance time.

   ⓘ**Note**

   If you have configured the different card readers as start-work and end-work check points, you can check **Absence time is not included in effective work hours** to exclude the absence time from the work hours.

   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.

⬛ⁱNote

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.

5. Click **Save**.

The added time period lists on the left panel of the window.

17.1.2 Add Shift

You can add the shift for the shift schedule.

Before You Start
Add a time period first. See **Add Time Period** for details.

Perform this task when you need to add shift.

Steps
1. Enter Time and Attendance module.
2. Click **Shift Schedule Management → Shift Settings → Shift** to enter Shift Settings window.
3. Click **Add** to enter Add Shift page.
4. Input the name for shift.
5. Select the shift period from the drop-down list.
6. Select the added time period and click on the time bar to apply the time period.
7. Click **Save**.

The added shift lists on the left panel of the window.

17.1.3 Set 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.

Before You Start
In Time and Attendance module, the department list is the same with the organization in Access Control module. You should add departments and persons in Access Control module first. See **Manage Organization** and **Manage Person Information** for details.

Perform this task when you need to set department schedule.

Steps
1. Click **Time and Attendance → Shift Schedule Management** to enter the Shift Schedule Management page..
2. Select a department and click **Department Schedule** to pop up Department Schedule window.
3. Check **Time and Attendance** .

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. Set other parameters for the schedule, including Check-in Not Required, Check-out Not Required, Effective for Holiday, Effective for Overtime, or Effective for Multiple Shift Schedules.

⌐i̲⌐**Note**

After checking the **Effective for Multiple Shift Schedules**, you can select the effective time period(s) from the added time periods for the persons in the department.

Multiple Shift Schedules

It contains more than one time periods. The person can check in/out in any of the time periods and the attendance will be effective.

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.

7. **Optional:** Check **Set as Default for All Persons in Department**.

   All persons in the department will use this shift schedule by default.

8. **Optional:** If the selected department contains sub department(s), you can check **Set as Shift Schedule for All Sub Departments** to apply the department schedule to its sub departments.
9. Click **Save**.

17.1.4 Set Person Schedule

You can assign the shift schedule to one person. You can also view and export the person schedule details.

Before You Start

Add department and person in Access Control module. See ***Manage Organization*** and ***Manage Person Information*** for details.

Perform this task when you need to set person schedule.

Steps

1. Enter Time and Attendance module.
2. Click **Shift Schedule Management** to enter the Shift Schedule Management page.
3. Select the department and select one person.
4. Click **Person Schedule** to pop up Person Schedule window.
5. Check **Time and Attendance**.

   The configured person will apply the attendance schedule.

6. Select the shift from the drop-down list.

7. Set the start date and end date.
8. Set other parameters for the schedule, including Check-in Not Required, Check-out Not Required, Effective for Holiday, Effective for Overtime, and Effective for Multiple Shift Schedules.

> **ⓘ Note**
>
> After checking the **Effective for Multiple Shift Schedules**, you can select the effective time period(s) from the added time periods for the persons in the department.
>
> **Multiple Shift Schedules**
>
> It contains more than one time periods. The person can check in/out in any of the time periods and the attendance will be effective.
> 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.

9. Click **Save**.

17.1.5 Set Temporary Schedule

You can add a temporary schedule for the person and the person will be assigned with the shift schedule temporarily. You can also view and export the temporary schedule details.

Before You Start
Add department and person in Access Control module, and set the attendance rule for the person. See *Manage Organization* and *Manage Person Information* for details.

Perform this task when you need to set temporary schedule.

Steps

> **ⓘ Note**
>
> The temporary schedule has higher priority than department schedule and person schedule.

1. Enter Time and Attendance module.
2. Click **Shift Schedule Management** tab to enter the Shift Schedule Management page.
3. Select the department and select one person.
4. Click **Temporary Schedule** to pop up Temporary Schedule window.
5. Click 📅 to set the shift date.
6. Select the time period.
7. Click the time bar to apply the time period for the select date.
8. **Optional:** Click **Advanced Settings** and select advanced attendance rules for the temporary schedule.
9. Click **Add**.

17.1.6 Check and Edit Shift Schedule

You can check the shift schedule details and edit the schedule.

Perform this task when you need to check and edit shift schedule.

Steps
1. Enter Time and Attendance module.
2. Click **Shift Schedule Management** tab to enter the Shift Schedule Management page.
3. Select the department and corresponding person(s).
4. Click **View** to open Shift Schedule Details window.

    The shift schedule details display.

5. Edit the normal schedule details.
    1) Click **Normal Schedule** tab.
    2) Select a shift from the drop-down list.
    3) Click **Attendance Rule Settings** to open Attendance Rule Settings window.
    4) Select the attendance rules as desired and click **OK**.
    5) Click 🗓 to set the effective date.
    6) Click **Save**.
6. **Optional:** Click **Temporary Schedule** and perform one of the following operations.

Add	Add the temporary schedule for the selected person.
🖉	Edit the time period.
✕	Delete the temporary schedule.

17.2 Manually Correct Check-in/out Record

If the attendance status is not correct, you can manually correct the check-in or check out record. You can also edit, delete, search, or export the check-in or check-out record.

Before You Start
• You should add organizations and persons in Access Control module. For details, refer to *Manage Organization* and *Manage Person Information* .
• The person's attendance status is incorrect.

Perform the following steps to correct the check-in or check-out record.

Steps
1. Enter Time and Attendance module.
2. Click **Attendance Handling → Check-in/out Correction** to enter the Check-in/out Correction page.
3. Click **Add** to enter the Add Check-in/out Correction window.
4. Set the check-in/out correction parameters.
    - Check **Check-in** and set the actual start-work time.

- Check **Check-out** and set the actual end-work time.
5. Click **Employee Name** field and select the person for correction.
6. **Optional:** Input the remark information as desired.
7. Click **Add**.
8. **Optional:** After adding the check-in/out correction, perform one of the following operations.

Search	Set the search conditions and search the correction.
Modify	Edit the selected check-in/out correction.
Delete	Delete the selected check-in/out correction.
Report	Generate and view the check-in/out correction report.
Export	Export the check-in/out correction details to local PC.

Note

The exported details are saved in CSV format.

17.3 Add Leave and Business Trip

You can add leave and business trip application when the employee want to ask for leave or go on a business trip.

Before You Start
You should add organizations and persons in the Access Control module. For details, refer to **Manage Organization** and **Manage Person Information** .

Perform the following steps when you want to add a leave or business trip application.

Steps
1. Enter Time and Attendance module.
2. Click **Attendance Handling → Leave and Business Trip** to enter the Leave and Business Trip page.
3. Click **Add** to open the Add Leave and Business Trip Application window.
4. Select the leave and business trip type from the drop-down list.

Note

You can set the leave type in Advanced Settings. For details, refer to **Configure Leave Type** .

5. Click 📅 and set the time period for your leave or business trip.
6. Click **Employee Name** filed and select the person for the application in the pop-up Add Person window.
7. **Optional:** Input the remark information as desired.
8. Click **Add**.

The added leave and business trip displays on the Leave and Business Trip page.

9. **Optional:** After adding the leave and business trip application, perform one of the following operations.

Modify	Select the leave and business trip and click **Modify** to edit the leave or business application.
Delete	Select the leave and business trip and click **Delete** to delete the leave or business trip application.
Report	Click **Report** to generate the leave or business trip report.
Export	Click **Export** to export the leave or business trip details to local PC.

> **⌷Note**
> The exported details are saved in CSV format.

17.4 Calculate Attendance Data

You need to calculate the attendance data before searching and viewing the overview of the attendance data, employees' detailed attendance data, employees' abnormal attendance data, the employees' overtime working data, and card swiping log.

17.4.1 Automatically Calculate Attendance Data

You can set a schedule so that the client can calculate the attendance data automatically at the time you configured every day.

Perform this task if you need to set the time to make the client calculate attendance data automatically.

Steps

> **⌷Note**
> It will calculate the attendance data till the previous day.

1. Enter the Time and Attendance module.
2. Click **Attendance Handling → Attendance Calculation** to enter the attendance record calculation page.
3. In the Auto-Calculate Attendance panel, set the time that you want the client to calculate the data every day.
4. Click **Save**.

17.4.2 Manually Calculate Attendance Data

You can calculate the attendance data manually by setting the data range.

Perform the following steps to manually calculate the attendance data.

Steps
1. Enter the Time and Attendance module.
2. Click **Attendance Handling → Attendance Calculation** to enter the attendance record calculation page.
3. In the Manually Calculate Attendance panel, set the start time and end time to define the attendance data range.
4. Click **Calculate**.

   ⓘ**Note**

   It can only calculate the attendance data within three months.

17.5 Configure Advanced Settings

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

17.5.1 Configure Basic Parameters

You can configure the attendance basic parameters, including the start day of each week, the start date of each month, and the non-work day.

Perform the following steps to configure the attendance basic parameters.

Steps
1. Enter Time and Attendance module.
2. Click **Advanced Settings → Basic Settings** to enter the Basic Settings page.
3. Set the start day of each week and the start date of each month from the drop-down list.
4. Set the non-work day settings.

   Set as Non-Work Day

   Check the checkboxes to set the dates as non-work days.

   Set Non-Work Day's Color in Report

   Select the color from the Select Color window. The non-work days in the report will mark as the configured color.

   Set Non-Work Day's Mark in Report

   Input the mark and the non-work day field in the report will display with the mark.

5. Set the authentication type, which means the client will calculate the attendance data recorded based on the selected authentication type.
6. Click **Save**.

17.5.2 Configure Attendance Rule

You can configure the attendance rule for all shifts before setting shift. You can configure the rule for attendance/absence, check-in/out, and overtime.

Perform the following steps to configure the attendance rule.

Steps

 Note
The parameters configured here will be set as default for the newly added time period. It will not affect the existed one(s).

1. Enter Time and Attendance module.
2. Click **Advanced Settings → Attendance Rule Settings** to enter the Attendance Rule Settings page.
3. Set rule parameters, including attendance/absence parameters, check-in/out parameters, and overtime parameters.
4. **Optional:** Check **Non-scheduled Work Day** and set the overtime rule for non-work day.
5. Click **Save**.

17.5.3 Configure Attendance Check Point

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.

Before You Start
You should add access control device before configuring attendance check point. For details, refer to *Add Device* .

Perform the following steps to set the card reader of the access control point as the attendance check point.

Steps

 Note
By default, all card readers of the added access control devices are set as attendance checkpoint.

1. Enter the Time and Attendance module.
2. Click **Advanced Settings → Attendance Check Point Settings** to enter the Attendance Check Point Settings page.
3. **Optional:** Uncheck **Set All Card Readers as Check Points**.

Only the card readers in the list will be set as the attendance check points.

4. Click ➕ to enter the Add Attendance Check Point window.

5. Set the related parameters.

Check Point Name

Customize a name for the check point.

Card Reader

Select the card reader from the drop-down list as the attendance check point.

Check Point Function

Select the check point function from the drop-down list. You can set the check point as Start/End-Work check point, Start-Work check point, or End-Work check point.

Door Location

Input the door location's name.

Check Point Description

Input the check point's descriptions as desired.

6. Click **Add**.

The added attendance check point displays on the list.

7. **Optional:** After adding the attendance check point, perform one of the following operations.

    📝   Edit the attendance check point information.

    ❌   Delete the attendance check point in the list.

17.5.4 Configure Holiday

You can add the holiday during which the check-in or check-out function will be invalid.

Add Holiday with Fixed Date

You can configure a holiday which will take effect for only once.

Perform this task if you want to configure a holiday with fixed date.

