



Behavior Analysis Server

User Manual

© 2019 Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

This Manual is the property of Hangzhou Hikvision Digital Technology Co., Ltd. or its affiliates (hereinafter referred to as “Hikvision”), and it cannot be reproduced, changed, translated, or distributed, partially or wholly, by any means, without the prior written permission of Hikvision. Unless otherwise expressly stated herein, Hikvision does not make any warranties, guarantees or representations, express or implied, regarding to the Manual, any information contained herein.

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 <http://www.hikvision.com/en/>).

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

Trademarks Acknowledgement

- **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.
- **HDMI**™ The terms HDMI and HDMI High-Definition Multimedia Interface, and the HDMI Logo are trademarks or registered trademarks of HDMI Licensing Administrator, Inc. in the United States and other countries.

LEGAL 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 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

 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

Industry Canada ICES-003 Compliance

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




Applicable Models

– This manual is applicable to the models listed in the following table.

Series	Model
Behavior Analysis Server	DS-IE1016-03U/BA
	DS-IE1024-03U/BA
	DS-IE1032-03U/BA
	DS-IE1064-03U/BA

Symbol Conventions

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

Symbol	Description
 NOTE	Provides additional information to emphasize or supplement important points of the main text.
 WARNING	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
 DANGER	Indicates a hazard with a high level of risk, which if not avoided, will result in death or serious injury.

Safety Instructions

- 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 to 240 VAC or 12 VDC 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.

TABLE OF CONTENTS

Chapter 1 Introduction	1
Chapter 2 Activation and Login	3
2.1 Configuration Requirements	3
2.2 Activation	3
2.2.1 Activate via SADP Software	3
2.2.2 Activate via Web Browser	4
2.3 Login	5
Chapter 3 Configuration Wizard	6
3.1 Create an Analysis Cluster	6
3.1.1 Add a Smart Analysis Unit	6
3.1.2 Create a Stand-Alone Analysis Cluster	6
3.2 Add Resource	7
3.2.1 Add a Camera	7
3.2.2 Add a Video Recording	9
3.3 Perimeter Analysis Task	10
3.3.1 Create a Perimeter Analysis Task	10
3.3.2 Line Crossing Detection	11
3.3.3 Region Entrance Detection	13
3.3.4 Region Exiting Detection	15
3.3.5 Intrusion Detection	17
3.3.6 Loitering Detection	19
3.3.7 Parking Detection	22
3.3.8 Unattended Baggage Detection	24
3.3.9 Object Removal Detection	27
3.4 Trend Analysis Task	29
3.4.1 Create a Trend Analysis Task	29
3.4.2 People Density Analysis	30
3.4.3 Real-time People Counting	32
3.4.4 People Counting	34
3.5 Indoor Analysis Task	36
3.5.1 Create an Indoor Analysis Task	36
3.5.2 Physical Conflict Detection	37
3.5.3 Getting-up Detection	39

3.5.4 Key Person Getting-up Detection	42
3.5.5 Absence/Sleep on Duty Detection	44
3.5.6 Standing-up Detection	47
3.5.7 Sudden Change of Sound Intensity Detection	49
3.5.8 Climbing Detection.....	51
3.5.9 Overstaying Detection.....	52
3.5.10 Regional Overstaying Detection.....	54
3.5.11 Abnormal Number of People Detection	56
3.5.12 Sitting Detection.....	59
3.5.13 People Counting	61
3.6 Street Analysis Task	63
3.6.1 Create a Street Analysis Task.....	63
3.6.2 Falling-down Detection	64
3.6.3 Fast Moving Detection	66
3.6.4 Physical Conflict Detection.....	68
3.6.5 People Gathering Detection.....	70
Chapter 4 Task Management	73
4.1 Edit a Task.....	73
4.2 Delete a Task	74
4.3 Pause a Task	74
4.4 Start a Task	74
Chapter 5 Smart Analysis Unit Management	75
5.1 Add a Smart Analysis Unit	75
5.2 Add to Cluster.....	75
5.3 Remove from Cluster.....	75
5.4 Restart a Smart Analysis Unit.....	76
5.5 Close a Smart Analysis Unit.....	76
5.6 Configure Network Parameters.....	76
5.7 View Hardware Resource	77
Chapter 6 System Management	78
6.1 Basic Configuration	78
6.2 Service Configuration	78
6.3 Time Configuration.....	78
6.4 User Management	79
6.4.1 Add a User	79

6.4.2 Modify a Password	80
6.4.3 Delete a User	80
6.5 Log Management	81
6.5.1 Log Search	81
6.5.2 Download Maintenance Log	81
6.6 Smart Mode	81
6.7 Software Updating	82
6.8 Restore Defaults	83
6.9 Help Center	83
6.10 Version Information	83
6.11 Logout	83
6.12 Obtain iVMS-4200 Client Software	84
Chapter 7 Guarding Vision Client Configuration	85
7.1 Login	85
7.2 Add a Server	86
7.2.1 Add Server Manually	86
7.2.2 Add Server Online	87
7.3 Remote Configuration	87
7.4 Live View	88
7.5 Alarm Center	90
7.6 (Optional) Configure Storage Server	91
7.6.1 Install Storage Server	91
7.6.2 Add Storage Server	92
7.6.3 Configure Storage Server	93
7.7 Configure Storage Schedule	94

Chapter 1 Introduction

Behavior Analysis Server supports the following scenes: perimeter, trend, indoor and street.

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.
- Unattended Object: An alarm will be triggered when the unattended time of an object left 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.

Trend

- Crowd Trend Analysis: Count the number of people in the detection area, and generate a people heat map.
- Regional 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 in the detection area such as the supermarket, museum that features a large flow of people, and upload the data according to the time interval set.

Indoor

- Physical Conflict: An alarm will be triggered when the physical conflict time of two or more people exceeds the time set.
- Getting-up: An alarm will be triggered when a person in the detection area gets up.
- Key Person Getting-up: An alarm will be triggered when a targeted person gets up in the dangerous person detection area drawn.
- Absence/Sleep on Duty: An alarm will be triggered when the time a person on duty stays motionless or leaves the detection area exceeds the time set.
- Standing-up: An alarm will be triggered when a person in the detection area stands up.
- Sudden Change of Sound Intensity: An alarm will be triggered when the sound intensity in the detection area is abnormal.
- Climbing: An alarm will be triggered when a person climbs over the height set.
- Overstaying: An alarm will be triggered when the staying period of a person indoor

exceeds the time set.

- Regional Overstaying: An alarm will be triggered when the staying period of a person in detection area exceeds the time set.
- Abnormal Number of People: An alarm will be triggered when the number of people in the detection area does not match the value set.
- Sitting: An alarm will be triggered when the sedentary time of a person exceeds the time set.
- People Counting: Count the number of people with the same duration of stay during different time periods in the detection area, 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: An alarm will be triggered when the physical conflict time of persons 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 Configuration Requirements

You can get access to the server via Web browser. The requirements for your PC are shown below.

Table 2-1 Configuration Requirements

Operating System	CPU	Memory	Resolution	Browser
Microsoft Windows 7, Microsoft Windows 8	Intel® Pentium IV 3.0 GHz or above	1 GB or larger	1024 × 768 or higher	IE8 to IE11

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

Step 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.

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



NOTE

After server is activated, the **Activation Status** will change to **Active**.

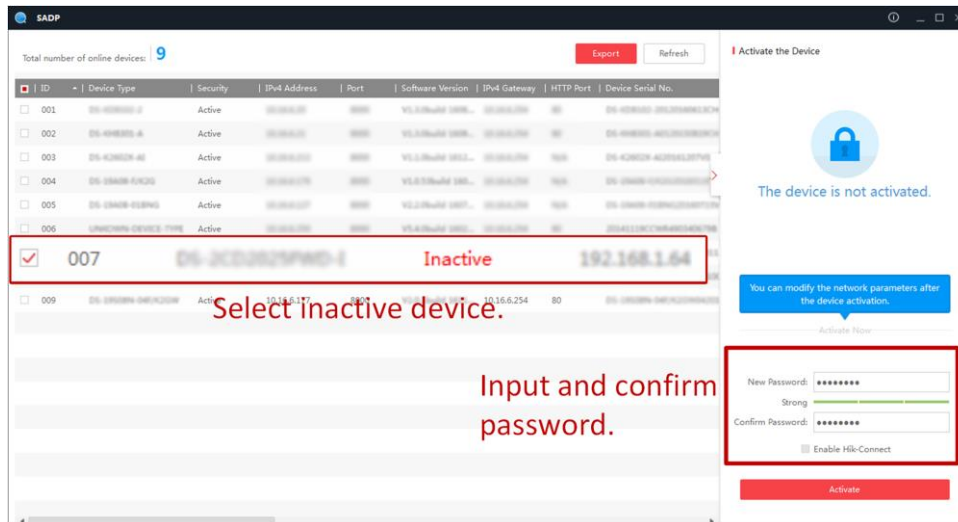


Figure 2-1 Activate Behavior Analysis Server

NOTE

- 8 to 32 characters allowed, including at least 2 of the following types: upper-case letters, lower-case letters, digits, and special characters.
- To protect your privacy and enterprise data, avoid device network security problem, we highly recommend you create a strong password in accordance with security rules.

Step 3 Modify server IP address.

1. Select the activated server. Enter IP address, subnet mask and gateway, etc. in the **Modify Network Parameters** window.
2. Enter the password and lick **Modify**. The popped up **Network Parameters Edited** indicates that network parameters settings take effect.

NOTE

- 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

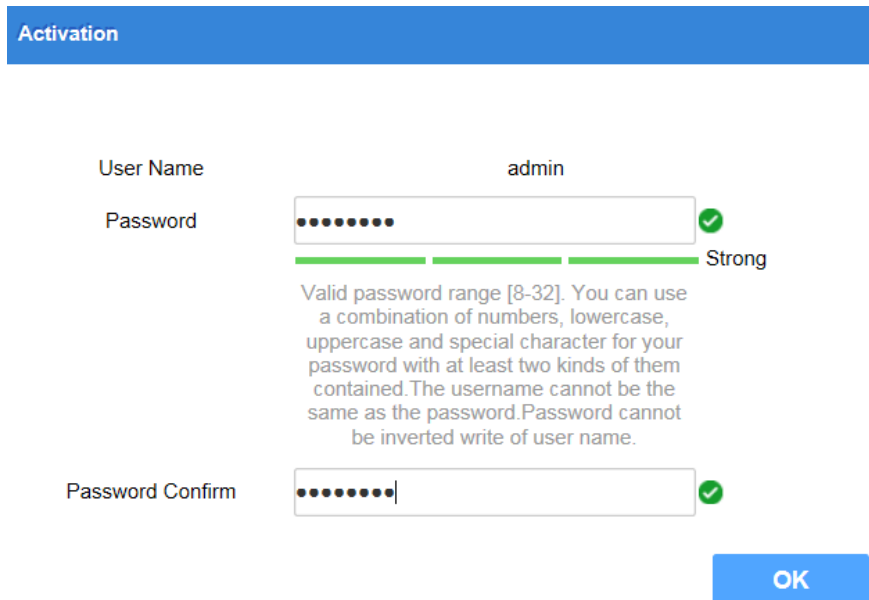
You can activate the server via Web browser.

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

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



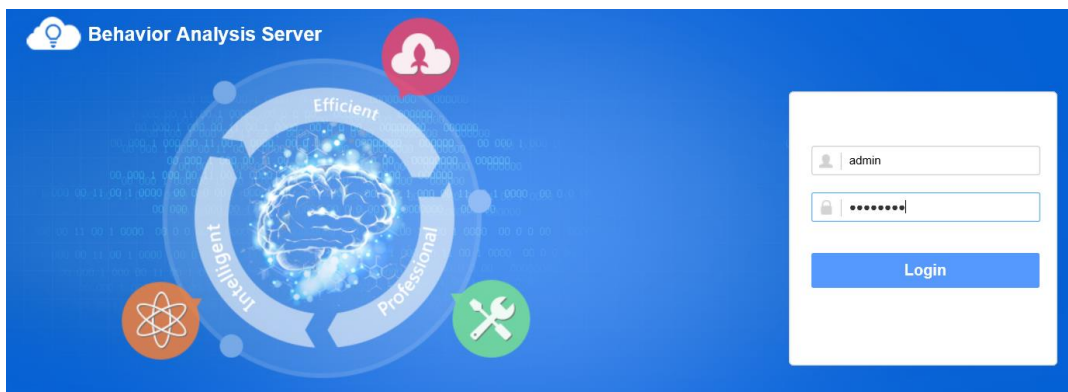
The screenshot shows the 'Activation' interface. At the top, there is a blue header with the word 'Activation' in white. Below the header, there are three input fields: 'User Name' with the value 'admin', 'Password' with a masked password and a green checkmark, and 'Password Confirm' with a masked password and a green checkmark. A green progress bar is shown below the password field, with the word 'Strong' to its right. Below the password field, there is a text box containing the following text: '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.' At the bottom right, there is a blue 'OK' button.

Figure 2-2 Activation Interface

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

2.3 Login

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



The screenshot shows the 'Behavior Analysis Server' login interface. The background is blue with a central graphic of a brain surrounded by the words 'Efficient', 'Intelligent', and 'Professional'. There are three icons: a lightbulb, a person, and a wrench. On the right side, there is a white login form with a blue 'Login' button. The form contains two input fields: 'User Name' with the value 'admin' and 'Password' with a masked password. The 'Login' button is blue with white text.

Figure 2-3 Login Interface

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

Chapter 3 Configuration Wizard

3.1 Create an Analysis Cluster

3.1.1 Add a Smart Analysis Unit

Add smart analysis units to create an analysis cluster.

Before you start

The smart analysis unit has been online.

Steps

Step 1 Click **Service -> Smart Unit**, and then click **Add**.

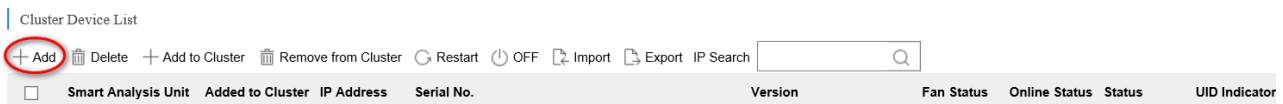


Figure 3-1 Add Smart Analysis Unit

Step 2 Enter **Name**, **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' with the value '131' and a green checkmark to its right; 'Smart Analysis Unit IP' with a blurred value and a green checkmark to its right; and 'Port' with the value '8088'. At the bottom of the dialog are two buttons: 'OK' (highlighted in blue) and 'Cancel'.

Figure 3-2 Enter Parameters

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

3.1.2 Create a 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

You have added at least one smart analysis unit.

Steps

Step 1 Select the smart analysis unit, and click **Create Cluster**.

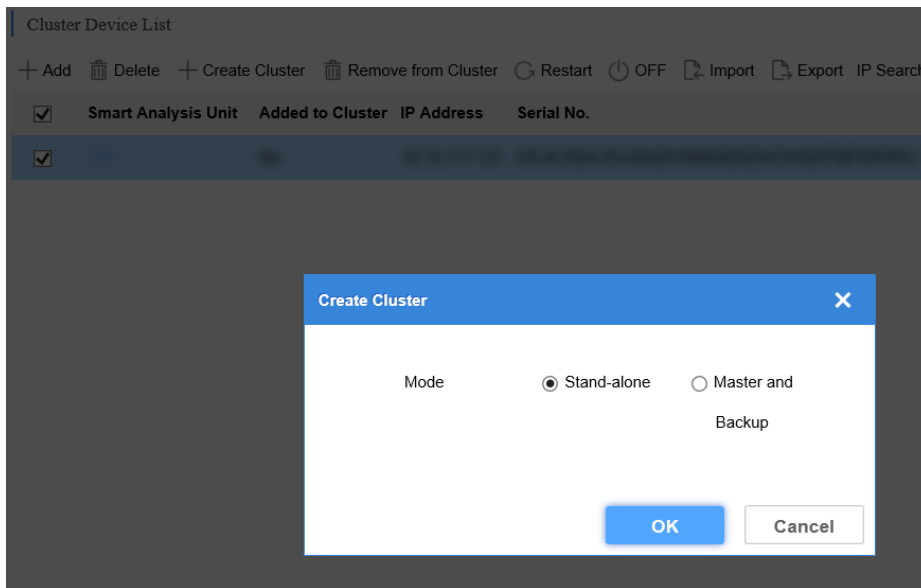


Figure 3-3 Create Stand-Alone Cluster

Step 2 Select **Mode** as **Stand-alone**, click **OK**.

3.2 Add Resource

Add camera and video recording for behavior analysis.

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.

Steps



- 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.

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

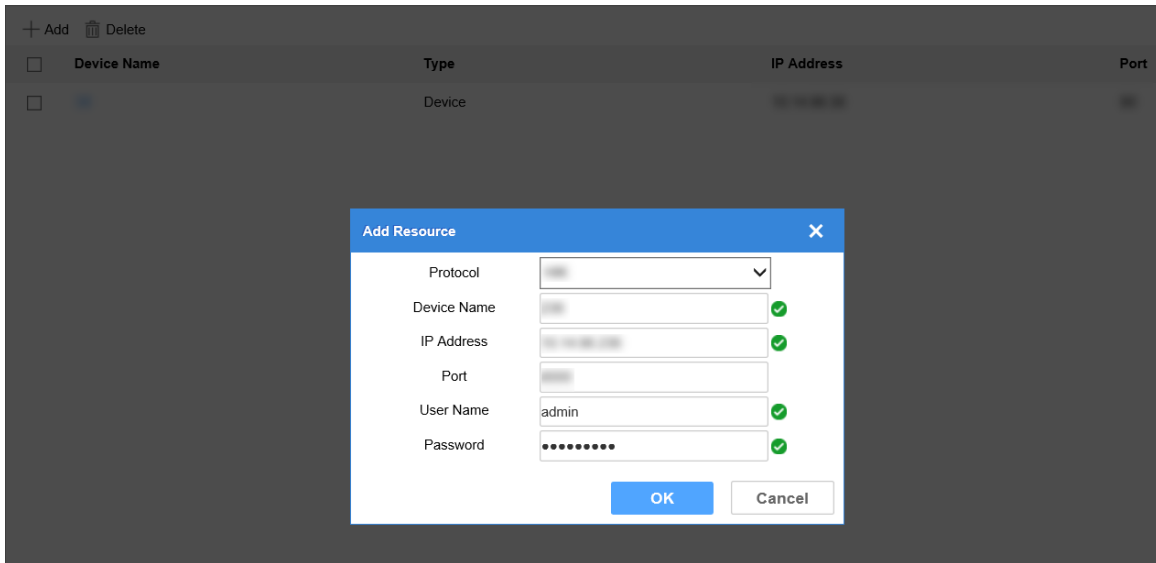


Figure 3-4 Add Camera

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

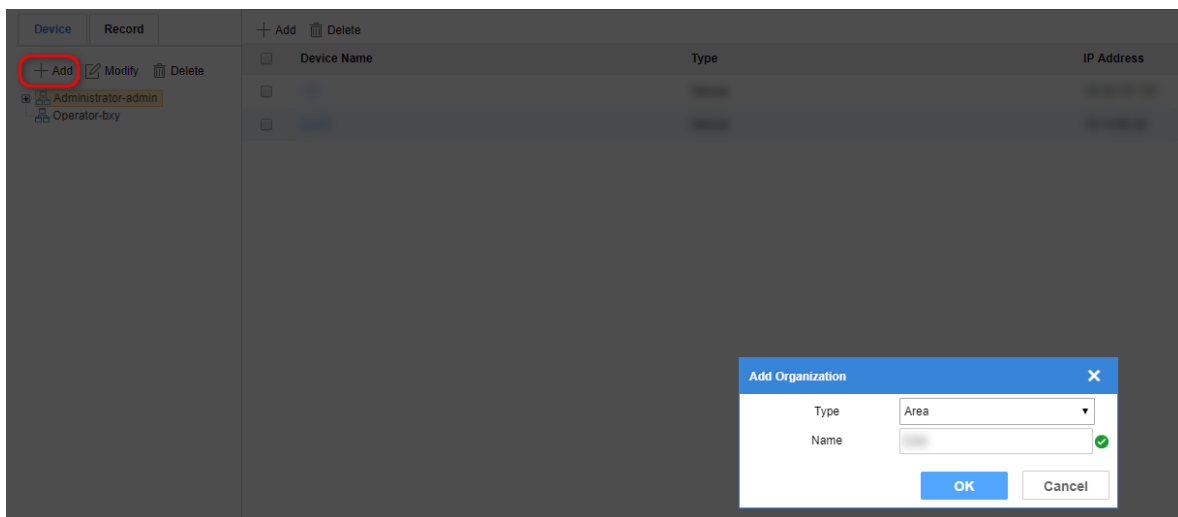


Figure 3-5 Add Area

 **NOTE**

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

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

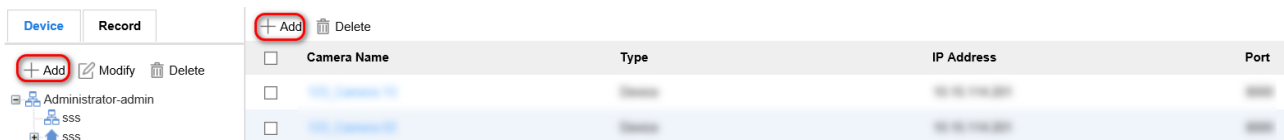


Figure 3-6 Add Camera

NOTE

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

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

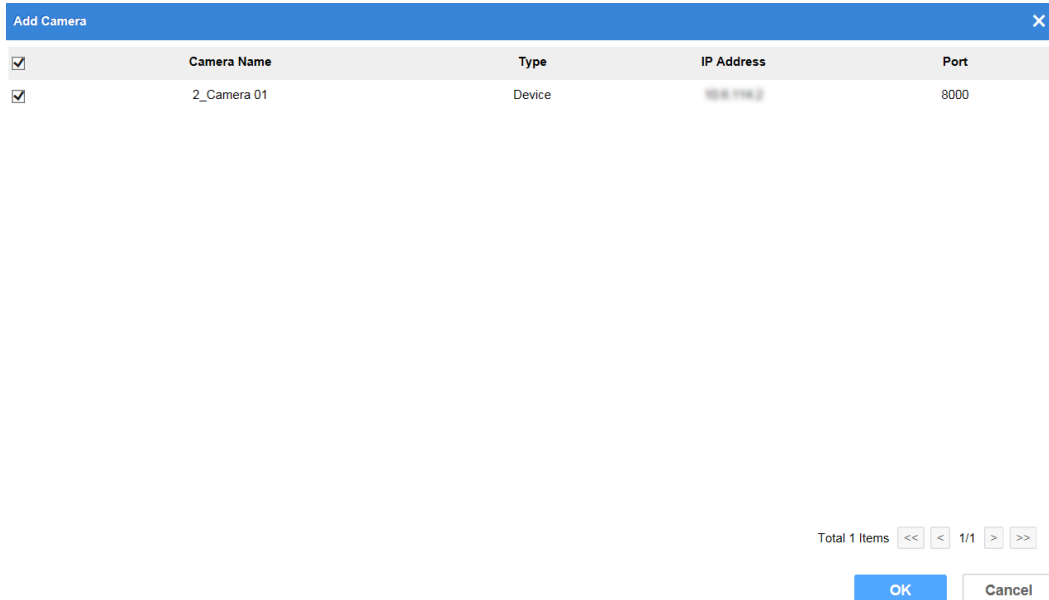


Figure 3-7 Add a Camera to Area

NOTE

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

3.2.2 Add a Video Recording

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

Steps

NOTE

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

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

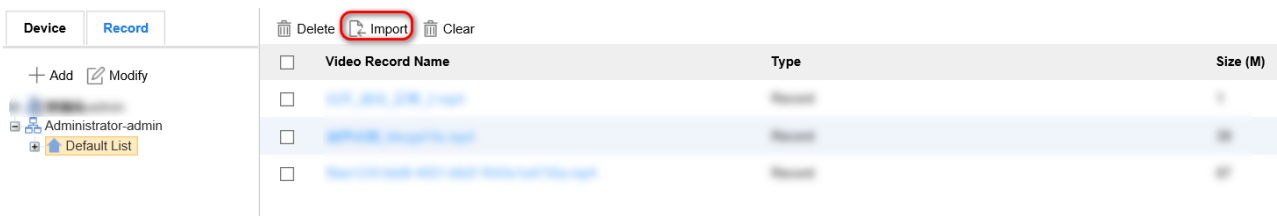


Figure 3-8 Import Video Interface

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

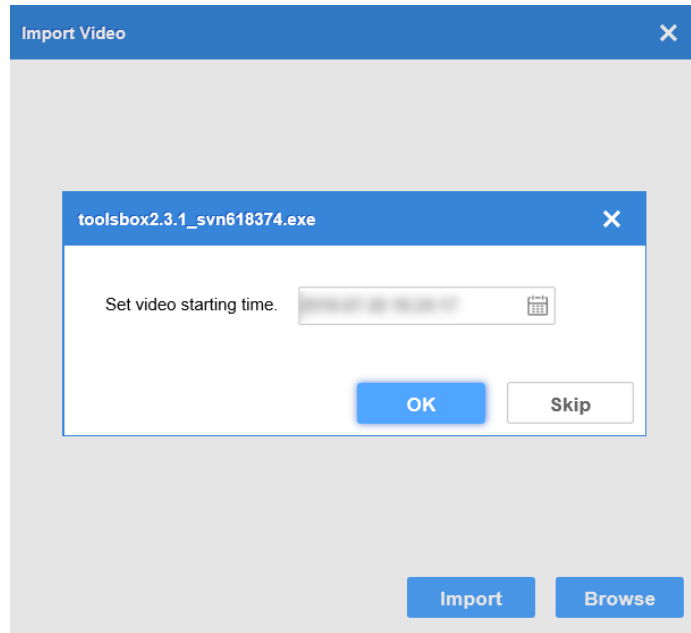


Figure 3-9 Set Video Starting Time.

