



# Abnormal Event Detection Server

User Manual

# Legal Information

©2022 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 THE 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 INFECTION, 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 LATTER 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 LVD Directive 2014/35/EU, the RoHS Directive 2011/65/EU.

 2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: [www.recyclethis.info](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: [www.recyclethis.info](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 Abnormal Event Detection 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 over-heating 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>
<b>2.1 PC Requirements .....</b>	<b>3</b>
<b>2.2 Activation.....</b>	<b>3</b>
<b>2.2.1 Activate via SADP Software.....</b>	<b>3</b>
<b>2.2.2 Activate via Web Browser .....</b>	<b>4</b>
<b>2.3 Log In .....</b>	<b>5</b>
<b>Chapter 3 Configuration Wizard .....</b>	<b>6</b>
<b>3.1 Create Analysis Cluster .....</b>	<b>6</b>
<b>3.1.1 Add a Node.....</b>	<b>6</b>
<b>3.1.2 Create an Analysis Cluster .....</b>	<b>7</b>
<b>3.1.3 Pre-allocation Resource .....</b>	<b>7</b>
<b>3.2 Add Camera and Video .....</b>	<b>8</b>
<b>3.2.1 Add a Camera.....</b>	<b>8</b>
<b>3.2.2 Add Video Recording.....</b>	<b>11</b>
<b>3.3 Create Behavior Task .....</b>	<b>11</b>
<b>3.3.1 Set Analysis Task Information .....</b>	<b>11</b>
<b>3.3.2 Add a Rule .....</b>	<b>13</b>
<b>3.4 Create AI Task .....</b>	<b>26</b>
<b>3.4.1 Import AI Algorithm Package .....</b>	<b>26</b>
<b>3.4.2 Allocate Analysis Resource.....</b>	<b>28</b>
<b>3.4.3 Create Video Analysis Task.....</b>	<b>29</b>
<b>3.4.4 Create Picture Analysis Task.....</b>	<b>30</b>
<b>3.4.5 Search AI Alarm .....</b>	<b>34</b>
<b>3.5 Task Management .....</b>	<b>36</b>
<b>3.5.1 Configure Task.....</b>	<b>36</b>
<b>3.5.2 Delete Task.....</b>	<b>37</b>
<b>3.5.3 Pause Task.....</b>	<b>37</b>
<b>3.5.4 Start Task .....</b>	<b>37</b>

<b>Chapter 4 Node and Cluster Management .....</b>	<b>38</b>
<b>4.1 Node Management .....</b>	<b>38</b>
4.1.1 Delete a Node .....	38
4.1.2 Restart a Node .....	38
4.1.2 Power a Node Off .....	38
<b>4.2 Cluster Management .....</b>	<b>39</b>
4.2.1 Add to Cluster .....	39
4.2.1 Remove from Cluster .....	39
<b>Chapter 5 System Management .....</b>	<b>40</b>
5.1 Basic Configuration .....	40
5.2 Service Configuration .....	40
5.3 Cloud Storage .....	41
5.4 Time Configuration .....	41
5.5 User Management .....	42
5.5.1 Add User .....	42
5.5.2 Modify admin Password .....	43
5.6 Restore Defaults .....	44
5.7 Event Configuration .....	44
5.8 Log Management .....	44
5.8.1 Search Log .....	44
5.8.2 Download Maintenance Log .....	45
5.9 Software Updating .....	45
5.10 Information .....	46
<b>Chapter 6 iVMS-4200 Client Configuration .....</b>	<b>48</b>
6.1 Log In .....	48
6.2 Add Server .....	49
6.2.1 Add Server Manually .....	49
6.2.2 Add Online Server .....	50
6.3 View Analysis Task Frame .....	51
6.4 Remote Configuration .....	52
6.5 Alarm Center .....	53

<b>6.5.1 Search Real-time Event</b> .....	53
<b>6.5.2 Search Event</b> .....	54
<b>6.6 Data Retrieval</b> .....	55
<b>6.7 Data Statistics</b> .....	57

## Chapter 1 Introduction

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

### Perimeter

- Crossing Line: 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 Baggage: An alarm will be triggered when the unattended time of a baggage 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: 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.
- Number of People Exception: 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.
- 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.
- Staying Overtime: An alarm will be triggered when the staying duration of personnel exceeds the time set.
- Uniform Detection: An alarm will be triggered when the time of uniform personnel in absence exceeds the time set.



- People Counting: Count the number of people in the detection area, and upload the data according to the time interval 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.
- Unattended Baggage Detection: An alarm will be triggered when the unattended time of a baggage left in the detection area exceeds the time set.

### **Escalator**

- Walking Backwards on Escalator: An alarm will be triggered when a person walks backwards on an escalator.
- Falling-Down on Escalator: An alarm will be triggered when a person falls down on an escalator.
- Carrying Large Luggage on Escalator: An alarm will be triggered when a person carries a large luggage on an escalator.
- Pushing Baby Stroller on Escalator: An alarm will be triggered when a person pushes a baby stroller on an escalator.

## 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, 8, 10	Intel® Pentium IV 3.0 GHz or more advanced version	1 GB or larger	1024 × 768 or higher	IE11 is recommended

---

 **Note**

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.

---

 **Note**

Initial Server IP Address: 192.168.1.64.

---

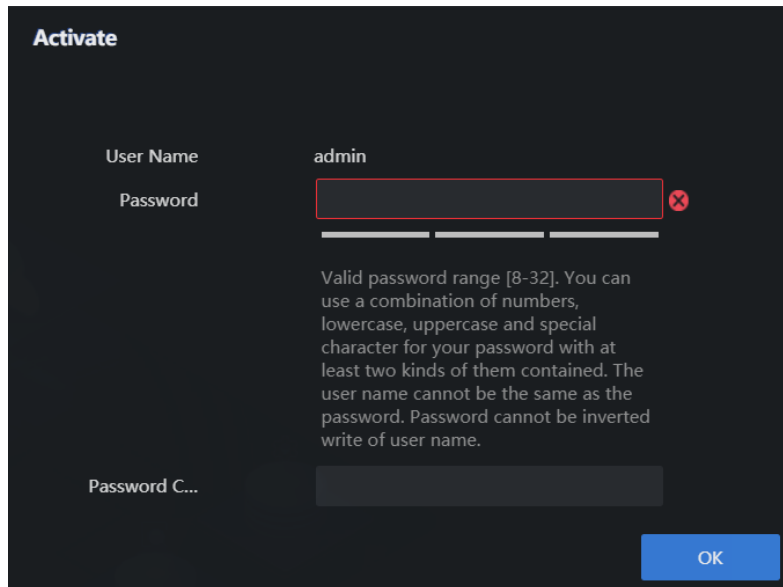
2. Check the desired server and set server password in the **Activate Device** window. Click **Activate**.



- 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**.



**Activate**

User Name admin

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 user name cannot be the same as the password. Password cannot be inverted write of user name.

Password C...

OK

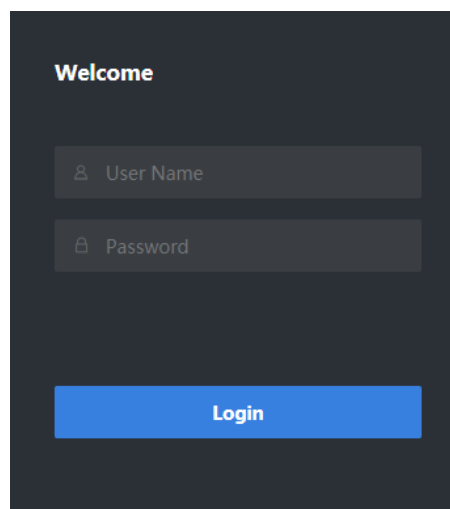
**Figure 2-2 Activation Interface**

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

## 2.3 Log In

### Steps

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



**Welcome**

User Name

Password

Login

**Figure 2-3 Log In**

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

## Chapter 3 Configuration Wizard

### 3.1 Create Analysis Cluster

#### 3.1.1 Add a Node

##### Before You Start

Ensure that the node of analysis cluster is the same as Weishi Cloud cluster.

##### Steps

1. Go to **System Management** → **Cluster Management** → **Node Management**.
2. Click **Add**.

---

##### Note

The name can include letters, numbers, underscore\_ and hyphen-. Other special characters are not allowed.

---

3. Enter **Name** and **Nodes IP**, keep **Port** as default value. The **User Name** is *admin* and **Password** is set when device activation.

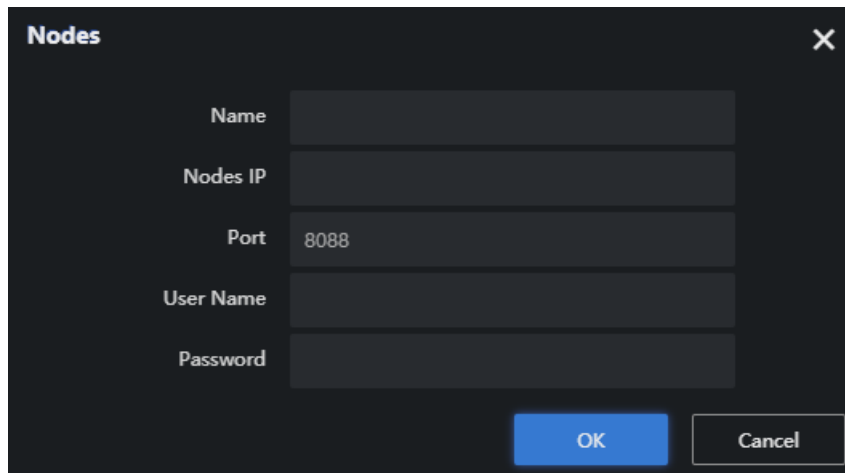


Figure 3-1 Add a Node

---

##### Note

- Please follow the above steps one by one if there are multiple nodes.
  - If you need to add the device to the domain management, platform, etc., please set up cluster first.
- 

4. Click **OK**.

### 3.1.2 Create an Analysis Cluster

The 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 the corresponding nodes have been added.

#### Steps

1. Go to **System Management** → **Cluster Management** → **Cluster Management**.
2. Tick the node, and click **Add to Cluster**.

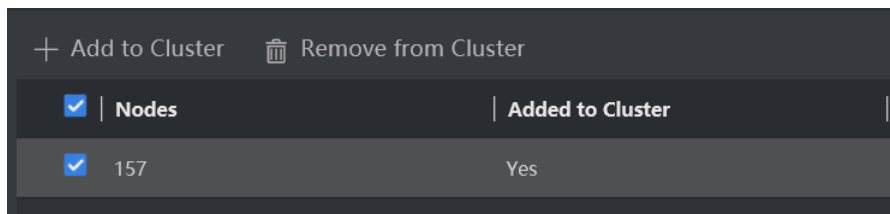


Figure 3-2 Create an Analysis Cluster

3. Click **OK**. System creates cluster automatically.
4. Click **Close** after configuration finished.

### 3.1.3 Pre-allocation Resource

Pre-allocation resource is used for resource reservation. It avoids some analysis task occupying too many resources, causing other analysis tasks to be in a waiting state. Please pre-allocate algorithm resource based on actual business requirements.

#### Steps

1. Go to **Resource** → **Resource Allocation** → **General Algorithm**, expand the algorithm to be allocated resource.

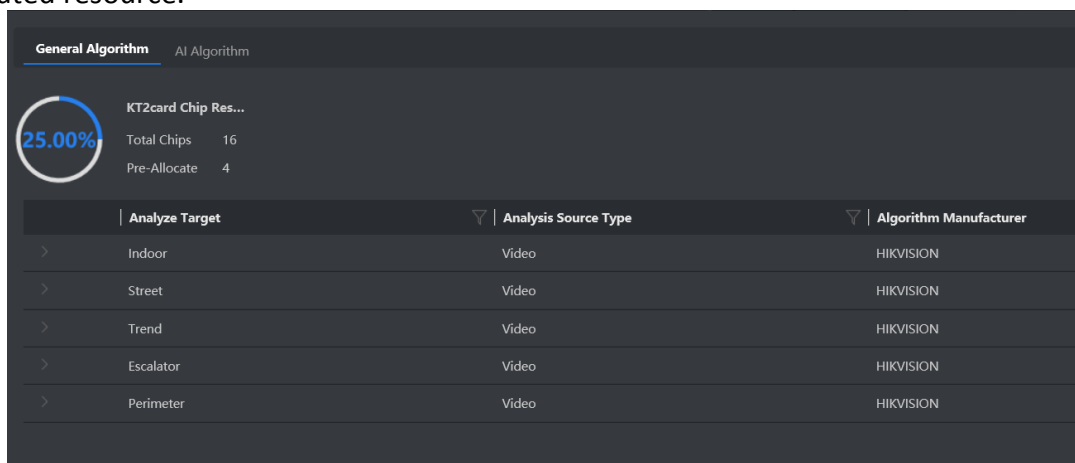




Figure 3-3 General Algorithm

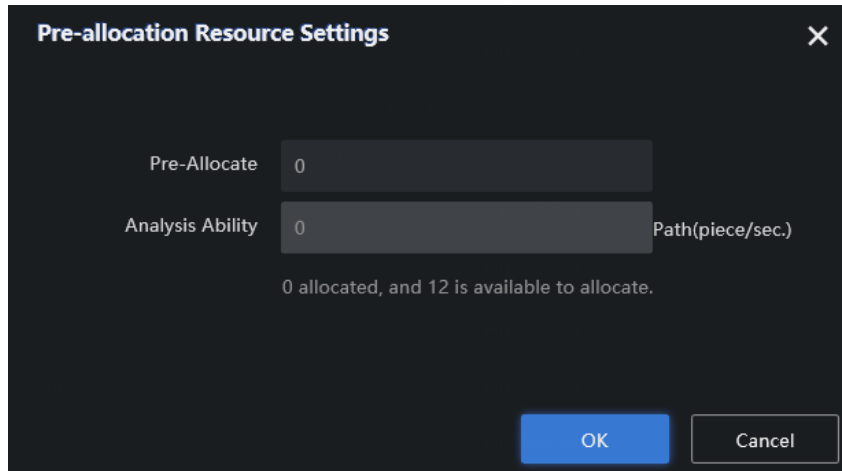
---

**Note**

The interfaces vary from device type.

---

2. Click  to show more details, and click  to allocate resource.



**Figure 3-4 Pre-allocation Resource**

3. Click **OK**.

## 3.2 Add Camera and Video

Add camera and video recording for Abnormal Event Detection.

### 3.2.1 Add a 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.

---

**Note**

-  is control center,  is district. The camera need to be added to control center first, then can be added to district.
  - The following steps take the example of adding camera to control center 'test'.
  - Export the template and fill in the camera information, and then add the camera in batches by importing the completed templates.
- 

#### Steps

1. Click **Resource** → **Camera Management** → **admin**.

2. Click , select **Type** as **Control Center**, enter Name, and then click **OK**.

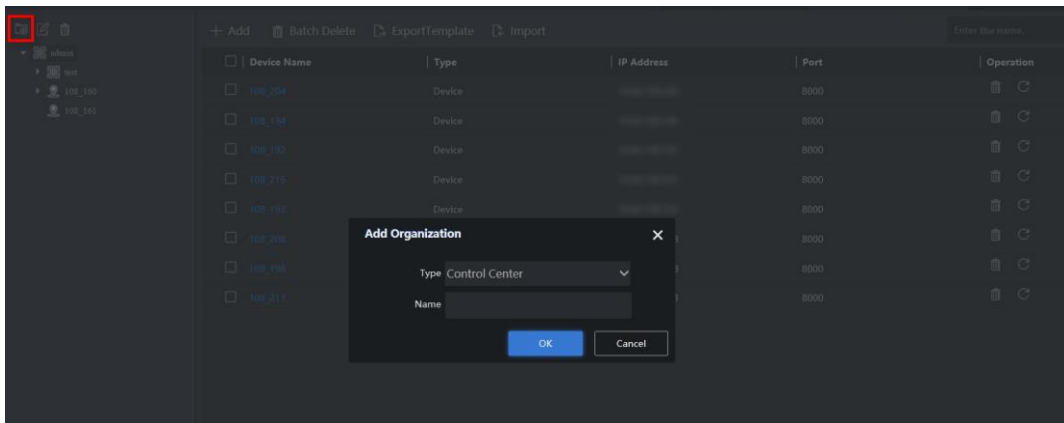


Figure 3-5 Add Control Center

3. Click the newly added control center 'test', and click **Add**. Enter the information of camera to be added, and click **OK**.