Steps

1. Enter the Time and Attendance module.

2. Click **Advanced Settings → Holiday Settings** to enter the Holiday Settings page.

3. Click ➕ to pop up the Add Holiday window.
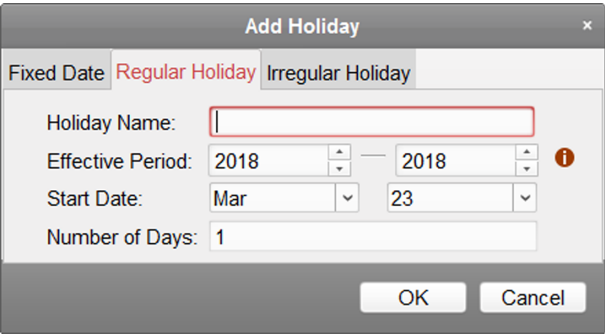
4. Click **Fixed Date** tab.
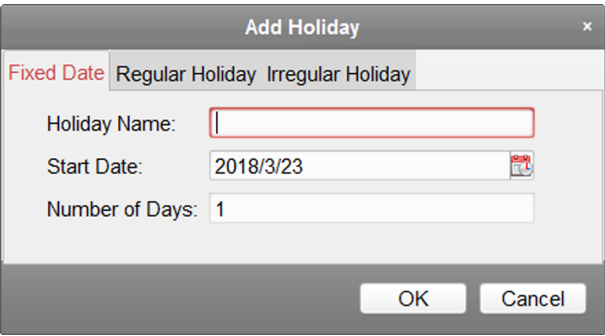
Figure 17-1 Add Holiday with Fixed Date

5. Customize a name for the holiday.
6. Set the start date as the first day of the holiday.
7. Set the number of days in the holiday.
8. **Optional:** After adding the holiday, perform one of the following operations.

    ☑   Edit the holiday information.

    ✖   Delete the holiday from the holiday list.

Add Regular Holiday

You can configure a holiday which will take effect annually on regular days during the effective period, such as New Year's Day, Independence Day, Christmas Day, etc.

Perform this task if you need to add a regular holiday.

Steps
1. Enter the Time and Attendance module.
2. Click **Advanced Settings → Holiday Settings** to enter the Holiday Settings page.
3. Click ➕ to pop up the Add Holiday window.
4. Click **Regular Holiday** tab.

Figure 17-2 Add Regular Holiday

5. Set the holiday parameters.
   Start Date

The first day of the holiday.

Effective Period

The years during which the holiday's start date will take effect. For example, if the holiday's effective period is set as 2018 to 2019, and the start date is set as December 31st, and the numbers of days is 3, then the holiday will be 2018/12/31 to 2019/01/02, 2019/12/31 to 2020/01/02.

6. Click **OK**.
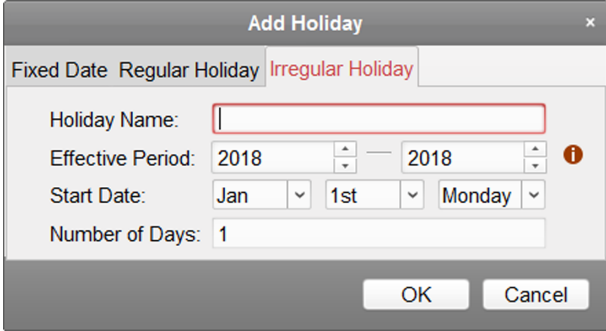7. **Optional:** After adding the holiday, perform one of the following operations.

    ✎   Edit the holiday information.

    ✕   Delete the holiday from the holiday list.

Add Irregular Holiday

You can configure a holiday which will take effect annually on irregular days during the effective period, such as Bank Holiday.

Perform this task if you want to add an irregular holiday.

Steps
1. Enter the Time and Attendance module.
2. Click **Advanced Settings → Holiday Settings** to enter the Holiday Settings page.
3. Click ➕ to pop up the Add Holiday window.
4. Click **Irregular Holiday** tab.

Figure 17-3 Add Irregular Holiday

5. Set the holiday parameters.

Start Date

The first day of the holiday.

Effective Period

The years during which the holiday's start date will take effect. For example, if the holiday's effective period is set as 2018 to 2019, and the start date is set as December 31st, and the

numbers of days is 3, then the holiday will be 2018/12/31 to 2019/01/02, 2019/12/31 to 2020/01/02.

[i] **Note**

If one holiday crosses two years and the effective period

6. Click **OK**.
7. **Optional:** After adding the holiday, perform one of the following operations.

[✎]   Edit the holiday information.

[✗]   Delete the holiday from the holiday list.

17.5.5 Configure Leave Type

You can customize the leave type according to actual needs. By default, there are three major leave types: Leave, Day Off in Lieu, and Go Out on Business.

Perform the following steps to add, edit, or delete the leave type.

Steps
1. Enter the Time and Attendance module.
2. Click **Advanced Settings → Leave Type Settings** to enter the Leave Type Settings page.
3. Click [+] to add a major leave type on the left panel.
4. **Optional:** Perform one of the following operations for major leave type.

[✎]   Edit the major leave type.

[✗]   Delete the major leave type.
5. Click [+] to add a minor leave type on the right panel.
6. **Optional:** Perform one of the following operations for major leave type.

[✎]   Edit the minor leave type.

[✗]   Delete the minor leave type.

17.6 View Attendance Report

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.

17.6.1 Get an Overview of Employees' Attendance Data

You can search the employee's required attendance times, actual attendance times, late times, early leave times, absent times, overwork times, leave times, etc. in a time period to get an overview of the employees' attendance data.

Before You Start
• You should add organizations and persons in Access Control module and the persons has swiped card. For details, refer to *Manage Organization* and *Manage Person Information* .
• Calculate the attendance data.

> 📖**Note**
> • The client will automatically calculate 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 *Manually Calculate Attendance Data* .

Perform the following steps to search the employees' all attendance data in a time period.

Steps
1. Enter the Time and Attendance module.
2. Click **Attendance Statistics → Attendance Summary** to enter the Attendance Summary page.
3. Select a department from the drop-down list.
4. **Optional:** Input the person name for search.
5. Select the attendance start date and end date that you want to search from.
6. **Optional:** Click **Reset** to reset all search conditions and edit the search conditions again.
7. Click **Search**.

   The result displays on the page. You can view the employee's required attendance times, actual attendance times, late times, early leave times, absent times, overwork times, leave times, etc.

8. **Optional:** After searching the result, perform one of the following operations.

Report	Generate the attendance report.
Export	Export the results to the local PC.

17.6.2 Search Employees' Detailed Attendance Data

You can search the employee's every attendance data with details, including the attendance date, the person belonged shift, time period, start-work status, end-work status, check-in time, check-out time, late period, early leave period, attendance period, absence period, leave period, and overwork period.

Before You Start

- You should add organizations and persons in Access Control module and the persons has swiped card. For details, refer to ***Manage Organization*** and ***Manage Person Information*** .
- Calculate the attendance data.

---

[i]**Note**

- The client will automatically calculate 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 ***Manually Calculate Attendance Data*** .

Perform the following steps to search the employee's detailed attendance data.

Steps

1. Enter the Time and Attendance module.
2. Click **Attendance Statistics → Attendance Details** to enter the Attendance Details page.
3. Select a department from the drop-down list.
4. **Optional:** Input the person name for search.
5. Select the attendance start date and end date that you want to search from.
6. **Optional:** Check the attendance status that you want to search.
7. **Optional:** Click **Reset** to reset all search conditions and edit the search conditions again.
8. Click **Search**.

   The detailed information of the attendance details displays below. You can view the attendance date, the person belonged shift, time period, start-work status, end-work status, check-in time, check-out time, late period, early leave period, attendance period, absence period, leave period, and overwork period.

9. **Optional:** After searching the result, perform one of the following operations.

Report	Generate the attendance report.
Export	Export the results to the local PC.

17.6.3 Search Employees' Abnormal Attendance Data

You can search and get the statistics of the employee's abnormal attendance data, including No., name and department of the employees, abnormal type, start/end time and date of attendance.

Before You Start

- You should add organizations and persons in Access Control module and the persons has swiped card. For details, refer to ***Manage Organization*** and ***Manage Person Information***
- Calculate the attendance data.

⌐ⓘ⌐**Note**

- The client will automatically calculate 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 ***Manually Calculate Attendance Data*** .

Perform the following steps to search the employee's abnormal attendance data.

Steps
1. Enter the Time and Attendance module.
2. Click **Attendance Statistics → Abnormal Attendance** to enter the Abnormal Attendance page.
3. Select a department from the drop-down list.
4. **Optional:** Input the person name for search.
5. Select the attendance start date and end date that you want to search from.
6. **Optional:** Click **Reset** to reset all search conditions and edit the search conditions again.
7. Click **Search**.

   The result displays below. You can view the employee No., the person name, the person belonged department, the abnormal type, the abnormal start time, the abnormal end time, and the abnormal date.

8. **Optional:** After searching the result, perform one of the following operations.

Report	Generate the attendance report.
Export	Export the results to the local PC.

17.6.4 Search Employees' Overtime Working Data

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.

Before You Start
- You should add organizations and persons in Access Control module and the persons has swiped card. For details, refer to ***Manage Organization*** and ***Manage Person Information*** .
- Calculate the attendance data.

⌐ⓘ⌐**Note**

- The client will automatically calculate 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 ***Manually Calculate Attendance Data*** .

Perform the following steps to search the overtime working data.

Steps
1. Enter the Time and Attendance module
2. Click **Attendance Statistics → Overtime Search** to enter the Overtime Search page.
3. Select a department from the drop-down list.
4. **Optional:** Input the person name for search.
5. Select the attendance start date and end date that you want to search from.
6. **Optional:** Click **Reset** to reset all search conditions and edit the search conditions again.
7. Click **Search**.

   The detailed information of the overtime work result displays below. You can view the employee No., the person name, the person belonged department, the overtime work's date, the overtime duration, and the overtime type.

8. **Optional:** After searching the result, perform one of the following operations.

Report	Generate the attendance report.
Export	Export the results to the local PC.

17.6.5 Check Employees' Card Swiping Logs

You can search and view the employees' card swiping logs when you want to check the employees' card swiping details.

Before You Start
- You should add organizations and persons in Access Control module and the persons has swiped card. For details, refer to **Manage Organization** and **Manage Person Information** .
- Calculate the attendance data.

> **⛾Note**
>
> - The client will automatically calculate 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 **Manually Calculate Attendance Data** .

Perform the following steps to searching and the view card swiping log.

Steps
1. Enter the Time and attendance module.
2. Click **Attendance Statistics → Card Swiping Log** to enter the Card Swiping Log page.
3. Configure the search conditions, including the employee department, employee name, or attendance date.
4. **Optional:** Click **Reset** to reset all search conditions.
5. Click **Search**.

The search result lists on this page.

You can view the result details, including the employee No., employee name, department, time, authentication mode, and card No.

6. **Optional:** After searching and view the card swiping log, perform one of the following operations.

Report	Generate the attendance report.
Export	Export the results to the local PC.

17.6.6 Generate Attendance Report

After the attendance data is calculated, you can generate reports which show the attendance status of the employees in the specific time period.

Generate Instant Report

It supports to generate the a series of attendance reports manually to view the employees' attendance results.

Before You Start
Calculate the attendance data.

⌷**Note**

You can calculate the attendance data manually, or set the schedule so that the client can calculate the data automatically every day. For details, refer to *Calculate Attendance Data* .

Perform the following steps to generate the attendance report instantly.

Steps
1. Enter the Time and Attendance module.
2. Click **Attendance Statistics → Report** to enter the Report page.
3. In the Instant Report panel, select a report type from the drop-down list.
4. Select a person or department.
5. Set the time period during which the attendance data will be displayed in the report.
6. Click **Generate**.

Configure Scheduled Report

It supports 5 report types and you can pre-define the report content and it will send the report automatically to the email address you configured.

Perform this task if you want to configure a scheduled report.

Steps

[i]**Note**

Set the email parameters before you want to enable auto-sending email functions. For details, refer to *Set Email Parameters* .

1. Enter the Time and Attendance module.
2. Click **Attendance Statistics → Report** to enter the Report page.
3. In the Scheduled Report panel, click **Add** to pre-define a report and set the report content.
4. Set the report content.

   Person

   Select the added person(s) and click $\boxed{>}$ to add the person.

5. **Optional:** Set the schedule to send the report to the email address(es) automatically.
   1) Set the **Auto-Sending Email** switch to ON to enable this function.
   2) Set the effective period during which the client will send the report on the selected sending date(s).
   3) Select the date(s) on which the client will send the report.
   4) Set the time at which the client will send the report.