 **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.

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

3.3 Perimeter Analysis Task

3.3.1 Create a Perimeter Analysis Task

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

Steps

Step 1 Click **Task Management** -> **New**.

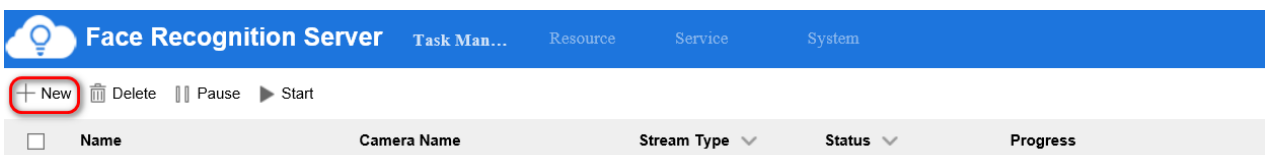


Figure 3-10 Task Management Interface

Step 2 Enter a task name.

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

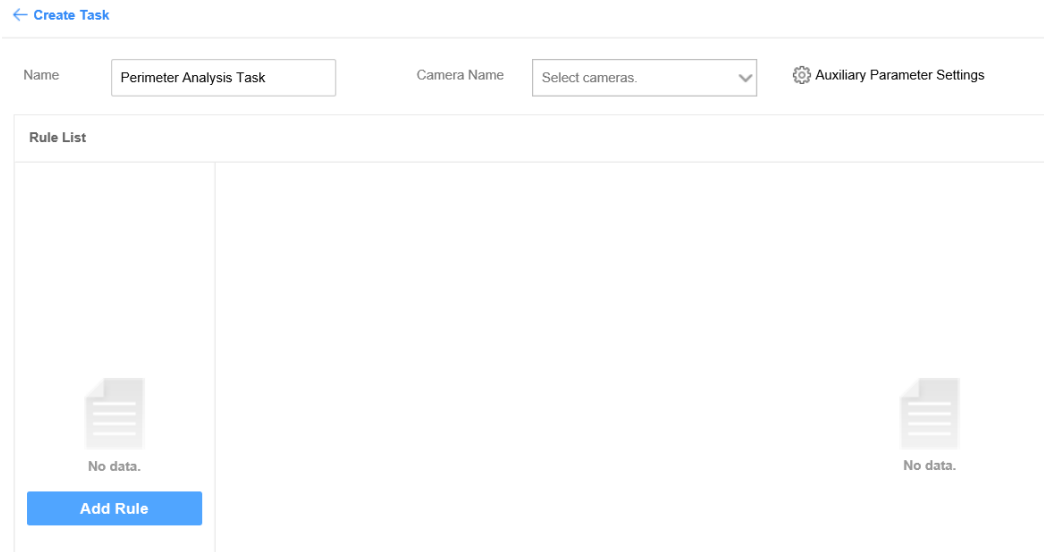


Figure 3-11 Create Task Interface

NOTE

Keep **Auxiliary Parameter Settings** by default.

Step 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

Step 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 **Perimeter**.
- **Event:** select **Line Crossing Detection**

Step 2 (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.

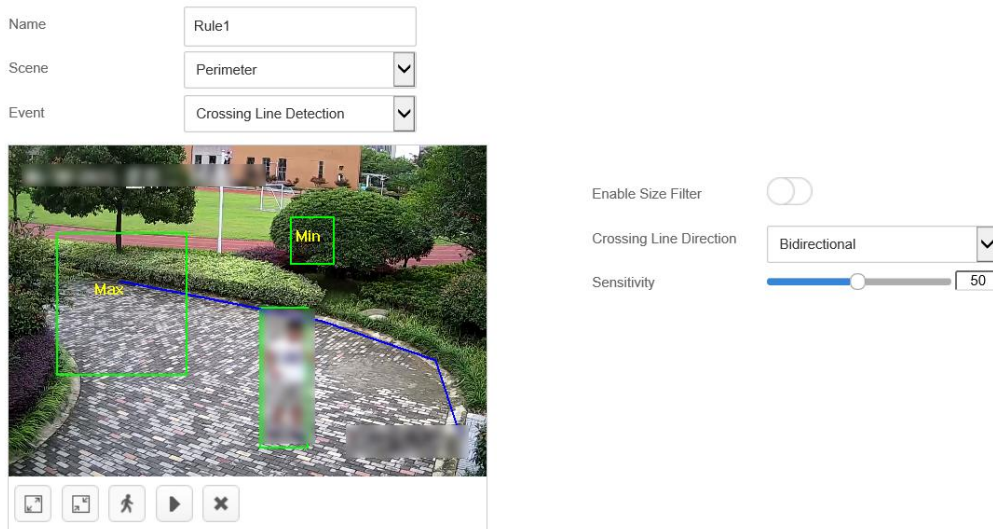



Figure 3-12 Draw Filter Target

Step 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.

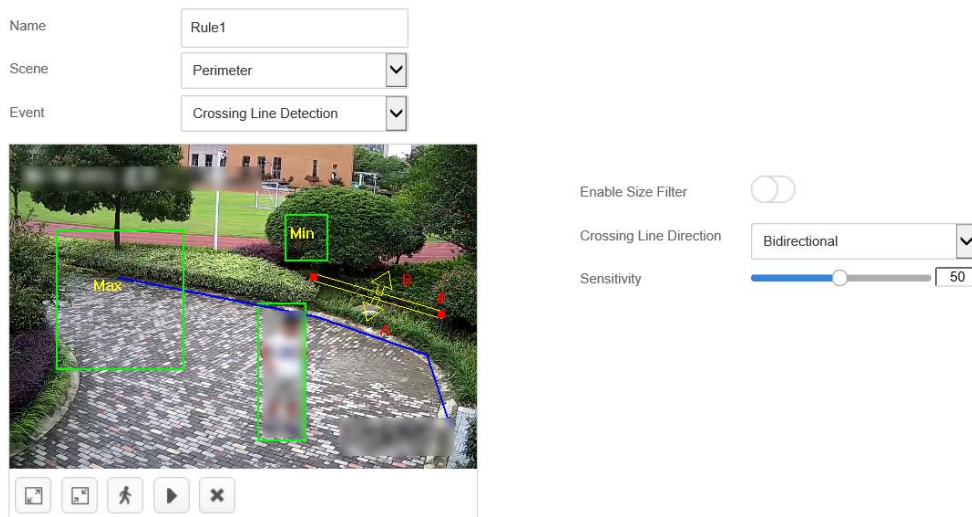




Figure 3-13 Set the Direction of Crossing Line.

NOTE

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

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

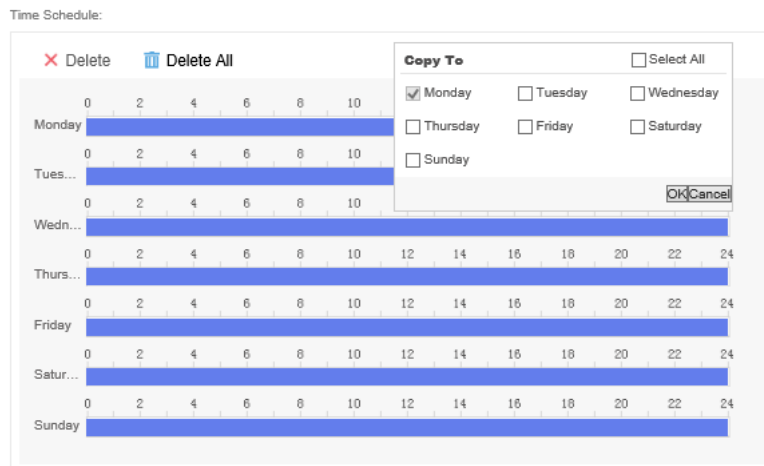


Figure 3-14 Set Detection Time Schedule

Step 5 Click **Save**.

3.3.3 Region Entrance Detection

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


Steps

Step 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**.

Step 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.

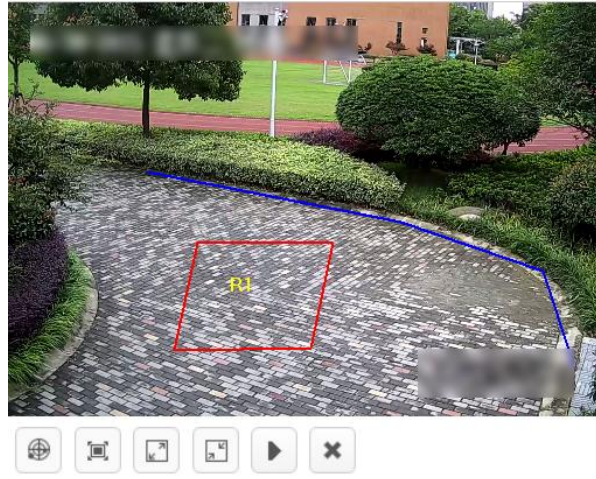



Figure 3-15 Custom Detection Area

- Full screen detection

Click  to do full screen detection.

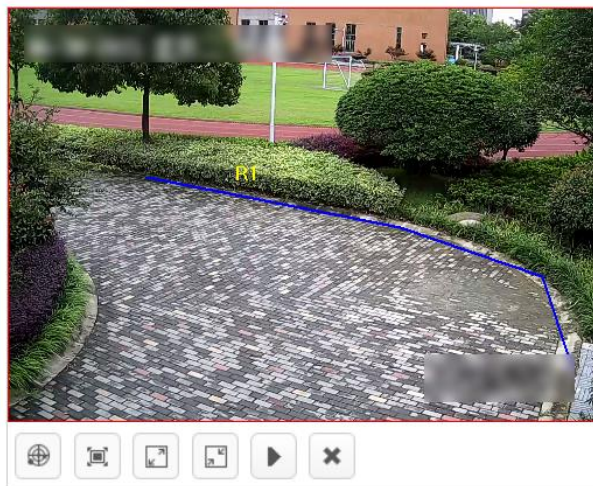




Figure 3-16 Full Screen Detection

Step 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.

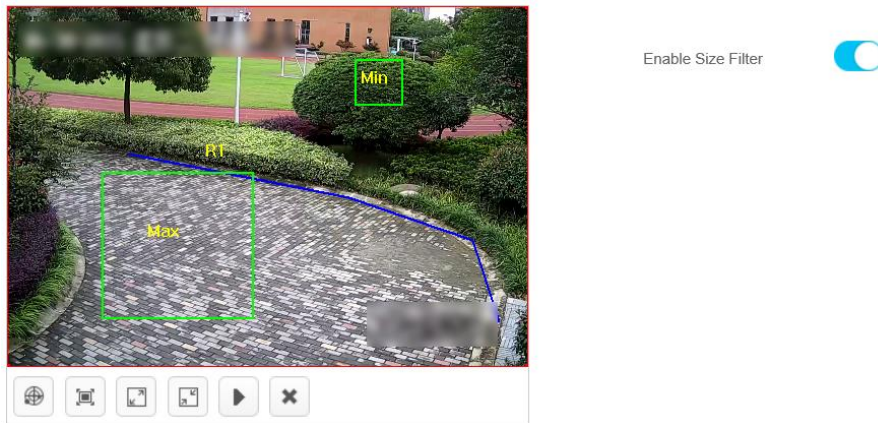




Figure 3-17 Draw Filter Target

NOTE

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

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

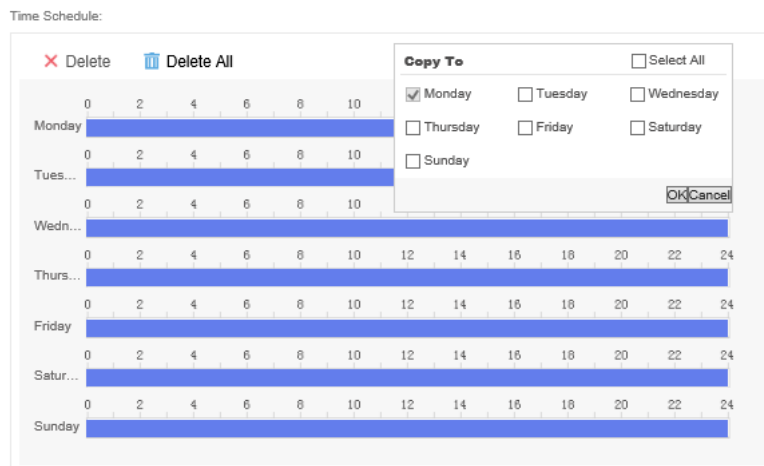


Figure 3-18 Set Detection Time Schedule

Step 5 Click **Save**.

3.3.4 Region Exiting Detection

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

Steps


Step 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 Exiting Detection**

Step 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.

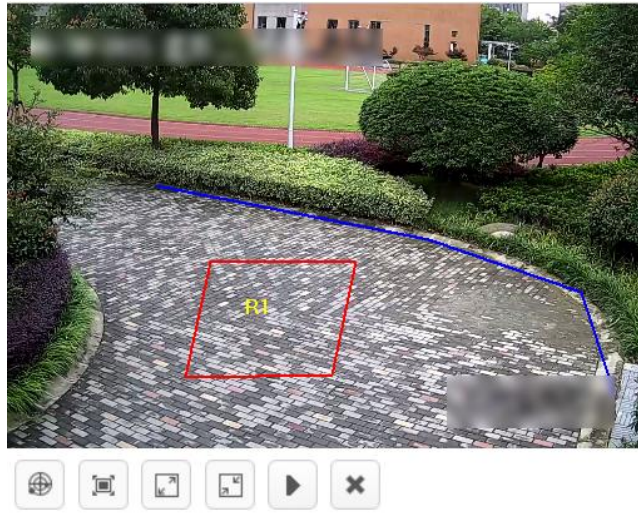


Figure 3-19 Custom Detection Area

- Full screen detection

Click  to do full screen detection.

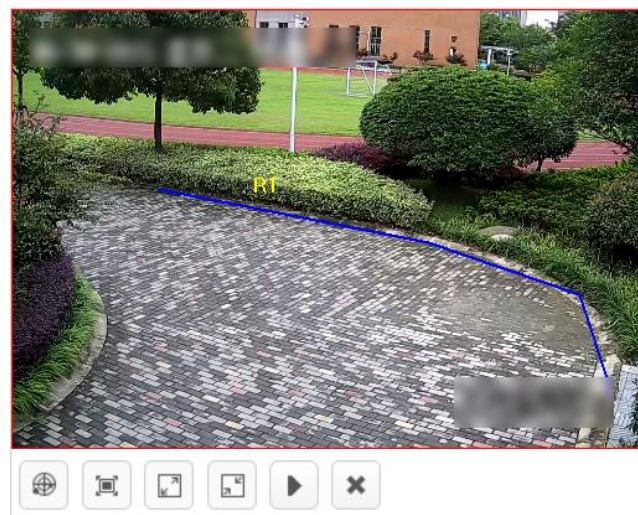




Figure 3-20 Full Screen Detection

Step 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.

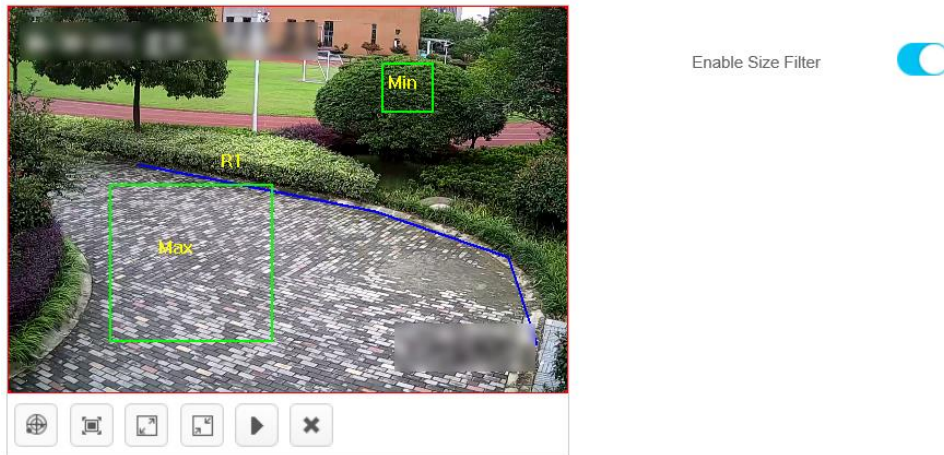




Figure 3-21 Draw Filter Target

 **NOTE**

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

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

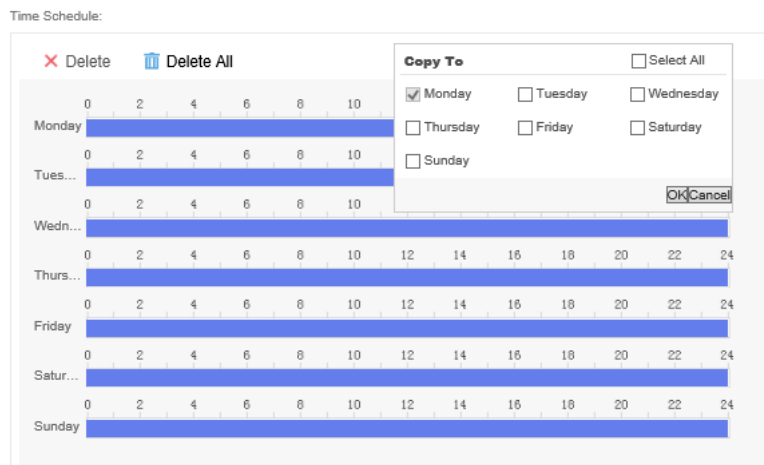


Figure 3-22 Set Detection Time Schedule

Step 5 Click **Save**.

3.3.5 Intrusion Detection

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


Steps

Step 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 **Perimeter**.
- **Event:** select **Intrusion Detection**

Step 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.

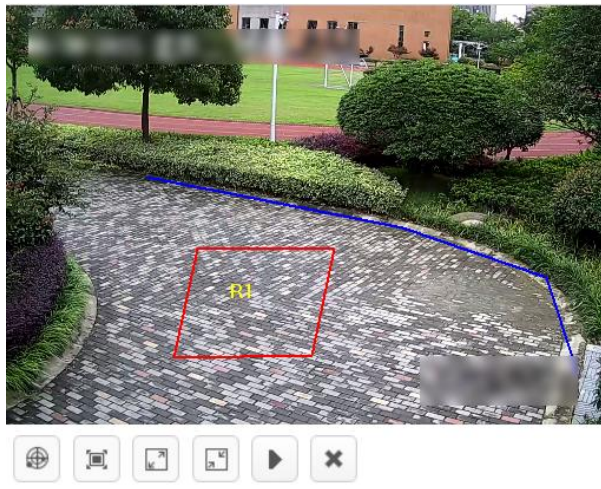


Figure 3-23 Custom Detection Area

- Full screen detection


Click  to do full screen detection.



Figure 3-24 Full Screen Detection

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




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




Figure 3-25 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.

Step 4 Set duration and sensitivity.

1. Set duration.
2. Set sensitivity. The higher the alarm sensitivity is, the easier an alarm can be triggered.

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

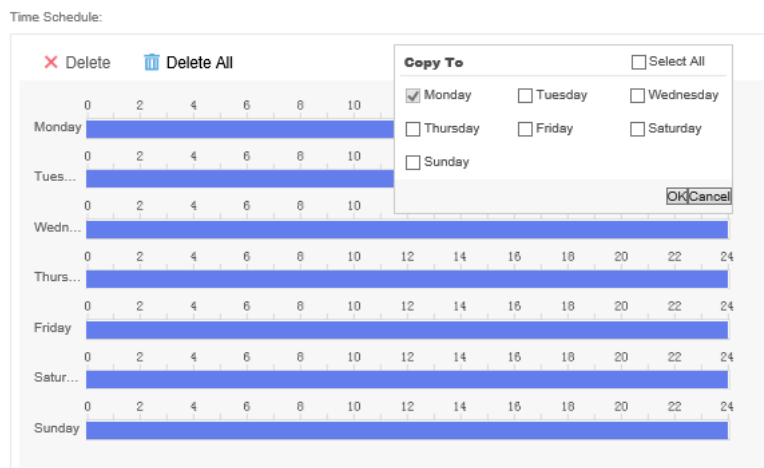


Figure 3-26 Set Detection Time Schedule

Step 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

Step 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 **Perimeter**.
- **Event:** select **Loitering Detection**.

Step 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 .

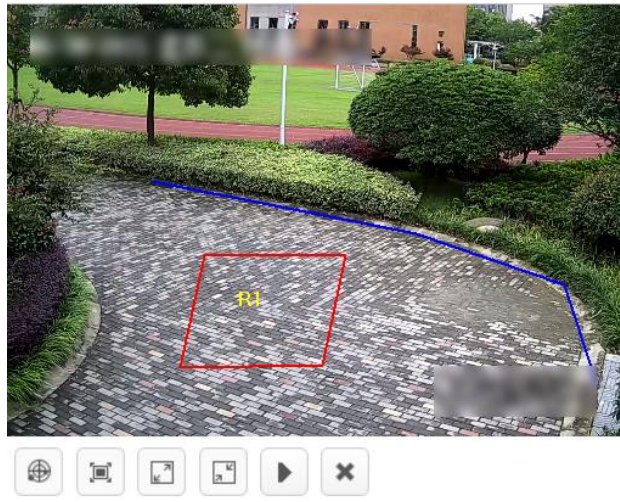


Figure 3-27 Custom Detection Area

- Full screen detection




Click  to do full screen detection.