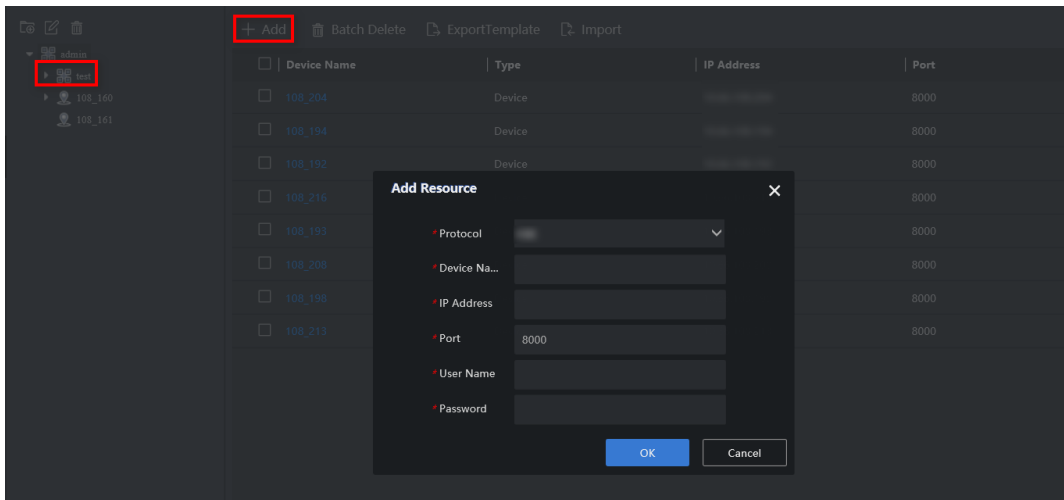



Figure 3-6 Add Camera

 **Note**

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

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



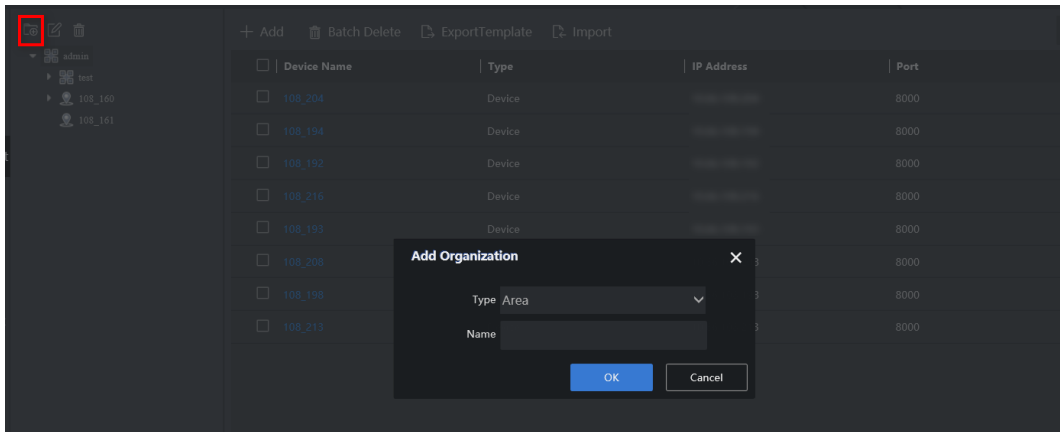


Figure 3-7 Add Area

### Note

Area name can include Chinese characters, numbers, lowercase letters, uppercase letters, hyphens- and underscore\_, with a maximum of 32 characters.

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

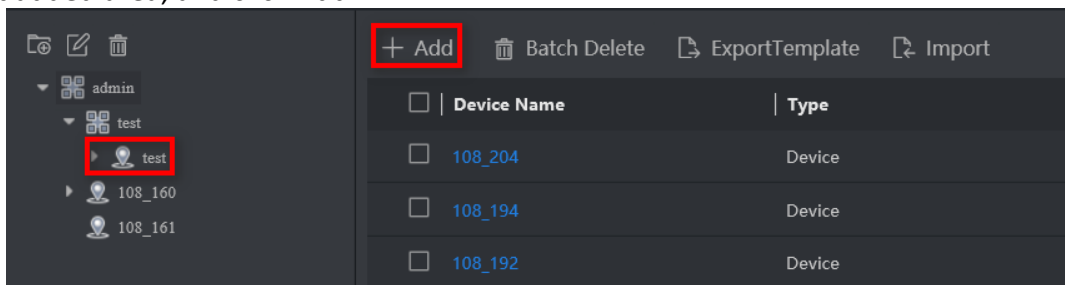


Figure 3-8 Add an Area

### Note

It can be armed after the camera is added to the area.

6. Tick the camera to be added to the area, and click **OK**.

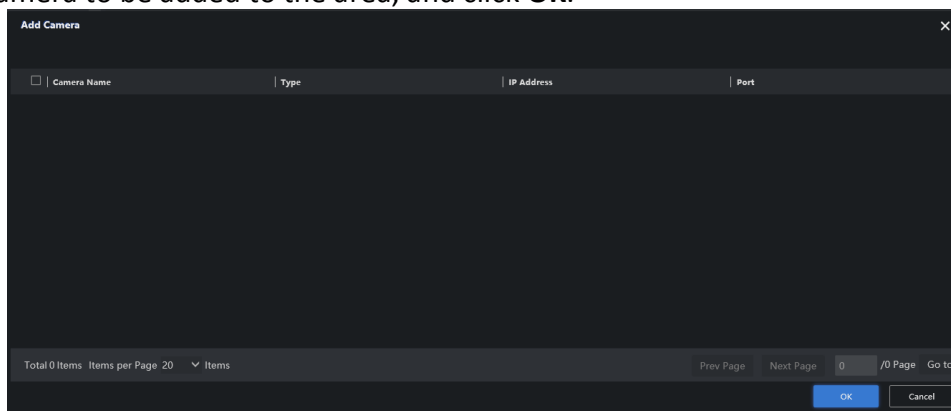


Figure 3-9 Add Camera to the Area

## 3.2.2 Add Video Recording

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

### Steps

1. Click **Resource** → **Record File**.

---

#### Note

The following steps take the default list of video import as an example. Please create the corresponding area first if you need to import other areas.

---

2. Expand the admin list, and click **Default List** → **Import**.

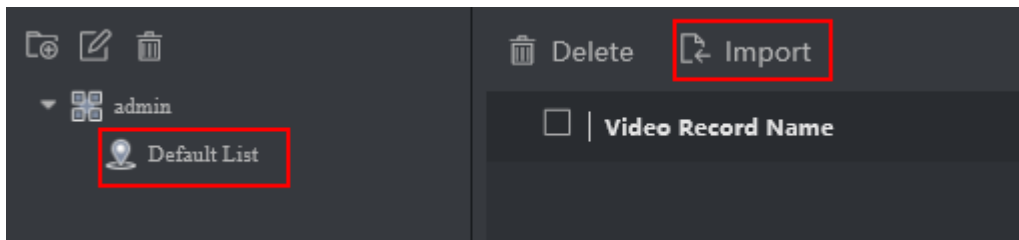


Figure 3-10 Import File

3. Click **Browse** to select record file, and set **Record Start Time** as the actual record time, click **OK**.

---

#### Note

Not set the record start time may cause the time in the recording analysis result to be inconsistent with the actual recording time.

---

4. Click **Import**.

---

#### Note

If system asks to install the control software, please download and install it. Please close the IE browser before installing the control.

---

## 3.3 Create Behavior Task

### 3.3.1 Set Analysis Task Information

You can create different tasks of perimeter scene, indoor scene, trend scene and indoor scene. Up to 8 detection events can be added for each task.

### Steps

1. Select **Target Arming** → **Task Management** → **Behavior Task**.
2. Click **New**.

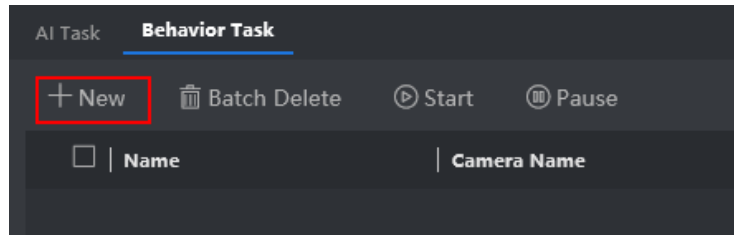


Figure 3-11 Create a New Task

3. Enter a task name.

 **Note**

After the task is created, the name displayed in the task list is *entered name-scene name*. Such as *\*\*\*-Perimeter*.

---

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

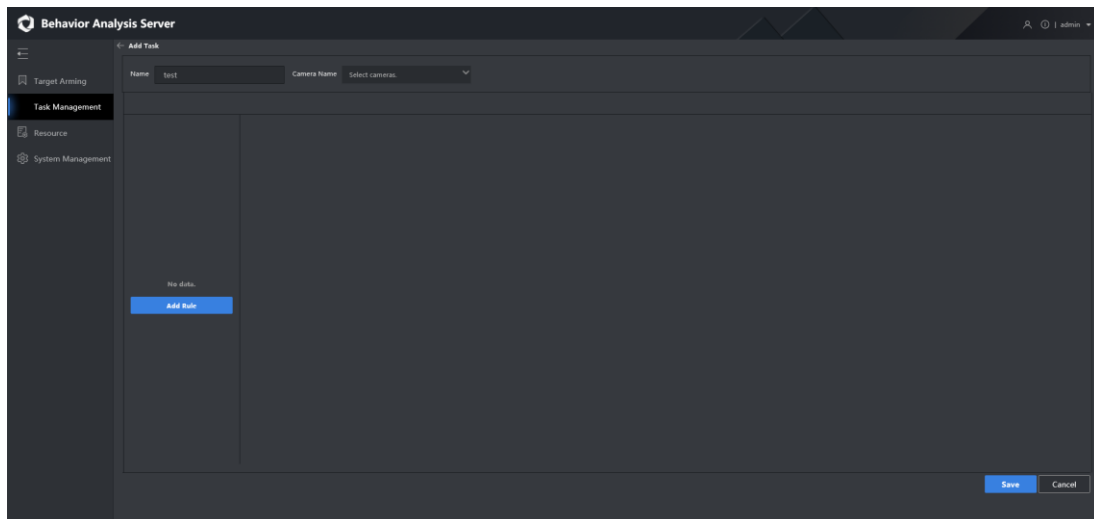


Figure 3-12 Create Task Interface

5. 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 Add a Rule




#### Operation Description

The meanings of each icons and parameters concern with the configuration of tasks are shown below.

**Table 3-1 Icons Description of Live View Window**

Icon	Description
	Draw a detection area. 1. Press the left mouse button and move the mouse to draw a detection area. 2. Click the right button to complete.
	Set full screen detection.
	Draw a square to set the maximum/minimum detection size of target. <hr/> <b>Note</b> The maximum size should be larger than the minimum one. <hr/>
	Draw a line for the detection of crossing behavior.
	Delete the area you have drawn.

**Table 3-2 Icons Description of Time Schedule Window**

Icon	Description
	Copy the current schedule of the day to other days.
	Delete the selected schedule.
	Clear out all the schedules.

#### Add a Perimeter Rule

In the Trend Analysis scene, there are 8 kinds of event analysis, and a task can add up to 8 detection events.

#### Configure Parameters of the rule

Configure the following parameters according to the actual need:

- Name: It is recommended to keep the name consistent with the event name.
- Scene: Select **Perimeter**.
- Event: Select desired events.

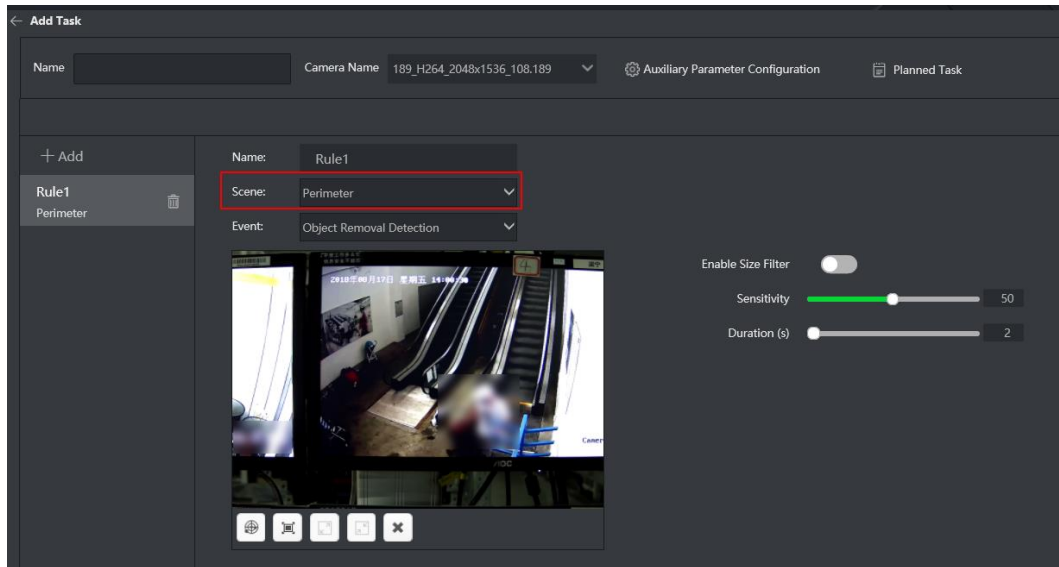









Figure 3-13 Add a Perimeter Rule

### Crossing Line Detection

1. Select **Crossing Line Detection** as **Event**.
2. Enable **Size Filter**.
  - Click  to draw a rectangle to set the maximum detection size of the target.
  - Click  to draw a rectangle to set the minimum detection size of the target.
3. Set a crossing line.
  - a. Click  to draw a line.
  - b. Move the mouse to the ends of the crossing line, press and hold the left mouse button to adjust the position and length.
  - c. Configure **Crossing Line Direction**.
4. Configure **Sensitivity**, and **Target Type**.
5. Set **Time Schedule**.
6. Click **Save** if no more events need to be added.

### Region Entrance Detection

1. Select **Region Entrance Detection** as **Event**.
2. Draw a detection area.
 



Click  to draw a desired area or  to perform a full-screen detection.
3. Enable **Size Filter**.
  - Click  to draw a rectangle to set the maximum detection size of the target.
  - Click  to draw a rectangle to set the minimum detection size of the target.
4. Configure **Target Type**.
5. Set **Time Schedule**.
6. Click **Save** if no more events need to be added.

