Intelligent Video Analysis Server for Traffic Event Detection

User's Manual

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

V2.0.1

Foreword

General

This manual introduces the installation, configuration and operations of the intelligent video analysis server for traffic event detection (hereinafter referred to as "the Server"). Read carefully before using the device, and keep the manual safe for future reference.

Models

IVS-TB8000-E

Safety Instructions

The following signal words might appear in the manual.

Signal Words	Meaning
⚠ DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
⚠ WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
⚠ CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, reductions in performance, or unpredictable results.
TIPS	Provides methods to help you solve a problem or save time.
NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V2.0.1	Baseline upgrade.	April 2023
V2.0.0	● Updated Client Installation, Client Configuration, and Business Application. ● Added Web Operations.	June 2022
V1.0.0	First release.	August 2021

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

Interface Declaration

This manual mainly introduces the relevant functions of the device. The interfaces used in its manufacture, the procedures for returning the device to the factory for inspection and for locating its faults are not described in this manual. Please contact technical support if you need information on these interfaces.

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

This section introduces content covering the proper handling of the device, hazard prevention, and prevention of property damage. Read carefully before using the device, and comply with the guidelines when using it.

Transportation Requirements

⚠

Transport the server under allowed humidity and temperature conditions.

Storage Requirements

⚠

Store the server under allowed humidity and temperature conditions.

Installation Requirements

⚠ WARNING

- Strictly comply with the local electrical safety code and standards. Make sure the ambient voltage is stable and meets the power supply requirements of the server.
- Do not expose the battery to environments with extremely low air pressure, or extremely high or low temperatures. Also, it is strictly prohibited for the battery to be exposed to extremely hot environments (such as direct sunlight or fire), and to cut or put mechanical pressure on the battery. This is to avoid the risk of fire and explosion.
- Use the standard power adapter. We will assume no responsibility for any problems caused by the use of a nonstandard power adapter.

⚠

- Do not place the device in a place exposed to sunlight or near heat sources.
- Keep the device away from dampness, dust, and soot.
- Put the device in a well-ventilated place, and do not block its ventilation.
- Install the switch horizontally on a stable surface to prevent it from falling.
- The device is a class I electrical appliance. Make sure that the power supply of the device is connected to a power socket with protective earthing.
- Use power cords that conform to your local requirements, and are rated specifications.
- Before connecting the power supply, make sure the input voltage matches the server power requirement.
- When installing the device, make sure that the power plug and appliance coupler can be easily reached to cut off power.
- Install the server in an area that only professionals can access.
- Extra protection is necessary for the device casing to reduce the transient voltage to the defined range.
- Install the device near a power socket for emergency disconnect.
- It is prohibited for non-professionals and unauthorized personnel to open the device casing.

Operation Requirements

⚠ **WARNING**

- This is a class A product. In a domestic environment this may cause radio interference in which case you may be required to take adequate measures.
- The device is heavy and needs to be carried by several persons together to avoid personal injuries.

⚠

- Make sure that the power supply is correct before use.
- Operate the device within the rated range of power input and output.
- Use the device under allowed humidity and temperature conditions.
- Do not drip or splash liquid onto the device, make sure that there is no object filled with liquid on the device to prevent liquid from flowing into it.
- Do not disassemble the device without professional instruction.
- Your configurations will be lost after performing a factory reset. Please be advised.
- Do not restart, shut down or disconnect the power to the device during an update.
- Make sure the update file is correct because an incorrect file can result in a device error occurring.
- The system cannot upgrade different types of AI modules at the same time.
- Do not frequently turn on/off the device. Otherwise, the product life might be shortened.
- Back up important data on a regular basis when using the device.
- Operating temperature: 10 °C to 35 °C (50 °F to 95 °F).

Maintenance Requirements

⚠ **WARNING**

- Make sure you use the same model when replacing the battery to avoid fire or explosion. Dispose the battery strictly following the instructions.
- Power off the device before maintenance.

⚠

- AI module does not support hot plug. If you need to install or replace the AI module, unplug the device power cord first. Otherwise, it will lead to file damage on the AI module.
- The device casing provides protection for internal components. Use a screwdriver to loosen the screws before detaching the casing. Make sure to put the casing back on and secure it in its original place before powering on and using the device.
- Clean the ventilation pipe regularly to avoid obstructions.
- It is prohibited for non-professionals and unauthorized personnel to open the device casing.
- The appliance coupler is a disconnection device. Keep it at a convenient angle when using it. Before repairing or performing maintenance on the device, first disconnect the appliance coupler.

Table of Contents

1 Product Introduction

This intelligent video analysis server for traffic event detection integrates server resources and intelligent analysis algorithms to analyze streams of network devices. It is widely used in traffic management and road operation and maintenance scenarios such as expressways, overpasses, tunnels, and cross-sea bridges.

1.1 Functions

Table 1-1 Function description

Function	Description
Parking detection	Detects an event when a vehicle moves and then stops, and the stop time exceeds the defined value.
Pedestrian detection	Detects an event when a pedestrian walks into the vehicle lane or an area where pedestrians are prohibited from entering, and the duration exceeds the defined value.
Non-motor vehicle detection	Detects battery-powered two-wheelers and tricycles.
Congestion detection	Detects an event when a lane is congested and the duration exceeds the defined value.
Traffic flow statistics	Statistics on the number of vehicles passing through a road section within a specified time.
Littering detection	Detects an event when an object littered by a person in a vehicle or a pedestrian disturbs traffic and the duration exceeds the defined value.
Emergency lane occupation detection	Detects an event when a vehicle enters the emergency lane.
Illegal lane change detection	Detects an event when a vehicle crosses the lane line (yellow or white solid line) and the duration exceeds the defined value.
Wrong-way driving detection	Detects an event when a vehicle is moving opposite to the specified direction and the duration exceeds the defined value.
Illegal backing detection	Detects an event when a vehicle is backing, for instance when missing the correct expressway intersection, and the duration exceeds the defined value.
Construction detection	Detects construction signs in the area for longer than the defined value.
Barrier detection	Detects barriers, such as boxes, that are in the area for longer than the defined value.
Accident detection	Detects an event when vehicles clash and the duration exceeds the defined value.
Radiation fog detection	Detects an event when radiation fog exists in the area and the duration exceeds the defined value.

Function	Description
Smoke detection	Detects an event when smog exists in the area and the duration exceeds the defined value.
Fire detection	Detects an event when fire exists in the area and the duration exceeds the defined value.
Crossing line detection	Detects an event when a vehicle crosses the lane line (yellow or white solid line) and the duration exceeds the defined value.
Speeding detection	Detects an event when the driving speed of a vehicle is higher than the defined value and the duration exceeds the defined value.
Underspeed detection	Detects an event when the driving speed of a vehicle is lower than the defined value and the duration exceeds the defined value.
Area intrusion	Detects an event when an object exists in an area and the duration exceeds the defined value.
Truck detection	Detects an event when a truck enters the detection zone.
Special vehicle detection	Detects an event when a special vehicle crosses the detection line.
Video exception detection	Detects an event when the video image changes.

1.2 Structure

1.2.1 Front Panel

Figure 1-1 Front panel

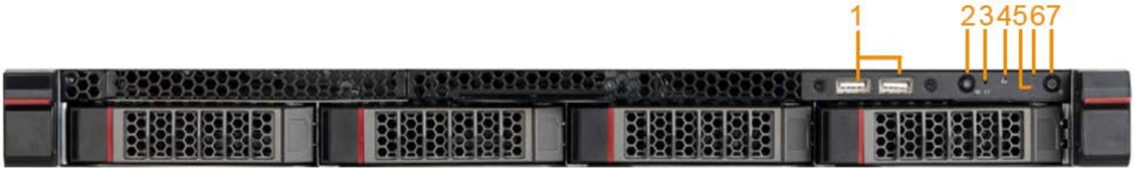


Table 1-2 Panel description

No.	Name	Description
1	USB2.0 port	Connects to external devices, such as a mouse and a keyboard.
2	UID switch and indicator	● When the server is off, press the button to enable the server and the indicator will be on. You can quickly find the location of the server through the indicator. ● When the server is enabled, press the button to disable it.
3	Reset button	Press and hold the button for 5 seconds, and the server will restore to factory defaults.

No.	Name	Description
4	Network status indicator	● Green light flashes: Network connected. ● Green light off: Network disconnected.
5	System status indicator	● Green light flashes: System runs normally. ● Red light flashes: System runs in redundancy or with decreased performance. It is a warning of system failure, such as on the redundant power supply or the cooling fan. ● Light off: System is not running.
6	HDD status indicator	● Green light flashes: HDD is active. ● Light off: HDD is inactive.
7	Power switch and indicator	Powered on or off. ● Light on: Powered on. ● Light off: Powered off.

1.2.2 Rear Panel

Figure 1-2 Rear panel

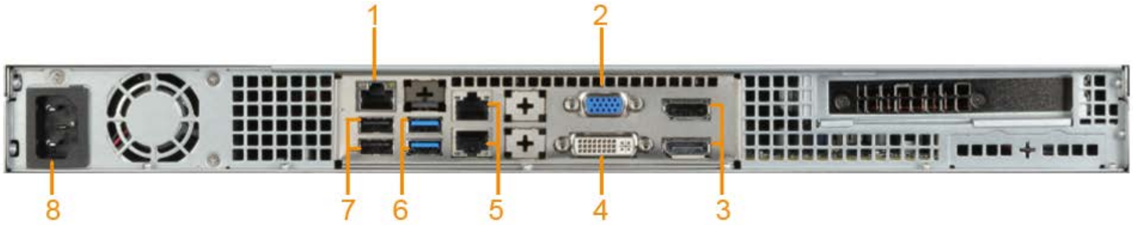
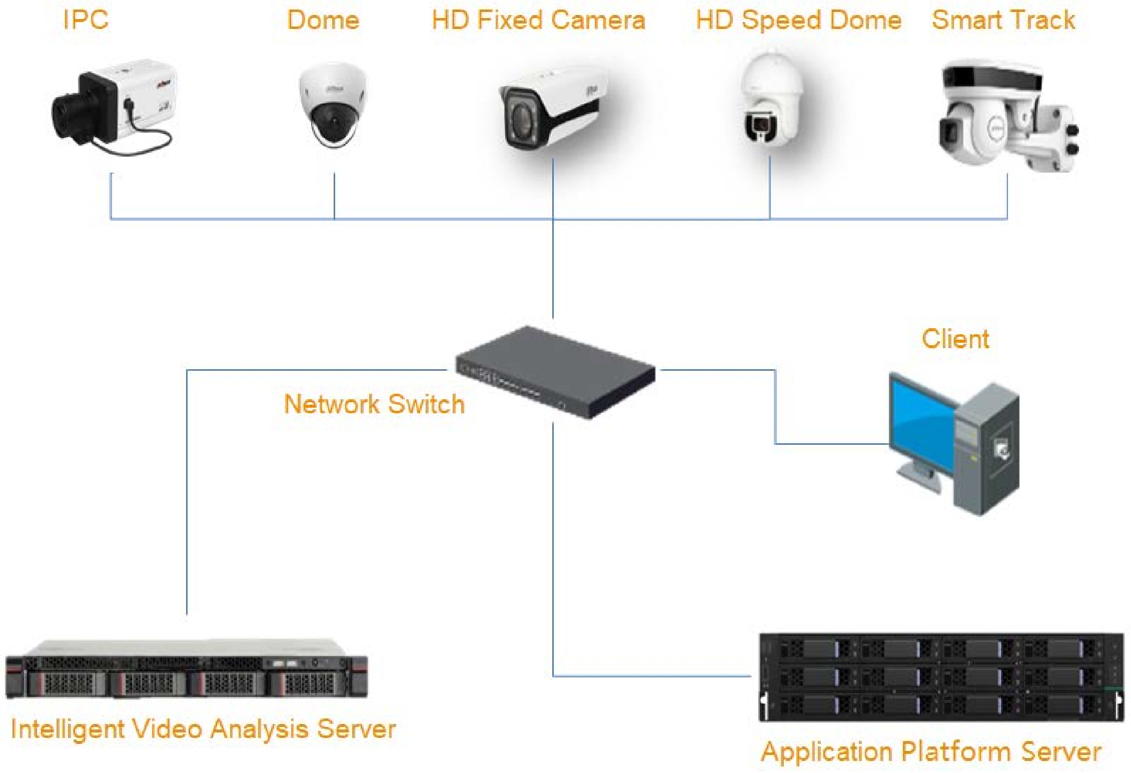


Table 1-3 Panel description

No.	Name	Description
1	IPMI_LAN	Port for remote management server.
2	VGA port	Connects to VGA display.
3	DP (DisplayPort)	Connects to DP display.
4	DVI-I port	Connects to DVI display.
5	Ethernet port	RJ45 (1000Base-T) port. Connects to the network.
6	USB3.0 port	Connects to external devices, such as a mouse and a keyboard.
7	USB2.0 port	
8	Power port	Connects to 220 VAC power supply.

1.3 Typical Networking

Figure 1-3 Typical networking



Networking description:

- Confirm that the devices in the network are connected.
- Log in to the intelligent analysis Client to operate the server. Set intelligent rules and record alarm events.
- One analysis card supports up to 32 channels of 1080P camera video data at the same time.
- The server is delivered with software installed completely by default. The default IP address is 192.168.1.108. Switch to the local IP once started. The default username and password are admin and admin123 respectively. Change your password in time on your first successful login.

2 Cable Connection

Background Information

Make sure that all cables are connected properly, and there is no obvious damage to the server and the cables.

Procedure

Step 1 Connect the display through VGA port, and connect the mouse and the keyboard through USB ports.

Step 2 Insert one end of the network cable into the Ethernet port on the rear panel of the server, and the other end to the network.

Step 3 Connect the power, and then the server will be started in about 20 seconds.

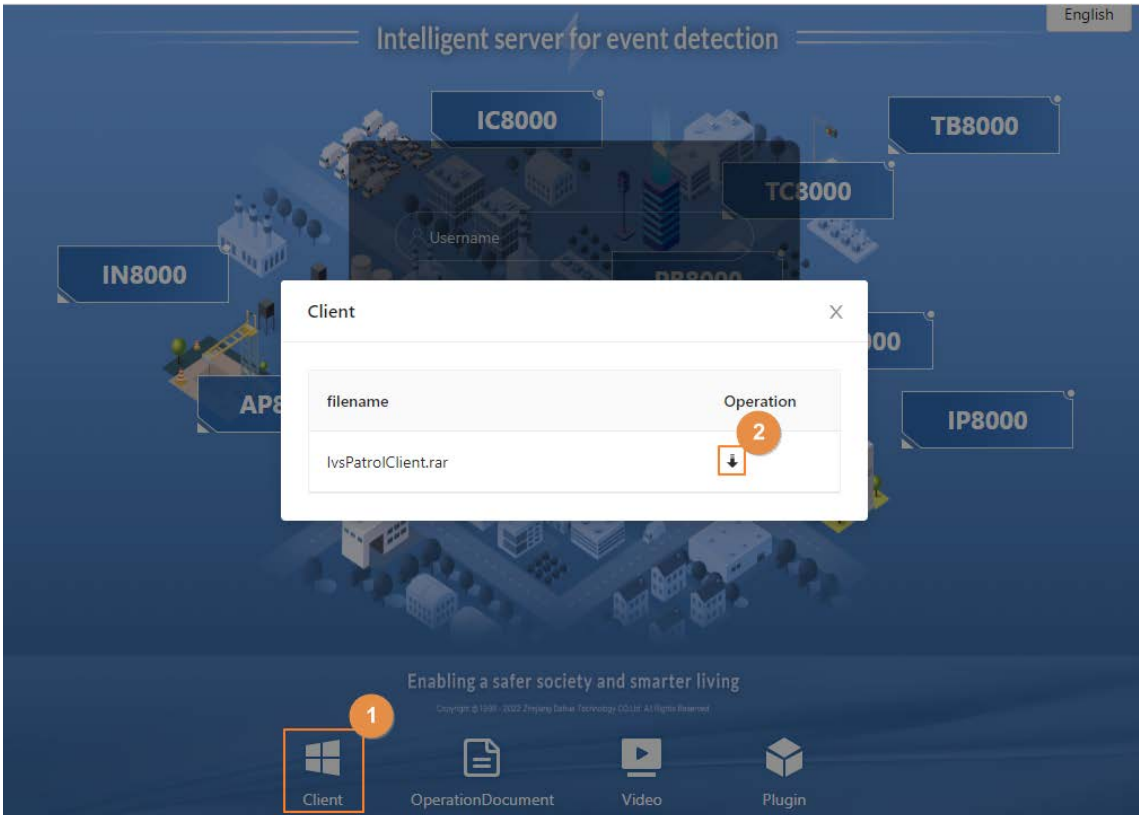
3 Client Installation

Download and install the Client Event Detection Intelligent Server (hereinafter referred to as "the Client") to before you can do any further operation and configuration.

Step 1 Download the Client.

1) Enter http://*server IP address* in the address bar of Chrome browser, and then press the Enter key.
2) Click **Client** at the bottom of the page, and then click ↓ to download the Client.

Figure 3-1 Download the Client



Client

filename	Operation
IvsPatrolClient.rar	↓

Step 2 Double-click the installation software, such as General_IvsPatrolClient_Chn_Base_IS_Version.exe.

The software name might vary with version and release date.

Step 3 Install the Client based on the instructions. Select **English** as the language of the Client.

After the installation is finished, the shortcut icon appears on the desktop.

Step 4 Select **I have read and agree to the terms of the Software License Agreement and Privacy Policy**, and then click **OK**.

Step 5 Double-click to open the Client.

Figure 3-2 Home

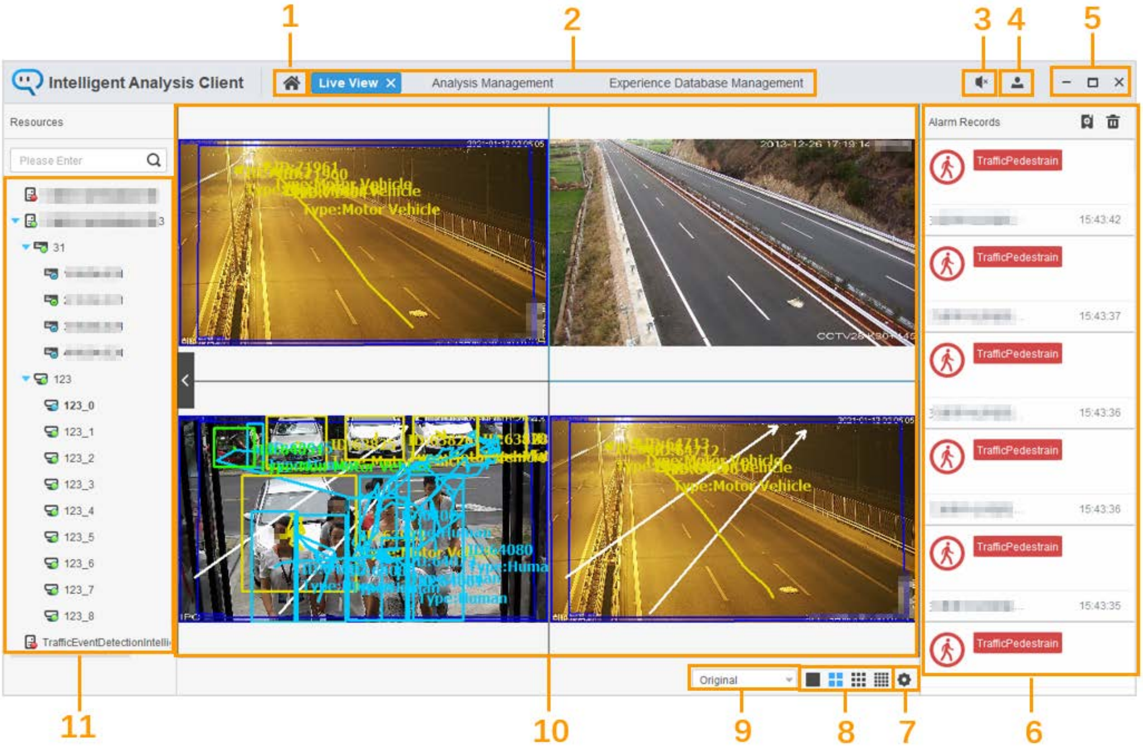


Table 3-1 Client home description

No.	Description
1	Home.
2	Function list.
3	Alarm sound on/off.
4	Click 👤 to view the system information, open source statement, license agreement, privacy policy and theme of the Client.
5	Minimize, maximize, and close the Client.
6	Alarm records.
7	Global configuration. You can customize information displayed in live videos.
8	Window split. Includes single screen, 4 splits, 9 splits, and 16 splits.
9	● Full screen: Displays the live view image in full screen. ● Original ratio: Displays the live view image in the actual ratio of the screen.
10	Live view video.
11	Device list. Displays servers added on the **Device Management** page.

4 Client Configuration

You can log in to the server through the Client, and then manage and configure detection solutions and rules.

4.1 Preparation

Before configuration, make sure that:

- The server is connected to the power supply.
- The Client is installed. For details, see "3 Client Installation".
- The network for the computer where the Client is to be installed has already been set up, and that the network cameras and the server are on the network segment.

4.2 Managing Server and Remote Devices

Add and link the traffic event detection server and remote devices to the Client before you can configure server and device parameters.

4.2.1 Managing Server

You can add, modify, and delete the information of the server.

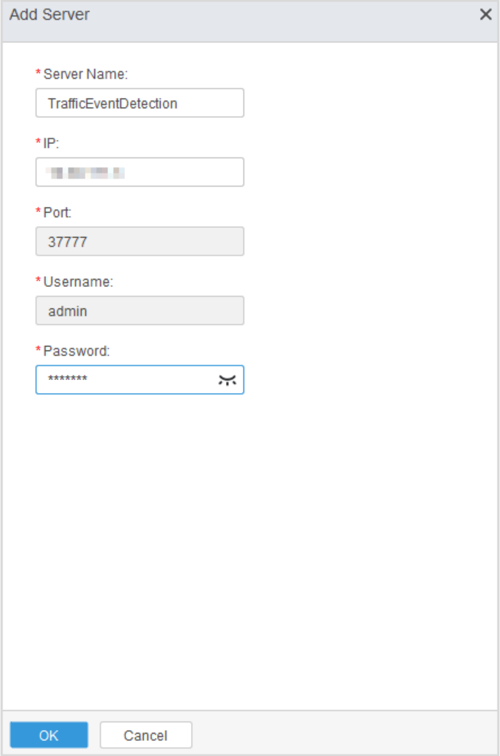
4.2.1.1 Adding Servers

Procedure

Step 1 Double-click to open the Client, and then click **Device Management**.

Step 2 Click + to add servers.

Figure 4-1 Add server



Add Server

* Server Name: TrafficEventDetection

* IP: [redacted]

* Port: 37777

* Username: admin

* Password: *******

Table 4-1 Description of adding device parameters

Parameter	Description
Server Name	Name the server on the Client to differentiate it from others.
IP	The IP address of the server.
Port	The protocol port number corresponding to the server, which is 37777 by default.
Username	Server login username and password. The default username is admin. The password is the password that you set when initializing the web client.
Password	

Step 3 Click **OK**.

After the server is added, it will be online automatically. The channel information is also displayed automatically.

Related Operations

- Click + to add more servers.
- To delete a server, click 🗑 corresponding to the server.

4.2.1.2 Logging in to and out of Server

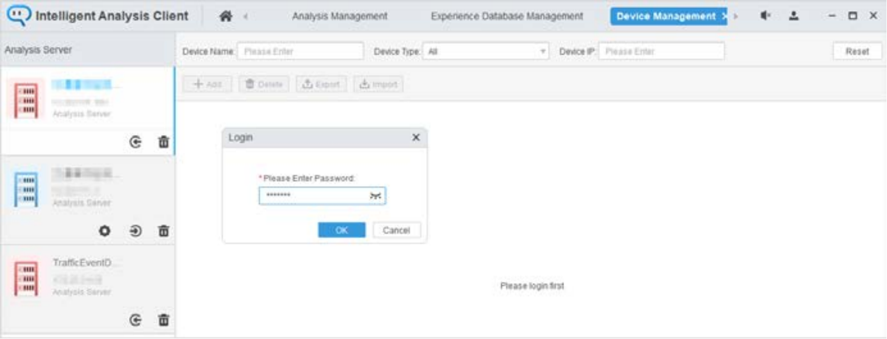
Logging in to the Server

Log in to the server to do live view, send out alarm search and other related operations.

There are two ways to log in.

