



# **Behavior Analysis Server**

**User Manual**

## Legal Information

©2020 Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

### 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 of this Manual at the Hikvision website ( <https://www.hikvision.com/> ).

Please use this Manual with the guidance and assistance of professionals trained in supporting the Product.

### Trademarks

**HIKVISION** and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.

Other trademarks and logos mentioned are the properties of their respective owners.

### Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS MANUAL AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED “AS IS” AND “WITH ALL FAULTS AND ERRORS”. HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION 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, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

YOU ACKNOWLEDGE THAT THE NATURE OF INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INSPECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE

DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.

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

## Regulatory Information

### FCC Information

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

FCC compliance: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

### FCC Conditions

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

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

### EU Conformity Statement



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



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



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

designated collection point. For more information see: <http://www.recyclethis.info> .

### **Industry Canada ICES-003 Compliance**

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




## Preface

### Applicable Model

This manual is applicable to DeepinMind Training Server.

### Symbol Conventions

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

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

### Safety Instruction

- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.
- In the use of the product, you must be in strict compliance with the electrical safety regulations of the nation and region. Please refer to technical specifications for detailed information.
- Input voltage should meet both the SELV (Safety Extra Low Voltage) and the Limited Power Source with 100~240 VAC according to the IEC60950-1 standard. Please refer to technical specifications for detailed information.
- Do not connect several devices to one power adapter as adapter overload may cause overheating or a fire hazard.
- Please make sure that the plug is firmly connected to the power socket.
- If smoke, odor or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.

# Contents

<b>Chapter 1 Introduction .....</b>	<b>1</b>
<b>Chapter 2 Activation and Login .....</b>	<b>3</b>
2.1 PC Requirements .....	3
2.2 Activation .....	3
2.2.1 Activate via SADP Software .....	3
2.2.2 Activate via Web Browser .....	5
2.3 Login .....	5
<b>Chapter 3 Configuration Wizard .....</b>	<b>7</b>
3.1 Create Analysis Cluster .....	7
3.1.1 Add Smart Analysis Unit .....	7
3.1.2 Create Stand-alone Analysis Cluster .....	8
3.2 Add Camera and Video .....	9
3.2.1 Add Camera .....	9
3.2.2 Add Video Recording .....	11
3.3 Perimeter Analysis Task .....	12
3.3.1 Create Perimeter Analysis Task .....	12
3.3.2 Line Crossing Detection .....	13
3.3.3 Region Entrance Detection .....	15
3.3.4 Region Exiting Detection .....	17
3.3.5 Intrusion Detection .....	19
3.3.6 Loitering Detection .....	21
3.3.7 Parking Detection .....	23
3.3.8 Unattended Baggage Detection .....	25
3.3.9 Object Removal Detection .....	27
3.4 Indoor Analysis Task .....	29
3.4.1 Create Trend Analysis Task .....	29

3.4.2 Getting-up Detection .....	30
3.4.3 Climbing Detection .....	33
3.4.4 Absence/Sleep on Duty Detection .....	34
3.4.5 Sudden Change of Sound Intensity Detection .....	37
3.4.6 Abnormal Number of People Detection .....	39
3.4.7 Standing-up Detection .....	42
3.4.8 Sitting Detection .....	44
3.4.9 Playing Mobile Phone Detection .....	46
3.4.10 People Entrance(Non Police) Detection .....	48
3.4.11 Police Absence Detection .....	50
3.4.12 Falling-down Detection .....	52
3.4.13 Physical Conflict Detection (Indoor) .....	54
3.4.14 Overstaying Detection .....	57
3.5 Trend Analysis Task .....	60
3.5.1 Create Trend Analysis Task .....	60
3.5.2 People Density Analysis .....	61
3.5.3 Real-time People Counting .....	63
3.5.4 People Counting .....	65
3.6 Street Analysis Task .....	67
3.6.1 Create Street Analysis Task .....	67
3.6.2 Falling-down Detection .....	68
3.6.3 Fast Moving Detection .....	70
3.6.4 Physical Conflict Detection (Street) .....	72
3.6.5 People Gathering Detection .....	74
3.7 Task Management .....	76
3.7.1 Configure Task .....	76
3.7.2 Delete Task .....	78
3.7.3 Pause Task .....	78

3.7.4 Start Task .....	78
<b>Chapter 4 Smart Analysis Unit Management .....</b>	<b>79</b>
4.1 Add Smart Analysis Unit to Cluster .....	79
4.2 Remove Computing Node from Cluster .....	79
4.3 Restart Smart Analysis Unit .....	79
4.4 Power Off Smart Analysis Unit .....	80
4.5 Delete Smart Analysis Unit .....	80
4.6 Configure Network Parameters .....	80
4.7 Enable UID Indicator .....	81
4.8 View Hardware Resource .....	81
<b>Chapter 5 System Management .....</b>	<b>83</b>
5.1 Basic Configuration .....	83
5.2 Service Configuration .....	83
5.3 Time Configuration .....	83
5.4 User Management .....	84
5.4.1 Add User .....	84
5.4.2 Modify Password .....	85
5.4.3 Delete User .....	85
5.5 Log Management .....	86
5.5.1 Search Log .....	86
5.5.2 Download Maintenance Log .....	86
5.6 Smart Mode .....	87
5.7 Software Updating .....	87
5.8 Restore Defaults .....	88
5.9 Help Center .....	88
5.10 Version Information .....	88
5.11 Logout .....	88
5.12 Obtain Guarding Vision Client Software .....	89

<b>Chapter 6 Guarding Vision Client Configuration .....</b>	<b>90</b>
6.1 Log in .....	90
6.2 Add Server .....	91
6.2.1 Add Server Manually .....	91
6.2.2 Add Online Server .....	92
6.3 Live View .....	93
6.3.1 View Analysis Task Frame .....	93
6.3.2 View Task Analysis Results(Trend Scene Only) .....	95
6.4 Remote Configuration .....	96
6.5 Alarm Center .....	99
6.5.1 Search Real-time Event .....	99
6.5.2 Search Event .....	101
6.6 Data Retrieval .....	102
6.7 Data Statistics .....	104

## Chapter 1 Introduction

Based on the latest deep-learning algorithms, Behavior Analysis Server adopts the high-density GPU structure, and supports detection towards different behavior events in different scenes, including perimeter scene, trend scene, indoor scene and street scene.

### Perimeter

- Line Crossing: An alarm will be triggered when a person crosses the warning line.
- Region Entrance: An alarm will be triggered when a person enters the detection area.
- Region Exiting: An alarm will be triggered when a person exits the detection area.
- Intrusion: An alarm will be triggered when the stay duration of a person in the detection area exceeds the time set.
- Loitering: An alarm will be triggered when the loitering time of a person in the detection area exceeds the time set.
- Parking: An alarm will be triggered when the parking time of a vehicle in the detection area exceeds the time set.
- Object Removal: An alarm will be triggered when the removal time of an object in the detection area exceeds the time set.
- Unattended Object: An alarm will be triggered when the unattended time of an object left in the detection area exceeds the time set.

### Indoor

- Getting-up: An alarm will be triggered when a person in the detection area gets up.
- Climbing: An alarm will be triggered when a person climbs over the height set.
- Absence/Sleep on Duty: An alarm will be triggered when the time of a person on duty stays motionless or in absence exceeds the time set.
- Sudden Change of Sound Intensity: An alarm will be triggered when the sound intensity in the detection area is abnormal.
- Abnormal Number of People: An alarm will be triggered when the number of people in the detection area does not match the value set.
- Standing-up: An alarm will be triggered when a person in the detection area stands up.
- Sitting: An alarm will be triggered when the sedentary time of a person exceeds the time set.
- Playing Mobile Phone: An alarm will be triggered when the time of a person in the detection area playing mobile phone exceeds the time set.
- People Entrance (Non Police): An alarm will be triggered when the staying duration of non-police personnel exceeds the time set.
- Police Absence: An alarm will be triggered when the absence time of the police in the detection area exceeds the time set.

- Falling-down: An alarm will be triggered when a person in the detection area falls down and does not stand up in the time set.
- Physical Conflict (Indoor): An alarm will be triggered when the physical conflict time of two or more people exceeds the time set.

### **Trend**

- People Density Analysis: Count the number of people in the detection area, and generate a people heat map.
- Real-time People Counting: Count the number of people within the same duration of stay during different time periods in the detection area, and upload the data according to the time interval set.
- People Counting: Count the number of people crossing the detection lines, and upload the data according to the time interval set.

### **Street**

- Falling-down: An alarm will be triggered when a person in the detection area falls down suddenly.
- Fast Moving: An alarm will be triggered when the time a person in the detection area moves fast exceeds the time set.
- Physical Conflict (Street): An alarm will be triggered when the time of probable physical conflict between people in the detection area exceeds the time set.
- People Gathering: An alarm will be triggered when the number of people in the detection area and the time people gather exceeds the threshold level.

## Chapter 2 Activation and Login

### 2.1 PC Requirements

You can get access to the server by IE browser. The requirements for your PC are shown as below.

**Table 2-1 PC Requirements**

Operating System	CPU	Memory	Resolution	Browser
Microsoft Windows 7, Microsoft Windows 10	Intel® Pentium IV 3.0 GHz or more advanced version	1 GB or larger	1024 × 768 or higher	IE8 to IE11



The interface varies from version to version.

---

### 2.2 Activation

The server is available only after being activated.

#### 2.2.1 Activate via SADP Software

##### Before You Start

- You have obtained SADP Software from the official website.
- The PC and server have been connected with each other on the same network segment.

##### Steps

1. Install and run the SADP software. The software searches all online devices within the local area network. Device type, IP address, activation status, device serial number and other information are shown in the list.



Initial Server IP Address: 192.168.1.64.

---

2. Check the desired server and set server password in the **Activate Device** window. Click **Activate**.



Input and confirm password.

 **Note**

- ### 3. Modify server IP address.

- You shall acknowledge that the use of the product with Internet access might be under network security risks. For avoidance of any network attacks and information leakage, strengthen your own protection. We highly recommend you to assess the network security regularly. If the device is under network security risks, contact with your dealer or the nearest service center.
- In order to increase the security of your product, it is necessary to configure all passwords and other security settings properly. Please be mindful of your user name and password.

## 2.2.2 Activate via Web Browser

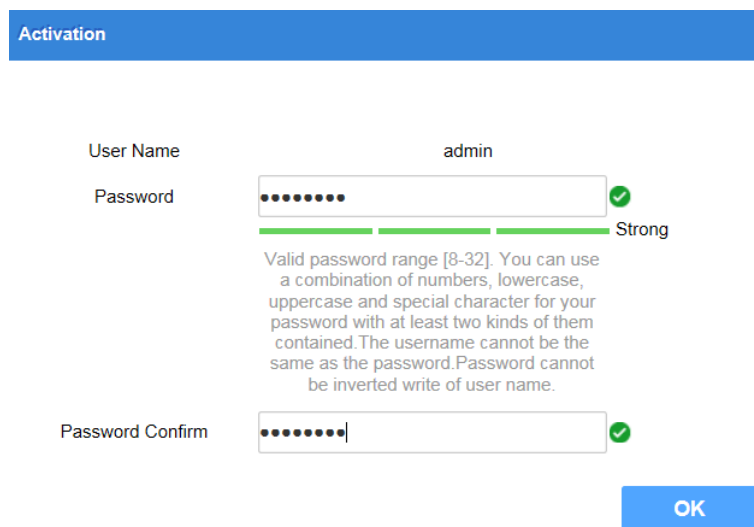
You can activate the server via Web browser.

### Before You Start

- The PC and server have been directly connected.
- You have changed the IP address of the PC and it connected to the server properly.

### Steps

1. Open IE browser. Enter 192.168.1.64 in the address bar and press **Enter**.



The screenshot shows a web browser window titled "Activation". It contains a form with the following fields and elements:

- User Name:** A text input field containing the text "admin".
- Password:** A password input field with masked characters (dots). To its right is a green checkmark icon.
- Password Strength:** A green progress bar below the password field, followed by the text "Strong".
- Password Hint:** A block of text below the password field: "Valid password range [8-32]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained. The username cannot be the same as the password. Password cannot be inverted write of user name."
- Password Confirm:** A password input field with masked characters (dots) and a cursor. To its right is a green checkmark icon.
- OK Button:** A blue button with the text "OK" located at the bottom right of the form.

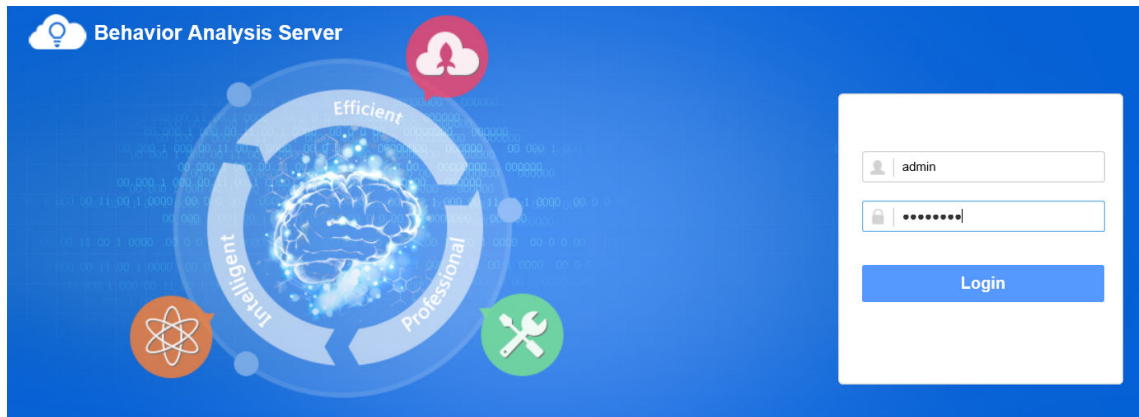
**Figure 2-2 Activation Interface**

2. Enter **Password** and confirm, then Click **OK**.

## 2.3 Login

### Steps

1. Open IE browser. Enter server IP address in the address bar and press **Enter**.



**Figure 2-3 Login Interface**

**2.** Enter user name and password. Click **Login**.

## Chapter 3 Configuration Wizard

### 3.1 Create Analysis Cluster

#### 3.1.1 Add Smart Analysis Unit

Add smart analysis unit(s) to create an analysis cluster.

##### Before You Start

Ensure that the smart analysis unit is online.

##### Steps

1. Go to **Service** → **Smart Unit**.
2. Click **Add**.

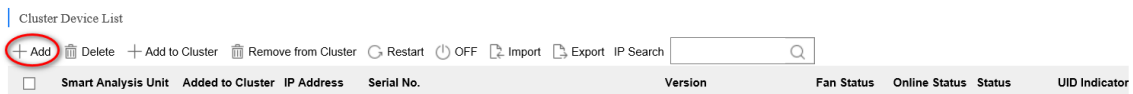


Figure 3-1 Add Smart Analysis Unit

3. Enter **Name** and **Smart Analysis Unit IP**, and keep **Port** as default value.

A screenshot of a dialog box titled 'Smart Analysis Unit' with a close button (X) in the top right corner. The dialog contains three input fields: 'Name', 'Smart Analysis Unit IP', and 'Port'. The 'Port' field has the value '8088' pre-filled. At the bottom right of the dialog are two buttons: 'OK' and 'Cancel'.

Figure 3-2 Configure Parameters

4. Click **OK**.



## Note

The name of each unit can not be duplicated. Letters, digits and special characters are allowed, excluding `[#~%!\$^&@:;""'"/\+\_\*`.

### 3.1.2 Create Stand-alone Analysis Cluster

The stand-alone analysis cluster contains at least one smart analysis unit. There is only one master node in the cluster, and the rest are computing nodes. If the master node is offline, the cluster will not be available.

#### Before You Start

Ensure that smart analysis units are online and on the same subnet.

#### Steps

1. Go to **Service → Smart Unit**.
2. Check the desired smart analysis unit, and click **Create Cluster**.

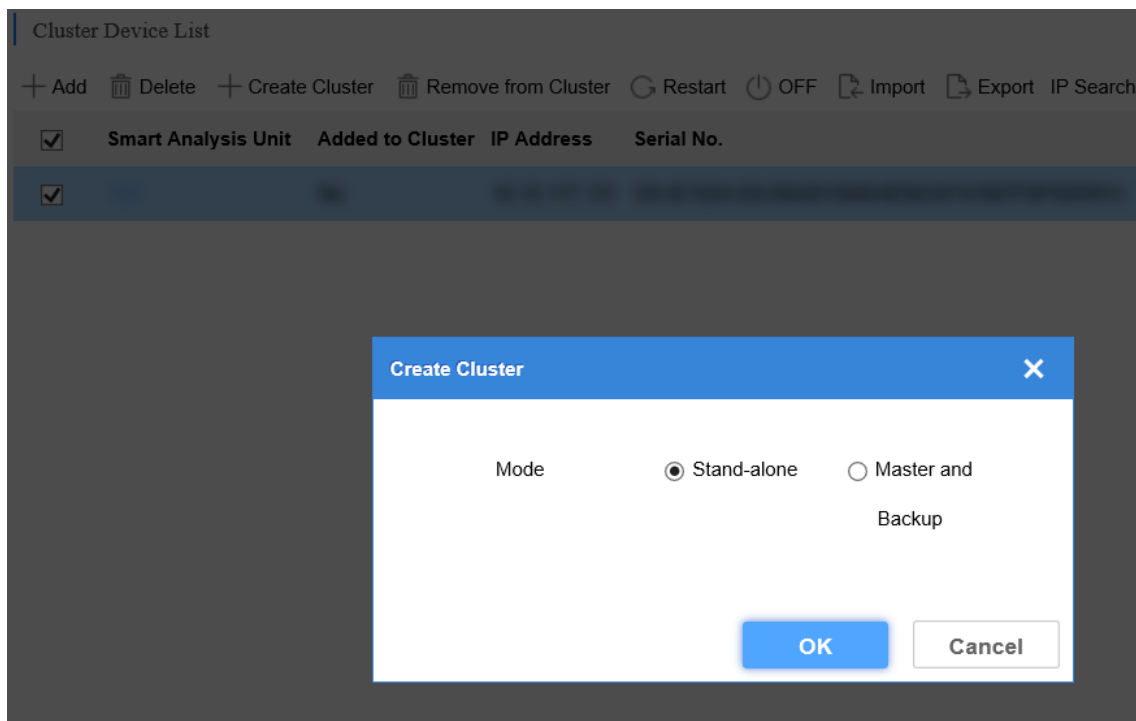


Figure 3-3 Create Stand-Alone Cluster

3. Select **Stand-alone** as **Mode**.
4. Click **OK**.

## 3.2 Add Camera and Video

Add camera and video recording for behavior analysis.

### 3.2.1 Add Camera

Add a camera that needs to be analyzed. Only one camera can be added for each time.

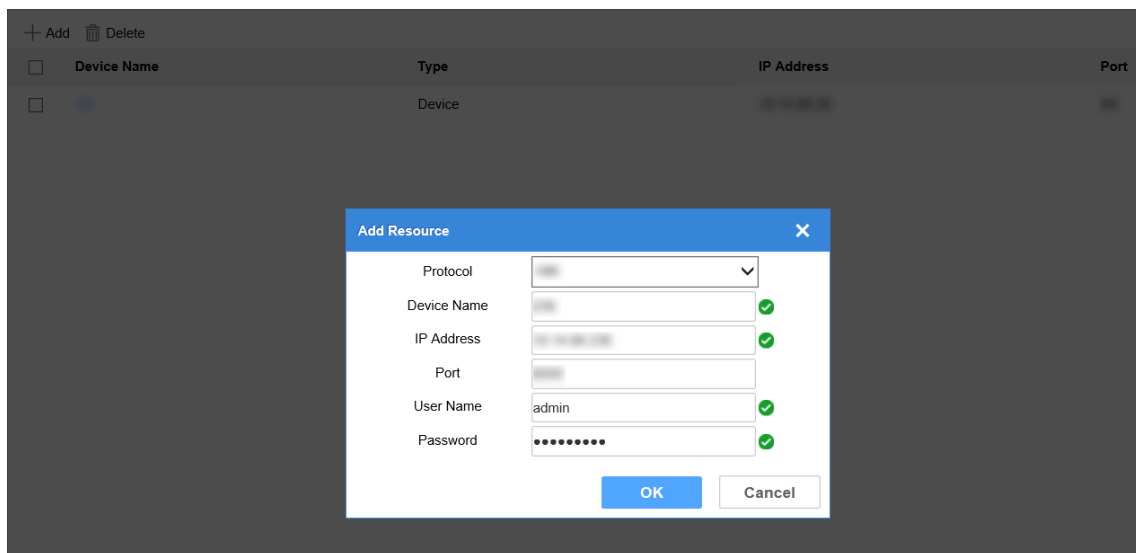
#### Before You Start

You have obtained the IP address, user name and login password of the camera.

- The control center is used to manage all cameras, and the area is a classification of these cameras according to the spatial location or specific requirements. For example, if the **Control Center** is set as **Binjiang District**, then the **Area** can be set as **Jiangnan Avenue**.
- Take adding camera to control center and user as admin as an example.

#### Steps

1. Click **Resource** → **Device**, click **Administrator-admin** and **Add** to enter camera information, and then click **OK**.



**Figure 3-4 Add Camera**

2. Click **Add**, select **Type** as **Area**, enter Name, and then click **OK**.

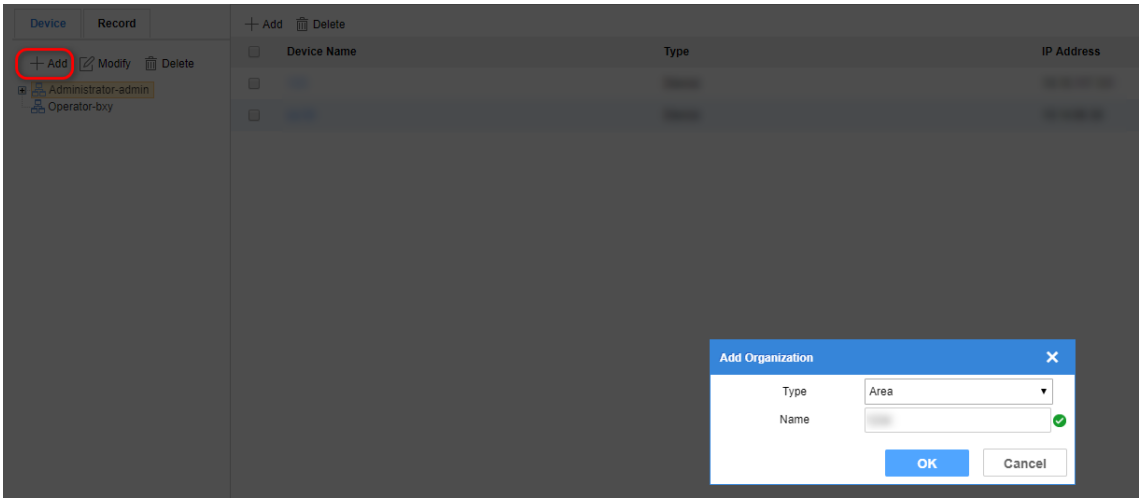


Figure 3-5 Add Area

 **Note**

Up to 32 characters allowed, including number, lowercase and uppercase, and special characters.

3. Select added area, and click **Add**.

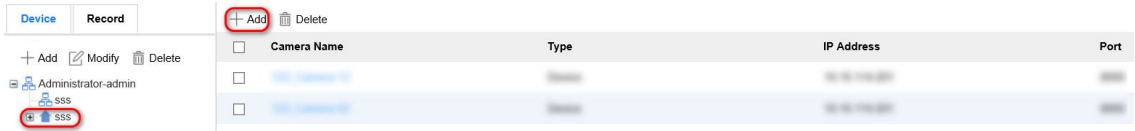


Figure 3-6 Add Camera

 **Note**

The camera can be armed only when it is added to area.

4. Select the desired camera, and click **OK**.

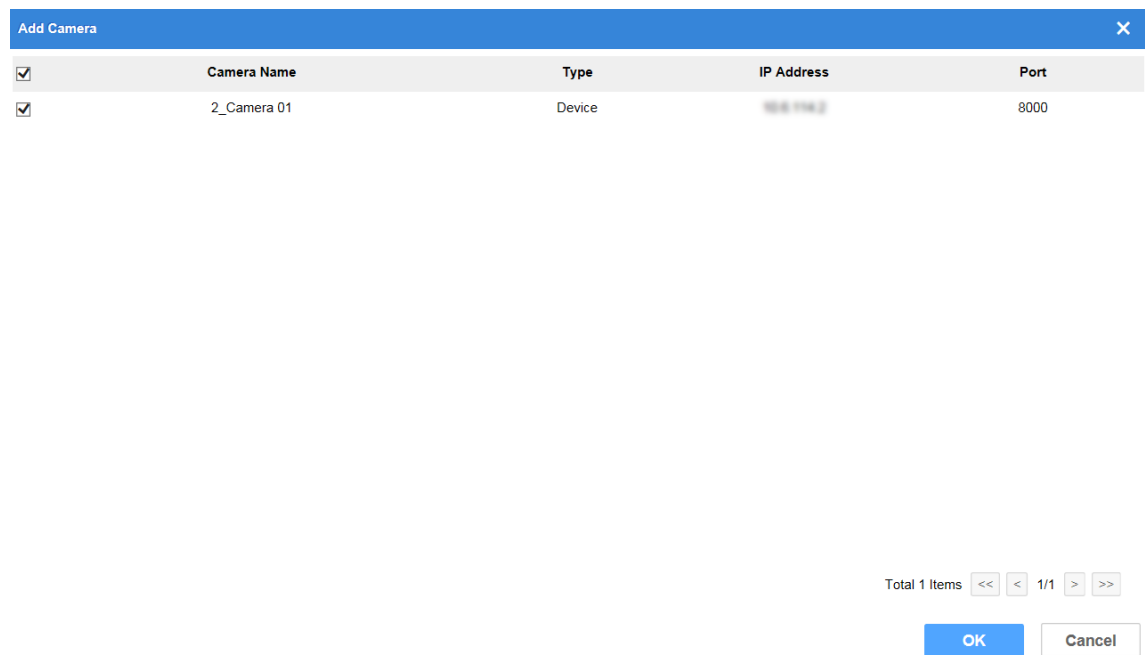


Figure 3-7 Add a Camera to Area

 **Note**

You can add control centers and areas for control center, and cameras for area.

3.2.2 Add Video Recording

Import the desired video. Skip this part if no video exists.

You can import a video recording into default list. Create an area if required.

Steps

1. Click **Resource** → **Record** , click **Administrator-admin** → **Default List** → **Import** .

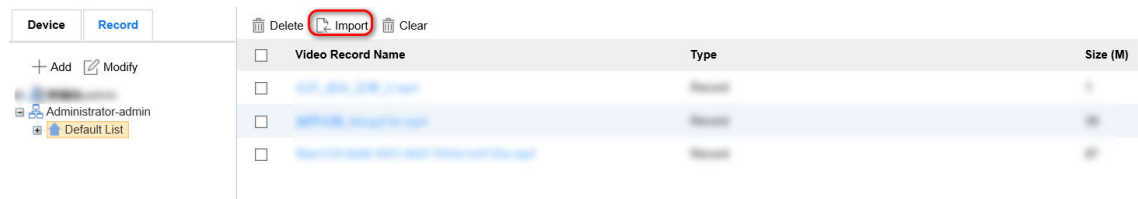
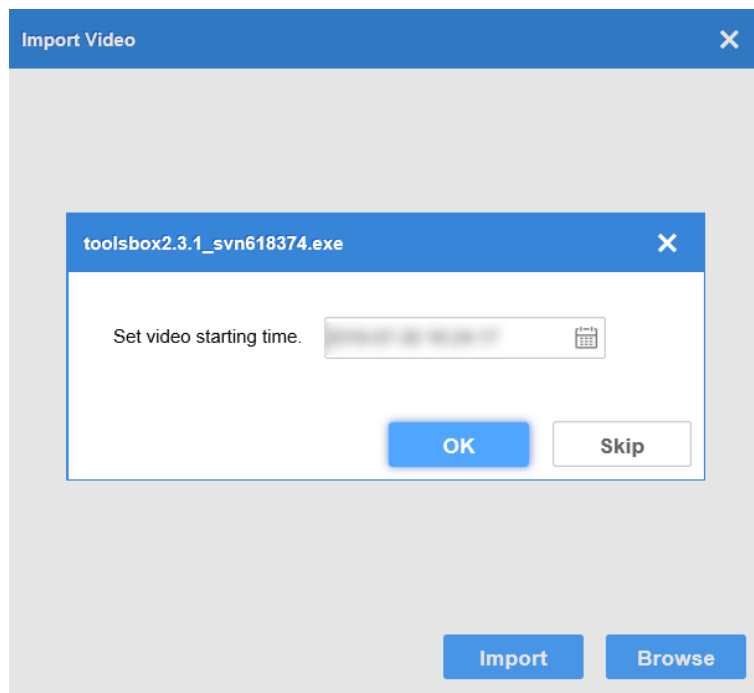


Figure 3-8 Import Video Interface

2. Click **Browse** to select video recording files, and set video starting time as actual recording time. Click **OK**.



**Figure 3-9 Set Video Starting Time**

---

### **Note**

When analyzing the video recording task, the actual time of video will be adopted if it is available. Otherwise, the starting time which is set will be adopted.