   Example

   If you set the effective period as *2018/3/10 to 2018/4/10*, select *Friday* as the sending date, and set the sending time as *20:00:00*, the client will send the report at 8 p.m. on Fridays during 2018/3/10 to 2018/4/10.

   [i]**Note**

   Make sure the attendance records are calculated before the sending time. You can calculate the attendance data manually, or set the schedule so that the client can calculate the data automatically every day. For details, refer to *Calculate Attendance Data* .

   5) Input the receiver email address(es).

   [i]**Note**

   You can click ✚ to add a new email address. Up to 5 email addresses are allowed.

6. Click **Save**.
7. **Optional:** After adding the scheduled report, you can do one or more of the followings:

Modify Report	Select one added report and click **Modify** to edit its settings.
Delete Report	Select one added report and click **Remove** to delete it.
Generate Report	Select one added report and click **Generate** to generate the report instantly and you can view the report details.

Chapter 18 Video Intercom

The client provides video intercom functions such as video intercom with the added video intercom devices, checking call logs, and sending notice to the residents.

You should add the device to the client and configure the person to link the device in the Access Control module.

Note
- 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 **Add Device** .
- For details about configuring person in the Access Control module, refer to .

18.1 Manage Calls between Client Software and Indoor/Door Station

You can call the residents via the client software and the residents can also call the client software via the indoor station or door station.

18.1.1 Call Indoor Station from Client

You can call the added indoor station via the client and perform video intercom.

Perform this task if you want to call the indoor station via the client.

Steps

Note
- 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.

1. Enter the **Access Control → Video Intercom** page.
2. Unfold the organization list on the left panel and 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 📞 in the Call Household column to start calling the selected resident.
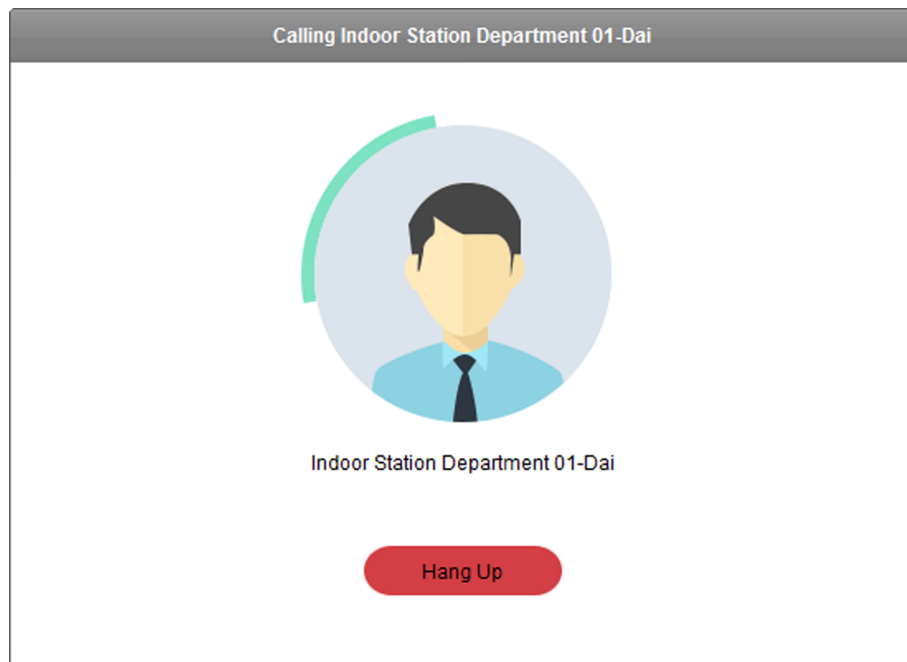
Figure 18-1 Start Calling Resident

After the call is answered, you will enter the In Call window.

5. **Optional:** After the call is answered, you can do one or more of the following operations:

Adjust the volume of the loudspeaker.

Hang up.

Adjust the volume of the microphone.

18.1.2 Call Client from Indoor Station/Door Station

The residents can call the security center via the indoor station or door station. The security personnel can perform the video intercom of the residents via the client.

Perform this task if you need to receive the call from indoor station or door station.

Steps

Note

- 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 the client can be set from 120s to 600s via the Remote Configuration of indoor station.
- The maximum speaking duration between door station and the client can be set from 90s to 120s via the Remote Configuration of door station.

1. Enter the **Access Control → Video Intercom** page.
2. Select the client software on the device interface of the indoor station or door station to start calling the client software.

   An incoming call dialog will pop up in the client software.
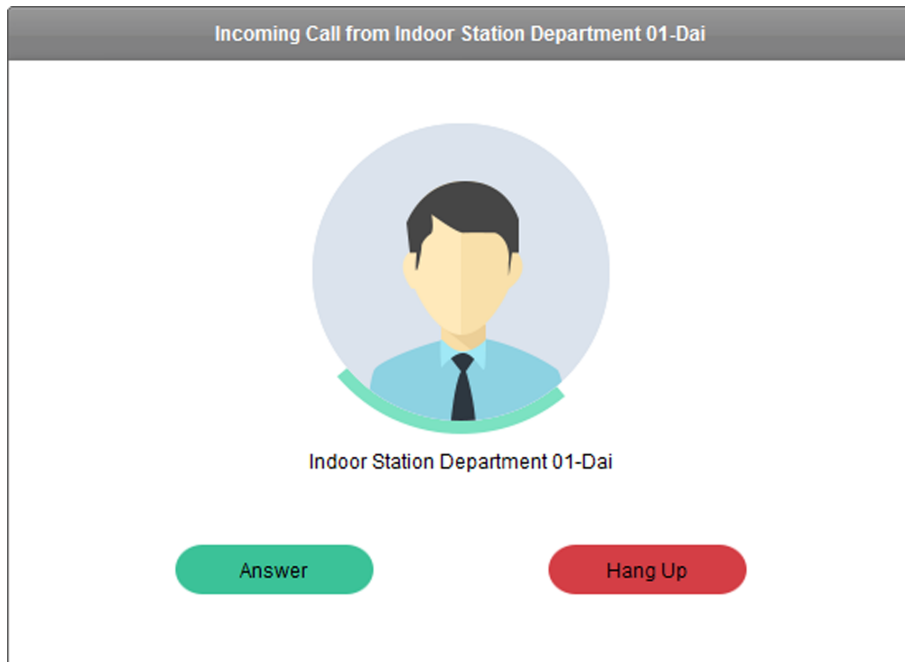
Figure 18-2 Incoming Call Window

3. Click **Answer** to answer the call.

   After the call is answered, you will enter the In Call window.
4. **Optional:** In the In Call window, you can do one or more of the following operations.

   - Adjust the volume of the loudspeaker.
   - Hang up.
   - Adjust the volume of the microphone.
   - Remotely open door for door station.

18.1.3 View Live Video of Door Station and Outer Door Station

You can get the live view of the door station and outer door station in the Main View module and control the door station or outer door station remotely.

Before You Start

Add a door station or an outer door station. For details, refer to **_Add Device_** .

Perform the following steps to view live videos of the door station or outer door station in the Main View module.

Steps

1. Enter the Main View page.
2. Start live view.
   - Double click a door station or an outer door station in the device list.
   - Drag a door station an outer door station to a display window.

   Note

   For detailed operations of live view, refer to **_Live View_** .

3. **Optional:** Right-click the live view window to open the right-click menu and click **Unlock** to open the door remotely.

   Note

   If the two door stations (such as at front door and back door) are connected, you can select to unlock one of the two doors remotely.

18.2 View Real-Time Call Logs

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.

Perform this task if you need to view the real-time video intercom call logs.

Steps

1. Enter the **Access Control → Video Intercom → 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.
4. 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 page, you can still find the deleted logs in **Search → Call Log** page. For details, refer to **_Search Call Logs_** .

18.3 Release Notice to Resident

You can create different types of notices and send them to the residents. Four notice types are available: advertising, property, alarm, and notice information.

Perform this task when you need to release a notice to the residents on the client software.

Steps
1. Enter the **Access Control** → **Video Intercom** → **Release Notice** page.
2. Click **New Notice** on the left panel to create a new notice.
3. Click ✚ in the **Send To** field to select the residents in the Select Resident window.
4. Input the notice subject.

   📖**Note**

   Up to 63 characters are allowed in the Subject field.

   ---

5. In the **Type** filed, 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.
   - The maximum size of one picture is 512 KB.

   ---

7. Input the notice content.

   📖**Note**

   Up to 1023 characters are allowed in the Content field.

   ---

8. Click **Send** to send the 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.

18.4 Search Video Intercom Information

You can search the call logs between the client software and video intercom devices, device unlocking logs, and the sent notice information.

18.4.1 Search Call Logs

You can search the call logs of the video intercom devices in the specified time period.

Perform this task if you need to search the call logs of the video intercom devices.

Steps

1. Enter the **Access Control → Search → Call Log** page.
2. Set the search conditions, including call status, device type, start time and end time.
3. Click **Search**.

   All the matched call logs will display.

4. **Optional:** Click **Export** to export the call logs to your PC.

18.4.2 Search Unlocking Logs

You can search the unlocking logs of the video intercom devices (Door Station or Door Station (V Series)) in the specified time period.

Perform this task if you need to search the video intercom device's unlocking logs.

Steps

1. Enter the **Access Control → Search → Unlocking Log** page.
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, including **Unlock by Password**, **Unlock by Duress**, **Unlock by Card**, **Unlock by Resident**, or **Unlock by Center**.

3. Click **Search**.

   All the matched unlocking logs will display.

4. **Optional:** Click in the Capture column in the result list to view the captured pictures.

   $\boxed{i}$**Note**

   The function should be supported by device.

   ---

5. **Optional:** Click **Export** to export the unlocking logs to your PC.

18.4.3 Search Notice

You can search the notice sent to the residents in the specified time period.

Perform this task if you need to search the notice sent to the residents.

Steps

1. Enter the **Access Control → Search → Notice** page.
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**. Or select **All** to search notices with all types.

3. Click **Search**.

All the matched notices will display.

4. **Optional:** Click ⚙ in the Operation column to view and edit the notice details, check the sending failed/sent succeeded/unread users, and resend the notice to the sending failed/ unread users.
5. **Optional:** Click **Export** to export the notices to your PC.

Chapter 19 View Face Picture Comparison Alarm

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.

19.1 View Captured Face Picture

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
Configure the capture rule for the device. For details, refer to the User Manual of the device

Perform this task when you need to view the captured face picture.

Steps
1. Click **Face Picture Comparison Alarm** on the control panel to enter this module.
2. Click ⊞ to set window division.
3. Double-click the camera name after clicking a display window to start the live view.

   Stop Live View

   Click ▭ for stopping live view.