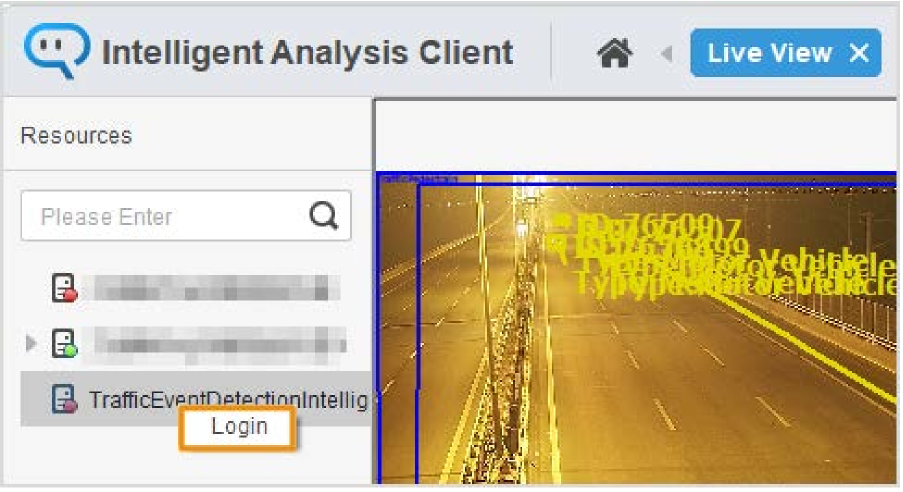
- Open the Client. On the **Device Management** page, select a server, click ⇐, and then enter the password.

Figure 4-2 Log in to the server (1)



- Open the Client. On the **Live View** page, right-click a server, and then click **Login**.

Figure 4-3 Log in to the server (2)

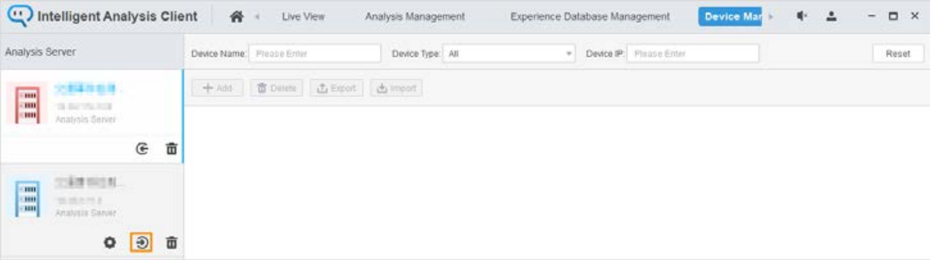


Logging out of the Server

There are two ways to log out:

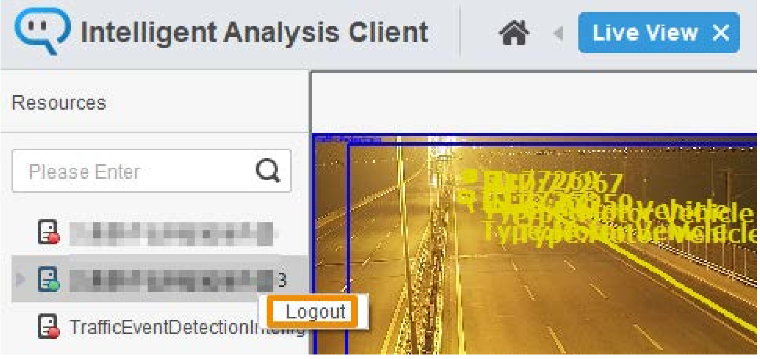
- Open the Client. On the **Device Management** page, select a server, and then click ⇥.

Figure 4-4 Log out of the server (1)



- Open the Client. On the **Live View** page, right-click a server, and then click **Logout**.

Figure 4-5 Log out of the server (2)



4.2.1.3 Setting Detection Mode

Background Information

The Client supports detection in global mode and non-global mode. In global mode, you do not need to draw lane lines and global detection zone, and devices with PTZ functions (such as PTZ camera) are supported. However, global mode consumes more performance than non-global mode. You can select a detection mode as needed.

- Rules supported in non-global mode: parking detection, pedestrian detection, non-motor vehicle detection, traffic jam detection, traffic flow statistics, littering detection, emergency lane occupation detection, illegal lane change detection, wrong-way driving detection, illegal backing detection, construction detection, barrier detection, accident detection, radiation fog detection, smoke detection, fire detection, crossing line detection, speeding detection, driving slow detection, area intrusion, truck detection, and special vehicle detection.
- Rules supported in global mode: parking detection, pedestrian detection, non-motor vehicle detection, traffic jam detection, traffic flow statistics, littering detection, wrong-way driving detection, illegal backing detection, construction detection, barrier detection, accident detection, radiation fog detection, smoke detection, fire detection, and video exception detection.

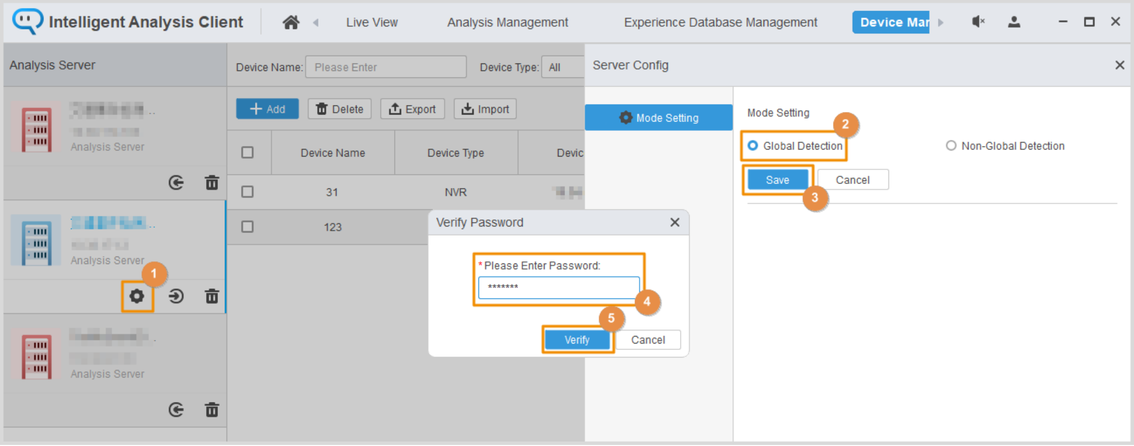
Procedure

Step 1 Open the Client, and then click **Device Management**.

Step 2 Click ⚙ corresponding to a server.

Step 3 Select **Global Detection** or **Non-Global Detection**, click **Save**, and then enter the password for verification.

Figure 4-6 Set the mode



Step 4 Click **Verify**.

Step 5 Click **Yes** in the pop-up window.

4.2.2 Managing Remote Devices

You can add, modify, or delete information from remote devices.

4.2.2.1 Adding Remote Devices and Channels

Add remote devices, such as bullet cameras, PTZ cameras, digital video recorders (DVR), and network video recorders (NVR), to the server to input video data. You can add remote devices either one by one or in batches.

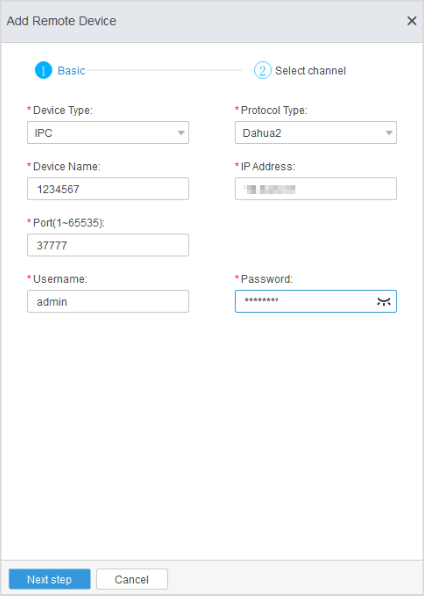
4.2.2.1.1 Adding Remote Devices One by One

Procedure

Step 1 Open the Client. On the **Device Management** page, select a server, and then click **Add**.

Step 2 Enter remote device information, and then click **Next Step**.

Figure 4-7 Add remote device



Add Remote Device

1 Basic — 2 Select channel

*Device Type: IPC

*Protocol Type: Dahua2

*Device Name: 1234567

*IP Address: [redacted]

*Port(1~65535): 37777

*Username: admin

*Password: ********

Table 4-2 Description of parameters for the added remote device

Parameter	Description
Device Type	Supports adding IPC and NVR.
Device Name	Name the remote device on the Client to differentiate it from other remote devices that were added.
Protocol Type	Supports stream media transfer protocols, including Dahua 2, ONVIF, HIKVISION and RTSP protocols. If the RTSP address is a pull stream address provided by the platform address, use the video player software such as VLC software first to test whether pull stream works normally with the address.
IP Address	Remote device IP.
Port	Protocol port number corresponding to the remote device.
Username	Username and password used for logging in to the remote device.
Password	

Step 3 Select channel of the remote devices, and then click **OK**.

Step 4 (Optional) Click **Continue add** to add another remote device.

Related Operations

To delete a remote device, click 🗑 in the **Operation** column, and then click **Yes**. To delete multiple remote devices, select the remote devices, click **Delete** on the top of the channel list, and then click **Yes**.

- When a remote device is deleted, its channels are also deleted.
- You cannot delete remote devices that are configured with analysis tasks.

4.2.2.1.2 Adding Remote Devices in Batches

Procedure

Step 1 Open the Client. On the **Device Management** page, select a server, and then click **Import**.

Step 2 Select the file from local computer.

Adding remote devices in batches will delete current channels and restart the server, please be advised.

Related Operations

On the top of the device list, enter a **Device Name** and select a **Device Type** to search for a remote device. You can also enter a **Device IP** to search for a remote device.

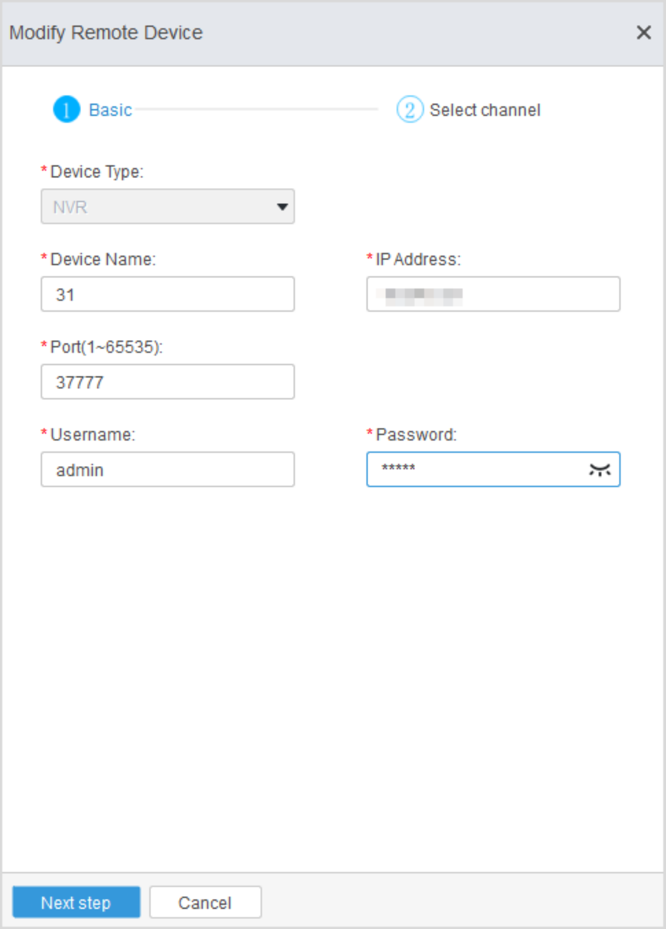
4.2.2.2 Modifying Device and Channel Information

Procedure

Step 1 Open the Client. On the **Device Management** page, select a server and click ✎ in the **Operation** column of a channel.

Step 2 Modify the information of the remote device, enter the password, and then click **Next step**.

Figure 4-8 Modify device information



Modify Remote Device

1 Basic — 2 Select channel

*Device Type: NVR

*Device Name: 31

*IP Address: [redacted]

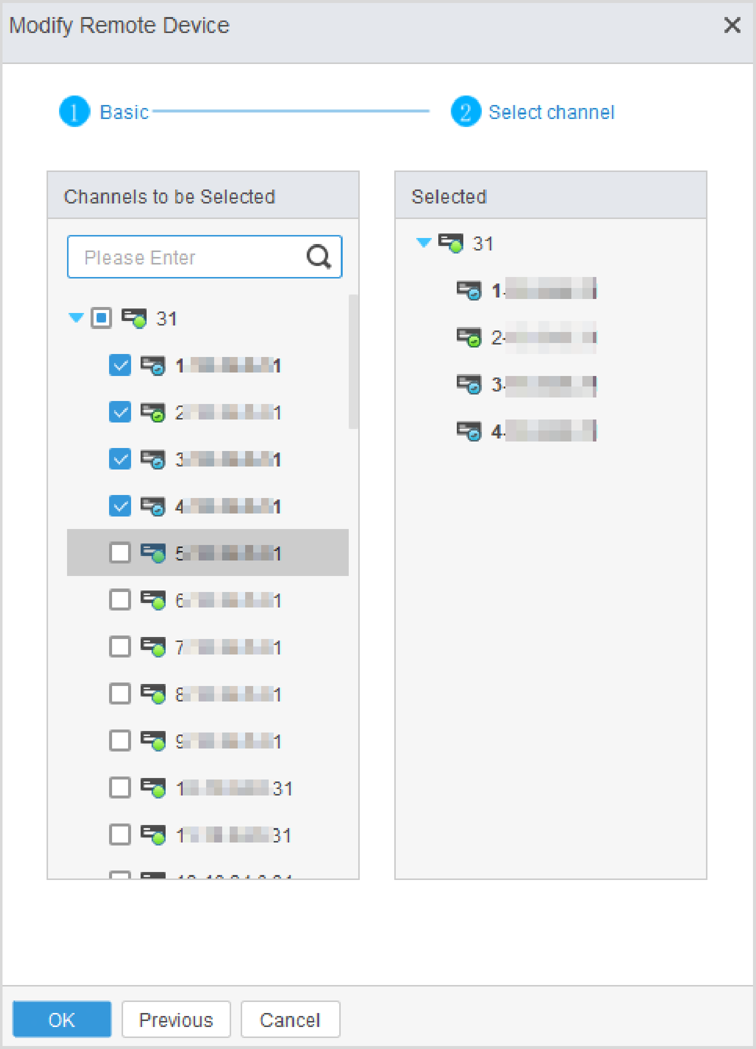
*Port(1~65535): 37777

*Username: admin

*Password: *****

Step 3 Select one or more video channels that you want to add, and then click **OK**.

Figure 4-9 Add channels



indicates that the channel has been configured with rules and cannot be deleted from the list.

4.3 Managing Algorithms

You can create algorithms by combining models exported from other servers with algorithm rules of the traffic event detection server.

4.3.1 Importing Algorithm Models

You can import algorithm packages from your computer. You can also export and delete models, and modify algorithm names.

Prerequisites

You have added a server and logged in to the server. For details, see "4.2.1 Managing Server ".

Procedure

Step 1 Log in to the Client.

Step 2 Select **Algorithm Management** > **Algorithm Model**.

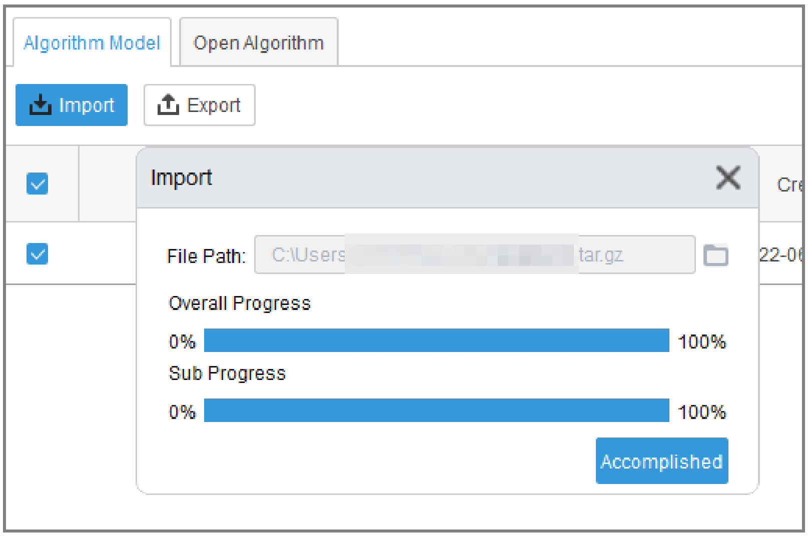
Step 3 Click **Import**.

Step 4 Select the path of the algorithm model that you want to import, and then click **Start**.

Step 5 After the algorithm model is imported, click **Accomplished**.

The list displays the imported algorithm.

Figure 4-10 Import an algorithm model



File Path: C:\Users[redacted]tar.gz

Overall Progress

0% 100%

Sub Progress

0% 100%

Related Operations

- Export the algorithm model: Select an algorithm model and click **Export** to export the algorithm model to your computer.
- Modify algorithm model name: Double-click the name of an algorithm model to modify the name, and then press the Enter key to save the modification.

4.3.2 Creating Open Algorithm

You can create an algorithm by combining an imported algorithm model with the built-in rules of a server.

Prerequisites

You have imported an algorithm model. For details, see "4.3.1 Importing Algorithm Models ".

Procedure

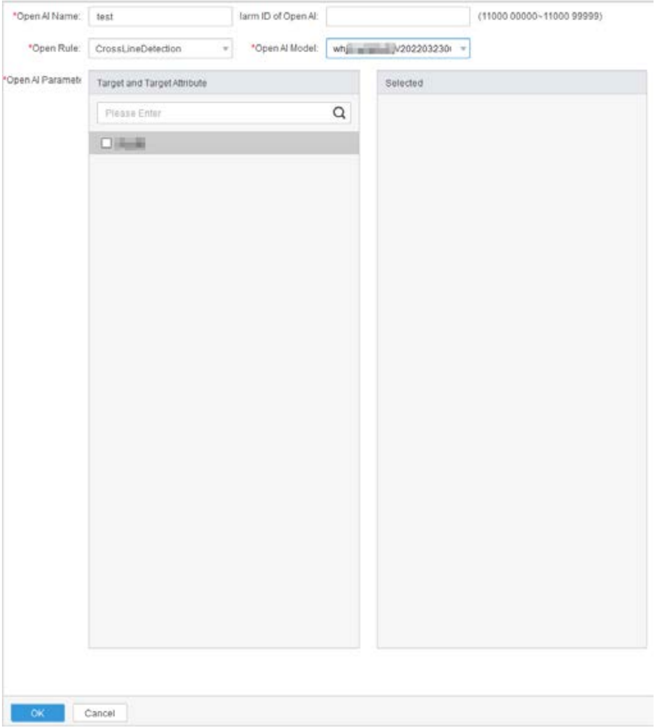
Step 1 Log in to the Client.

Step 2 Select **Algorithm Management** > **Open Algorithm**.

Step 3 Click **Add**.

Step 4 Configure the parameters.

Figure 4-11 Create an algorithm



*Open AI Name: test
larm ID of Open AI: (11000 00000~11000 99999)
*Open Rule: CrossLineDetection
*Open AI Model: wh[redacted]V202203230
*Open AI Paramet

Table 4-3 Parameters of creating algorithms

Parameter	Description
Open AI Name	The name of the algorithm.
Alarm ID of Open AI	The ID of the alarm, which is used to report alarms to supported platforms.
Open Rule	Select a built-in rule, including **CrossLineDetection**, **CrossRegionDetection**, **RegionalStatistics**, and **StayDetection**.
Open AI Model	Select an imported algorithm model.
Open AI Parameters	The targets and target attributes of the selected algorithm model. Select one or more attributes that you need. The selected targets and attributes are displayed on the right-side list.

Step 5 Click **OK**.

The created algorithm is displayed on the list and is enabled by default. The algorithm is also added to **Event Search** and **Analysis Management**.

Related Operations

- Click ⬤ to disable the algorithm.

  - After the algorithm is disabled, you cannot configure rules for the algorithm.
  - If the algorithm is associated with tasks, you must remove the tasks before disabling the algorithm.
- Click ✎ to modify the alarm name and alarm ID.
- Click 🗑 to delete an algorithm. To delete multiple algorithms, select the algorithms and click **Delete** at the top of the list.

4.4 Managing Experience Databases

Add experience databases to reduce false alarms in littering detection,

4.4.1 Adding Experience Databases One by One

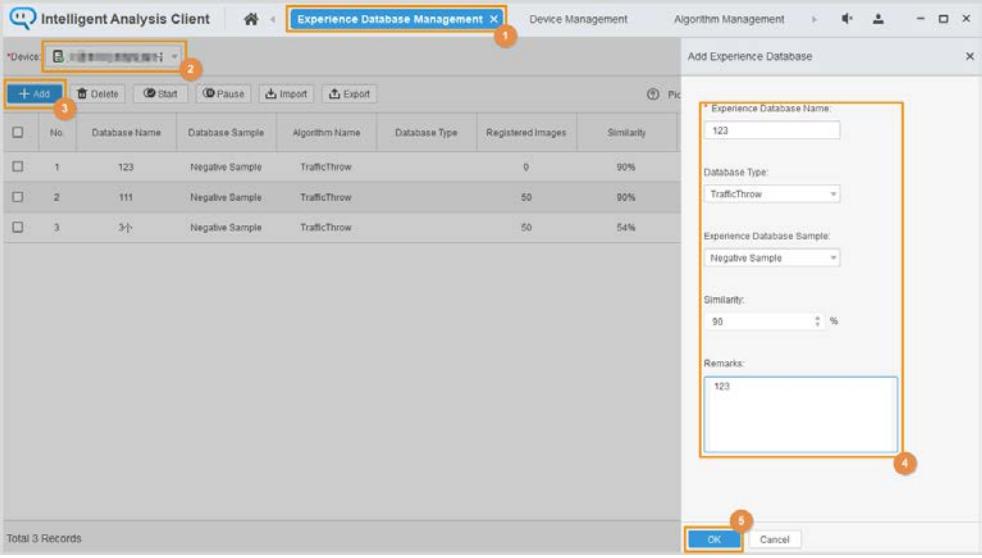
Procedure

Step 1 Log in to the Client.

Step 2 Select **Experience Database Management**.

Step 3 Select a server, and then click **Add**.

Figure 4-12 Add an experience database



*Device: [redacted]

□	No.	Database Name	Database Sample	Algorithm Name	Database Type	Registered Images	Similarity
□	1	123	Negative Sample	TrafficThrow		0	90%
□	2	111	Negative Sample	TrafficThrow		50	90%
□	3	3个	Negative Sample	TrafficThrow		50	54%

* Experience Database Name: 123

Database Type: TrafficThrow

Experience Database Sample: Negative Sample

Similarity: 90 %

Remarks: 123

Step 4 Enter the experience database information, and then click **OK**.

Related Operations

- Click ✎ to edit the corresponding experience database.
- Click 🗑 to delete the corresponding experience database.

4.4.2 Adding Experience Database in Batches

Procedure

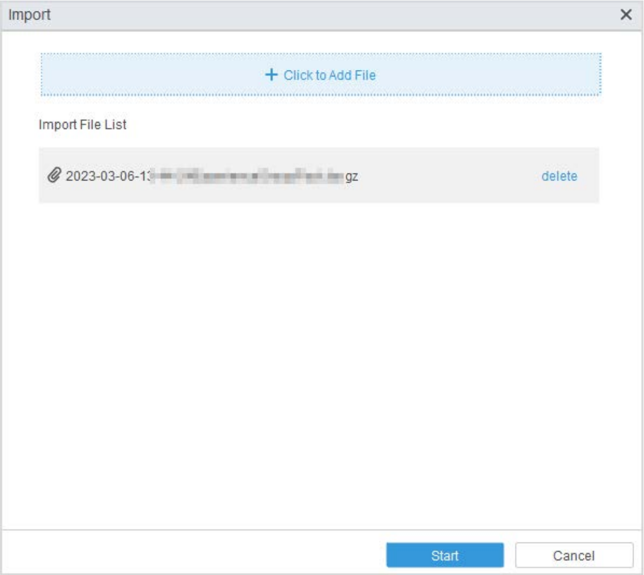
Step 1 Log in to the Client.

Step 2 Select **Experience Database Management**.

Step 3 Select a server, and then click **Import**.

Step 4 Click **Click to Add File** to upload the file from your local computer, and then click **Start**.

Figure 4-13 Add experience databases in bathes



Step 5 After you upload the file, click **Accomplished**.

Related Operations

- Click ✎ to edit the corresponding experience database.
- Click 🗑 to delete the corresponding experience database.

4.5 Managing Intelligent Analysis Tasks

You can add intelligent analysis tasks of the traffic event detection server and configure rules as needed. When an event that matches the configured rules occurs, the system sends an alarm.

4.5.1 Adding Channels

After adding channels, you can source channels from the added channels under rule detection.

Prerequisites

You have added a server in the client and bind a remote device. For details, see "4.2 Managing Server and Remote Devices".