- 
3. Click **OK** to complete the operation.

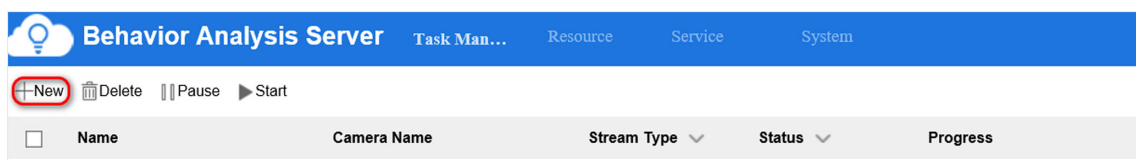
## 3.3 Perimeter Analysis Task

### 3.3.1 Create Perimeter Analysis Task

Create a perimeter analysis task. Up to 8 detection events can be added for each task.

#### Steps

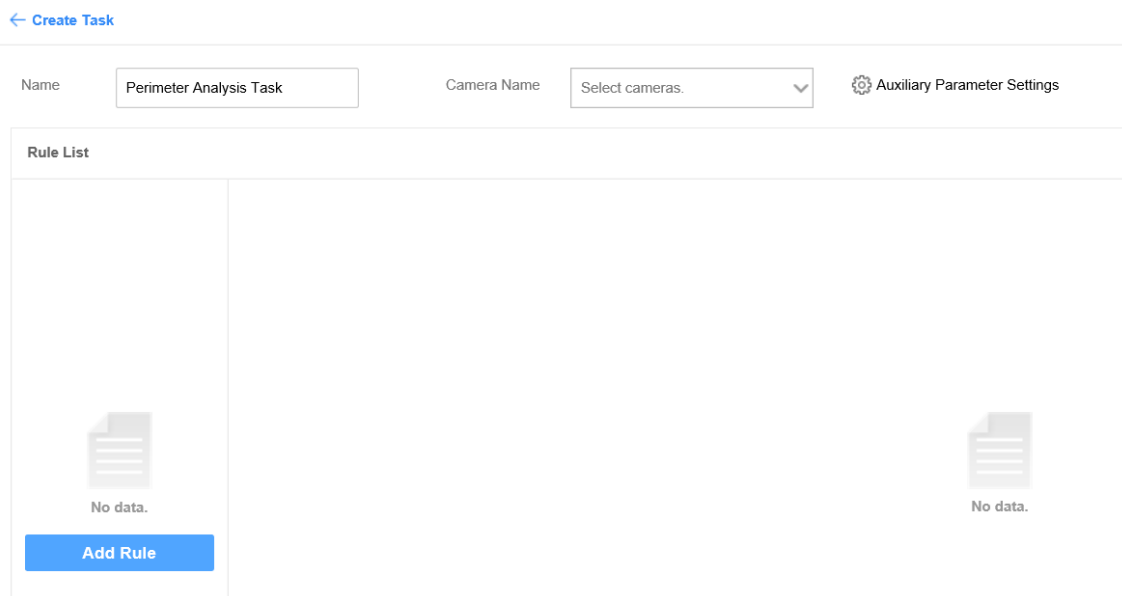
1. Click **Task Management** → **New** .



**Figure 3-10 Create a New Task**

2. Enter a task name.

3. Select the corresponding camera or video recording. Only one camera or video recording is allowed for each task.



**Figure 3-11 Create Task Interface**



### Note

Keep **Auxiliary Parameter Settings** by default.

4. Click **Add Rule** to add related detection events. The rules for configuring different detection events are different. See more details in following sections.





### Note

You can select different scenes in any rules. If multiple scenes are selected in a rule, the analysis tasks of those scenes will be created at the same time.

### 3.3.2 Line Crossing Detection

An alarm will be triggered when a target crosses the warning line.

#### Steps

1. Select **Line Crossing** as **Event**.
2. **Optional:** Enable **Size Filter**.
  - 1) Click  to draw the maximum size of the target.
  - 2) Click  to draw the minimum size of the target.


### Note

If size filter is enabled, only targets whose size is between the minimum and maximum sizes will be detected.




**Figure 3-12 Draw Filter Target**


### 3. Set crossing line.

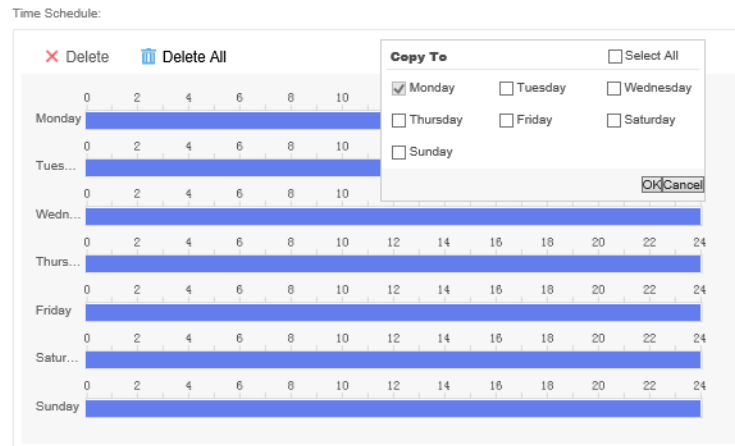
- 1) Click  to draw a crossing line.
- 2) Move the mouse to the ends of the crossing line, press and hold the left mouse button to adjust the position and length of the line.
- 3) Set the direction of crossing line.
- 4) Set sensitivity. The higher the alarm sensitivity is, the easier an alarm can be triggered.

### Note

Click the drawn graph and then click  to delete the line. The maximum size should be larger than the minimum one.

### 4. Select **Target Type**.

5. Set detection time schedule, and the all-day detection is set by default. Click  to apply the settings to other days.



**Figure 3-13 Set Detection Time Schedule**

6. Click **Save**.

### 3.3.3 Region Entrance Detection

An alarm will be triggered when a target enters the detection area.


#### Steps

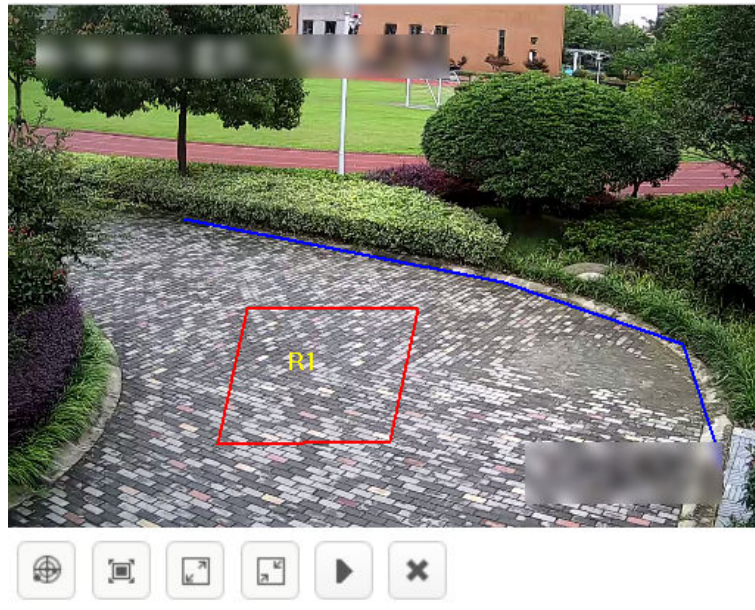
1. Click **Add** to configure rule parameters.

- **Name:** the name of rule. It is recommended that the name of rule be consistent with the name of event.
- **Scene:** select **Perimeter**.
- **Event:** select **Region Entrance Detection**.


2. Draw detection area.

- Custom detection area

Click , press the left mouse button and move the mouse to draw detection area, and press the right button to complete the operation.





**Figure 3-14 Custom Detection Area**


- Full screen detection  
Click  to do full screen detection.




**Figure 3-15 Full Screen Detection**

- 3. Optional: Enable Size Filter.** Only targets between the minimum and maximum sizes will be detected.
- 1) Click  to draw the maximum size of the target.
  - 2) Click  to draw the minimum size of the target.

## Note

Click the drawn graph and then click  to delete the area. The maximum size should be larger than the minimum one.

4. Select a target type according to your needs.
5. Set detection time schedule, all day by default. Click  to apply the settings to other days.

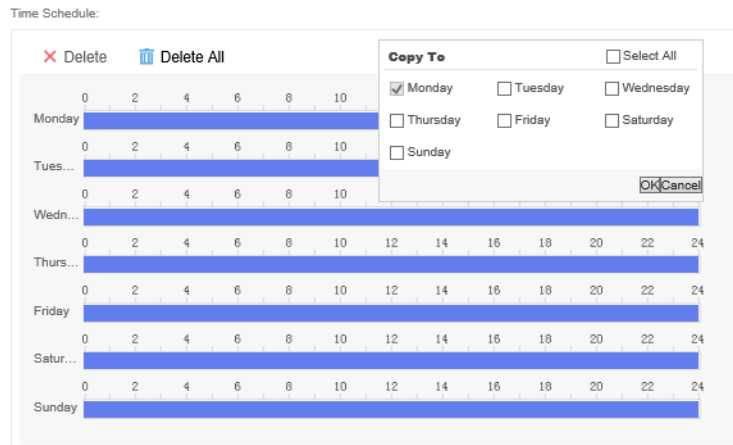


Figure 3-16 Set Detection Time Schedule


6. Click **Save**.

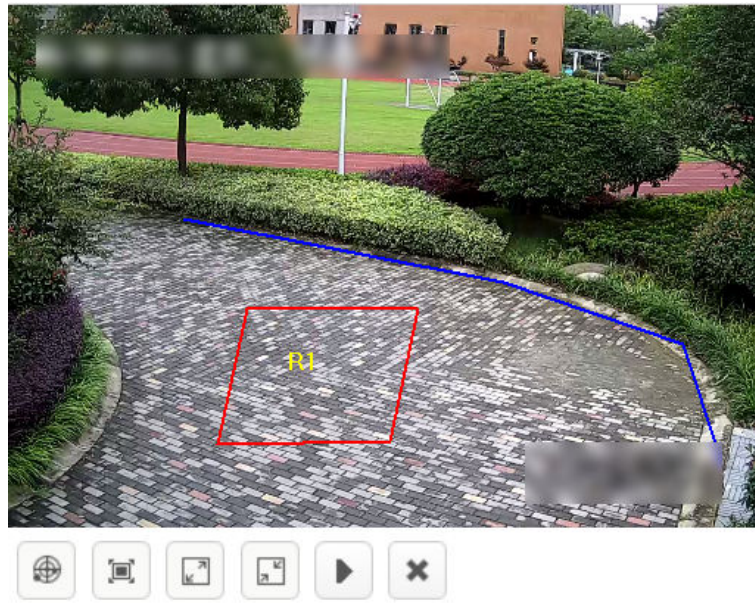
## 3.3.4 Region Exiting Detection

An alarm will be triggered when a target exits the detection area.


### Steps

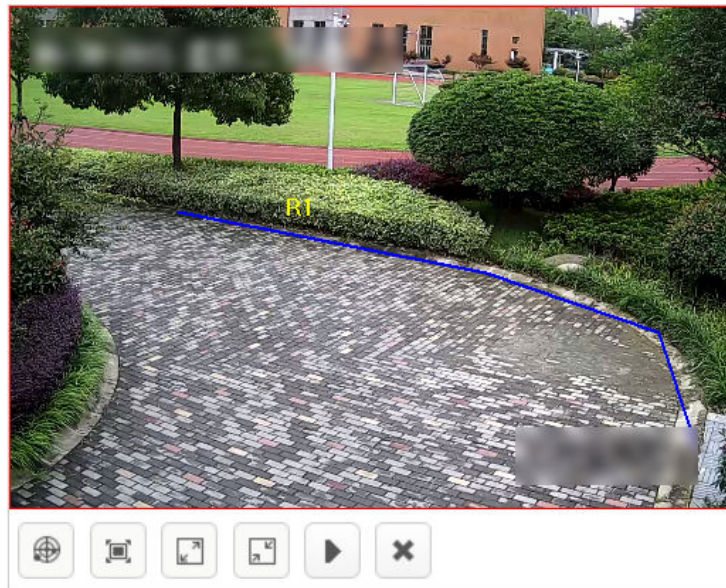
1. Select **Region Entrance** as **Event**.
2. Draw detection area.
  - Custom detection area

Click , press the left mouse button and move the mouse to draw detection area, and press the right button to complete the operation.





**Figure 3-17 Custom Detection Area**

- Full screen detection  
Click  to do full screen detection.





**Figure 3-18 Full Screen Detection**

- 3. Optional: Enable Size Filter.** Only targets between the minimum and maximum sizes will be detected.
- 1) Click  to draw the maximum size of the target.
  - 2) Click  to draw the minimum size of the target.



## Note

Click the drawn graph and then click  to delete the area. The maximum size should be larger than the minimum one.

4. Select **Target Type**.
5. Set detection time schedule, and the all-day detection is set by default. Click  to apply the settings to other days.

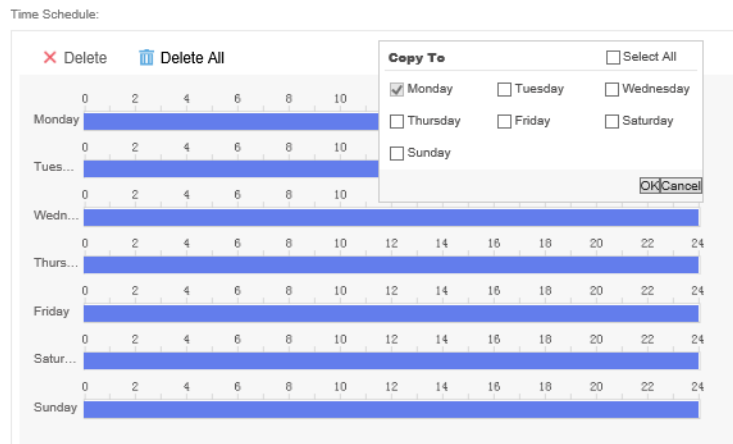


Figure 3-19 Set Detection Time Schedule


6. Click **Save**.

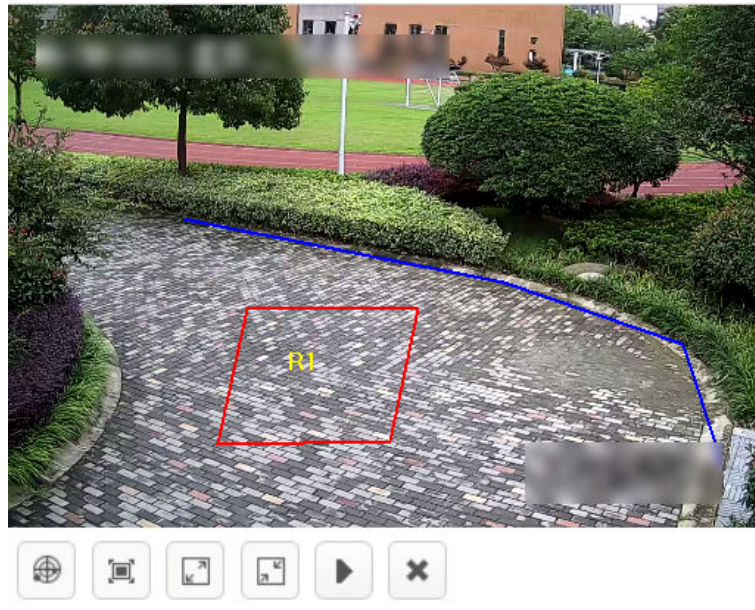
## 3.3.5 Intrusion Detection

An alarm will be triggered if the stay duration of the target exceeds the time set.


### Steps

1. Select **Intrusion** as **Event**.
2. Draw detection area.
  - Custom detection area

Click , press the left mouse button and move the mouse to draw detection area, and press the right button to complete the operation.





**Figure 3-20 Custom Detection Area**

- Full screen detection  
Click  to do full screen detection.



**Figure 3-21 Full Screen Detection**

### 3. Optional: Enable Size Filter.

- 1) Click  to draw the maximum size of the target.
- 2) Click  to draw the minimum size of the target.



## Note

If size filter is enabled, only targets whose size is between the minimum and maximum sizes will be detected.



## Note

Click the drawn graph and then click to delete the area. The maximum size should be larger than the minimum one.

4. Set **Duration(s)**, **Target Type**, and **Sensitivity**. The higher the alarm sensitivity is, the easier an alarm can be triggered.
5. Set detection time schedule, and the all-day detection is set by default. Click to apply the settings to other days.

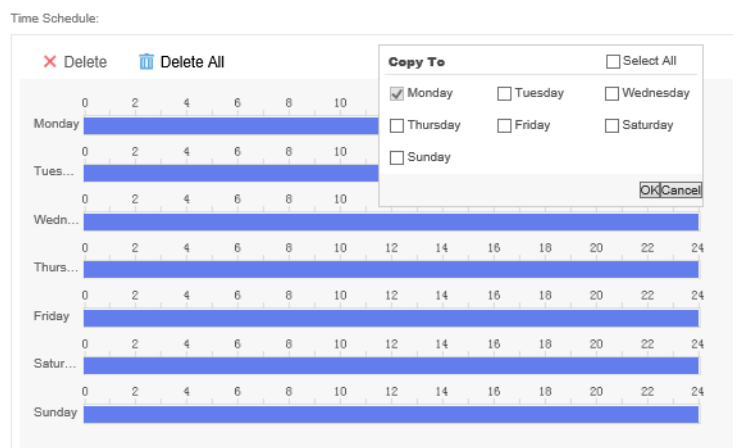


Figure 3-22 Set Detection Time Schedule

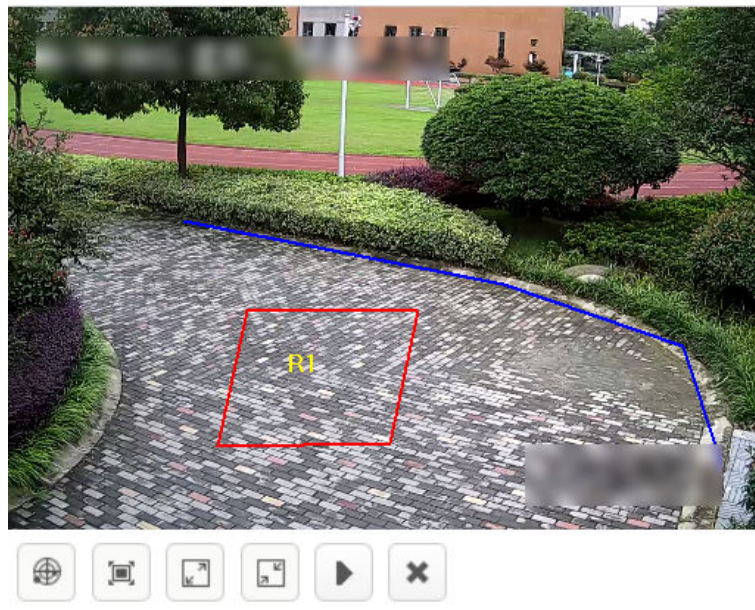
6. Click **Save**.

## 3.3.6 Loitering Detection


An alarm will be triggered if the loitering time of the target exceeds the time set.

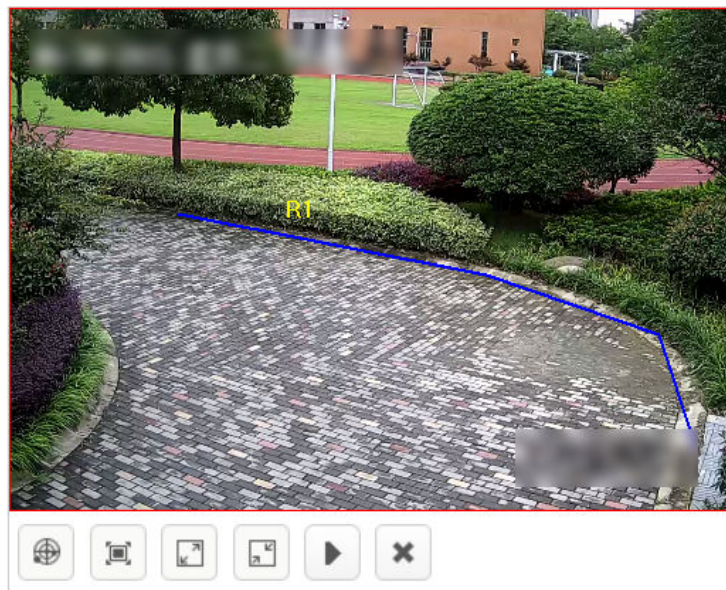
### Steps

1. Click **Add** to configure rule parameters.
  - **Name**: the name of rule. It is recommended that the name of rule be consistent with the name of event.
  - **Scene**: select **Perimeter**.
  - **Event**: select **Loitering Detection**.
2. Draw detection area.
  - Custom detection area
    - Click , press the left mouse button and move the mouse to draw detection area, and press the right button to complete the operation.





**Figure 3-23 Custom Detection Area**

- Full screen detection  
Click  to do full screen detection.



**Figure 3-24 Full Screen Detection**

- 3. Optional: Enable Size Filter.** Only targets between the minimum and maximum sizes will be detected.
- 1) Click  to draw the maximum size of the target.
  - 2) Click  to draw the minimum size of the target.



## Note

Click the drawn graph and then click to delete the area. The maximum size should be larger than the minimum one.

### 4. Set **duration** and **target type**.

### 5. Set detection time schedule, all day by default. Click to apply the settings to other days.

Time Schedule:

✖ Delete
🗑 Delete All

Day	0	2	4	6	8	10	12	14	16	18	20	22	24
Monday													
Tues...													
Wedn...													
Thurs...													
Friday													
Satur...													
Sunday													

**Copy To**
☐ Select All
   
☒ Monday
 ☐ Tuesday
 ☐ Wednesday
   
☐ Thursday
 ☐ Friday
 ☐ Saturday
   
☐ Sunday

Figure 3-25 Set Detection Time Schedule

### 6. Click **Save**.

## 3.3.7 Parking Detection

An alarm will be triggered if the parking time of the target exceeds the time set.

### Steps

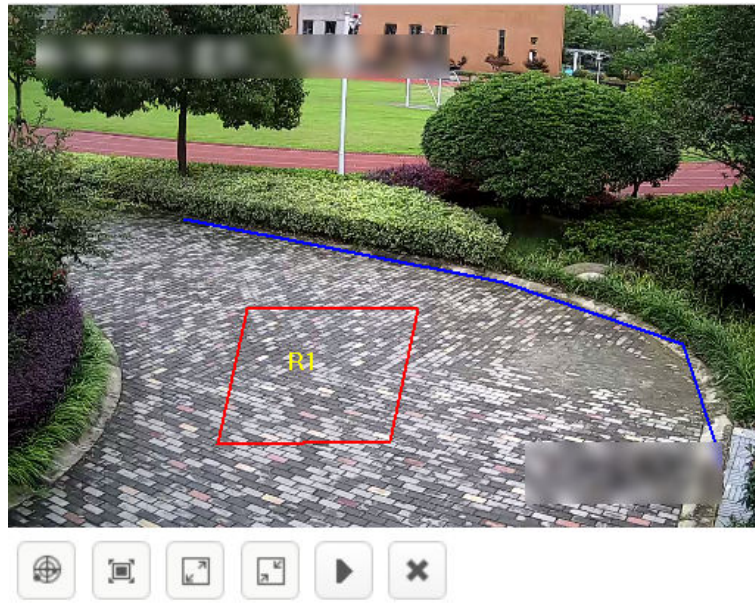
#### 1. Click **Add** to configure rule parameters.

- **Name:** the name of rule. It is recommended that the name of rule be consistent with the name of event.
- **Scene:** select **Perimeter**.
- **Event:** select **Parking Detection**.


#### 2. Draw detection area.

- Custom detection area

Click , press the left mouse button and move the mouse to draw detection area, and press the right button to complete the operation.





**Figure 3-26 Custom Detection Area**

- Full screen detection  
Click  to do full screen detection.



**Figure 3-27 Full Screen Detection**

- 3. Optional: Enable Size Filter.** Only targets between the minimum and maximum sizes will be detected.
- 1) Click  to draw the maximum size of the target.
  - 2) Click  to draw the minimum size of the target.



## Note

Click the drawn graph and then click to delete the area. The maximum size should be larger than the minimum one.

4. Set **duration**, **target type**, and **sensitivity**. The higher the alarm sensitivity is, the easier an alarm can be triggered.
5. Set detection time schedule, all day by default. Click to apply the settings to other days.

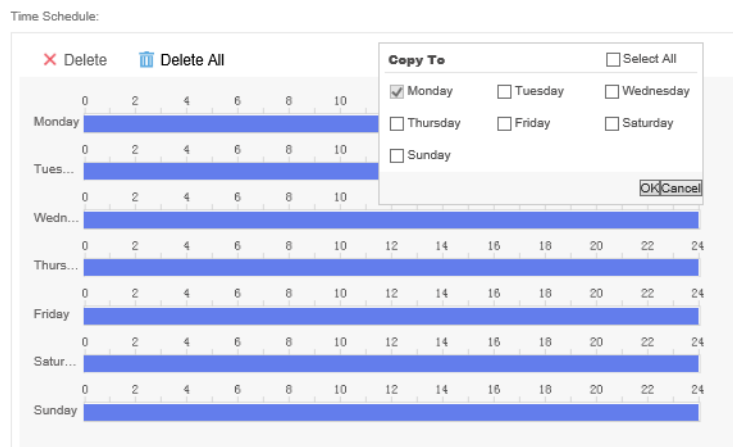


Figure 3-28 Set Detection Time Schedule

6. Click **Save**.

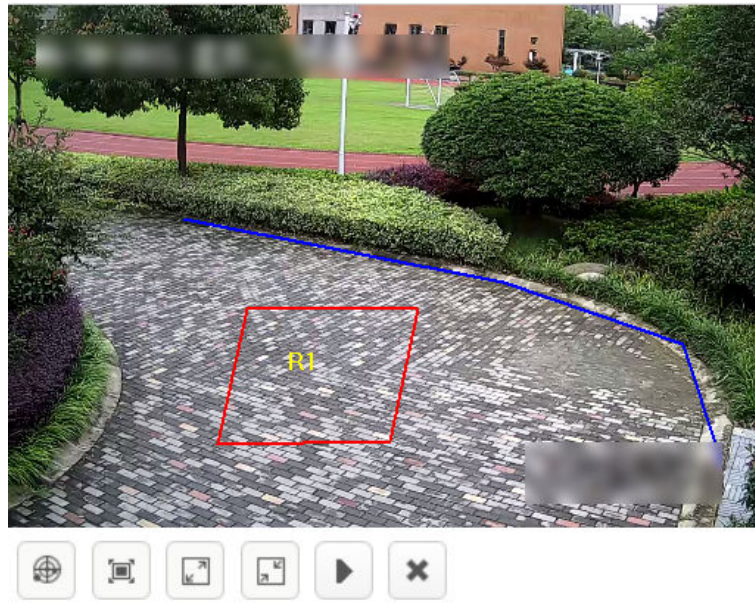
## 3.3.8 Unattended Baggage Detection

An alarm will be triggered if the unattended time of object exceeds the time set.