Figure 3-28 Full Screen Detection

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

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

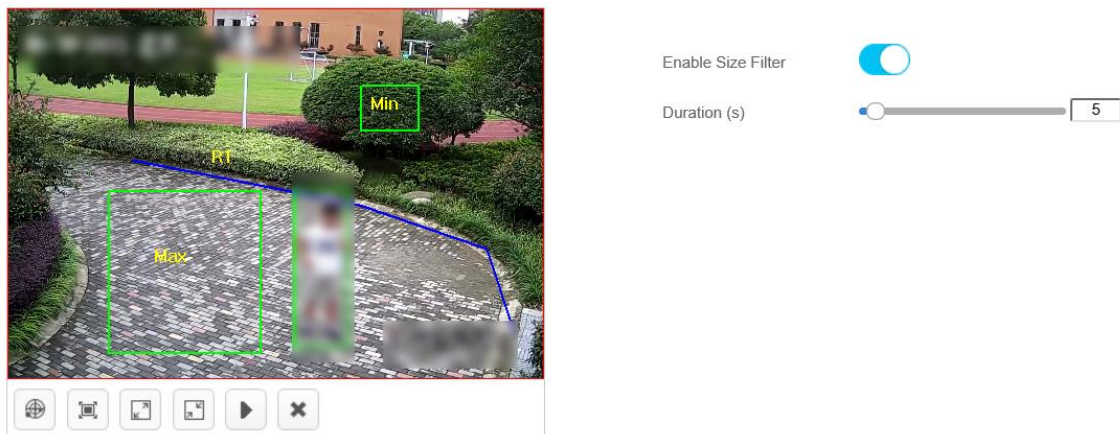



Figure 3-29 Draw Filter Target

 **NOTE**

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

Step 4 Set duration

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

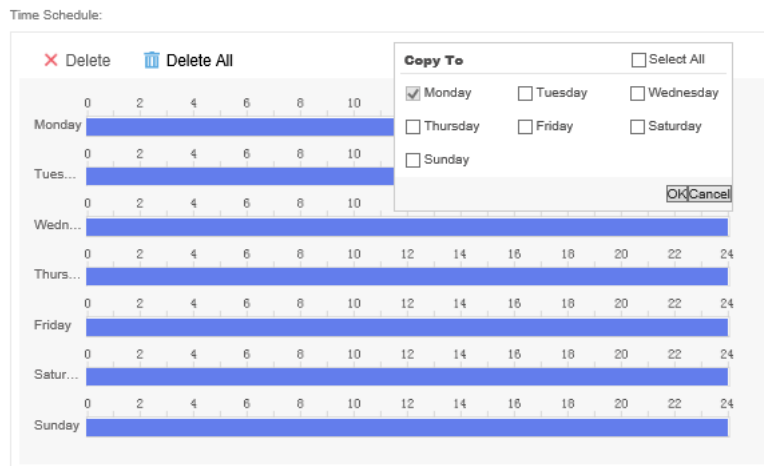


Figure 3-30 Set Detection Time Schedule

Step 6 Click **Save**.

3.3.7 Parking Detection


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

Step 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 **Perimeter**.
- **Event:** select **Parking Detection**.

Step 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.

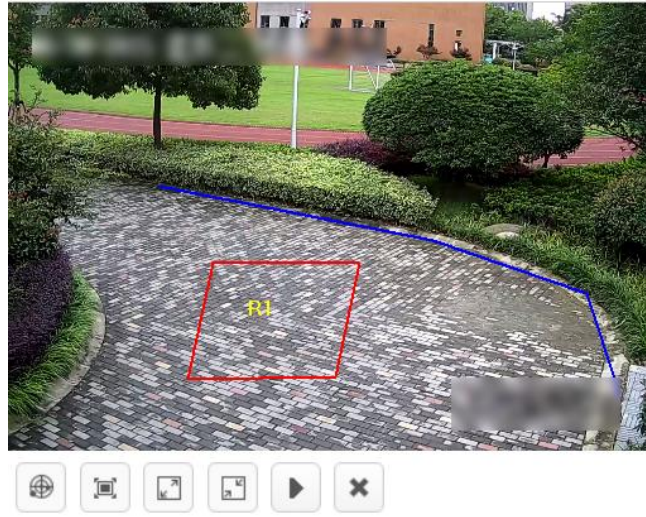



Figure 3-31 Custom Detection Area

- Full screen detection

Click  to do full screen detection.

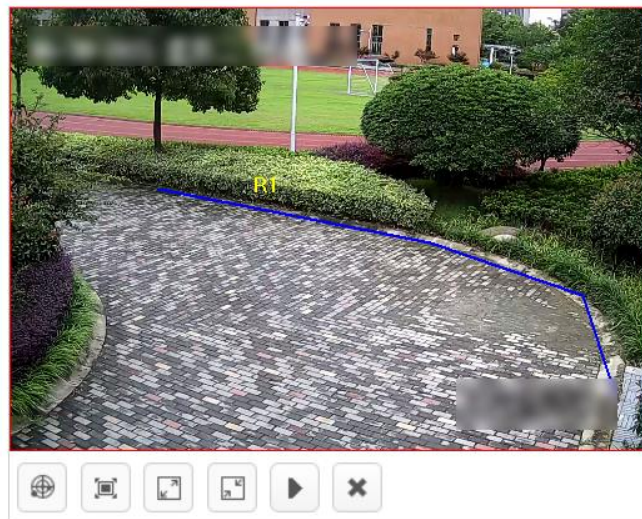


Figure 3-32 Full Screen Detection

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




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




Figure 3-33 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.

Step 4 Set duration and sensitivity.

1. Set duration.
2. Set sensitivity. The higher the alarm sensitivity is, the easier an alarm can be triggered.

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

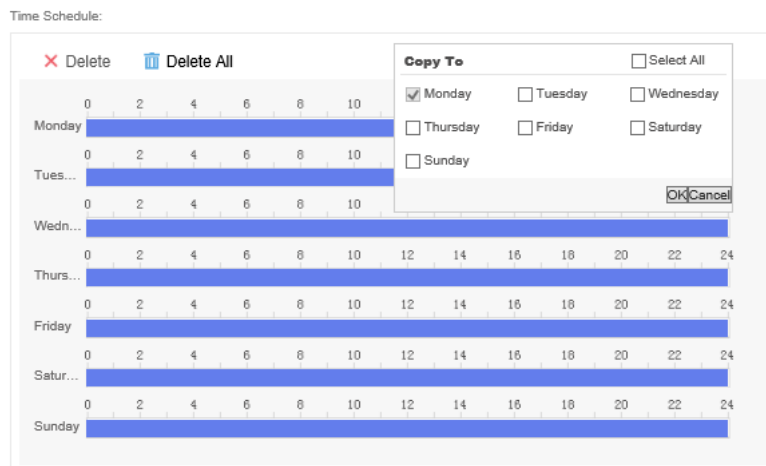


Figure 3-34 Set Detection Time Schedule

Step 6 Click **Save**.

3.3.8 Unattended Baggage Detection


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

Step 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 **Perimeter**.
- **Event:** select **Unattended Object Detection**.

Step 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.

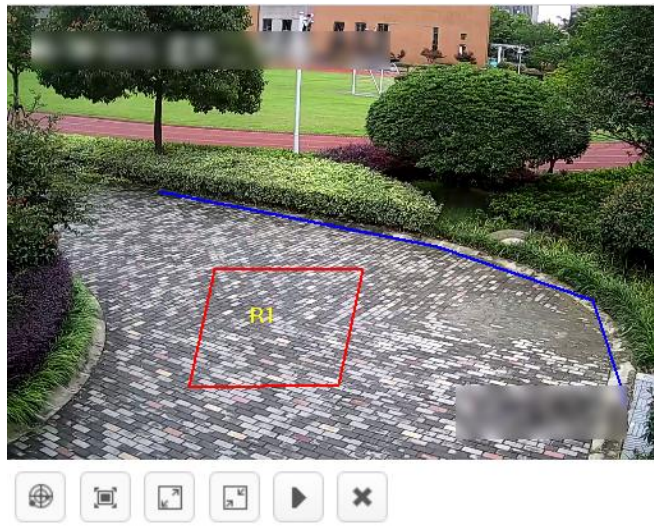



Figure 3-35 Custom Detection Area

- Full screen detection

Click  to do full screen detection.

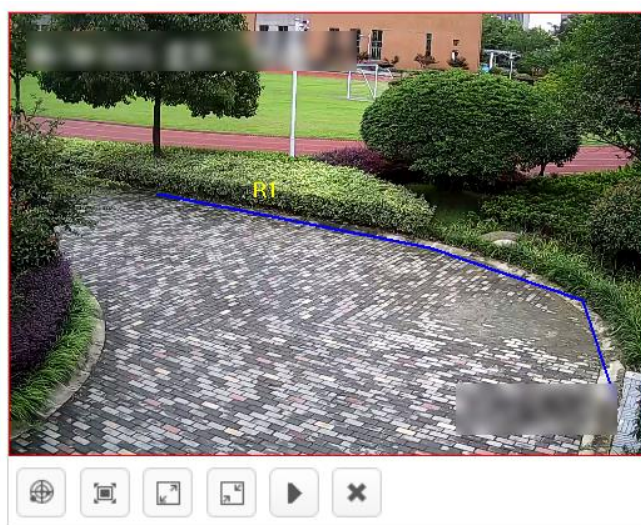




Figure 3-36 Full Screen Detection

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

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

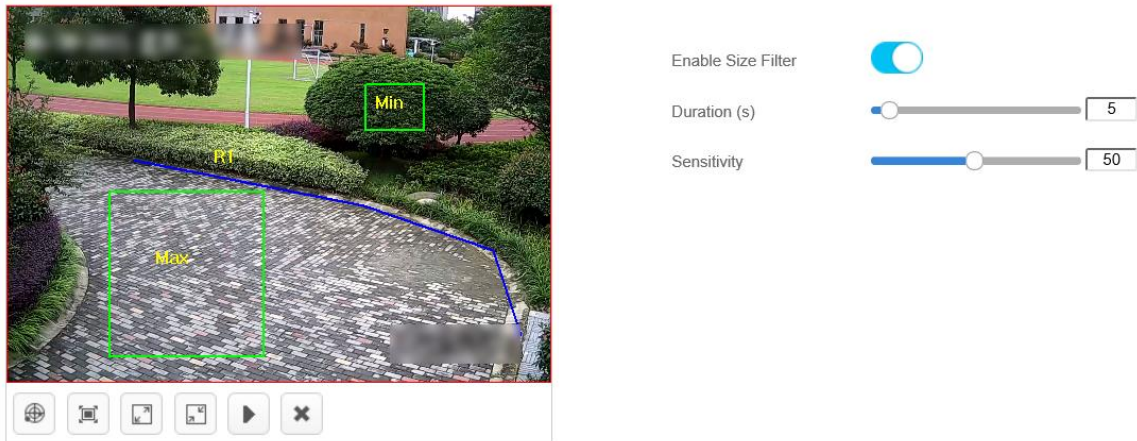



Figure 3-37 Draw Filter Target

 **NOTE**

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

Step 4 Set duration and sensitivity.

1. Set duration.
2. Set sensitivity. The higher the alarm sensitivity is, the easier an alarm can be triggered.

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

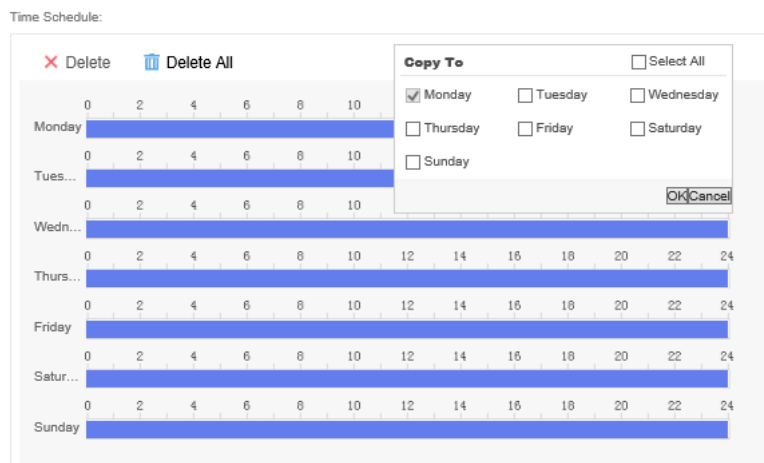


Figure 3-38 Set Detection Time Schedule

Step 6 Click **Save**.

3.3.9 Object Removal Detection


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

Step 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 **Perimeter**.
- **Event:** select **Object Removal Detection**.

Step 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 .

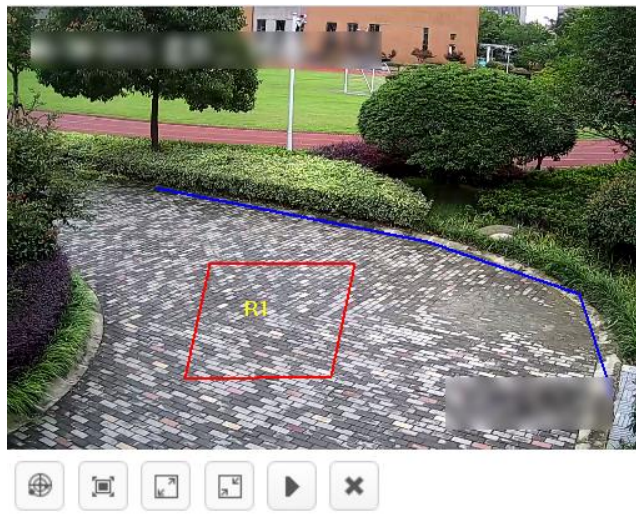



Figure 3-39 Custom Detection Area

- Full screen detection

Click  to do full screen detection.

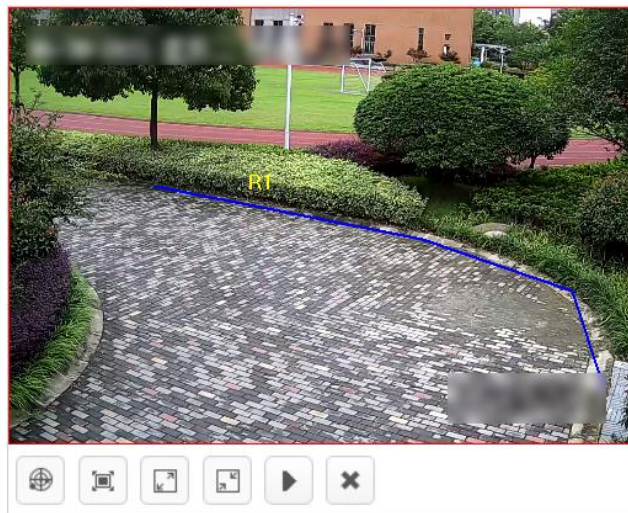


Figure 3-40 Full Screen Detection

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




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



Figure 3-41 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.

Step 4 Set duration and sensitivity.

1. Set duration.
2. Set sensitivity. The higher the alarm sensitivity is, the easier an alarm can be triggered.

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

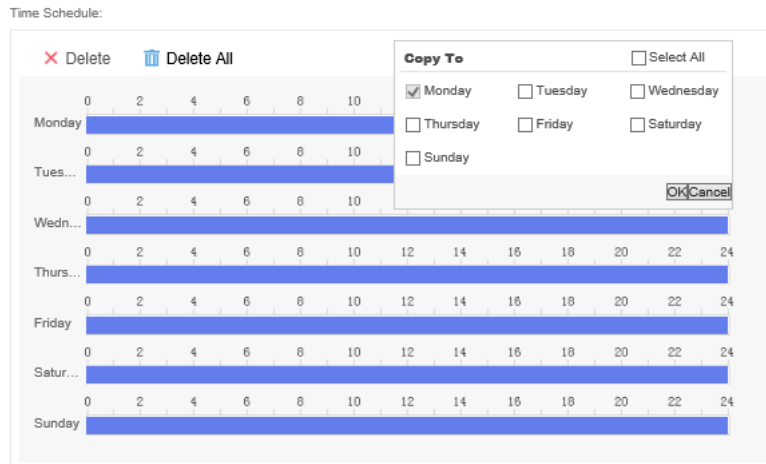


Figure 3-42 Set Detection Time Schedule

Step 6 Click **Save**.

3.4 Trend Analysis Task

3.4.1 Create a Trend Analysis Task

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

Steps

Step 1 Click **Task Management** -> **New**.

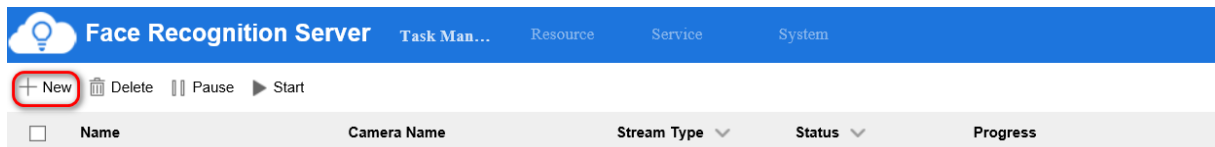


Figure 3-43 Task Management Interface

Step 2 Enter a task name.

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

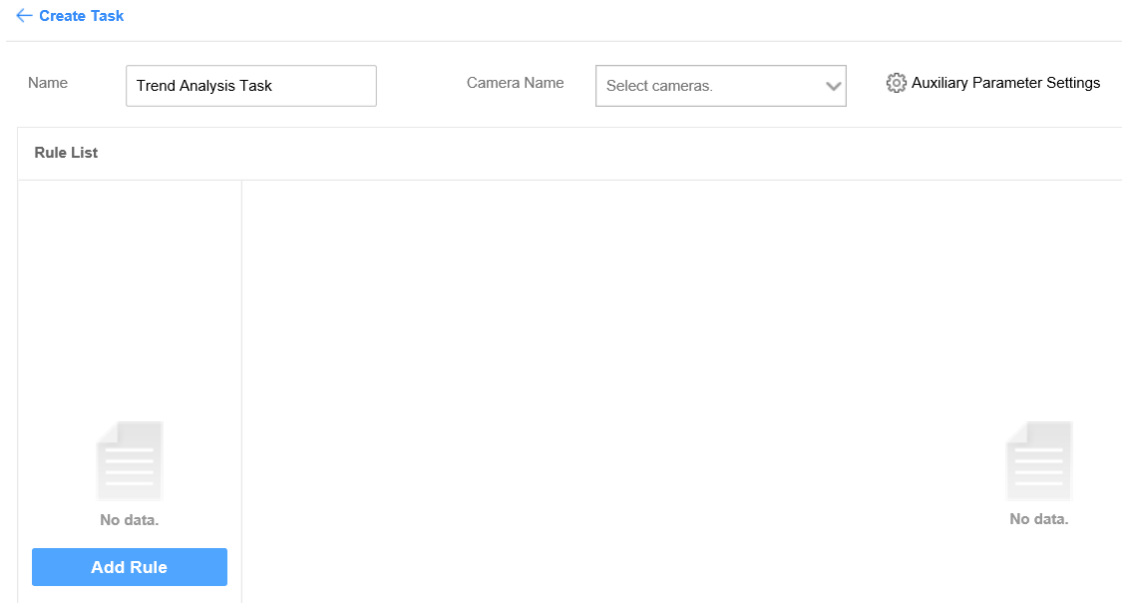


Figure 3-44 Create Task Interface



NOTE

Keep **Auxiliary Parameter Settings** by default.

Step 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 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 People Density Analysis

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


Steps

Step 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 **Trend**.
- **Event:** select **People Density Analysis**.

Step 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 .

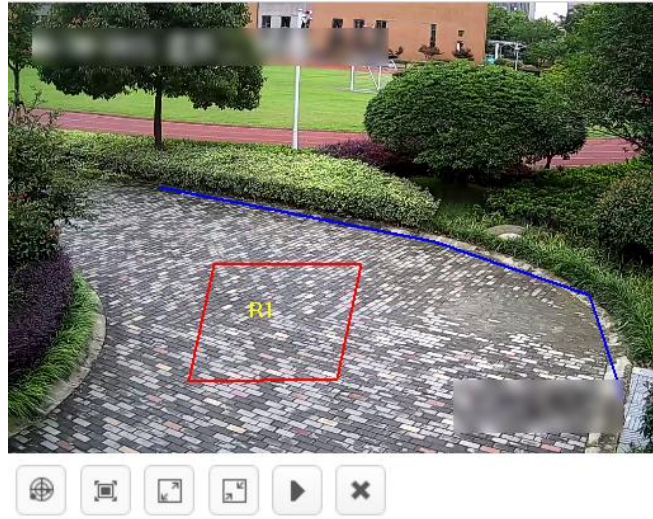



Figure 3-45 Custom Detection Area

- Full screen detection

Click  to do full screen detection.

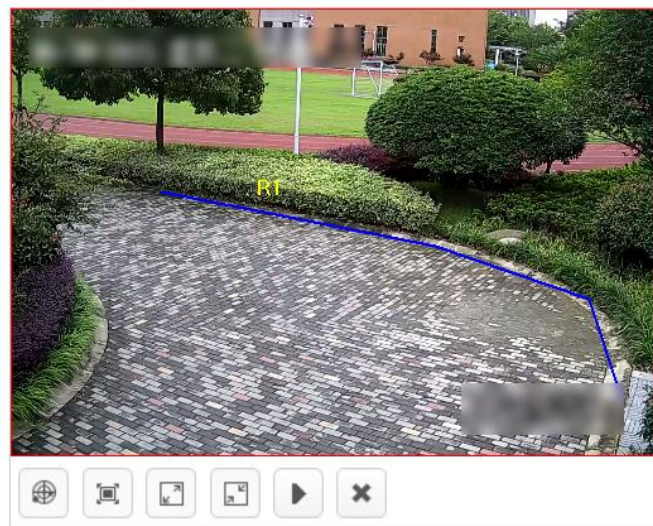



Figure 3-46 Full Screen Detection


 **NOTE**

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

Step 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

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

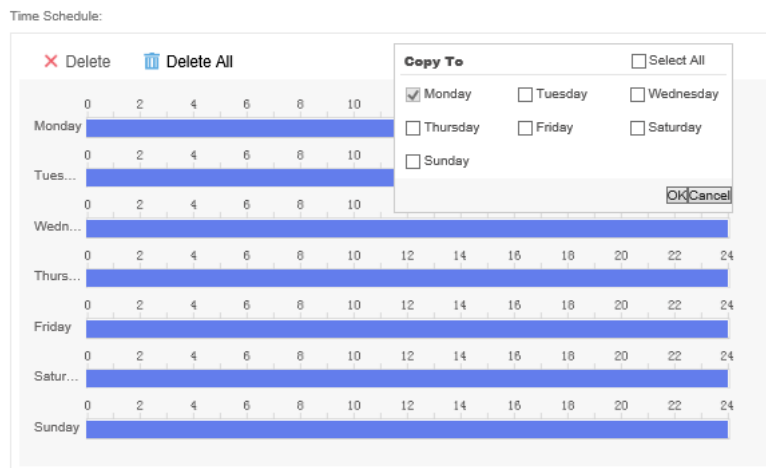


Figure 3-47 Set Detection Time Schedule

Step 5 Click **Save**.