4.5.1.1 Adding Channels One by One

Procedure

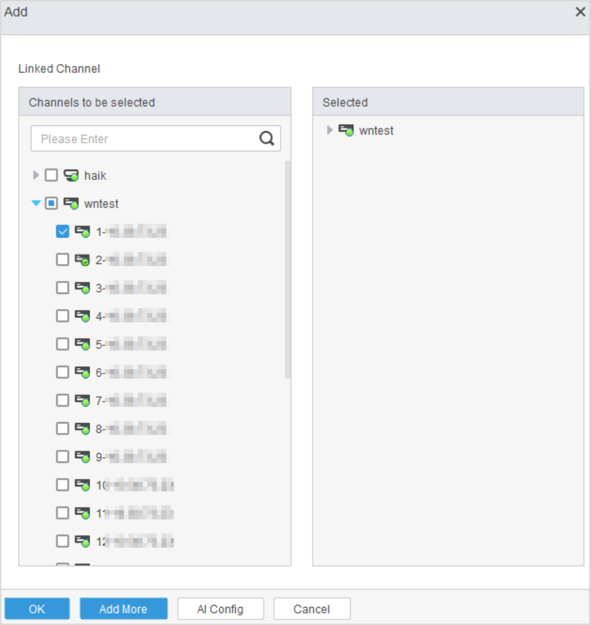
Step 1 Log in to the Client.

Step 2 Click **Analysis Management**, select a server, and then click **Add**.

Step 3 Select a video source channel from **Channels to be Selected**, and then click **AI Config** to go to the **Rule Config** page.

Only one channel can be selected.

Figure 4-14 Add a channel



4.5.1.2 Adding Channels in Batches

Procedure

Step 1 Log in to the Client.

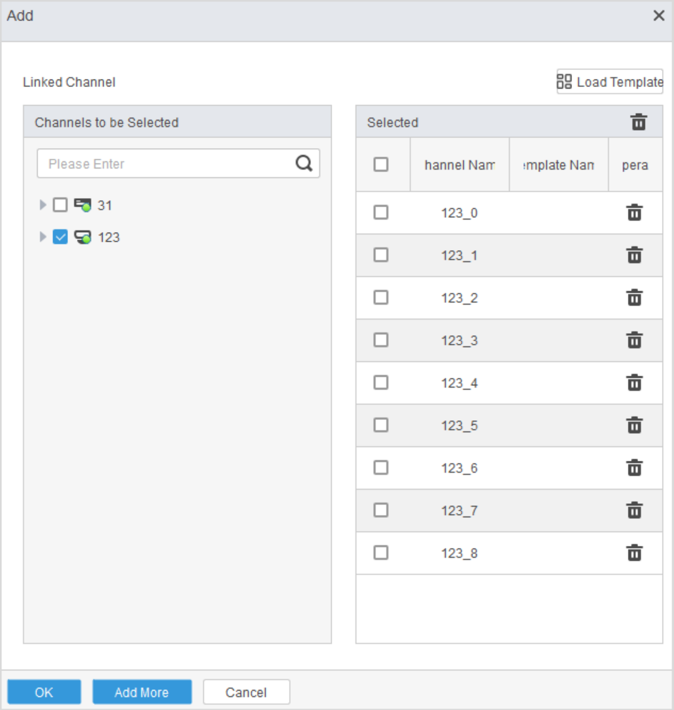
Step 2 Click **Analysis Management**, select a server, and then click **Batch Add**.

Step 3 Select multiple channels from **Channels to be Selected**.

- The selected channels appear in **Selected**.
- Clear channels on the left-side list or click 🗑 in the right-side list to clear channels.

Step 4 Click **OK** to finish adding or click **Add More** to repeat Step 3.

Figure 4-15 Add channels in batches



☐	hannel Nam	mplate Nan	pera
☐	123_0		🗑
☐	123_1		🗑
☐	123_2		🗑
☐	123_3		🗑
☐	123_4		🗑
☐	123_5		🗑
☐	123_6		🗑
☐	123_7		🗑
☐	123_8		🗑

Related Operations

- To start analysis in batches, select multiple channels and click **Start**.
- To pause analysis in batches, select multiple channels and click **Pause**.
- To delete channels in batches, select multiple channels and click **Delete**.
- Enter a channel name in **Channel Name** to search for a channel.
- Select algorithms from **Algorithm Name** to filter channels.
- Click to view the configuration of a task.
- In global mode, click to switch to non-global mode.

4.5.2 Configuring Rules

On the **Rule Config** page, configure smart rules for selected video channels. When a target violates the rules, the system automatically sends an alarm.

You can configure multiple IVS rules for a channel. However, you cannot configure IVS rules and open rules for a channel at the same time.

Prerequisites

You have selected channels for configuring rules. For details, see " 4.5.1 Adding Channels".

4.5.2.1 Parking Detection

An alarm will be triggered when the duration of a vehicle parking on the expressway exceeds the defined value. When a traffic jam occurs or vehicles move slowly, parking alarm will not be triggered.

Procedure

Step 1 On the **Rule Config** page, select **Parking Detection** from the **Rule Config** drop-down list.

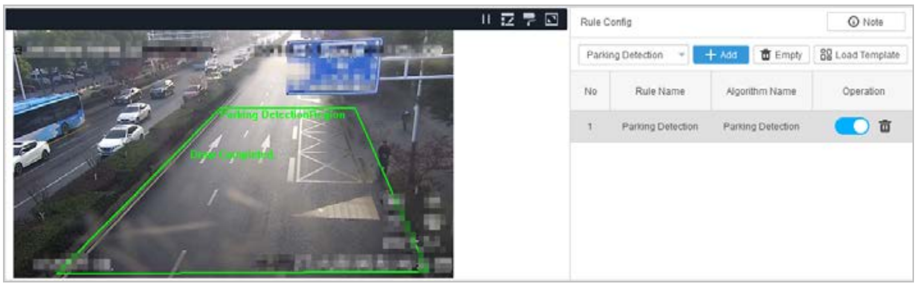
Step 2 Click **Add**.

After you add a rule, the rule is enabled by default.

Step 3 Drag the angles to adjust the detection zone or click to draw a detection zone.

- The detection zone should cover the valid vehicle targets, and avoid being too large to be interfered from other objects.
- Click the screen to start drawing, and right-click the screen to finish drawing.
- By default, the detection zone covers the whole image.

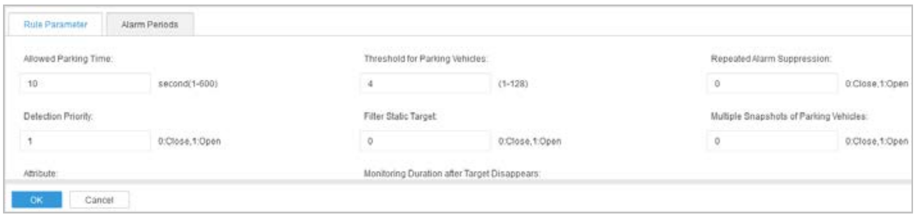
Figure 4-16 Parking detection



No	Rule Name	Algorithm Name	Operation
1	Parking Detection	Parking Detection	

Step 4 Configure parameters on the **Rule Parameter** tab.

Figure 4-17 Parking detection parameters



Allowed Parking Time: 10 second(1-600)

Threshold for Parking Vehicles: 4 (1-128)

Repeated Alarm Suppression: 0 0:Close,1:Open

Detection Priority: 1 0:Close,1:Open

Filter Static Target: 0 0:Close,1:Open

Multiple Snapshots of Parking Vehicles: 0 0:Close,1:Open

Attribute:

Monitoring Duration after Target Disappears:

Table 4-4 Description of parking detection parameters

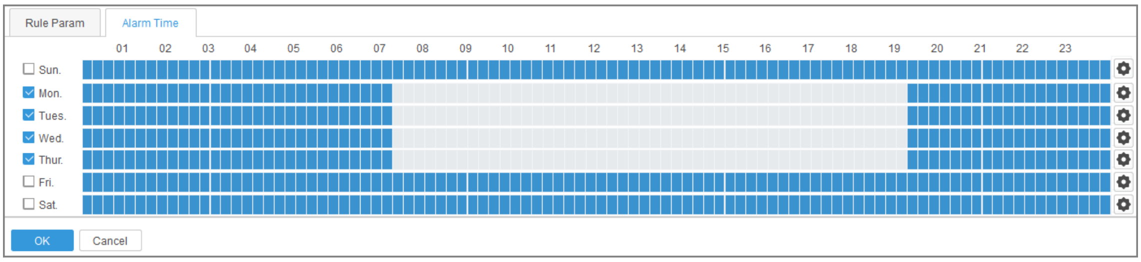
Parameter	Description
Allowed Parking Time	An alarm is triggered when the parking duration exceeds the specified value. A shorter duration means that more targets can be captured. However, the false alarm rate increases at the same time. To filter out more invalid targets, we recommend you set the value to 10 s.
Threshold for Parking Vehicles	The maximum number of parking alarms that can be triggered. Parking events are no longer reported if the number of triggered alarms reaches the defined value.
Repeated Alarm Suppression	If you enable this function, repeated alarms are avoided. We recommend you enable this function.
Detection Priority	If you enable this function, the number of alarm failures caused by ID change is reduced.
Filter Static Target	If you enable this function, only moving vehicles can be captured. Otherwise, both moving and static vehicles can be captured.
Multiple Snapshots of Parking Vehicles	If you enable this function, a vehicle is captured multiple times if it parks a specified parking area multiple times. Otherwise, the vehicle is captured only once no matter how many times it parks.
Attribute	You can choose **General Vehicle**, **Police Car** or **Engineering Rescue Vehicles** as the objects.
Monitoring Duration after Target Disappears	The event ends when the disappearing duration of the object reaches the defined time.

Step 5 Configure the alarm time.

1. Click the **Alarm Periods** tab.
2. Select an alarm time by using one of the following methods:
    - Click ⚙ corresponding to a date and then add or modify an alarm time period.
    - On the **Alarm Periods** tab, left-click the screen and move the mouse to the left. Then, the pointer becomes an eraser and the time period is decreased. To increase a time period, left-click the screen and move the mouse to the right.

- By default, parking alarm is enabled all day. You can modify the alarm time as needed.
- After you select multiple dates, you only need to modify the alarm time period for a date. The alarm time of other dates is updated at the same time.
- You can configure 9 time periods at most for a day.

Figure 4-18 Configure the alarm time



☐ Sun.
☑ Mon.
☑ Tues.
☑ Wed.
☑ Thur.
☐ Fri.
☐ Sat.

Step 6 Click **OK**.

The configuration is saved and applied, and the **Rule Config** page is closed.

Related Operations

- Click **Empty** to clear all configured rules.
- Click **Load Template**, select a template, and then click **OK**. Rule parameters are configured based on the template.

4.5.2.2 Pedestrian Detection

An alarm will be triggered when a pedestrian appears in the detection zone and stays longer than the defined time.

Procedure

Step 1 On the **Rule Config** page, select **Pedestrian Detection** from the **Rule Config** drop-down list.

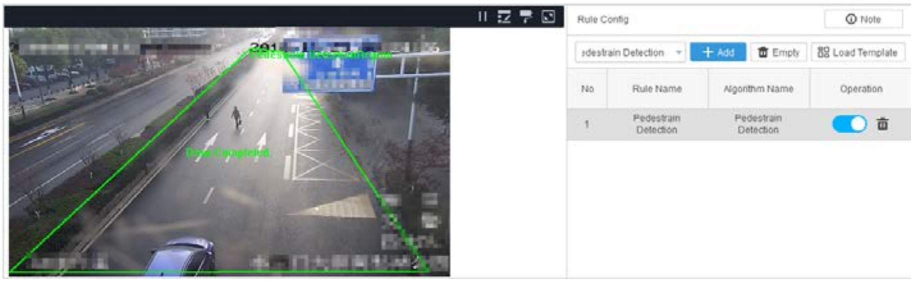
Step 2 Click **Add**.

After you add a rule, the rule is enabled by default.

Step 3 Drag the angles to adjust the detection zone or click ▨ to draw a detection zone.

- The detection zone should cover the valid vehicle targets, and avoid being too large to be interfered from other objects.
- Click the screen to start drawing, and right-click the screen to finish drawing.
- By default, the detection zone covers the whole image.

Figure 4-19 Pedestrian detection

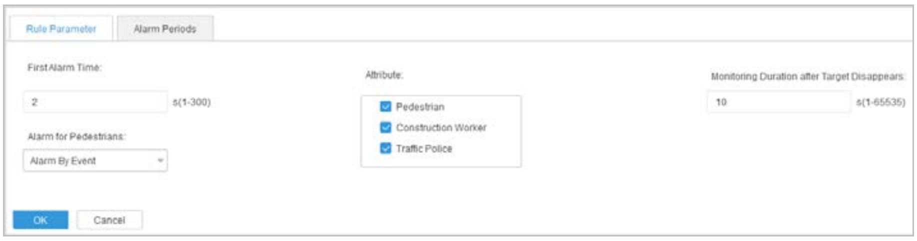


Rule Config

No	Rule Name	Algorithm Name	Operation
1	Pedestrain Detection	Pedestrain Detection	

Step 4 Click **Rule Parameter**, and then configure **Alarm Periods**.

Figure 4-20 Pedestrian detection parameters



First Alarm Time: 2 s(1-300)

Alarm for Pedestrians: Alarm By Event

Attribute:

- ☑ Pedestrian
- ☑ Construction Worker
- ☑ Traffic Police

Monitoring Duration after Target Disappears: 10 s(1-65535)

Table 4-5 Description of pedestrian detection parameters

Parameter	Description
First Alarm Time	An alarm will be triggered when a pedestrian appears in the detection zone and stays longer than the defined time.
Attribute	You can select **Pedestrian**, **Construction Worker** or **Traffic Police** from the list.
Monitoring Duration after Target Disappears	The event ends when the disappearing duration of the object reaches the defined time.
Alarm for Pedestrians	You can select **Alarm by Event** or **Alarm by Target** from the drop down list as the alert type.

Step 5 Configure **Alarm Periods**. For details, see Step5 in "4.5.2.1 Parking Detection".

Step 6 Click **OK**.

The configuration is saved and applied, and the **Rule Config** page is closed.

Related Operations

- Click **Empty** to clear all configured rules.
- Click **Load Template**, select a template, and then click **OK**. Rule parameters are configured based on the template.

4.5.2.3 Non-motor Vehicle Detection

An alarm will be triggered when non-motor vehicles, such as electric mopeds and trishaws, are driving in vehicle lane for longer than the defined value.

Procedure

Step 1 On the **Rule Config** page, select **Non-motor Vehicle Detection** from the **Rule Config** drop-down list.

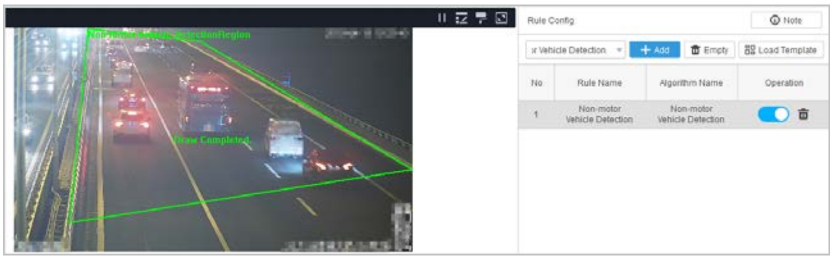
Step 2 Click **Add**.

After you add a rule, the rule is enabled by default.

Step 3 By default, the detection zone covers the whole image. Drag the angles to adjust the detection zone or click to draw a detection zone. (Click the screen to start drawing, and right-click the screen to finish drawing.)

- The detection zone should cover the valid vehicle targets, and avoid being too large to be interfered from other objects.
- Click the screen to start drawing, and right-click the screen to finish drawing.
- The detection zone covers the whole image by default.

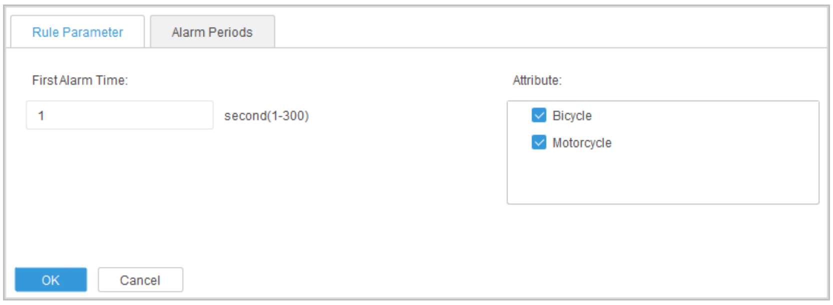
Figure 4-21 Non-motor vehicle detection



No	Rule Name	Algorithm Name	Operation
1	Non-motor Vehicle Detection	Non-motor Vehicle Detection	

Step 4 Click the **Rule Parameter** to configure the parameters.

Figure 4-22 Non-motor vehicle detection parameters



First Alarm Time: 1 second(1-300)

Attribute:
☑ Bicycle
☑ Motorcycle

Table 4-6 Description of non-motor vehicle detection parameters

Parameter	Description
First Alarm Time	An alarm will be triggered when a non-motor vehicle appears in the detection zone and stays longer than the defined time.
Attribute	You can select **Bicycle**, **Motorcycle** as the objects.

Step 5 Configure **Alarm Periods**. For details, see Step5 in "4.5.2.1 Parking Detection".

Step 6 Click **OK**.

The configuration is saved and applied, and the **Rule Config** page is closed.

Related Operations

- Click **Empty** to clear all configured rules.
- Click **Load Template**, select a template, and then click **OK**. Rule parameters are configured based

on the template.

4.5.2.4 Congestion Detection

An alarm will be triggered when the number of vehicles parking in the lane and the jam proportion exceeds the defined values.

Procedure

Step 1 On the **Rule Config** page, select **Congestion Detection** from the **Rule Config** drop-down list.

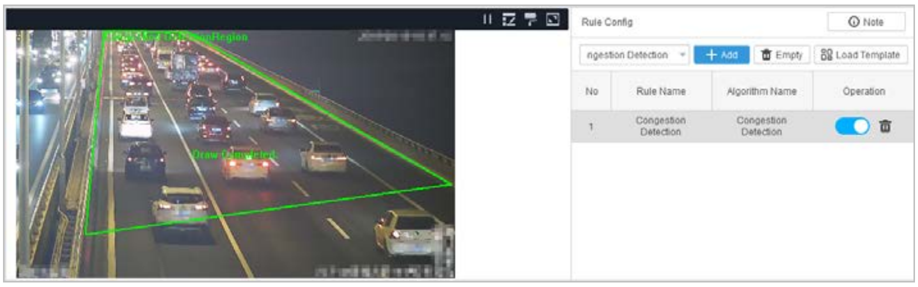
Step 2 Click **Add**.

After you add a rule, the rule is enabled by default.

Step 3 Drag the angles to adjust the detection zone or click ▣ to draw a detection zone.

- The detection zone should cover the valid vehicle targets, and avoid being too large to be interfered from other objects.
- Click the screen to start drawing, and right-click the screen to finish drawing.
- The detection zone covers the whole image by default.

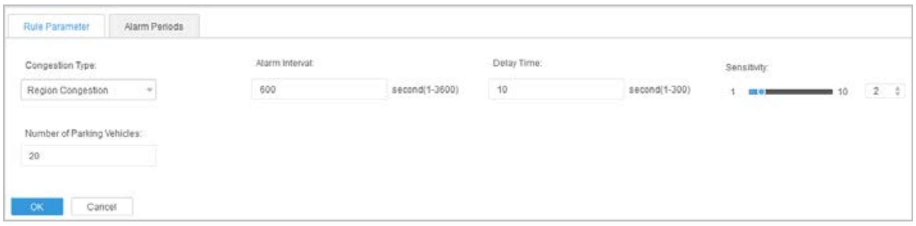
Figure 4-23 Congestion detection



No	Rule Name	Algorithm Name	Operation
1	Congestion Detection	Congestion Detection	● 🗑

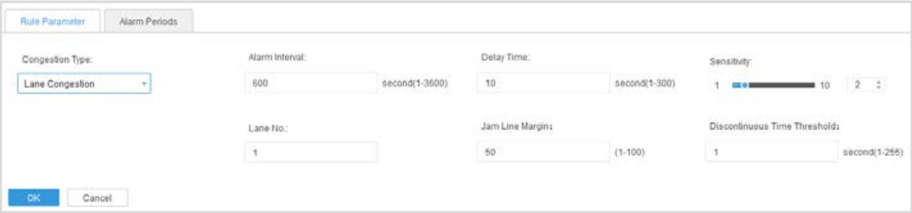
Step 4 Click **Rule Parameter**, and then configure the parameters.

Figure 4-24 Region congestion detection parameters



Congestion Type: Region Congestion
Alarm Interval: 600 second(1-3600)
Delay Time: 10 second(1-300)
Sensitivity: 1 — 10 2
Number of Parking Vehicles: 20

Figure 4-25 Lane congestion detection parameters



Congestion Type: Lane Congestion
Alarm Interval: 600 second(1-3600)
Delay Time: 10 second(1-300)
Sensitivity: 1 — 10 2
Lane No.: 1
Jam Line Margin: 50 (1-100)
Discontinuous Time Threshold: 1 second(1-255)

Table 4-7 Description of congestion detection parameters

Parameter	Description
Congestion Type	The congestion type. Valid values: **Region Congestion** and **Lane Congestion**.
Alarm Interval	Interval between the time of alarming after traffic congestion is detected and the time to report it. If alarms are triggered continuously within the defined interval, the alarm information is reported only once.
Delay Time	An alarm will be triggered when the duration exceeds the defined value.
Sensitivity	The higher the sensitivity is, the more easily an alarm is detected and triggered. The false alarm rate also increases. We recommend you to leave it as default.
Number of Parking Vehicles	An alarm will be triggered when the number of vehicles exceeds the defined value.
Lane No.	If no lane is drawn, enter the lane number for traffic congestion detection.
Jam Line Margin	Traffic congestion occurs when the congestion proportion exceeds the defined value. An alarm will be triggered when both the first and second congestion conditions are met. ● First congestion condition: The ratio of the vehicle queue length and the detection lane length exceed the congestion proportion. ● Second congestion condition: The vehicle drive at a speed of nearly zero. 📖 In consideration of traffic congestion detection validity and the interference of parking event, 50% is recommended.
Discontinuous Time Threshold	The difference between the last congestion time and the current congestion time, namely, the unblocked time. If the unblocked time exceeds this defined value, there is no congestion and the number of alarms is cleared.

Step 5 Configure **Alarm Periods**. For details, see Step5 in "4.5.2.1 Parking Detection".

Step 6 Click **OK**.

The configuration is saved and applied, and the **Rule Config** page is closed.

Related Operations

- Click **Empty** to clear all configured rules.
- Click **Load Template**, select a template, and then click **OK**. Rule parameters are configured based on the template.

4.5.2.5 Littering Detection

An alarm will be triggered when a litter is detected in the detection zone for longer than the defined value.

Procedure

Step 1 On the **Rule Config** page, select **Littering Detecion** from the **Rule Config** drop-down list.

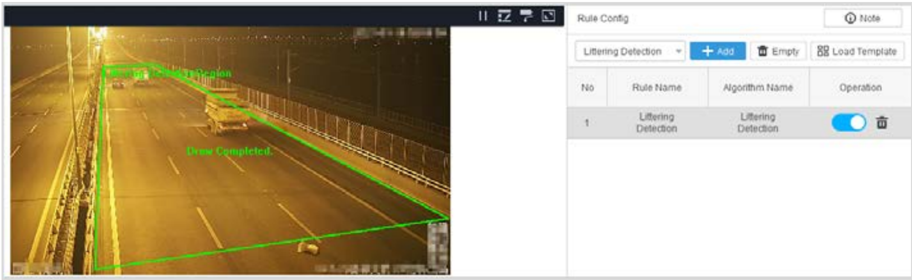
Step 2 Click **Add**.

After you add a rule, the rule is enabled by default.

Step 3 Drag the angles to adjust the detection zone or click to draw a detection zone.

- The detection zone should cover the valid vehicle targets, and avoid being too large to be interfered from other objects.
- Click the screen to start drawing, and right-click the screen to finish drawing.
- By default, the detection zone covers the whole image.

Figure 4-26 Littering detection

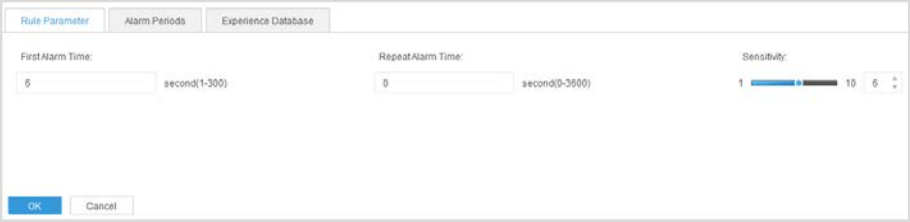


No	Rule Name	Algorithm Name	Operation
1	Littering Detection	Littering Detection	

Step 4 Click **Rule Parameter**, and then configure the parameters.