### Region Exiting Detection

1. Select **Region Exiting Detection** as **Event**.
2. Draw a detection area.

Click  to draw a desired area or  to perform a full-screen detection.

3. Enable **Size Filter**.

- Click  to draw a rectangle to set the maximum detection size of the target.
- Click  to draw a rectangle to set the minimum detection size of the target.

4. Configure **Target Type**.

5. Set **Time Schedule**.

6. Click **Save** if no more events need to be added.



### Intrusion Detection

1. Select **Intrusion Detection** as **Event**.

2. Draw a detection area.

Click  to draw a desired area or  to perform a full-screen detection.

3. Enable **Size Filter**.

- Click  to draw a rectangle to set the maximum detection size of the target.
- Click  to draw a rectangle to set the minimum detection size of the target.

4. Configure **Duration(s)**, **Target Type**, and **Sensitivity**.

5. Set **Time Schedule**.

6. Click **Save** if no more events need to be added.



### Loitering Detection

1. Select **Loitering Detection** as **Event**.

2. Draw a detection area.

Click  to draw a desired area or  to perform a full-screen detection.

3. Enable **Size Filter**.

- Click  to draw a rectangle to set the maximum detection size of the target.
- Click  to draw a rectangle to set the minimum detection size of the target.

4. Configure **Duration**.

5. Set **Time Schedule**.

6. Click **Save** if no more events need to be added.



### Parking Detection

1. Select **Parking Detection** as **Event**.

2. Draw a detection area.

Click  to draw a desired area or  to perform a full-screen detection.

3. Enable **Size Filter**.

- Click  to draw a rectangle to set the maximum detection size of the target.
- Click  to draw a rectangle to set the minimum detection size of the target.

4. Configure **Duration** and **Sensitivity**.

5. Set **Time Schedule**.

6. Click **Save** if no more events need to be added.



### Object Removal Detection

1. Select **Object Removal Detection** as **Event**.

2. Draw a detection area.

Click  to draw a desired area or  to perform a full-screen detection.

3. Enable **Size Filter**.

- Click  to draw a rectangle to set the maximum detection size of the target.
- Click  to draw a rectangle to set the minimum detection size of the target.

4. Configure **Duration** and **Sensitivity**.

5. Set **Time Schedule**.

6. Click **Save** if no more events need to be added.



### Unattended Baggage Detection

1. Select **Unattended Baggage Detection** as **Event**.

2. Draw a detection area.

Click  to draw a desired area or  to perform a full-screen detection.

3. Enable **Size Filter**.

- Click  to draw a rectangle to set the maximum detection size of the target.
- Click  to draw a rectangle to set the minimum detection size of the target.

4. Configure **Duration** and **Sensitivity**.

5. Set **Time Schedule**.

6. Click **Save** if no more events need to be added.

### Add an Indoor Rule

In the indoor scene, there are 13 kinds of event analysis, and a task can add up to 16 detection events.

#### Configure Parameters of the rule

Configure the following parameters according to the actual need:

- Name: It is recommended to keep the name consistent with the event name.
- Scene: Select **Indoor**.
- Event: Select desired events.

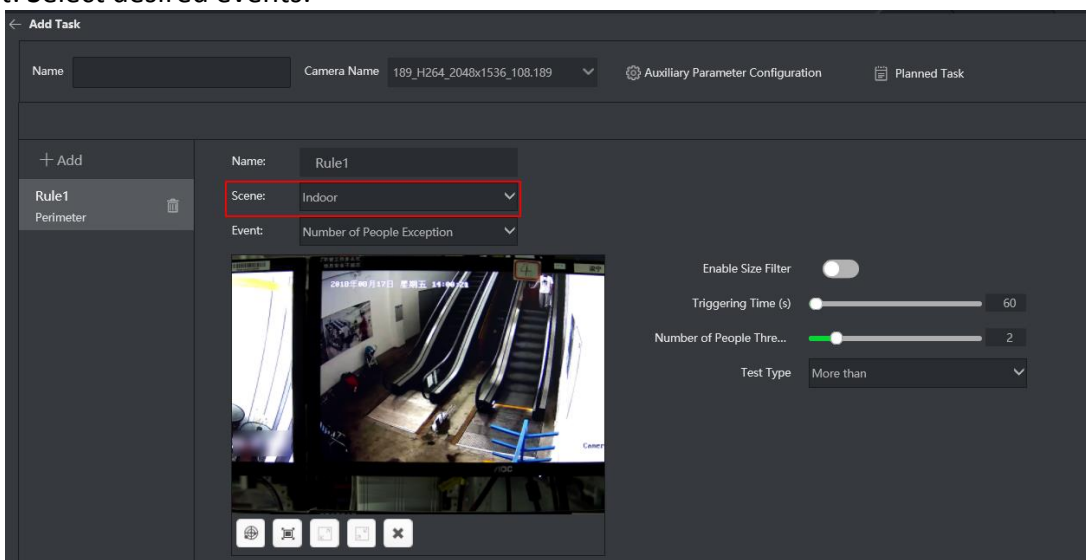










Figure 3-14 Add an Indoor Rule

### Number of People Exception

1. Select **Number of People Exception** as **Event**.
2. Draw a detection area.  
Click  to draw a desired area or  to perform a full-screen detection.
3. Enable **Size Filter**.
  - Click  to draw a rectangle to set the maximum detection size of the target.
  - Click  to draw a rectangle to set the minimum detection size of the target.
4. Configure **Triggering Time(s)** and **Number of People Threshold**.
5. Set **Test Type**.
  - More than: If the number of people in the detection area is greater than the set number threshold and exceeds the trigger time, an alarm message will be generated.
  - Less than: If the number of people in the detection area is less than the set number threshold and exceeds the trigger time, an alarm message will be generated.
  - Equal to: If the number of people in the detection area is equal to the set threshold and exceeds the trigger time, an alarm message is generated.
  - Not equal to: If the number of people in the detection area is not equal to the set threshold and exceeds the trigger time, an alarm message is generated.
6. Set **Time Schedule**.
7. Click **Save** if no more events need to be added.

### Standing Up Detection

1. Select **Standing Up Detection** as **Event**.
2. Draw a detection area.  
Click  to draw a desired area or  to perform a full-screen detection.
3. Enable **Size Filter**.
  - Click  to draw a rectangle to set the maximum detection size of the target.
  - Click  to draw a rectangle to set the minimum detection size of the target.
4. Configure **Sensitivity**.
5. Set **Time Schedule**.
6. Click **Save** if no more events need to be added.

### Detection for Sudden Change of Sound Intensity

---

#### Note

Only 1 sound intensity detection rule can be created under a task.

---

1. Select **Detection for Sudden Change of Sound Intensity** as **Event**.
2. Configure detection mode.
  - Sensitivity Detection: If there are abnormal sounds such as screams, quarrels, etc. in the monitoring area, an alarm will be triggered. The specific sensitivity value can be set to the default value first, and then adjusted according to the actual alarm situation.
  - Decibel Threshold (dB): Detect the volume of the sound in the monitoring area, if it is greater than the decibel threshold, an alarm is triggered.





 **Note**

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





---

3. Click **Sound Intensity Test** to check real-time sound volume, and adjust the threshold according to the test result.
4. Set **Time Schedule**.
5. Click **Save** if no more events need to be added.



**Falling Down**

1. Select **Falling Down** as **Event**.
2. Draw a detection area.  
Click  to draw a desired area or  to perform a full-screen detection.
3. Configure **Duration**.
4. Set **Time Schedule**.
5. Click **Save** if no more events need to be added.



**Getting Up Detection**



1. Select **Getting Up Detection** as **Event**.
2. Draw a detection area.  
Click  to draw a desired area or  to perform a full-screen detection.
3. Enable **Size Filter**.
  - Click  to draw a rectangle to set the maximum detection size of the target.
  - Click  to draw a rectangle to set the minimum detection size of the target.
4. Configure **Sensitivity**.
5. Set **Getting Up Mode** according to the actual need.
  - Wide Bed Mode
  - Bunk Bed Mode
  - Setting and Getting Up Mode
6. Set **Time Schedule**.
7. Click **Save** if no more events need to be added.

**Physical Conflict (Indoor)**





1. Select **Physical Conflict (Indoor)** as **Event**.
2. Draw a detection area.  
Click  to draw a desired area or  to perform a full-screen detection.
3. Configure **Sensitivity**.
4. Set **Time Schedule**.
5. Click **Save** if no more events need to be added.

**Absence Detection**



1. Select **Absence Detection** as **Event**.
2. Draw a detection area.  
Click  to draw a desired area or  to perform a full-screen detection.
3. Enable **Size Filter**.

- Click  to draw a rectangle to set the maximum detection size of the target.
  - Click  to draw a rectangle to set the minimum detection size of the target.
4. Configure detailed parameters.
    - Configuration Mode
    - Alarm Time when Nobody Detected(s)
    - Person On Duty
  5. Set **Time Schedule**.
  6. Click **Save** if no more events need to be added.



### Staying Overtime

1. Select **Staying Overtime** as **Event**.
2. Draw a detection area.  
Click  to draw a desired area or  to perform a full-screen detection.
3. Enable **Size Filter**.
  - Click  to draw a rectangle to set the maximum detection size of the target.
  - Click  to draw a rectangle to set the minimum detection size of the target.
4. Configure **Duration**.
5. Set **Time Schedule**.
6. Click **Save** if no more events need to be added.



### People Counting


1. Select **People Counting** as **Event**.
2. Draw a detection area.  
Click  to draw a desired area or  to perform a full-screen detection.
3. Configure **Alarm Interval(s)**.
4. Set **Time Schedule**.
5. Click **Save** if no more events need to be added.

### Playing Mobile Phone





1. Select **Playing Mobile Phone** as **Event**.
2. Draw a detection area.  
Click  to draw a desired area or  to perform a full-screen detection.
3. Configure **Duration**.
4. Set **Time Schedule**.
5. Click **Save** if no more events need to be added.

### Climbing Detection





1. Select **Climbing Detection** as **Event**.
2. Click , and left click mouse to draw a line, right click mouse to stop drawing.
3. Select Crossing Line Direction.
  - Bidirectional
  - A to B
  - B to A
4. Enable **Size Filter**.
  - Click  to draw a rectangle to set the maximum detection size of the target.

- Click  to draw a rectangle to set the minimum detection size of the target.
5. Set **Time Schedule**.
  6. Click **Save** if no more events need to be added.

### Sitting Detection

1. Select **Sitting Detection** as **Event**.
2. Draw a detection area.  
Click  to draw a desired area or  to perform a full-screen detection.
3. Enable **Size Filter**.
  - Click  to draw a rectangle to set the maximum detection size of the target.
  - Click  to draw a rectangle to set the minimum detection size of the target.
4. Configure **Duration**.
5. Set **Time Schedule**.
6. Click **Save** if no more events need to be added.

### Uniform Detection

1. Select **Uniform Detection** as **Event**.
2. Draw a detection area.  
Click  to draw a desired area or  to perform a full-screen detection.
3. Enable **Size Filter**.
  - Click  to draw a rectangle to set the maximum detection size of the target.
  - Click  to draw a rectangle to set the minimum detection size of the target.
4. Configure **Alarm Interval(s)**.
5. Set **Time Schedule**.
6. Click **Save** if no more events need to be added.

### Add a Trend Rule

In the Trend Analysis scene, there are 3 kinds of event analysis, and a task can add up to 8 detection events.

#### Configure Parameters of the rule

Configure the following parameters according to the actual need:

- Name: It is recommended to keep the name consistent with the event name.
- Scene: Select **Trend Analysis**.
- Event: Select desired events.

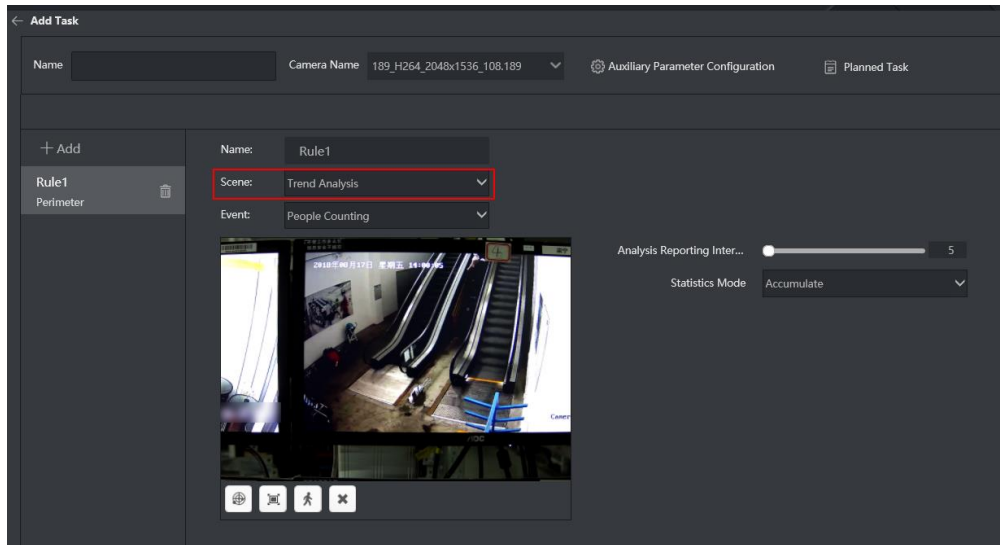


Figure 3-15 Add a Trend Rule

## Crowd Trend Analysis






### Note



Up to 4 crowd trend analysis rules can be created under a task.

1. Select **Crowd Trend Analysis** as **Event**.
2. Draw a detection area.
  - Click to draw a desired area or to perform a full-screen detection.
3. Configure detailed parameters.
  - **Crowd Density Detection Mode**
    - Default Mode: Suitable for large scenes, such as squares.
    - Detection Mode: Suitable for larger scenes, such as supermarkets.
    - Density Mode: Suitable for small scenes, such as conference rooms.
  - **Analysis Reporting Intervals:** The time interval for uploading the density of people.
  - **Alarm Reporting Intervals:** The time interval for uploading personnel density alarms.
  - **Low Alarm Threshold:** The minimum people number that generate low-level alarms for personnel density.
  - **Low Alarm Name:** Customize.
  - **Medium Alarm Threshold:** The minimum people number that generate medium-level alarms for personnel density.
  - **Medium Alarm Name:** Customize.
  - **High Alarm Threshold:** The minimum people number that generate high-level alarms for personnel density.
  - **High Alarm Name:** Customize.
4. Set **Time Schedule**.
5. Click **Save** if no more events need to be added.

## People Counting

1. Select **People Counting** as **Event**.
2. Draw a detection area.  
Click  to draw a desired area or  to perform a full-screen detection.
3. Set a crossing line.
  - a. Click  to draw a line.
  - b. Move the mouse to the ends of the crossing line, press and hold the left mouse button to adjust the position and length.
4. Configure detailed parameters.
  - Analysis Reporting Interval(s)
  - Statistics Mode
    - Accumulate: The previous statistics is accumulated instead of being cleared.
    - Reset Everyday: Clear the statistics every midnight.
5. Set **Time Schedule**.
6. Click **Save** if no more events need to be added.

### Regional People Counting

1. Select **People Counting** as **Event**.
2. Draw a detection area.  
Click  to draw a desired area or  to perform a full-screen detection.
3. Set **Analysis Reporting Interval(s)**.
4. Set **Time Schedule**.
5. Click **Save** if no more events need to be added.

### Add a Street Rule

In the Street Behavior scene, there are 5 kinds of event analysis, and a task can add up to 8 detection events.