   Full Screen

   Click ⊡ to show the full screen.
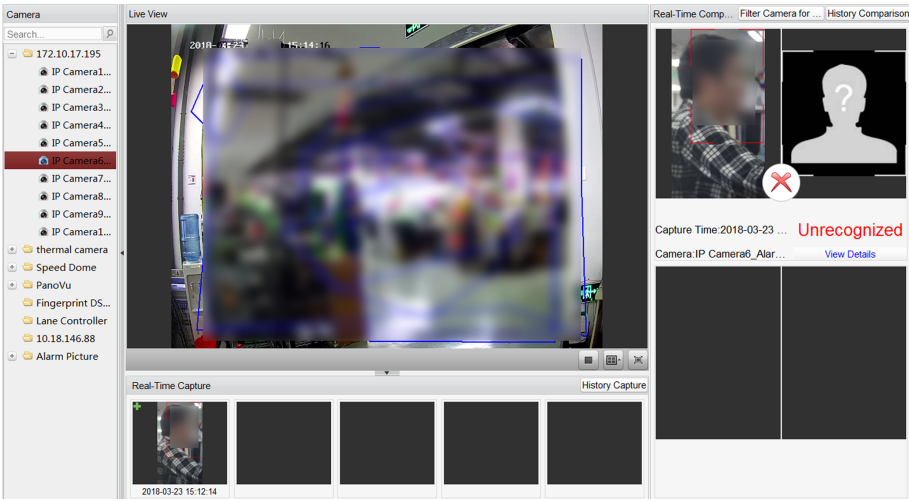
Figure 19-1 View Captured Face Picture

The captured face pictures and capture time will display in the Real-Time Capture list in real time.
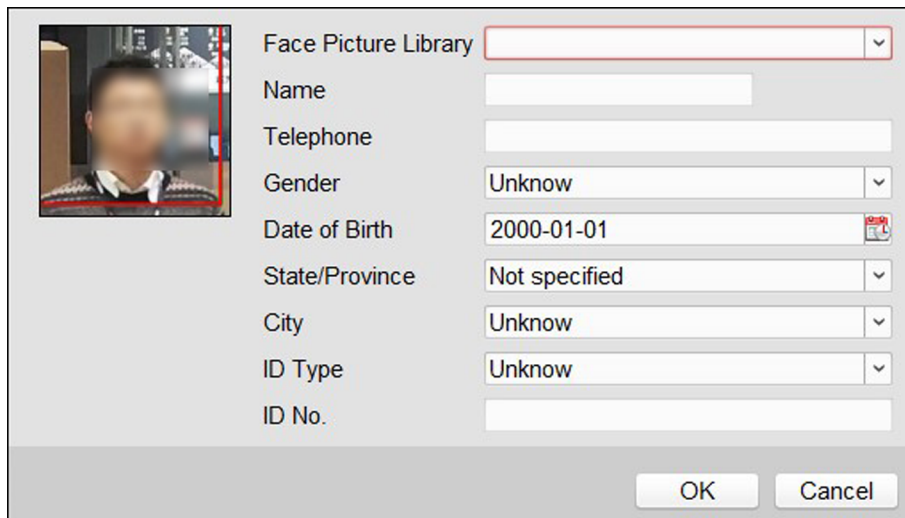
4. Click **Filter Camera for Alarm** to display the alarm pictures of the selected camera(s) that you concerned.

5. Optional: Click **History Capture** to view the historical captured face pictures.

> 📖**Note**
>
> - 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.

6. Optional: Add the captured face picture to the face picture library.
1) Click ➕ on the upper upper-left corner of the captured face picture to open the window.

Figure 19-2 Add Face Picture to Face Picture Library

2) Select a face picture library from the drop-down list.
3) Input the person details.
4) Click **OK**.

> 📖**Note**
>
> 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.

7. Optional: Click **History Comparison** to view the historical matched face pictures.

> 📖**Note**
>
> - 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.

19.2 View Matched Face Pictures

If the captured face picture matches with the face picture in the face picture library, you can view the matched person information. You can view the real-time or historical face picture comparison records.

Before You Start
Configure the capture rule for the device. For details, refer to the User Manual of the device.

Perform this task when you need to view the matched face picture.

Steps
1. Click **Face Picture Comparison Alarm** on the control panel to enter this module.
2. Click ▦ to set window division.
3. Double-click the camera name after clicking a display window to start the live view.

   Stop Live View

   Click ▬ for stopping live view.

   Full Screen

   Click ▣ to show the full screen.

   🛈**Note**

   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.

4. Click **Filter Camera for Alarm** to display the alarm pictures of the selected camera(s) that you concerned.
5. **Optional:** Click **History Comparison** to view the historical matched face pictures.

   🛈**Note**

   - 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.

19.3 View Face Picture Comparison Alarm Logs

You can view the face capture alarm logs and face picture comparison alarm logs. You can also export them to the local PC.

19.3.1 Search Face Picture Comparison Alarm Logs

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.

Perform this task when you need to search the client logs, or export the logs to the local PC.

Steps
1. Click **Tool → Search Alarm Log** on the client menu bar.
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.

ⓘNote

You can view the alarm logs if the camera has been configured with Storage Server to save the alarm pictures. Refer to ***Store Picture and Video on Storage Device*** for setting the picture storage on Storage Server.

The matched alarm logs will display.

5. **Optional:** Export 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**.

   ⓘ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) Select the logs that you want to export.
   2) Click **Export Selected**.
   3) Click ⋯ to select a saving path on local PC and create a name for the exported file.
   4) Click **OK**.

   ⓘNote

   The file exported is in XML file.

19.3.2 Open Face Picture Comparison Alarm Logs

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.

Before You Start

Export the logs to the local PC. Refer to ***Search Face Picture Comparison Alarm Logs*** .

Perform this task when you need to open the alarm log file.

Steps
1. Click **Tool → Search Alarm Log** on the client menu bar.
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**.

    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 20 Statistics

Statistics module provides eight modules for data statistics via the software: heat map, people counting, counting, road traffic, face picture retrieval, license plate retrieval, behavior analysis, and captured face analysis.

20.1 Heat Map Report

Heat map is a graphical representation of data represented by colors and the heat map data can be displayed in line chart. You can use the heat map function of the camera to analyze the visit times and dwell time of customers in a configured area.

Before You Start

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. See *Add Device* for details about adding heat map network camera.

Perform this task when you need to generate a heat map report.

Steps

1. Click **Heat Map** on the control panel to open Heat Map page.
2. Select a heat map camera in the camera list.
3. Select the report type as needed and set the start time.
4. Click **Generate Heat Map** to show the heat map of the camera.
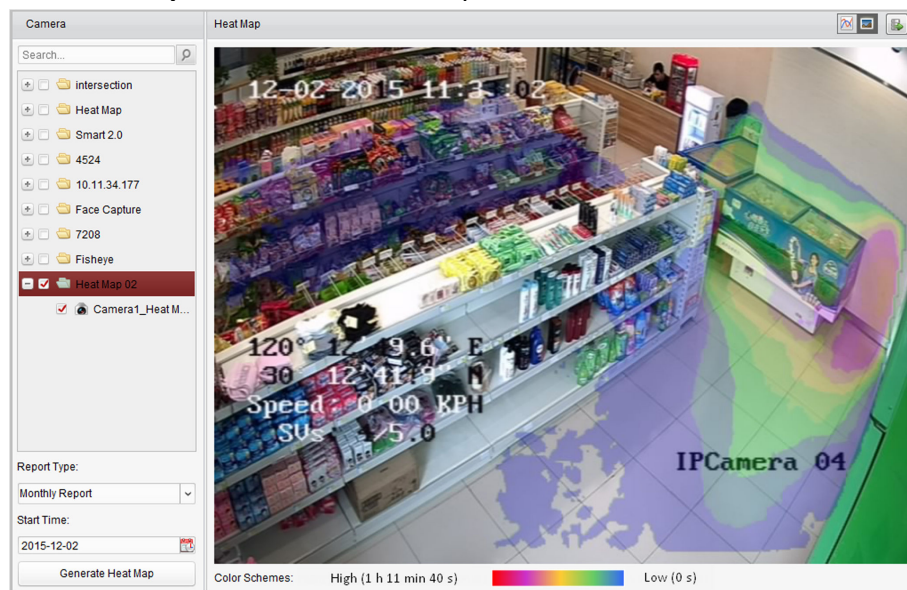
Figure 20-1 Results

5. **Optional:** After generating heat map report, you can perform the following operations.

Display in Line Chart	Click ⊠ to display the statistics in line chart.
Display in Picture Mode	Click ▇ to display the statistics 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.
Save Statistics Data	Click ▇ to save the detailed data of heat map to your PC.

20.2 People Counting Report

You can check the people counting statistics of the added people counting device and the statistics can be displayed in line chart or histogram. You can export the detailed data for local storage.

Before You Start

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. Refer to *Add Device* for details about adding people counting device.

Perform this task when you need to generate people counting report.

Steps
1. Click **People Counting** on the control panel to open 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 the statistics type.

      One Camera in Multi-period

      Select one camera for generating the statistics in two time periods.

      One Camera in One Period

      Select one camera for generating the statistics in one time period.
   3) Select the data type.

      Enter

      The people entered will be counted.

      Exit
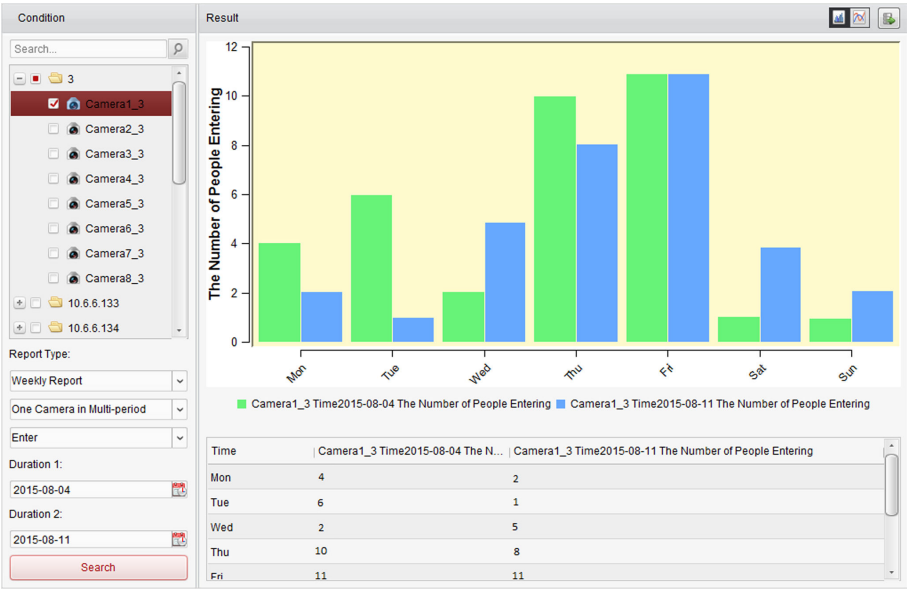
      The people exited will be counted.

      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** to get the people counting statistics and detailed data for each hour, day, or month.

Figure 20-2 Results

The statistics are shown in histogram form.

5. **Optional:** Perform the following operations after search.

Switch to Line Chart	Click ⚞ to switch it to line chart.

> **Note**
> By default, the statistics are shown in histogram form.

Save to Local PC	Click ⚞ to save the detailed data of people counting to your PC.

20.3 Counting Report

You can check the counting statistics of the added counting device and the statistics can be displayed in line chart or histogram. You can export the detailed data for local storage.

Before You Start
Add a counting device to the software and properly configure the corresponding area. The added device should have been configured with counting settings. Refer to ***Add Device*** for details about adding counting device.

Perform this task when you need to generate counting report.

Steps
1. Click **Counting** on the control panel to open 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 the statistics type.

One Camera in Multi-period

Select one camera for generating the statistics in two time periods.

One Camera in One Period

Select one camera for generating the statistics in one time period.

3) Select 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** to get the people counting statistics and detailed data for each hour, day or month.

Figure 20-3 Results

The statistics are shown in histogram form. You can click ⊠ to switch it to line chart.

5. **Optional:** Click ⊡ to save the detailed data of counting to your PC.

20.4 Road Traffic Report

If you add road traffic monitoring device to the client, you can search and view the captured pictures of the detected vehicle or license plate. Three types are available for searching the corresponding pictures: Vehicle Detection, Mixed-traffic Detection, and Traffic Violations.

Before You Start
- Add a road traffic monitoring device to the software and properly configure the corresponding detection area. The added device should have been configured with corresponding settings for capturing pictures. Refer to **Add Device** for details about adding the device.
- For Traffic Violations, add the storage server to software first and you should configure the storage server for the device and check **Picture Storage** and **Additional Information Storage** . See **Store Picture and Video on Storage Device** for details.

Perform this task when you need to generate a road traffic report.

Steps
1. Click **Road Traffic** on the control panel to open Road Traffic page.
2. Select a road traffic monitoring camera in the camera panel.
3. Set the search condition for finding the related pictures.
   1) Select the query type and the pictures triggered by the event type can be found.

      Vehicle Detection

      Detect the passed vehicle and capture the picture of its license plate; besides, the vehicle color, vehicle logo and other information can be recognized automatically.

      Mixed-traffic Detection

      Search 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).

      Traffic Violations

      Check the captured pictures of the vehicle that violates the traffic rules (such as illegal parking and congestion).
   2) Input the license plate number for searching the pictures.
   3) Click 🗓 to set the start time and end time.
4. Click **Search**.

   ⓘ**Note**

   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.