- **First Alarm Time**: An alarm will be triggered when litter appears in the detection zone and stays longer than the defined time.
- **Repeat Alarm Time**: If litter continuously appears within the set time, the alarm is triggered only once.
- **Sensitivity**: The higher the sensitivity is, the more easily an alarm is detected and triggered. The false alarm rate also increases. We recommend you to leave it as default.

Figure 4-27 Littering detection parameters



First Alarm Time: 6 second(1-300)

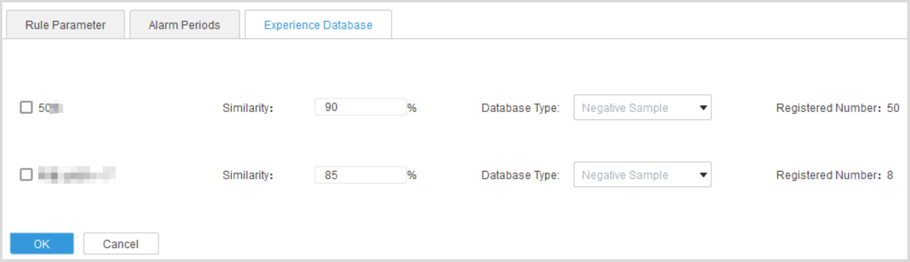
Repeat Alarm Time: 0 second(0-3600)

Sensitivity: 1 10 6

Step 5 Configure **Alarm Periods**. For details, see Step5 in "4.5.2.1 Parking Detection".

Step 6 Click **Experience Database** to configure the experience database of traffic flow detection.

Figure 4-28 Configure experience database



☐ 50[redacted] Similarity: 90 % Database Type: Negative Sample Registered Number: 50

☐ [redacted] Similarity: 85 % Database Type: Negative Sample Registered Number: 8

- **Similarity**: When the similarity between detection targets and negative sample reaches the defined value, the alarm will not be triggered; An alarm will be triggered when the similarity between detection targets and the negative sample does not reach the defined value.

- **Registered Number**: The total number of the negative sample.

Step 7 Click **OK**.

The configuration is saved and applied, and the **Rule Config** page is closed.

Related Operations

- Click **Empty** to clear all configured rules.
- Click **Load Template**, select a template, and then click **OK**. Rule parameters are configured based on the template.

4.5.2.6 Emergency Lane Occupation Detection

An alarm will be triggered when a vehicle occupies the emergency lane.

Procedure

Step 1 On the **Rule Config** page, select **Driving in Emergency Lane** from the **Rule Config** drop-down list.

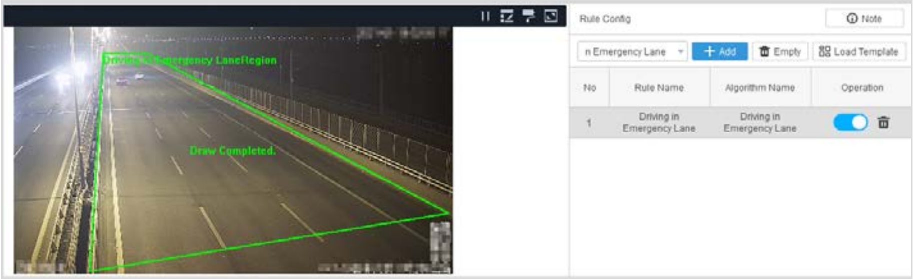
Step 2 Click **Add**.

After you add a rule, the rule is enabled by default.

Step 3 Drag the angles to adjust the detection zone or click ☑ to draw a detection zone.

- The detection zone should cover the valid vehicle targets, and avoid being too large to be interfered from other objects.
- Click the screen to start drawing, and right-click the screen to finish drawing.
- By default, the detection zone covers the whole image.

Figure 4-29 Emergency lane occupation detection

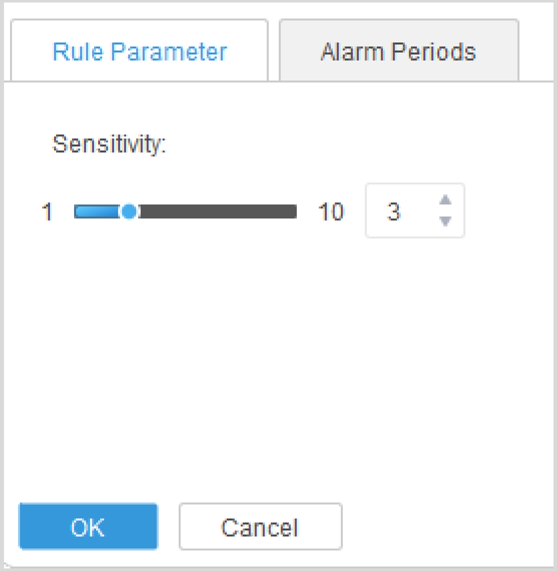


No	Rule Name	Algorithm Name	Operation
1	Driving in Emergency Lane	Driving in Emergency Lane	

Step 4 Click the **Rule Parameter** tab, and then set the sensitivity.

The higher the sensitivity is, the easier an alarm is detected and triggered. The false alarm rate also increases. We recommend you to leave it as default.

Figure 4-30 Parameter of emergency lane occupation detection



Sensitivity: 1–10: 3

Step 5 Configure **Alarm Periods**. For details, see Step5 in "4.5.2.1 Parking Detection".

Step 6 Click **OK**.

The configuration is saved and applied, and the **Rule Parameter** page is closed.

Related Operations

- Click **Empty** to clear all configured rules.
- Click **Load Template**, select a template, and then click **OK**. Rule parameters are configured based on the template.

4.5.2.7 Illegal Lane Change Detection

An alarm will be triggered when a vehicle passing the lane line (white solid line or yellow solid line) is detected.

Prerequisites

The scene has at least 2 lanes, and you have drawn at least 2 lane lines.

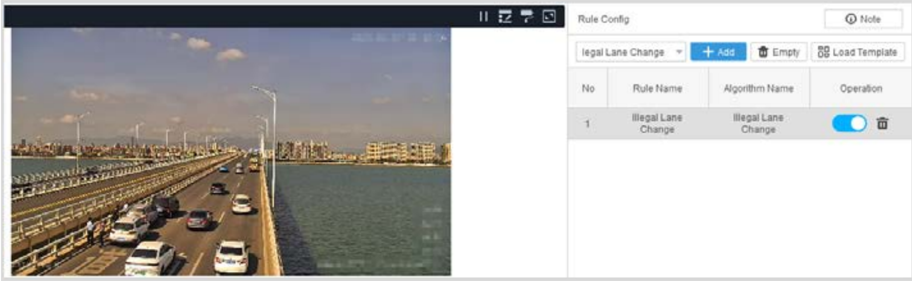
Procedure

Step 1 On the **Rule Config** page, select **illegal Lane Change** from the **Rule Config** drop-down list.

Step 2 Click **Add**.

After you add a rule, the rule is enabled by default.

Figure 4-31 Illegal lane change detection

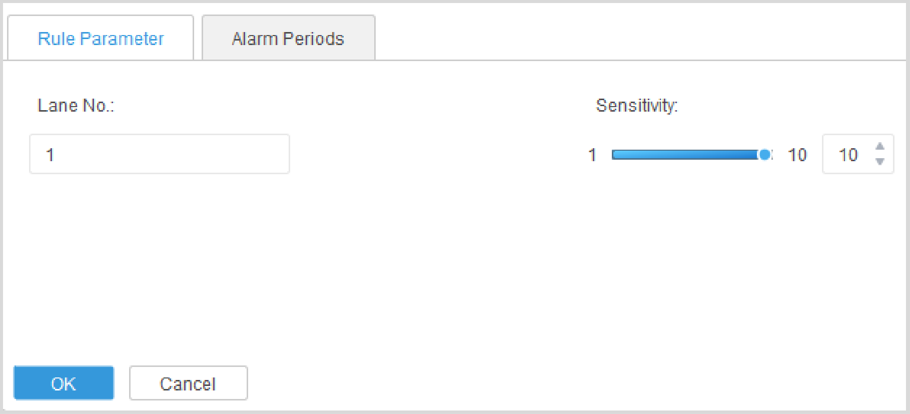


No	Rule Name	Algorithm Name	Operation
1	Illegal Lane Change	Illegal Lane Change	

Step 3 Click **Rule Parameter**, and then configure the parameters.

- **Lane No**: Enter the number of the lane that you want to detect.
- **Sensitivity**: The higher the sensitivity is, the more easily an alarm is detected and triggered. The false alarm rate also increases. We recommend you to leave it as default.

Figure 4-32 Parameters of illegal lane change detection



Lane No.: 1

Sensitivity: 10

Step 4 Configure **Alarm Periods**. For details, see Step5 in "4.5.2.1 Parking Detection".

Step 5 Click **OK**.

The configuration is saved and applied, and the **Rule Config** page is closed.

Related Operations

- Click **Empty** to clear all configured rules.
- Click **Load Template**, select a template, and then click **OK**. Rule parameters are configured based on the template.

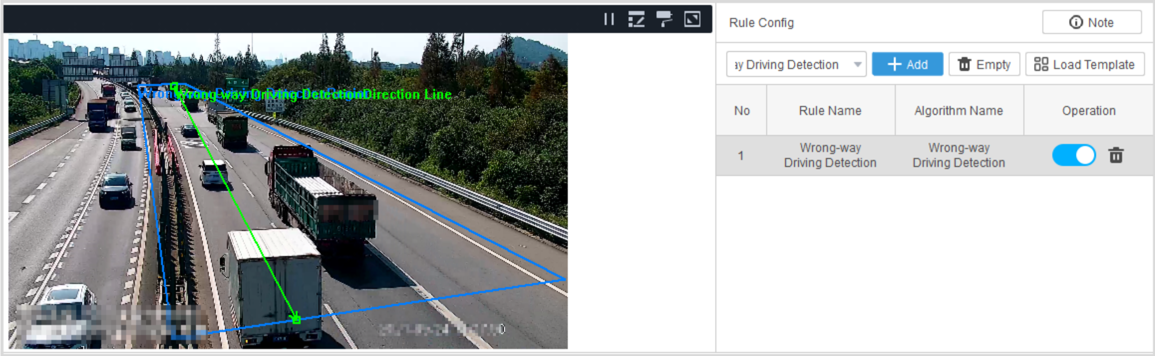
4.5.2.8 Wrong-Way Driving Detection

Procedure

Step 1 On the **Rule Config** page, select **Wrong-way Driving Detection** from the **Rule Config** drop-down list.

Step 2 Click **Add**.

Figure 4-33 Wrong-way driving detection



Rule Config

ⓘ Note

ay Driving Detection ▾ | + Add | Empty | Load Template

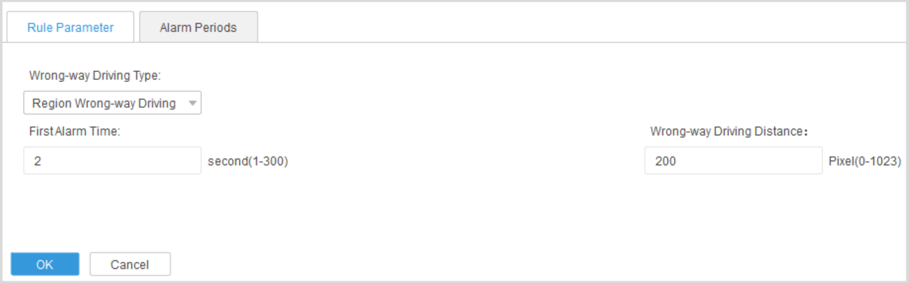
No	Rule Name	Algorithm Name	Operation
1	Wrong-way Driving Detection	Wrong-way Driving Detection	●

After you add a rule, the rule is enabled by default.

Step 3 Click **Rule Config**, and then configure the parameters.

- **Wrong-way Driving Type**: Select **Region Wrong-way Driving** or **Lane Wrong-way Driving**. For **Region Wrong-way Driving**, you need to draw the detection zone and direction line, see Step 4.
- **Wrong-way Driving Distance**: An alarm will be triggered when a vehicle drives in the wrong way for a distance that is longer than the defined pixels.
- **Lane No**: Enter a lane number if you select **Lane Retrograde**.
- **First Alarm Time**: An alarm is triggered when a vehicle drives in the wrong way.

Figure 4-34 Region wrong-way driving parameters



Rule Parameter | Alarm Periods

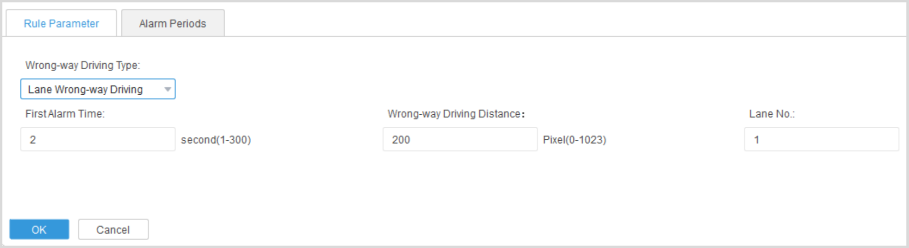
Wrong-way Driving Type:
Region Wrong-way Driving ▾

First Alarm Time: 2 second(1-300)

Wrong-way Driving Distance: 200 Pixel(0-1023)

OK | Cancel

Figure 4-35 Lane retrograde parameters



Rule Parameter | Alarm Periods

Wrong-way Driving Type:
Lane Wrong-way Driving ▾

First Alarm Time: 2 second(1-300)

Wrong-way Driving Distance: 200 Pixel(0-1023)

Lane No.: 1

OK | Cancel

Step 4 For **Region Wrong-way Driving**, you need to draw the detection zone and direction line.

- The detection zone covers the whole image by default. Drag the angles to adjust the detection zone or click ▨ to draw a detection zone. (Click the screen to start drawing, and right-click the screen to finish drawing.)
- Drag the endpoint of the direction line to adjust the direction line.

The detection zone should cover the valid vehicle targets, and avoid being too large to be interfered from other objects.

Step 5 Configure **Alarm Periods**. For details, see Step5 in "4.5.2.1 Parking Detection".

Step 6 Click **OK**.

The configuration is saved and applied, and the **Rule Config** page is closed.

Related Operations

- Click **Empty** to clear all configured rules.
- Click **Load Template**, select a template, and then click **OK**. Rule parameters are configured based on the template.

4.5.2.9 Illegal Backing Detection

When a vehicle is backing and the backing time exceeds the defined value, an alarm will be triggered. For example, a vehicle is backing on the highway.

Procedure

Step 1 On the **Rule Config** page, select **Backing Detection** from the **Rule Config** drop-down list.

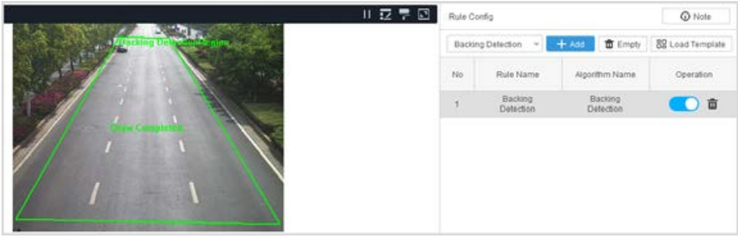
Step 2 Click **Add**.

After you add a rule, the rule is enabled by default.

Step 3 Drag the angles to adjust the detection zone or click ☑ to draw a detection zone.

- By default, the detection zone covers the whole image.
- Click the screen to start drawing, and right-click the screen to finish drawing.
- The detection zone should cover the valid vehicle targets, and avoid being too large to be interfered from other objects.

Figure 4-36 Illegal backing detection

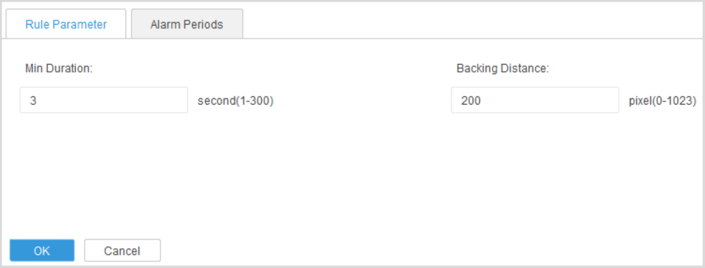


No	Rule Name	Algorithm Name	Operation
1	Backing Detection	Backing Detection	

Step 4 Click **Rule Parameter**, and then configure the parameters.

- **Min Duration**: An alarm will be triggered when the backing time of a vehicle exceeds the defined time.
- **Backing Distance**: An alarm will be triggered when a vehicle backs off for a distance that is longer than the set pixels.

Figure 4-37 Illegal backing detection parameters



Min Duration: 3 second(1-300)

Backing Distance: 200 pixel(0-1023)

Step 5 Configure **Alarm Periods**. For details, see Step5 in "4.5.2.1 Parking Detection".

Step 6 Click **OK**.

The configuration is saved and applied, and the **Rule Config** page is closed.

Related Operations

- Click **Empty** to clear all configured rules.
- Click **Load Template**, select a template, and then click **OK**. Rule parameters are configured based on the template.

4.5.2.10 Construction Detection

When a construction sign is detected and it stays longer than the defined value, the road section is identified as a construction zone and an alarm will be triggered.

Procedure

Step 1 On the **Rule Config** page, select **Construction Detection** from the **Rule Config** drop-down list.

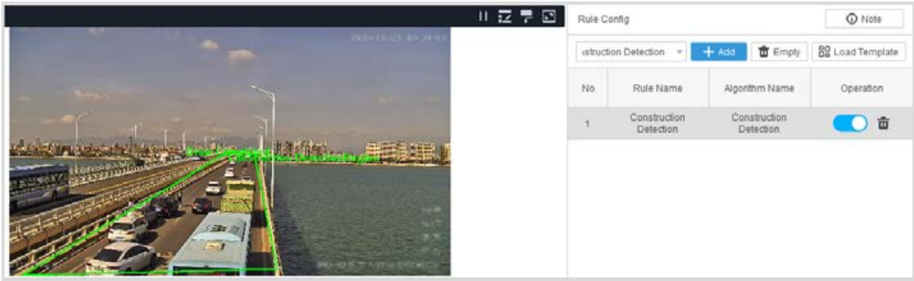
Step 2 Click **Add**.

After you add a rule, the rule is enabled by default.

Step 3 Drag the angles to adjust the detection zone or click ▣ to draw a detection zone.

- The detection zone should cover the valid vehicle targets, and avoid being too large to be interfered from other objects.
- Click the screen to start drawing, and right-click the screen to finish drawing.
- By default, the detection zone covers the whole image.

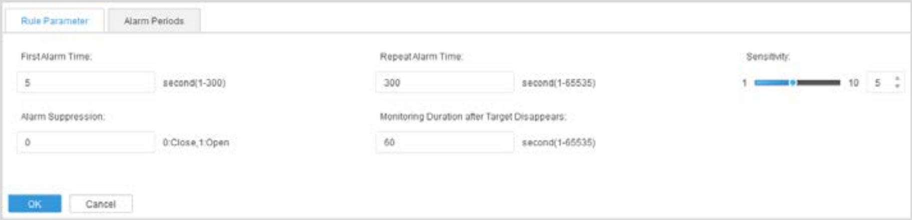
Figure 4-38 Construction detection



No	Rule Name	Algorithm Name	Operation
1	Construction Detection	Construction Detection	

Step 4 Click **Rule Parameter**, and then configure the parameters.

Figure 4-39 Construction detection parameters



First Alarm Time: 5 second(1-300)

Repeat Alarm Time: 300 second(1-65535)

Sensitivity: 1 10 5

Alarm Suppression: 0 0:Close,1:Open

Monitoring Duration after Target Disappears: 60 second(1-65535)

Table 4-8 Description of construction detection parameters

Parameter	Description
First Alarm Time	An alarm will be triggered when the construction sign stays longer than the defined time.
Repeat Alarm Time	The interval between 2 alarms. If alarms are triggered continuously within the defined interval, the alarm will only be reported once. If the event is removed, alarm details contain 3 alarm images, which are the image of first trigger, the image within the repeated alarm interval, and the image when the event is removed.
Alarm Suppression	Repeated alarm takes effect when this function is disabled. ● 0: disabled. ● 1: enabled.
Monitoring Duration after Target Disappears	The event ends when the disappearing duration of the object reaches the defined time.
Sensitivity	The higher the sensitivity is, the easier it is to detect and trigger an alarm. The false alarm rate also increases. We recommend you leave it as default.

Step 5 Configure **Alarm Periods**. For details, see Step5 in "4.5.2.1 Parking Detection".

Step 6 Click **OK**.

The configuration is saved and applied, and the **Rule Config** page is closed.

Related Operations

- Click **Empty** to clear all configured rules.
- Click **Load Template**, select a template, and then click **OK**. Rule parameters are configured based on the template.

4.5.2.11 Barrier Detection

An alarm will be triggered when a barrier, such as a box, stays in the detection area for longer than the defined value.

Procedure

Step 1 On the **Rule Config** page, select **Road Obstacle Detection** from the **Rule Config** drop-down list.

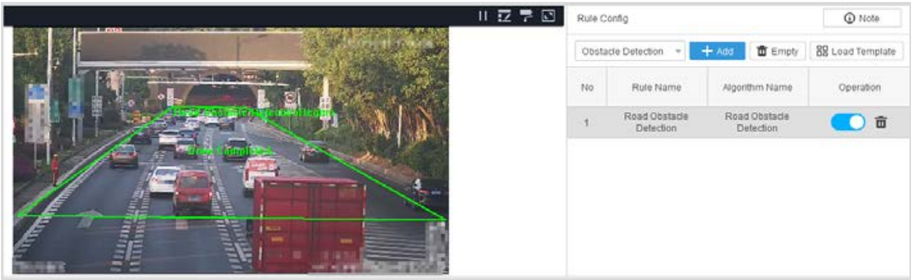
Step 2 Click **Add**.

After you add a rule, the rule is enabled by default.

Step 3 Drag the angles to adjust the detection zone or click to draw a detection zone.

- The detection zone should cover the valid vehicle targets, and avoid being too large to be interfered from other objects.
- Click the screen to start drawing, and right-click the screen to finish drawing.
- By default, the detection zone covers the whole image.

Figure 4-40 Barrier detection

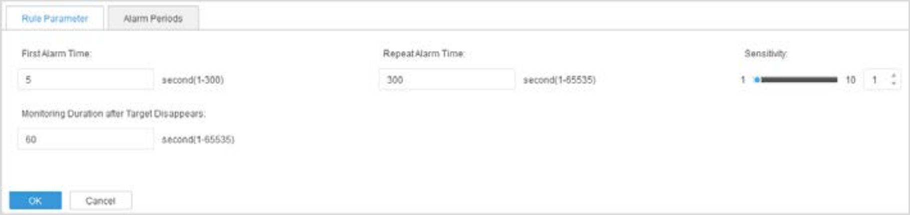


Rule Config

No	Rule Name	Algorithm Name	Operation
1	Road Obstacle Detection	Road Obstacle Detection	

Step 4 Click **Rule Parameter**, and then configure the parameters.

Figure 4-41 Barrier detection parameters



First Alarm Time: 5 second(1-300)

Repeat Alarm Time: 300 second(1-65535)

Sensitivity: 1 10 1

Monitoring Duration after Target Disappears: 60 second(1-65535)

Table 4-9 Description of barrier detection parameters

Parameter	Description
First Alarm Time	An alarm will be triggered when a barrier stays longer than the defined time.
Repeat Alarm Time	The interval between 2 alarms. If alarms are triggered continuously within the defined interval, the alarm will only be reported once. If the event is removed, alarm details contain 3 alarm images, which are the image of first trigger, the image within the repeated alarm interval, and the image when the event is removed.
Sensitivity	The higher the sensitivity is, the easier it is to detect and trigger an alarm. The false alarm rate also increases. We recommend you leave it as default.
Monitoring Duration after Target Disappears	The event ends when the disappearing duration of the object reaches the defined time.

Step 5 Configure **Alarm Periods**. For details, see Step5 in "4.5.2.1 Parking Detection".

Step 6 Click **OK**.

The configuration is saved and applied, and the **Rule Config** page is closed.

Related Operations

- Click **Empty** to clear all configured rules.
- Click **Load Template**, select a template, and then click **OK**. Rule parameters are configured based on the template.

4.5.2.12 Accident Detection

An alarm will be triggered when vehicles crash and the event lasts longer than the defined value.

Procedure

Step 1 On the **Rule Config** page, select **Accident Detection** from the **Rule Config** drop-down list.