### Steps

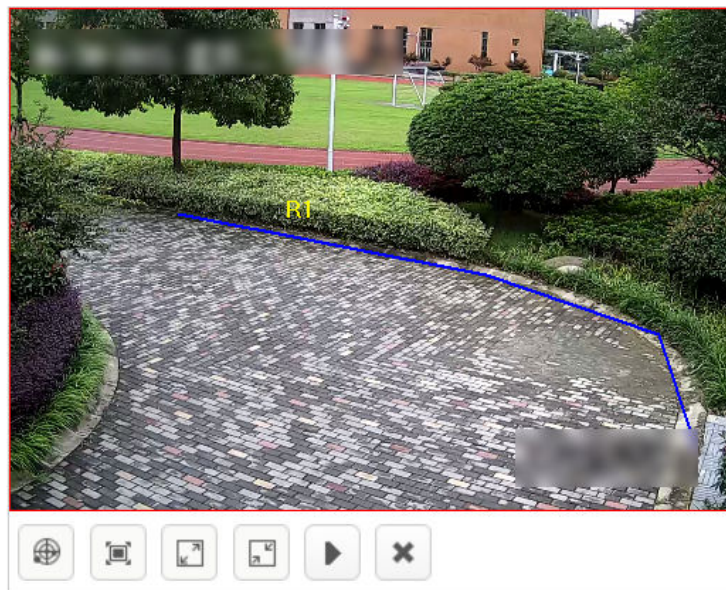
1. Click **Add** to configure rule parameters.
  - **Name**: the name of rule. It is recommended that the name of rule be consistent with the name of event.
  - **Scene**: select **Perimeter**.
  - **Event**: select **Unattended Object Detection**.
2. Draw detection area.
  - Custom detection area

Click , press the left mouse button and move the mouse to draw detection area, and press the right button to complete the operation.





**Figure 3-29 Custom Detection Area**

- Full screen detection  
Click  to do full screen detection.



**Figure 3-30 Full Screen Detection**

- 3. Optional: Enable Size Filter.** Only targets between the minimum and maximum sizes will be detected.
- 1) Click  to draw the maximum size of the target.
  - 2) Click  to draw the minimum size of the target.



## Note

Click the drawn graph and then click to delete the area. The maximum size should be larger than the minimum one.

4. Set **duration**, **target type**, and **sensitivity**. The higher the alarm sensitivity is, the easier an alarm can be triggered.
5. Set detection time schedule, all day by default. Click to apply the settings to other days.

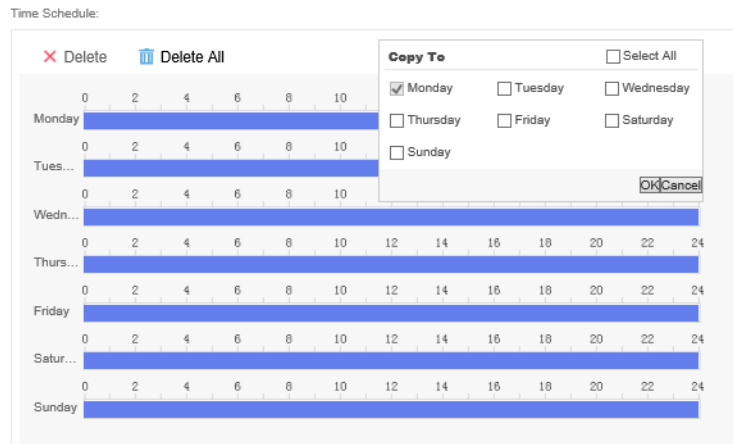


Figure 3-31 Set Detection Time Schedule

6. Click **Save**.

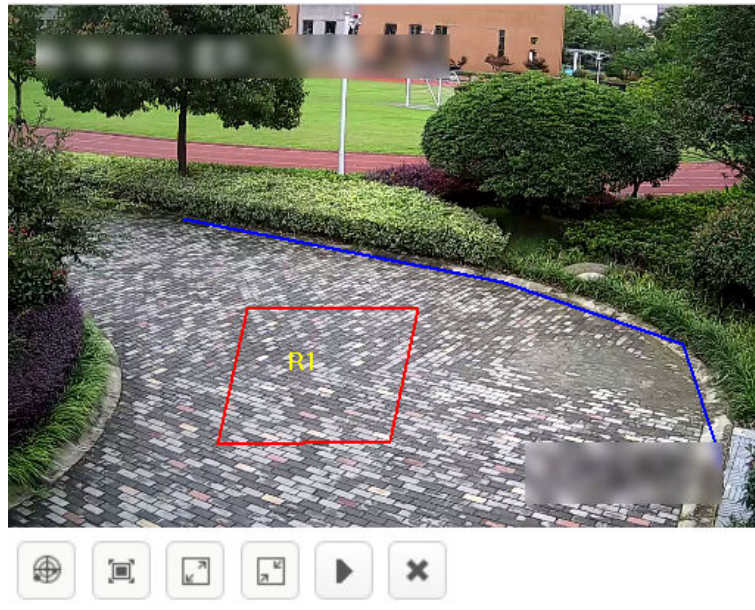
## 3.3.9 Object Removal Detection

An alarm will be triggered if the removal time of object exceeds the time set.


### Steps

1. Click **Add** to configure rule parameters.
  - **Name:** the name of rule. It is recommended that the name of rule be consistent with the name of event.
  - **Scene:** select **Perimeter**.
  - **Event:** select **Object Removal Detection**.
2. Draw detection area.
  - Custom detection area

Click , press the left mouse button and move the mouse to draw detection area, and press the right button to complete the operation.





**Figure 3-32 Custom Detection Area**

- Full screen detection  
Click  to do full screen detection.



**Figure 3-33 Full Screen Detection**

- 3. Optional: Enable Size Filter.** Only targets between the minimum and maximum sizes will be detected.
- 1) Click  to draw the maximum size of the target.
  - 2) Click  to draw the minimum size of the target.



## Note

Click the drawn graph and then click to delete the area. The maximum size should be larger than the minimum one.

4. Set **duration**, **target type**, and **sensitivity**. The higher the alarm sensitivity is, the easier an alarm can be triggered.
5. Set detection time schedule, all day by default. Click to apply the settings to other days.

Time Schedule:

Figure 3-34 Set Detection Time Schedule

6. Click **Save**.

## 3.4 Indoor Analysis Task

### 3.4.1 Create Trend Analysis Task

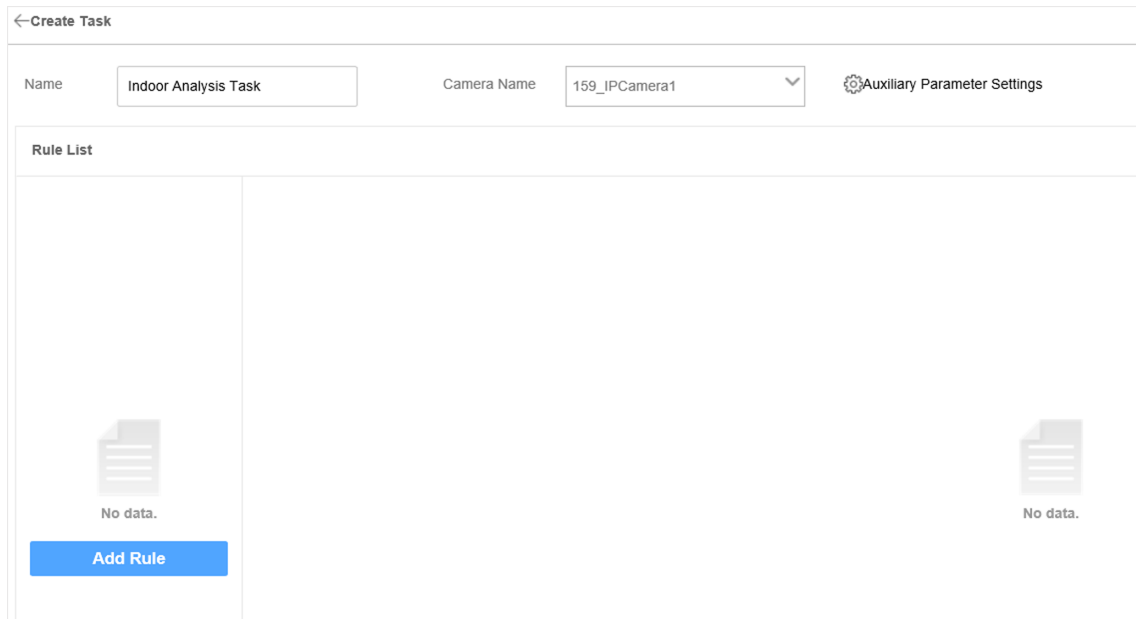
Create an indoor analysis task. Up to 8 detection events can be added for each task.

#### Steps

1. Click **Task Management** → **New**.

Figure 3-35 Create a New Task

2. Enter a task name.
3. Select the corresponding camera or video recording. Only one camera or video recording is allowed for each task.



**Figure 3-36 Create Task Interface**



### Note

Keep **Auxiliary Parameter Settings** by default.

4. Click **Add Rule** to add related detection events. The rules for configuring different detection events are different. See more details in following sections.



### Note


You can select different scenes in any rules. If multiple scenes are selected in a rule, the analysis tasks of those scenes will be created at the same time.

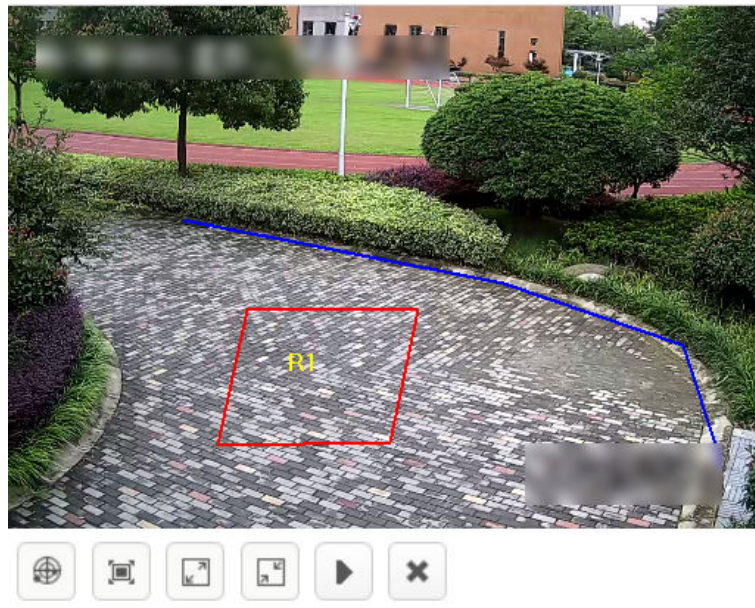
### 3.4.2 Getting-up Detection

Detect getting-up movement of people in the area, such as getting up or getting out of bed during the break period.

#### Steps

1. Click **Add** to configure rule parameters.
  - **Name**: the name of rule. It is recommended that the name of rule be consistent with the name of event.
  - **Scene**: select **Indoor**.
  - **Event**: select **Getting-up Detection**.
2. Draw detection area.
  - Custom detection area

Click  , press the left mouse button and move the mouse to draw detection area, and press the right button to complete the operation.



**Figure 3-37 Custom Detection Area**



- Full screen detection

Click  to do full screen detection.



**Figure 3-38 Full Screen Detection**


**3. Optional: Enable Size Filter.** Only targets between the minimum and maximum sizes will be detected.


- 1) Click  to draw the maximum size of the target.
- 2) Click  to draw the minimum size of the target.

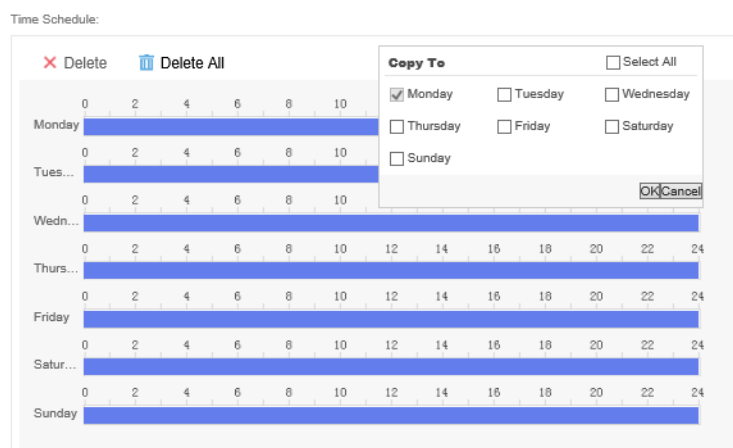


**Figure 3-39 Draw Filter Target**

## Note

Click the drawn graph and then click  to delete the area. The maximum size should be larger than the minimum one.

- 4. Set sensitivity.** The higher the alarm sensitivity is, the easier an alarm can be triggered.
- 5. Set Getting-up Mode.** You need to select relevant mode according to actual bed type.
  - Wide Bed Mode
  - Bunk Bed Mode
  - Sitting and Getting-up Mode
- 6. Set detection time schedule, all day by default.** Click  to apply the settings to other days.




**Figure 3-40 Set Detection Time Schedule**

7. Click **Save**.

## 3.4.3 Climbing Detection

Detect the movement of person who climbs over the height set. For example, such events as climbing and hanging.

### Steps

1. Click **Add** to configure rule parameters.
  - **Name**: the name of rule. It is recommended that the name of rule be consistent with the name of event.
  - **Scene**: select **Indoor**.
  - **Event**: select **Climbing Detection**.
2. Click , press and hold the left mouse button to draw limited height line, and then click the right button.
3. Set crossing line direction.

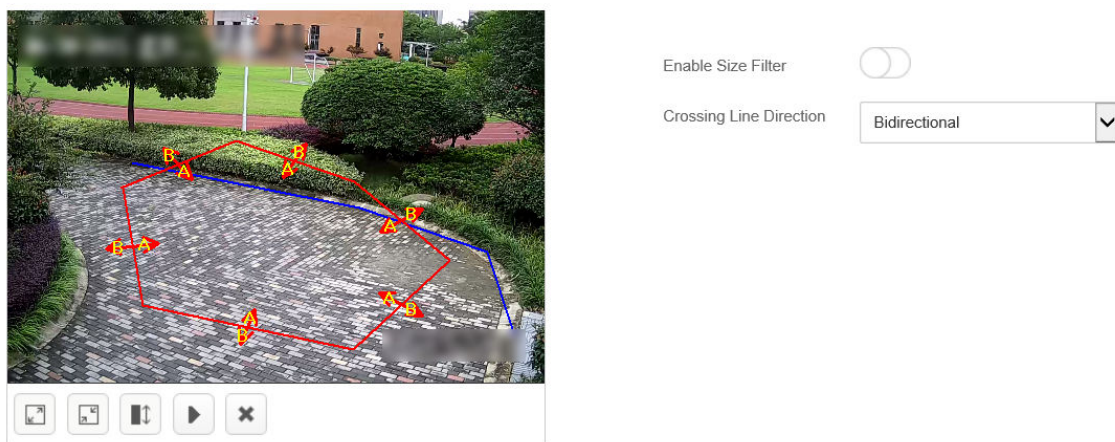






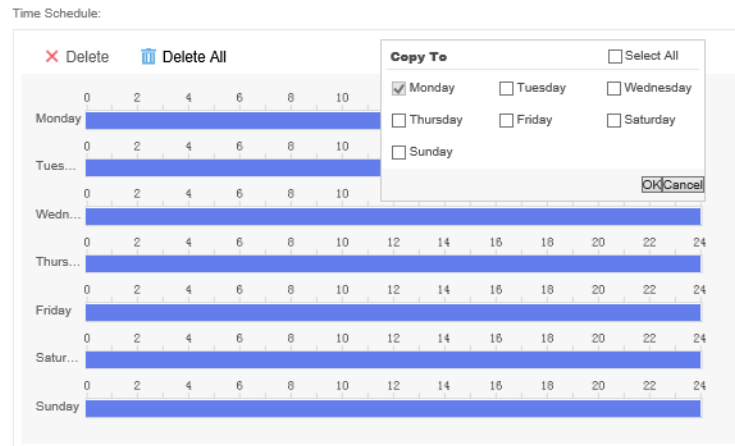
Figure 3-41 Set Climbing Area

---

### Note

Click the drawn graph and then click  to delete the area.

4. **Optional**: Enable **Size Filter**. Only targets between the minimum and maximum sizes will be detected.
  - 1) Click  to draw the maximum size of the target.
  - 2) Click  to draw the minimum size of the target.
5. Set detection time schedule, all day by default. Click  to apply the settings to other days.



**Figure 3-42 Set Detection Time Schedule**

6. Click **Save**.

### 3.4.4 Absence/Sleep on Duty Detection

Detect the movement of a person on duty in the detection area who is absent or staying motionless. For example, a person is absent or has a sleep during the night duty.


#### Steps

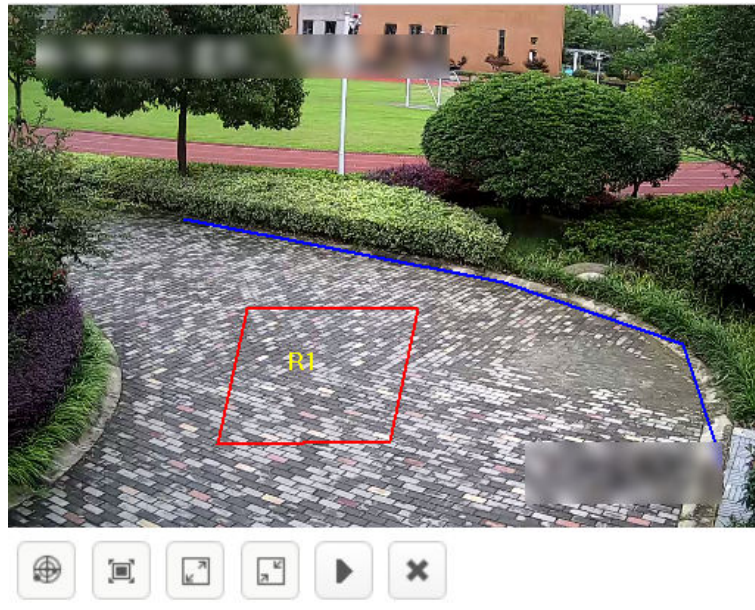
1. Click **Add** to configure rule parameters.

- **Name:** the name of rule. It is recommended that the name of rule be consistent with the name of event.
- **Scene:** select **Indoor**.
- **Event:** select **Absence/Sleep on Duty Detection**.


2. Draw detection area.

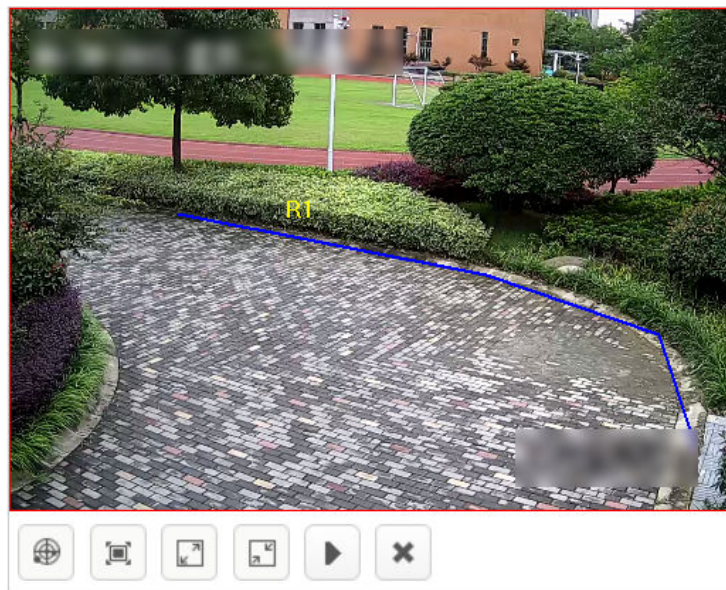
- Custom detection area

Click  , press the left mouse button and move the mouse to draw detection area, and press the right button to complete the operation.





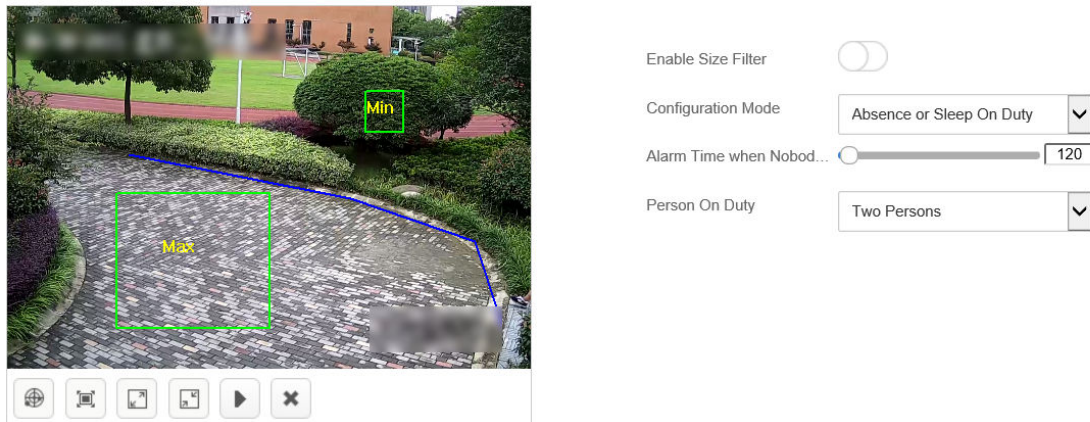
**Figure 3-43 Custom Detection Area**

- Full screen detection  
Click  to do full screen detection.



**Figure 3-44 Full Screen Detection**


- 3. Optional: Enable Size Filter.** Only targets between the minimum and maximum sizes will be detected.
- 1) Click  to draw the maximum size of the target.
  - 2) Click  to draw the minimum size of the target.



**Figure 3-45 Draw Filter Target**

---

### **Note**

Click the drawn graph and then click  to delete the area. The maximum size should be larger than the minimum one.

---

#### **4. Configure detection parameters in details.**

##### **Configuration Mode**

- Absence
- Sleep on Duty
- Absence or Sleep on Duty

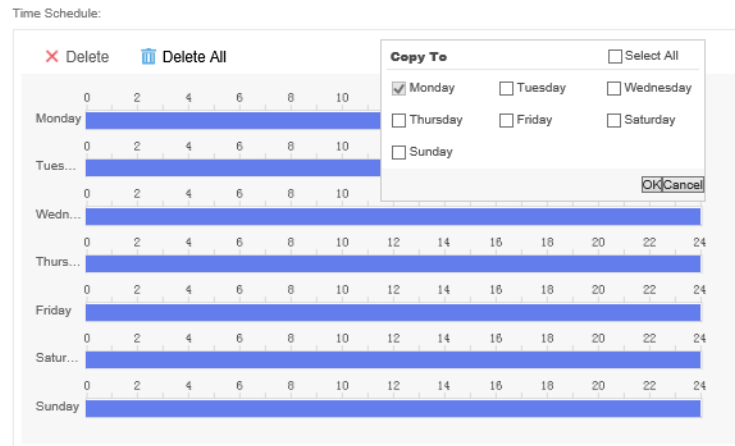
##### **Alarm Time when Nobody is on Duty**

An alarm will be triggered if the absence time period exceeds the time set.

##### **Persons on duty**

The number of people on duty.

#### **5. Set detection time schedule, all day by default. Click to apply the settings to other days.**



**Figure 3-46 Set Detection Time Schedule**

6. Click **Save**.

### 3.4.5 Sudden Change of Sound Intensity Detection

Detect whether the sound intensity in the area is normal or not. For example, such events as screaming or quarreling lead to sudden change of sound intensity.

#### Steps

1. Click **Add** to configure rule parameters.

- **Name:** the name of rule. It is recommended that the name of rule be consistent with the name of event.
- **Scene:** select **Indoor**.
- **Event:** select **Detection for Sudden Change of Sound Intensity**.

2. Configure detection mode.

#### Sensitivity Detection

Detect the sound according to various characteristics. An alarm will be triggered if there is an abnormal sound. For example, such events as screaming or quarreling lead to sudden change of sound intensity. You can keep the sensitivity value by default, and then make adjustments according to the actual alarm situation.

#### Decibel Threshold Detection

Detect the sound volume in the area. An alarm will be triggered if the volume is greater than the decibel threshold level.



Figure 3-47 Full Screen Detection

 **Note**

Decibel threshold detection is easier to trigger alarm than sensitivity detection.

3. Click **Sound Intensity Test** to check real-time volume. Adjust the threshold according to the testing result.

Detection Mode

Sensitivity Detection

▼

Decibel Threshold (dB)

70

Sensitivity


60

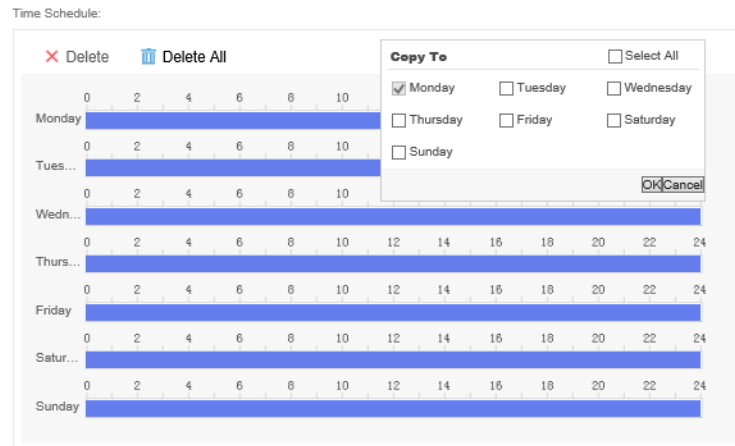
Sound Intensity Test

Sound...

Real-Time Volume

Figure 3-48 Sound Intensity Test

4. Set detection time schedule, all day by default. Click  to apply the settings to other days.



**Figure 3-49 Set Detection Time Schedule**

5. Click **Save**.

### 3.4.6 Abnormal Number of People Detection


Detect whether the number of people is normal or not.

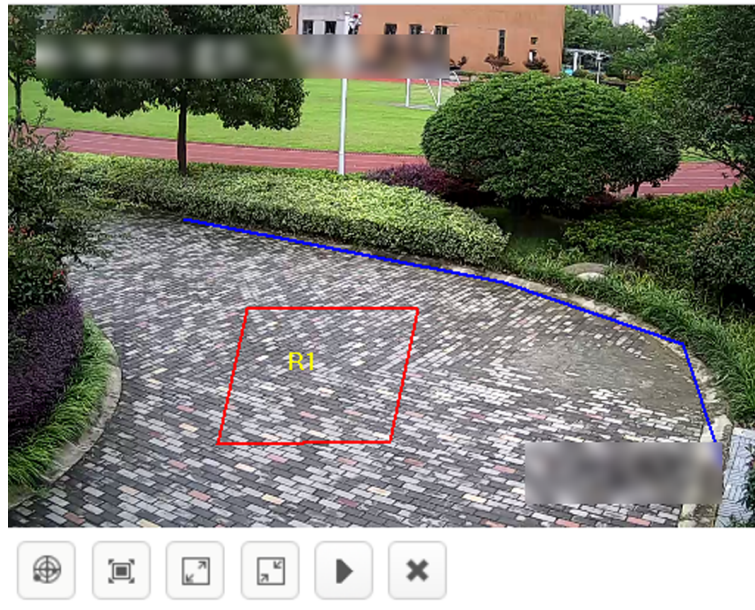
#### Steps

1. Configure rule parameters.


- **Name:** the name of rule. It is recommended that the name of rule be consistent with the name of event.
- **Scene:** select **Indoor**.
- **Event:** select **Abnormal Number of People**.