5. **Optional:** After searching, you can perform the following operations.

   | View Picture Details | Click 🖼 to pop up Picture Preview window to view the captured pictures and the related information. |

Download Picture	Check **Select Current Picture** or **Select All** on Picture Preview window and click **Download**, or check the checkboxes of the picture items on Road Traffic page and click **Export Picture** to download the selected pictures.

20.5 Face Picture Retrieval

When the connected device (NVR or HDVR) supports face search, you can search the related picture and play the picture related video file.

20.5.1 Search Face Picture by Uploaded Picture

You can upload a face picture from your PC and compare the uploaded picture with the captured face pictures.

Before You Start
Add the device to the software and properly configure the corresponding settings. Refer to **Add Device** for details about adding the device.

Perform this task when you need to search the face picture by picture.

Steps

Note

This function should be supported by the connected device.

1. Click **Face Picture Retrieval** on the control panel to open the Face Picture Retrieval page.
2. Select device(s) in the camera panel.
3. Select **Picture** from the drop-down list to search by picture.
4. Select a face picture for search.
   1) Click **Select Picture** to upload the pictures from your PC.
   2) Select a detected face from uploaded picture for matching the captured face pictures.

Note

- 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.

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. Set the maximum number of displayed results.
7. Click 🗓 to set the start time and end time for searching the captured face pictures or video files.

8. Click **Search** to start searching.

The search results of the pictures are displayed in list.

9. Export the pictures and save them in your PC.

Export Picture

Export all the pictures retrieval.

Export Current Page

Export the pictures in the current page.

Export Segment

You can download the pictures by packages.Each package contains up to 1,000 pictures.

10. 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**.
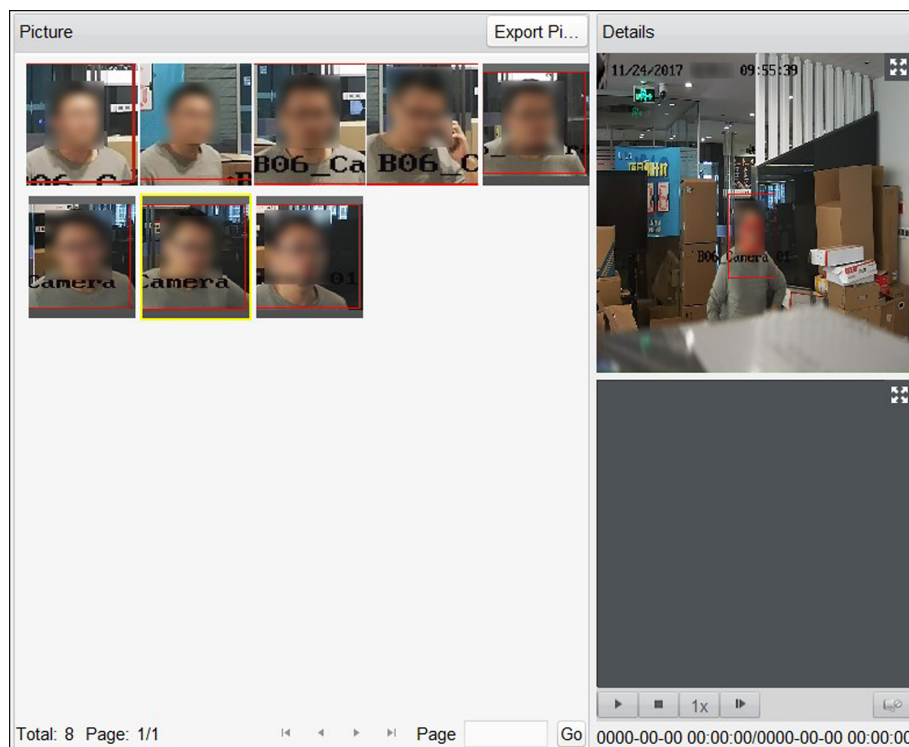
Figure 20-4 Result

The client will search and compare the faces in the captured pictures based on the face picture you selected.

11. Optional: After searching, you can do one or more the following operations.

View Details	Click on a picture from the list to view details. You can also click ⊞ to show the large picture, and click ⊞ to restore.
Play Related Videos	Click ▶ to play the picture's related video file in the view window on the bottom right.

> **ⓘNote**
> - You can click ⊞ to show the large video, and click ⊞ to restore.
> - You can click 1x to adjust the play speed of the playback, click ▶ to play back the video files frame by frame, click 🔇 to enable the audio, double-click the playback window to maximize the window.

Save Pictures to PC	Click **Export Picture** and select the pictures as desired to export to local PC.

20.5.2 Search Face Picture by Event

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. Refer to ***Add Device*** for details about adding the device.

Perform this task when you need to search the face picture by event.

Steps

> **ⓘNote**
> This function should be supported by the connected device.

1. Click **Face Picrure Retrieval** on the control panel to open the Face Picrure Retrieval page.
2. Select device(s) in the camera panel.
3. Select **Event Type** from drop-down list to search by event type.
4. Select event type.

    All

    Search all captured face pictures.

    Face Picture Comparison

    Search the captured pictures which match with the face pictures in face picture library.

    Stranger Detection Alarm

    Search the pictures captured when the stranger detection alarm is triggered.

5. Set the maximum number of displayed results.
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.
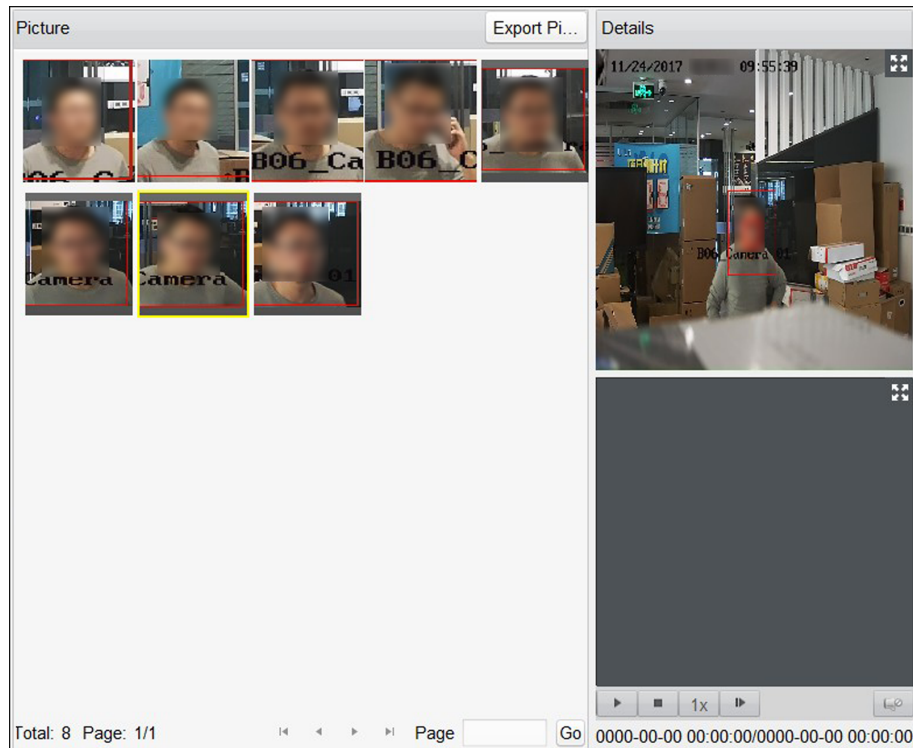
Figure 20-5 Search Result

The search results of the pictures are displayed in list.

8. Export the pictures and save them in your PC.

Export Picture

Export all the pictures retrieval.

Export Current Page

Export the pictures in the current page.

Export Segment

You can download the pictures by packages.Each package contains up to 1,000 pictures.

9. **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.

10. Optional: After searching, you can do one or more the following operations.

View Details	Click on a picture from the list to view details. You can also click ▦ to show the large picture, and click ▦ to restore.
Play Related Videos	Click ▶ to play the picture's related video file in the view window on the bottom right.

> **⌈i⌉Note**
> - You can click ▦ to show the large video, and click ▦ to restore.
> - You can click **1x** to adjust the play speed of the playback, click ▶ to play back the video files frame by frame, click ▣ to enable the audio, double-click the playback window to maximize the window.

Save Pictures to PC	Click **Export Picture** and select the pictures as desired to export to local PC.

20.5.3 Search Face Picture by Person Name

You can search the device's captured face pictures by person name.

Before You Start
Add the device to the software and properly configure the corresponding settings. Refer to ***Add Device*** for details about adding the device.

Perform this task when you need to search the face picture by person name.

Steps

> **⌈i⌉Note**
> This function should be supported by the connected device.

1. Click **Face Picture Retrieval** on the control panel to open the Face Picture Retrieval page.
2. Select device(s) in the camera panel.
3. Select **Person Name** from the drop-down list to search by person name.
4. Enter a keyword for the person name.
5. Set the maximum number of displayed results.
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.

8. Export the pictures and save them in your PC.

   Export Picture

   Export all the pictures retrieval.

   Export Current Page

   Export the pictures in the current page.

Export Segment

You can download the pictures by packages. Each package contains up to 1,000 pictures.

9. 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.
10. After searching, you can do one or more the following operations.

View Details	Click on a picture from the list to view details. You can also click ⊞ to show the large picture, and click ⊞ to restore.
Play Related Videos	Click ▶ to play the picture's related video file in the view window on the bottom right.

> **ℹ️Note**
> - You can click ⊞ to show the large video, and click ⊞ to restore.
> - You can click **1x** to adjust the play speed of the playback, click ▶ to play back the video files frame by frame, click 🔊 to enable the audio, double-click the playback window to maximize the window.

Save Pictures to PC	Click **Export Picture** and select the pictures as desired to export to local PC.

20.6 License Plate Retrieval

When the connected device supports license plate search, you can search the related picture and play the picture related video file.

Before You Start
Add the device to the software and properly configure the corresponding settings. See ***Add Device*** for details about adding the device.

Perform this task when you need to search the license plate.

Steps
1. Click **License Plate Retrieval** on the control panel to open License Plate Retrieval page.
2. Select a device in the camera list.

⛉**Note**

This function should be supported by the connected device (NVR or HDVR).

---

3. **Optional:** Input the license plate number in the field for search.
4. Click 📅 to set the start time and end time for searching the matched license plate pictures.
5. Click **Search** to start searching.

   The search results of the pictures are displayed in list.

6. **Optional:** After searching license plate, you can perform the following operations.

View Details	Click on a picture from the list to view details. You can also click 🔲 to show the large picture, and click 🔳 to restore.
Play Related Videos	Click ▶ to play the picture's related video file in the view window on the bottom right. ⛉**Note** • You can click 🔲 to show the large video, and click 🔳 to restore. • You can click 1x to adjust the play speed of the playback, click ⏸ to play back the video files frame by frame, click 🔇 to enable the audio, double-click the playback window to maximize the window.
Save Pictures to PC	Click **Export Picture** and select the pictures as desired to export to local PC.

20.7 View Behavior Analysis Related Pictures and Videos

When the connected device supports behavior search, you can search the related picture and view the related pictures and video files.

Before You Start

Add the device to the software and properly configure the corresponding settings. See ***Add Device*** for details about adding the device.

Perform this task when you need to view behavior analysis related pictures and videos.

Steps

1. Click **Behavior Analysis** on the control panel to open 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.
5. **Optional:** After searching the behavior, you can perform the following operations.

View Details	Click on a picture from the list to view details. You can also click ⊞ to show the large picture, and click ⊞ to restore.
Play Related Videos	Click ▶ to play the picture's related video file in the view window on the bottom right.

> **⃣Note**
> - You can click ⊞ to show the large video, and click ⊞ to restore.
> - You can click **1x** to adjust the play speed of the playback, click ▐▶ to play back the video files frame by frame, click 🔊 to enable the audio, double-click the playback window to maximize the window.

Save Pictures to PC	Click **Export Picture** and select the pictures as desired to export to local PC.

20.8 Human Body Picture Retrieval

For the DeepinMind device, you can search the captured human body pictures by uploading a picture from local PC . The client can 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. Refer to ***Add Device*** for details about adding the device.

Perform this task when you need to search human body picture by picture.

Steps

> **⃣Note**
> This function should be supported by the connected device.