3.4.3 Real-time People Counting

Count people in detection area.


Steps

Step 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 **Trend**.
- **Event:** select **Real-time People Counting**.

Step 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.

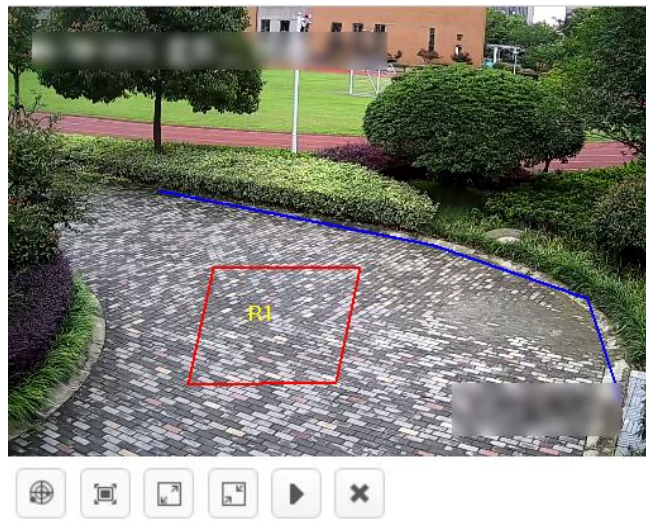



Figure 3-48 Custom Detection Area

- Full screen detection

Click  to do full screen detection.

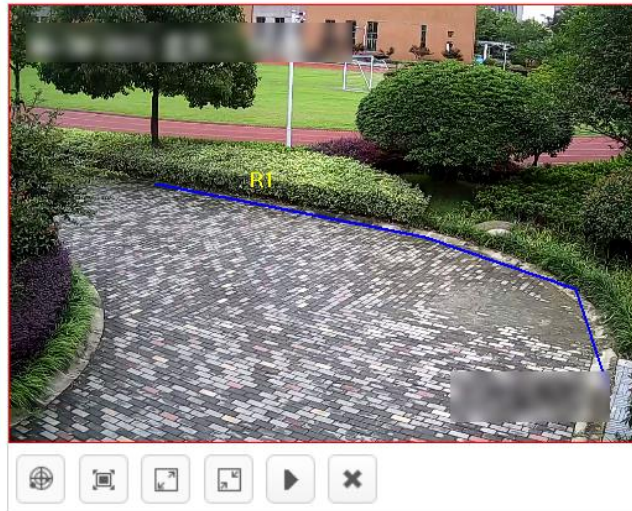




Figure 3-49 Full Screen Detection

 **NOTE**

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

Step 3 Set the report interval of number of people in the area.

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

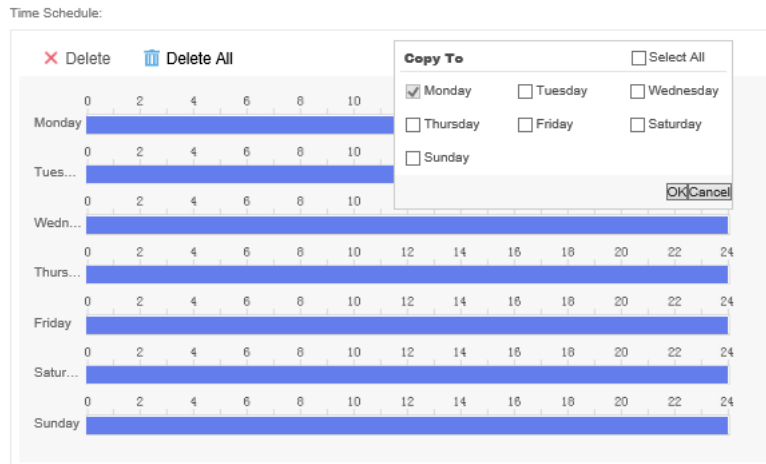


Figure 3-50 Set Detection Time Schedule

Step 5 Click **Save**.

3.4.4 People Counting



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

Steps

Step 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 **Trend**.
- **Event:** select **People Counting**

Step 2 Draw detection area and line.

- Custom detection area
 1. Click , press the left mouse button and move the mouse to draw detection area, and press the right button to complete the operation.
 2. 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.

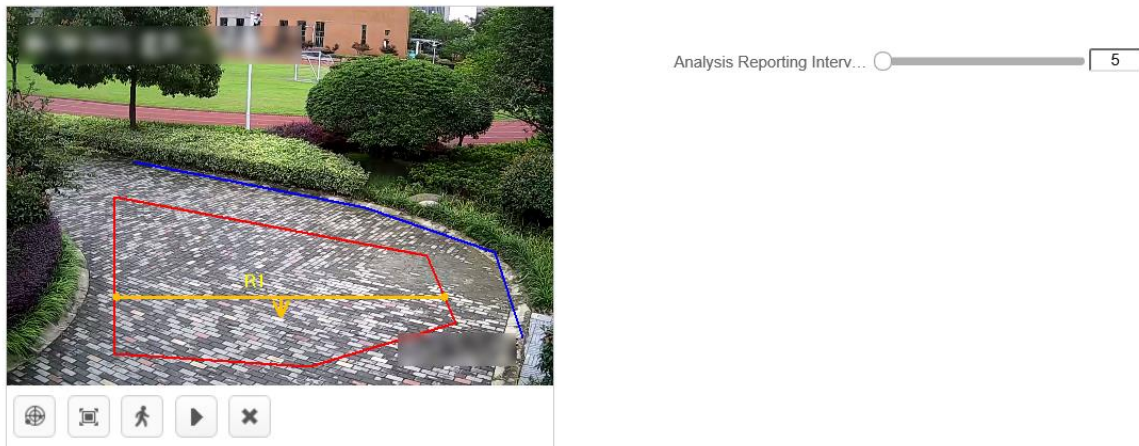




Figure 3-51 Custom Detection Area

- Full screen detection

1. Click  to do full screen detection.
2. 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.

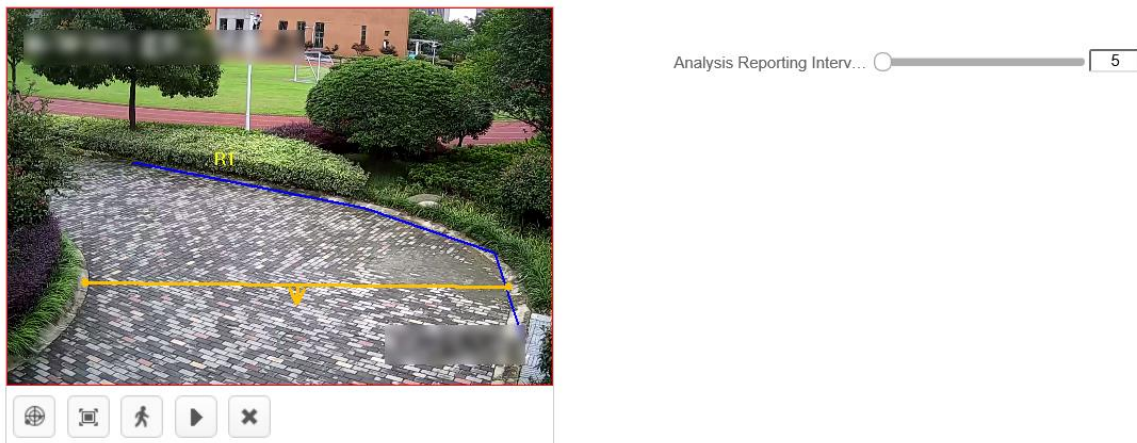




Figure 3-52 Full Screen Detection

 **NOTE**

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

Step 3 Set the report interval of people counting.

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

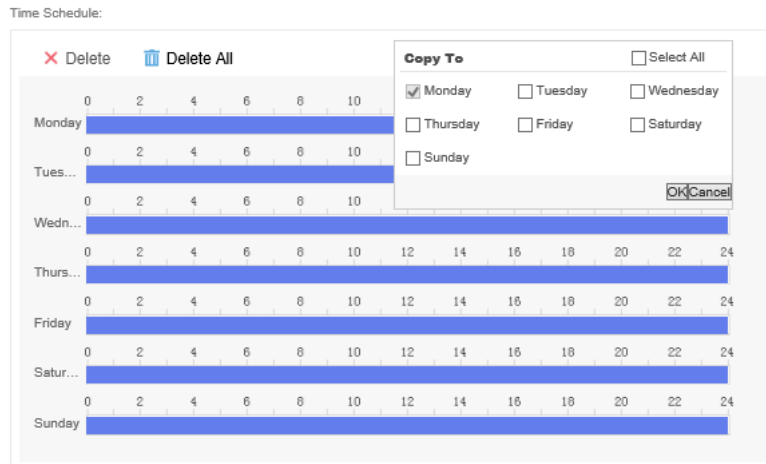


Figure 3-53 Set Detection Time Schedule

Step 5 Click **Save**.

3.5 Indoor Analysis Task

3.5.1 Create an Indoor Analysis Task

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

Steps

Step 1 Click **Task Management** -> **New**.

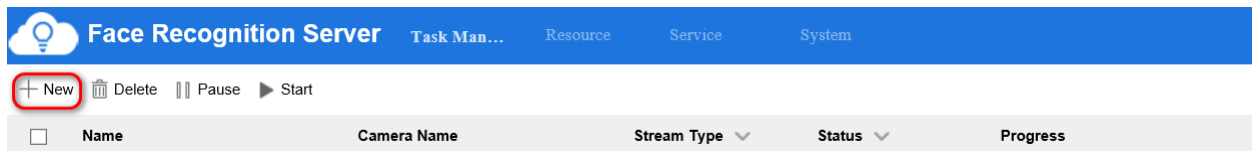


Figure 3-54 Task Management Interface

Step 2 Enter a task name.

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

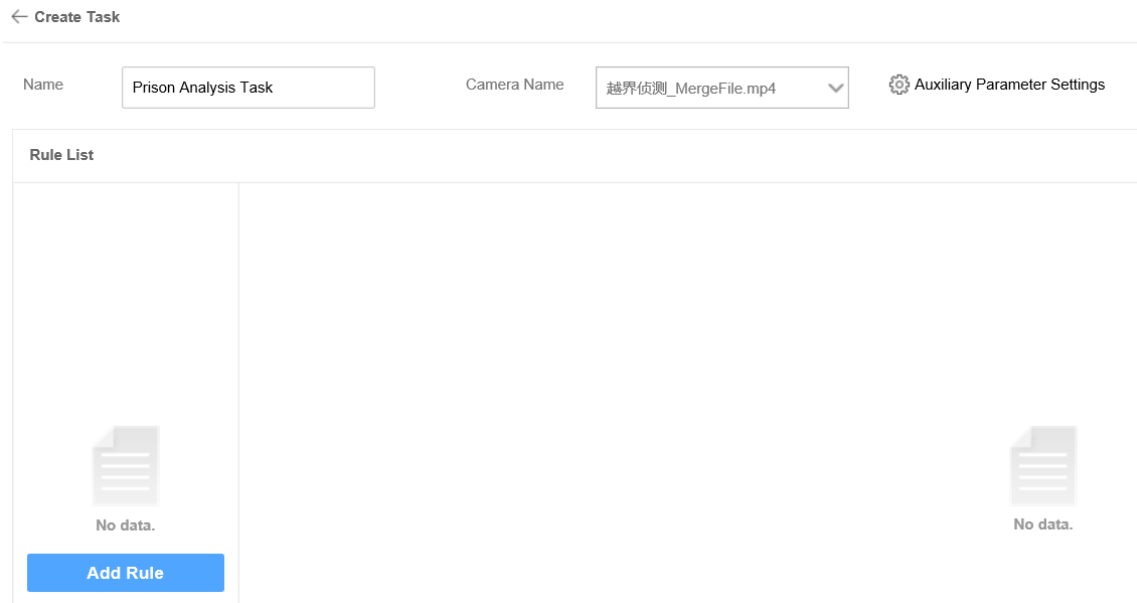


Figure 3-55 Create Task Interface



NOTE

Keep the **Auxiliary Parameter Settings** by default.

Step 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 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 Physical Conflict Detection

Detect physical conflict of people in the area, such as fight.

Step 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 **Physical Conflict Detection**.

Step 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 3-56 Custom Detection Area

- Full screen detection

Click  to do full screen detection.

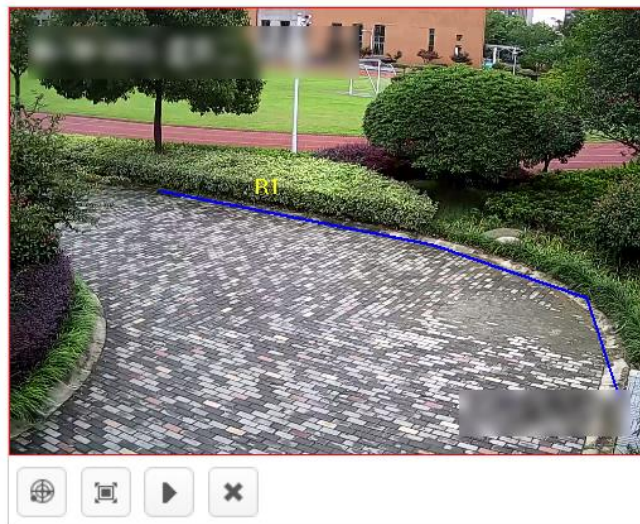




Figure 3-57 Full Screen Detection

 **NOTE**

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

Step 3 Set duration and sensitivity.

1. Set duration.
2. Set sensitivity. The higher the alarm sensitivity is, the easier an alarm can be triggered.

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

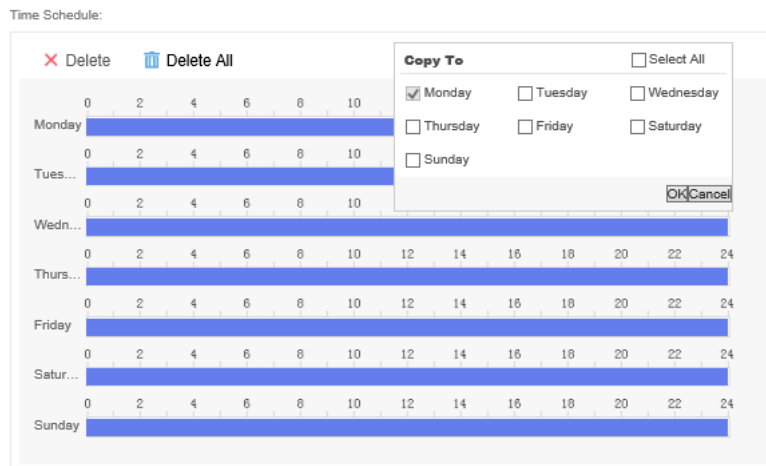


Figure 3-58 Set Detection Time Schedule

Step 5 Click **Save**.

3.5.3 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

Step 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 **Getting-up Detection**.

Step 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.

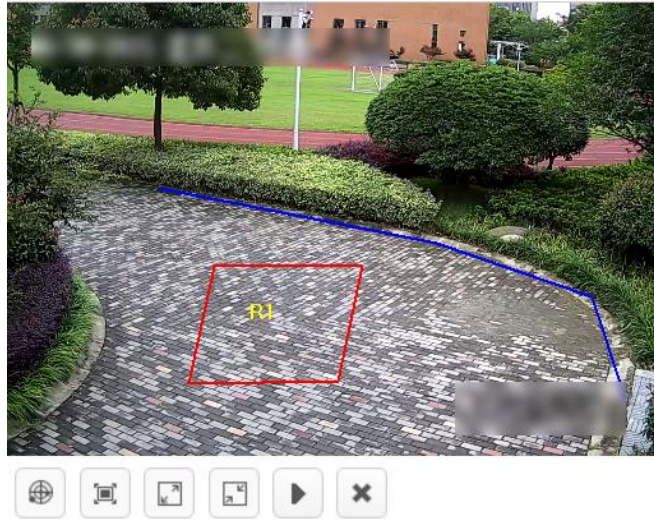


Figure 3-59 Custom Detection Area

- Full screen detection




Click  to do full screen detection.



Figure 3-60 Full Screen Detection

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

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

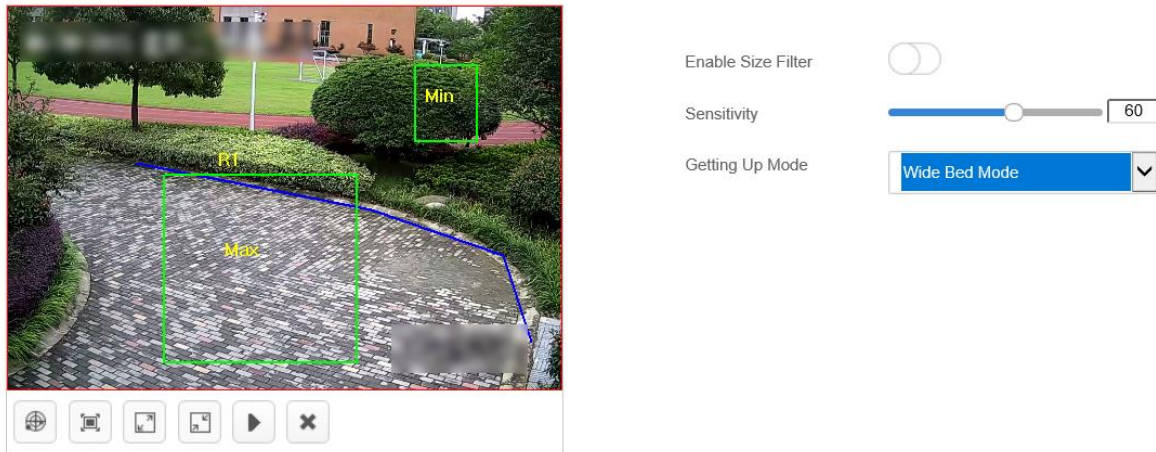



Figure 3-61 Draw Filter Target


NOTE

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

Step 4 Set Sensitivity. The higher the alarm sensitivity is, the easier an alarm can be triggered.

Step 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

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

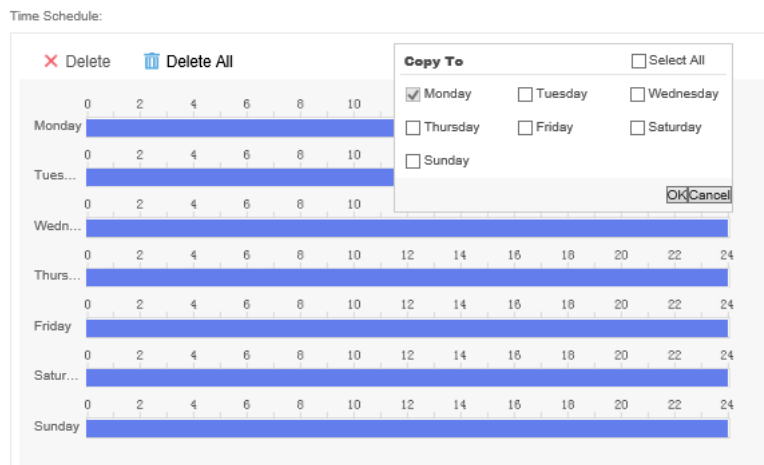


Figure 3-62 Set Detection Time Schedule

Step 7 Click **Save**.

3.5.4 Key Person Getting-up Detection

Detect getting-up movement of key person in the area. For example, a convicted or dangerous prisoner gets up or gets out of bed during the break time.


Steps

Step 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 **Key Person Getting-up Detection**.

Step 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.

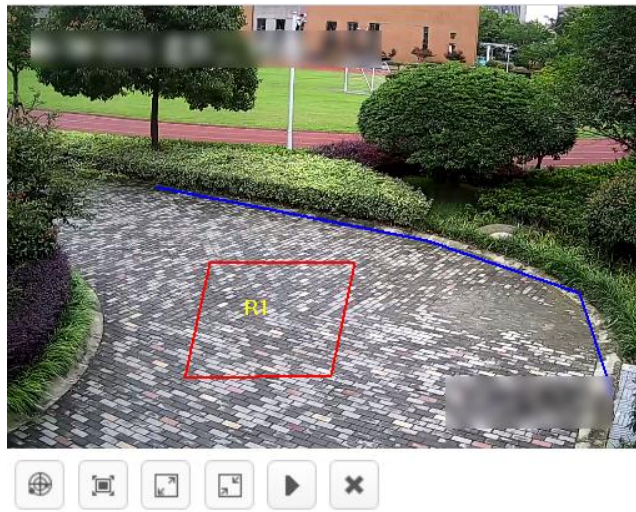


Figure 3-63 Custom Detection Area

- Full screen detection.




Click  to do full screen detection.



Figure 3-64 Full Screen Detection

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

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

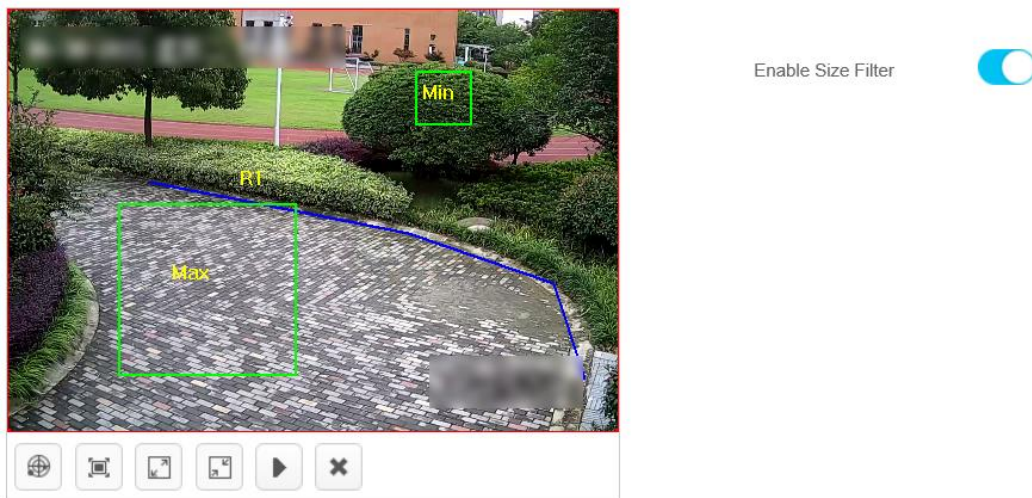



Figure 3-65 Draw Filter Target

 **NOTE**

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

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

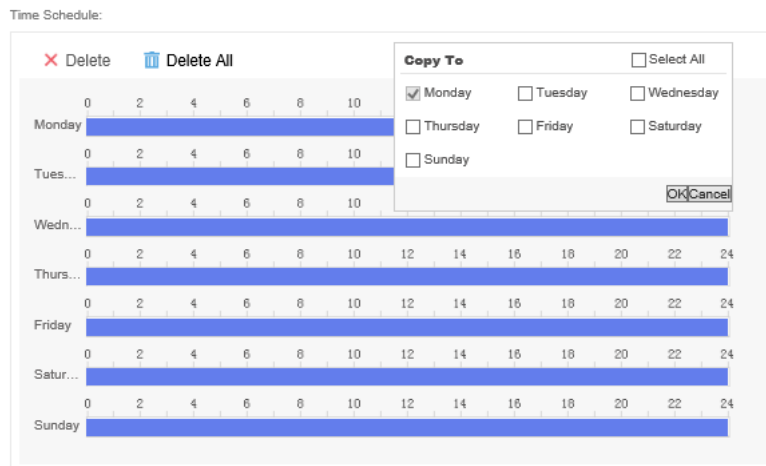


Figure 3-66 Set Detection Time Schedule

Step 5 Click **Save**.