#### Configure Parameters of the rule

Configure the following parameters according to the actual need:

- Name: It is recommended to keep the name consistent with the event name.
- Scene: Select **Street Behavior**.
- Event: Select desired events.

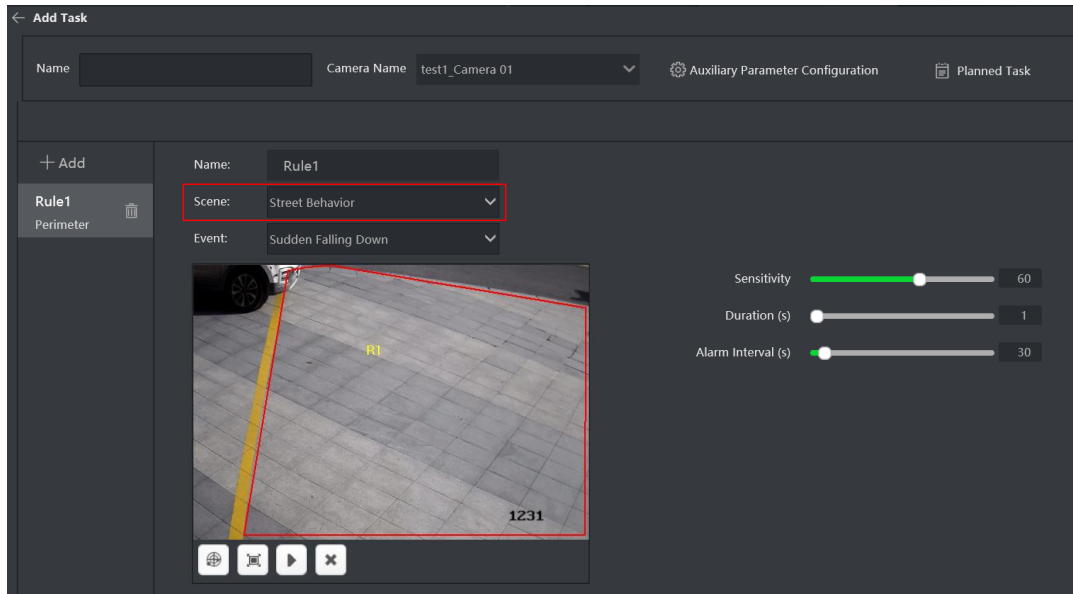






Figure 3-16 Add a Street Rule



### Sudden Falling Down

1. Select **Sudden Falling Down** as **Event**.
2. Draw a detection area.  
Click  to draw a desired area or  to perform a full-screen detection.
3. Configure **Sensitivity**, **Duration(s)** and **Alarm Interval(s)**.
4. Set **Time Schedule**.
5. Click **Save** if no more events need to be added.

### People Gathering Detection



1. Select **People Gathering** as **Event**.
2. Draw a detection area.  
Click  to draw a desired area or  to perform a full-screen detection.
3. Configure **Sensitivity** and **Duration(s)**.
4. Set **Alarm Interval(s)** and **Min. People**.
  - Alarm Interval(s): The shortest time interval between two alarms.
  - Min. People: The minimum number of people for the event.
5. Set **Time Schedule**.
6. Click **Save** if no more events need to be added.

### Physical Conflict (Street)



1. Select **Physical Conflict (Street)** as **Event**.
2. Draw a detection area.  
Click  to draw a desired area or  to perform a full-screen detection.
3. Configure **Sensitivity** and **Duration**.
4. Set **Detection Mode** and **Alarm Interval(s)**.
  - Alarm Interval(s): The shortest time interval between two alarms.
  - Detection Mode: Keep the value as default.

5. Set **Time Schedule**.
6. Click **Save** if no more events need to be added.

### Fast Moving Detection

1. Select **Fast Moving Detection** as **Event**.
2. Draw a detection area.  
Click  to draw a desired area or  to perform a full-screen detection.
3. Configure **Sensitivity** and **Duration**.
4. Set **Running Mode**.
  - Single-Person Running: If it detects that the time for a single person to move quickly in the area exceeds the set time, an alarm message will be generated.
  - Multiple-Person Running: If it detects that the time for multiple person to move quickly in the area exceeds the set time, an alarm message will be generated.
5. Set **Time Schedule**.
6. Click **Save** if no more events need to be added.

### Unattended Baggage Detection

1. Select **Unattended Baggage Detection** as **Event**.
2. Draw a detection area.  
Click  to draw a desired area or  to perform a full-screen detection.
3. Configure **Duration** and **Sensitivity**.
4. Set **Time Schedule**.
5. Click **Save** if no more events need to be added.



#### Note

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

---

## Add an Escalator Rule

In the Escalator Analysis scene, there are 4 kinds of event analysis, and a task can add up to 4 detection events.

### Configure Parameters of the rule

Configure the following parameters according to the actual need:

- Name: It is recommended to keep the name consistent with the event name.
- Scene: Select **Escalator**.
- Event: Select desired events.

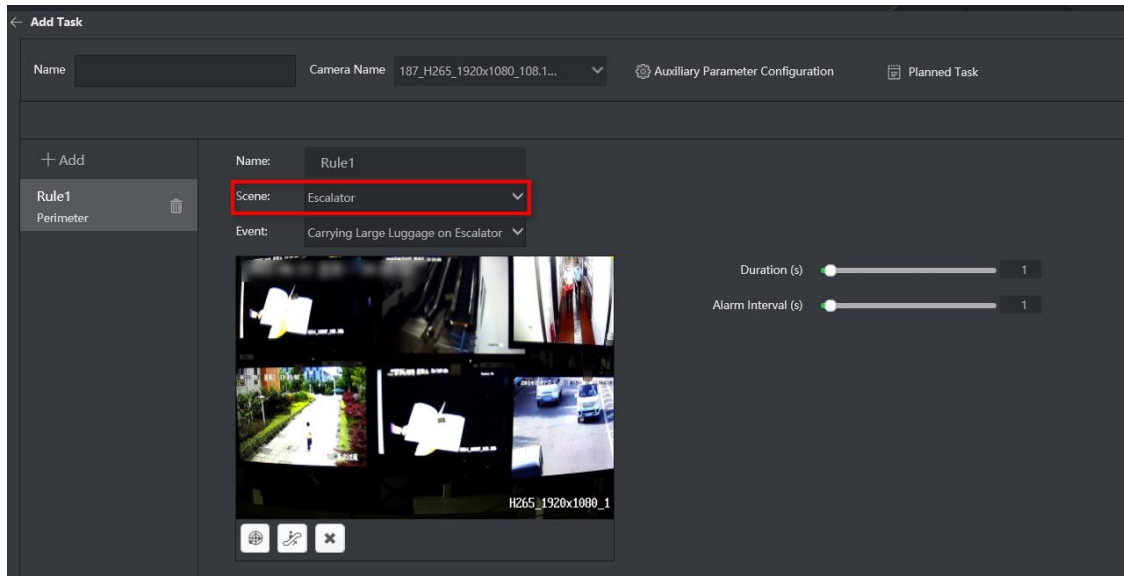




Figure 3-17 Add an Escalator Rule

### Walking Backwards on Escalator



1. Select **Walk Backwards on Escalator** as **Event**.
2. Draw a detection area and an escalator area.
  - a. Click . Press the left mouse button and move the mouse to draw a detection area. Click the right button to complete.
  - b. Click . Press the left mouse button and move the mouse to draw an escalator area. Click the right button to complete.

#### Note

The escalator area and the detection area of different events need to be consistent (areas of other events are automatically reused after drawing the detection area and the escalator area, and will be updated synchronously after modification).

3. Set **Duration(s)** and **Alarm Interval(s)**.
4. Set **Time Schedule**. Full-time detection occurs by default.
5. Click **Save** if no more events need to be added.

### Falling-Down on Escalator

1. Select **Falling-Down on Escalator** as **Event**.
2. Click  to draw a detection area, and click  to draw an escalator area.



#### Note

The escalator area and the detection area of different events need to be consistent (areas of other events are automatically reused after drawing the detection area and the escalator area, and will be updated synchronously after modification).



3. Set **Duration(s)** and **Alarm Interval(s)**.
4. Set **Time Schedule**. Full-time detection occurs by default.
5. Click **Save** if no more events need to be added.

#### Carrying Large Luggage on Escalator

1. Select **Carrying Large Luggage as Event**.
  2. Click  to draw a detection area, and Click  to draw an escalator area.
- 



##### **Note**

The escalator area and the detection area of different events need to be consistent (areas of other events are automatically reused after drawing the detection area and the escalator area, and will be updated synchronously after modification).

---

3. Set **Duration(s)** and **Alarm Interval(s)**.
4. Set **Time Schedule**. Full-time detection occurs by default.
5. Click **Save** if no more events need to be added.

#### Pushing Baby Stroller on Escalator

1. Select **Pushing Baby Stroller on Escalator as Event**.
  2. Click  to draw a detection area, and Click  to draw an escalator area.
- 

##### **Note**

The escalator area and the detection area of different events need to be consistent (areas of other events are automatically reused after drawing the detection area and the escalator area, and will be updated synchronously after modification).

---

3. Set **Duration(s)** and **Alarm Interval(s)**.
4. Set **Time Schedule**. Full-time detection occurs by default.
5. Click **Save** if no more events need to be added.

## 3.4 Create AI Task

### 3.4.1 Import AI Algorithm Package

Importing AI algorithm package(s) is required for creating analysis task(s).

---

##### **Note**

When the platform submits an AI algorithm task, all algorithm packages are issued by the platform and are not imported by the web page.

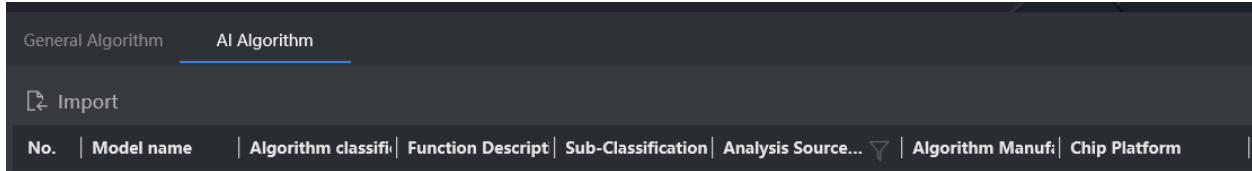
---

## Before You Start

Get an AI algorithm package.

## Steps

1. Go to **Resource** → **Algorithm Management** → **AI Algorithm**, and click **Import**.



**Figure 3-18 Add AI Algorithm Package**

2. Click **Browse**, and select the desired algorithm package and description file (.json file).

### Note

AI algorithm packages include encrypted algorithm packages and non-encrypted packages, and the former is only applicable to the device it is imported to. The License Key file need to be imported when importing the encryption algorithm package.

3. Configure the parameters.

### Model Name

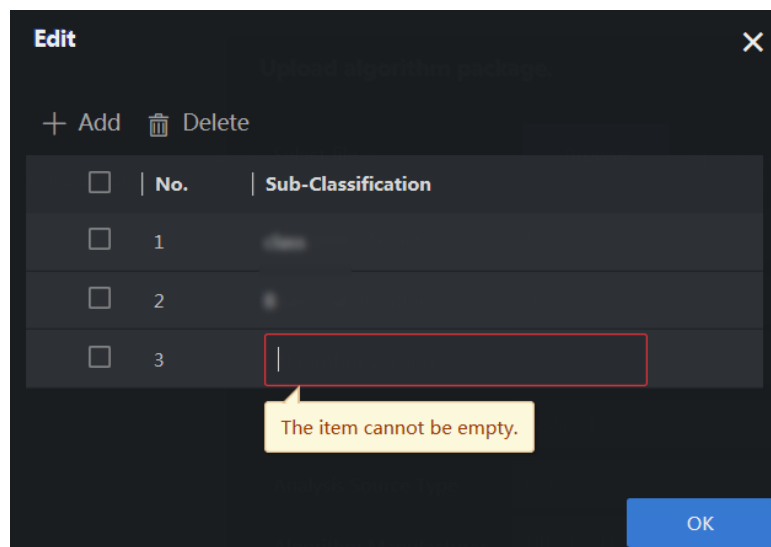
Enter a name as desired.

### Algorithm Classification

Keep the default values. After you configure the analysis source type, the system automatically selects the corresponding algorithm classification.

### Sub-Classification

Enter the sub-classification of analysis type. Click **Edit** → **Add** to add sub-classification as desired.



**Figure 3-19 Add Sub-Classification**

### AI Algorithm Version

Keep the version as default value.

### Chip Platform


Be consistent with the chip application type. Check the type in model management interface of AI Training Platform.

### Analysis Source Type

Keep the default values.

Figure 3-20 Algorithm Package Parameter

4. Click **OK**.

5. Optional: Click  or  to check details or delete the corresponding algorithm.

No.	Model name	Algorithm clas	Function Desc	Sub-Classical	Analysis Sou...	Algorithm Ma	Chip Platform	AI Algorithm Vers	Algorithm Versio	Details	Operation
1											
2											
3											

Figure 3-21 Algorithm List

## 3.4.2 Allocate Analysis Resource

### Before You Start

Import AI algorithm package(s).

### Steps

1. Go to **Resource** → **Resource Allocation** → **AI Algorithm**. Click  to show more details of algorithm information, and click  to allocate resources for AI algorithm package.

---

**Note**

Allocate resource of **Video Analysis Channel(s)** for video analysis task, and **Picture Analysis Channel(s)** for picture analysis task.

---

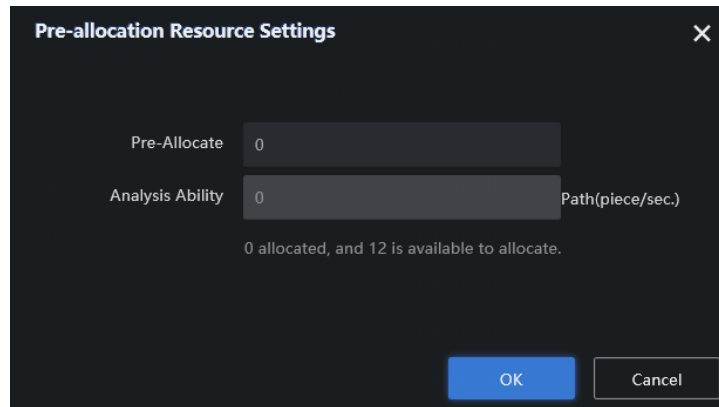


Figure 3-22 Allocate Resource for AI Algorithm Package

---

**Note**

If the value of available resource is zero, the corresponding analysis task cannot be performed.

---

### 3.4.3 Create Video Analysis Task

You can create video analysis task(s) of AI algorithms, and arm cameras (except capture cameras) through the web interface. Detection, classification, behavior, OCR model, and mixed analysis tasks are allowed to be created.

#### Before You Start

- Import video analysis algorithm(s).
- Allocate video analysis resource.

#### Steps

1. Go to **Target Arming** → **Task Management** → **AI Task**, and click **New**.
2. Configure related parameters.

#### Name

Enter a name as desired.

#### Camera Name

Select the desired camera(s) for arming. Creating video analysis task(s) of AI algorithms and arming cameras except capture cameras are allowed.

#### Sub-Classification/Version No.

Select a value as desired.