1. Click **Human Body Retrieval** on the control panel to open the Human Body Retrieval page.
2. Select device(s) in the camera panel.
3. Select a human body you want to search for.
   1) Select **By Picture** as the search mode.
   2) Click **Select Picture** to select a picture for comparison from local PC.

   > **⃣Note**
   > - 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.

   All the human bodies in this picture will be analyzed and displayed.
4. Set the similarity level.

Example

If you set the similarity as 40, the captured pictures have no less than 40% similarity with the uploaded human body picture will list.

5. Set the maximum number of displayed results.

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 of the pictures are displayed in list.
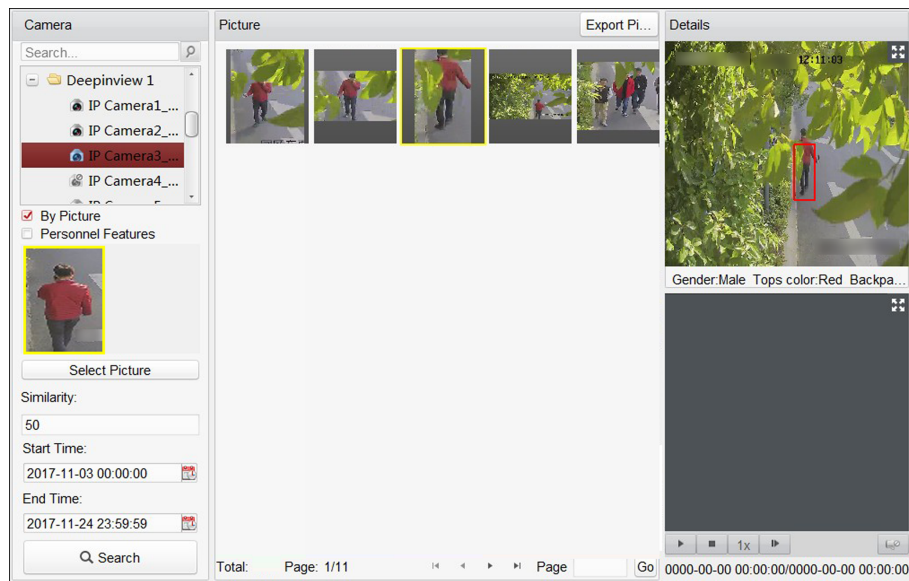
Figure 20-6 Search Result

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. **Optional:** After searching human body, you can do one or more the following operations.

View Details	Click on a picture from the list to view details. You can also click ⊞ to show the large picture, and click ⊞ to restore.
Play Related Videos	Click ▶ to play the picture's related video file in the view window on the bottom right.

- You can click [icon] to show the large video, and click [icon] to restore.
- You can click [icon] to adjust the play speed of the playback, click [icon] to play back the video files frame by frame, click [icon] to enable the audio, double-click the playback window to maximize the window.

Save Pictures to PC   Click **Export Picture** and select the pictures as desired to export to local PC.

20.9 Vehicle Retrieval

For the DeepinMind device, you can search the device's captured vehicle pictures by setting the search conditions, such as plate number, captured time, etc.

Before You Start
Add the device to the software and properly configure the corresponding settings. See *Add Device* for details about adding the device.

Perform this task when you need to search the vehicle.

Steps

---

[i] **Note**

This function should be supported by the connected device.

---

1. Click **Vehicle Retrieval** on the control panel to open Vehicle Retrieval page.
2. Select device(s) in the camera panel.
3. Enter the keyboard of license plate number for search.
4. Set the maximum number of displayed results.
5. Click [icon] to set the start time and end time for searching the captured vehicle pictures or video files.
6. Click **Search** to start searching.
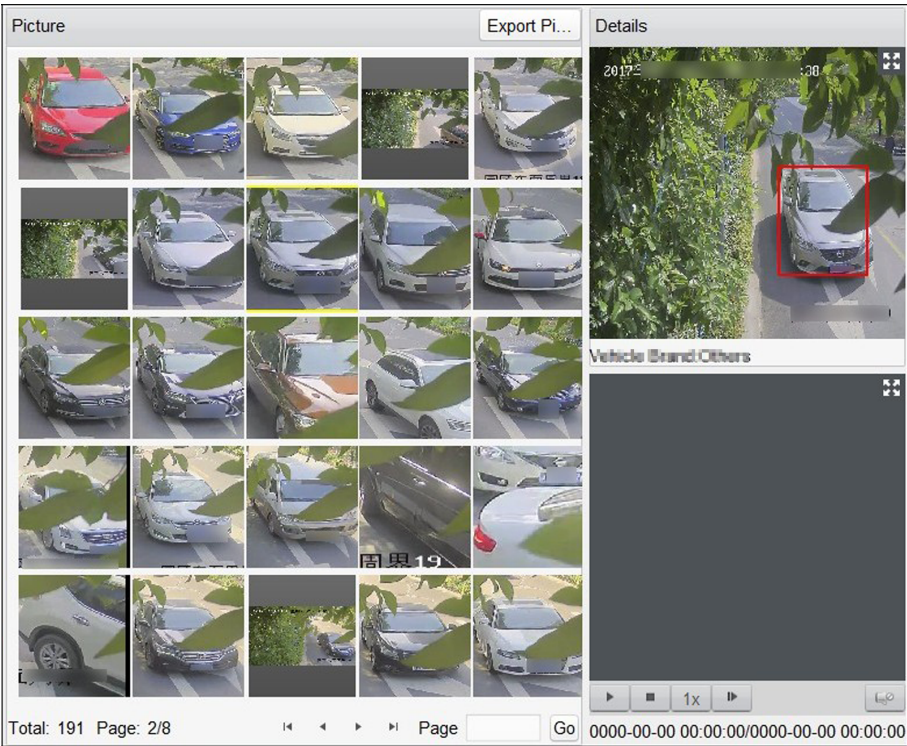
Figure 20-7 Results

The search results of the pictures are displayed in list.

7. **Optional:** After searching vehicle, you can perform the following operations.

View Details	Click on a picture from the list to view details. You can also click ⊞ to show the large picture, and click ⊞ to restore.
Play Related Videos	Click ▶ to play the picture's related video file in the view window on the bottom right.

ℹ️**Note**

- You can click ⊞ to show the large video, and click ⊞ to restore.
- You can click 1x to adjust the play speed of the playback, click ▮▶ to play back the video files frame by frame, click 🔊 to enable the audio, double-click the playback window to maximize the window.

Save Pictures to PC	Click **Export Picture** and select the pictures as desired to export to local PC.

20.10 Queue Management

Queue management supports data analysis and report output from multiple dimensions.

Commonly Used Data Analysis

- To see queuing-up people number of a certain waiting time level in a queue/region, use queuing-up time analysis, check a target region and set a waiting time level.
- To compare queuing-up people number of a certain waiting time level in multiple queues/ regions, use queuing-up time analysis, check target regions and set a waiting time level.
- To compare queuing-up people number of different waiting time levels in multiple queues/ regions, use queuing-up time analysis, check target regions and set waiting time levels.
- To see the time and duration that a queue stays a certain length in a queue/region, use queue status analysis, check a target region and set a queue length level.
- To compare the time and duration that a queue stays a certain length in multiple queues/ regions, use queue status analysis, check target regions and set a queue length level.
- To compare the time and duration that a queue stays at different length in multiple queues/ regions, use queue status analysis, check target regions and set queue length levels.

20.10.1 Queuing-Up Time Analysis

Queuing-Up Time Analysis calculates people number of different waiting time levels. Regional comparison and multiple waiting time level comparison are supported.

Compare Queuing-up People Amount for Different Regions

You can search the queuing-up people amount for a certain waiting time level, and compare the people amount in different regions. The statistics data can show in daily report, weekly report, or monthly report.

Before You Start
Add the device to the software and properly configure the corresponding settings. See *Add Device* for details about adding the device.

Perform this task to compare the queuing-up people amount in different regions.

Steps

[i]**Note**

This function should be supported by the connected device.

1. Enter Queue Management module.
2. Click **Queuing-up Time Analysis** Tab.
3. Select **Regional Comparison** as the statistics type.
4. Click ⊞ to unfold the region list and select the region(s).
5. Select a waiting time level and enter the seconds for calculating people amount waiting for the specified time period.
6. Select the report type including **Daily Report**, **Weekly Report** and **Monthly Report**.
7. Set the statistic time.

> **Note**
>
> You should select one date for daily report or weekly report, and select the month for monthly report. For example, if you select **Weekly Report** as the report type, you need to select one date and the week statistics from Monday to Sunday will be displayed in the search result.

8. Click **Search** to generate the statistics result.

   The line chart of the calculated people amount in the specified waiting time will show on the result area. The lines with different colors indicate the people from the selected regions.
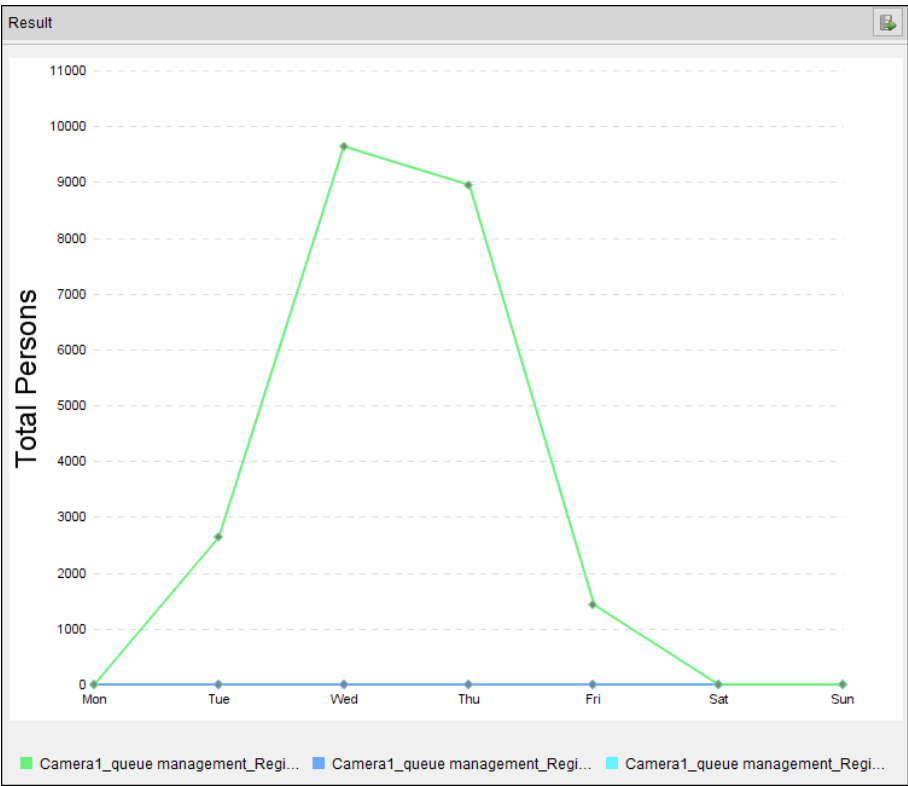
Figure 20-8 Result

9. **Optional:** Click ▣ in the upper-right corner to export the data in Excel file.

Compare Queuing-up People Amount for Different Waiting Time Levels

For a certain region, the queuing-up people amount can be calculated according to the waiting time level (e.g. the waiting time is shorter than the specified seconds.). You can search and compare the people amount for the multiple waiting time levels. The statistics data can show in daily report, weekly report, or monthly report.

Before You Start
Add the device to the software and properly configure the corresponding settings. See **Add Device** for details about adding the device.

Perform this task to compare the queuing-up people amount in different waiting time.

Steps

ⓘ**Note**

This function should be supported by the connected device.

1. Enter Queue Management module.
2. Click **Queuing-up Time Analysis** Tab.
3. Select **Multi-level Comparison** as the statistics type.
4. Click ⊞ to unfold the region list and select the region(s).
5. Select the waiting time level and enter the seconds for calculating people amount waiting for the specified time period.
6. Select the report type including **Daily Report**, **Weekly Report** and **Monthly Report**.
7. Set the statistic time.