3.5.5 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

Step 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 **Absence/Sleep on Duty Detection**.

Step 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.

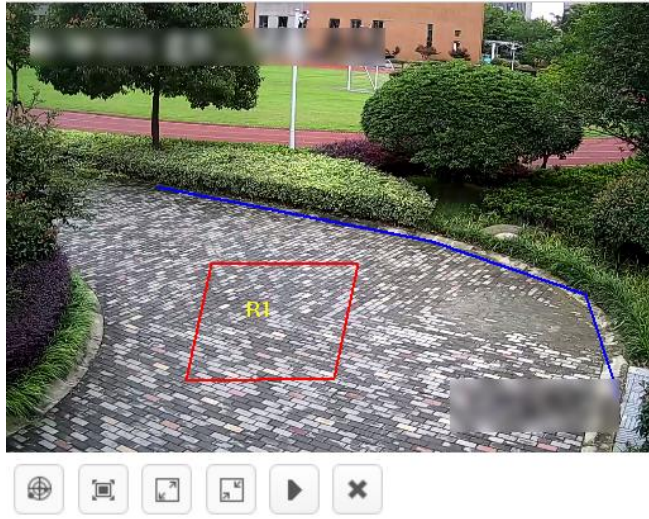



Figure 3-67 Custom Detection Area

- Full screen detection

Click  to do full screen detection.

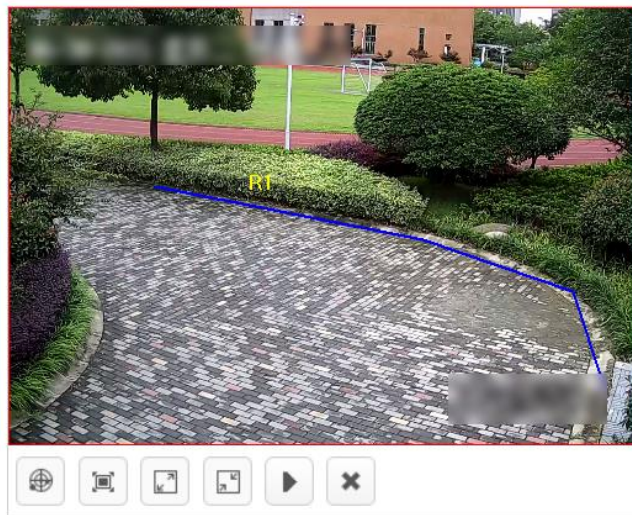




Figure 3-68 Full Screen Detection

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

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

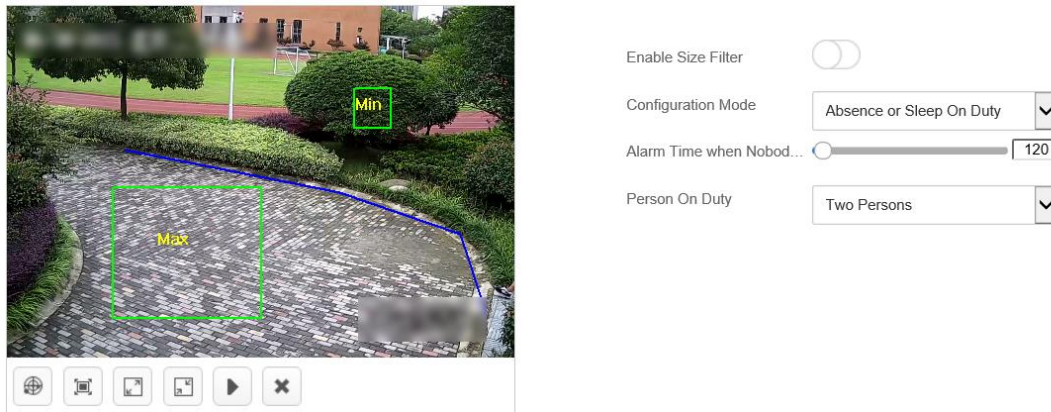




Figure 3-69 Draw Filter Target

NOTE

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

Step 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.
- **Number of Persons on Duty**

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

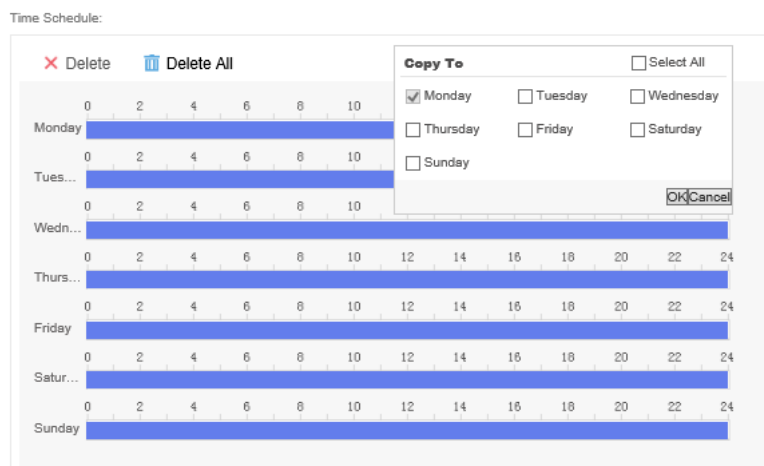


Figure 3-70 Set Detection Time Schedule

Step 6 Click **Save**.

3.5.6 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

Step 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 **Standing-up Detection**.

Step 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.

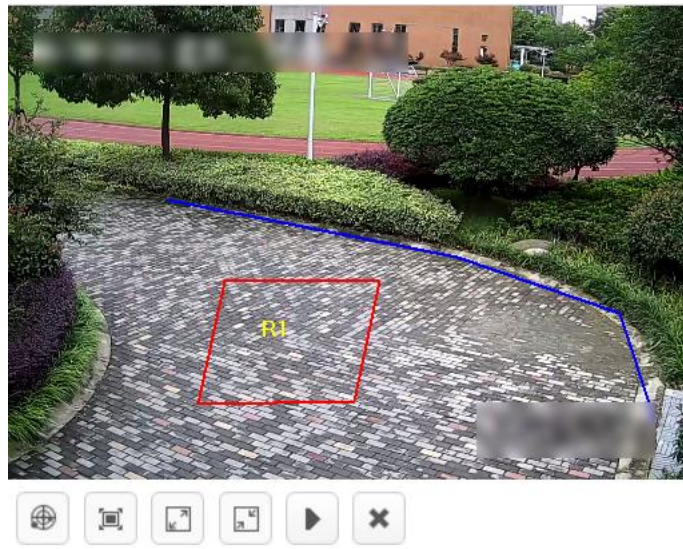



Figure 3-71 Custom Detection Area

- Full screen detection

Click  to do full screen detection.

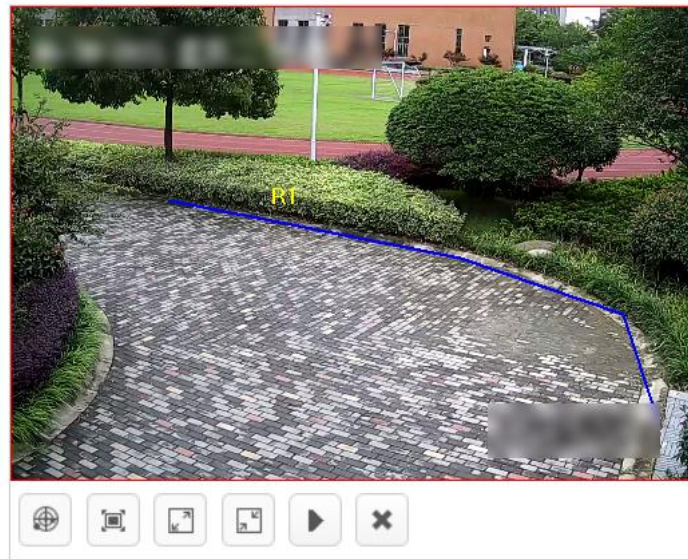




Figure 3-72 Full Screen Detection

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

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

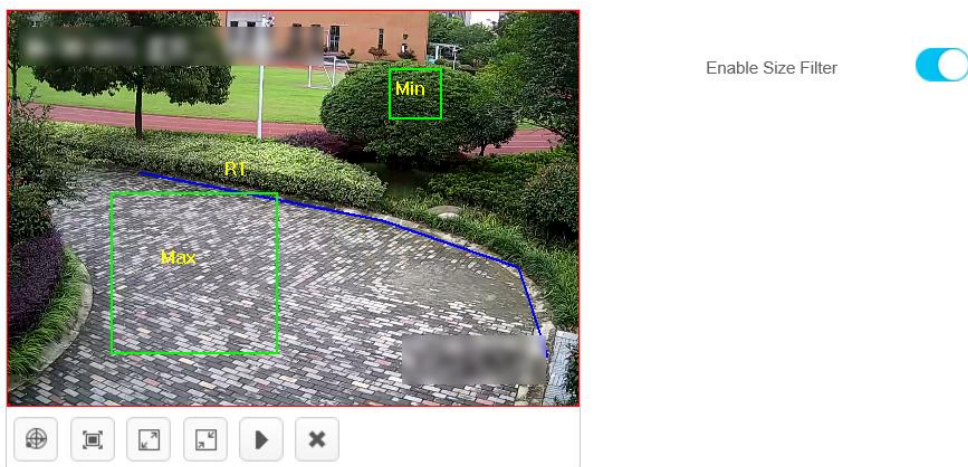



Figure 3-73 Draw Filter Target

 **NOTE**

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

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

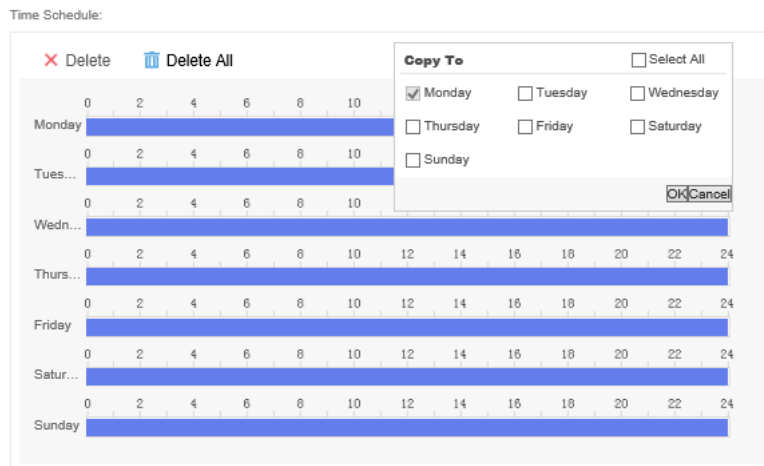


Figure 3-74 Set Detection Time Schedule

Step 5 Click **Save**.

3.5.7 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

Step 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 **Detection for Sudden Change of Sound Intensity**.

Step 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.

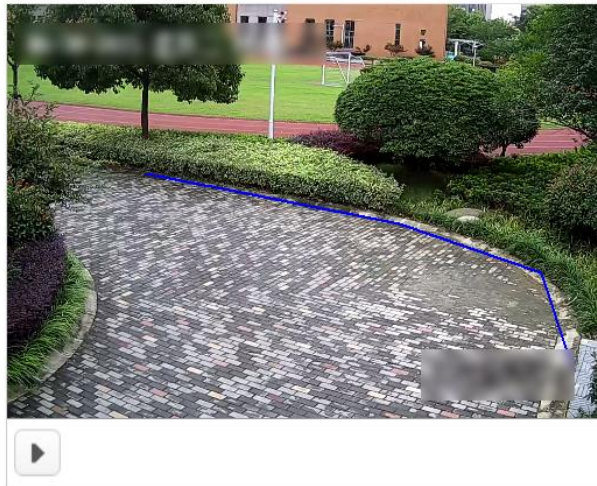


Figure 3-75 Full Screen Detection

 **NOTE**

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

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

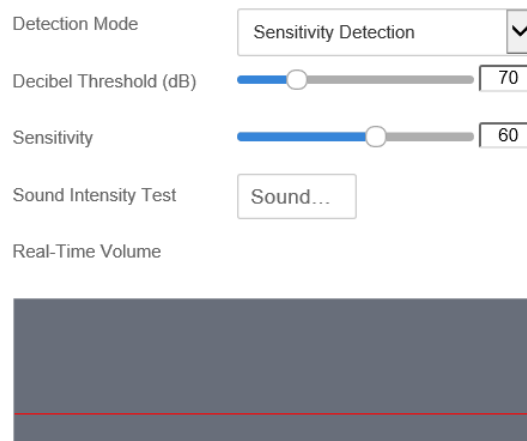



Figure 3-76 Sound Intensity Test

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

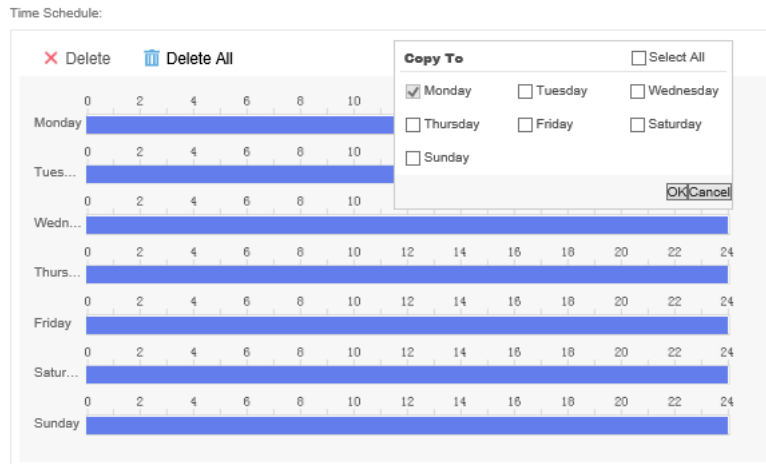


Figure 3-77 Set Detection Time Schedule

Step 5 Click **Save**.


3.5.8 Climbing Detection

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

Steps

Step 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 **Climbing Detection**.

Step 2 Click , press and hold the left mouse button to draw limited height line, and then click the right button.

Step 3 Set crossing line direction.

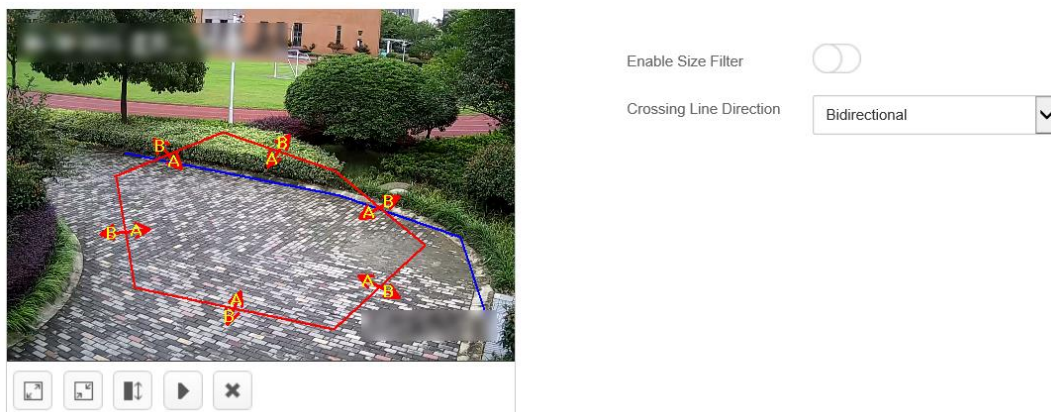






Figure 3-78 Set Climbing Area

 **NOTE**

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

Step 4 (Optional) Enable **Size Filter**. Only targets between the minimum and maximum sizes will be detected.

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

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

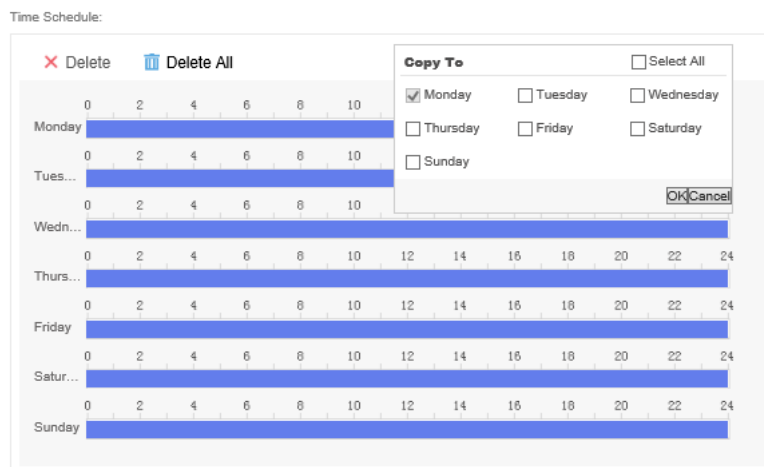


Figure 3-79 Set Detection Time Schedule

Step 6 Click **Save**.

3.5.9 Overstaying Detection

Detect the behavior of staying in the toilet overtime.


Steps

Step 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 **Overstaying Detection**.

Step 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.

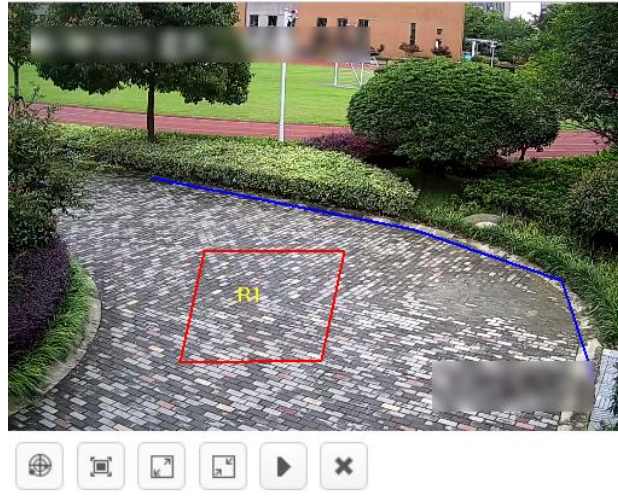


Figure 3-80 Custom Detection Area

- Full screen detection


Click  to do full screen detection.



Figure 3-81 Full Screen Detection

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




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




Figure 3-82 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.

Step 4 Set duration.

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

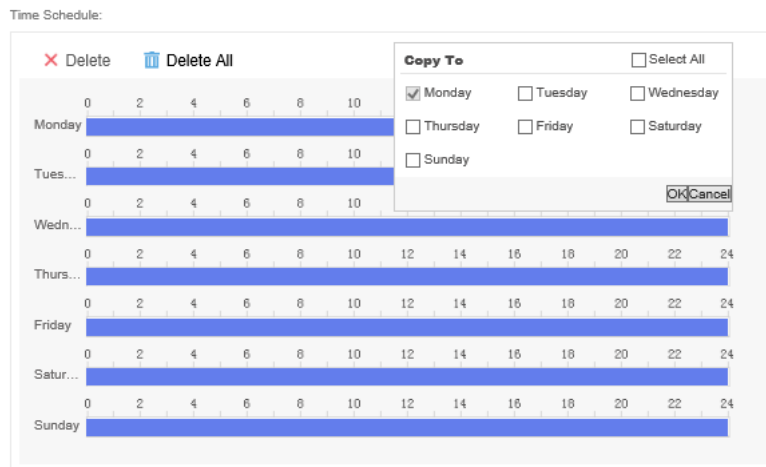


Figure 3-83 Set Detection Time Schedule

Step 6 Click **Save**.

3.5.10 Regional Overstaying Detection

Detect the behavior of regional overstaying.


Steps

Step 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 **Regional Overstaying Detection**.

Step 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.

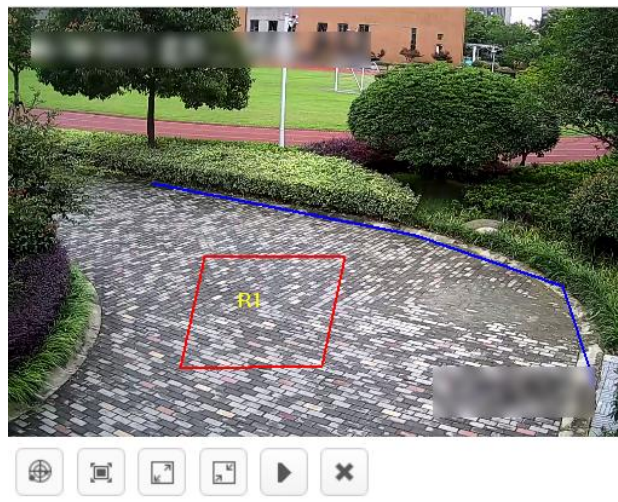


Figure 3-84 Custom Detection Area

- Full screen detection


Click  to do full screen detection.



Figure 3-85 Full Screen Detection

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




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




Figure 3-86 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.

Step 4 Set duration.

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

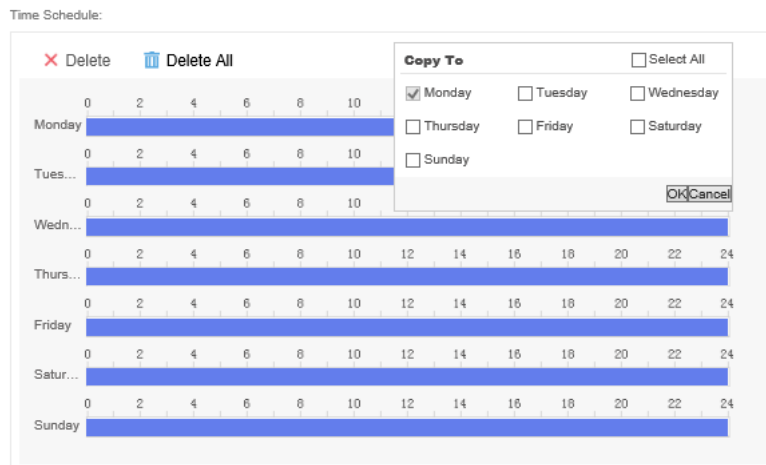


Figure 3-87 Set Detection Time Schedule

Step 6 Click **Save**.

3.5.11 Abnormal Number of People Detection

Detect whether the number of people is normal or not.


Steps

Step 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**.

Step 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.

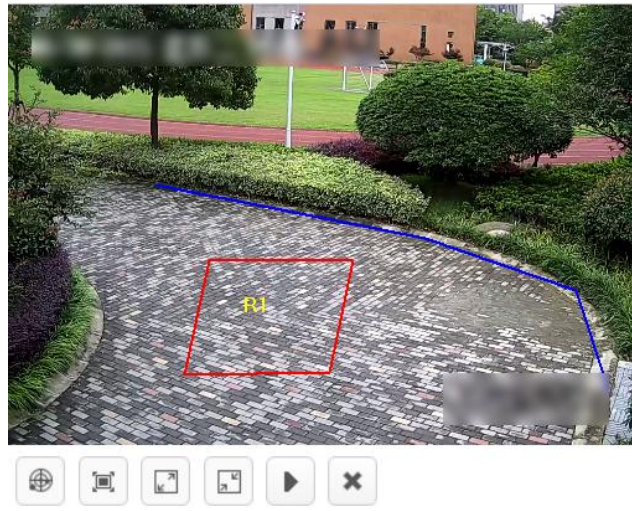


Figure 3-88 Custom Detection Area

- Full screen detection.

Click  to do full screen detection.