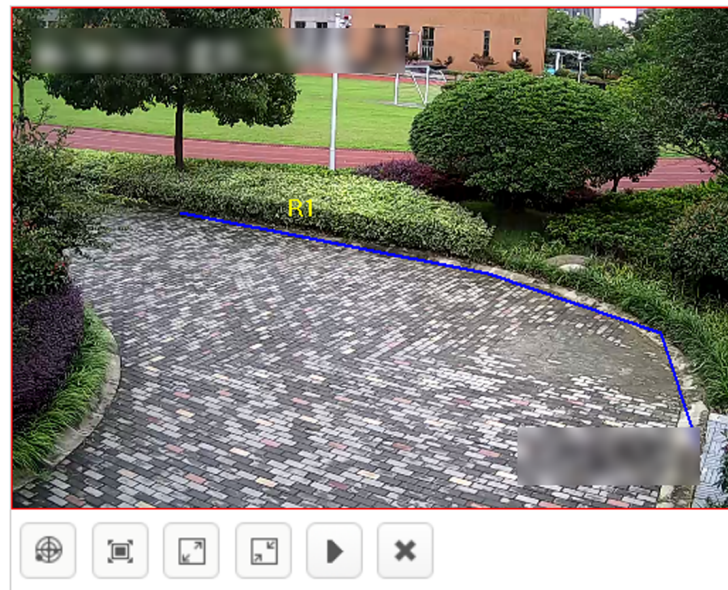
2. Draw detection area.

- Click  , press the left mouse button and move the mouse to draw detection area, and press the right button to complete the operation.




**Figure 3-50 Custom Detection Area**


- Click  to do full screen detection.



**Figure 3-51 Full Screen Detection**

- 3. Optional:** Check **Enable Size Filter**. Only targets between the minimum and maximum sizes will be detected.

Click  , press and hold the left button to draw the maximum size of the target.

Click  the drawn graph and then click to delete the area. The maximum size should be larger than the minimum one.

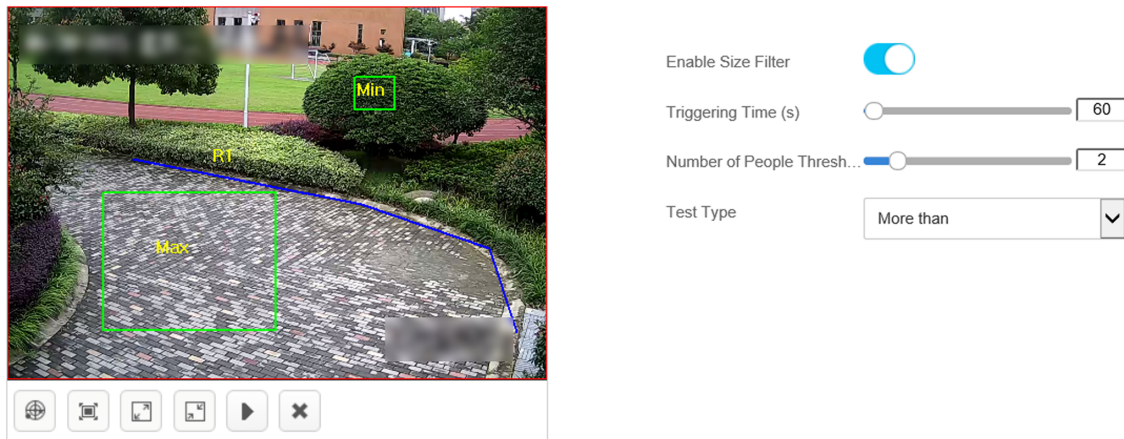



Figure 3-52 Draw Filter Target

### Note

Click the drawn graph and then click  to delete the area. The maximum size should be larger than the minimum one.

#### 4. Set **Triggering Time** and **Number of People Threshold**.

#### 5. Set detection mode.

##### **More than**

An alarm will be triggered when the duration exceeds the triggering time and the number of people in detection area is greater than the threshold level set.

##### **Less than**

An alarm will be triggered when the duration exceeds the triggering time and the number of people in detection area is less than the threshold level set.

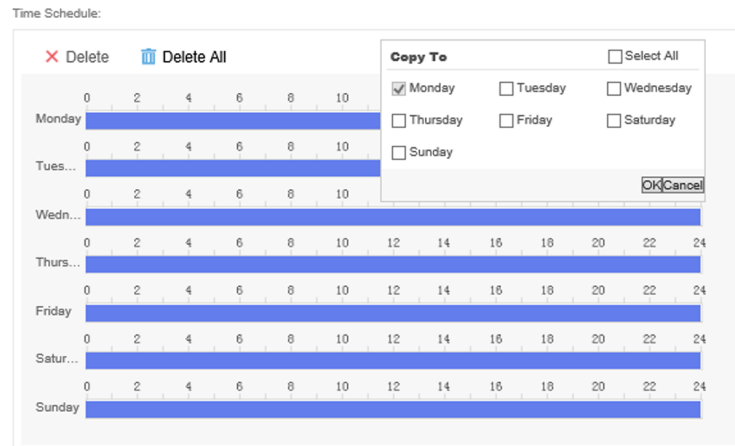
##### **Equal to**

An alarm will be triggered when the duration exceeds the triggering time and the number of people in detection area is equal to the threshold level set.

##### **Not equal to**

An alarm will be triggered when the duration exceeds the triggering time and the number of people in detection area is not equal to the threshold level set.

#### 6. Set detection time schedule, all day by default. Click to apply the settings to other days.



**Figure 3-53 Set Detection Time Schedule**

7. Click **Save**.

### 3.4.7 Standing-up Detection

Detect the standing movement of a person in the area. For example, the person who is being interrogated stands up from the seat during the trial.


#### Steps

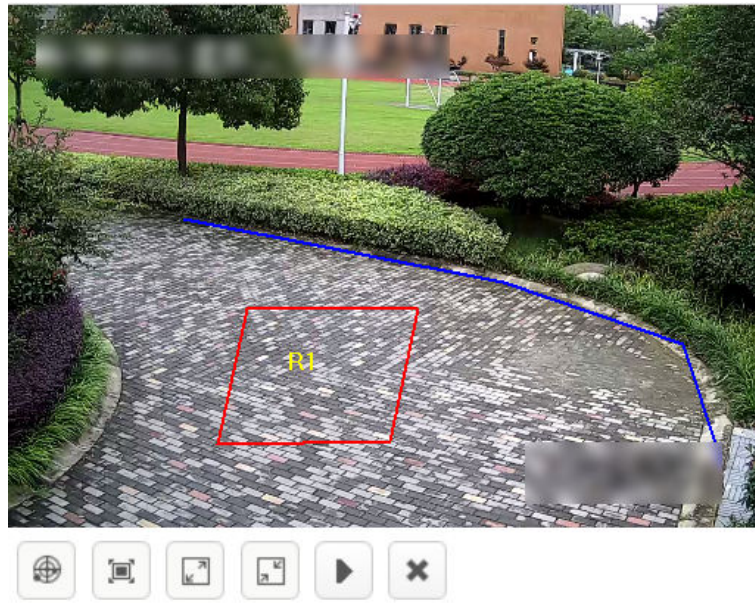
1. Click **Add** to configure rule parameters.

- **Name:** the name of rule. It is recommended that the name of rule be consistent with the name of event.
- **Scene:** select **Indoor**.
- **Event:** select **Standing-up Detection**.


2. Draw detection area.

- Custom detection area

Click  , press the left mouse button and move the mouse to draw detection area, and press the right button to complete the operation.





**Figure 3-54 Custom Detection Area**

- Full screen detection  
Click  to do full screen detection.



**Figure 3-55 Full Screen Detection**

- 3. Optional: Enable Size Filter.** Only targets between the minimum and maximum sizes will be detected.
- 1) Click  to draw the maximum size of the target.
  - 2) Click  to draw the minimum size of the target.



## Note

Click the drawn graph and then click to delete the area. The maximum size should be larger than the minimum one.

4. Set **sensitivity**. The higher the alarm sensitivity is, the easier an alarm can be triggered.
5. Set detection time schedule, all day by default. Click to apply the settings to other days.

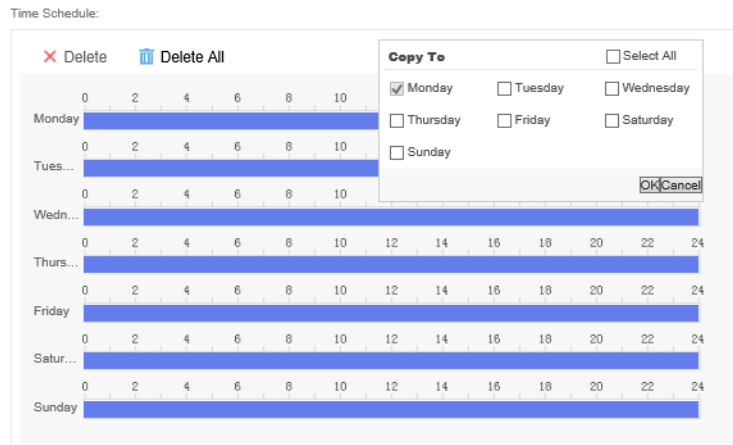


Figure 3-56 Set Detection Time Schedule

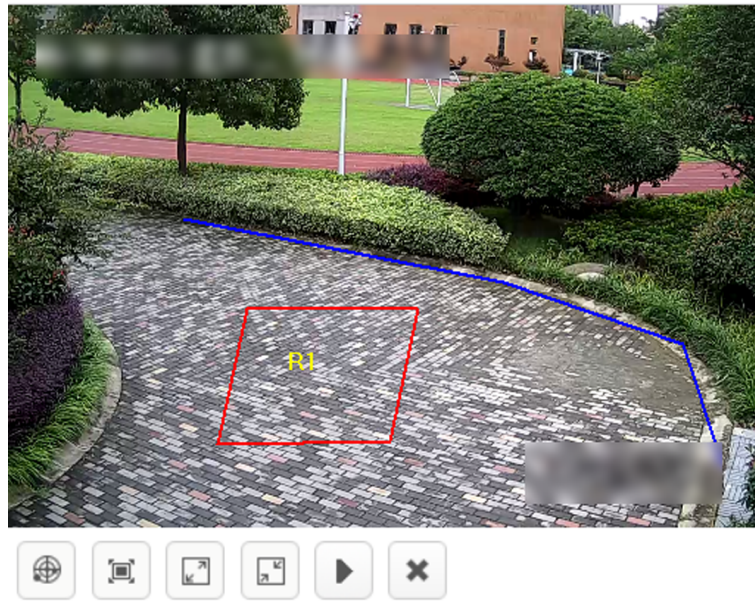
6. Click **Save**.

## 3.4.8 Sitting Detection


Detect the sedentary time of a person. For instance, the interrogator or person who is interrogated stays motionless in the seat for a long time.

### Steps

1. Configure rule parameters.
  - **Name:** the name of rule. It is recommended that the name of rule be consistent with the name of event.
  - **Scene:** select **Indoor**.
  - **Event:** select **Sitting Detection**.
2. Draw detection area.
  - Click , press the left mouse button and move the mouse to draw detection area, and press the right button to complete the operation.




**Figure 3-57 Custom Detection Area**

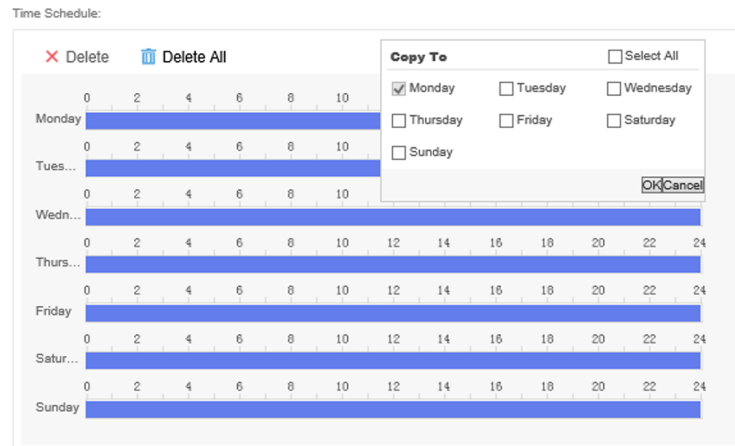
- Click  to do full screen detection.



**Figure 3-58 Full Screen Detection**

**3. Set Duration.**

**4. Set detection time schedule, all day by default. Click  to apply the settings to other days.**




### Figure 3-59 Set Detection Time Schedule

**5. Click Save.**

### 3.4.9 Playing Mobile Phone Detection

Detect the behavior of playing mobile phone in certain area.


## Steps

1. Click **Add** to configure rule parameters.
  - **Name:** the name of rule. It is recommended that the name of rule be consistent with that of event.
  - **Scene:** select **Indoor**.
  - **Event:** select **Playing Mobile Phone Detection**.
2. Draw detection area.
  - Custom detection area
    - Click  , press the left mouse button and move the mouse to draw detection area, and press the right button to complete.



**Figure 3-60 Custom Detection Area**

- Full screen detection

Click  to do full screen detection.



**Figure 3-61 Full Screen Detection**



## Note

Click the drawn graph and then click to delete the area. The maximum size should be larger than the minimum one.

### 3. Set **Duration**.

### 4. Set detection time schedule, all day by default. Click to apply the settings to other days.

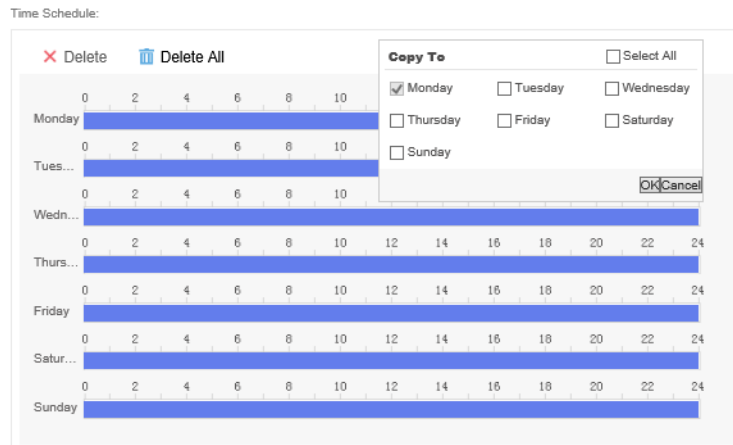


Figure 3-62 Set Detection Time Schedule

### 5. Click **Save**.

## 3.4.10 People Entrance(Non Police) Detection

Detect the entrance behavior of non police person in certain area.

### Steps

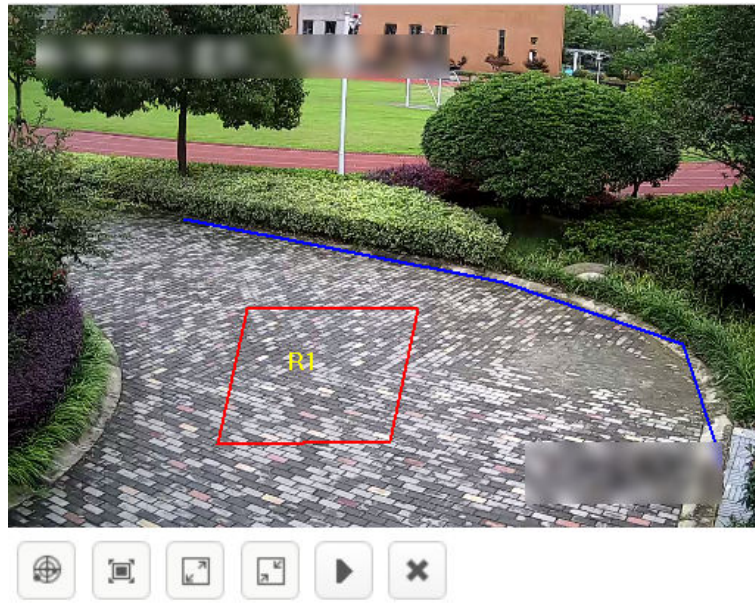
#### 1. Click **Add** to configure rule parameters.

- **Name:** the name of rule. It is recommended that the name of rule be consistent with the name of event.
- **Scene:** select **Indoor**.
- **Event:** select **People Entrance(Non Police) Detection**.


#### 2. Draw detection area.

- Custom detection area

Click , press the left mouse button and move the mouse to draw detection area, and press the right button to complete.





**Figure 3-63 Custom Detection Area**

- Full screen detection  
Click  to do full screen detection.



**Figure 3-64 Full Screen Detection**

- 3. Optional: Enable Size Filter.** Only targets between the minimum and maximum sizes will be detected.
- 1) Click  to draw the maximum size of the target.
  - 2) Click  to draw the minimum size of the target.



## Note

Click the drawn graph and then click to delete the area. The maximum size should be larger than the minimum one.

### 4. Set **Duration**.

### 5. Set detection time schedule, all day by default. Click to apply the settings to other days.

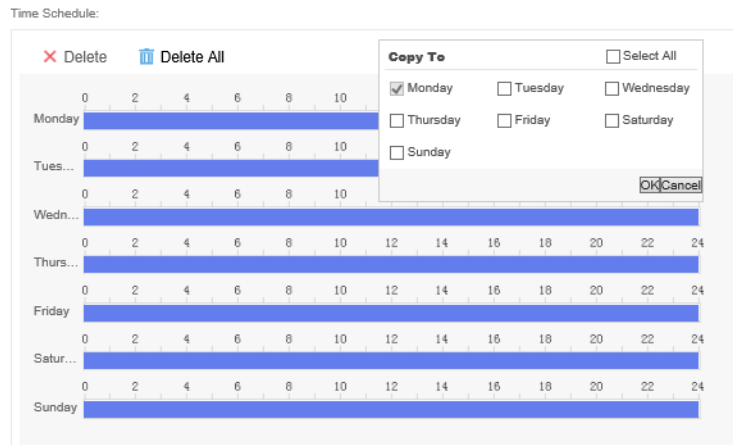


Figure 3-65 Set Detection Time Schedule

### 6. Click **Save**.

## 3.4.11 Police Absence Detection

Detect the occasion that no police is in the detection area.

### Steps

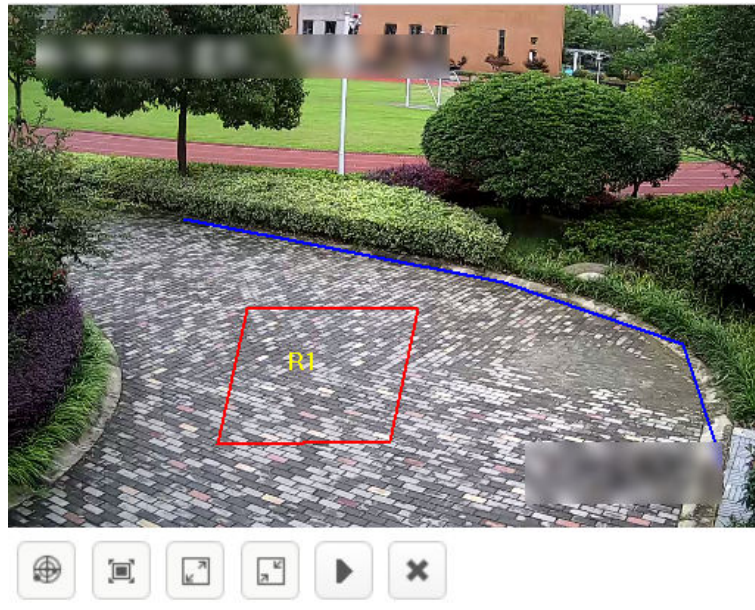
#### 1. Click **Add** to configure rule parameters.

- **Name:** the name of rule. It is recommended that the name of rule be consistent with that of event.
- **Scene:** select **Indoor**.
- **Event:** select **Police Absence Detection**.


#### 2. Draw detection area.

- Custom detection area

Click , press the left mouse button and move the mouse to draw detection area, and press the right button to complete.





**Figure 3-66 Custom Detection Area**

- Full screen detection  
Click  to do full screen detection.



**Figure 3-67 Full Screen Detection**

- 3. Optional: Enable Size Filter.** Only targets between the minimum and maximum sizes will be detected.
- 1) Click  to draw the maximum size of the target.
  - 2) Click  to draw the minimum size of the target.

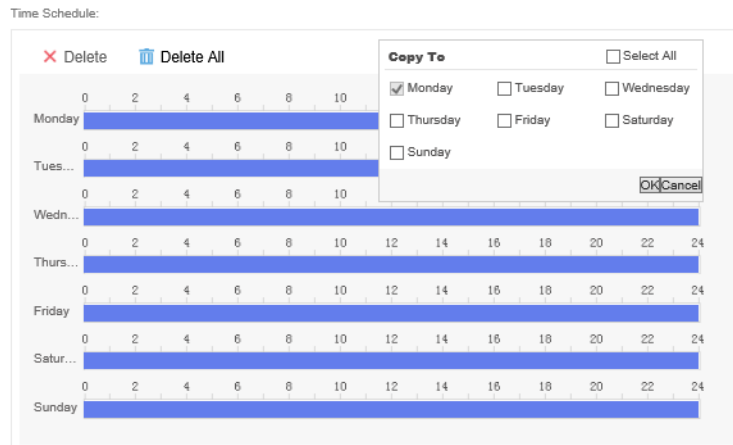


## Note

Click the drawn graph and then click to delete the area. The maximum size should be larger than the minimum one.

### 4. Set **Duration**.

### 5. Set detection time schedule, all day by default. Click to apply the settings to other days.



**Figure 3-68 Set Detection Time Schedule**

### 6. Click **Save**.

## 3.4.12 Falling-down Detection

Detect the falling-down behavior of person in the certain area.

### Steps

#### 1. Click **Add** to configure rule parameters.

- **Name:** the name of rule. It is recommended that the name of rule be consistent with the name of event.
- **Scene:** select **Indoor**.
- **Event:** select **Falling-down Detection**.

#### 2. Draw detection area.


- Custom detection area

Click , press the left mouse button and move the mouse to draw detection area, and press the right button to complete.



**Figure 3-69 Custom Detection Area**


- Full screen detection

Click  to do full screen detection.



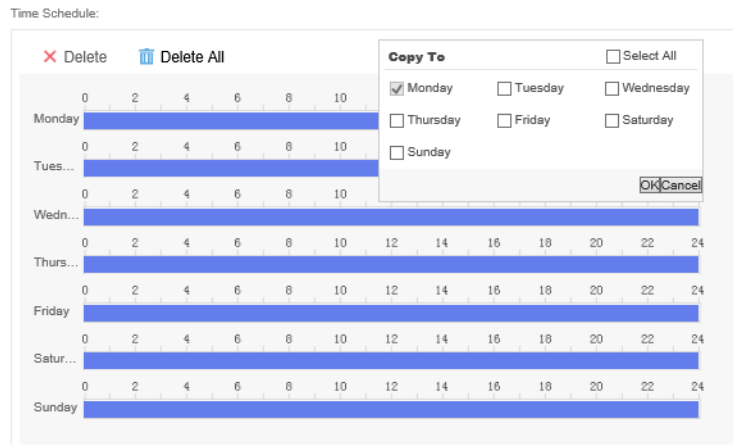
**Figure 3-70 Full Screen Detection**

## Note

Click the drawn graph and then click  to delete the area. The maximum size should be larger than the minimum one.

### 3. Set **Duration**.

### 4. Set detection time schedule, all day by default. Click to apply the settings to other days.



**Figure 3-71 Set Detection Time Schedule**

### 5. Click **Save**.

## 3.4.13 Physical Conflict Detection (Indoor)

Detect the violent motion of people in the scene, such as fight.


### Steps

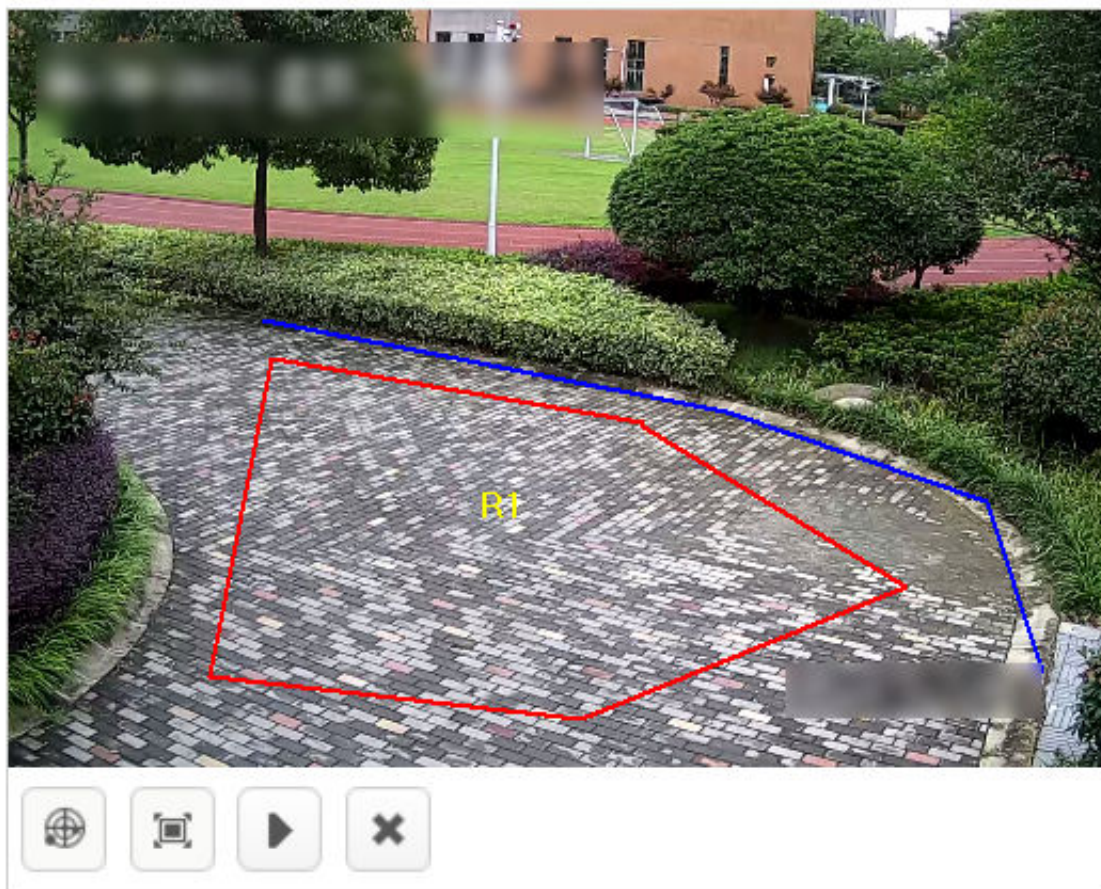
#### 1. Click **Add** to configure rule parameters.

- **Name:** the name of rule. It is recommended that the name of rule be consistent with the name of event.
- **Scene:** select **Indoor**.
- **Event:** select **Physical Conflict Detection (Indoor)**.