ⓘ**Note**

You should select one date for daily report or weekly report, and select the month for monthly report. For example, if you select **Weekly Report** as the report type, you need to select one date and the week statistics from Monday to Sunday will be displayed in the search result.

8. Click **Search** to generate the statistics result.

The line chart of the calculated people amount in the same region will show on the result area. The lines with different colors match the waiting time levels.

Figure 20-9 Result

9. **Optional:** Click ⬇ in the upper-right corner to export the data in Excel file.

20.10.2 Queue Status Analysis

Queue Status Analysis calculates the time and duration that a queue stays a certain length. Regional comparison and multiple queue length level comparison are supported.

Compare Queuing-up Duration for Different Regions

When the queue stays at a certain length, you can search and compare the durations in different regions. The statistics data can show in daily report, weekly report or monthly report.

Before You Start

Add the device to the software and properly configure the corresponding settings. See ***Add Device*** for details about adding the device.

Perform this task to compare the queuing-up duration in different regions.

Steps

ⓘ**Note**

This function should be supported by the connected device.

1. Enter Queue Management module.
2. Click **Queue Status Analysis** Tab.
3. Select **Regional Comparison** as the statistics type.
4. Click ⊞ to unfold the region list and select the region(s).
5. Select a queue length level and enter the value for calculating duration when the queue stays at the length.
6. Select the report type including **Daily Report**, **Weekly Report** and **Monthly Report**.
7. Set the statistic time.

ⓘ**Note**

You should select one date for daily report or weekly report, and select the month for monthly report. For example, if you select **Weekly Report** as the report type, you need to select one date and the week statistics from Monday to Sunday will be displayed in the search result.

8. Click **Search** to generate the statistics result.

The line chart of the calculated duration for staying the specified queue length will show on the result area. The lines with different colors match the selected regions.
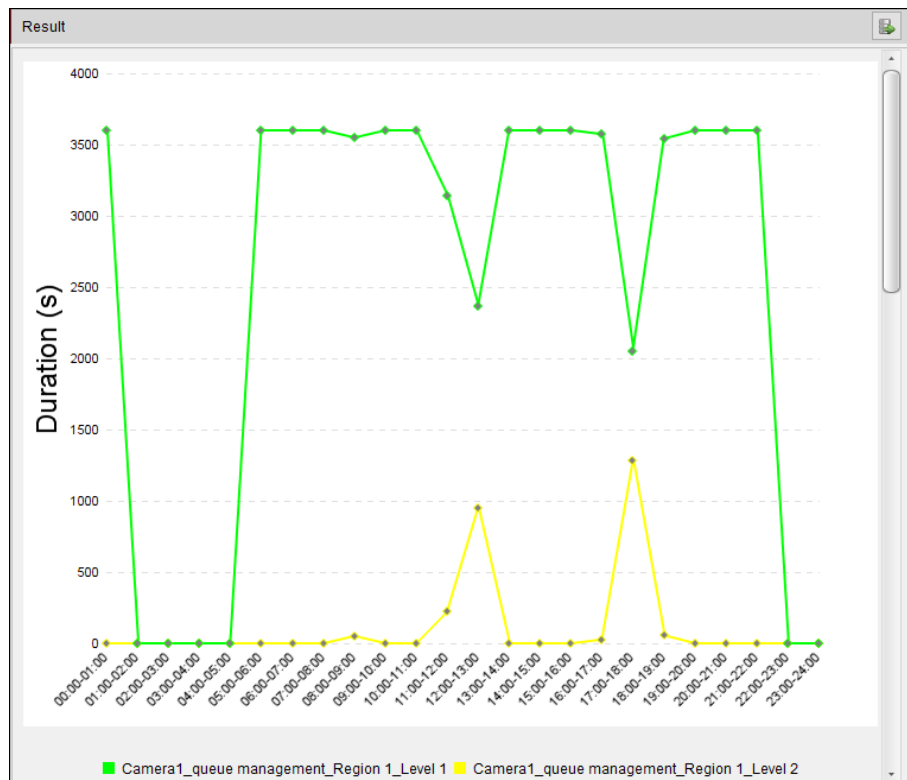
Figure 20-10 Result

9. Optional: Click 🔳 in the upper-right corner to export the data in Excel file.

Compare Queuing-up Duration for Different Queue Length Levels

For the queue in a certain region, you can search the duration when a queue stays a certain length and compare the durations for different queue length levels. The statistics data can show in daily report, weekly report, or monthly report.

Before You Start

Add the device to the software and properly configure the corresponding settings. See **Add Device** for details about adding the device.

Perform this task to compare the queuing-up duration for different queue length.

Steps

---

 i Note

This function should be supported by the connected device.

---

1. Enter Queue Management module.
2. Click **Queue Status Analysis** Tab.
3. Select **Multi-level Comparison** as the statistics type.
4. Click to unfold the region list and select the region(s).
5. Select the queue length level and enter the value for calculating duration when the queue stays at the length.
6. Select the report type including **Daily Report**, **Weekly Report** and **Monthly Report**.
7. Set the statistic time.

---

 i Note

You should select one date for daily report or weekly report, and select the month for monthly report. For example, if you select **Weekly Report** as the report type, you need to select one date and the week statistics from Monday to Sunday will be displayed in the search result.

---

8. Click **Search** to generate the statistics result.

The line chart of the calculated duration in the same region will show on the result area. The lines with different colors match the queue length levels.
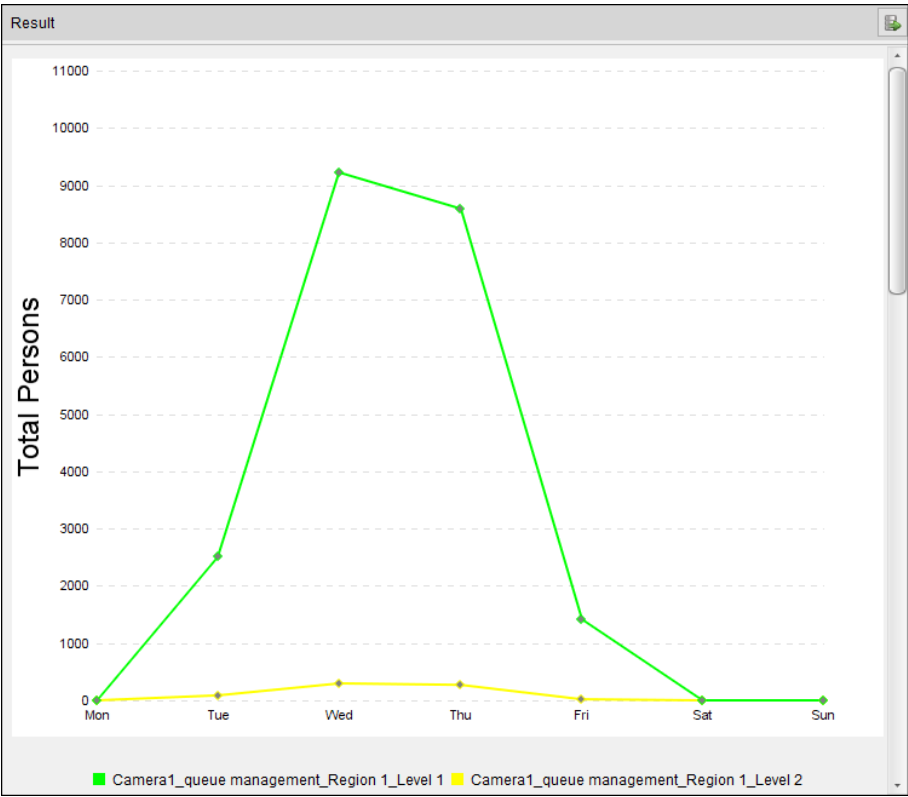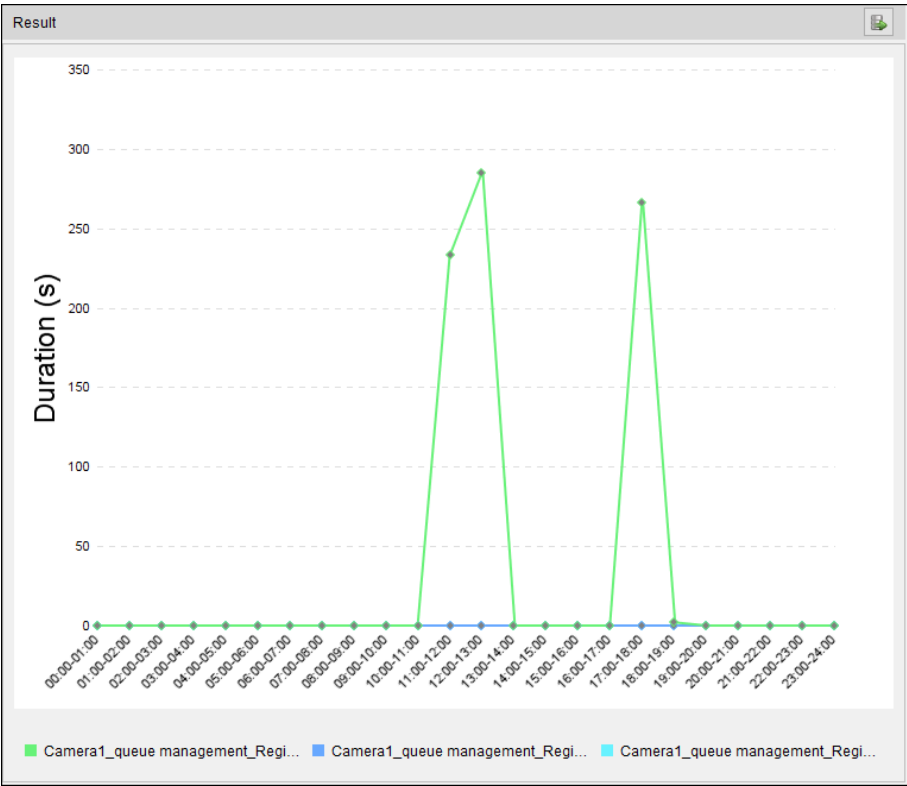
Figure 20-11 Result

9. **Optional:** Click ![icon] in the upper-right corner to export the data in Excel file.

20.11 Face Recognition Check-in

You can search for the attendance record of the persons added in face picture library during the specified period and export the data to the local PC.

Before You Start
Add the device to the software and properly configure the corresponding settings. See **Add Device** for details about adding the device.
Perform this task to search for the attendance record.

Steps

![i]**Note**

This function should be supported by the connected device.

---

1. Enter Face Recognition Check-in module.
2. Click ![icon] to unfold the camera list and select the camera(s).

⌐！¬**Note**

You can only select the cameras belongs to one device.

3. Check one or multiple face picture libraries to search the persons attendance in the selected library.
4. Set the date and time range for check-ins.
5. Enter the maximum number of the result to show.
6. Click **Search** to start searching.

   The searched result shows the attendance record including the face picture, face library, name, and check-in counts.

Figure 20-12 Result

7. **Optional:** Click **Export All** in the upper right corner to export the data to local PC.

Chapter 21 Log Management

In the Log Management module, you can search the log files (client logs and remote logs) and filter the results, back up log files, and export alarm pictures.

21.1 Search Logs

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.

21.1.1 Search Client Logs

You can search the log files of the client, or the logs of the remote devices.

Perform the following steps to search the log files of the client.

Steps
1. Open the Log Search page.
2. Select **Client Logs** as the to-be-searched log type.
3. Click 📅 to specify the start time and end time.

   ⃞ℹ️Note

   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.
5. **Optional:** Narrow the time range or filter the log type for search if there are too many log files.

   ⃞ℹ️Note

   See **Filter Logs** for detailed information about filtering logs.

21.1.2 Search Connected Device Logs

You can search the remote logs, namely, the log files of the connected device.

Perform the following steps to search the log files of the connected device.

Steps
1. Open the Log Search page.
2. Select **Remote Logs** as the to-be-searched log type.

3. Click 🗓 to specify the start time and end time.

> **ℹ 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.

> **ℹ Note**
> Narrow the time range or filter the log type for search if there are too many log files.

21.2 Filter Logs

After being searched out successfully, the log files can be filtered by the keyword or condition, and thus you can find the logs as you want.