3. Click **Add Rule**, and configure related parameters as needed.

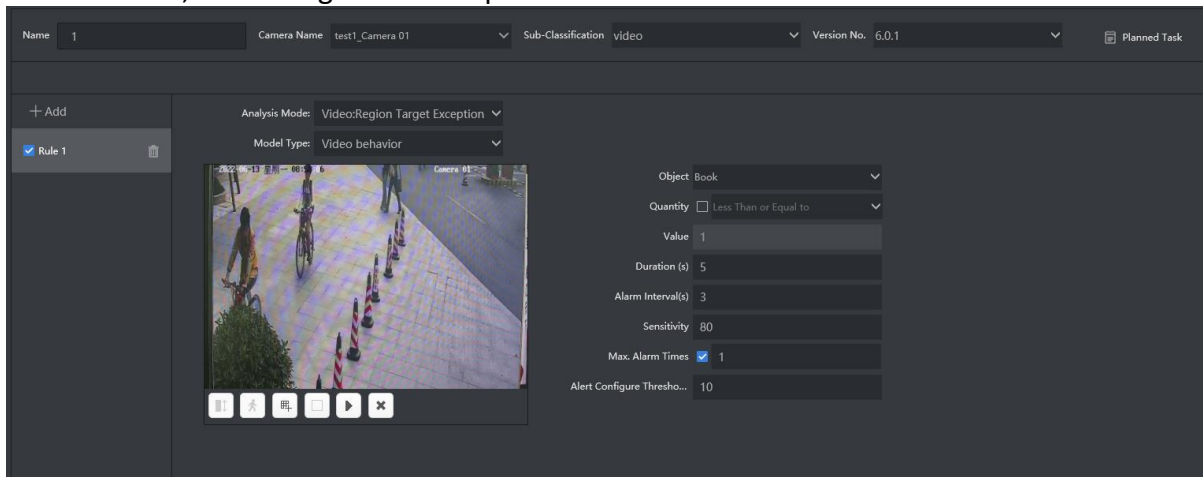


Figure 3-23 Create Task

**Note**

The parameters to be configured vary from different rules. The figure above is for illustration purpose only.

4. Click **Save**.

5. Optional: Check the results through the client.

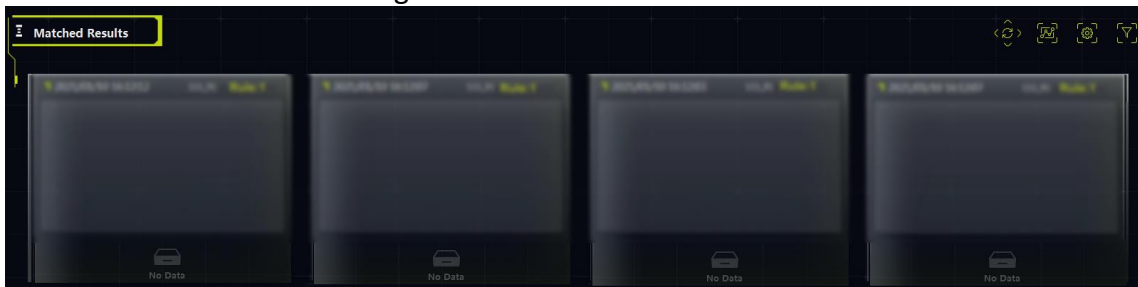


Figure 3-24 Check Analysis Result

### 3.4.4 Create Picture Analysis Task

Picture analysis task(s) should be created through the client. Detection, classification, OCR model, and mixed analysis tasks are allowed to be created.

**Before You Start**

- Allocate video analysis resource.
- Install the corresponding client and check AI dashboard.

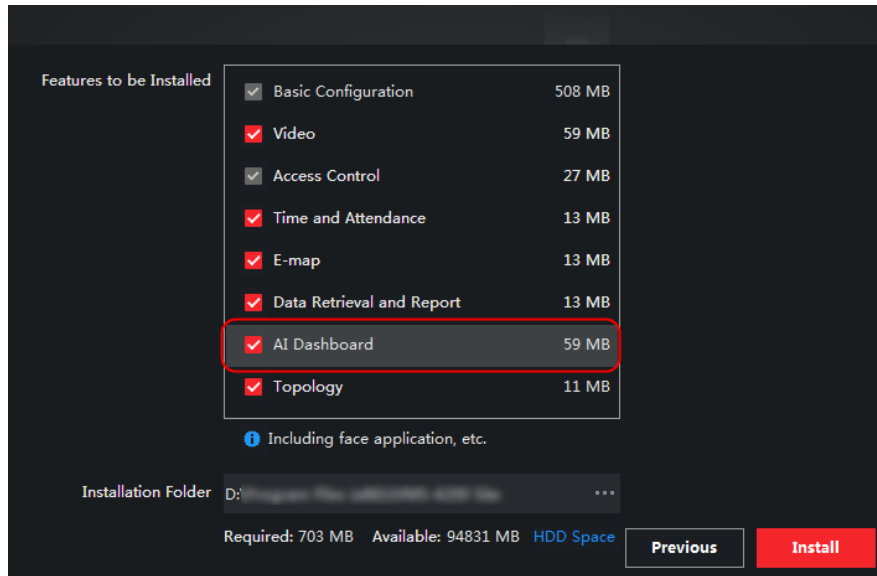


Figure 3-25 Check AI Dashboard

### Steps

1. Log in to the client, and go to **Device Management** → **Add** to add the server.
2. Configure related parameters.

#### Name

Enter a name as desired.

#### Address

Enter the IP address of the server. For stand-alone cluster, enter the actual IP address of cluster. For working and backup cluster, enter the virtual IP address.

#### Port

Keep it as the default value.

#### User Name/Password

Enter the user name and password for login.

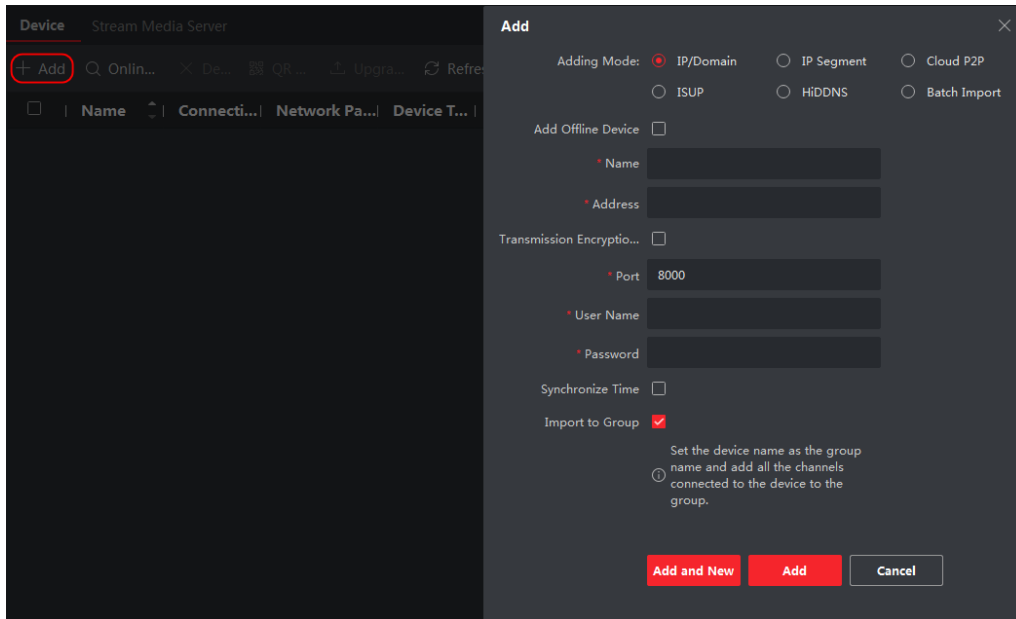


Figure 3-26 Add Server

3. Go back to the homepage, and click **AI Dashboard**.

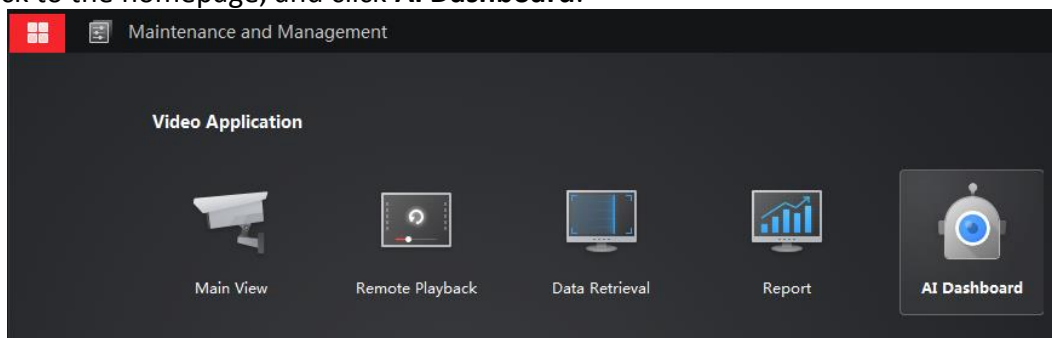


Figure 3-27 AI Dashboard

4. Go to **AI Open Platform** → .

5. Check the desired devices, and click **OK** to get imported AI algorithm package.

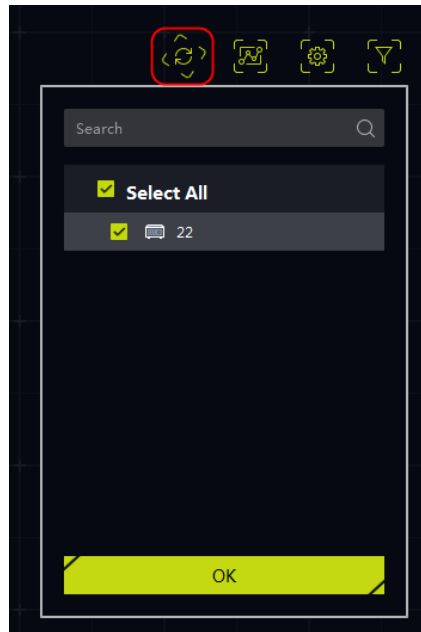


Figure 3-28 Model Package

6. Click **Picture Importing & Analysis**, and select a folder path.
7. Configure other parameters as required.

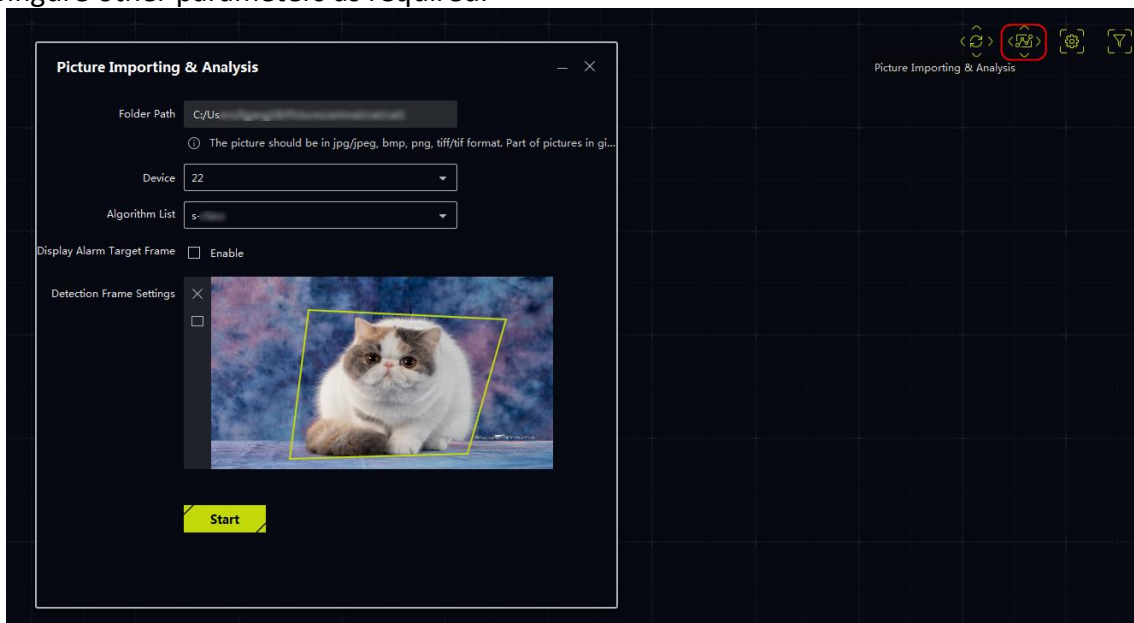


Figure 3-29 Import Picture

8. Click **Start**, and check analysis results after finished.



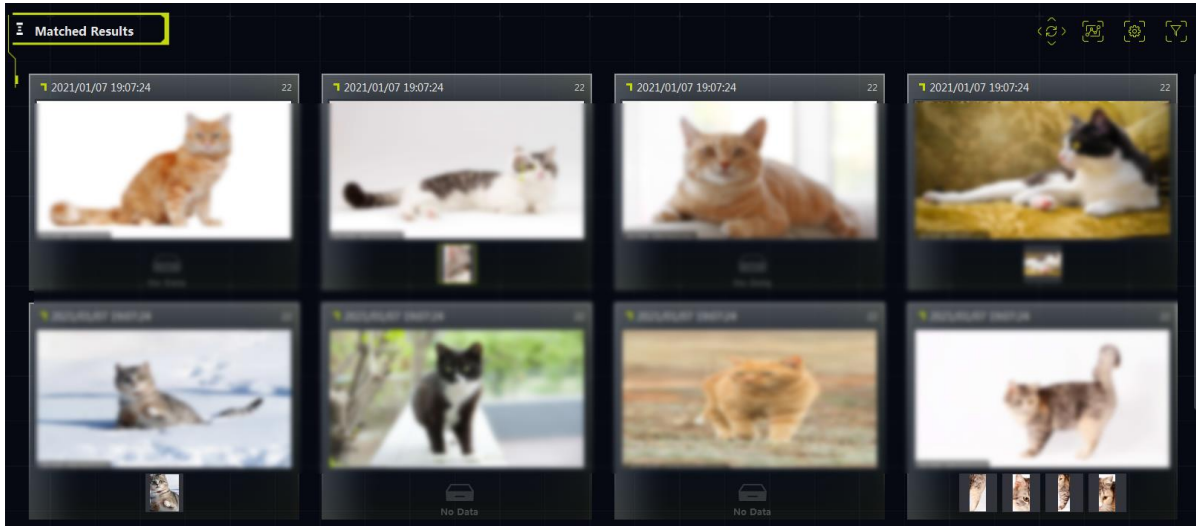


Figure 3-30 Check Analysis Result

### 3.4.5 Search AI Alarm

The AI alarm events can be searched through the client.

#### Before You Start

Install the client.