#### 2. Draw detection area.

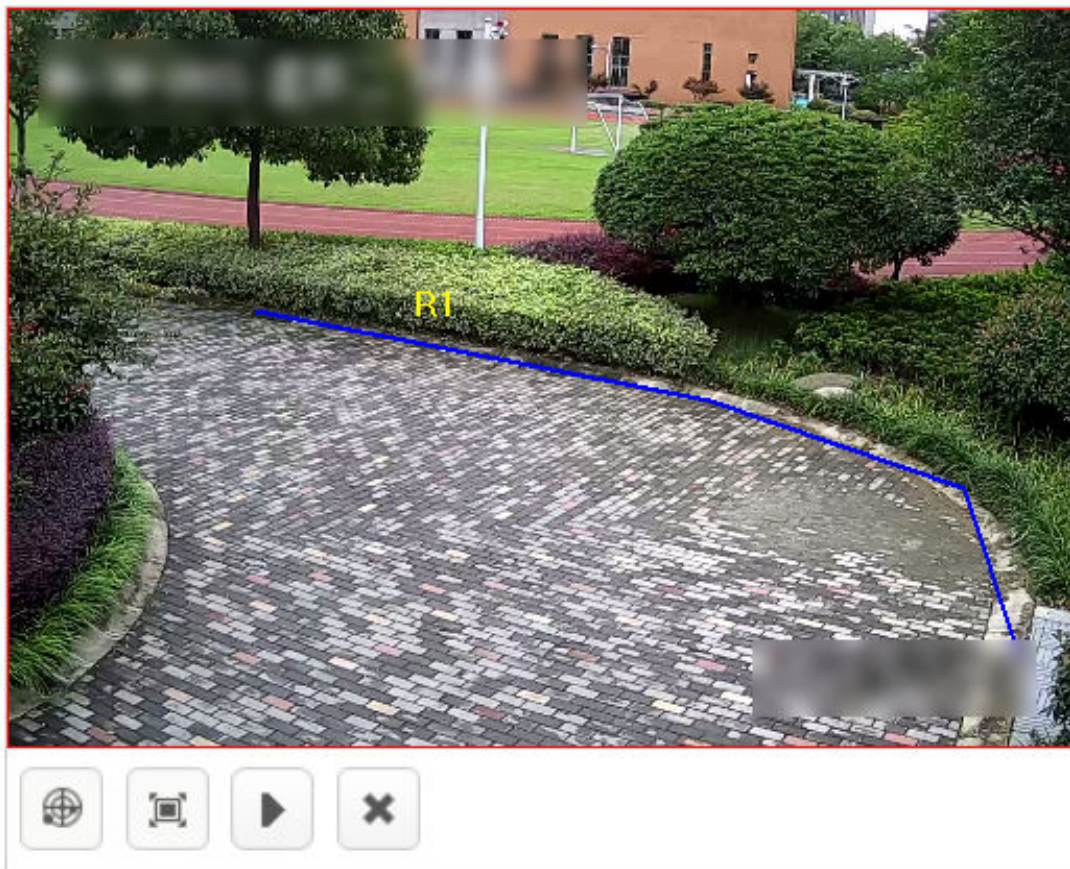
- Custom detection area

Click , press the left mouse button and move the mouse to draw detection area, and press the right button to complete the operation.





**Figure 3-72 Custom Detection Area**

- Full screen detection  
Click  to do full screen detection.




**Figure 3-73 Full Screen Detection**


**3. Optional: Enable Size Filter.** Only targets between the minimum and maximum sizes will be detected.

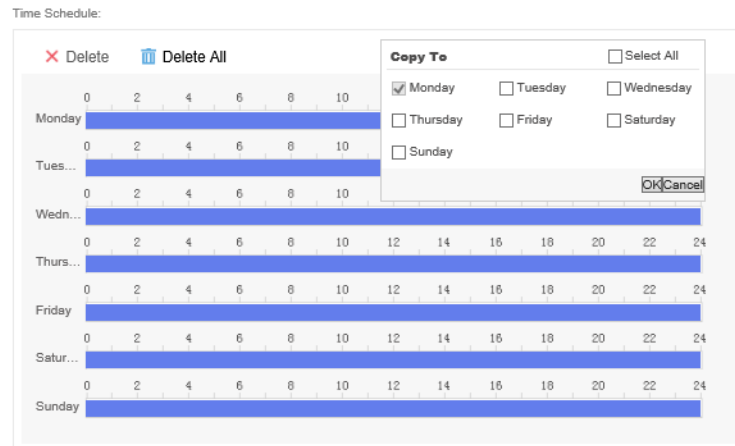
- 1) Click  to draw the maximum size of the target.
- 2) Click  to draw the minimum size of the target.

---

 **Note**

Click the drawn graph and then click  to delete the area. The maximum size should be larger than the minimum one.

- 
- 4. Set sensitivity.** The higher the alarm sensitivity is, the easier an alarm can be triggered.
  - 5. Set detection time schedule,** all day by default. Click  to apply the settings to other days.



**Figure 3-74 Set Detection Time Schedule**

6. Click **Save**.

### 3.4.14 Overstaying Detection

Detect the behavior of staying in the toilet overtime.


#### Steps

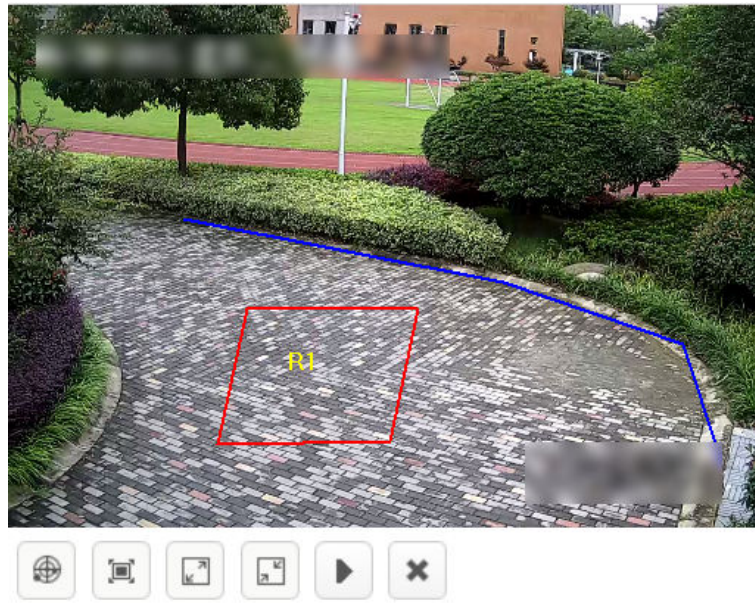
1. Click **Add** to configure rule parameters.

- **Name:** the name of rule. It is recommended that the name of rule be consistent with the name of event.
- **Scene:** select **Indoor**.
- **Event:** select **Overstaying Detection**.


2. Draw detection area.

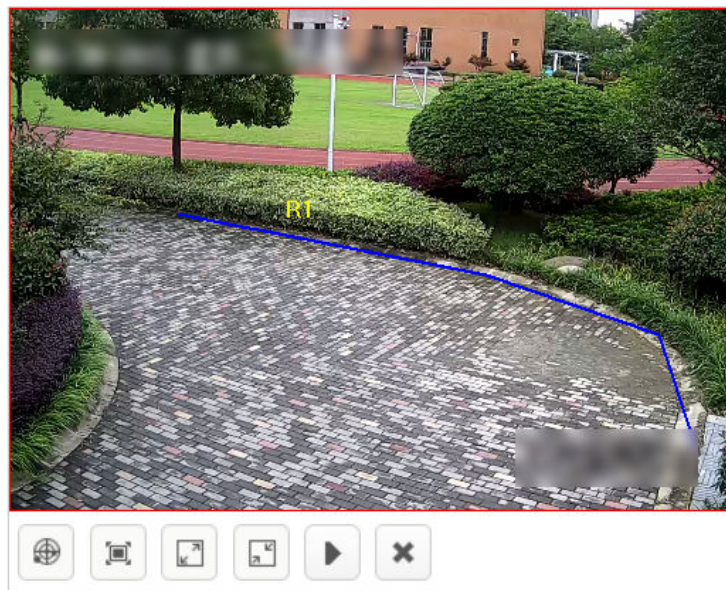
- Custom detection area

Click , press the left mouse button and move the mouse to draw detection area, and press the right button to complete the operation.



**Figure 3-75 Custom Detection Area**

- Full screen detection  
Click  to do full screen detection.



**Figure 3-76 Full Screen Detection**




- 3. Optional: Enable Size Filter.** Only targets between the minimum and maximum sizes will be detected.
- 1) Click  to draw the maximum size of the target.
  - 2) Click  to draw the minimum size of the target.



Figure 3-77 Draw Filter Target

### Note

Click the drawn graph and then click  to delete the area. The maximum size should be larger than the minimum one.

#### 4. Set **Duration**.

#### 5. Set detection time schedule, all day by default. Click to apply the settings to other days.

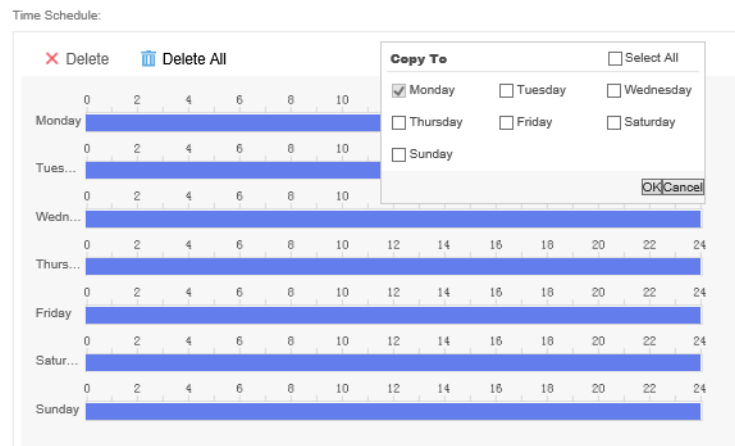


Figure 3-78 Set Detection Time Schedule

#### 6. Click **Save**.

### 3.5 Trend Analysis Task

#### 3.5.1 Create Trend Analysis Task

Create a trend analysis task. Up to 8 detection events can be added for each task.

**Steps**

1. Click **Task Management** → **New** .

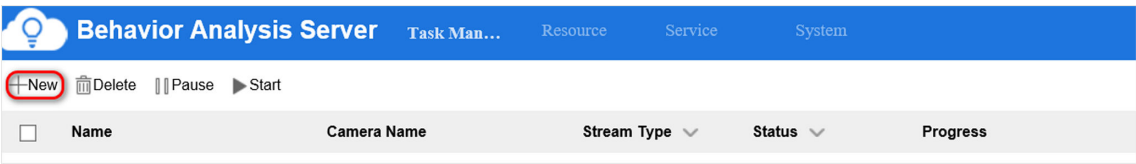


Figure 3-79 Create a New Task

2. Enter a task name.
3. Select the corresponding camera or video recording. Only one camera or video recording is allowed for each task.

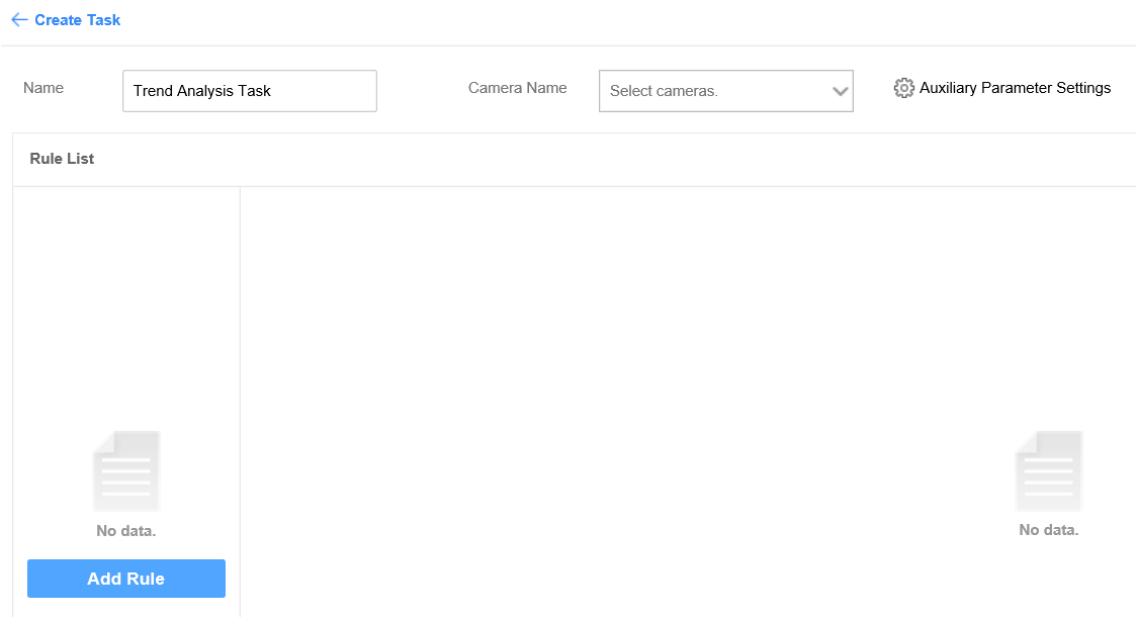


Figure 3-80 Create Task Interface

**Note**

Keep **Auxiliary Parameter Settings** by default.

4. Click **Add Rule** to add related detection events. The rules for configuring different detection events are different. See more details in following sections.

### Note

You can select different scenes in any rules. If multiple scenes are selected in a rule, the analysis tasks of those scenes will be created at the same time.

### 3.5.2 People Density Analysis

Detect the density of people in the area and generate a heat map.


#### Steps

1. Click **Add** to configure rule parameters.

- **Name:** the name of rule. It is recommended that the name of rule be consistent with the name of event.
- **Scene:** select **Trend**.
- **Event:** select **People Density Analysis**.

2. Draw detection area.

- Custom detection area

Click  , press the left mouse button and move the mouse to draw detection area, and press the right button to complete the operation.

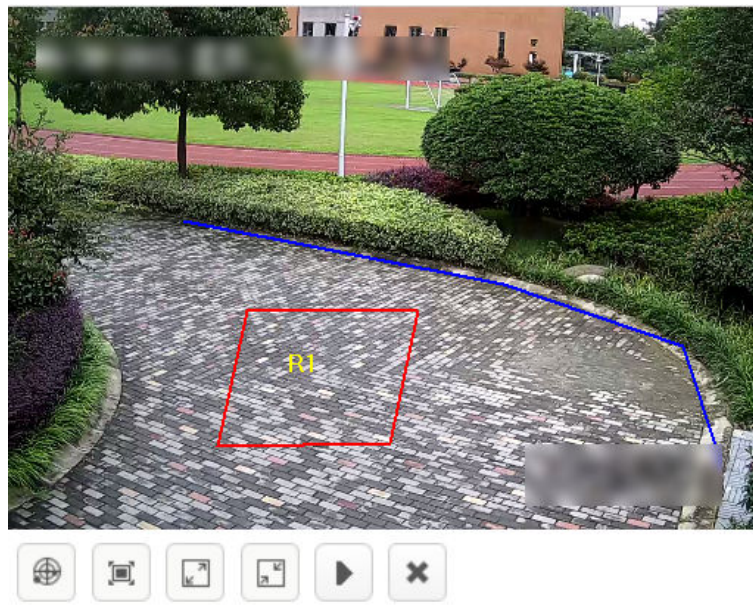

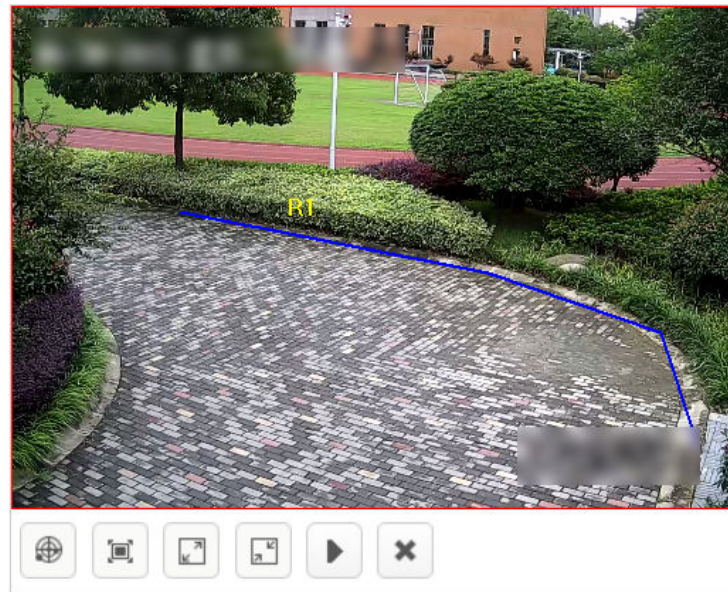


Figure 3-81 Custom Detection Area

- Full screen detection

Click  to do full screen detection.



**Figure 3-82 Full Screen Detection**

### 3. Configure detection parameters in details.

#### **Crowd Density Detection Mode**

- **Default Mode:** applicable to outdoor large area scenes, such as square
- **Detection Mode:** applicable to large area scenes, such as supermarket
- **Density Mode:** applicable to small area scenes, such as meeting room

#### **Analysis Reporting Interval**

the interval of uploading analysis results

#### **Alarm Reporting Interval**

the minimum interval between two alarms

#### **Low Alarm Threshold**

the minimum number of people that triggers the low alarm of people density

#### **Low Alarm Name**

custom name

#### **Medium Alarm Threshold**

the minimum number of people that triggers the medium alarm of people density

#### **Medium Alarm Name**

custom name

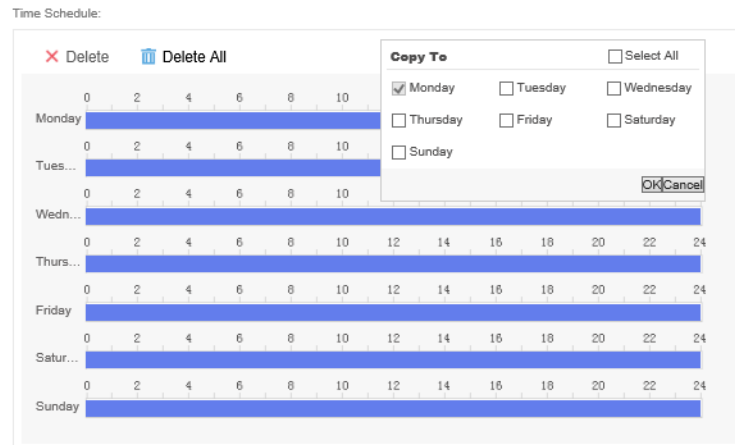
#### **High Alarm Threshold**

the minimum number of people that triggers the high alarm of people density

#### **High Alarm Name**

custom name

4. Set detection time schedule, all day by default. Click  to apply the settings to other days.



**Figure 3-83 Set Detection Time Schedule**


5. Click **Save**.

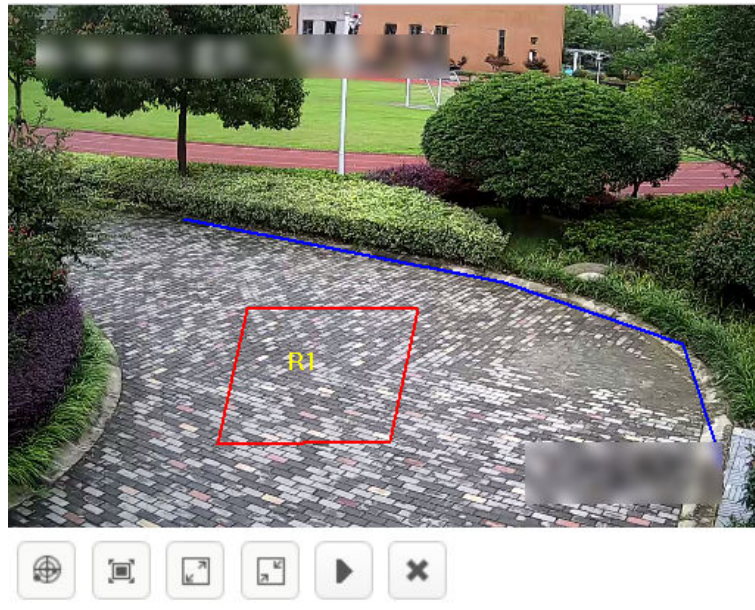
### 3.5.3 Real-time People Counting

Count people in detection area.


#### Steps

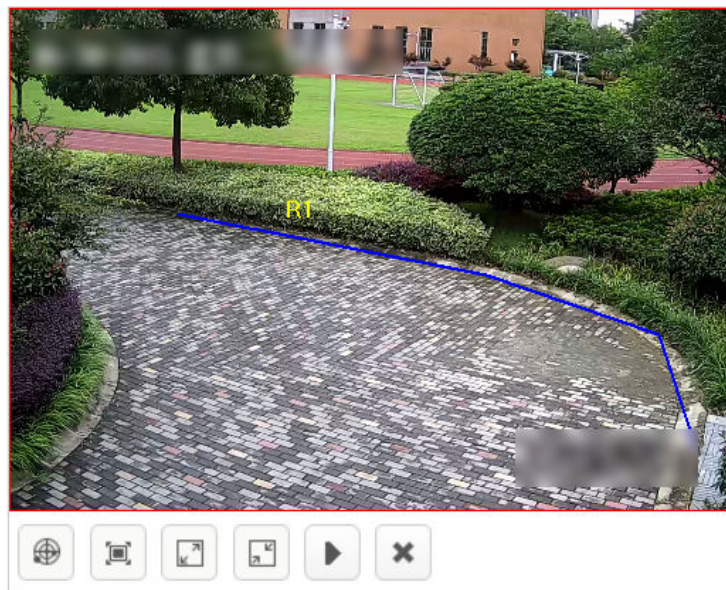
1. Click **Add** to configure rule parameters.
  - **Name**: the name of rule. It is recommended that the name of rule be consistent with the name of event.
  - **Scene**: select **Trend**.
  - **Event**: select **Real-time People Counting**.
2. Draw detection area.
  - Custom detection area

Click , press the left mouse button and move the mouse to draw detection area, and press the right button to complete the operation.




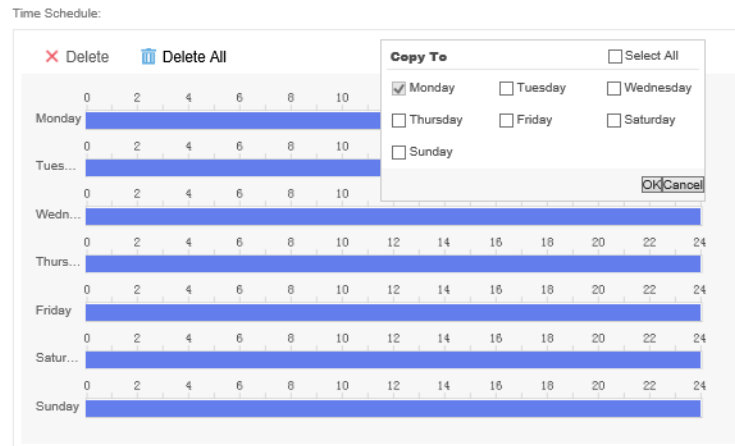
**Figure 3-84 Custom Detection Area**

- Full screen detection  
Click  to do full screen detection.



**Figure 3-85 Full Screen Detection**

3. Set the report interval of number of people in the area.
4. Set detection time schedule, all day by default. Click  to apply the settings to other days.



**Figure 3-86 Set Detection Time Schedule**

5. Click **Save**.

### 3.5.4 People Counting



Count the number of people in the area and report the result by time set.

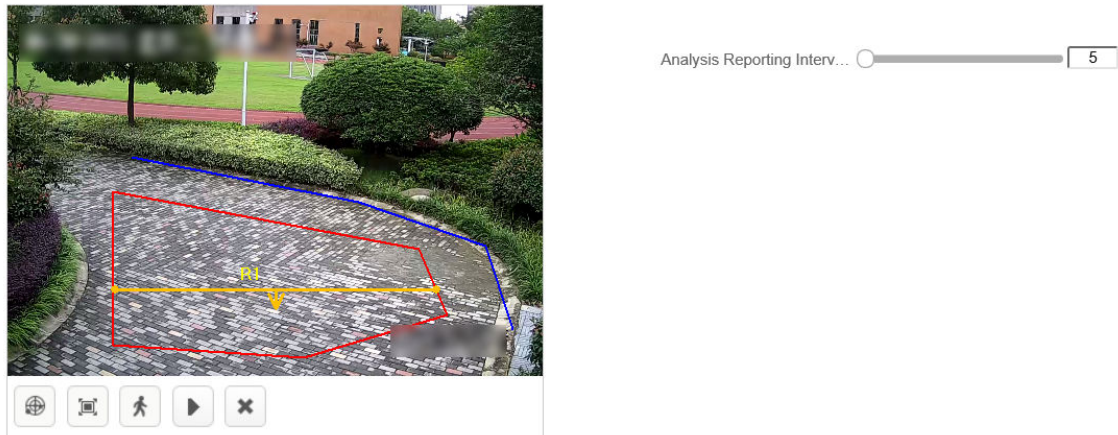
#### Steps

1. Click **Add** to configure rule parameters.



- **Name:** the name of rule. It is recommended that the name of rule be consistent with the name of event.
- **Scene:** select **Trend**.
- **Event:** select **People Counting**.

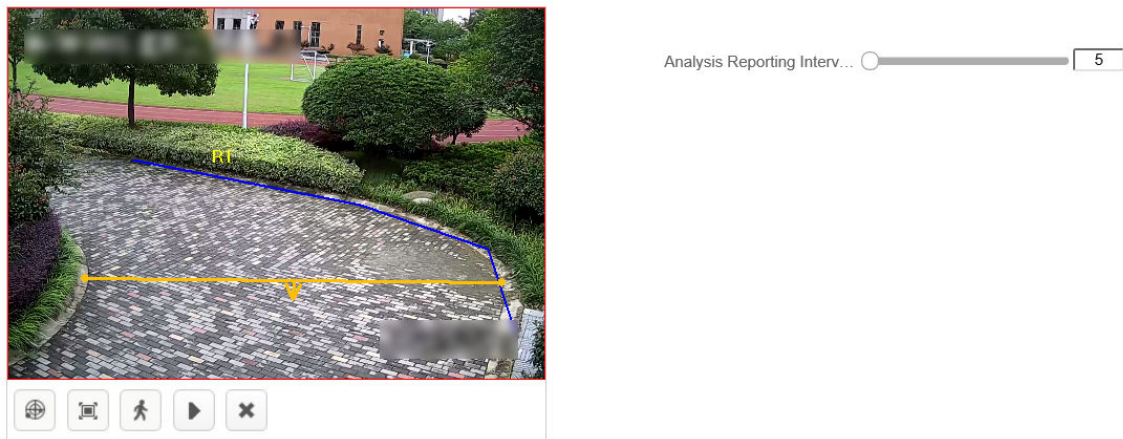
2. Draw detection area and line.

- Custom detection area
  - a. Click  , press the left mouse button and move the mouse to draw detection area, and press the right button to complete the operation.
  - b. Click  to draw a detection line. Move the mouse to the ends of the detection line, press and hold the left mouse button to adjust the position and length of the line.



**Figure 3-87 Custom Detection Area**


- Full screen detection
  - a. Click  to do full screen detection.
  - b. Click  to draw a detection line. Move the mouse to the ends of the detection line, press and hold the left mouse button to adjust the position and length of the line.




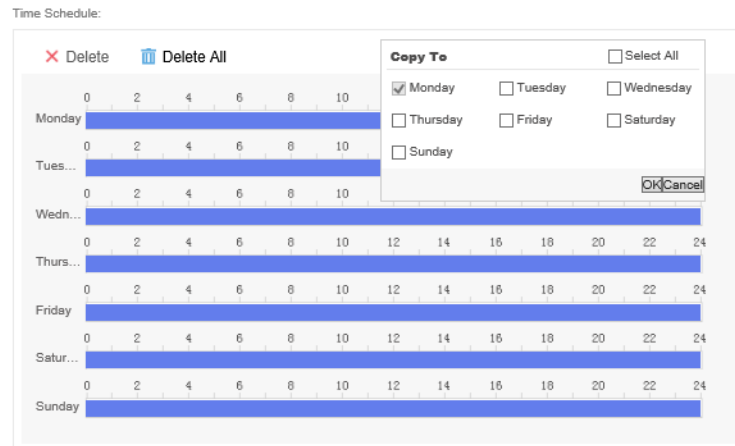
**Figure 3-88 Full Screen Detection**



### Note

Click the drawn graph and then click  to delete the area.

3. Set the report interval of people counting.
4. Set detection time schedule, all day by default. Click  to apply the settings to other days.