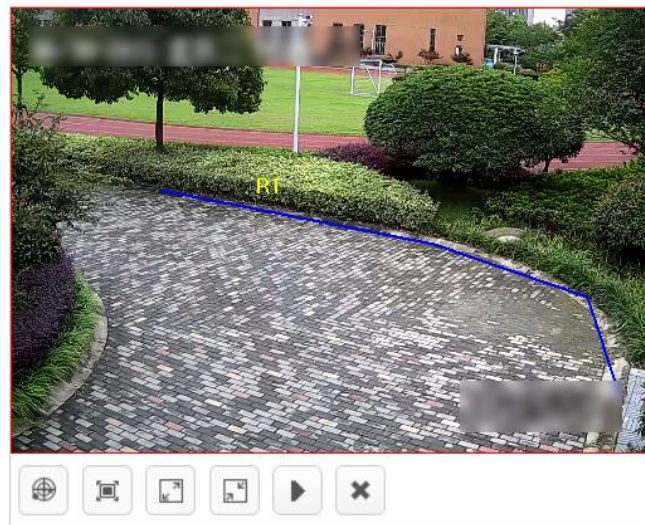


Figure 3-89 Full Screen Detection

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




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



Figure 3-90 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.

Step 4 Set triggering time and number of people threshold.

Step 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.

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

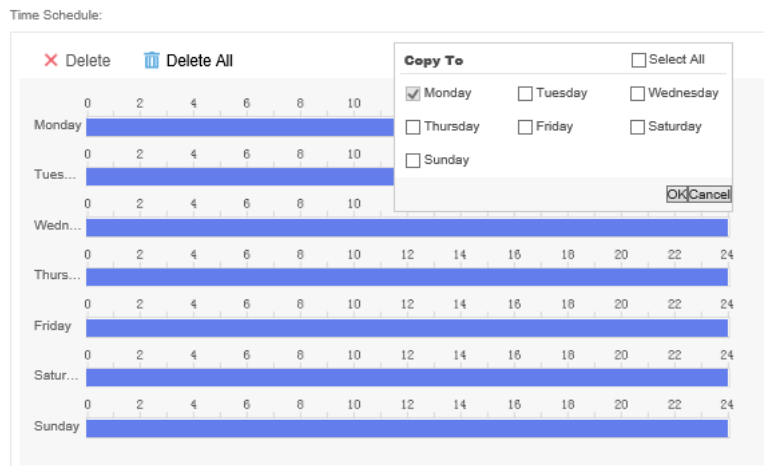


Figure 3-91 Set Detection Time Schedule

Step 7 Click **Save**.

3.5.12 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

Step 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**.

Step 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.

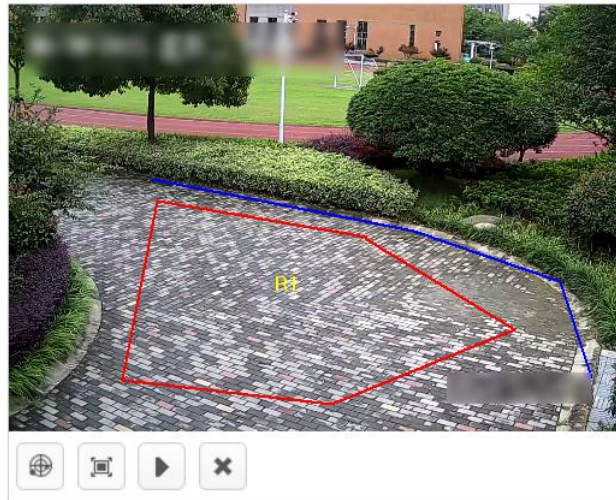


Figure 3-92 Custom Detection Area

- Full screen detection



Click  to do full screen detection.




Figure 3-93 Full Screen Detection

 **NOTE**

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

Step 3 Set duration.

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

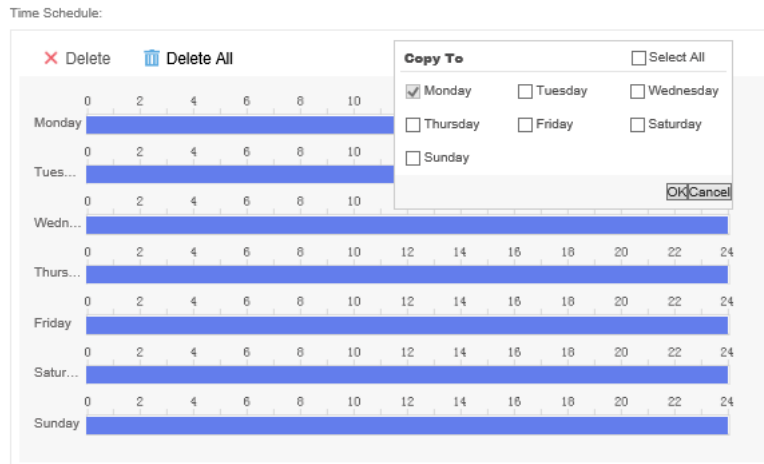


Figure 3-94 Set Detection Time Schedule

Step 5 Click **Save**.

3.5.13 People Counting

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


Steps

Step 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 **People Counting**.

Step 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.

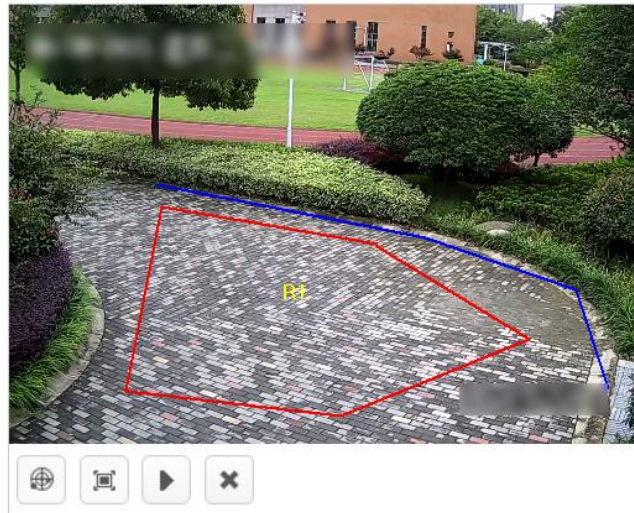



Figure 3-95 Custom Detection Area

- Full screen detection.

Click  to do full screen detection.

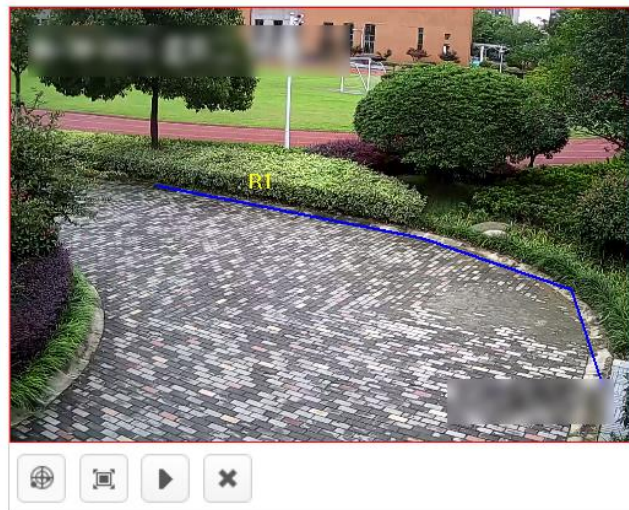



Figure 3-96 Full Screen Detection

 **NOTE**

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

Step 3 Set alarm interval.



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

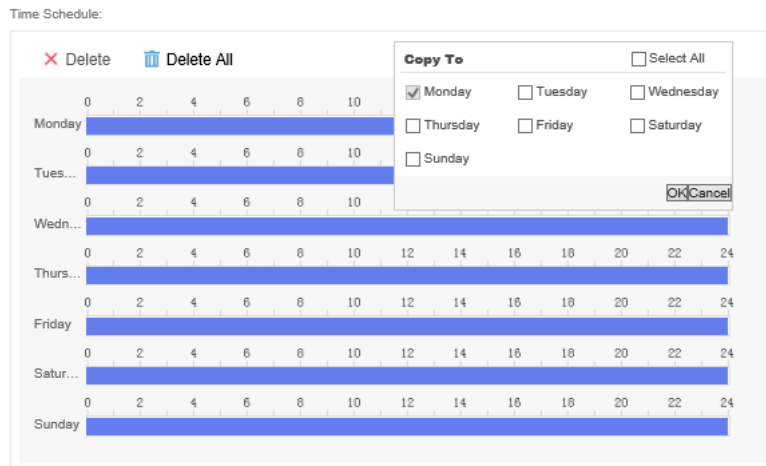


Figure 3-97 Set Detection Time Schedule

Step 5 Click **Save**.

3.6 Street Analysis Task

3.6.1 Create a Street Analysis Task

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

Steps

Step 1 Click **Task Management** -> **New**.

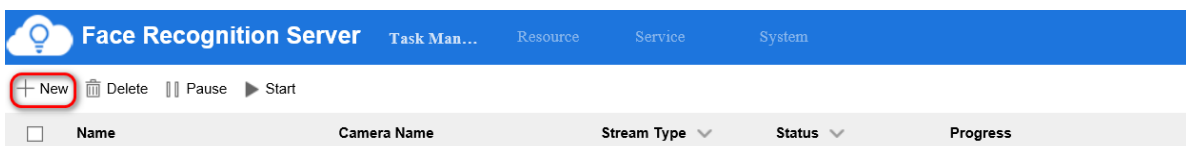



Figure 3-98 Task Management Interface



Step 2 Enter a task name.

Step 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.  No data. 

Add Rule

Figure 3-99 Create Task Interface

 **NOTE**

Keep **Auxiliary Parameter Settings** by default.

Step 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

Step 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**.

Step 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.

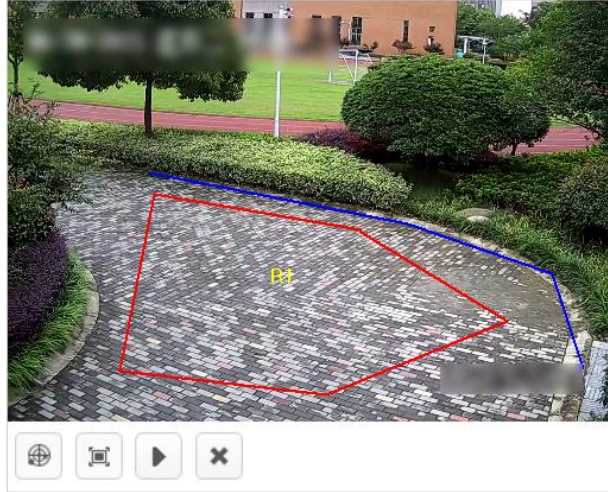


Figure 3-100 Custom Detection Area

- Full screen detection

Click  to do full screen detection.

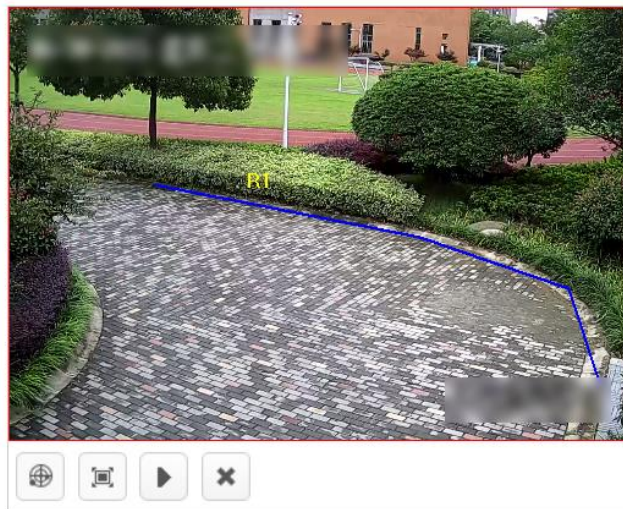




Figure 3-101 Full Screen Detection

 **NOTE**

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

Step 3 Set Sensitivity. The higher the alarm sensitivity is, the easier an alarm can be triggered.

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

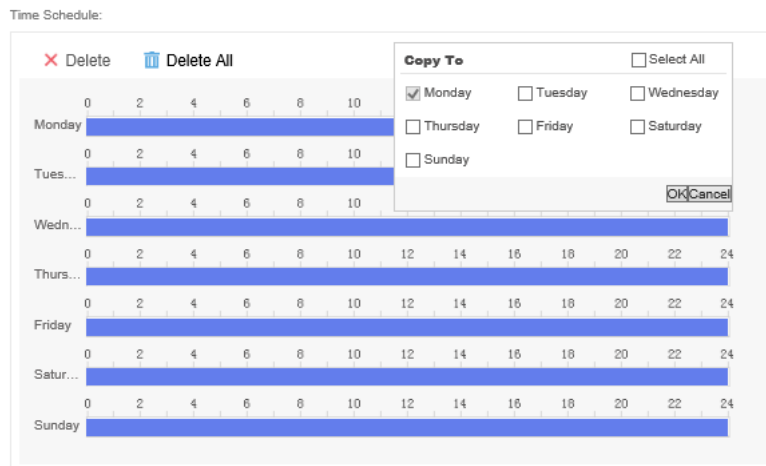


Figure 3-102 Set Detection Time Schedule

Step 5 Click **Save**.

3.6.3 Fast Moving Detection

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


Steps

Step 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**.

Step 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.

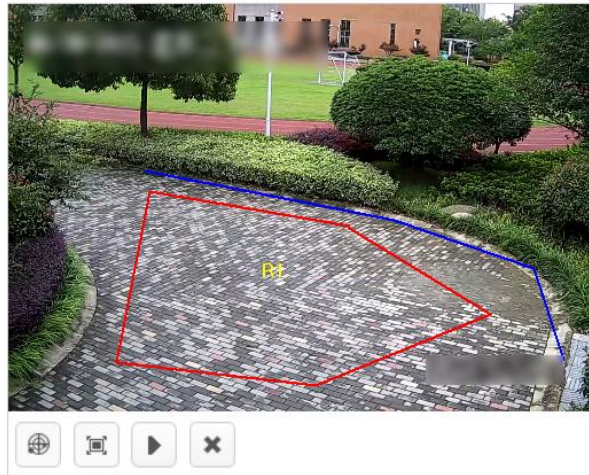



Figure 3-103 Custom Detection Area

- Full screen detection

Click  to do full screen detection.

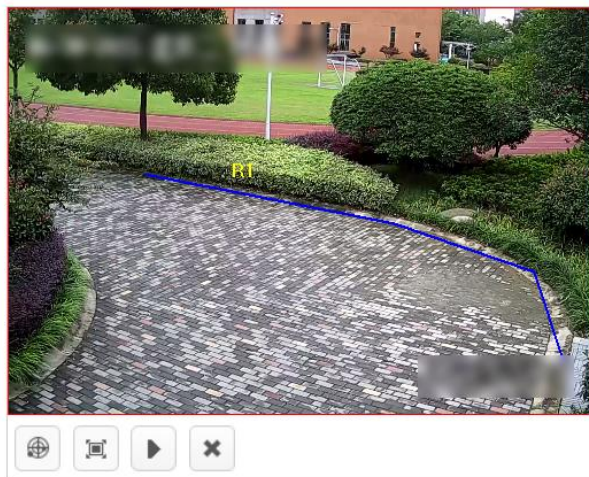



Figure 3-104 Full Screen Detection

 **NOTE**

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

Step 3 Set sensitivity and duration. The higher the alarm sensitivity is, the easier an alarm can be triggered.

Step 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.

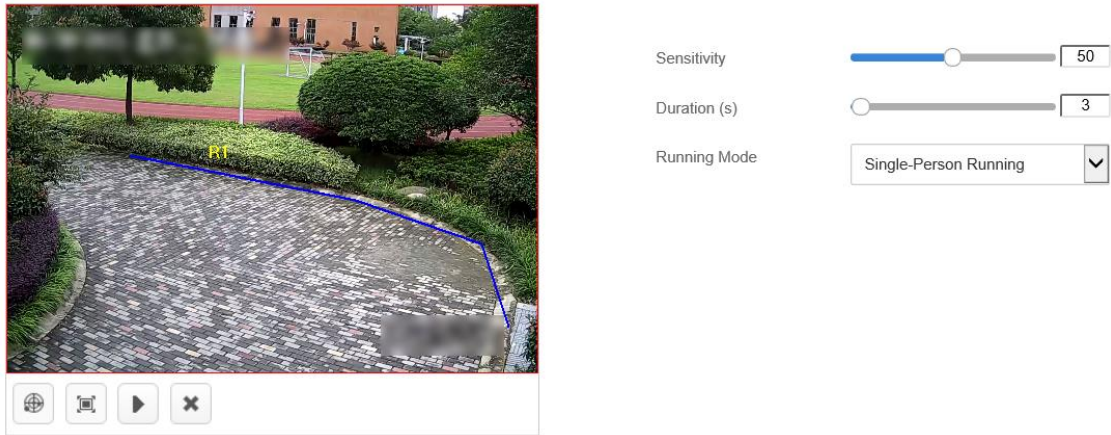



Figure 3-105 Set Rule Parameters in Details

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

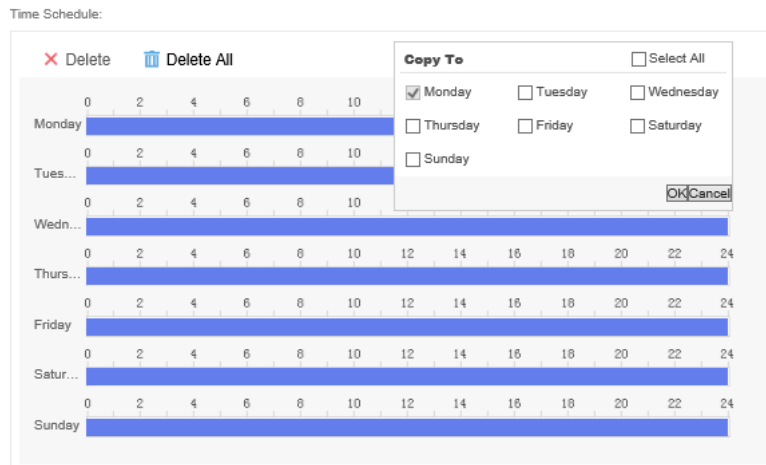


Figure 3-106 Set Detection Time Schedule

Step 6 Click **Save**.

3.6.4 Physical Conflict Detection

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


Steps

Step 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**.

Step 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.

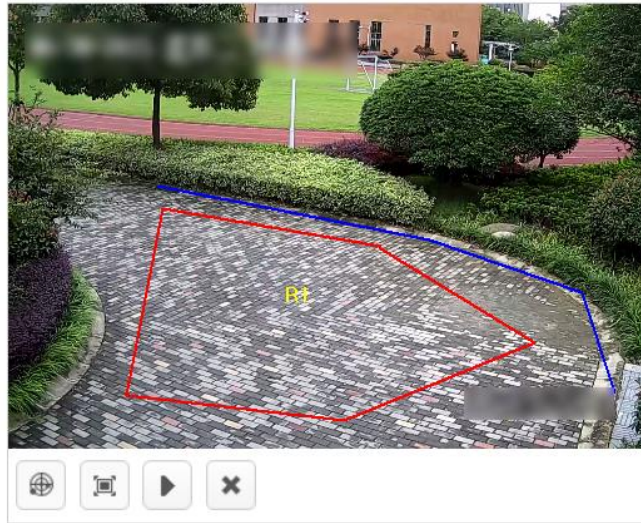


Figure 3-107 Custom Detection Area

- Full screen detection



Click  to do full screen detection.



Figure 3-108 Full Screen Detection

 **NOTE**

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

Step 3 Set sensitivity and duration. The higher the alarm sensitivity is, the easier an alarm can be triggered.

Step 4 Set detection mode and alarm interval.

- **Alarm Mode:** default value.
- **Alarm Internal:** the minimum internal between two alarms.

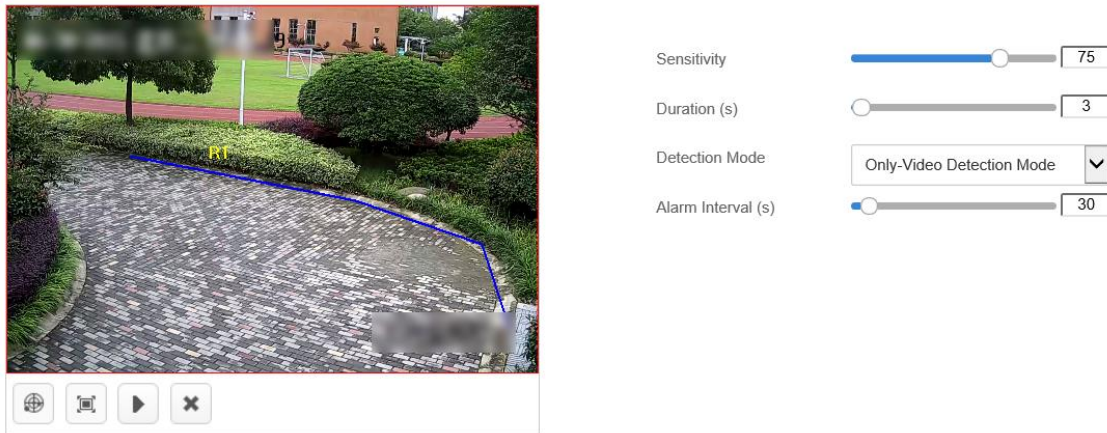


Figure 3-109 Set Rule Parameters in Details

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

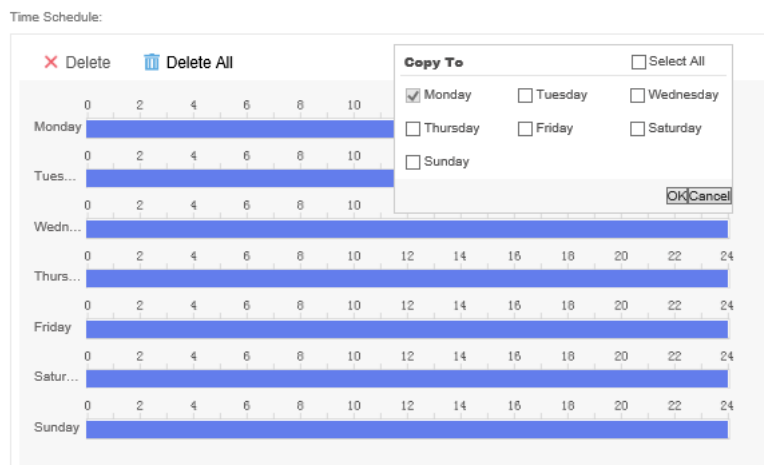


Figure 3-110 Set Detection Time Schedule

Step 6 Click **Save**.

3.6.5 People Gathering Detection

Detect gathering behavior of people in street scene.


Steps

Step 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**.

Step 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.

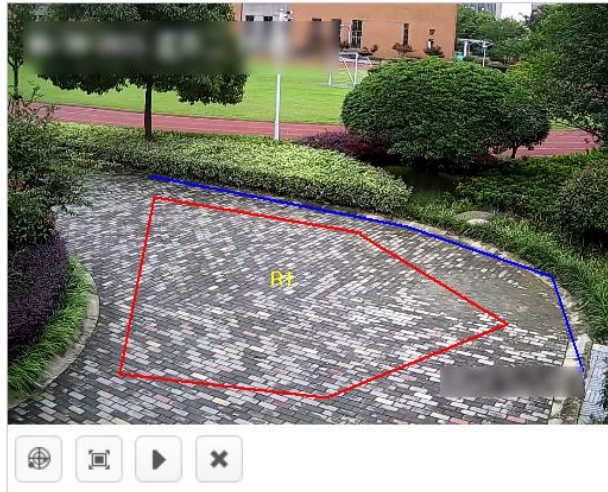


Figure 3-111 Custom Detection Area

- Full screen detection



Click  to do full screen detection.