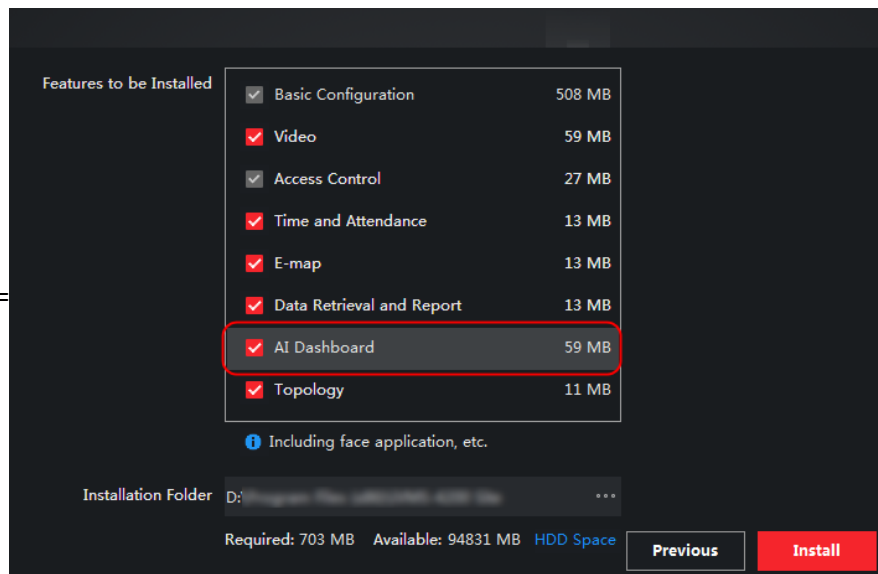


Figure 3-31 Check AI Dashboard

#### Steps

1. Log in to the client, and go to **Device Management** → **Add** to add the server.
2. Configure related parameters.

#### Name

Enter a name as desired.

## Address

Enter the IP address of the server. For stand-alone cluster, enter the actual IP address of cluster. For working and backup cluster, enter the virtual IP address.

## Port

Keep it as the default value.

## User Name/Password

Enter the user name and password for login.

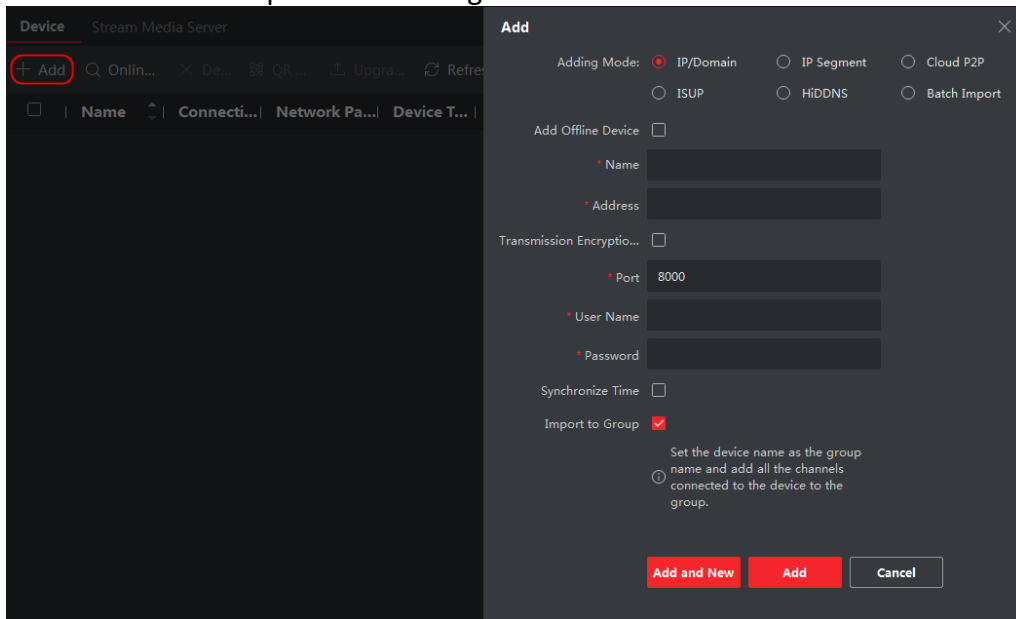


Figure 3-32 Add Server

3. Go back to the homepage, and click **Data Retrieval**.

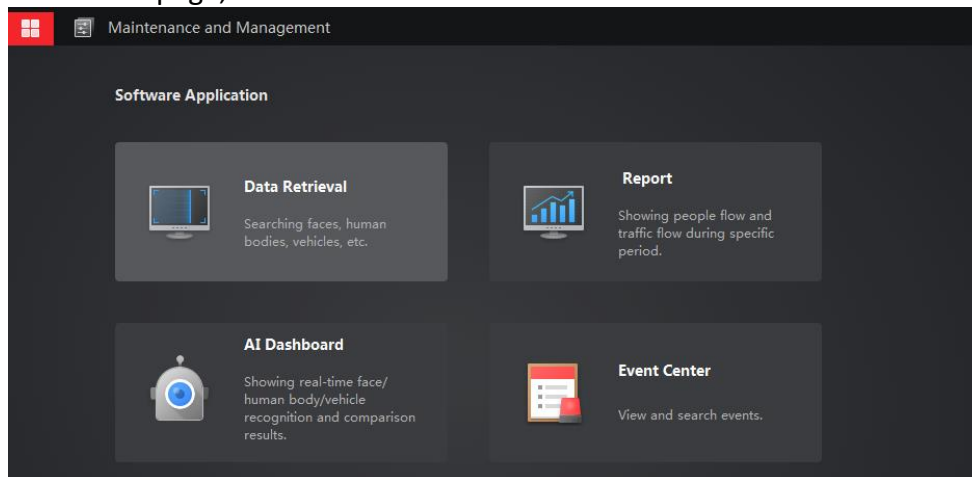


Figure 3-33 Data Retrieval

4. Click **AI Dashboard Retrieval** and set search conditions, then click **Search**.

## Video & Capture Analysis Task

Alarm events triggered by video analysis tasks.

## Picture Importing & Analysis Task

Alarm events triggered by picture analysis tasks.

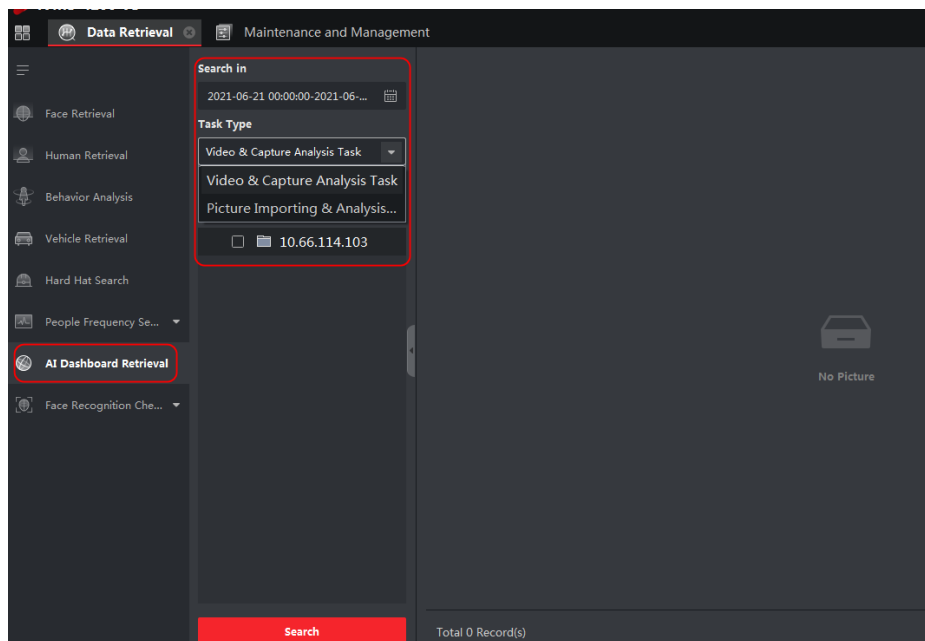


Figure 3-34 Search AI Alarm Event

## 3.5 Task Management

### 3.5.1 Configure Task

Configure the established detection rule or add a new one.

#### Steps

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

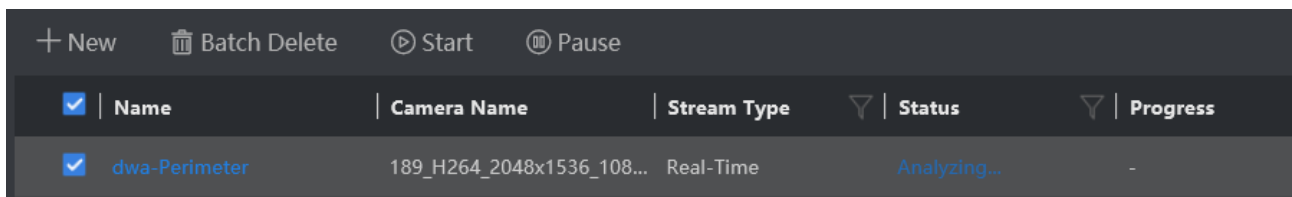


Figure 3-35 Task Management Interface

#### Note

Move your mouse to **Sub Classification Name**, **Stream Type** or **Status** to filter tasks.

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

### 3.5.2 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 **Batch Delete**, and click **OK** in the popped up box.

### 3.5.3 Pause Task

Pause a task which is being analyzed.

#### Steps

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

### 3.5.4 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 Node and Cluster Management

### 4.1 Node Management

#### 4.1.1 Delete a Node

A node can only be added once. If you need to add it to other analysis clusters, please delete the node from the added analysis cluster first.

##### Before You Start

The node is online and not in the cluster.

##### Steps

1. Go to **System Management** → **Cluster Management** → **Node Management**, and tick the node to be deleted.
2. Click **Delete**, and click **OK** in the pop-up window.

#### 4.1.2 Restart a Node

##### Before You Start

The node is online.

##### Steps

1. Go to **System Management** → **Cluster Management** → **Node Management**, and tick the node to be restarted.
2. Click **Restart**, and click **OK** in the pop-up window.

#### 4.1.2 Power a Node Off

After powering off the node, it can only be turned on by pressing the power supply. If the device has a BMC, it can be powered on remotely through the BMC.

##### Before You Start

The node is online.

##### Steps

1. Go to **System Management** → **Cluster Management** → **Node Management**, and tick the node to be powered off.
2. Click **OFF**, and click **OK** in the pop-up window.

## 4.2 Cluster Management

### 4.2.1 Add to Cluster

Move the new node into cluster to enhance the analysis ability.

#### Before You Start

The node is added.

#### Steps

1. Go to **System Management** → **Cluster Management** → **Cluster Management**.
2. Tick the node, and click **Add to Cluster**.

### 4.2.1 Remove from Cluster

#### Steps

1. Go to **System Management** → **Cluster Management** → **Cluster Management**.
2. Tick the node, and click **Remove from Cluster**.

---

#### **Note**

Please do not remove the node arbitrarily after the cluster is formed.

---

## Chapter 5 System Management

### 5.1 Basic Configuration

Keep the default value and no configuration is required.

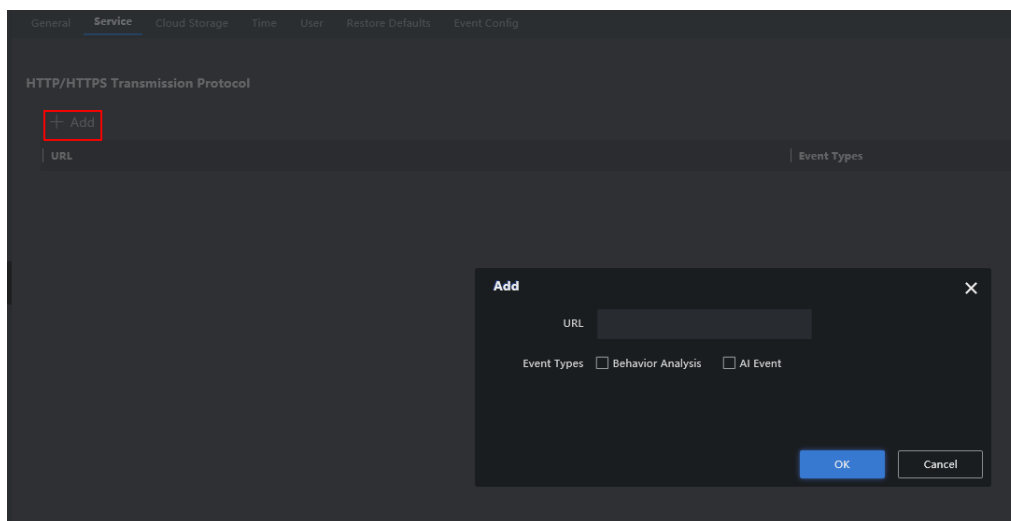
The filter function is enabled by default, so that the device can only be accessed through the IP address of the device. If port mapping is enabled, please turn off this function for normally device access.

### 5.2 Service Configuration

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

#### Steps

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



**Figure 5-1 Service Configuration Interface**

2. Configure the receiving address of the third party device. Select **Event Types**.
3. Click **OK**.

## 5.3 Cloud Storage

No need to manual configure. It is used local machine for storage and modification is not allowed.

## 5.4 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 Management** → **System Config** → **Time**.

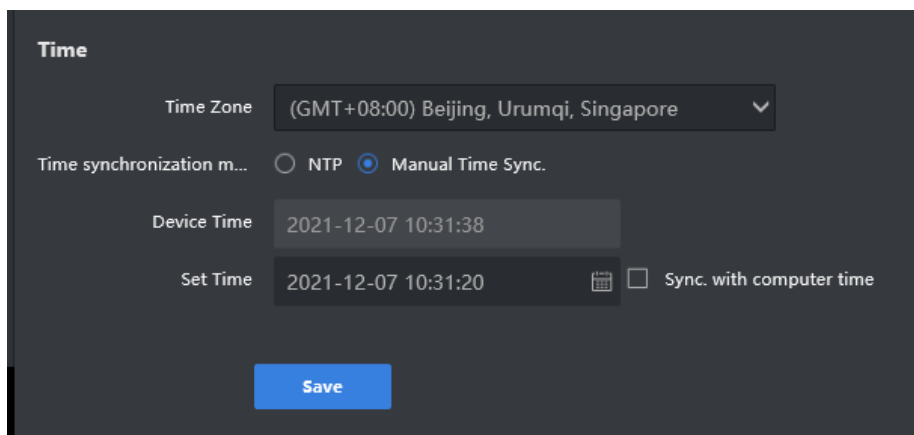


Figure 5-2 Time Configuration Interface

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**.



## 5.5 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, and consumers. Operators and consumers can only modify their own passwords.

### 5.5.1 Add User

Up to 31 users (excluding admin) can be added.

#### Before You Start

Log in the system as admin.