**Figure 3-89 Set Detection Time Schedule**

5. Click **Save**.

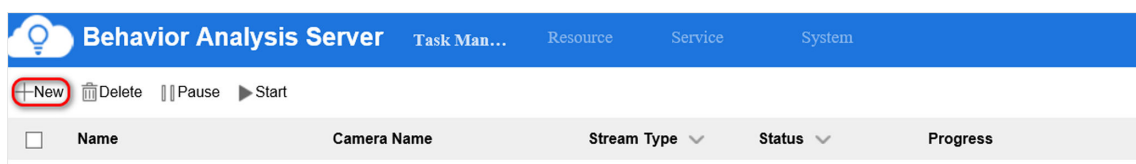
## 3.6 Street Analysis Task

### 3.6.1 Create Street Analysis Task

Create a street analysis task. Up to 8 detection events can be added for each task.

#### Steps

1. Click **Task Management** → **New** .



**Figure 3-90 Create a New Task**

2. Enter a task name.

3. Select the corresponding camera or video recording. Only one camera or video recording is allowed for each task.

[← Create Task](#)

---

Name  Camera Name  Auxiliary Parameter Settings

---

Rule List

 No data. <a href="#">Add Rule</a>	 No data.
--	--------------

**Figure 3-91 Create Task Interface**



### Note

Keep Auxiliary Parameter Settings by default.

4. Click Set Rule to add related detection events. The rules for configuring different detection events are different. See more details in following sections.



### Note

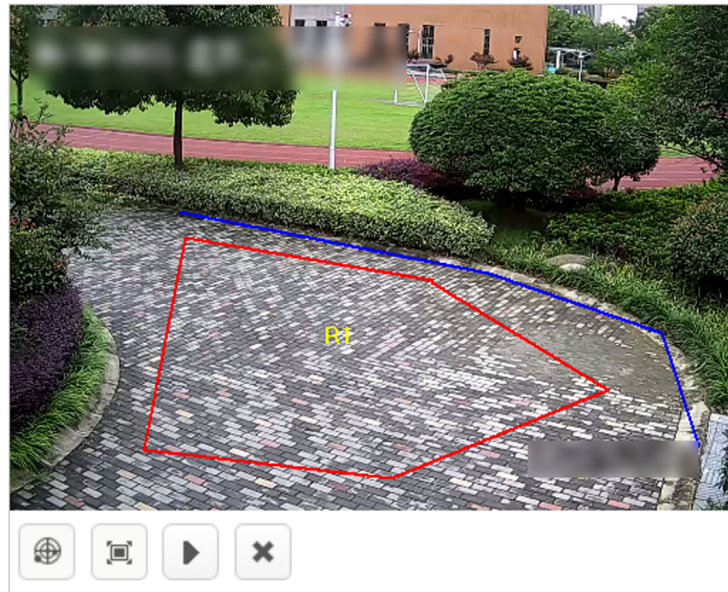
You can select scenes in any rules. If multiple scenes are selected in a rule, the analysis tasks of those scenes will be created at the same time.

### 3.6.2 Falling-down Detection


Detect people in the area who falls down suddenly.

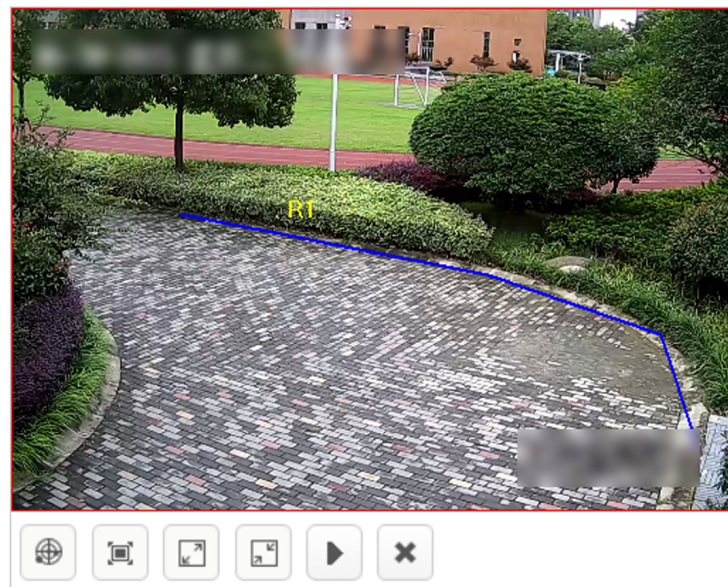
#### Steps

1. Configure rule parameters.
  - **Name:** the name of rule. It is recommended that the name of rule be consistent with the name of event.
  - **Scene:** select **Street**.
  - **Event:** select **Falling-down Detection**.
2. Draw detection area.
  - Click , press the left mouse button and move the mouse to draw detection area, and press the right button to complete the operation.




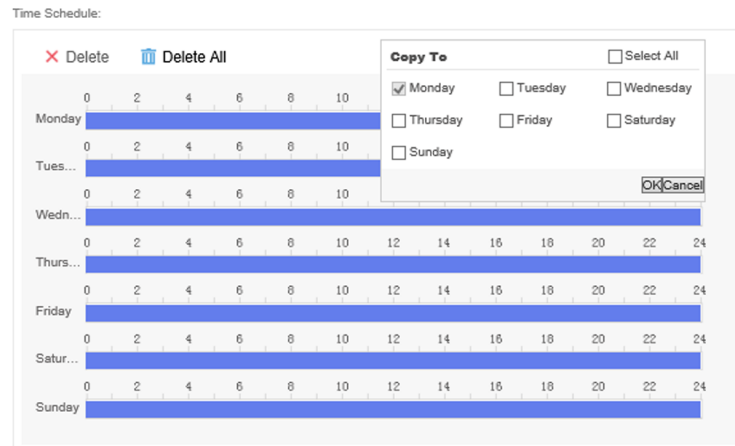
**Figure 3-92 Custom Detection Area**

- Click  to do full screen detection.



**Figure 3-93 Full Screen Detection**

3. Set **Sensitivity**. The higher the alarm sensitivity is, the easier an alarm can be triggered.
4. Set detection time schedule, all day by default. Click  to apply the settings to other days.



**Figure 3-94 Set Detection Time Schedule**

5. Click **Save**.

### 3.6.3 Fast Moving Detection


Detect the fast moving behavior of people in the scene, such as running.

#### Steps

1. Configure rule parameters.


- **Name:** the name of rule. It is recommended that the name of rule be consistent with the name of event.
- **Scene:** select **Street**.
- **Event:** select **Fast Moving Detection**.

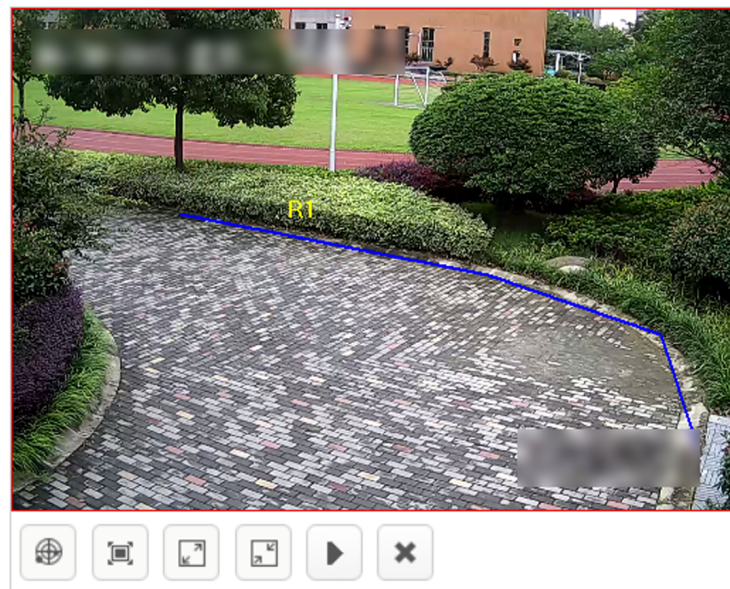
2. Draw detection area.

- Click  , press the left mouse button and move the mouse to draw detection area, and press the right button to complete the operation.




**Figure 3-95 Custom Detection Area**

- Click  to do full screen detection.



**Figure 3-96 Full Screen Detection**

3. Set **Sensitivity** and **Duration**. The higher the alarm sensitivity is, the easier an alarm can be triggered.
4. Set **Running Mode**.
  - Single-person Running: An alarm will be triggered if the fast moving time of a single person exceeds the time set.

- Multiple-person Running: An alarm will be triggered if the fast moving time of multiple persons exceeds the time set.
5. Set detection time schedule, all day by default. Click  to apply the settings to other days.

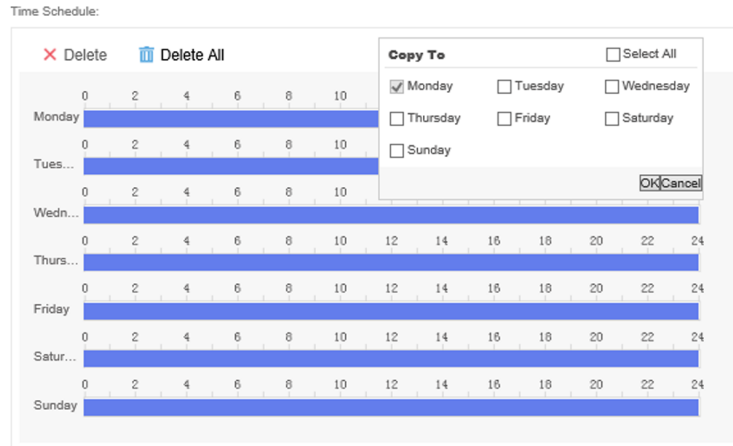



Figure 3-97 Set Detection Time Schedule

6. Click **Save**.

### 3.6.4 Physical Conflict Detection (Street)

Detect the violent motion of people in the scene, such as fight.

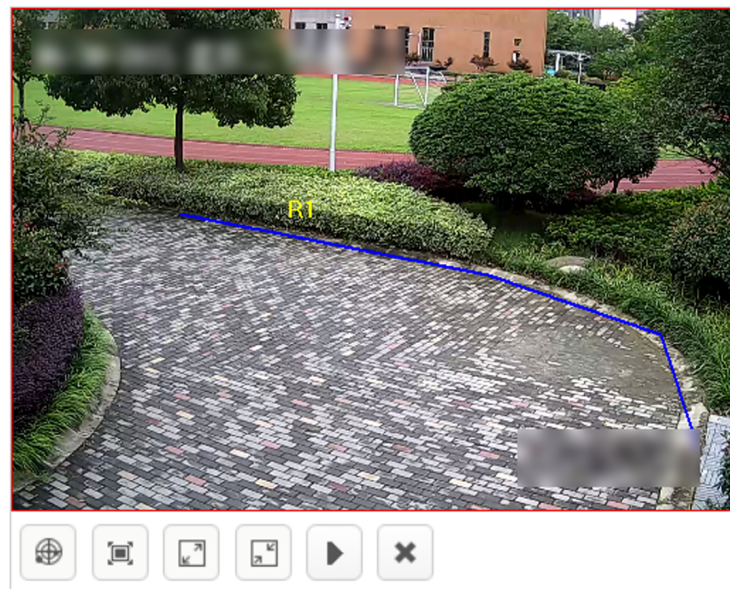
#### Steps

1. Configure rule parameters.
  - **Name:** the name of rule. It is recommended that the name of rule be consistent with the name of event.
  - **Scene:** select **Street**.
  - **Event:** select **Physical Conflict Detection (Street)**.
2. Draw detection area.
  - Click  , press the left mouse button and move the mouse to draw detection area, and press the right button to complete the operation.




**Figure 3-98 Custom Detection Area**

- Click  to do full screen detection.

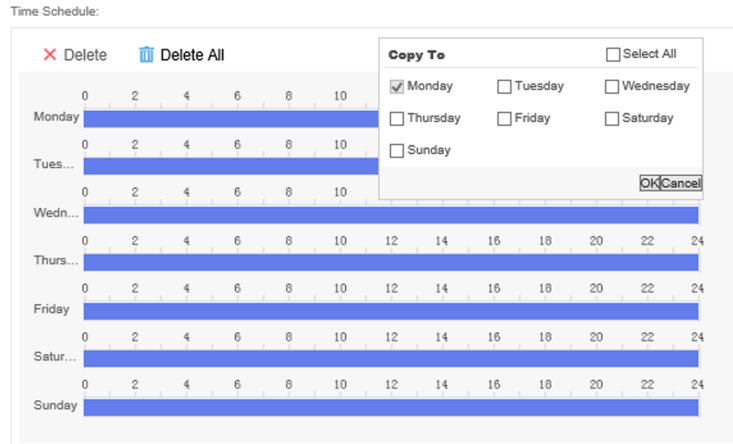


**Figure 3-99 Full Screen Detection**

3. Set **Duration** and **Sensitivity**. The higher the alarm sensitivity is, the easier an alarm can be triggered.
4. Set **Detection Mode** and **Alarm Interval**.
  - Alarm Mode: default value.
  - Alarm Interval: the minimum interval between two alarms.

5. Set detection time schedule, all day by default. Click  to apply the settings to other days.

Time Schedule:



**Figure 3-100 Set Detection Time Schedule**

6. Click **Save**.

### 3.6.5 People Gathering Detection


Detect gathering behavior of people in street scene.

#### Steps

1. Configure rule parameters.


- **Name:** the name of rule. It is recommended that the name of rule be consistent with the name of event.
- **Scene:** select **Street**.
- **Event:** select **People Gathering Detection**.

2. Draw detection area.

- Click  , press the left mouse button and move the mouse to draw detection area, and press the right button to complete the operation.




**Figure 3-101 Custom Detection Area**

- Click  to do full screen detection.

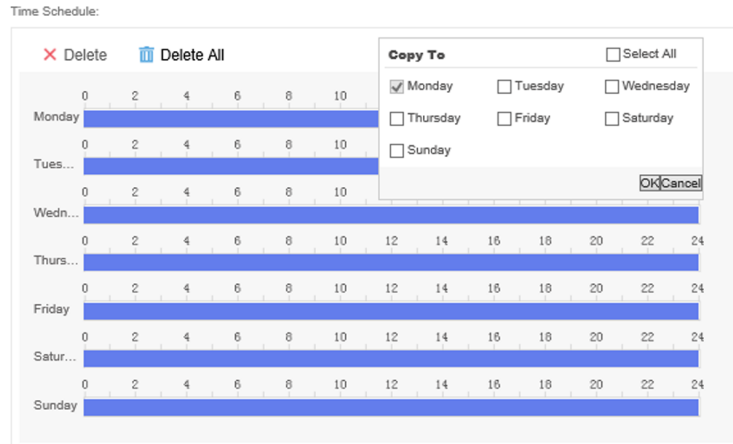


**Figure 3-102 Full Screen Detection**

3. Set **Sensitivity** and **Duration**. The higher the alarm sensitivity is, the easier an alarm can be triggered.
4. Set the alarm interval and minimum number of people.
  - Alarm Interval(s): the minimum interval between two alarms
  - Min. People: the minimum number of gathering people

5. Set detection time schedule, all day by default. Click  to apply the settings to other days.

Time Schedule:



× Delete Delete All

Copy To ☐ Select All

☒ Monday ☐ Tuesday ☐ Wednesday

☐ Thursday ☐ Friday ☐ Saturday

☐ Sunday

Ok Cancel

**Figure 3-103 Set Detection Time Schedule**

6. Click **Save**.

## 3.7 Task Management

### 3.7.1 Configure Task

Configure the established detection rule or add a new one.

#### Steps

1. Click **Task Management**, select a task and click the name.

New

Delete

Pause

Start

<input type="checkbox"/>	Name	Camera Name	Stream Type ▾	Status ▾
<input type="checkbox"/>	Rule1-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule2-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule3-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule4-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule5-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule6-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule7-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule8-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule9-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule10-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule11-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule12-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule13-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule14-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule15-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule16-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule17-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule18-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule19-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule20-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule21-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule22-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule23-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule24-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule25-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule26-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule27-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule28-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule29-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule30-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule31-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule32-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule33-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule34-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule35-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule36-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule37-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule38-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule39-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule40-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule41-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule42-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule43-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule44-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule45-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule46-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule47-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule48-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule49-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule50-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule51-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule52-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule53-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule54-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule55-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule56-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule57-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule58-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule59-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule60-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule61-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule62-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule63-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule64-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule65-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule66-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule67-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule68-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule69-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule70-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule71-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule72-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule73-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule74-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule75-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule76-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule77-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule78-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule79-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule80-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule81-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule82-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule83-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule84-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule85-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule86-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule87-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule88-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule89-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule90-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule91-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule92-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule93-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule94-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule95-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule96-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule97-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule98-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule99-Perimeter	38_IpCamera_1	Real Time	Complete
<input type="checkbox"/>	Rule100-Perimeter	38_IpCamera_1	Real Time	Complete

Figure 3-104 Task Management Interface

 **Note**

Move your mouse to **Stream Type** or **Status** to filter tasks.

2. Click rule name in **Rule List**, configure detection rules according to actual needs.

← Edit Task

Name

Rule1-Perimeter

Camera Name

38\_IpCamera\_1

Auxiliary Parameter Settings

Rule List

+ Add

Rule1

Perimeter

Name

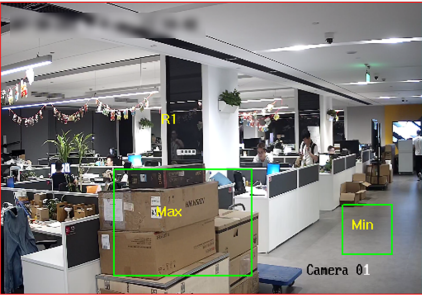
Rule1

Scene

Perimeter

Event

Object Removal Detection



Enable Size Filter

Sensitivity

50

Duration (s)

2

Figure 3-105 Configure Detection Rules

77

3. Click **Add** to add new detection rules.

### 3.7.2 Delete Task

Delete a task which is completed or no longer needs to be analyzed.

#### Steps

1. Click **Task Management**, and select the task to be deleted.
2. Click **Delete**, and click **OK** in the popped up box.

### 3.7.3 Pause Task

Pause a task which is being analyzed.

#### Steps

1. Click **Task Management**, and select the task to be paused.
2. Click **Pause**.

### 3.7.4 Start Task

Continue to analysis a task which was paused.

#### Steps

1. Click **Task Management**, and select the paused task.
2. Click **Start**.

## Chapter 4 Smart Analysis Unit Management

### 4.1 Add Smart Analysis Unit to Cluster

Add new smart analysis unit(s) into cluster to enhance analysis capacity.

#### Before You Start

Smart unit(s) has been added.

#### Steps

1. Go to **Service → Smart Unit**.
2. Check the desired smart unit(s).
3. Click **Add to Cluster**.
4. Click **OK** to add the new smart analysis unit into cluster.

### 4.2 Remove Computing Node from Cluster

Remove computing node(s) from cluster.

#### Before You Start

Smart analysis unit(s) is online.

#### Steps

1. Go to **Service → Smart Unit**.
2. Check the desired node(s).
3. Click **Remove From Cluster**.
4. Click **OK**.

### 4.3 Restart Smart Analysis Unit

#### Before You Start

Smart analysis unit(s) is online.

#### Steps

1. Click **Service → Smart Unit**.
2. Check smart analysis unit to be restarted.
3. Click **Restart**.
4. Click **OK**.

## 4.4 Power Off Smart Analysis Unit

### Before You Start

Smart analysis unit(s) is online.

### Steps

1. Go to **Service → Smart Unit** .
2. Check the desired smart analysis unit(s).
3. Click **OFF**.
4. Click **OK**.



### Note

Press the power button to turn the device on after the smart analysis unit is powered off.

---

## 4.5 Delete Smart Analysis Unit

A smart analysis unit can only be added to one node. You need to delete an analysis unit from a node before add it to another one.

### Steps



### Caution

If an offline smart analysis unit is deleted, it can only be added to the latest one node who just added it.

---

1. Go to **Service → Smart Unit** .
2. Check the desired smart unit(s).
3. Click **Delete**.
4. Click **OK**.

## 4.6 Configure Network Parameters

Configure the network parameters of smart analysis unit(s) through IE browser.

### Before You Start

Ensure that the desired device connects to the network cable.

### Steps

1. Go to **Service → Smart Unit** , and then click on the name of smart analysis unit.

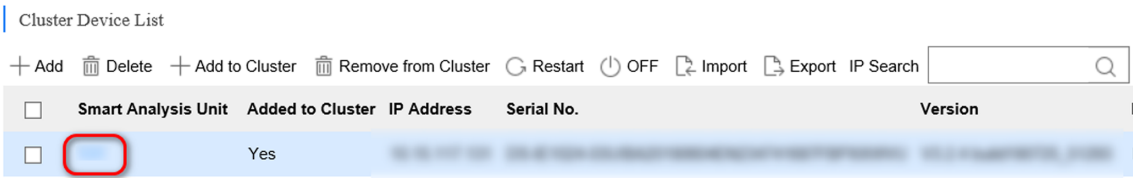


Figure 4-1 Cluster Device List

2. Click **Network Configuration**. Edit network parameters as needed.

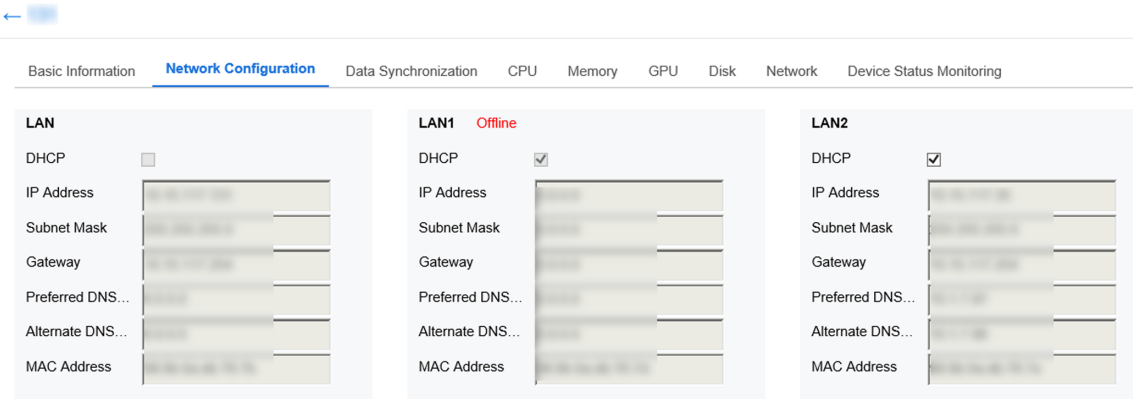


Figure 4-2 Edit Network Parameters

 **Note**

- Master or back-up node(s), which is added to cluster, is not allowed to be configured.
- Re-add the smart analysis unit(s) after its parameters changed.

3. Click **OK**.


### 4.7 Enable UID Indicator

Enable UID indicator to locate the sever quickly.

**Steps**

1. Go to **Task Management → Smart Unit** .
2. Click  in the list of **UID Indicator**.

 **Note**

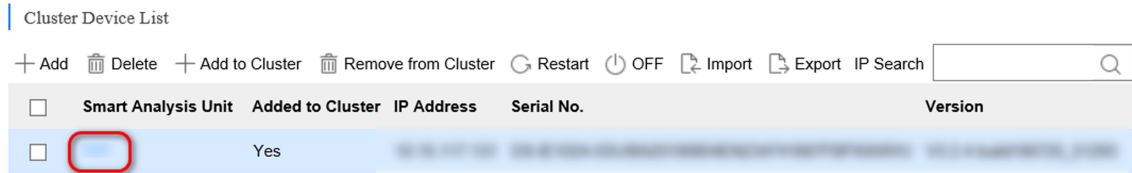
Click  again to close the indicator.

### 4.8 View Hardware Resource

View detailed information such as CPU, memory, GPU and Disk Usage, etc.

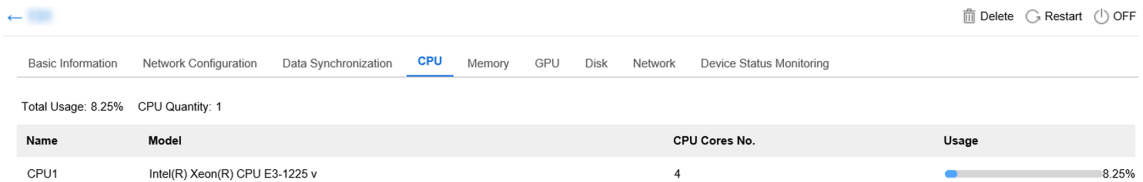
## Steps

1. Go to **Service** → **Smart Unit** , and then click the name of smart analysis unit.



**Figure 4-3 Cluster Device List**

2. Click different tabs to view the usage of hardware.



**Figure 4-4 View Hardware Resource**

## Chapter 5 System Management

### 5.1 Basic Configuration

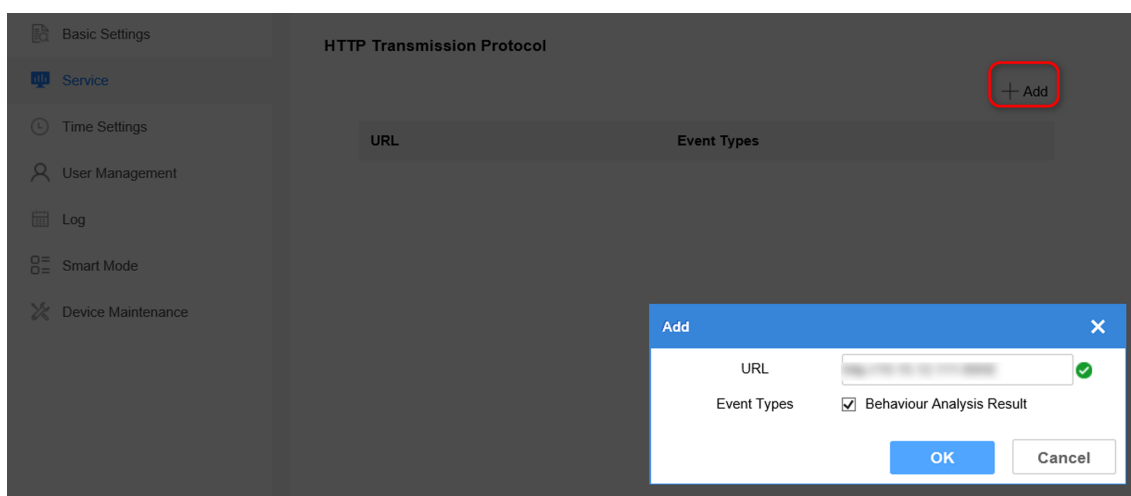
The local filter function is enabled by default. In default status, the device can only be accessed via the IP address of itself. Disable local filter to access the device if port mapping is enabled.

### 5.2 Service Configuration

The results of task analysis can be uploaded to a third party device.

#### Steps

1. Click **System** → **Service** , and then click **Add**.



**Figure 5-1 Service Configuration Interface**

2. Configure the receiving address of the third party device.



#### Note

Send task analysis results to the configured address via HTTP transmission protocol.

---

3. Click **OK**.

### 5.3 Time Configuration

Enable time sync as required. System time can be set by NTP sync or manually synchronization.

#### Before You Start

Obtain the IP address and port information of the NTP server for NTP sync.

## Steps

1. Go to **System** → **Time Settings** .

### Time Settings

Time Zone	(GMT+08:00) Beijing, Urumqi, Singapore ▼
Device Time	<input type="text"/>
NTP Method	<input type="radio"/> NTP <input checked="" type="radio"/> Manual Time Sync.
Set Time	<input type="text"/> <input type="button" value="Calendar"/> <input type="checkbox"/> Sync. with computer time

Figure 5-2 Time Configuration Interface

2. Select **NTP** or **Manual Time Sync.** as needed.

### Note

If **Sync. with computer time** is checked, the device time will be synchronized with the computer.