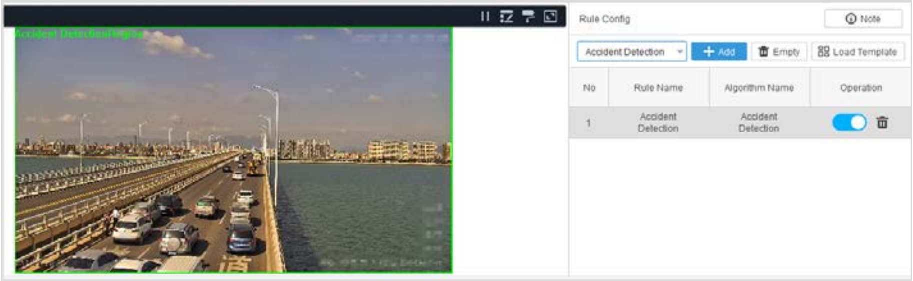
Step 2 Click **Add**.

After you add a rule, the rule is enabled by default.

Step 3 Drag the angles to adjust the detection zone or click to draw a detection zone.

- The detection zone should cover the valid vehicle targets, and avoid being too large to be interfered from other objects.
- Click the screen to start drawing, and right-click the screen to finish drawing.
- By default, the detection zone covers the whole image.

Figure 4-42 Accident detection



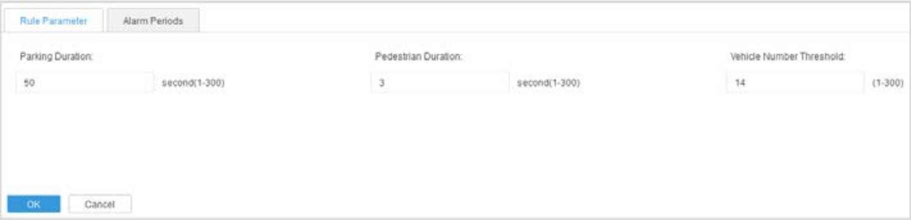
Rule Config

Accident Detection

No	Rule Name	Algorithm Name	Operation
1	Accident Detection	Accident Detection	

Step 4 Click the **Rule Config** tab, and then configure the parameters.

Figure 4-43 Accident detection parameters



Parking Duration: 50 second(1-300)

Pedestrian Duration: 3 second(1-300)

Vehicle Number Threshold: 14 (1-300)

Table 4-10 Description of accident detection parameters

Parameter	Description
Parking Duration	This parameter is used together with **Pedestrian Duration**. The timing starts when the accident vehicle remains stationary, and the accident condition 1 is met when the defined time is reached.

Parameter	Description
Pedestrian Duration	This parameter is used together with **Parking Duration**. The timing starts when a person appears in the detection zone, and the accident condition 2 is satisfied when the defined time is reached.
Vehicle Number Threshold	When the number of stationary vehicles exceeds the value, no alert is triggered.

Step 5 Configure **Alarm Periods**. For details, see Step5 in "4.5.2.1 Parking Detection".

Step 6 Click **OK**.

The configuration is saved and applied, and the **Rule Config** page is closed.

Related Operations

- Click **Empty** to clear all configured rules.
- Click **Load Template**, select a template, and then click **OK**. Rule parameters are configured based on the template.

4.5.2.13 Radiation Fog Detection

An alarm will be triggered when radiation fog is detected in the detection zone and the duration exceeds the defined value.

Procedure

Step 1 On the **Rule Config** page, select **Visibility Detection** from the **Rule Config** drop-down list.

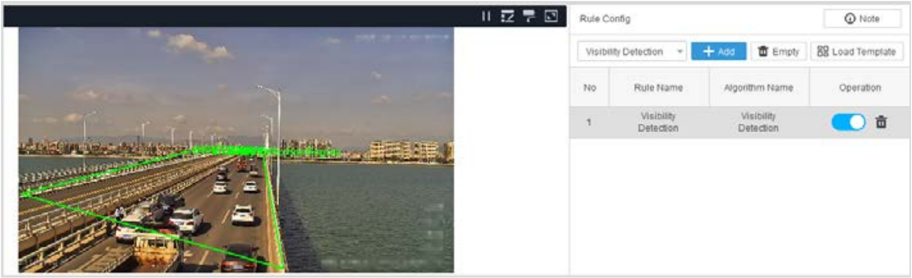
Step 2 Click **Add**.

After you add a rule, the rule is enabled by default.

Step 3 Drag the angles to adjust the detection zone or click to draw a detection zone.

- The detection zone should cover the valid vehicle targets, and avoid being too large to be interfered from other objects.
- Click the screen to start drawing, and right-click the screen to finish drawing.
- By default, the detection zone covers the whole image.

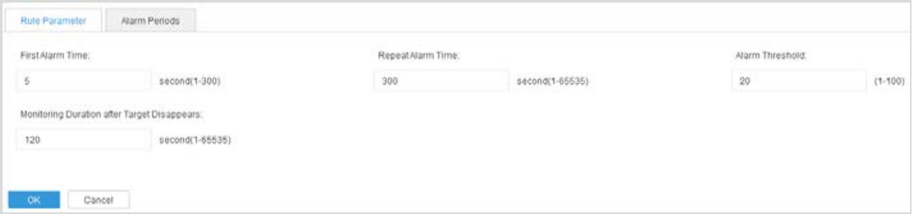
Figure 4-44 Visibility detection



No	Rule Name	Algorithm Name	Operation
1	Visibility Detection	Visibility Detection	

Step 4 Click **Rule Parameter**, and then configure the parameters.

Figure 4-45 Visibility detection parameters



First Alarm Time: 5 second(1-300)

Repeat Alarm Time: 300 second(1-65535)

Alarm Threshold: 20 (1-100)

Monitoring Duration after Target Disappears: 120 second(1-65535)

Table 4-11 Description of radiation fog detection parameters

Parameter	Description
First Alarm Time	An alarm will be triggered when a radiation fog exists and it stays longer than the defined value.
Repeat Alarm Time	The interval between the time of alarming after radiation fog is detected and the time to report it. If alarms are triggered continuously within the defined interval, the alarm information is reported only once. 📖 If the event is removed, alarm details contain 3 alarm images, which are the image of first trigger, the image within the repeated alarm interval, and the image when the event is removed.
Alarm Threshold	An alarm will be triggered when the concentration of the radiation fog exceeds the defined value.
Monitoring Duration after Target Disappears	The event ends when the object disappears beyond the defined time.

Step 5 Configure **Alarm Periods**. For details, see Step5 in "4.5.2.1 Parking Detection".

Step 6 Click **OK**.

The configuration is saved and applied, and the **Rule Config** page is closed.

Related Operations

- Click **Empty** to clear all configured rules.
- Click **Load Template**, select a template, and then click **OK**. Rule parameters are configured based on the template.

4.5.2.14 Smoke Detection

An alarm will be triggered when smoke is detected in the detection zone and the duration exceeds the defined value.

Procedure

Step 1 On the **Rule Config** page, select **Smoke Detection** from the **Rule Config** drop-down list.

Step 2 Click **Add**.

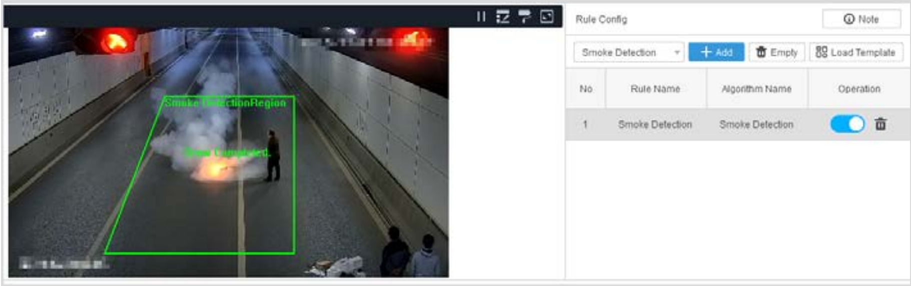
📖

After you add a rule, the rule is enabled by default.

Step 3 Drag the angles to adjust the detection zone or click ☑ to draw a detection zone.

- The detection zone should cover the valid vehicle targets, and avoid being too large to be interfered from other objects.
- Click the screen to start drawing, and right-click the screen to finish drawing.
- By default, the detection zone covers the whole image.

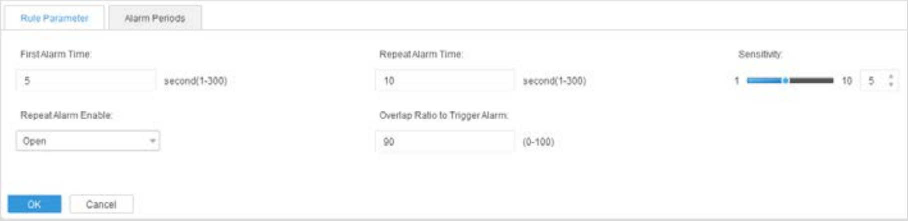
Figure 4-46 Smoke detection



No	Rule Name	Algorithm Name	Operation
1	Smoke Detection	Smoke Detection	

Step 4 Click the **Rule Parameter** tab, and then configure the parameters.

Figure 4-47 Smoke detection parameters



First Alarm Time: 5 second(1-300)

Repeat Alarm Time: 10 second(1-300)

Sensitivity: 1 10 5

Repeat Alarm Enable: Open

Overlap Ratio to Trigger Alarm: 90 (0-100)

Table 4-12 Description of smoke detection parameters

Parameter	Description
First Alarm Time	An alarm will be triggered when smoke stays longer than the defined value.
Repeat Alarm Time	If alarms are triggered continuously within the defined interval, the alarm information is reported only once.
Repeat Alarm Enable	Repeated alarm only takes effect after you enable this function.
Overlap Ratio to Trigger Alarm	Compare the previous frame with the next frame. If the overlapping area exceeds the defined value, an alarm will be triggered.
Sensitivity	The higher the sensitivity is, the easier it is to detect and trigger an alarm. The false alarm rate also increases. We recommend you leave it as default.

Step 5 Configure **Alarm Periods**. For details, see Step5 in "4.5.2.1 Parking Detection".

Step 6 Click **OK**.

The configuration is saved and applied, and the **Rule Config** page is closed.

Related Operations

- Click **Empty** to clear all configured rules.
- Click **Load Template**, select a template, and then click **OK**. Rule parameters are configured based on the template.

4.5.2.15 Fire Detection

An alarm will be triggered when fire is detected in the detection zone and the duration exceeds the defined value.

Procedure

Step 1 On the **Rule Config** page, select **Fire Detection** from the **Rule Config** drop-down list.

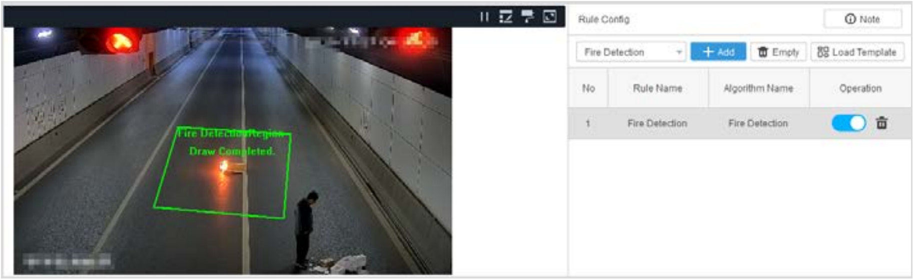
Step 2 Click **Add**.

After you add a rule, the rule is enabled by default.

Step 3 Drag the angles to adjust the detection zone or click ☒ to draw a detection zone.

- The detection zone should cover the valid vehicle targets, and avoid being too large to be interfered from other objects.
- Click the screen to start drawing, and right-click the screen to finish drawing.
- By default, the detection zone covers the whole image.

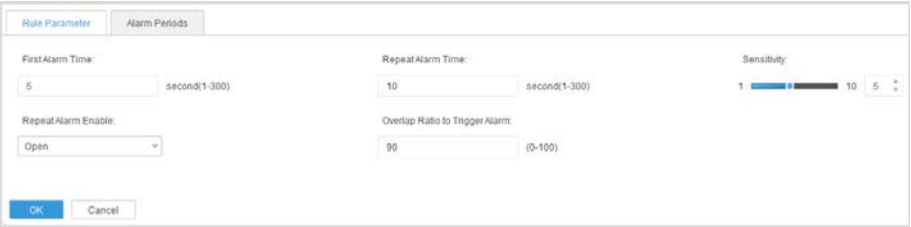
Figure 4-48 Fire detection



No	Rule Name	Algorithm Name	Operation
1	Fire Detection	Fire Detection	

Step 4 Click **Rule Parameter**, and then configure the parameters.

Figure 4-49 Fire detection parameters



First Alarm Time: 5 second(1-300)

Repeat Alarm Time: 10 second(1-300)

Sensitivity: 1 10 5

Repeat Alarm Enable: Open

Overlap Ratio to Trigger Alarm: 90 (0-100)

Table 4-13 Description of fire detection parameters

Parameter	Description
First Alarm Time	An alarm will be triggered when fire stays longer than the defined value.
Repeat Alarm Time	If alarms are triggered continuously within the defined interval, the alarm information is reported only once.
Repeat Alarm Enable	Repeated alarm takes effect after you enable this function. ● **Open**: Enabled. ● **Close**: Disabled.
Overlap Ratio to Trigger Alarm	Compare the previous frame with the next frame. If the overlapping area exceeds the defined value, an alert will be triggered.

Parameter	Description
Sensitivity	The higher the sensitivity is, the easier it is to detect and trigger an alarm. The false alarm rate also increases. We recommend you leave it as default.

Step 5 Configure **Alarm Periods**. For details, see Step5 in "4.5.2.1 Parking Detection".

Step 6 Click **OK**.

The configuration is saved and applied, and the **Rule Config** page is closed.

Related Operations

- Click **Empty** to clear all configured rules.
- Click **Load Template**, select a template, and then click **OK**. Rule parameters are configured based on the template.

4.5.2.16 Crossing Line Detection

An alarm will be triggered when a vehicle crosses a solid yellow line or solid white line.

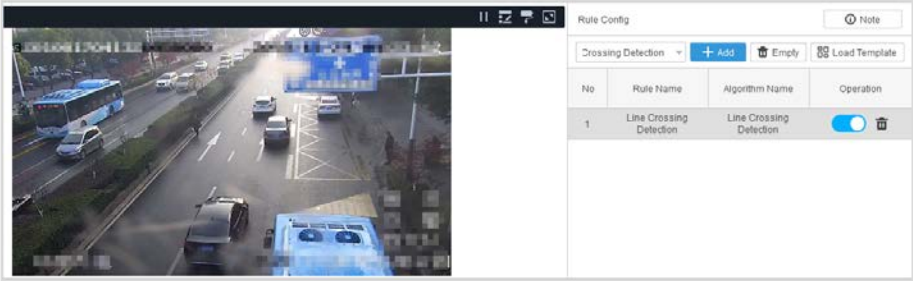
Procedure

Step 1 On the **Rule Config** page, select **Line Crossing Detection** from the **Rule Config** drop-down list.

Step 2 Click **Add**.

After you add a rule, the rule is enabled by default.

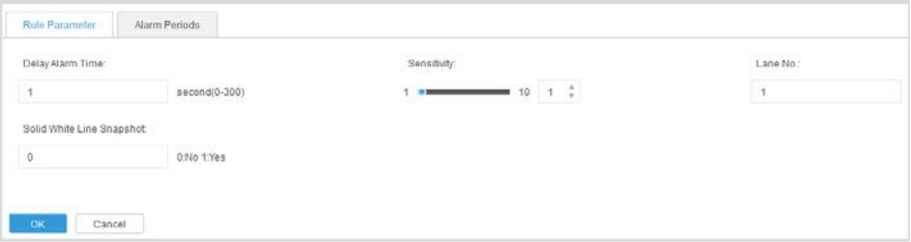
Figure 4-50 Crossing line detection



No	Rule Name	Algorithm Name	Operation
1	Line Crossing Detection	Line Crossing Detection	

Step 3 Click **Rule Parameter**, and then configure the parameters.

Figure 4-51 Crossing line detection parameters



Delay Alarm Time: 1 second(0-300)

Sensitivity: 1 10 1

Lane No.: 1

Solid White Line Snapshot: 0 0:No 1:Yes

Table 4-14 Parameter descriptions for cross line detection

Parameter	Description
Delay Alarm Time	When a vehicle crosses a solid line for a time period that is longer than the defined time, an alarm will be triggered.

Parameter	Description
Lane No	The sequence number of the lane to be detected.
Solid White Line Snapshot	Specify whether to detect solid white lines. Solid yellow lines are detected by default.
Sensitivity	The higher the sensitivity is, the easier an alarm is detected and triggered. The false alarm rate also increases.

Step 4 Configure **Alarm Periods**. For details, see Step5 in "4.5.2.1 Parking Detection".

Step 5 Click **OK**.

The configuration is saved and applied, and the **Rule Config** page is closed.

Related Operations

- Click **Empty** to clear all configured rules.
- Click **Load Template**, select a template, and then click **OK**. Rule parameters are configured based on the template.

4.5.2.17 Speeding Detection

When the speed of a vehicle is higher than the defined maximum speed and the duration exceeds the defined value, an alarm will be triggered.

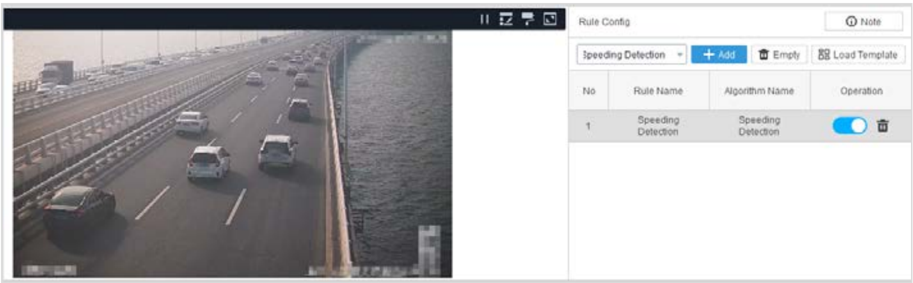
Procedure

Step 1 On the **Rule Config** page, select **Speeding Detection** from the **Rule Config** drop-down list.

Step 2 Click **Add**.

After you add a rule, the rule is enabled by default.

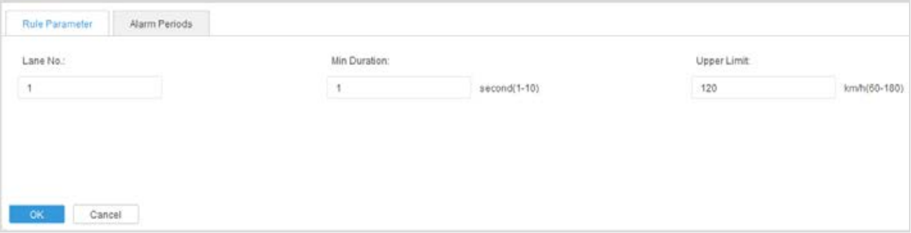
Figure 4-52 Speeding detection



No	Rule Name	Algorithm Name	Operation
1	Speeding Detection	Speeding Detection	

Step 3 Click **Rule Parameter**, and then configure the parameters.

Figure 4-53 Speeding detection parameters



Lane No.: 1

Min Duration: 1 second(1-10)

Upper Limit: 120 km/h(60-180)

Table 4-15 Description of speeding detection parameters

Parameter	Description
Lane No	The number of the lane to be detected. If you have not drawn lane lines.
Min Duration	When the speed of a vehicle is higher than the defined maximum speed and the duration exceeds the defined value, an alarm will be triggered.
Upper Limit	

Step 4 Configure **Alarm Periods**. For details, see Step5 in "4.5.2.1 Parking Detection".

Step 5 Click **OK**.

The configuration is saved and applied, and the **Rule Config** page is closed.

Related Operations

- Click **Empty** to clear all configured rules.
- Click **Load Template**, select a template, and then click **OK**. Rule parameters are configured based on the template.

4.5.2.18 Underspeed Detection

An alarm will be triggered when the driving speed is lower than the defined minimum speed and the duration exceeds the defined value.

Procedure

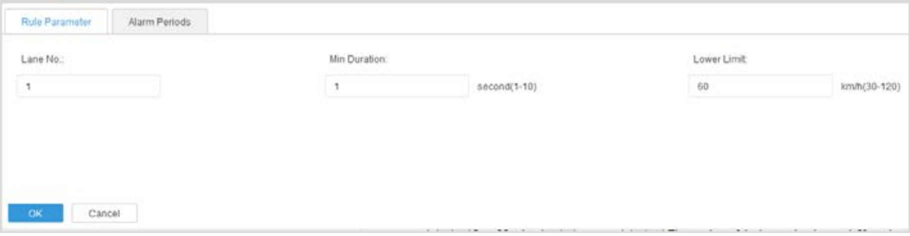
Step 1 On the **Rule Config** page, select **Low Speed Detection** from the **Rule Config** drop-down list.

Step 2 Click **Add**.

After you add a rule, the rule is enabled by default.

Step 3 Click **Rule Parameter**, and then configure the parameters.

Figure 4-54 Driving slowly detection parameters



Lane No.: 1

Min Duration: 1 second(1-10)

Lower Limit: 60 km/h(30-120)

Table 4-16 Description of driving slowly detection parameters

Parameter	Description
Lane No	The number of the lane to be detected. If you have not drawn lane lines.
Min Duration	When the speed of a vehicle is higher than the defined maximum speed and the duration exceeds the defined value, an alarm will be triggered.
Low Limit	

Step 4 Configure **Alarm Periods** For details, see Step5 in "4.5.2.1 Parking Detection".

Step 5 Click **OK**.

The configuration is saved and applied, and the **Rule Config** page is closed.

Related Operations

- Click **Empty** to clear all configured rules.
- Click **Load Template**, select a template, and then click **OK**. Rule parameters are configured based on the template.

4.5.2.19 Intrusion

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

Procedure

Step 1 On the **Rule Config** page, select **Intrusion** from the **Rule Config** drop-down list.

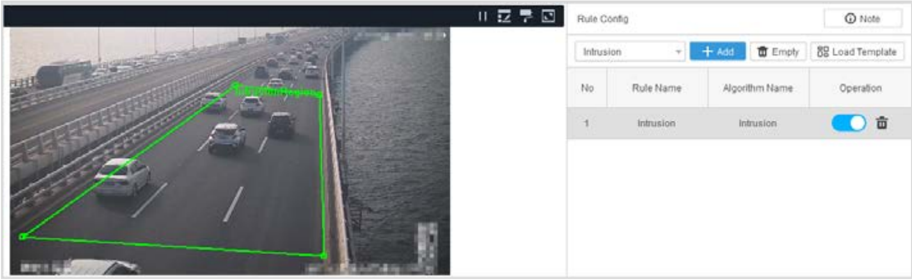
Step 2 Click **Add**.

After you add a rule, the rule is enabled by default.

Step 3 Drag the angles to adjust the detection zone or click ☑ to draw a detection zone.

- The detection zone should cover the valid vehicle targets, and avoid being too large to be interfered from other objects.
- Click the screen to start drawing, and right-click the screen to finish drawing.
- The detection zone covers the whole image by default.

Figure 4-55 Intrusion

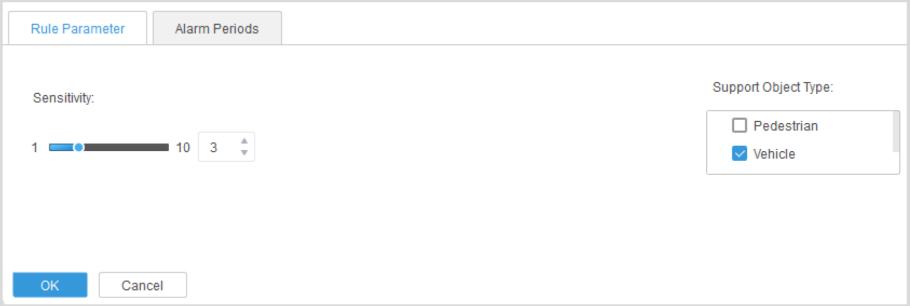


Intrusion

No	Rule Name	Algorithm Name	Operation
1	Intrusion	Intrusion	● 🗑

Step 4 Click the **Rule Parameter** tab, and then configure the parameters.

Figure 4-56 Description of intrusion



Sensitivity: 1 10 3

Support Object Type:

☐ Pedestrian

☑ Vehicle

- **Sensitivity**: The higher the sensitivity is, the easier it is to detect and trigger an alarm. The false alarm rate also increases. We recommend you leave it as default.
- **Supported Object Type**: You can select **Pedestrian** or **Vehicle** as the object.

Step 5 Configure **Alarm Periods**. For details, see Step5 in "4.5.2.1 Parking Detection".

Step 6 Click **OK**.

The configuration is saved and applied, and the **Rule Config** page is closed.

Related Operations

- Click **Empty** to clear all configured rules.
- Click **Load Template**, select a template, and then click **OK**. Rule parameters are configured based on the template.

4.5.2.20 Truck in Restricted Area

An alarm will be triggered when a truck enters the detection zone.

Procedure

Step 1 On the **Rule Config** page, select **Large Vehicle in Lane** from the **Rule Config** drop-down list.