Figure 3-112 Full Screen Detection

 **NOTE**

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

Step 3 Set sensitivity and duration. The higher the alarm sensitivity is, the easier an alarm can be triggered.

Step 4 Set the alarm interval and minimum number of people.

- **Alarm Internal(s):** the minimum internal between two alarms
- **Min. People:** the minimum number of gathering people



Figure 3-113 Set Rule Parameters in Details

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

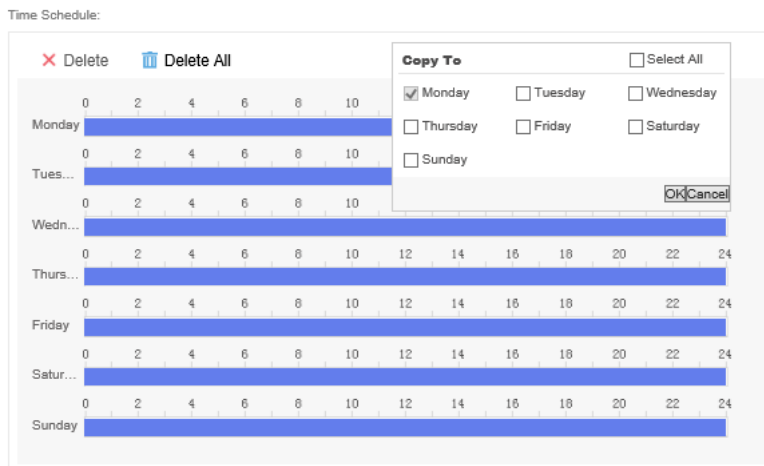


Figure 3-114 Set Detection Time Schedule

Step 6 Click **Save**.

Chapter 4 Task Management

4.1 Edit a Task

Edit the established detection rule or add a new one.

Steps

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

<input type="checkbox"/>	Name	Camera Name	Stream Type	Status
<input type="checkbox"/>	Task 1	Camera 1	Stream 1	Running
<input type="checkbox"/>	Task 2	Camera 1	Stream 1	Running
<input type="checkbox"/>	Task 3	Camera 1	Stream 1	Running
<input type="checkbox"/>	Task 4	Camera 1	Stream 1	Running
<input type="checkbox"/>	Task 5	Camera 1	Stream 1	Running
<input type="checkbox"/>	Task 6	Camera 1	Stream 1	Running
<input type="checkbox"/>	Task 7	Camera 1	Stream 1	Running
<input type="checkbox"/>	Task 8	Camera 1	Stream 1	Running
<input type="checkbox"/>	Task 9	Camera 1	Stream 1	Running
<input type="checkbox"/>	Task 10	Camera 1	Stream 1	Running

Figure 4-1 Task Management Interface

NOTE

Move mouse to **Stream Type** and **Status** to filter tasks.

Step 2 Click rule name in **Rule List**, edit detection rules as needed.

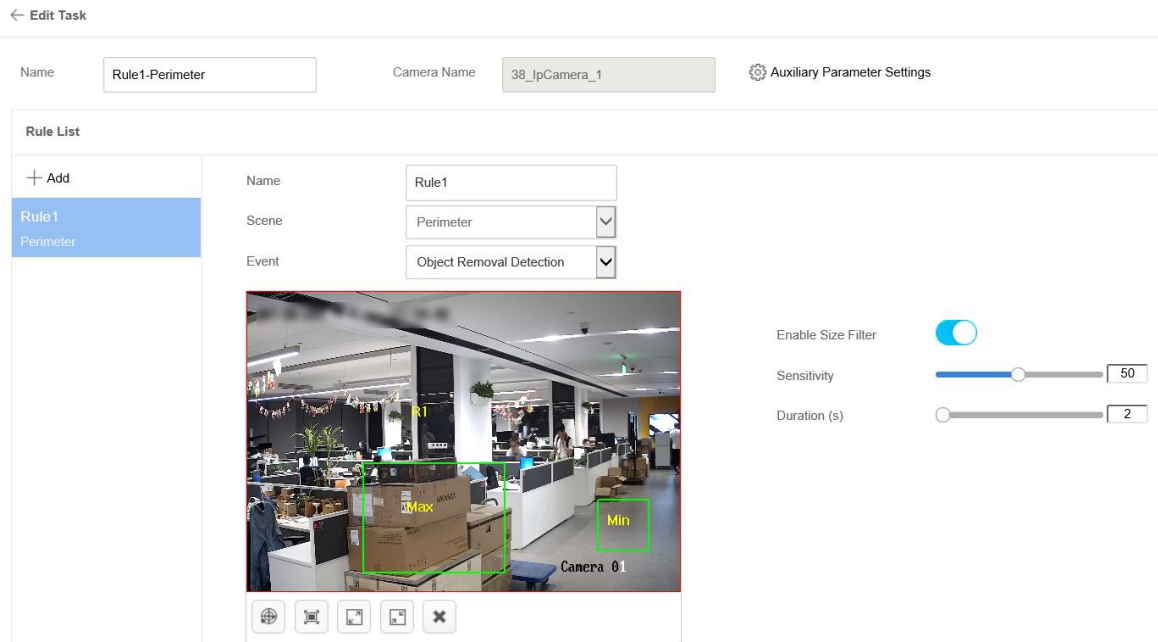


Figure 4-2 Edit Detection Rules

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

4.2 Delete a Task

Delete tasks that have been completed or no longer need to be analyzed.

Steps

Step 1 Click **Task Management**, and select the task to be deleted.

Step 2 Click **Delete**, and click **OK** in the popped up box.

4.3 Pause a Task

Steps

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

Step 2 Click **Pause**.

4.4 Start a Task

Steps

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

Step 2 Click **Start**.

Chapter 5 Smart Analysis Unit Management

5.1 Add a Smart Analysis Unit

Add a new smart analysis unit.

Steps

Step 1 Click **Service** -> **Smart Unit**, and then click **Add**.

Step 2 Enter smart analysis unit parameters.

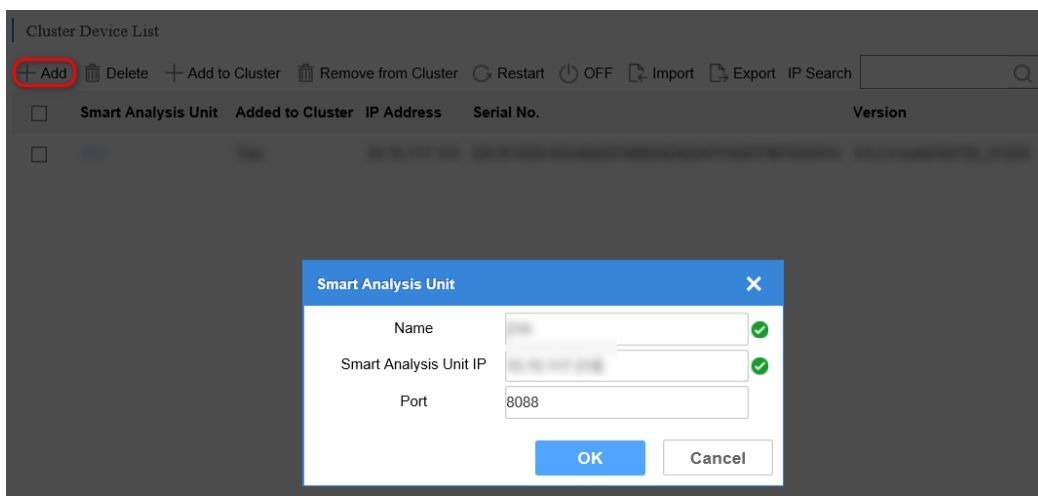


Figure 5-1 Add Smart Analysis Unit

5.2 Add to Cluster

Add the new smart analysis unit into cluster to enhance analysis ability.

Steps

Step 1 Click **Service** -> **Smart Unit**, and then click **Add**.

Step 2 Enter **Name**, **Smart Analysis Unit IP** and keep **Port** as default value.

Step 3 Click **OK** to add the new smart analysis unit into cluster.

5.3 Remove from Cluster

Remove the nodes from cluster. The cluster will be disbanded if master or backup nodes are removed.

Steps

Step 1 Click **Service** -> **Smart Unit**.

Step 2 Check the nodes to be removed from cluster, and click **Remove From Cluster**.

Step 3 Click **OK**.

5.4 Restart a Smart Analysis Unit

Steps

Step 1 Click **Service** -> **Smart Unit**.

Step 2 Check smart analysis unit to be restarted, click **Restart**.

Step 3 Click **OK**.

5.5 Close a Smart Analysis Unit

Press the power button to turn it on if the smart analysis unit is closed.

Steps

Step 1 Click **Service** -> **Smart Unit**.

Step 2 Check smart analysis unit to be closed, click **OFF**.

Step 3 Click **OK**.

5.6 Configure Network Parameters

Configure smart analysis unit network parameters.

Steps

Step 1 Click **Service** -> **Smart Unit**, and then click on the name of smart analysis unit.

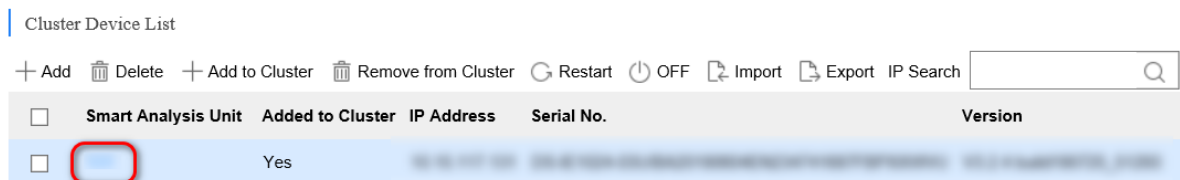


Figure 5-2 Cluster Device List

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

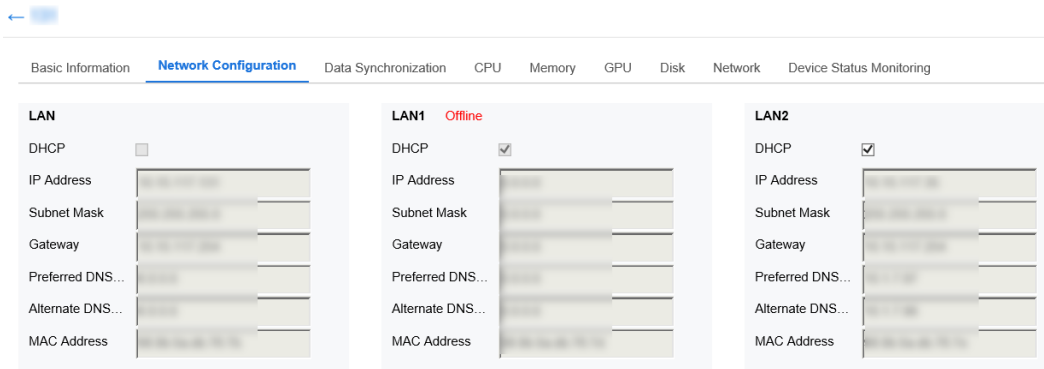


Figure 5-3 Edit Network Parameters

5.7 View Hardware Resource

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

Steps

Step 1 Click **Service** -> **Smart Unit**, and then click on the name of smart analysis unit.

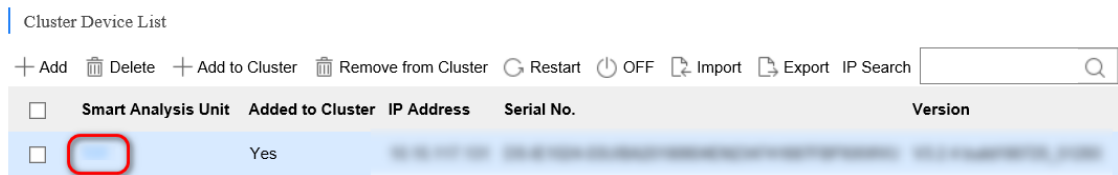


Figure 5-4 Cluster Device List

Step 2 Click the tab to view the usage of hardware.

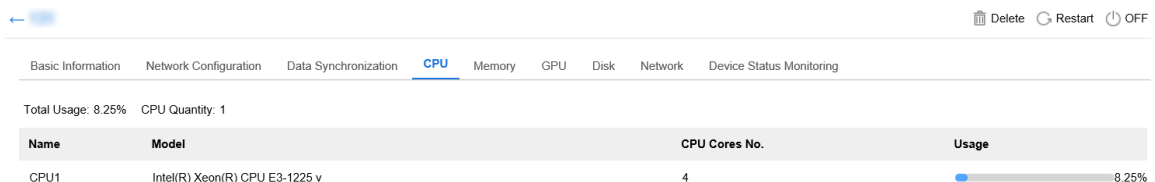


Figure 5-5 View Hardware Resource

Chapter 6 System Management

6.1 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.

6.2 Service Configuration

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

Steps

Step 1 Click **System** -> **Service**, and then click **Add**.

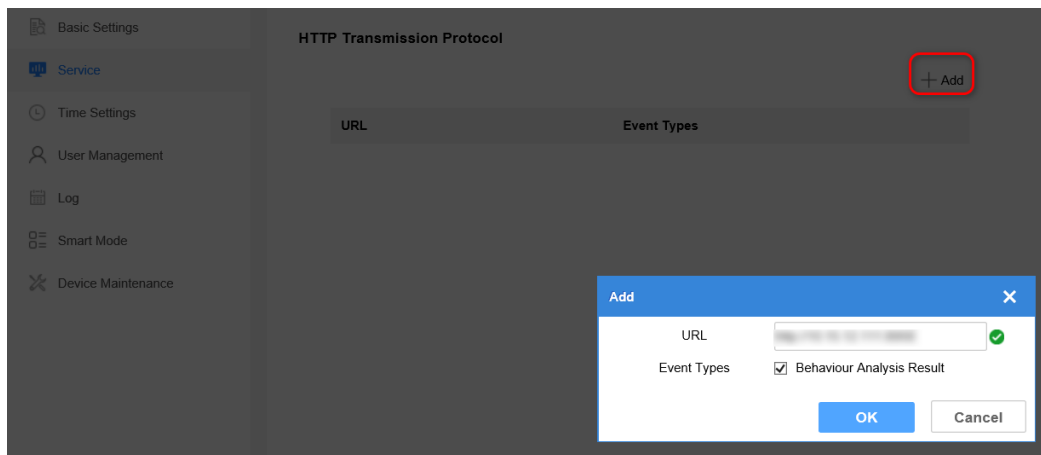


Figure 6-1 Service Configuration Interface

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



NOTE

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

Step 3 Click **OK**.

6.3 Time Configuration

Enable time sync as required. System time can be set by NTP sync or manual time sync. The IP address and port information of the NTP server should be obtained at first for NTP sync.

Steps

Step 1 Click **System** -> **Time Settings**.

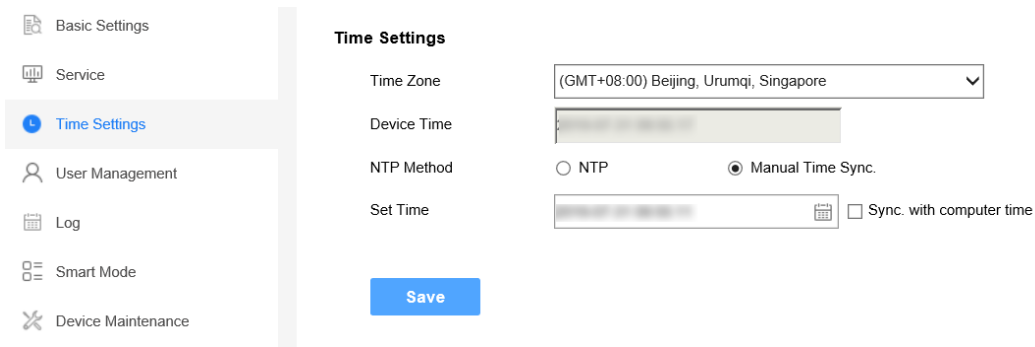


Figure 6-2 Time Configuration Interface

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



NOTE

Check **Sync. with computer time**, the device time will synchronize with the computer.

Step 3 Click **Save**.

6.4 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.

6.4.1 Add a User

Up to 31 users can be added.

Steps

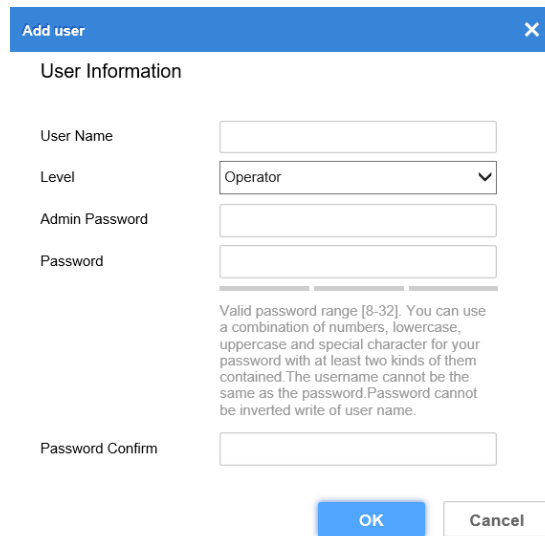
Step 1 Click **System** -> **User Management**.

Step 2 Click **Add** and enter user information in the popped up box.



NOTE

To protect your privacy and enterprise data, avoid device network security problem, we highly recommend you create a strong password in accordance with security rules.



Add user [X]

User Information

User Name

Level

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 6-3 Add User

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

6.4.2 Modify a Password

Steps

Step 1 Click **System** -> **User Management**.

Step 2 Click on the user name line, and then click **Modify**.

Step 3 Enter the admin password, new password and confirm the new password. Click **OK**.

6.4.3 Delete a User

The default user admin cannot be deleted.

Steps

Step 1 Click **System** -> **User Management**.

Step 2 Click the user name line, click **Delete**.

Step 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.

6.5 Log Management

6.5.1 Log Search


The 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

Step 1 Click **System** -> **Log**.

Step 2 Select the type of log. Set the starting and ending time of search.

Step 3 Click , and corresponding log information will be displayed.

Step 4 (optional) Click **Export**, and click **OK** in the popped up box to export the log as needed.

6.5.2 Download Maintenance Log

Maintenance log is used by professional maintenance personnel to maintain device.

Steps

Step 1 Click **System** -> **Device Maintenance**.

Maintenance Log



Figure 6-4 Download Maintenance Log

Step 2 Click **Download Maintenance Log**, and click **OK** in the popped up box. It may take a few minutes to export the maintenance log. Please wait and select the save path as prompted.

6.6 Smart Mode

Smart mode includes **Single Smart Mode** and **Multi-Smart Mode**. Single smart mode is set by default.

- **Single Smart Mode:** Only the analysis capability of the device algorithm supported. Algorithm packages with other task analysis capabilities cannot be uploaded.
- **Multi-Smart Mode:** Algorithm packages with other task analysis capabilities are supported to be uploaded.

Before you start

The cluster has been disbanded.

Steps

Step 1 Click **System** -> **Smart Mode**.

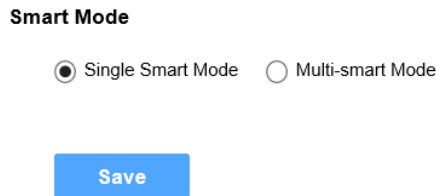


Figure 6-5 Switch Smart Mode

Step 2 Select the **Single Smart Mode** or **Multi-smart Mode** as needed.

Step 3 Click **Save**.

6.7 Software Updating

Update the software via Web interface.

Before you start

- The smart analysis unit has been online without any exception.
- You have obtained updating files.

Steps

Step 1 Click **System** -> **Device Maintenance**.



Figure 6-6 Software Updating

Step 2 Check the smart analysis unit to be upgraded. Click **Browse** and select the file. Click **Upgrade** after the file is uploaded

Step 3 Click **OK** to start upgrading. The device will restart automatically after upgrading.

6.8 Restore Defaults

Restore defaults includes **Restore** and **Default**.

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

Before you start

The cluster has been disbanded.

Steps

Step 1 Click **System** -> **Device Maintenance**.

Restore Defaults

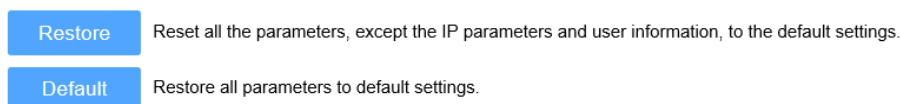


Figure 6-7 Restore Defaults

Step 2 Select **Restore** or **Default** as needed.

6.9 Help Center

You can refer to the help document by going to **Help** -> **Help Document** on the top-right corner of the interface to view or download the document.

6.10 Version Information

You can check version information of different modules by going to **Help** -> **Version** on the top-right corner of the interface.

6.11 Logout

Steps

Step 1 Click **admin** -> **Logout** on the top-right corner of the interface.

Step 2 Click **OK** in the popped up box.

6.12 Obtain iVMS-4200 Client Software

Steps

Step 1 Click **4200 Download** at the top-right corner of the interface to download iVMS-4200 Client Software.

Step 2 Install iVMS-4200 Client Software.

Chapter 7 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.

7.1 Login

Before you start

You have obtained and installed Guarding Vision client software.

Steps

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

 A screenshot of a Windows-style dialog box titled "Register Administrator". The dialog has a dark title bar with a close button (X) on the right. The main area is light gray and contains the following elements: a green instruction line "Please create a super user before proceeding."; a "Super User:" label followed by a text input field containing "admin"; a "Password:" label followed by a password input field with 10 black dots; a "Confirm Password:" label followed by another password input field with 10 black dots; a checkbox labeled "Enable Auto-login" which is currently unchecked; and at the bottom right, two buttons labeled "Register" and "Cancel".

Figure 7-1 Register Super User



NOTE

- Special characters (V:*?"<>|) are invalid when setting user name.
- You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained. Password cannot be the same as or opposite to the user name.

Step 2 (Optional) Check **Enable Auto-login**. The current user will log in automatically next time.

7.2 Add a Server

Add the server to the client for management after login.

7.2.1 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

Step 1 Click **Hikvision Device**, and then click **Add**.

Step 2 Select **Adding Mode** as **IP/Domain**. Enter parameters of the desired server.