#### Steps

1. Go to **System Management** → **System Config** → **User**.

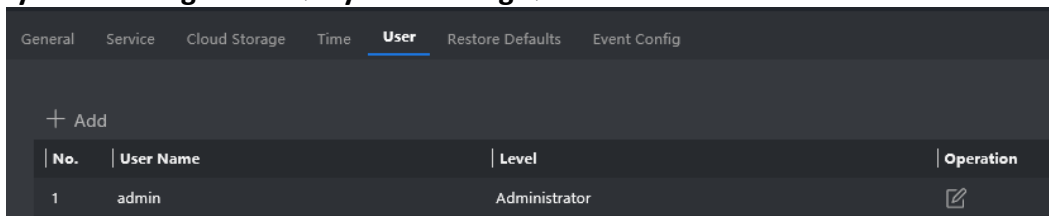
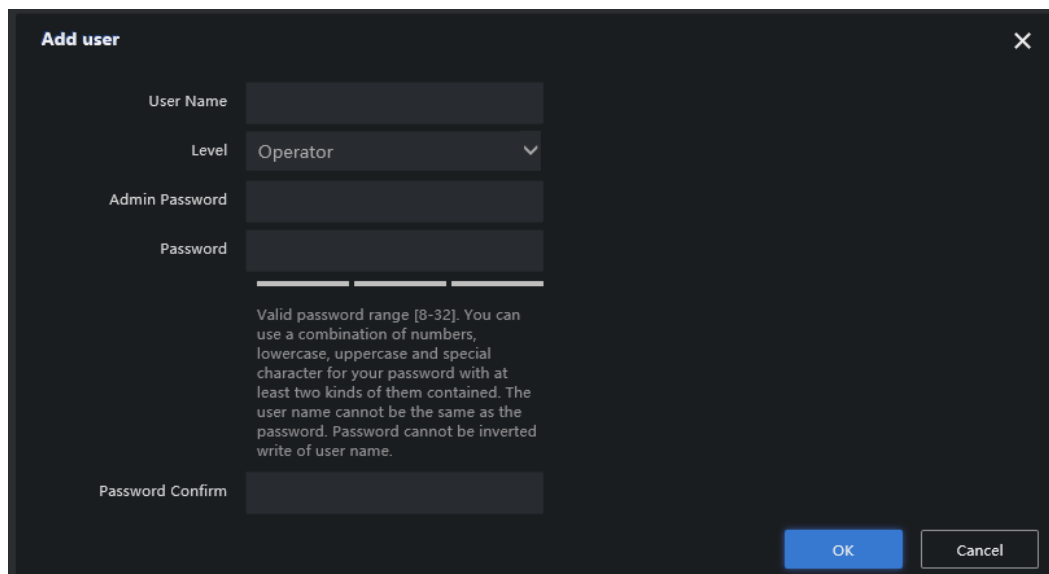


Figure 5-3 Add Users

2. Click **Add** and enter user information.



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

- User Name:
- Level:  (dropdown menu)
- Admin Password:
- Password:
- Password Confirm:

Below the password fields, there is a note: "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 user name cannot be the same as the password. Password cannot be inverted write of user name."

At the bottom right, there are 'OK' and 'Cancel' buttons.

Figure 5-4 Enter Information



#### 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.

4. Related options:

- Modify user password: Click  of the user row to modify the user password.
  - Delete user: Click  of the user row to delete it.
- 

### Note

When deleting a user, clearing user resources refers to deleting the device added by the user. If the user resources are not cleared, only the user will be deleted, and the resources created by the user will be moved to the administrator.

---

## 5.5.2 Modify admin Password

Only the administrator user can modify its own password.

### Before You Start

Log in the system as admin.

### Steps

1. Go to **System Management** → **System Config** → **User**.
2. Click  , and enter **Old Password**, **New Admin Password** and **Password Confirm**.

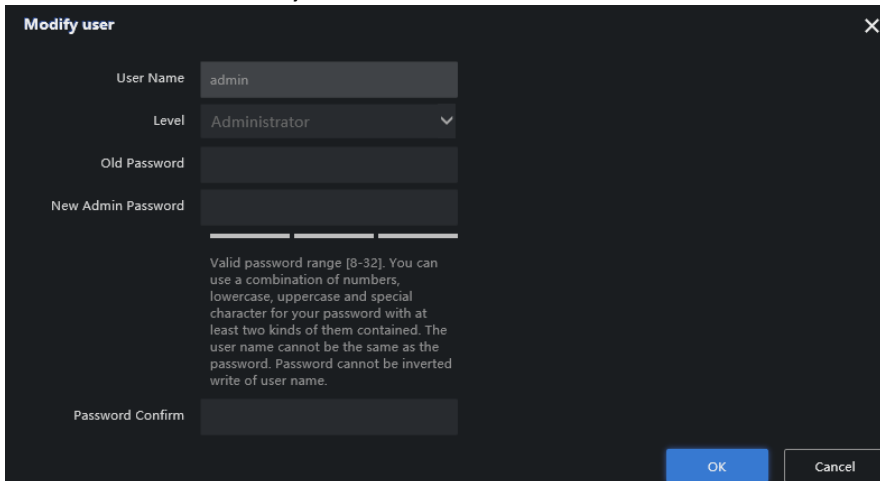


Figure 5-5 Enter Information

3. Click **OK**.

## 5.6 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: The A7 device only retains the device IP address, and the rest of the parameters are restored to the factory settings.

### Steps

1. Go to **System Management** → **System Config** → **Restore Defaults**.
2. Select **Restore** or **Default** as needed.



### Note

When the A7 device select **Default**, the IP will be restored to 192.168.1.64.

---

## 5.7 Event Configuration

### Steps

1. Go to **System Management** → **System Config** → **Event Config**.
2. Select **Scene Type** and check event as needed.
3. Click **Save**.


## 5.8 Log Management

### 5.8.1 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 Management** → **Log**.
2. Select the type of log.
3. Set the starting and ending time of search, then click **Search**.
4. Optional: Enter keywords in the search box and click  to search.
5. Optional: Click **Export**, and click **OK** in the popped up box to export desired log(s).

## 5.8.2 Download Maintenance Log

Maintenance log is used by professional maintainer to maintain device.

### Steps

1. Go to **System Management** → **Log**.
2. Click **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.

## 5.9 Software Updating

Update the software via Web interface.

### Before You Start

- Ensure that device is online without any exception.
- Obtain upgrading files.

### Steps

1. Go to **System Management** → **Software Upgrade**.

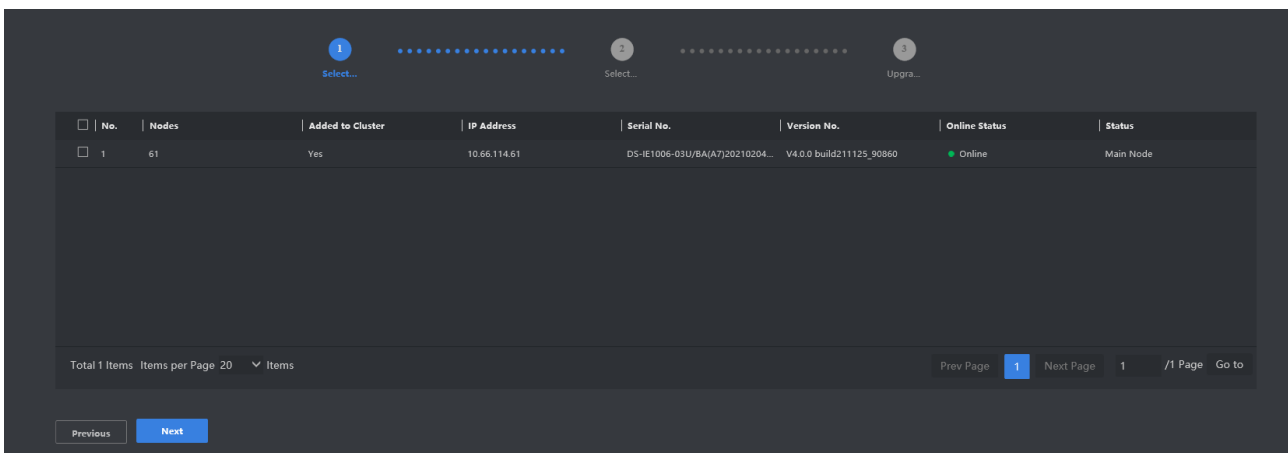


Figure 5-6 Software Upgrading

2. Tick the desired device, and click **Next**.
3. Click **Browse** and select a desired file.
4. Click **Next** after the file is uploaded.
5. Click **OK** to start upgrading.

---


 **Note**

The device will restart automatically after upgrading completed.

---

## 5.10 Information


### Hardware Status

Check hardware status by going to **System Management** → **Maintenance** → **Hardware Status**. Click  to see information, such as **CPU**, **Memory**, **GPU**, **Disk**, **Network**, **Device Status Monitoring**, and **Network Configuration**.


### Service Status

1. Check service status by going to **System Management** → **Maintenance** → **Service Status**.
2. Click **Node Information** or **Resource Statistics** to view the corresponding details.


### Online User

Check the total number of users or the number of online users by clicking  on the upper-right corner of the interface.

### Help Center

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

### Version Information

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

### Open Source Software Licenses

Check open source software licenses by going to  → **Open Source Software Licenses** on the upper-right corner of the interface.

### Log Out

#### Steps

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



## Chapter 6 iVMS-4200 Client Configuration

Accessing to the server via iVMS-4200 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 iVMS-4200 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**.

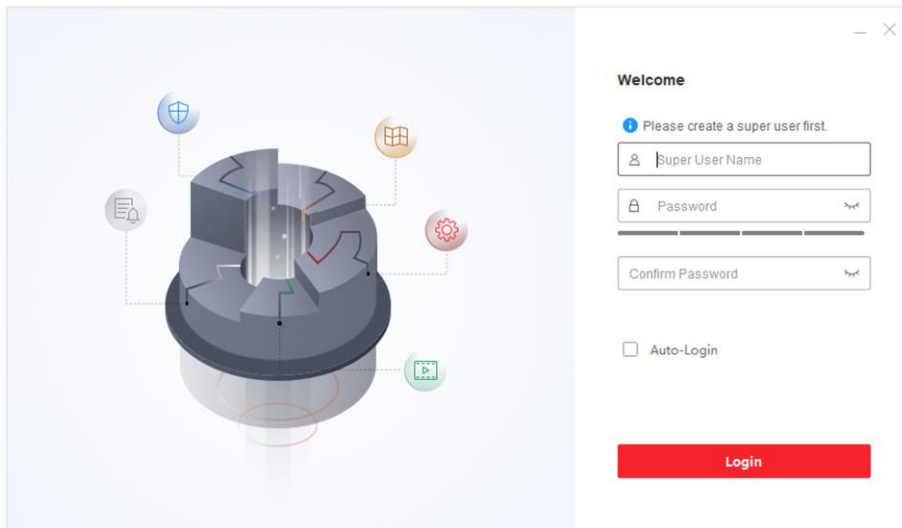


Figure 6-1 Create Super User

### 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 of 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

1. Go to **Device Management** → **Device**.
2. Click **Add**.

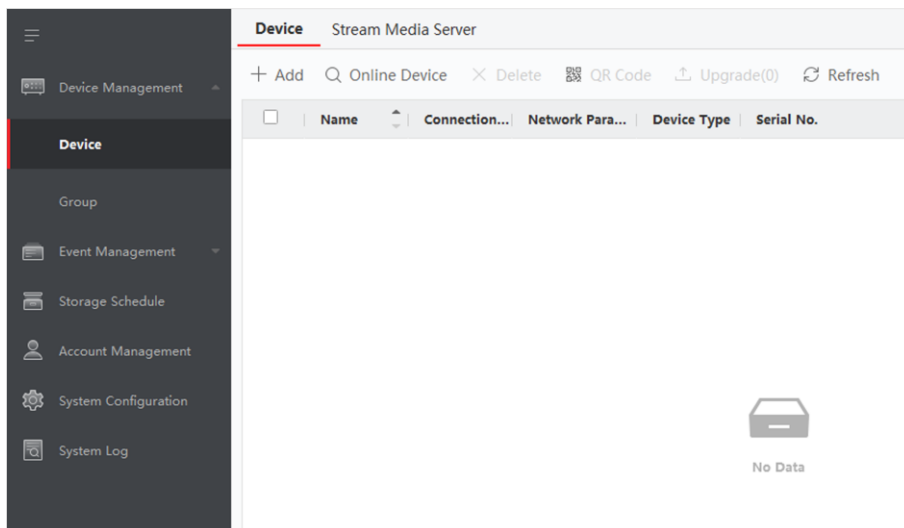


Figure 6-2 Add Device Manually

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



The screenshot shows a dialog box titled "Add" with a close button (X) in the top right corner. It contains the following fields and options:

- Adding Mode:** Three radio buttons:  IP/Domain,  IP Segment,  Cloud P2P.
- HiDDNS and  Batch Import.
- Add Offline Device:**
- \* Name:** A text input field.
- \* Address:** A text input field.
- \* Transmission Encrypti...:**
- \* Port:** A text input field containing "8000".
- \* User Name:** A text input field.
- \* Password:** A text input field.
- Synchronize Time:**
- Import to Group:**
- A help icon (i) with the text: "Set the device name as the group name and add all the channels connected to the device to the group."
- At the bottom, there are three buttons: "Add and New" (red), "Add" (red), and "Cancel" (white).

Figure 6-3 Configure Device Parameters

4. Click **Add**.

---

 **Note**

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 **Device Management** → **Device**.
2. Click **Online Device** and check the desired device.

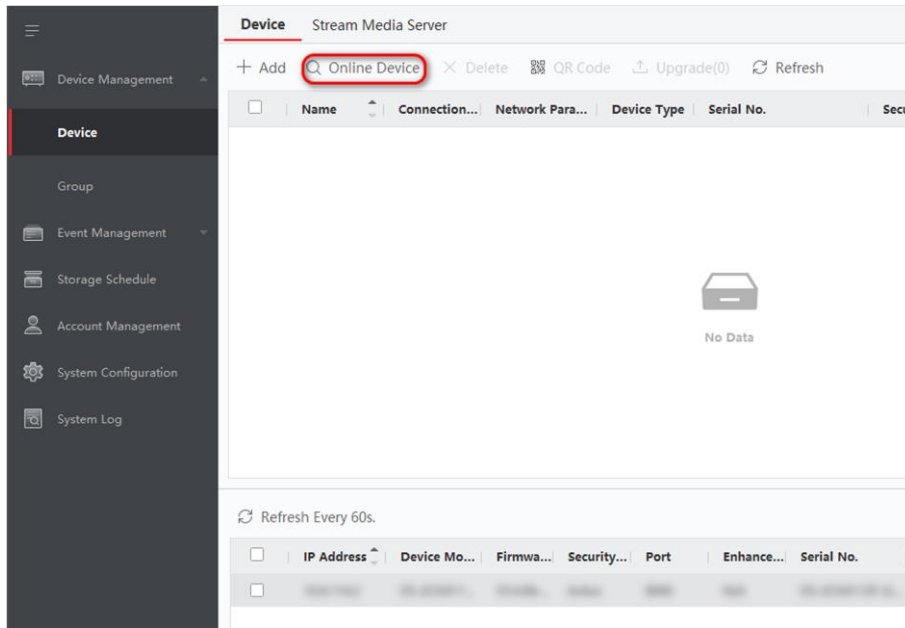


Figure 6-4 Add Online Device

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 View Analysis Task Frame

View the video frame of analysis task.

### Steps

1. Click  → **AI Dashboard** → **Abnormal Event Detection**.
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.

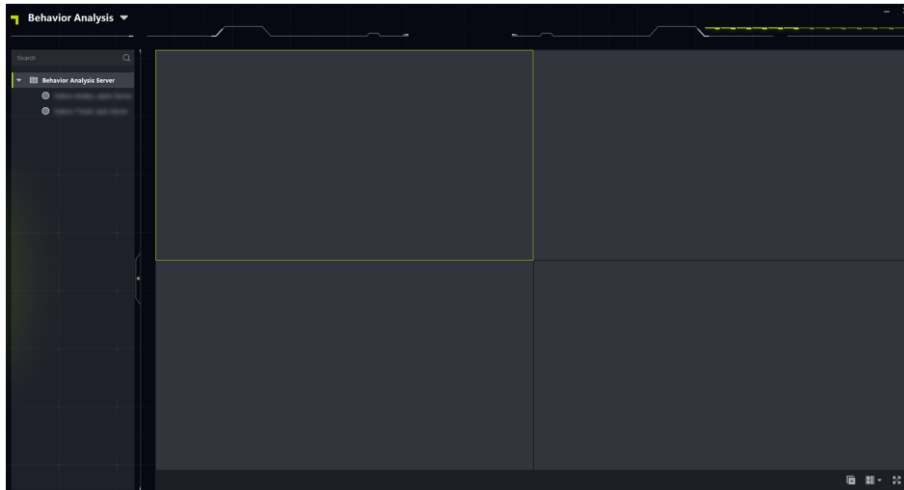


Figure 6-7 View Real-time Analysis Results

**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

## 6.4 Remote Configuration

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

### Steps

Click **Device Management** → **Device**, click in list of **Operation**.