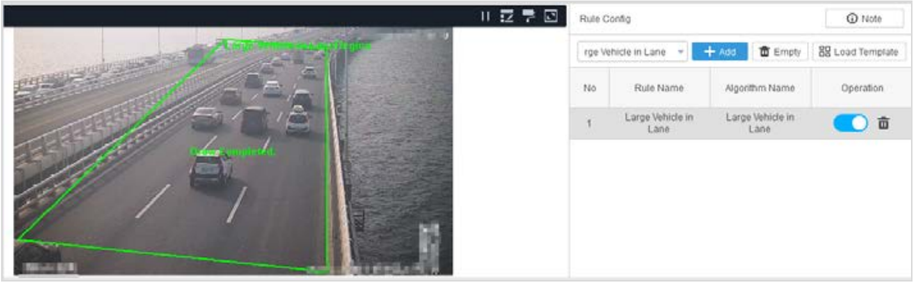
Step 2 Click **Add**.

After you add a rule, the rule is enabled by default.

Step 3 Drag the angles to adjust the detection zone or click to draw a detection zone.

- The detection zone should cover the valid vehicle targets, and avoid being too large to be interfered from other objects.
- Click the screen to start drawing, and right-click the screen to finish drawing.
- By default, the detection zone covers the whole image.

Figure 4-57 Truck in restricted area

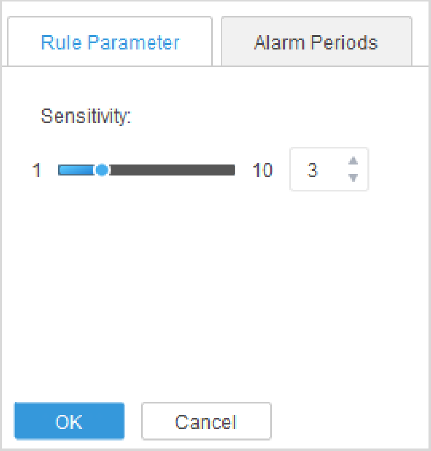


No	Rule Name	Algorithm Name	Operation
1	Large Vehicle in Lane	Large Vehicle in Lane	

Step 4 Click **Rule Parameter**, and then configure the sensitivity.

The higher the sensitivity is, the more easily an alarm is detected and triggered. The false alarm rate also increases. We recommend you to leave it as default.

Figure 4-58 Parameter of large vehicle in lane



Sensitivity: 1 — 10 3

Step 5 Configure **Alarm Periods**. For details, see Step5 in "4.5.2.1 Parking Detection".

Step 6 Click **OK**.

The configuration is saved and applied, and the **Rule Config** page is closed.

Related Operations

- Click **Empty** to clear all configured rules.
- Click **Load Template**, select a template, and then click **OK**. Rule parameters are configured based on the template.

4.5.2.21 Special Vehicle Detection

An alarm will be triggered when a special vehicle crosses the detection line.

Procedure

Step 1 On the **Rule Config** page, select **Dangerous Goods Vehicle Detection** from the **Rule Config** drop-down list.

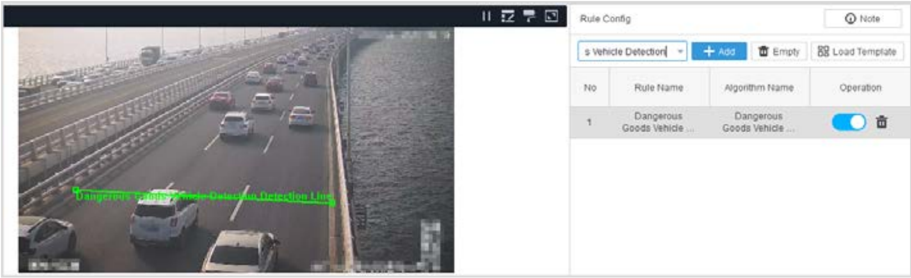
Step 2 Click **Add**.

After you add a rule, the rule is enabled by default.

Step 3 Drag the angles to adjust the detection zone or click ☑ to draw a detection zone.

- The detection zone should cover the valid vehicle targets, and avoid being too large to be interfered from other objects.
- Click the screen to start drawing, and right-click the screen to finish drawing.
- By default, the detection zone covers the whole image.

Figure 4-59 Dangerous goods vehicle detection

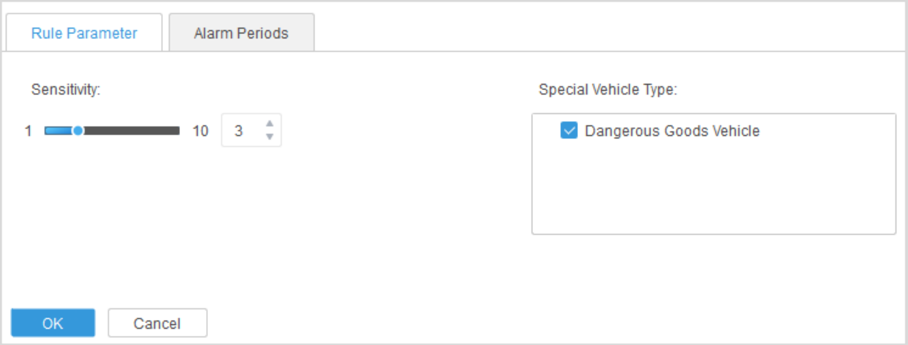


No	Rule Name	Algorithm Name	Operation
1	Dangerous Goods Vehicle ...	Dangerous Goods Vehicle ...	

Step 4 Click **Rule Parameter**, and then configure the parameters.

- **Sensitivity**: The higher the sensitivity is, the more easily an alarm is detected and triggered. The false alarm rate also increases. We recommend you to leave it as default.
- **Special Vehicle Type**: Select **Dangerous Goods Vehicle**.

Figure 4-60 Parameters of special vehicle detection



Sensitivity: 1 10 3

Special Vehicle Type:

☑ Dangerous Goods Vehicle

Step 5 Configure **Alarm Periods**. For details, see Step5 in "4.5.2.1 Parking Detection".

Step 6 Click **OK**.

The configuration is saved and applied, and the **Rule Config** page is closed.

Related Operations

- Click **Empty** to clear all configured rules.
- Click **Load Template**, select a template, and then click **OK**. Rule parameters are configured based on the template.

4.5.2.22 Video Exception Detection

An alarm will be triggered when detects the video image changes.

Procedure

Step 1 On the **Rule Config** page, select **Video Exception Detection** from the **Rule Config** drop-down list.

Step 2 Click **Add**.

- After you add a rule, the rule is enabled by default.
- In global mode, a rule can be added only once.

Step 3 Click the **Rule Parameter** tab, and then select **Image Change**.

Step 4 Configure **Alarm Periods**. For details, see Step5 in "4.5.2.1 Parking Detection".

Step 5 Click **OK**.

The configuration is saved and applied, and the **Rule Config** page is closed.

Related Operations

- Click **Empty** to clear all configured rules.
- Click **Load Template**, select a template, and then click **OK**. Rule parameters are configured based on the template.

4.5.2.23 Traffic Flow Statistics

Statistics on the number of vehicles passing through a road section within a specified time.

Procedure

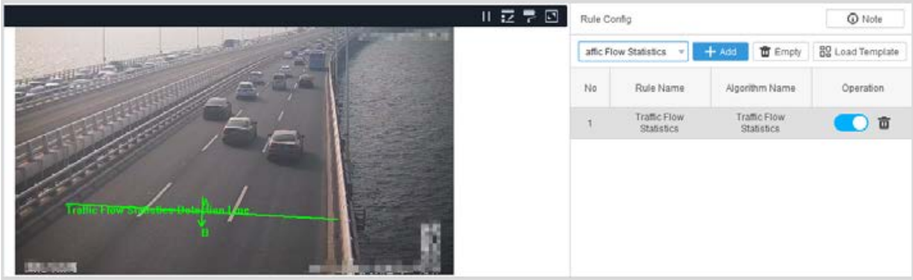
Step 1 On the **Rule Config** page, select **Traffic Flow Statistics** from the **Rule Config** drop-down list.

Step 2 Click **Add**.

- After you add a rule, the rule is enabled by default.
- In global mode, a rule can be added only once.

Step 3 Drag the angles to adjust the detection zone or click to draw a detection line.

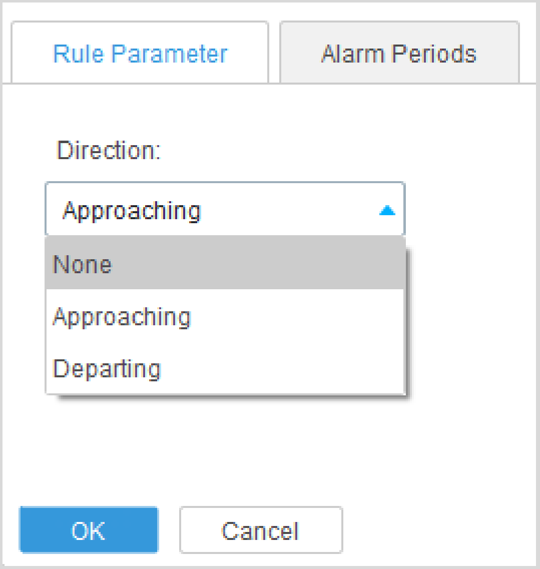
Figure 4-61 Traffic flow statistics



No	Rule Name	Algorithm Name	Operation
1	Traffic Flow Statistics	Traffic Flow Statistics	

Step 4 Click the **Rule Parameter** tab, and then configure the parameters.

Figure 4-62 parameters of traffic flow statistics



Direction: Approaching

- **None**: The direction of traffic flow is not specified, and you need to configure the lane number.

- **Approaching**: The direction of traffic flow is A<-B.
- **Departing**: The direction of traffic flow is A->B.

Step 5 Configure **Alarm Periods**. For details, see Step5 in "4.5.2.1 Parking Detection".

Step 6 Click **OK**.

The configuration is saved and applied, and the **Rule Config** page is closed.

Related Operations

- Click **Empty** to clear all configured rules.
- Click **Load Template**, select a template, and then click **OK**. Rule parameters are configured based on the template.

4.5.3 Configuring Lane Lines

Draw lane lines to determine and help detect illegal lane change wrong-way driving, traffic jams and other events. In global mode, there is no need to draw lane lines and the **Lane Line** page does not exist.

Procedure

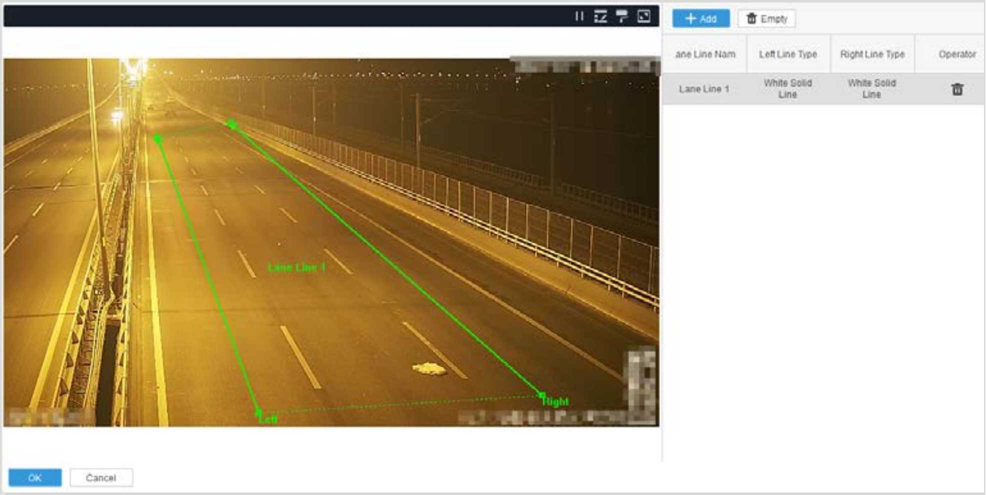
Step 1 Click **Lane Line**.

Step 2 Click **Add** to draw lane lines.

Point to the starting position of the lane line on the left, and click to draw. Move your mouse to the end position of the lane line, and click to complete drawing. Move your mouse to the starting position of another lane line. Repeat these steps to draw another line.

- The lane line must cover the largest vehicle targets that travel in the lane.
- In the image, roads that are far away are displayed by the camera as narrow. This influences judgment. To avoid error reports, you can widen the lane line on both sides.
- The detection range should exclude distant areas or turns as much as possible.
- One lane includes 2 lane lines. Keep the arrow and the driving direction as the same when drawing the lane line.

Figure 4-63 Draw lane lines



ane Line Nam	Left Line Type	Right Line Type	Operator
Lane Line 1	White Solid Line	White Solid Line	🗑

Step 3 Click **OK**.

Related Operations

Click **Empty** to clear all lane lines.

4.5.4 Configuring Calibration Plotting

Calibration is for speed measurement in speed detection events. Draw a quadrilateral on the real-time video image, which corresponds to a rectangle in the actual scene. Set the length of the rectangle, and the system detects the passing time of the vehicle to calculate the travelling speed of the vehicle.

Prerequisites

You have selected a channel configured with rules. For details, see " 4.5.1 Adding Channels".

Background Information

- To ensure that the length of the calibration quadrilateral corresponds to the length in the actual scene, we recommend you to follow the order of "upper left > lower left > lower right > upper right" when drawing the quadrilateral.
- We recommend that the left and right sides of the quadrilateral along the lane line to make the drawing as accurate as possible. The vertical line should fit the lane line or the actual road edge line. The horizontal line can be drawn with reference to a horizontal object.
- The quadrilateral should be as large as possible to reduce the chances of calibration errors being produced. It should be drawn according to the actual length that needs to be calibrated, including most of the road surface in the picture.
- Do not include parts of the road surface that are too far away from the detection zone of the camera. The size should be determined according to the field of view of the camera.

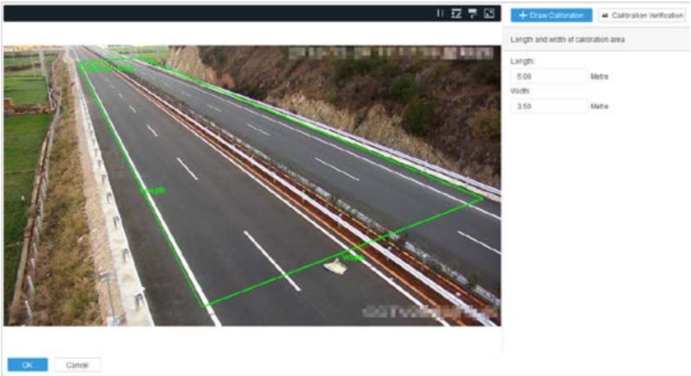
Procedure

Step 1 Click **Calibration Plotting**.

Step 2 Click **Draw Calibration** to draw a calibration area as needed.

Move your mouse to the starting position of the calibration region on the image, and then click to draw. Right-click the unclosed region, and the system will automatically close the region to complete drawing.

Figure 4-64 Draw a calibration area



Length and width of calibration area

Length: 5.00 Metre

Width: 3.50 Metre

Step 3 Enter the **Length** and **Width** to set the actual length and width of the calibration region.

In the preceding image, the quadrilateral covers 3 lanes. If the width of each lane is 3.5 m, the width of the calibration region is 10.5 m.

⚠

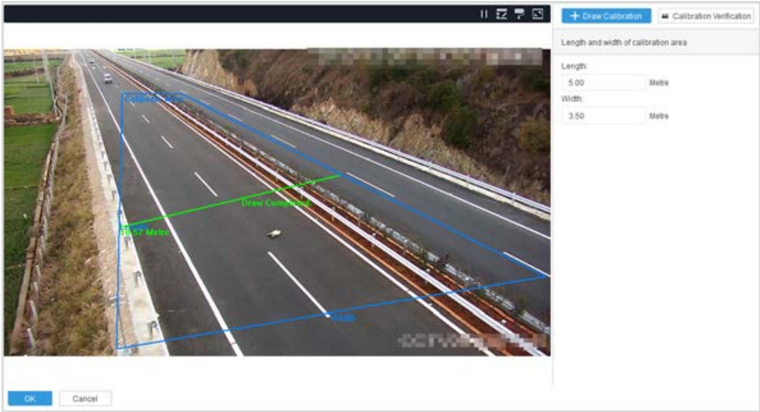
The filled length and width must be the same as the actual ones; otherwise the accuracy of speed measurement will be affected.

Step 4 Click **Calibration Verification** to draw a test line.

After the test line is drawn, the actual length of the test line calculated by the algorithm is displayed. Check whether the figure is the same as the actual length.

The test line should be drawn longitudinally. We recommend that you draw it along the white line in the middle of the road. Compare the length calculated by the algorithm with the actual length of the white line on the ground to ensure that the length of the calibration area is accurate.

Figure 4-65 Verify calibration



Length and width of calibration area

Length: 5.00 Metre

Width: 3.50 Metre

Step 5 Click **OK**.

4.5.5 Configuring Detection Zone

Configure the area to be detected to avoid the area being too large and to reduce the false alarm rate. In global mode, there is no need to draw lane lines and the **Detection Area** page does not exist.

Prerequisites

You have selected a channel configured with rules. For details, see "4.5.1 Adding Channels".

Background Information

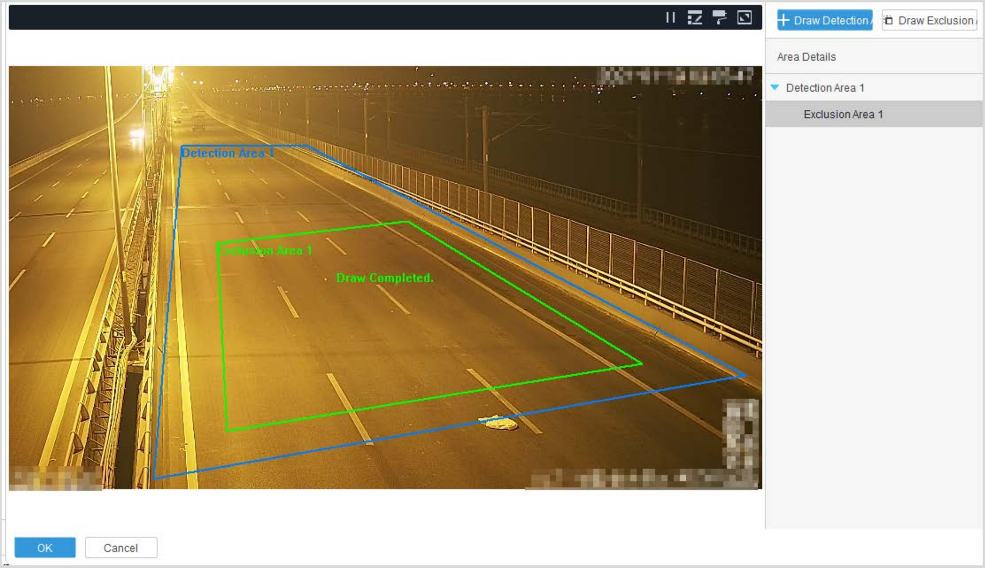
- You can only draw excluded zones in the detection zone.
- You can draw up to 1 detection zone and 10 exclusion zones.
- You can expand the detection zone to cover the large vehicle targets.
- To avoid error reports, the detection range should not cover distant areas or turns.

Procedure

Step 1 Click **Detection Area**.

Step 2 Click **Draw Detection Area** and **Draw Exclusion Area** to draw a detection zone and excluded zone respectively on the image.

Figure 4-66 Draw detection area and exclusion area



4.5.6 Configuring Size Filter

Draw 1 larger and 1 small box, and an alarm will be triggered only when the size of the detected target is within the size of the 2 boxes.

Prerequisites

You have selected a channel configured with rules. For details, see "4.5.1 Adding Channels".

Procedure

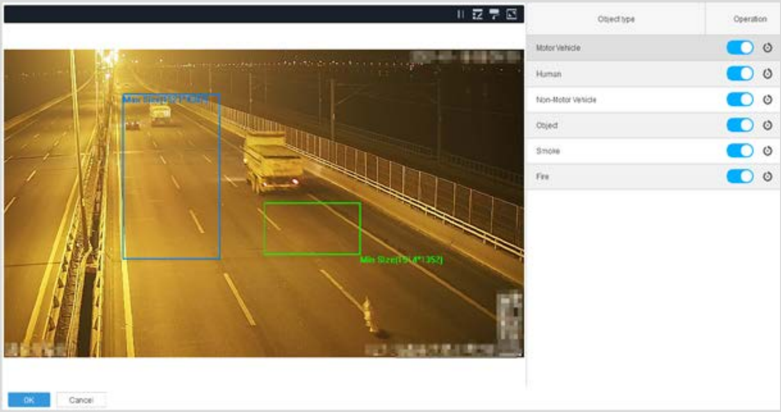
Step 1 Click **Size Filter**.

Step 2 Select the object type.

Step 3 Adjust the size of the boxes on the image.

An alarm will be triggered when the size of the target is within the size of the large box and the small box.

Figure 4-67 Size filter



Repeat Step 2 and Step 3 to draw filter boxes with multiple object types.

Related Operations

- Click ○ to enable size filtering. Click ● to disable size filtering.
- Click ⟲ to restore filter boxes to default size.

4.5.7 Managing Templates

You can create templates to configure rule parameters and alarm time period for multiple analysis tasks and channels.

4.5.7.1 Creating Templates

Procedure

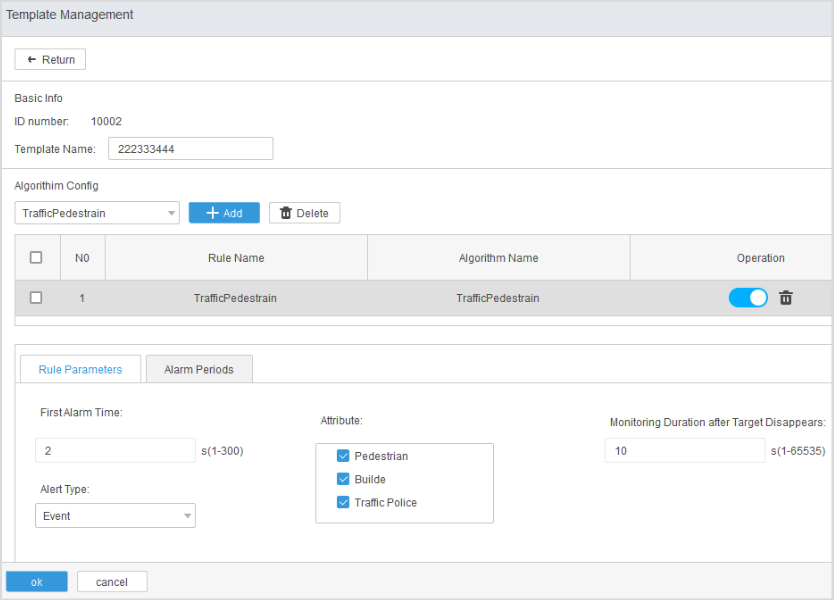
Step 1 Log in to the Client, and then select **Analysis Management** > **Manage Template** > **Add**.

Step 2 Set the template name.

Step 3 Select an algorithm from the **algorithm config** drop-down list and click **Add**.

Step 4 Configure rule parameters and alarm time. For details, see corresponding topic under "4.5.2 Configuring Rules".

Figure 4-68 Create a template



Template Management

← Return

Basic Info

ID number: 10002

Template Name: 222333444

Algorithim Config

TrafficPedestrain ▾ + Add 🗑 Delete

□	N0	Rule Name	Algorithm Name	Operation
□	1	TrafficPedestrain	TrafficPedestrain	● 🗑

Rule Parameters | Alarm Periods

First Alarm Time: 2 s(1-300)

Alert Type: Event

Attribute: ☑ Pedestrian ☑ Builde ☑ Traffic Police

Monitoring Duration after Target Disappears: 10 s(1-65535)

ok cancel

Step 5 (Optional) Repeat Step 3 and Step 4 to add more algorithm rules.

Step 6 Click **OK**.

4.5.7.2 Loading Templates

Prerequisites

You have added a channel. For details, see "4.5.1 Adding Channels".

Procedure

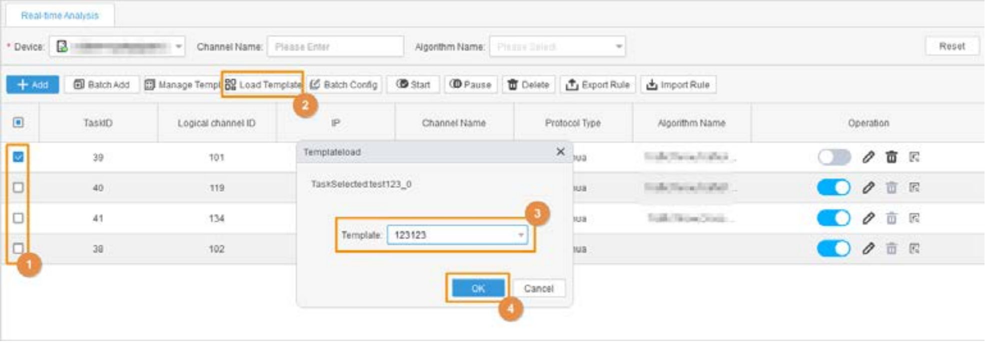
Step 1 Log in to the Client, and then click **Analysis Management**.