3. Click **Save**.

## 5.4 User Management

The system enabled an admin user by default. Only the admin user can add, delete users and modify user passwords. User types include administrators, operators, consumers. Operators and consumers can only modify their own passwords.

### 5.4.1 Add User

Up to 31 users can be added.

## Steps

1. Go to **System** → **User Management** .
2. Click **Add** and enter user information.

Add user

×

User Information

User Name

Level

Operator

▼

Admin Password

Password

Valid password range [8-32]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained. The username cannot be the same as the password. Password cannot be inverted write of user name.

Password Confirm

OK

Cancel

**Figure 5-3 Add User**



### Note

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

3. Click **OK** to complete the operation.

### 5.4.2 Modify Password

#### Steps

1. Go to **System → User Management**.
2. Click the user name, and then click **Modify**.
3. Enter the admin password and new password, and then confirm your new password.
4. Click **OK**.

### 5.4.3 Delete User

The default user admin cannot be deleted.

### Steps

1. Go to **System → User Management** .
2. Click the user name line, click **Delete**.
3. Click **OK** and enter admin password. Click **OK** again.



### Note

Clearing user resource means deleting the device added by the user. If the user is deleted with the resource remained, the device added by the user will be moved to the administrator.

---


## 5.5 Log Management

### 5.5.1 Search Log

The system log includes running log, alarm log, and operation log. Searching and exporting logs are allowed.

- Running Log: Record the completion and failure information of detection event.
- Operation Log: Record the operation information of Web interface.
- Alarm Log: Record error and alarm information of device.

### Steps

1. Go to **System → Log** .
2. Select the type of log.
3. Set the starting and ending time of search.
4. Click  , and corresponding log information will be displayed.
5. **Optional:** Click **Export**, and click **OK** in the popped up box to export desired log(s).

### 5.5.2 Download Maintenance Log

Maintenance log is used by professional maintainer to maintain device.

### Steps

1. Go to **System → Device Maintenance** .
2. Click **Download Maintenance Log**, and click **OK** in the popped up box.



### Note

It may take a few minutes to export maintenance log(s). Please wait and select the save path as needed.

---



4. Click **Upgrade** after the file is uploaded.

5. Click **OK** to start upgrading.



### Note

The device will restart automatically after upgrading completed.

---

## 5.8 Restore Defaults

Restore defaults includes Restore and Default.

### Before You Start

Ensure that the cluster has been disbanded.

- Restore: Restore all parameters, except IP address and user information, to default settings. The device will restart automatically and it is required to re-activate.
- Default: Restore all parameters to default settings. The device will restart automatically and it is required to re-activate.

### Steps



### Note

This operation is not allowed in Multi-smart Mode. Switch to Single Smart Mode first.

---

1. Go to **System → Device Maintenance**.
2. Select **Restore** or **Default** as needed.

## 5.9 Help Center

Refer to the help document by going to **Help → Help Document** on the upper-right corner of the interface to view or download the document.

## 5.10 Version Information

Check version information of different modules by going to **Help → Version** on the upper-right corner of the interface.

## 5.11 Logout

### Steps

1. Go to **admin → Logout** on the upper-right corner of the interface.
2. Click **OK**.

## 5.12 Obtain Guarding Vision Client Software

In this device, Guarding Vision Client Software refers to 4200 Client Software.

### Steps

1. Click **4200 Download** at the top-right corner of the interface to download Guarding Vision Client Software.
2. Install Guarding Vision Client Software.

## Chapter 6 Guarding Vision Client Configuration

Accessing to the server via Guarding Vision Client (client for short) is allowed.

### Note

The client software interface updates from time to time. Please refer to the actual interface display.

### 6.1 Log in

#### Before You Start

You have obtained and installed Guarding Vision client software.

#### Steps

1. Open the client. Create a super user when enable the client for the first time. Enter super user name and password. Click **Log in**.

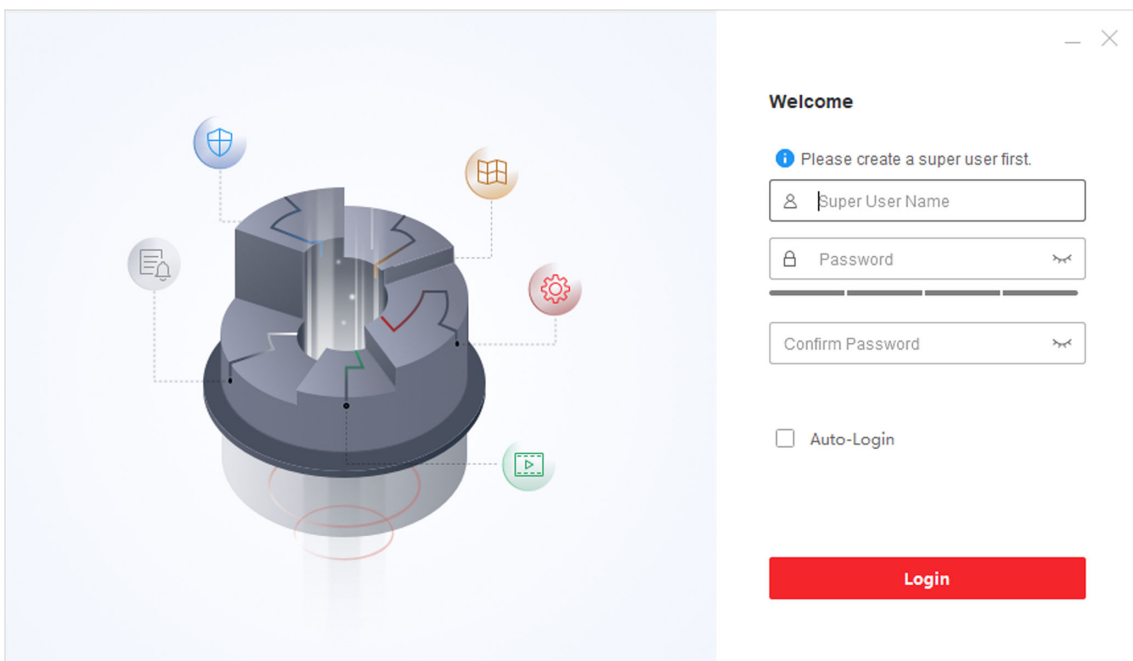


Figure 6-1 Create Super User

### Note

- Special characters V:\*?"<>| are not allowed in user name.
- 8 to 16 characters allowed, including at least 2 of the following types: digits, lower-case letters, upper-case letters and special characters. Password cannot be the same as or opposite to the user name.

- 2. Optional:** Check **Enable Auto-login**. The current user will log in automatically next time.
- 3.** Set three security questions and answers for finding your password.

## 6.2 Add Server

Add the server to the client for management after login.

### 6.2.1 Add Server Manually

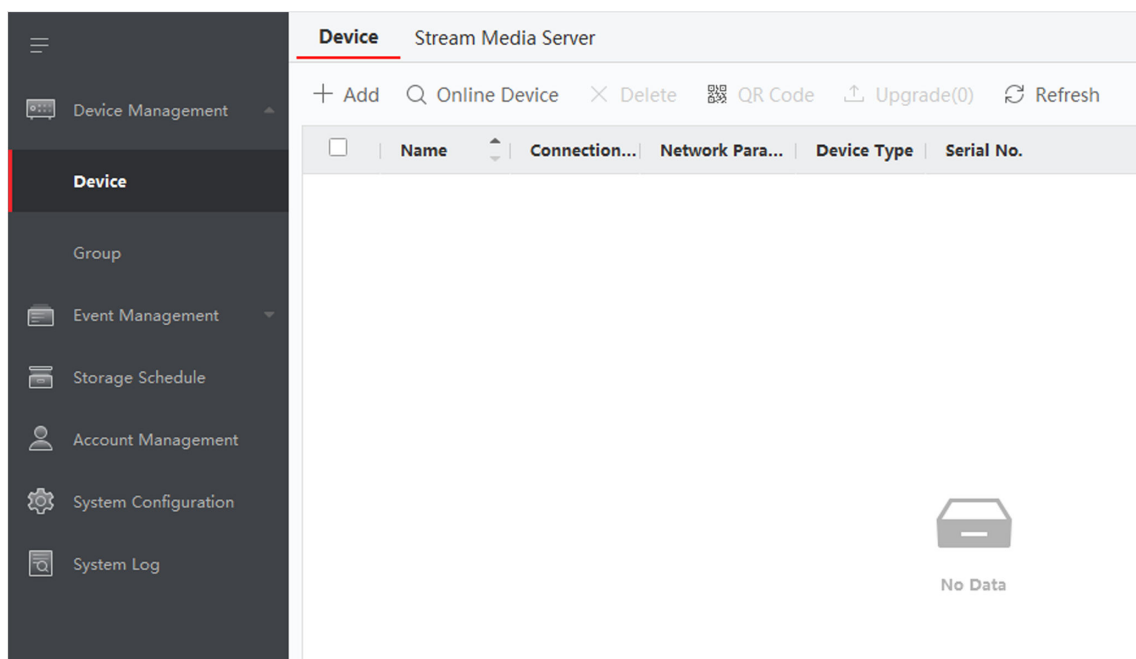
Enter the server IP address to add a server.

#### Before You Start

You have obtained the IP address, user name and login password of the server.

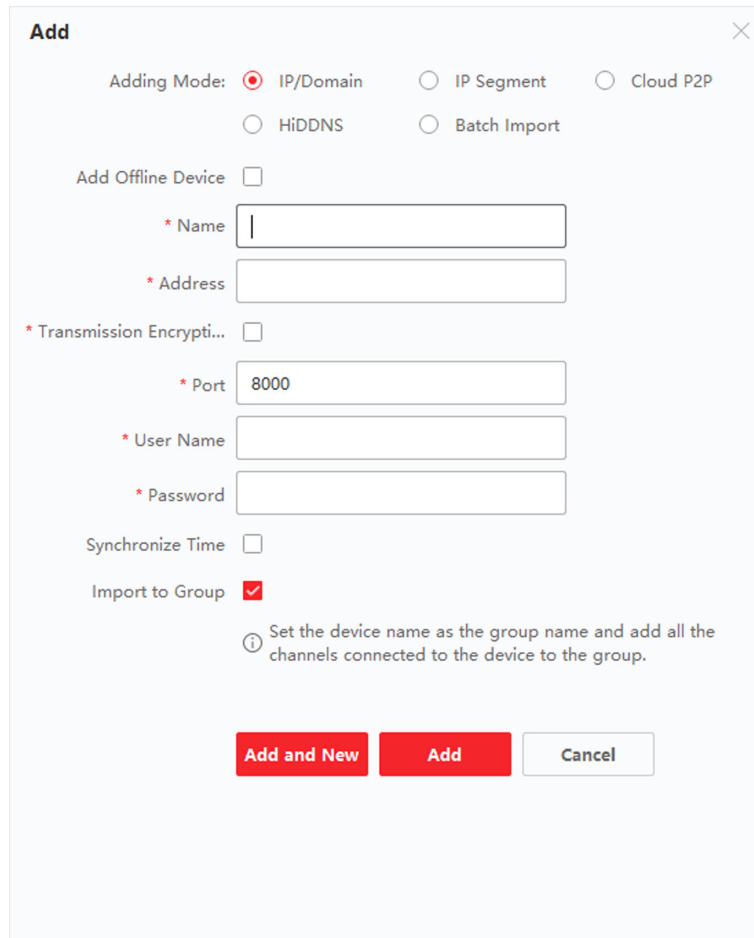
#### Steps

- Go to **Maintenance and Management → Device**.
- Click **Add**.



**Figure 6-2 Add Device Manually**

- 3.** Select **IP/Domain** as **Adding Mode**, and Enter **Name**, **IP Address**, **User Name** and **Password** in the pop-up window.



The 'Add' dialog box contains the following fields and options:

- Adding Mode:** Radio buttons for **IP/Domain** (selected), **IP Segment**, **Cloud P2P**, **HiDDNS**, and **Batch Import**.
- Add Offline Device:** A checkbox that is currently unchecked.
- \* Name:** A text input field.
- \* Address:** A text input field.
- \* Transmission Encrypti...:** A checkbox that is currently unchecked.
- \* Port:** A text input field containing the value '8000'.
- \* User Name:** A text input field.
- \* Password:** A text input field.
- Synchronize Time:** A checkbox that is currently unchecked.
- Import to Group:** A checkbox that is checked, accompanied by an information icon and the text: 'Set the device name as the group name and add all the channels connected to the device to the group.'
- Buttons:** 'Add and New' (red), 'Add' (red), and 'Cancel' (white with gray border).

**Figure 6-3 Configure Device Parameters**

**4. Click Add.**



Check **Import to Group** to add all server channels to the group named by the server alias.

---

### 6.2.2 Add Online Server

Online adding is applicable to adding devices that are on the same network segment as the client software.

#### Before You Start

The desired server has been in the online device list.

#### Steps

1. Go to **Maintenance and Management** → **Device** .
2. Click **Online Device** and check the desired device.

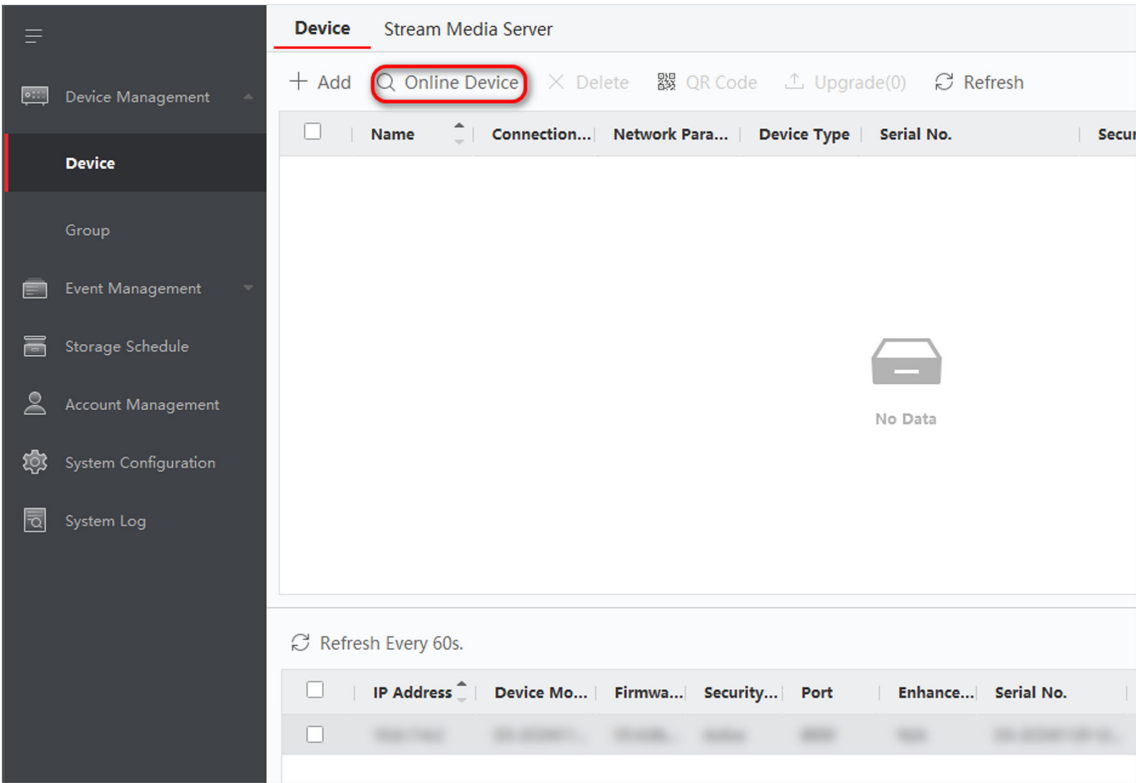


Figure 6-4 Add Online Device

- 3. Enter **Name**, **User Name** and **Password** in the pop-up window.
- 4. Click **Add**.

 **Note**

If multiple servers are selected at the same time, the software will add those servers with the same user name and password and use the server's IP address as the server name.


6.3 Live View

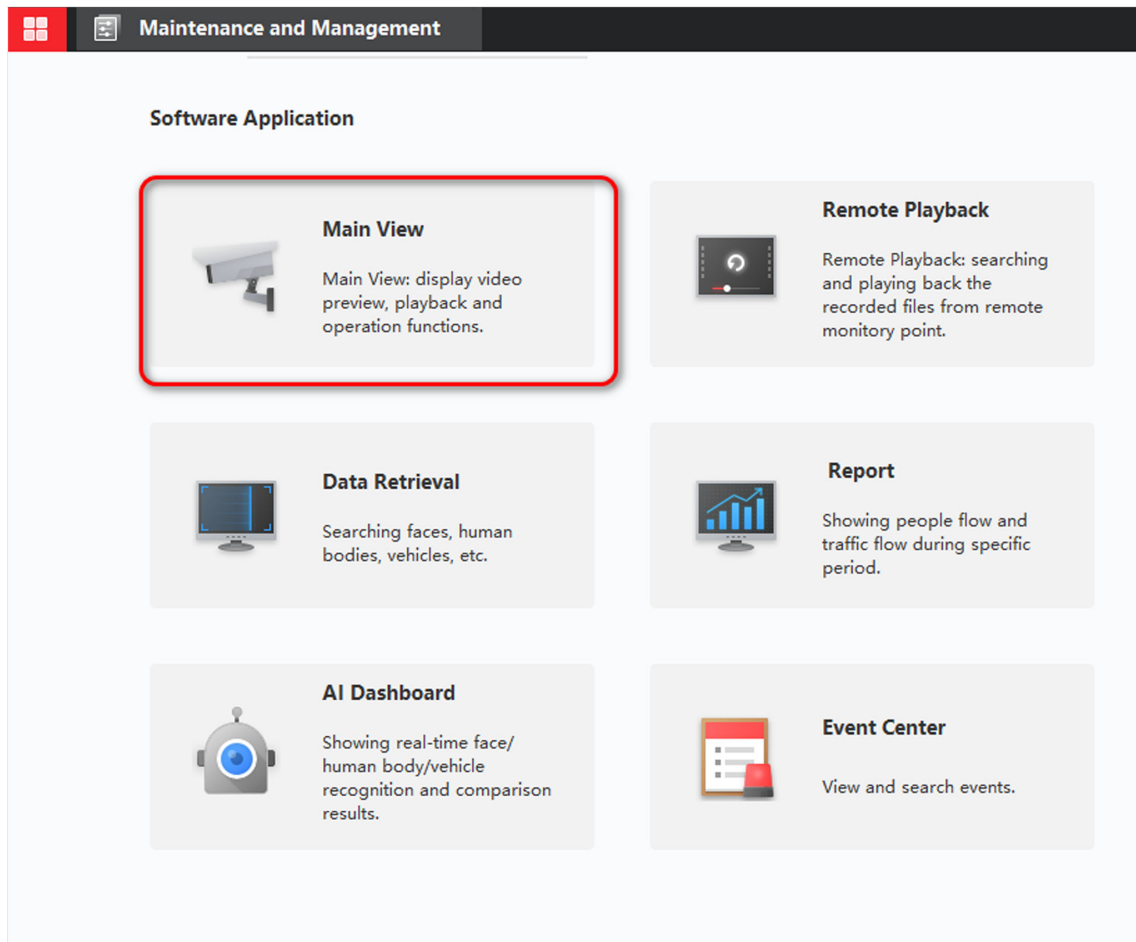
View the real-time video frame and analysis results of tasks.

6.3.1 View Analysis Task Frame

View the video frame of analysis task.

Steps

- 1. Click  → **Main View** .



**Figure 6-5 Click Main View**

2. To view the real-time frame of the video , you can press the left button of mouse and drag the desired task to the playing window, or select a playing window and then double-click the desired task.

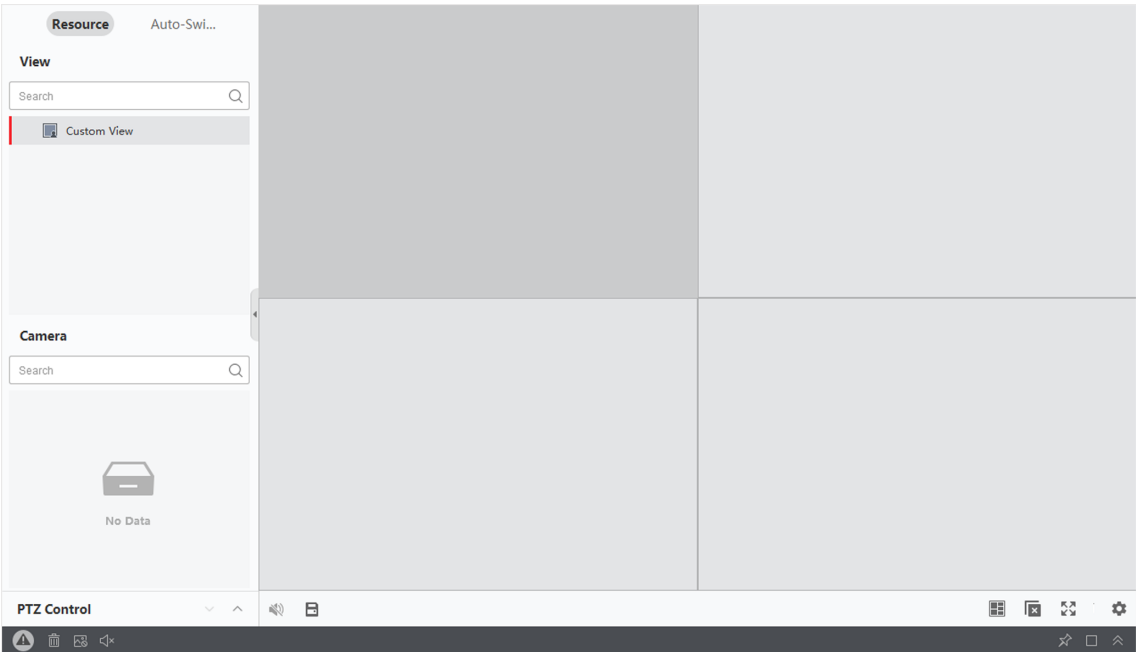







Figure 6-6 Main View Interface

 **Note**

Select a group to drag directly to any position on the right window, or double-click the group to preview all the tasks in the group.

Table 6-1 Operation Description

Operation	Description
	Capture
	Start to record
	Switch to real-time playback
	Close current live view window
	Stop all live views

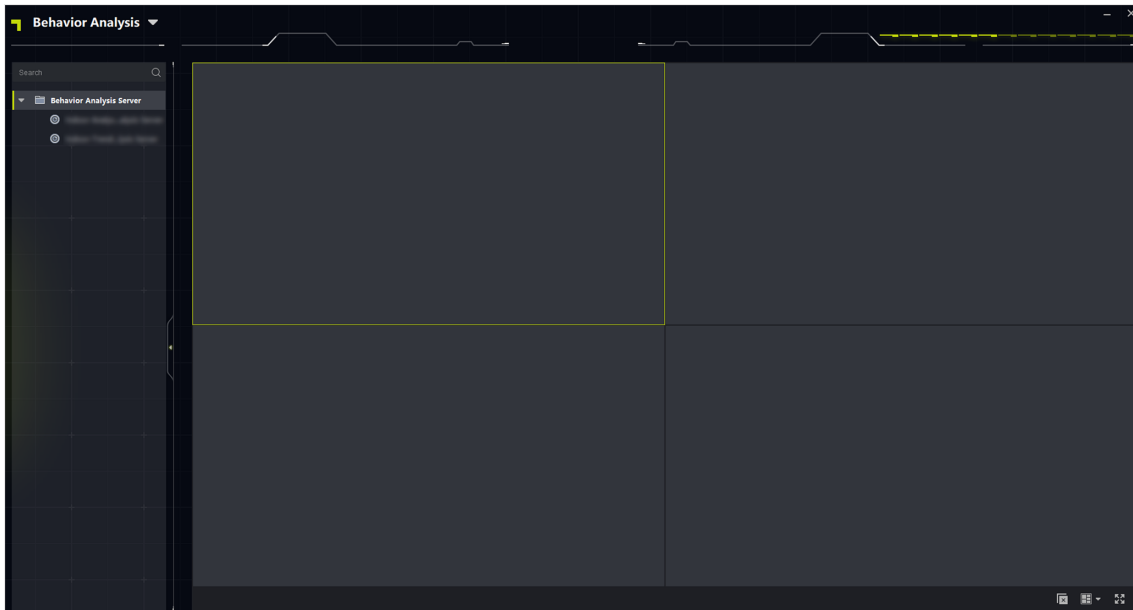
6.3.2 View Task Analysis Results(Trend Scene Only)

View the real-time analysis results of tasks in trend scene. For example, the window of People Counting task can show how many people entered and exited in the duration.

Steps

1. Click  → AI Dashboard → Behavior Analysis .

2. To view the real-time frame of the video , you can press the left button of mouse and drag the desired task to the playing window, or select a playing window and then double-click the desired task.





**Figure 6-7 View Real-time Analysis Results**

### **Note**

Select a group to drag directly to any position on the right window, or double-click the group to preview all the tasks in the group.

**Table 6-2 Operation Description**

Operation	Description
	Close current live view window
	Stop all live views


### **Note**

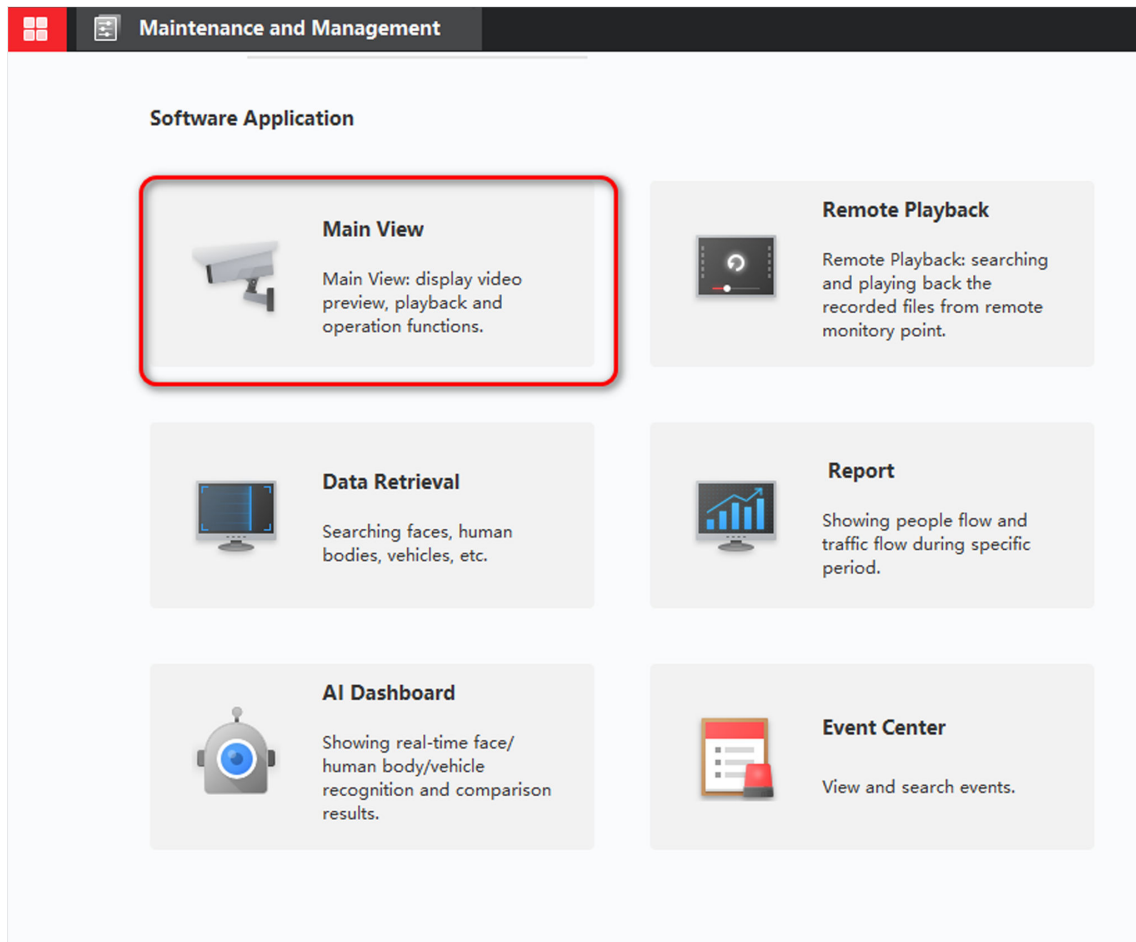
- People counting task shows the number of people entered and exited in a time period.
- Real-time people counting task shows the current number of people in detection area.
- People density analysis task shows the line chart and heat map generated in a time period.