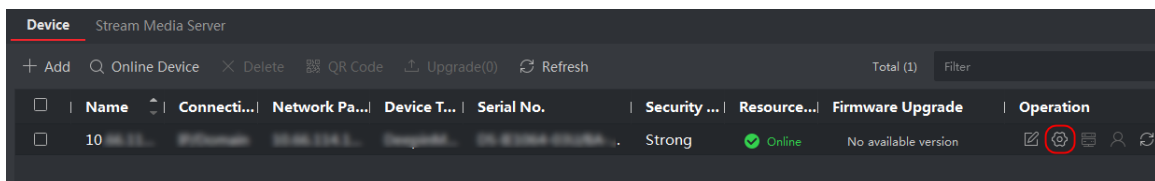


Figure 6-8 Select Remote Configuration

<input type="checkbox"/>	Name	Camera Name	Stream Type	Status	Progress	CreateTime
<input type="checkbox"/>	Real-Time Analysis	192.168.1.100	Real-Time	Analyzing...	-	2021-03-06 23:57:02
<input type="checkbox"/>	Real-Time Analysis	192.168.1.100	Real-Time	Analyzing...	-	2021-03-06 23:56:40
<input type="checkbox"/>	Real-Time Analysis	192.168.1.100	Real-Time	Analyzing...	-	2021-03-06 23:55:59
<input type="checkbox"/>	Real-Time Analysis	192.168.1.100	Real-Time	Analyzing...	-	2021-03-06 23:55:32
<input type="checkbox"/>	Real-Time Analysis	192.168.1.100	Real-Time	Analyzing...	-	2021-03-06 11:17:59
<input type="checkbox"/>	Real-Time Analysis	192.168.1.100	Real-Time	Analyzing...	-	2021-03-05 18:14:28
<input type="checkbox"/>	Real-Time Analysis	192.168.1.100	Real-Time	Analyzing...	-	2021-03-05 18:12:54


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**.

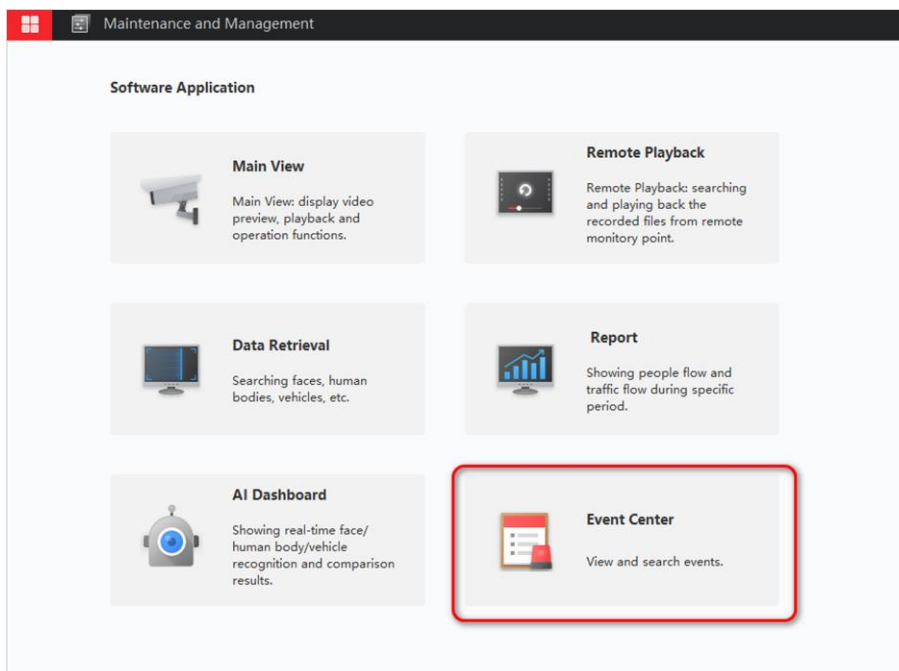


Figure 6-11 Click Event Center

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

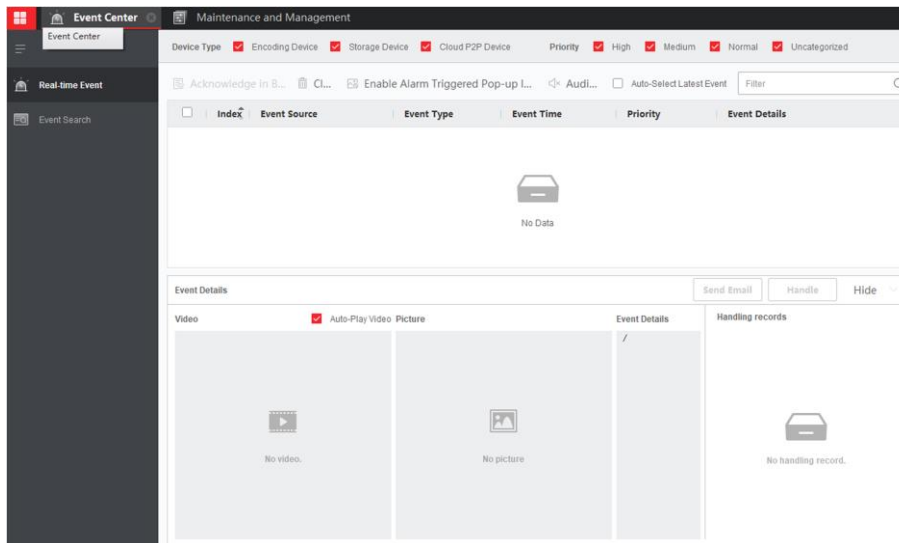


Figure 6-12 Real-time Event Alarm Information

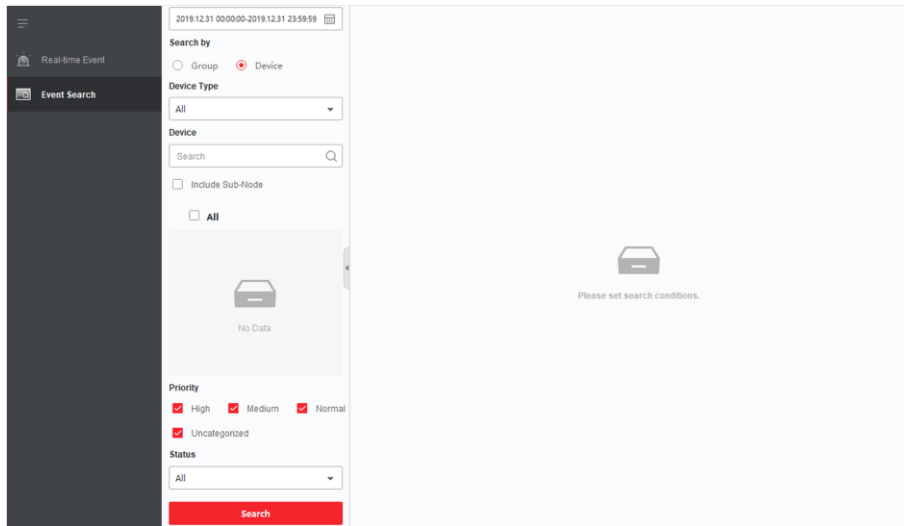
Operation	Description
Clear List	Click  or click the right button of mouse in the alarm information list and click <b>Clear</b> to clear the alarm information.
Alarm Sound	The alarm sound is off by default. Click  to turn on the alarm sound and  to close.
Alarm Pop-up Window	The alarm pop-up window is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

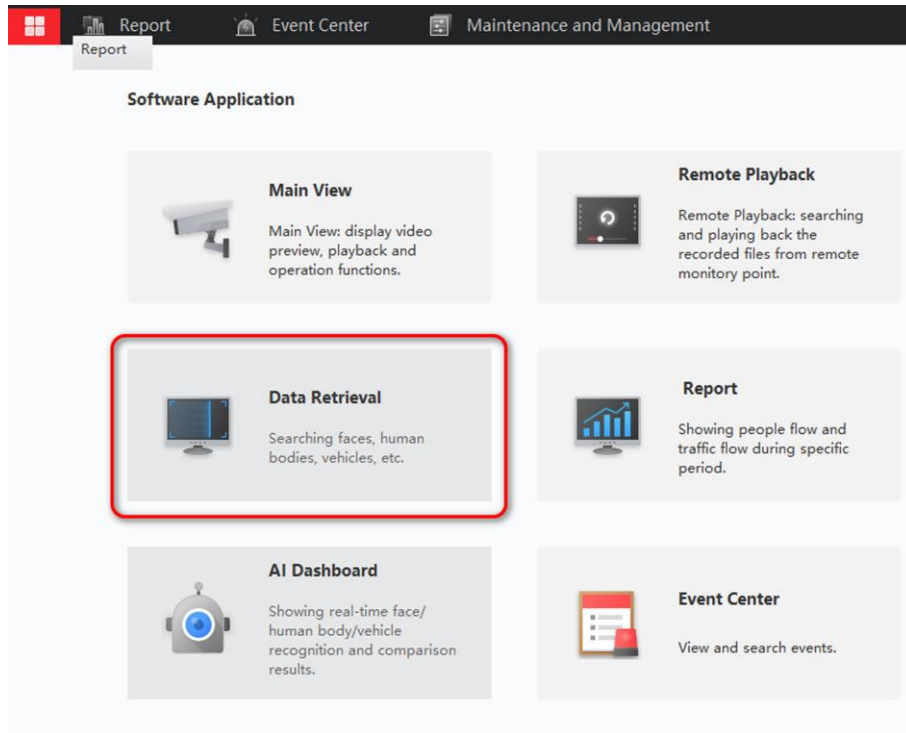
2. Set searching conditions, and click **Search**.
3. Click on the desired event to view details.

## 6.6 Data Retrieval

Search alarm event and export related images.

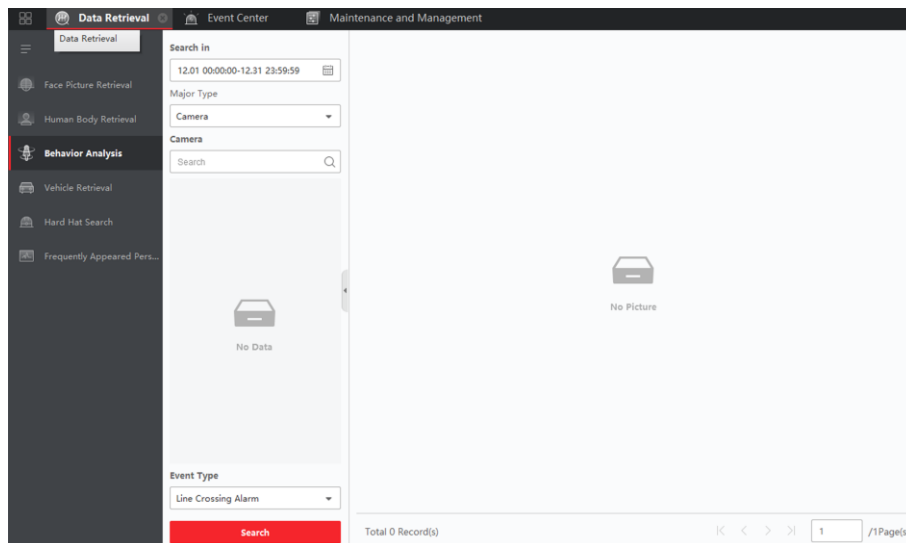
### Steps

1. Go to  → **Data Retrieval**.



**Figure 6-14 Data Retrieval**

2. Click **Abnormal Event Detection** 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.

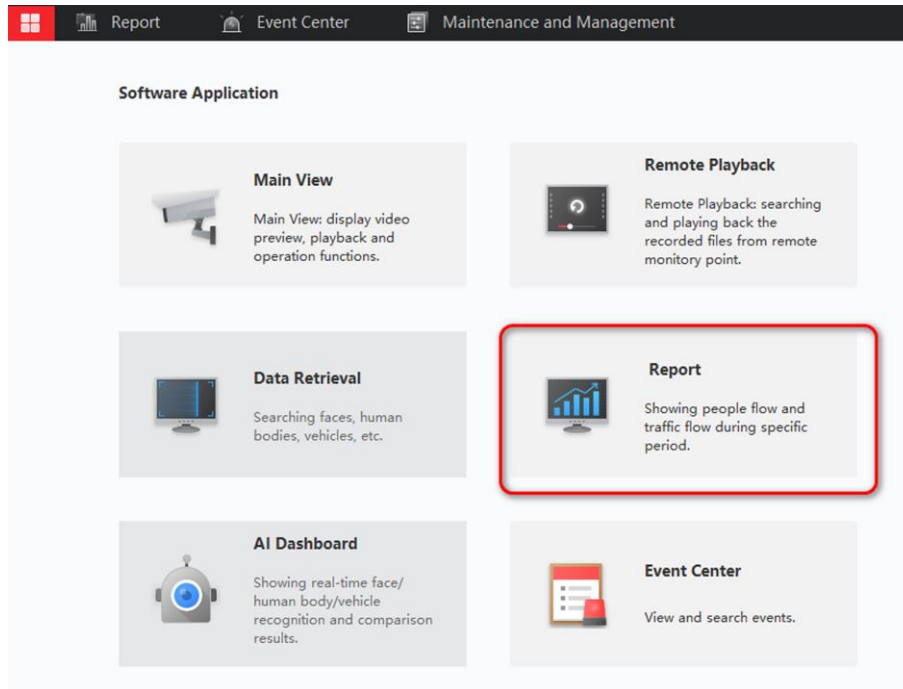
5. Optional: Click **Export** to download related images of the event.

## 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

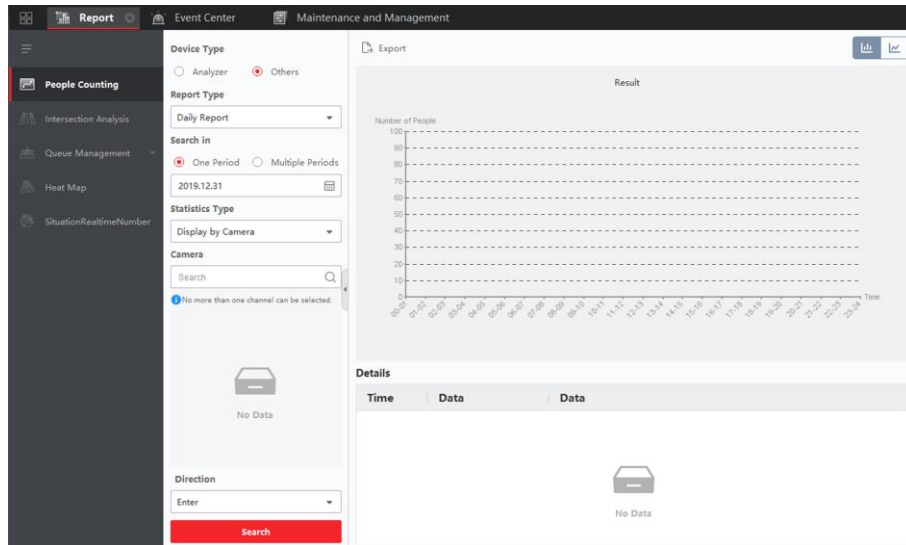
1. Go to  → **Report**.



**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