Step 2 Select channels for which you want to load a template, and then click **Load Template**.

Step 3 Select a template.

Step 4 Click **OK**.

Figure 4-69 Load a template



4.5.8 Batch Configuration

You can configure parameters for multiple channels at a time.

Procedure

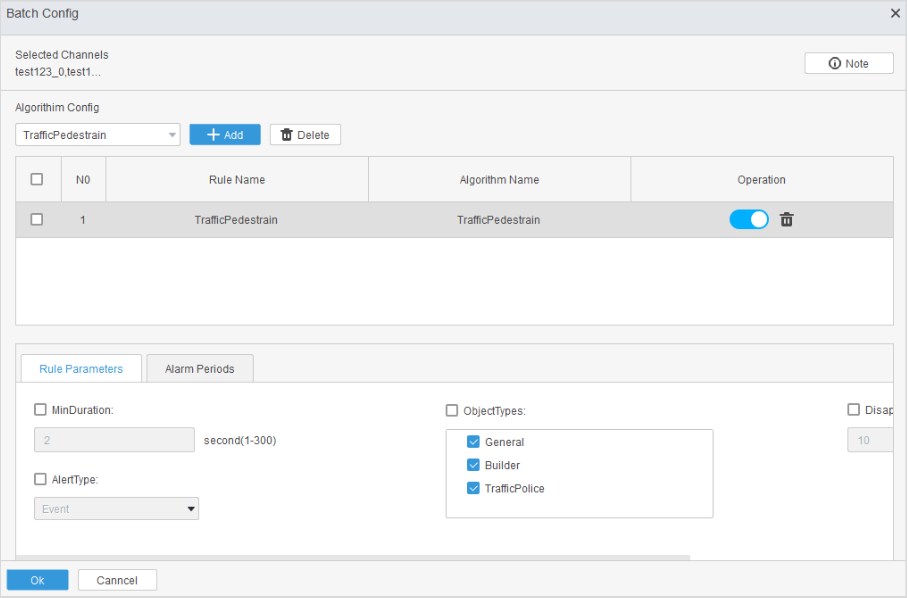
Step 1 Log in to the Client, and then click **Analysis Management**.

Step 2 Select multiple channels, and then click **Batch Config**.

Step 3 Select an algorithm from the **Algorithm Config** drop-down list, and then click **Add**.

Step 4 Configure rule parameters and alarm time. For details on the rule parameters, see corresponding topic under "4.5.2 Configuring Rules".

Figure 4-70 Batch configuration



Parameter values displayed in batch configuration are default values, not the ones that are configured in actual channels.

Step 5 (Optional) Repeat Step 2 and Step 3 to add more algorithm rules.

Step 6 Click **Ok**.

4.6 Setting Recording Storage

Prerequisites

You have logged in to a server.

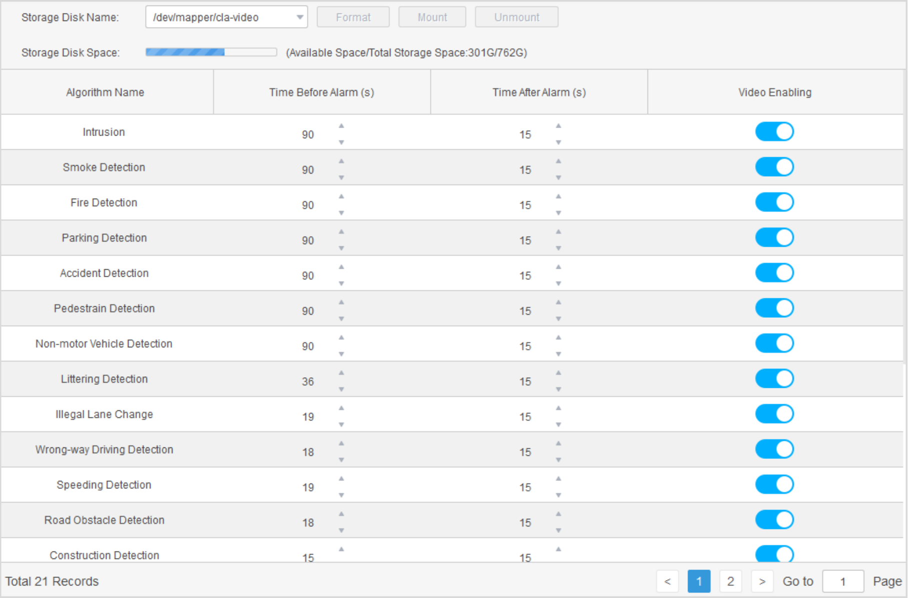
Procedure

Step 1 Log in to the Client, and then click **Video Management**.

Step 2 Select a storage disk for the server. You can format, mount, or unmount a disk.

Step 3 Enable recording for corresponding events. By default, the video recorded 15 s before and after an alarm is saved to the selected disk. The length of the video is 90 s at most.

Figure 4-71 Set recording storage



Storage Disk Name: /dev/mapper/cla-video

Storage Disk Space: (Available Space/Total Storage Space:301G/762G)

Algorithm Name	Time Before Alarm (s)	Time After Alarm (s)	Video Enabling
Intrusion	90	15	●
Smoke Detection	90	15	●
Fire Detection	90	15	●
Parking Detection	90	15	●
Accident Detection	90	15	●
Pedestrain Detection	90	15	●
Non-motor Vehicle Detection	90	15	●
Littering Detection	36	15	●
Illegal Lane Change	19	15	●
Wrong-way Driving Detection	18	15	●
Speeding Detection	19	15	●
Road Obstacle Detection	18	15	●
Construction Detection	15	15	●

Total 21 Records

5 Business Application

This section introduces how to view live video and alarm events through the server on the Client.

5.1 Live View

After you remotely log in to the server on the Client and add remote devices, you can view real-time videos, vehicle conditions on lanes, and alarm events.

Procedure

Step 1 Double-click to open the Client.

Step 2 Click **Live View**.

Step 3 Click ▶ to expand the server list, and the channel list is displayed.

- indicates the server is offline. Right-click **Login** on the server to log in to the server.
- indicates the server is online. Right-click **Logout** on the server to log out of the server.

Step 4 (Optional) Select the display scale and window layout of video image.

- In the Original drop-down list at the bottom of the **Live View** page, select the display scale of the video image.
  - **Full Screen**: The image is expanded to cover the whole screen.
  - **Original**: The image is displayed with its original size.
- Select a window layout from ■ ▦ ▦ ▦. Select single screen, 4-split, 9-split, or 16-split as needed.

Step 5 Enable live view.

- Select a live view window, and then double-click a channel to enable real-time view.
- Drag a channel to a live view window to enable real-time view.
- Select a live view window, right-click a channel, and then select **Start Preview** to enable real-time view.

- indicates channels with live view enabled. Right-click the channel to select **Stop Preview** to close the monitoring screen.
- indicates channels with live view disabled. Right-click the channel to select **Start Preview** to open the monitoring screen.

Step 6 Click to subscribe to alarm information. Only alarm information on subscribed channels can be displayed.

After configuring smart rules, an alarm pop-up is displayed at the lower-right corner of your computer, while the traffic event detection alarm is displayed at the right side of the **Live View** page.

Figure 5-1 Subscribe to alarm information

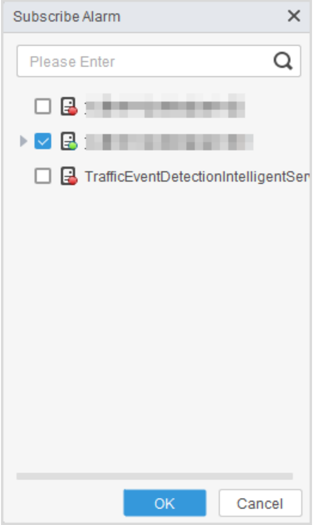
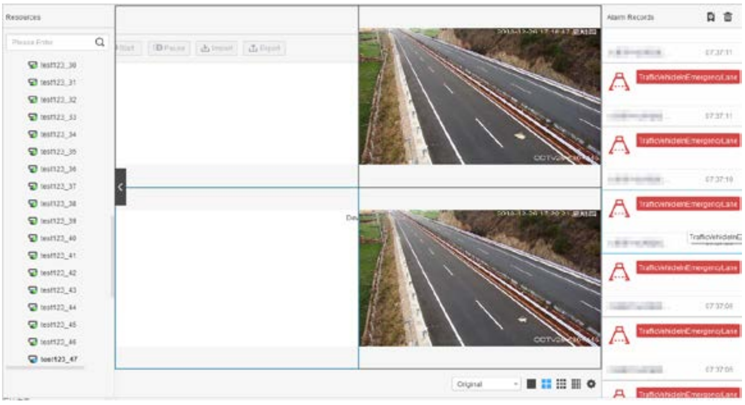


Figure 5-2 Live view



5.2 Reviewing Alarm Results

You can review alarm results to optimize algorithms, and play and download the recordings of alarm events.

Procedure

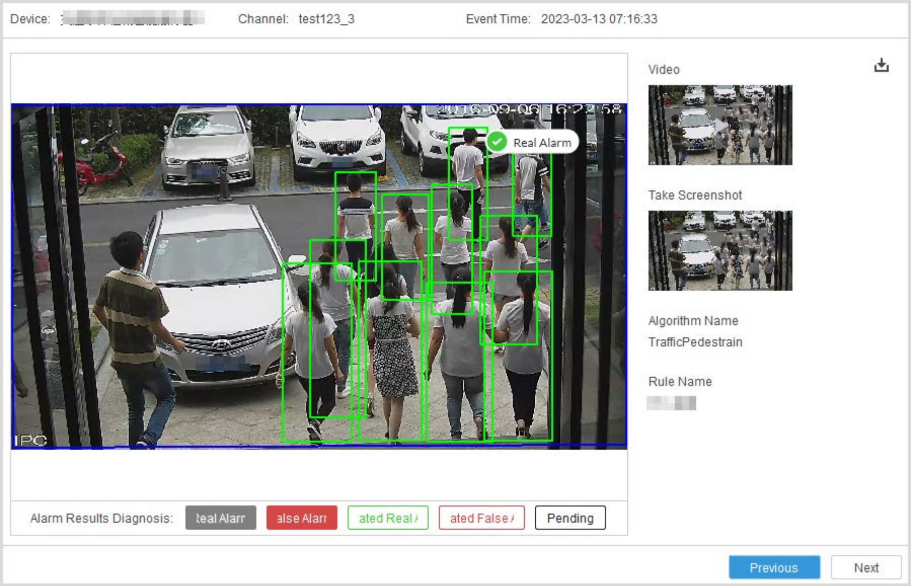
Step 1 Double-click the pop-up window at the lower-right corner of the desktop or double-click the alarm event in the right side of the **Live View** page.

Step 2 (Optional) Click ▶ to view the recording.

You can click **download** to download the recording to your computer.

Only dav and mp4 formats are supported. The dav format contains intelligent frames, and the mp4 format does not contain intelligent frames.

Figure 5-3 View recording



Device: [redacted] Channel: test123_3 Event Time: 2023-03-13 07:16:33

Algorithm Name
TrafficPedestrain

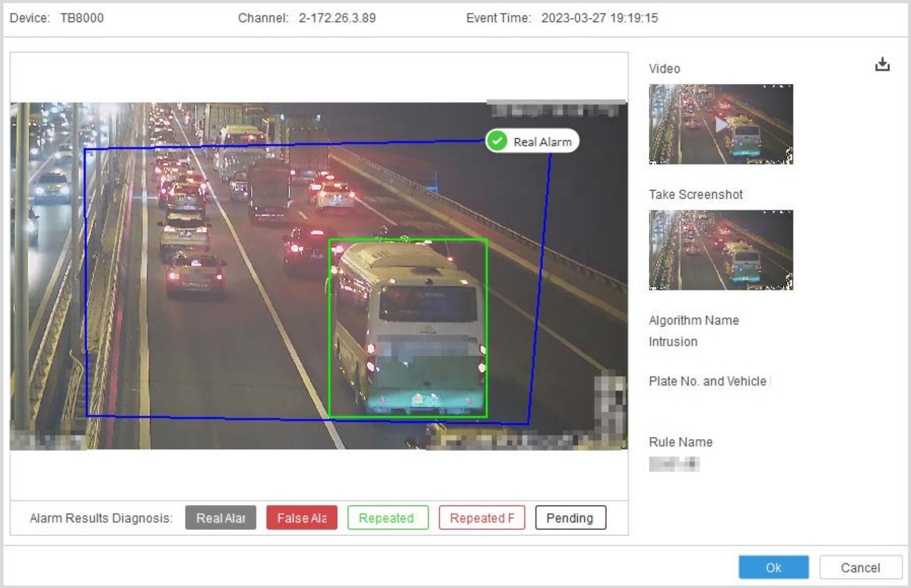
Rule Name
[redacted]

Step 3 Review alarm results to optimize algorithms.

After you click **Real Alarm**, **False Alarm**, **Repeated Real Alarm**, **Repeated False Alarm**, or **Pending**, a corresponding label appears on the screenshot.

- **Real Alarm**: Confirm that the alarm is a real alarm.
- **False Alarm**: Confirm that the alarm is a false alarm.
- **Repeated Real Alarm**: Confirm that the alarm is a real but repeated alarm.
- **Repeated False Alarm**: Confirm that the alarm is a false but repeated alarm.
- **Pending**: Do not review the alarm.

Figure 5-4 Detailed alarm information



Device: TB8000 Channel: 2-172.26.3.89 Event Time: 2023-03-27 19:19:15

Algorithm Name
Intrusion

Plate No. and Vehicle

Rule Name
[redacted]

5.3 Searching for Events

5.3.1 Searching for Alarm Events

Procedure

Step 1 Open the Client, and then select **Event Search** > **Alarm Search**.

Step 2 Select an intelligent server and the channels.

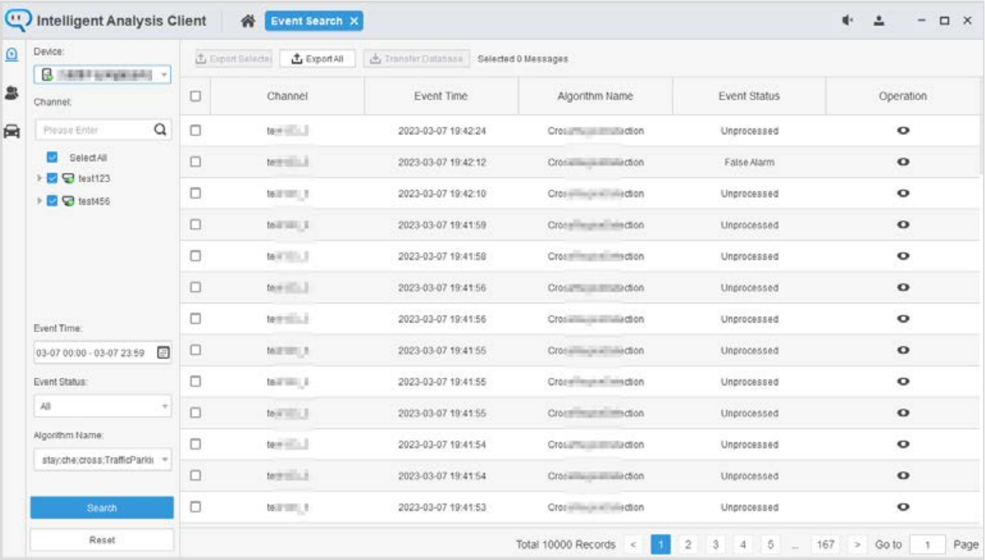
You must select at least 1 channel.

Step 3 Set **Event Time**, **Event Status**, and **Algorithm Name**.

Step 4 Click **Search**.

Click **Reset** to clear all search conditions.

Figure 5-5 Search for events



Device: [redacted]

Channel: Please Enter

☑ Select All

☑ test123

☑ test456

Event Time: 03-07 00:00 - 03-07 23:59

Event Status: All

Algorithm Name: stay;che;cross;TrafficParki

Search

Reset

Selected 0 Messages

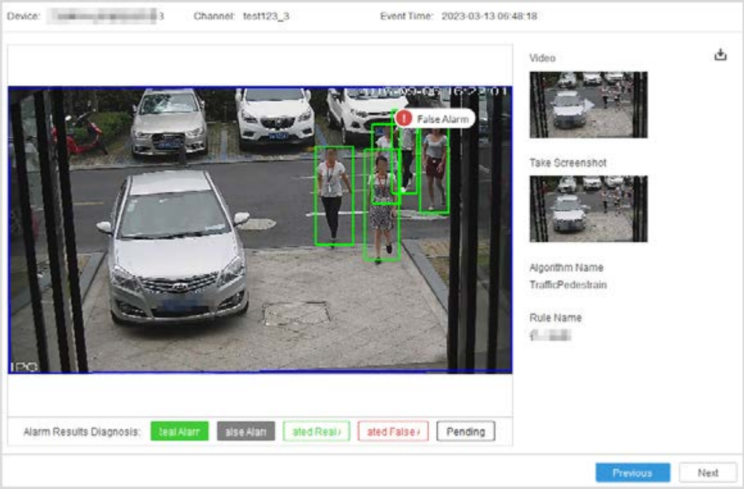
□	Channel	Event Time	Algorithm Name	Event Status	Operation
□	te[redacted]	2023-03-07 19:42:24	Cro[redacted]ction	Unprocessed	👁
□	te[redacted]	2023-03-07 19:42:12	Cro[redacted]ction	False Alarm	👁
□	te[redacted]	2023-03-07 19:42:10	Cro[redacted]ction	Unprocessed	👁
□	te[redacted]	2023-03-07 19:41:59	Cro[redacted]ction	Unprocessed	👁
□	te[redacted]	2023-03-07 19:41:58	Cro[redacted]ction	Unprocessed	👁
□	te[redacted]	2023-03-07 19:41:56	Cro[redacted]ction	Unprocessed	👁
□	te[redacted]	2023-03-07 19:41:56	Cro[redacted]ction	Unprocessed	👁
□	te[redacted]	2023-03-07 19:41:55	Cro[redacted]ction	Unprocessed	👁
□	te[redacted]	2023-03-07 19:41:55	Cro[redacted]ction	Unprocessed	👁
□	te[redacted]	2023-03-07 19:41:55	Cro[redacted]ction	Unprocessed	👁
□	te[redacted]	2023-03-07 19:41:54	Cro[redacted]ction	Unprocessed	👁
□	te[redacted]	2023-03-07 19:41:54	Cro[redacted]ction	Unprocessed	👁
□	te[redacted]	2023-03-07 19:41:53	Cro[redacted]ction	Unprocessed	👁

Total 10000 Records < 1 2 3 4 5 ... 167 > Go to 1 Page

Step 5 Double-click an event or click 👁 to view details.

- You can click **Previous** or **Next** to view the previous or next alarm.
- The green box traces the target triggering the alarm.

Figure 5-6 Detailed information of an alarm



Device: [redacted]3 Channel: test123_3 Event Time: 2023-03-13 06:48:18

Algorithm Name
TrafficPedestrain

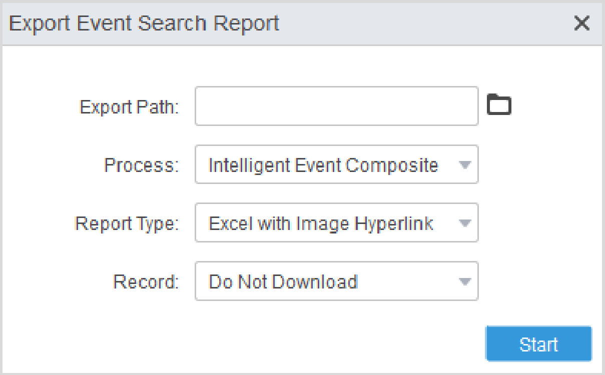
Rule Name
[redacted]

Alarm Results Diagnosis:

Step 6 (Optional) Export event information.

Select the events you want, and click **Export Selected**. You can also click **Export All** to export all event information.

Figure 5-7 Export search records



Export Event Search Report

Export Path:

Process: Intelligent Event Composite

Report Type: Excel with Image Hyperlink

Record: Do Not Download

Table 5-1 Description of export parameters

Parameter	Description
Export Path	Select the local path for exported information.
Process	● **No process**: No tracking box for the target on the exported image. ● **Compose Intelligent Event Image**: There is a tracking box for the target on the exported image.
Report Type	● **No report**: no report for the exported information. ● **CSV File (separated by comma)**: The exported information includes a CSV file. ● **Excel with image hyperlink**: The exported information includes an Excel file. Click the image and it will be linked to a large image. ● **Text File (separated by tab)**: The exported information includes a Text file.
Report	You can select **mp4** or **dav** or **Do Not Download** from the drop-down list.

5.3.2 Searching for Traffic Flow Statistics

You can search for or export traffic flow statistics on a channel within a defined period of time.

Procedure

Step 1 Open the Client, and then select **Event Search** > **Vehicle Statistics Search**.

Step 2 Select an intelligent server and the channels under it.

You must select at least 1 channel.

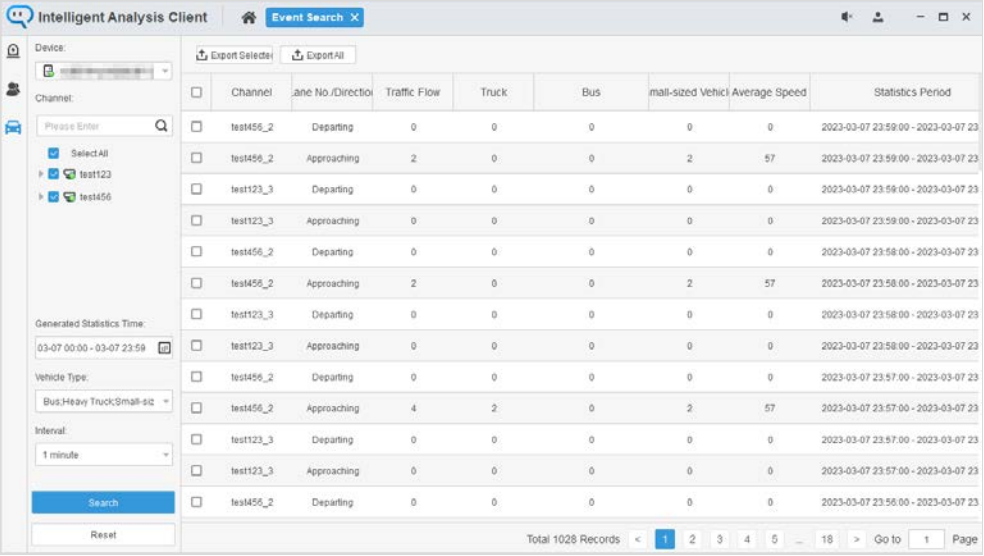
Step 3 Select at least 1 lane. You can also select multiple lanes.

Step 4 Set **Generated Statistics Time**, **Vehicle Type**. and **Interval**.

Step 5 Click **Search**.

Click **Reset** to clear all search conditions.

Figure 5-8 Traffic flow statistics



Generated Statistics Time: 03-07 00:00 - 03-07 23:59

Vehicle Type: Bus;Heavy Truck;Small-siz

Interval: 1 minute

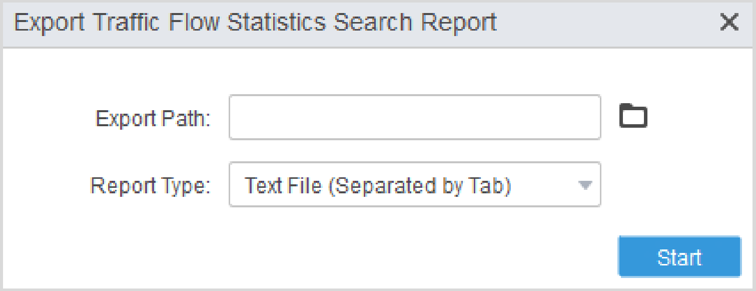
□	Channel	ane No./Directio	Traffic Flow	Truck	Bus	mall-sized Vehicl	Average Speed	Statistics Period
□	test456_2	Departing	0	0	0	0	0	2023-03-07 23:59:00 - 2023-03-07 23
□	test456_2	Approaching	2	0	0	2	57	2023-03-07 23:59:00 - 2023-03-07 23
□	test123_3	Departing	0	0	0	0	0	2023-03-07 23:59:00 - 2023-03-07 23
□	test123_3	Approaching	0	0	0	0	0	2023-03-07 23:59:00 - 2023-03-07 23
□	test456_2	Departing	0	0	0	0	0	2023-03-07 23:58:00 - 2023-03-07 23
□	test456_2	Approaching	2	0	0	2	57	2023-03-07 23:58:00 - 2023-03-07 23
□	test123_3	Departing	0	0	0	0	0	2023-03-07 23:58:00 - 2023-03-07 23
□	test123_3	Approaching	0	0	0	0	0	2023-03-07 23:58:00 - 2023-03-07 23
□	test456_2	Departing	0	0	0	0	0	2023-03-07 23:57:00 - 2023-03-07 23
□	test456_2	Approaching	4	2	0	2	57	2023-03-07 23:57:00 - 2023-03-07 23
□	test123_3	Departing	0	0	0	0	0	2023-03-07 23:57:00 - 2023-03-07 23
□	test123_3	Approaching	0	0	0	0	0	2023-03-07 23:57:00 - 2023-03-07 23
□	test456_2	Departing	0	0	0	0	0	2023-03-07 23:56:00 - 2023-03-07 23

Total 1028 Records < 1 2 3 4 5 ... 18 > Go to 1 Page

Step 6 Export traffic flow statistics.