## 6.4 Remote Configuration

The client allows remote configuration of the server, including adding, editing, deleting and pausing the analysis tasks.

### Steps

1. Click  → **Main View** .



**Figure 6-8 Click Main View**

2. Select a task and click  → **Remote Configuration** → **Basic Settings** .

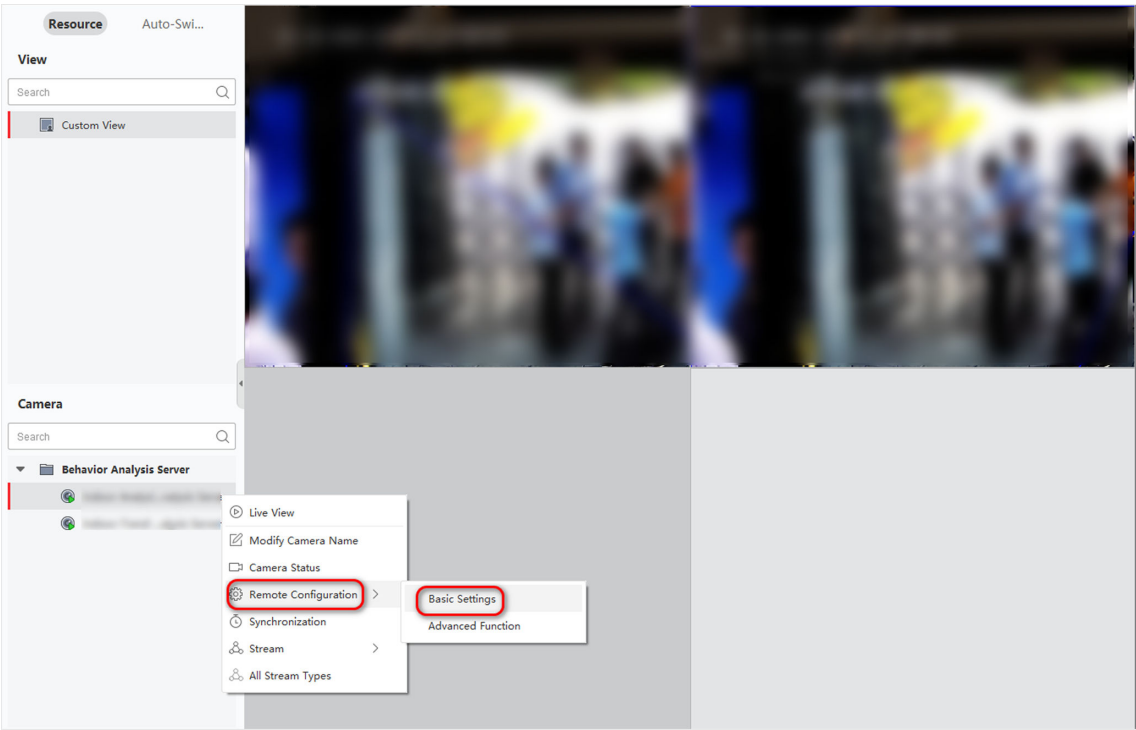


Figure 6-9 Select Remote Configuration

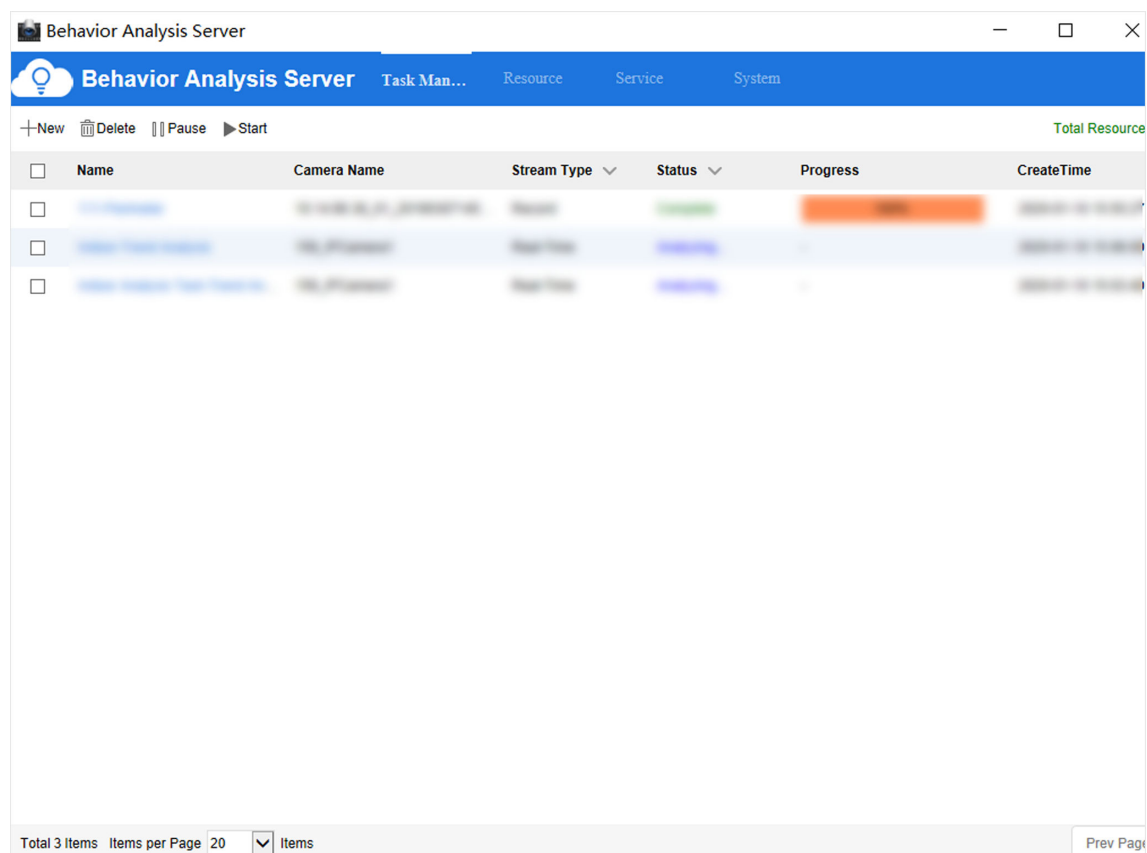


Figure 6-10 Remote Configuration Interface

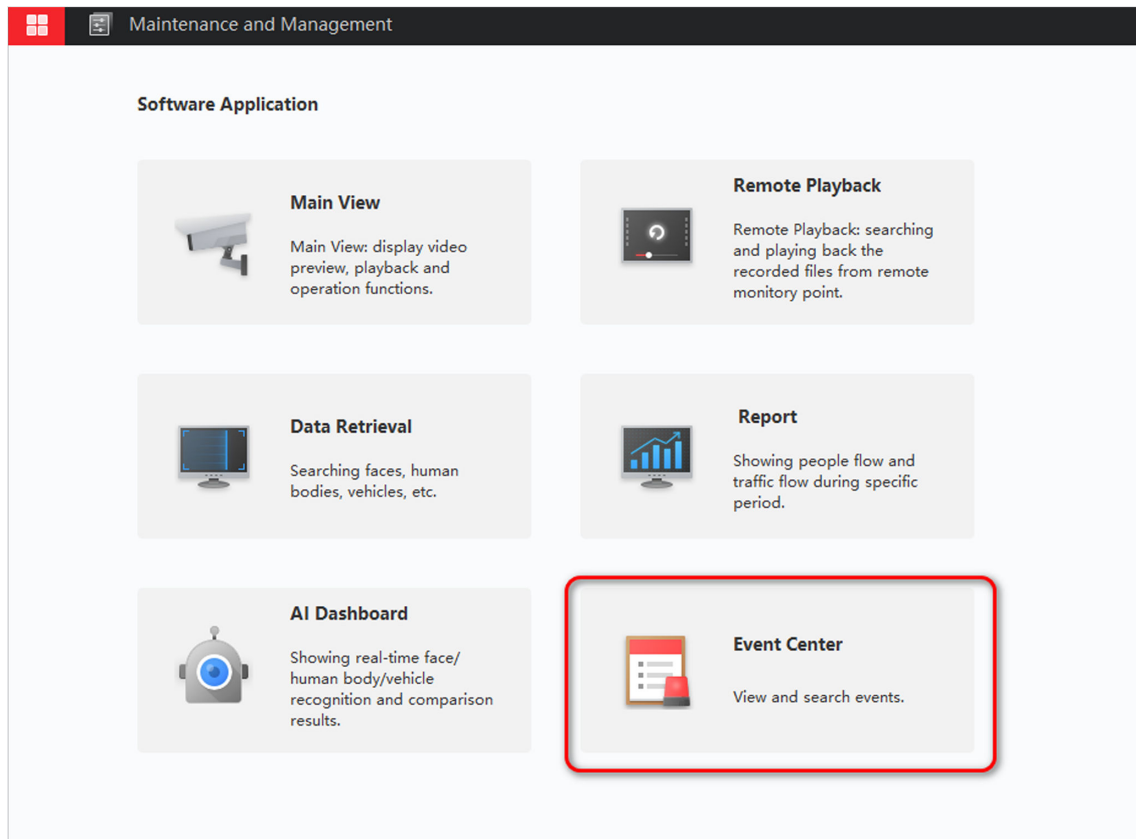
## 6.5 Alarm Center

### 6.5.1 Search Real-time Event

It allows to view alarm information, preview real-time alarm channel, and automatically pop up the window when an alarm triggered.

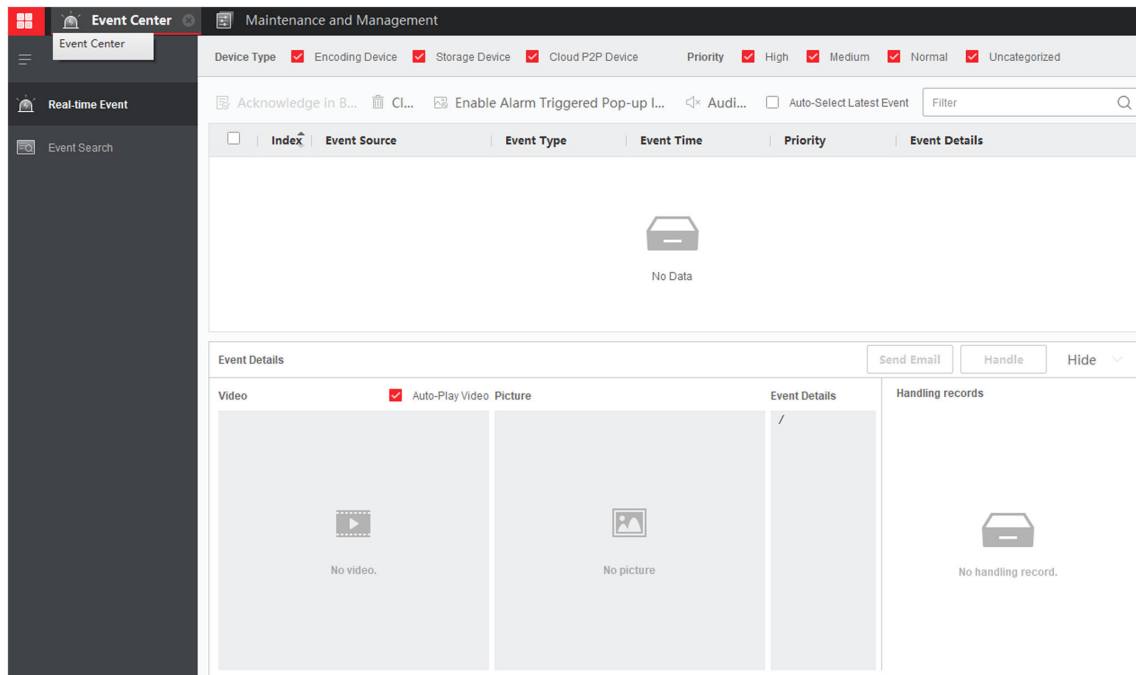
#### Steps

1. Click  → Event Center .



**Figure 6-11 Click Event Center**

2. Click **Real-time Event** to view real-time alarm information.



**Figure 6-12 Real-time Event Alarm Information**

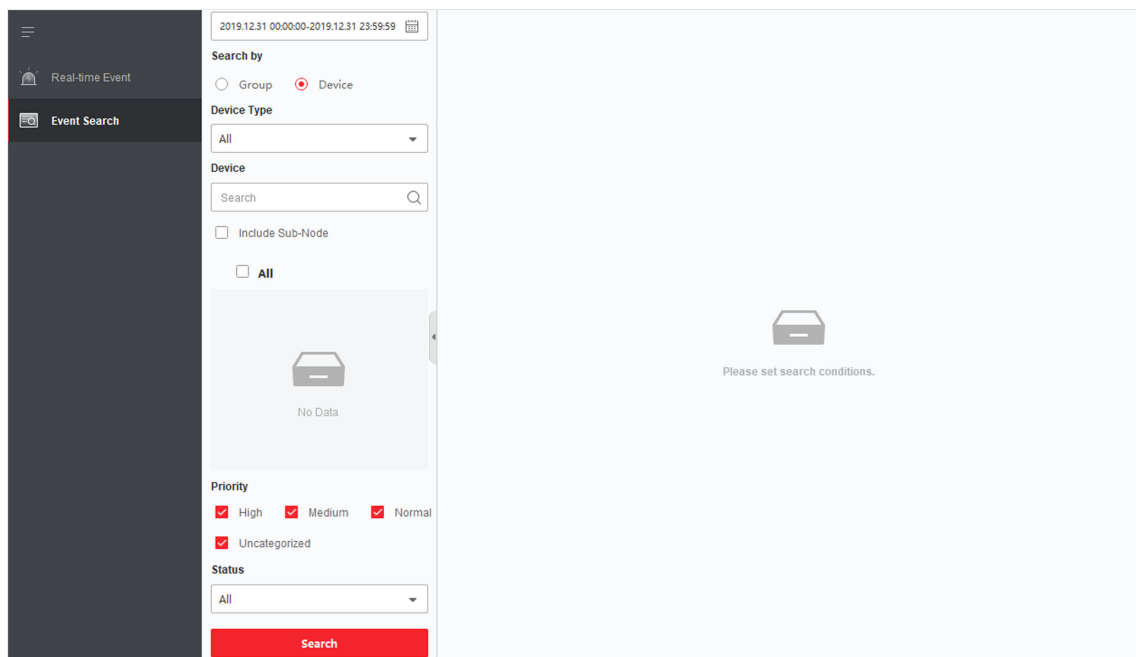
Operation	Description
Clear List	Click  or click the right button of mouse in the alarm information list and click <b>Clear</b> to clear the alarm information.
Alarm Sound	The alarm sound is off by default. Click  to turn on the alarm sound and  to close.
Alarm Pop-up Window	The alarm pop-up window is off by default. Click  to turn on the alarm pop-up window and  to close.
Event Details	Click the desired alarm information to view the alarm image. Click <b>Handle</b> to record the handling suggestions.

## 6.5.2 Search Event

Quick search for alarm events.

### Steps

1. Go to **Event Center** → **Event Search** .



**Figure 6-13 Event Alarm Information**

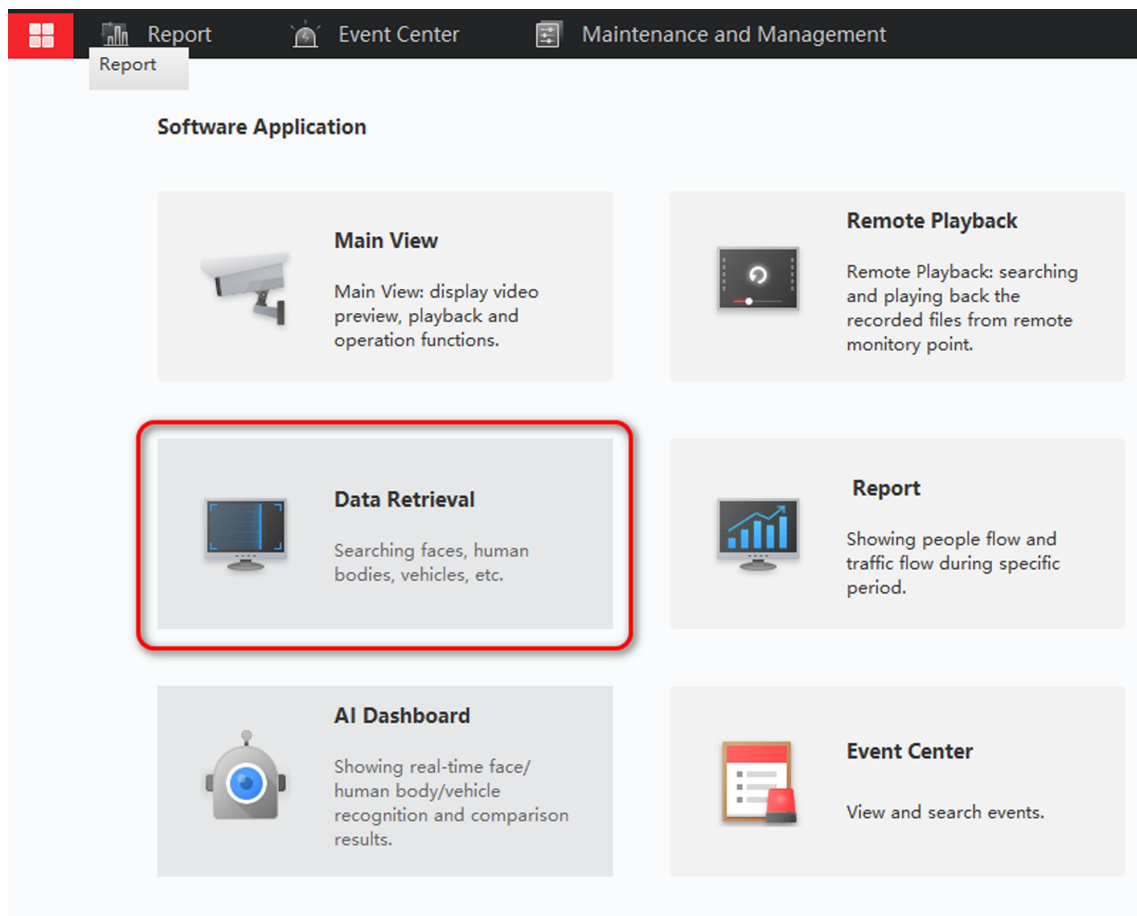
2. Set searching conditions, and click **Search**.
3. Click on the desired event to view details.

## 6.6 Data Retrieval

Search alarm event and export related images.

### Steps

1. Go to  → **Data Retrieval** .



**Figure 6-14 Data Retrieval**

2. Click **Behavior Analysis** and configure the searching conditions.
3. Click **Search**.

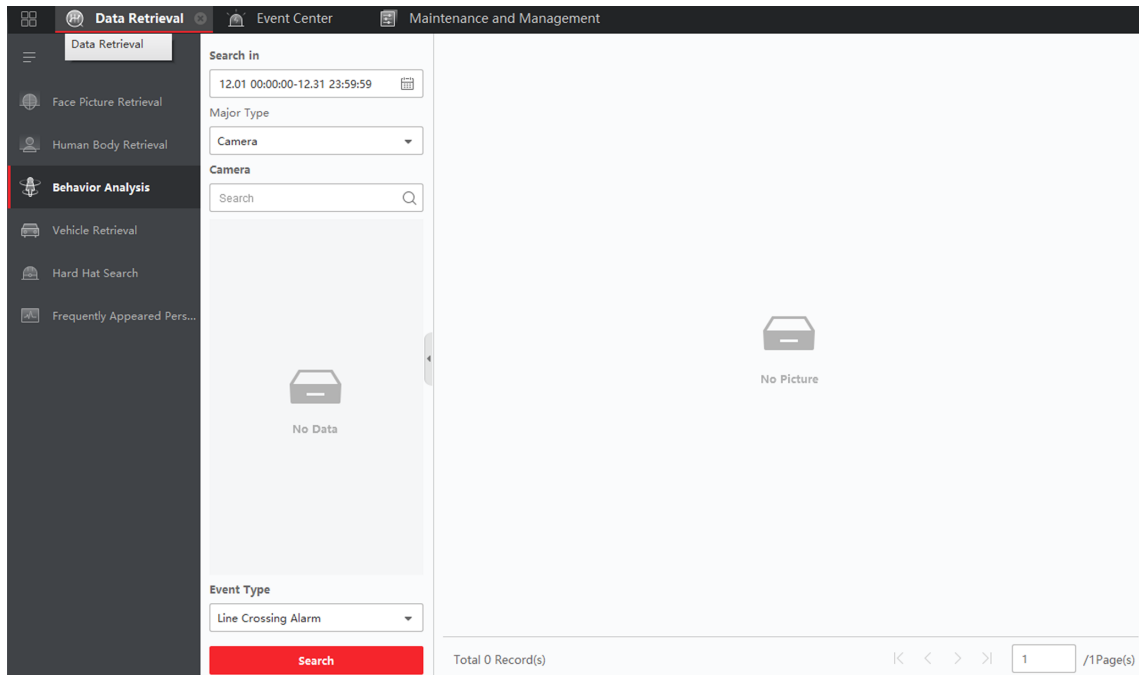


Figure 6-15 Data Retrieval Results



## Note

Only search by task name or rule name is allowed.

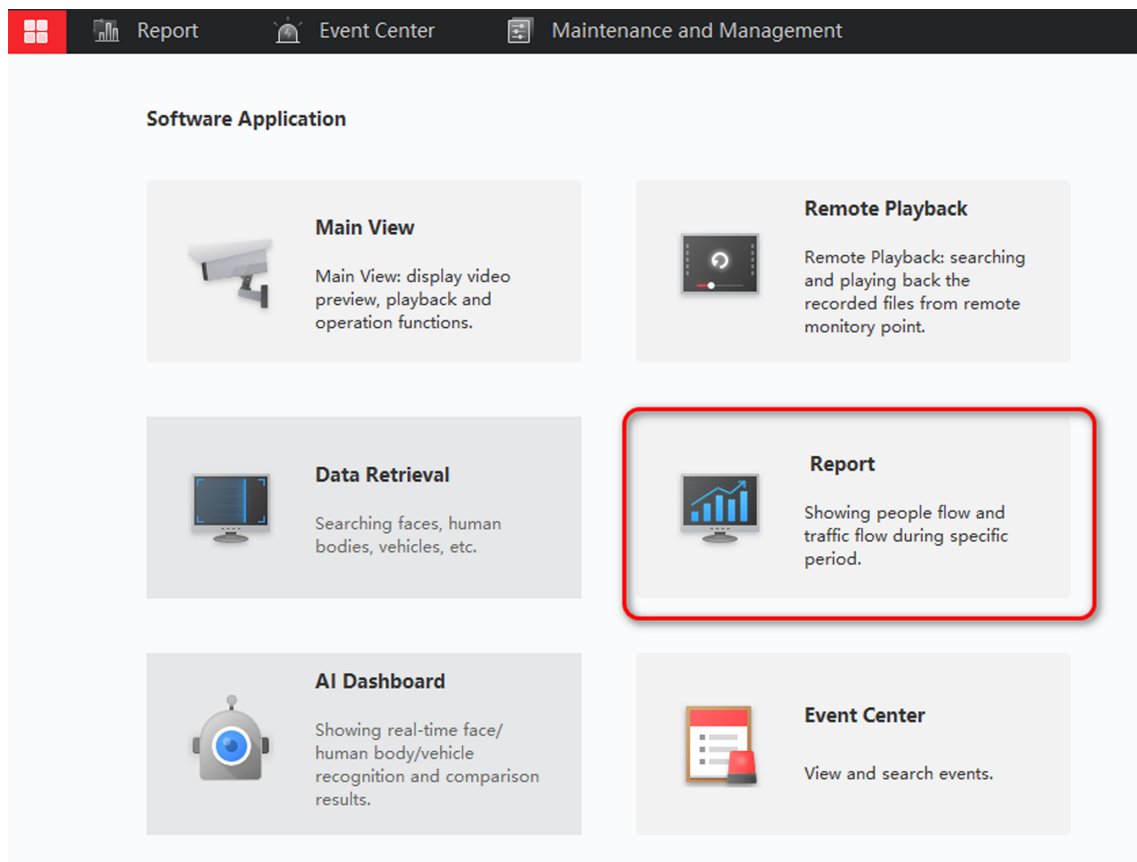
4. Click on the image of alarm event to view details.
5. **Optional:** Click **Export** to download related images of the event.

## 6.7 Data Statistics

Search the people flow volume and real-time number of people in trend analysis task. It supports to export related reports.

### Steps

1. Go to  → **Report** .



**Figure 6-16 Data Report**

2. Select **People Counting** or **Real-time People Counting** according to your actual needs.
3. Configure the searching conditions and then click **Search**.

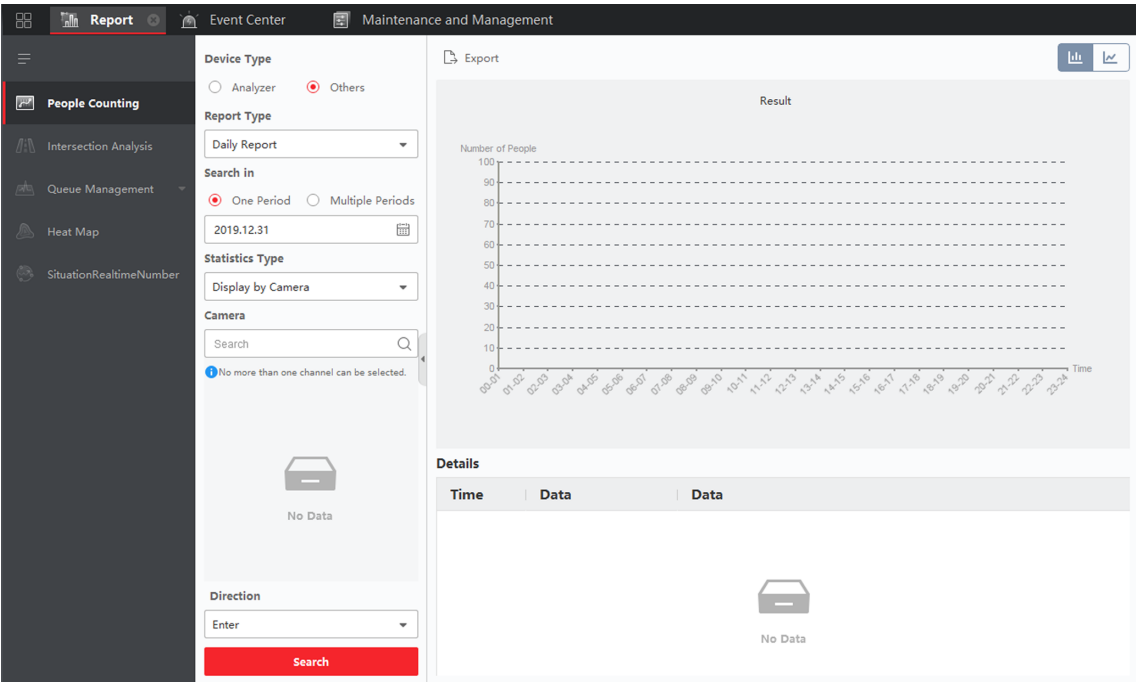


Figure 6-17 Report Results

- 4. Click on the image of alarm event to view details.
- 5. **Optional:** Click **Export** to download related images of the event.



See Far, Go Further