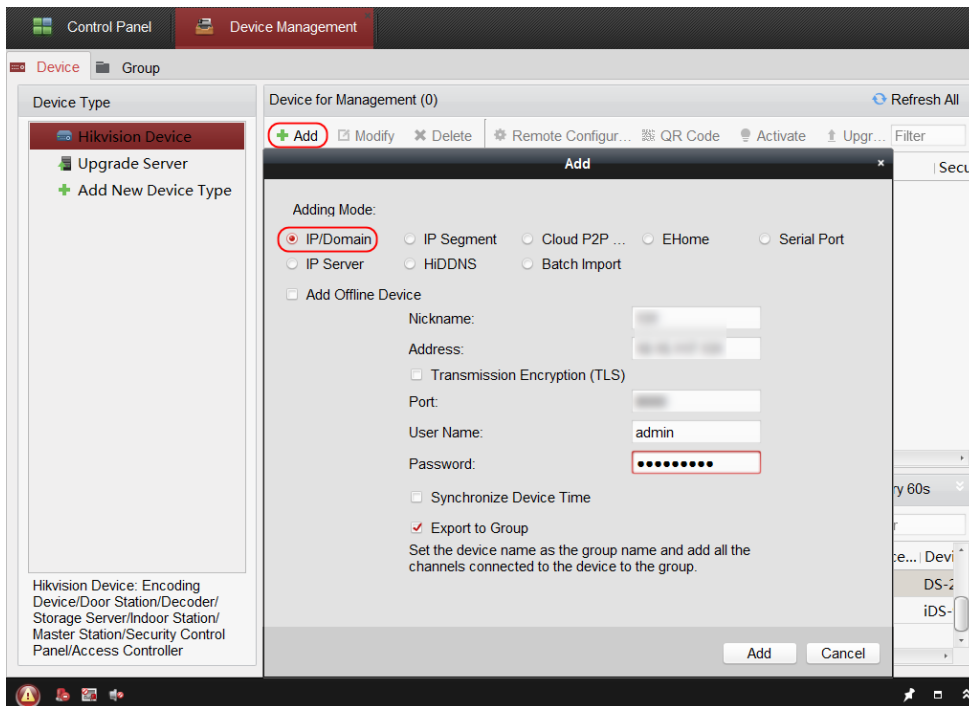


Figure 7-2 Manual Adding

Step 3 Click **Add**.



Check **Import to Group** to add all server channels to the groups named according to the server alias.

7.2.2 Add Server Online

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

Step 1 Click **Hikvision Device**. Click the desired server which is in the online device list.

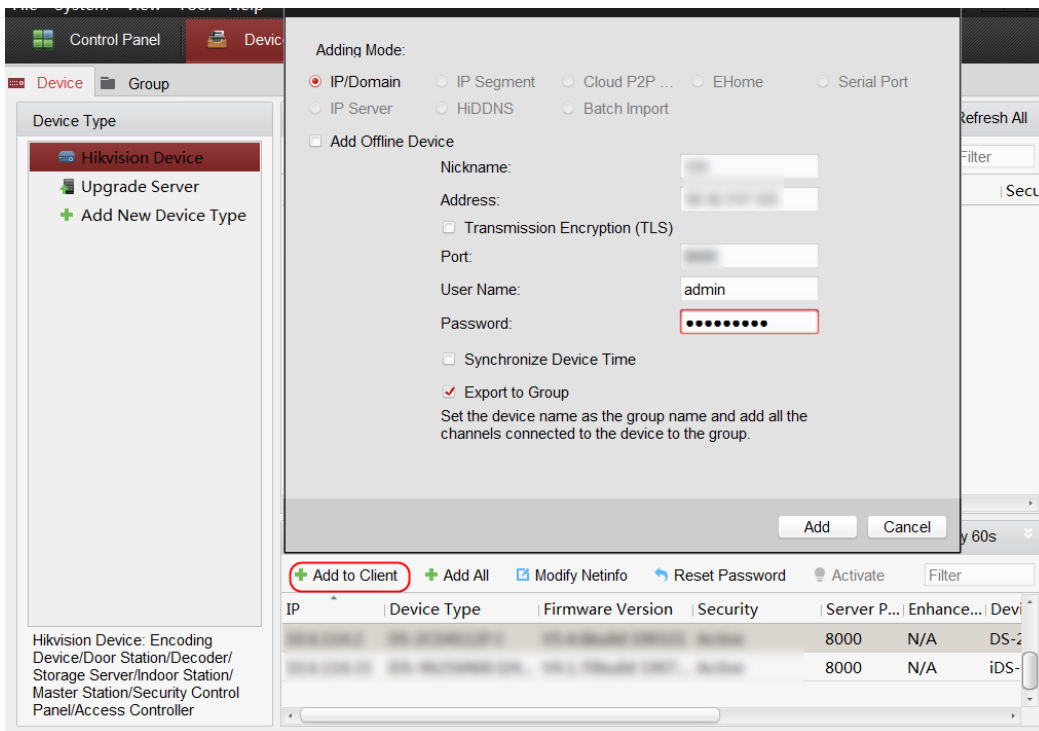


Figure 7-3 Online Adding

Step 2 Click **Add to Client** and enter nickname, address, port, user name and password on the popped up box.

Step 3 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.

7.3 Remote Configuration

Configure the server via Guarding Vision client software.

Steps

Step 1 Click **Hikvision Device**. Click the added server.



Figure 7-4 Select Server

Step 2 Click **Remote Configuration** -> **General**. The Server Web configuration interface will pop up.

Step 3 Configure parameters according to actual needs.

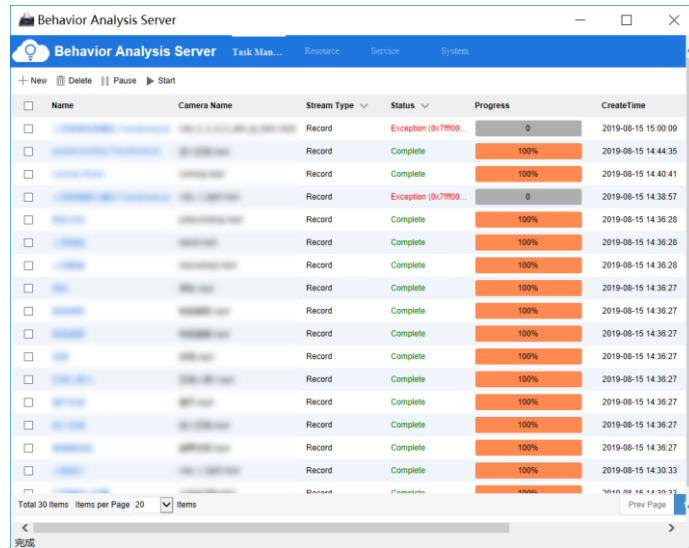


Figure 7-5 Server Web Interface

7.4 Live View

Preview the analysis task interface.

Steps

Step 1 Click **Control Panel** -> **Main View**.

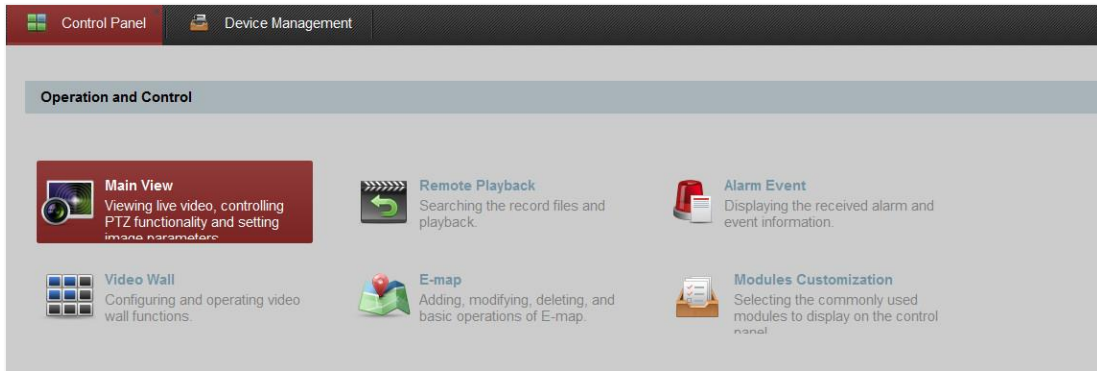


Figure 7-6 Live View Interface

Step 2 In the camera bar, drag the camera to the window to be played, or select the playing window and double-click the camera, then the window displays the real-time video of the camera.

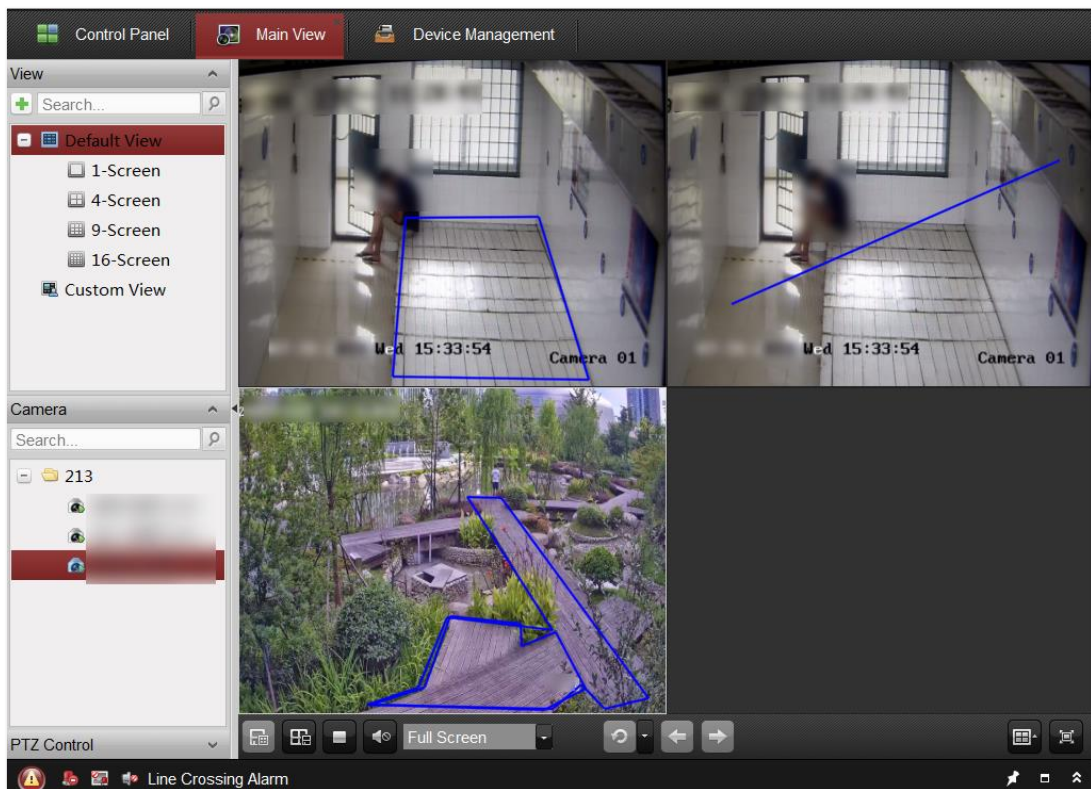







Figure 7-7 Live View Interface

NOTE

- On the bottom-right corner of the window,  means the image of live view,  means starting to record,  means switching to instant playback,  on the bottom-right corner of the window indicates closing the live view image.
- Select a group to drag directly to any position on the right window, or double-click the group to preview all the cameras in the group. Click  to stop previewing all image of channels.

7.5 Alarm Center

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

Steps

Click **Control Panel** -> **Alarm Event**. Enter the alarm information interface.




Figure 7-8 Click Alarm Event

View detailed alarm information, including alarm time, alarm source, alarm details, alarm content, etc. The red font indicates the unprocessed alarm information, and the black one indicates the processed alarm information.



...	Alarm Time	Alarm Source	Alarm Details	Alarm Content	Live View	Send Email	Video Wall Display	Note
1...	2019-07-31 15:3...	Encoding Device:213 ...			🟢	✉	🖥	
1...	2019-07-31 15:3...	Encoding Device:213 ...			🟢	✉	🖥	
1...	2019-07-31 15:3...	Encoding Device:213 ...			🟢	✉	🖥	
1...	2019-07-31 15:3...	Encoding Device:213 ...			🟢	✉	🖥	
1...	2019-07-31 15:3...	Encoding Device:213 ...			🟢	✉	🖥	
1...	2019-07-31 15:3...	Encoding Device:213 ...			🟢	✉	🖥	
1...	2019-07-31 15:3...	Encoding Device:213 ...			🟢	✉	🖥	
1...	2019-07-31 15:3...	Encoding Device:213 ...			🟢	✉	🖥	
1...	2019-07-31 15:3...	Encoding Device:213 ...			🟢	✉	🖥	
1...	2019-07-31 15:3...	Encoding Device:213 ...			🟢	✉	🖥	
1...	2019-07-31 15:3...	Encoding Device:213 ...			🟢	✉	🖥	
1...	2019-07-31 15:3...	Encoding Device:213 ...			🟢	✉	🖥	
1...	2019-07-31 15:3...	Encoding Device:213 ...			🟢	✉	🖥	
1...	2019-07-31 15:3...	Encoding Device:213 ...			🟢	✉	🖥	
1...	2019-07-31 15:3...	Encoding Device:213 ...			🟢	✉	🖥	
1...	2019-07-31 15:3...	Encoding Device:213 ...			🟢	✉	🖥	
1...	2019-07-31 15:3...	Encoding Device:213 ...			🟢	✉	🖥	
1...	2019-07-31 15:3...	Encoding Device:213 ...			🟢	✉	🖥	

Figure 7-9 Alarm Information


● Clear List

Click  or click the right button of mouse in the alarm information list and click **Clear** 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.

- **Live View**

Click  to preview the real-time image of camera which triggered the alarm.

7.6 (Optional) Configure Storage Server

To store alarm captures and video files.

7.6.1 Install Storage Server

Steps

Step 1 Check **Storage Server** when installing Guarding Vision client software.

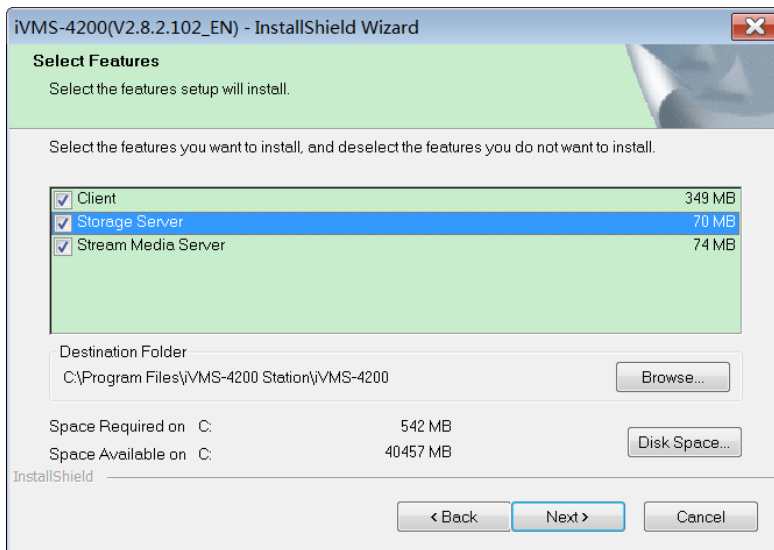



Figure 7-10 Select Features

NOTE

If **Storage Server** is checked when you install Guarding Vision client software, the PC itself can serve as a storage server.

Step 2 After the installation completed, double-click the desktop shortcut icon  to enable the storage server.

Step 3 Set the password if it is the first time to enable the storage server.



Figure 7-11 Set Password

7.6.2 Add Storage Server

Steps

Step 1 Click **Device Management**.

Step 2 Click **Hikvision Device**. Click **Add**.

Step 3 Select **IP/Domain** as **Adding Mode**. Enter parameters of the desired storage server.

- **IP:** IP address of PC with storage server installed.
- **User Name:** admin.
- **Password:** The password set when enables the storage server for the first time.

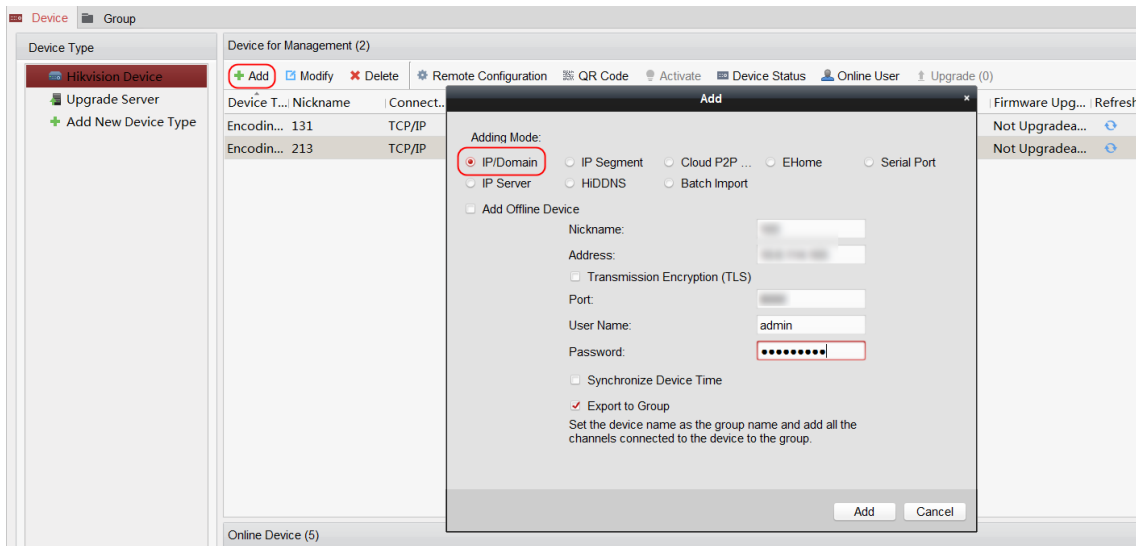


Figure 7-12 Add Storage Server

Step 4 Click **Add**.

7.6.3 Configure Storage Server

Steps

Step 1 Click **Hikvision Device**. Select a storage server and click **Remote Configuration**.

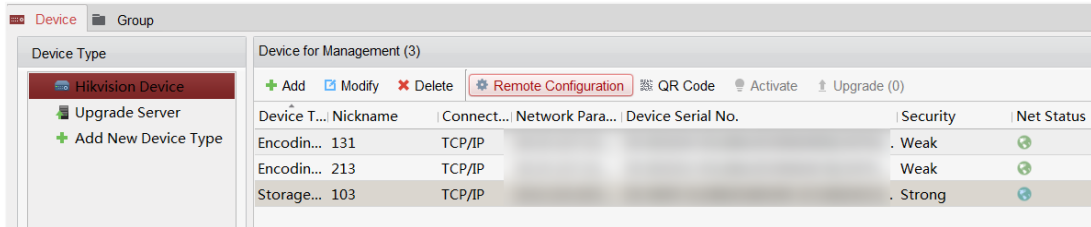


Figure 7-13 Select Server

Step 2 Click **Storage** -> **General**.



Formatting will erase all data on the partition.

Step 3 Check disk partition, and click **Format**. Click **OK** in the popped up box.

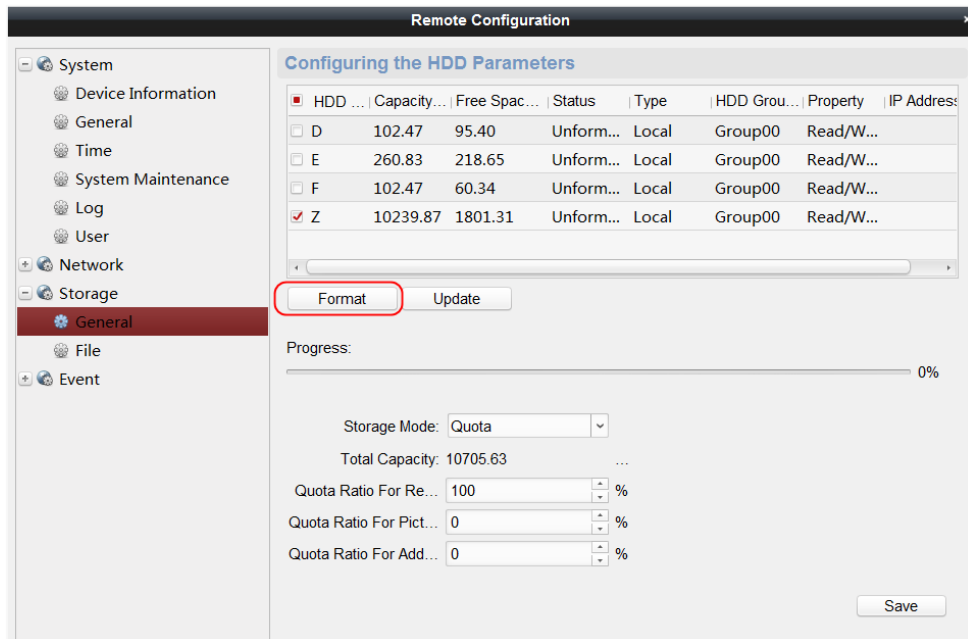


Figure 7-14 Storage Server Configuration

Step 4 Set the storage quota ratio for recording and capturing. Click **Save**.



Restart the storage server when the configuration completed.

7.7 Configure Storage Schedule

Steps

Step 1 Click **Control Panel > Storage Schedule**.

Step 2 Configure storage section and storage schedule.

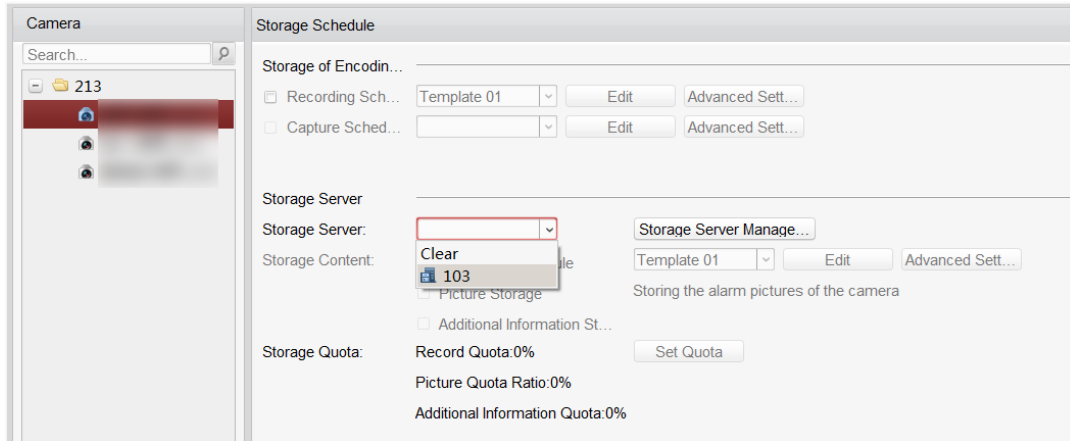


Figure 7-15 Configure Storage Schedule

Step 3 Check **Recording Schedule** in **Storage Server** tab, and select a template. The recording time in the template can be edited according to actual needs.

Step 4 Select the desired detection task, check **Recording Schedule** and **Picture Storage**, and then set the record quota percentage.

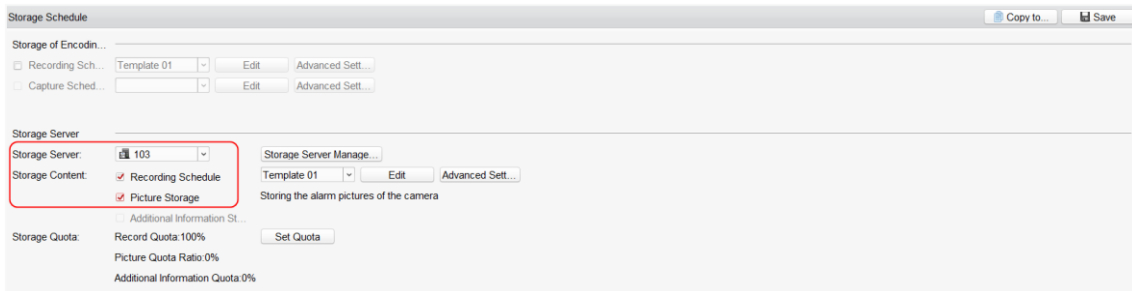


Figure 7-16 Storage Schedule Configuration

Step 5 Click **Save**.