Before You Start
Search logs. See *Search Client Logs* and *Search Connected Device Logs* for details.

Perform the following steps to filter logs.

Steps
1. Click **Log Search** on the control panel to enter the Log Search page.
2. Click **Log Filter** or ▼ on the Log Search page to expand the Log Filter panel.
3. Select filtering mode.
   - 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.
4. **Optional:** Click **More...** to filter the log files more accurately.
5. Click **Filter** to start filtering.

21.3 Back Up Logs

The log files, including the client logs and server logs, can be exported for backup.

Perform this task if you need to back up logs.

Steps
1. Click **Log Search** on the control panel to open the Log Search page.
2. Set the condition and search the log file.
3. Click **Backup Log** to open the Backup Log window.
4. Click ⋯ and select a local saving path and set a name for the file.
5. Click **Backup** to export the selected log file for backup.
6. **Optional:** After backup the log file, you can perform the following operation.

Check Backup Log Files Information	Click **File → Open Log File** on the menu bar to check the information of the backup log files on local PC.

21.4 Export Pictures

The alarm pictures, which are stored in the storage server, can be exported to the local PC.

Before You Start
Add storage device to the client for storing the video files and pictures of the added encoding devices, see *Store Picture and Video on Storage Device*

Perform the following steps to export pictures.

Steps
1. Click **Log Search** on the control panel to open the Log Search page.
2. Search client logs.

   > **Note**
   > See *Search Client Logs* for details.

3. Select **Alarm Log** as the log type when filtering the results.

   > **Note**
   > See *Filter Logs* for details.

4. Select the alarm pictures.
5. Click **Export Picture** to open the Export Picture window.
6. Click ⊡ and select a local saving path, and then set a name for the file.
7. Click **Export** to export the selected pictures.

Chapter 22 Account Management

Multiple user accounts can be added to the client software, and you are allowed to assign different permissions to different users if needed.

Perform this task to add an user account.

Steps

🛈**Note**

The user account you registered to log in the software is set as the super user.

1. Enter the Account Management page.
2. Click **Add User** to open the Add User window.
3. Select the user type from the drop-down list.

    Administrator

    The administrator account has all permissions by default, and can modify the passwords and permissions of all operators and its own.

    Operator

    The operator account has no permission by default and you can assign the permissions manually. An operator can only change the password of its own account.

4. Input the user name, password, and confirm password as desired.

    ⚠️**Caution**

    The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: 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.

5. Check the checkboxes to assign the permissions to the created user.
6. **Optional:** Select a user in the Copy from drop-down list to copy the permissions of the selected user.
7. **Optional:** Click **Default Permission** to restore the default permissions of this user.
8. Click **Save**.

    🛈**Note**

    Up to 50 user accounts can be added for the client software.

After created user account successfully, the user account is added to the user list on the Account Management page.

9. **Optional:** Perform the following operations after the user account is created.

Edit User	Select a user from the list and click **Edit User** to edit the user information.
	🅸**Note** Only the password of the super user can be edited.
Delete User	Select the user from the list and click **Delete User**.
	🅸**Note** You cannot delete the super user.
Copy to	For super and administrator user, you can click **Copy to** to copy the permissions to other user(s).

Chapter 23 System Configuration

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, video intercom parameters, access control settings, and security certificate can be configured.

23.1 Set General Parameters

You can configure the frequently-used parameters, including log expired time, network performance, and etc.

Perform the following task when you need to set the above mentioned parameters.

Steps
1. Open the System Configuration page.
2. Click **General** tab to enter the General Settings page.
3. Configure the general parameters.

   Log Expiry Date

   The time for keeping the log files. Once exceeded, the files will be deleted.

   Network Performance

   Set the network conditions to **Normal**, **Better** or **Best**.

   Maximum Mode

   Select **Maximize** or **Full Screen** as the maximum mode. **Maximize** mode can maximize the display and show the taskbar. **Full Screen** mode can display the client in full-screen mode.

   Enable Auto-login

   Log into the client software automatically.

   Pop up Security Prompt When Using Default Password

   If the default password of the added device has not been changed, the prompt will pop up for notification.

   Enable Alarm Triggered Pop-up Image

   Enable the image pop-up when alarms occur. You can also click or to enable/disable the image pop-up in Alarm Event interface.

   Pop Up Alarm Image for Minimized Client When Alarm Triggered Pop-up Image Enabled

   Enable the alarm image popping up when the client is minimized if the Alarm Triggered Pop-up Image function is enabled.

Note

For enabling the Alarm Triggered Pop-up Image, refer to **_Alarm Configuration_** .

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

Enable the keyboard or joystick. After enabled, you can set the shortcuts for the keyboard and joystick.

Note

For details, refer to **_Set Keyboard and Joystick Shortcuts_** .

Registration Management Server Port

EHome port for registration management server. The port number should be between 2000 to 65535. The default port number is 7660.

Note

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.

4. Click **Save**.

23.2 Set Live View and Playback Parameters

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

Perform the following task when you need to set the parameters for live view and playback.

Steps
1. Open the System Configuration page.
2. Click **Live View and Playback** tab.
3. Configure the live view and playback parameters.

   Merge Downloaded Video Files

   Set the maximum size of merged video file for downloading the video file by date.

   Search Video Files Stored in

   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

   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

   Skip the unconcerned video during VCA playback and the unconcerned video will not be played during VCA playback.
4. Click **Save**.

23.3 Set Image Parameters

The image parameters of the client can be configured, such as view scale, play performance, etc.

Perform the following task when you need to set image parameters.

Steps
1. Open the System Configuration page.
2. Click **Image** tab to enter the Image Settings interface.

3. Configure the image parameters.

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**.

ⓘ**Note**

You can also set the view scale in Live View module. For details, refer to *Live View* .

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 size of the display window.

ⓘ**Note**

When the window division is larger than 9, it will switch to sub-stream automatically.

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 on the live view image.

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 and fire source information on the captured pictures.

ⓘ**Note**

After enabled this function, the Picture Format in **System Configuration → Live View and Playback** will change to JPEG and is not editable.

4. Click **Save**.

23.4 Set File Saving Path

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.

Perform the following task when you need to set the file saving path.

Steps
1. Open the System Configuration page.
2. Click **File** tab to enter the File Saving Path Settings page.
3. Click ⋯ and select a local path for the files.
4. Click **Save**.

23.5 Set Icons Shown on Toolbar

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.

Perform the following task when you need to set icons shown on Toolbar.

Steps
1. Open the System Configuration page.
2. Click **Toolbar** tab to enter the Toolbar Settings page.
3. Select the icon to display on the toolbar.
4. **Optional:** Drag the icon to set the icon order when displaying on the toolbar.

Table 23-1 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.

Table 23-2 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.

5. Click **Save**.

23.6 Set Keyboard and Joystick Shortcuts

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.

Perform this task when you need to set keyboard and joystick shortcuts.

Steps

Note

This configuration page will display after enabling keyboard and joystick in General Settings. For details, refer to *Set General Parameters* .

1. Open the System Configuration page.
2. Click **Keyboard and Joystick** tab to enter the Keyboard and Joystick Shortcut Settings page.
3. Select the COM port from the drop-down list for keyboard if the keyboard is connected to the PC installed with the client.
4. Set shortcuts 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.
5. Click **Save**.

23.7 Set Alarm Sound

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.

Perform the following task when you need to set the alarm sound.

Steps

1. Open the System Configuration page.
2. Click **Alarm Sound** tab to enter the Alarm Sound Settings page.
3. **Optional:** Click ⋯ and select the audio files from the local path for different alarms.

> 📖ⁱNote
>
> There are six pre-defined alarm sound type in the list.

4. **Optional:** Add customized alarm sound.
   1) Click **Add** to add customized alarm sound.
   2) Double click the **Type** field to customize the alarm sound name as desired.
   3) Click ⋯ and select the audio files from the local path for different alarms.
5. **Optional:** Click 🔊 for a testing of the audio file.
6. **Optional:** Select the added custom alarm sound and click **Delete** to delete it.
7. Click **Save**.

> 📖ⁱNote
>
> The format of the audio file can only be WAV.

23.8 Set Email Parameters

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.

Perform the following task when you need to set email parameters.

Steps

1. Open the System Configuration page.
2. Click **Email** tab to enter the Email Settings interface.
3. Input the required information.

   Server Authentication (Optional)

   If your email server requires authentication, check this checkbox to use authentication to log into the server and enter the login user name and password of your email account.

   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.

Receiver 1 to 3

Input the email address of the receiver. Up to 3 receivers can be set.

4. **Optional:** Check **Enable SSL** to increase the security of email sending.
5. **Optional:** Click **Send Test Email** to send an email to the receiver for test.
6. Click **Save**.

23.9 Set Video Intercom Parameters

You can configure the video intercom parameters according to actual needs.

Perform the following task when you need to set video intercom parameters.

Steps
1. Open the System Configuration page.
2. Click the **Video Intercom** tab to enter the Video Intercom Settings page.
3. Input the required information.

Ringtone

Click ⋯ and select the audio file from the local path for the ringtone of indoor station. Optionally, you can click 📢 for a testing of the audio file.

4. Click **Save**.

23.10 Set Access Control Parameters

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.

Perform the following steps to set the access control parameters.

Steps
1. Open the System Configuration page.
2. Click **Access Control** tab to enter the Access Control Settings interface.
3. Check **Auto-synchronize Access Control Event** to enable this function and set the time for synchronization.
4. Click **Save**.

23.11 Manage Security Certificate

For the data security purpose, the security certificate of clients and added servers (stream media server) should be same.

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.

23.11.1 Export Certificate from Client

You can export the security certificate from the current client and import the exported certificate file to the server or other clients.

Perform the following steps to export the security certificate from the client.

Steps
1. Open the System Configuration page.
2. Click **Security Certificate** tab to enter the security certificate interface.
3. Save the certificate file in the local PC.

> ⓘ**Note**
> The certificate file is in XML format.

4. Click **Save**.

> ⓘ**Note**
> - 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, refer to *Import Certificate to Stream Media Server* .

23.11.2 Import Certificate to Client

If there are multiple clients accessing the same server, you should import the same certificate to the clients and server.

Before You Start
You should export the security certificate from one of the client.

> ⓘ**Note**
> For details, refer to *Export Certificate from Client* .

Perform the following steps to import the security certificate to the client.

Steps
1. Copy the certificate file exported from other client to the local PC.
2. Open the System Configuration page.
3. Click **Security Certificate** tab to enter the security certificate interface.
4. Click **Import**.
5. Select the certificate file from your local PC.
6. Click **Save**.

> ⓘ**Note**
> Please restart the system to take effect.

Appendix A. 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

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.

Appendix B. Troubleshooting

Here are some common symptoms when operating the client software. We provide the possible causes and corresponding solutions to solve the problems.

B.1 Failed to get the live view of a certain device.

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.

B.2 Local recording and remote recording are confused.

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.

B.3 Failed to download the video files or the downloading speed is too slow.

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 required 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.

Appendix C. FAQ (Frequently Asked Questions)

Here are some frequently asked questions when operating the client software. We provide the corresponding answers to help the users to solve the problems.

C.1 During live view, why an error message with error code 91 prompts ?

Question

During live view, why an error message with error code 91 prompts ?

Answer

For live view of multiple windows, the channel may not support sub stream. You should disable the function of **Auto-change Stream Type** in **System Configuration → Image** , and select the appropriate steam type for live view.

C.2 During live view, why the image is blurred or not fluent?

Question

During live view, why the image is blurred or not fluent?

Answer

Check the driver of video card. We highly recommend you update the driver of video card to the latest version.

C.3 Why the memory leaked and the client crashed after running for a while?

Question

Why the memory leak and the client crashed after running for a while?

Answer

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.

C.4 During live view, when getting stream via the Stream Media Server, why an error message with error code 17 prompts?

Question

During live view, when getting stream via the Stream Media Server, why an error message with error code 17 prompts?

Answer

Check the port mapping of Stream Media Server, especially RTSP port.

Appendix D. Error Code

Code	Error Name	Description
Guarding Vision		
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	Not supported.	
29	Operation 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		

Code	Error Name	Description
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.

UD11065N