Select the events you want, and click **Export Selected**. You can also click **Export All** to export all event information.

Figure 5-9 Export search records



Export Path:

Report Type: Text File (Separated by Tab)

- Export Path: Select the local path for exported information.
- Report Type:
  - **CSV File (separated by comma)**: The exported information includes a CSV file.
  - **Excel with image hyperlink**: The exported information includes an Excel file. Click the image and it will be linked to a large image.
  - **Text File (separated by tab)**: The exported information includes a Text file.

6 Web Operations

You can log in to the webpage to configure server settings.

6.1 Initializing Password

When you log in to the web page for the first time, you need to initialize the password. Then, you can log in to the admin account.

Procedure

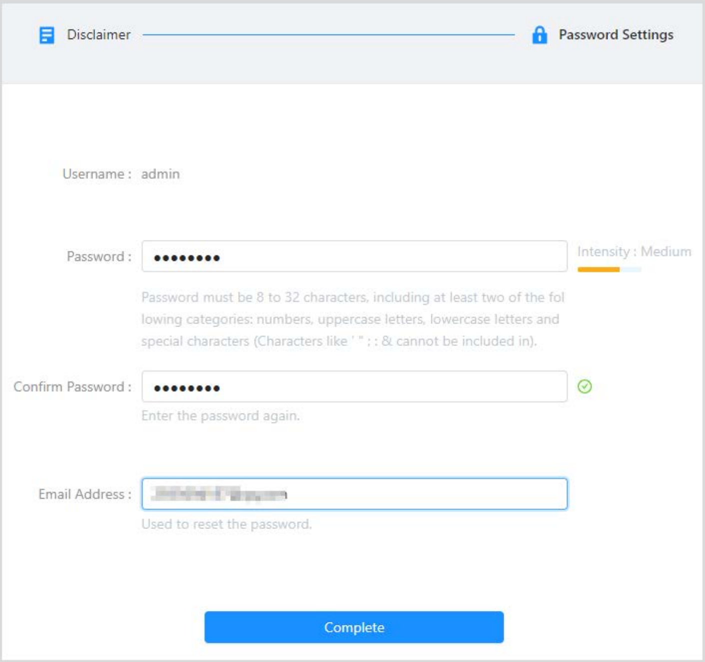
Step 1 Enter http://192.168.1.108 in the address bar of the Google Chrome.

We recommend you use Google Chrome.

Step 2 Read the **Privacy Policy** and **Software License Agreement**, and then select **I have read and agree to the terms of the Software License Agreement and Privacy Policy**. Click **Next**.

Step 3 Set a new password, confirm the password, and then enter your email address.

Figure 6-1 Initialization



Username : admin

Password : ••••••••

Intensity : Medium

Password must be 8 to 32 characters, including at least two of the fol lowing categories: numbers, uppercase letters, lowercase letters and special characters (Characters like ' " ; : & cannot be included in).

Confirm Password : ••••••••

Enter the password again.

Email Address : [redacted]

Used to reset the password.

Step 4 Click **Complete**.

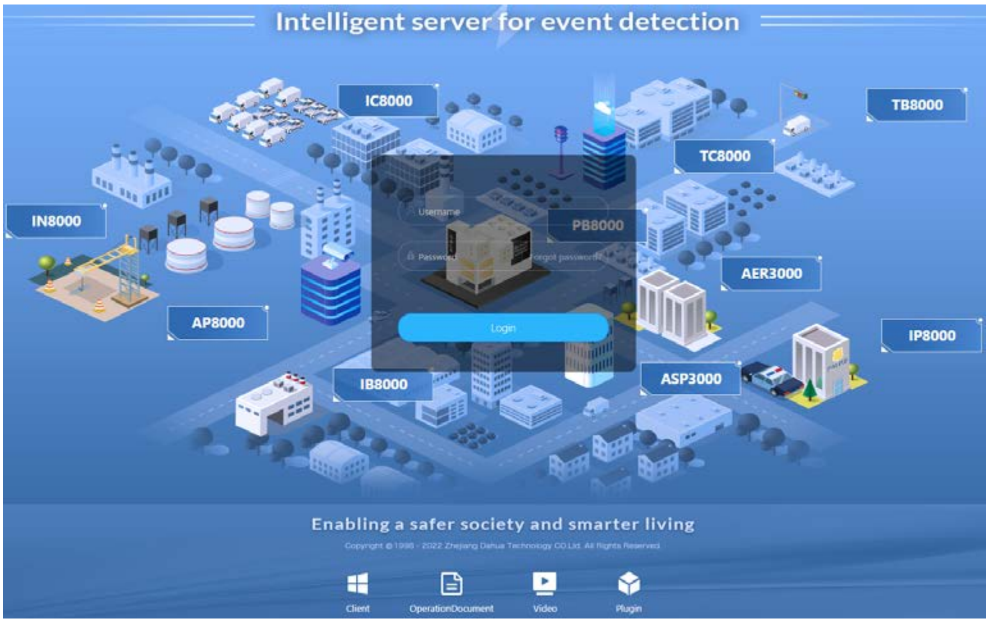
6.2 Login

Procedure

Step 1 Enter http://server IP in the address bar of Google Chrome, and then press the Enter.

Step 2 Enter the username and password, and then click **Login**.

Figure 6-2 Log in to the web page


Intelligent server for event detection
IC8000
TB8000
TC8000
IN8000
Username
Password
Forgot password?
PB8000
AER3000
AP8000
IP8000
Login
IB8000
ASP3000
Enabling a safer society and smarter living
Copyright © 1995 - 2022 Zhejiang Dahua Technology CO.Ltd. All Rights Reserved.
Client
OperationDocument
Video
Plugin

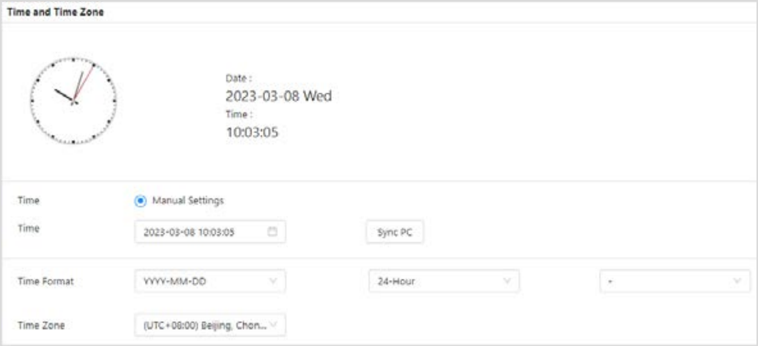
- The password is the password that you set during initialization.
- If you forget the password, click **Forgot Password?** to reset password through the email.

6.3 Setting Time

Background Information

You can set server time on the **Time and Time Zone** page.

Figure 6-3 Set time



Time and Time Zone

Date :
2023-03-08 Wed
Time :
10:03:05

Time ● Manual Settings
Time 2023-03-08 10:03:05 Sync PC
Time Format YYYY-MM-DD 24-Hour -
Time Zone (UTC+08:00) Beijing, Chon...

Table 6-1 Time setting parameters

Parameter	Description
Date and Time	The current date and time of the server.
Time	Set the current system time of the server. You can click **Sync PC** to keep the system time consistent with the time of your computer.
Time Format	The time format.

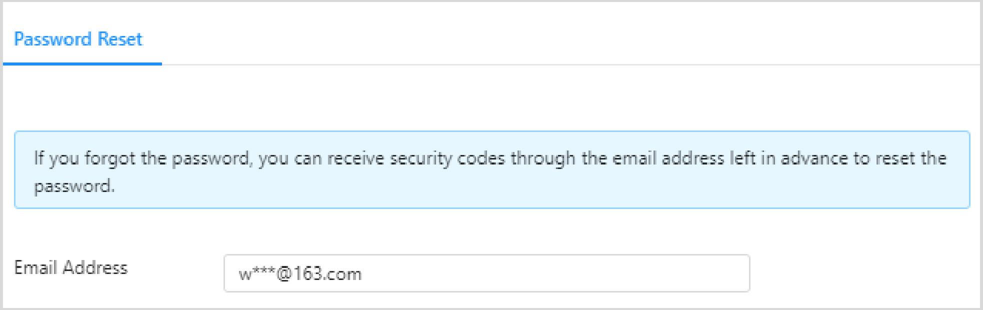
Parameter	Description
Time Zone	The time zone of the server should be consistent with the actual time zone.

6.4 Account Management

When you forget your password, you can use the email address to receive security code and reset the password.

Enter your email address, and then click **Save**.

Figure 6-4 Account management



Password Reset

If you forgot the password, you can receive security codes through the email address left in advance to reset the password.

Email Address: w***@163.com

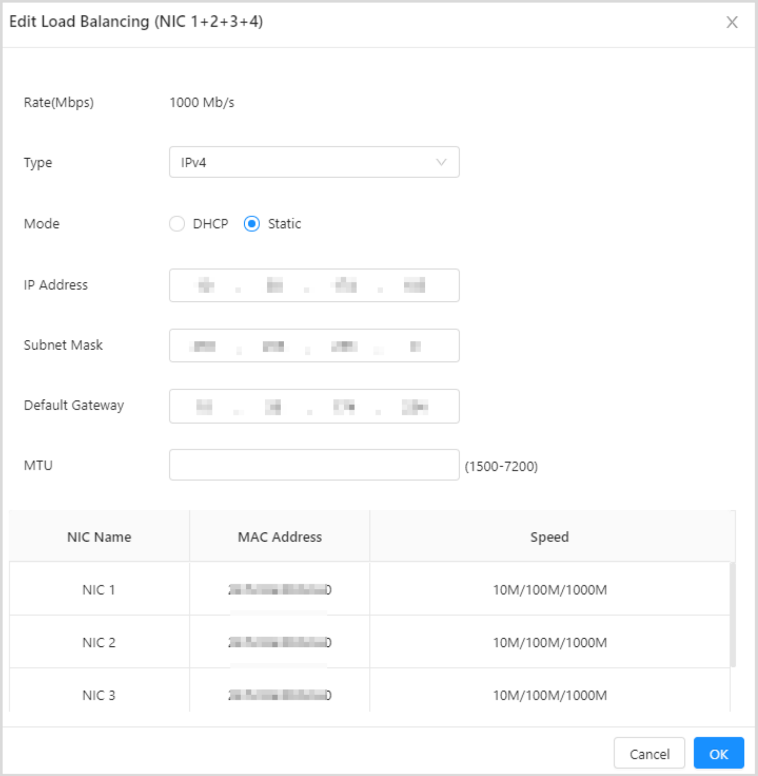
6.5 Network Configuration

6.5.1 TCP/IP

Configure network parameters of the server.

Modifying Network Adapter

Figure 6-5 Modify network adapter



Edit Load Balancing (NIC 1+2+3+4)

Rate(Mbps) 1000 Mb/s

Type IPv4

Mode ○ DHCP ● Static

IP Address [redacted]

Subnet Mask [redacted]

Default Gateway [redacted]

MTU (1500-7200)

NIC Name	MAC Address	Speed
NIC 1	[redacted]	10M/100M/1000M
NIC 2	[redacted]	10M/100M/1000M
NIC 3	[redacted]	10M/100M/1000M

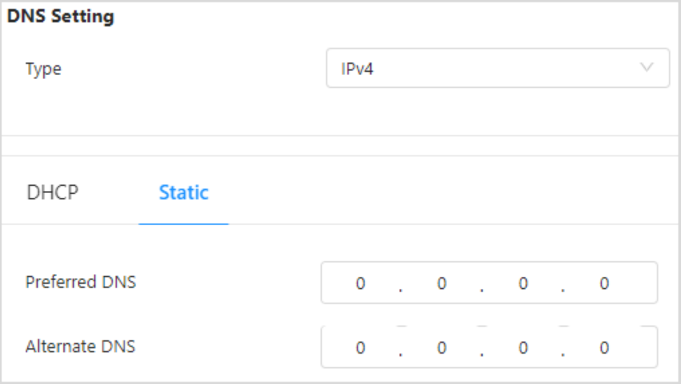
Table 6-2 Network adapter parameters

Parameter	Description
Rate(Mbps)	The speed of the network adapter.
Type	The type of the network adapter. The default type is IPv4.
Mode	● **DHCP**: Acquire IP address automatically. ● **Static**: Enter the IP address manually.
IP Address	Modify the IP address when you select **Static**.
Subnet Mask	Modify the subnet mask of the IP address when you select **Static**.
Default Gateway	Modify the default gateway of the IP address when you select **Static**.
MTU	Set the parameter according to your needed. The default value is 1500.

Setting DNS

You can set preferred or alternate DNS through DHCP, or manually set them.

Figure 6-6 Set DNS



DNS Setting

Type: IPv4

DHCP | Static

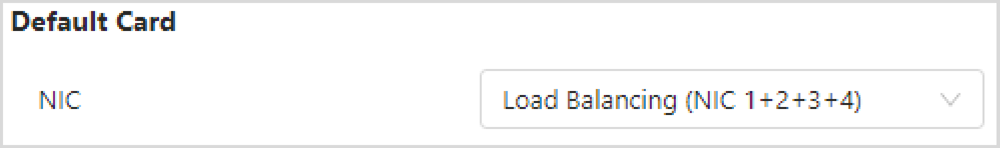
Preferred DNS: 0 . 0 . 0 . 0

Alternate DNS: 0 . 0 . 0 . 0

Default Network Adapter

The default network adapter is used for fault tolerance.

Figure 6-7 Default card



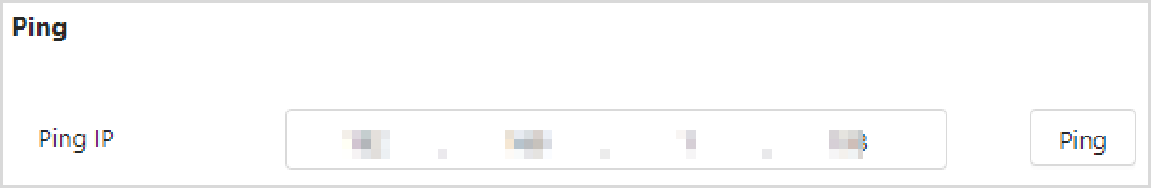
Default Card

NIC: Load Balancing (NIC 1+2+3+4)

6.5.2 Ping

Enter the IP address, and then click Ping to check the network connection.

Figure 6-8 Ping IP



Ping

Ping IP: [redacted]

6.5.3 Route Configuration

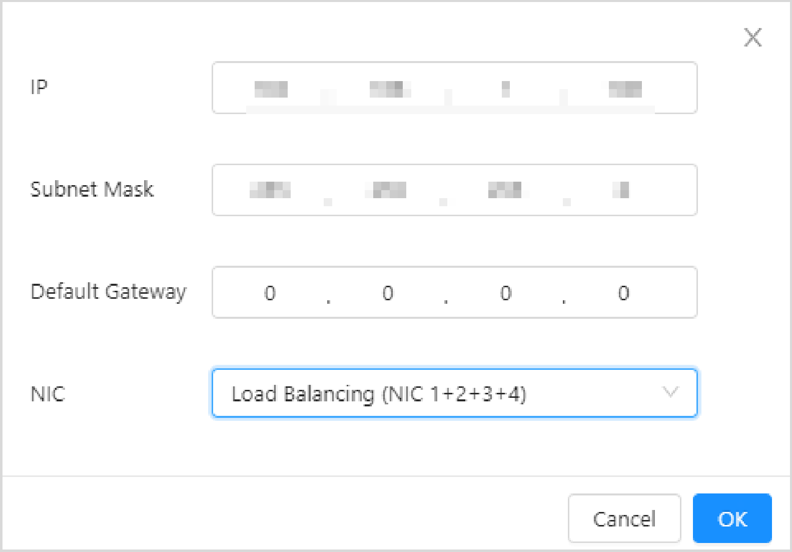
You can configure route to connect the subnet of another network segment.

Procedure

Step 1 Log in to the webpage, and then select **System Settings** > **Network Config** > **Route Config**.

Step 2 Click **Add**, and then configure the **IP**, **Subnet Mask**, **Default Gateway** and **NIC**.

Figure 6-9 Route configuration



IP: [redacted]

Subnet Mask: [redacted]

Default Gateway: 0 . 0 . 0 . 0

NIC: Load Balancing (NIC 1+2+3+4)

Step 3 Click **OK**.

6.6 Basic Configuration

You can log in to the server throng remote tool after enabling SSH and enable HTTPS can ensure the security of the data.

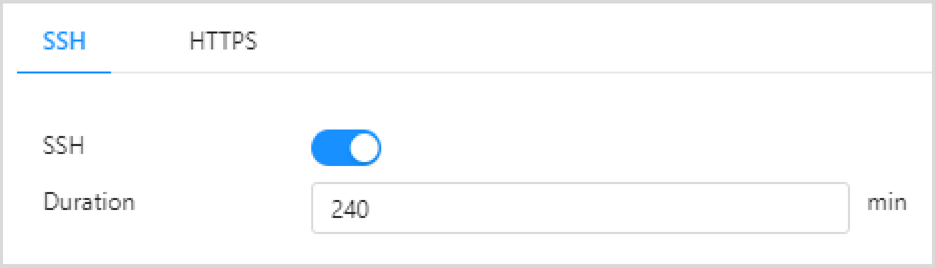
Procedure

Step 1 Log in to the webpage.

Step 2 Enable **SSH**.

1) Select **System Config** > **Basic** > **SSH**.

Figure 6-10 SSH



SSH: ●

Duration: 240 min

2) Click ○ to enable SSH.

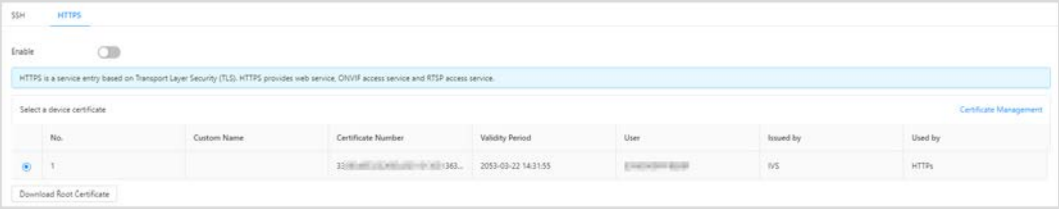
3) Set the **Duration** of SSH, and then click **Save**.

4) Enter the password of the server, and then click **OK**.

Step 3 Enable **HTTPS**.

1) Select **System Config** > **Basic** > **HTTPS**.

Figure 6-11 HTTPS



Enable ○

HTTPS is a service entry based on Transport Layer Security (TLS). HTTPS provides web service, ONVIF access service and RTSP access service.

Select a device certificate

	No.	Custom Name	Certificate Number	Validity Period	User	Issued by	Used by
●	1		33[redacted]363...	2053-03-22 14:31:55	[redacted]	IVS	HTTPs

2) Click to enable HTTPS.
3) Click **Save**.
4) Enter the password of the server, and then click **OK**.

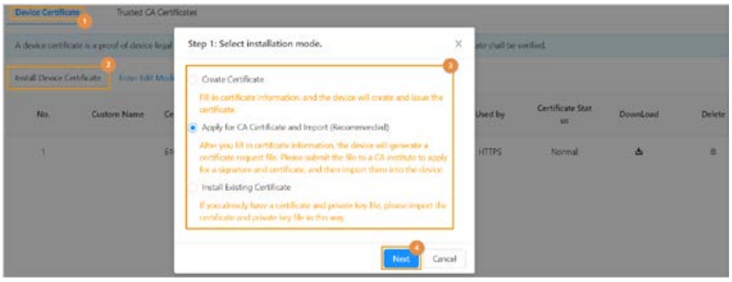
6.7 Installing CA Certificate

Install device certificate and CA certificate.

Installing Device Certificate

Log in to the WEB, select **System Settings** > **CA Certificate** > **Device Certificate**. Click **Install Device Certificate**, and then install device certificate according to the instructions.

Figure 6-12 Install device certificate



Step 1: Select installation mode.

○ Create Certificate

Fill in certificate information, and the device will create and issue the certificate.

● Apply for CA Certificate and Import (Recommended)

After you fill in certificate information, the device will generate a certificate request file. Please submit the file to a CA institute to apply for a signature and certificate, and then import them into the device.

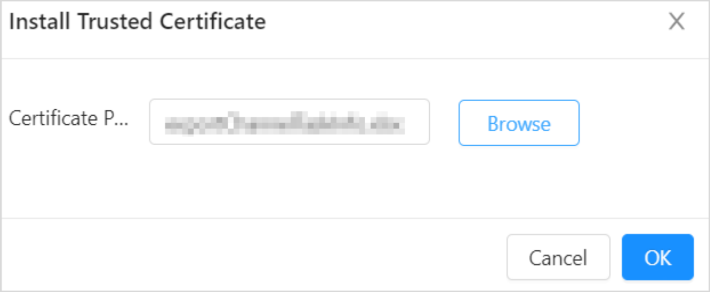
○ Install Existing Certificate

If you already have a certificate and private key file, please import the certificate and private key file in this way.

Installing Trusted CA Certificates

Log in to the WEB, select **System Settings** > **CA Certificate** > **Trusted CA Certificates**. Click **Install Trusted CA Certificate**, and then install trusted CA certificate according to the instructions.

Figure 6-13 Install CA certificate



Install Trusted Certificate

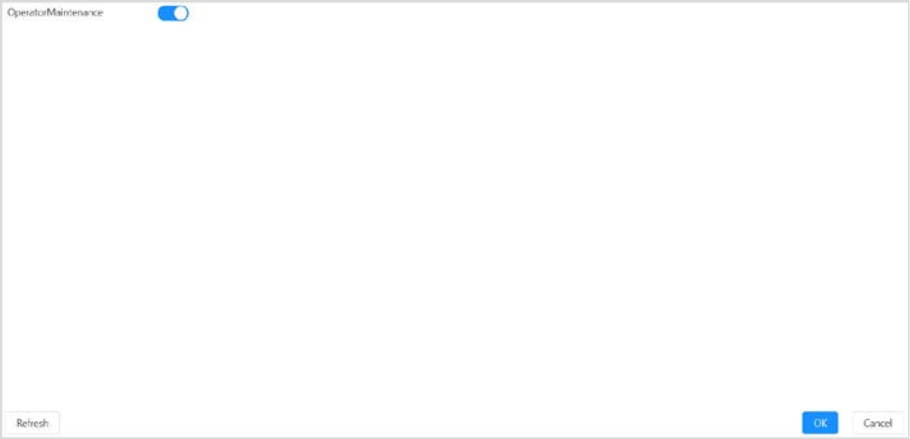
Certificate P...

6.8 Operator Maintenance Management

After enabling operator maintenance function (enabled by default), you can view the information of task delivery and experience database loading.

Operator maintenance function is enabled by default. Click to enable this function, and then click **OK**.

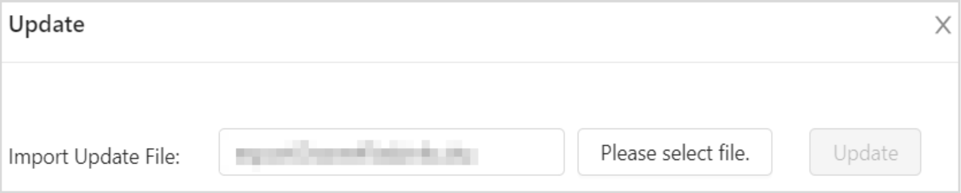
Figure 6-14 Operator maintenance



6.9 System Upgrade

Click **Upgrade**, and then select the upgrade file from your local computer. Click **Update** to upgrade the system.

Figure 6-15 Upgrade



6.10 Version Information

Click **Version** to view system version and security baseline version.

6.11 Legal Information

Click **Legal Info** to view **Software License Agreement**, **Open Source Software Notice** and **Privacy Policy**.

7 Solution Application (CyberCity)

Procedure

Step 1 Open the browser, and then enter http://*Cybercity IP address*, click **Download** to download the Client.

Step 2 Enter the IP address, port, username, password and select **English** as the language of the Client.

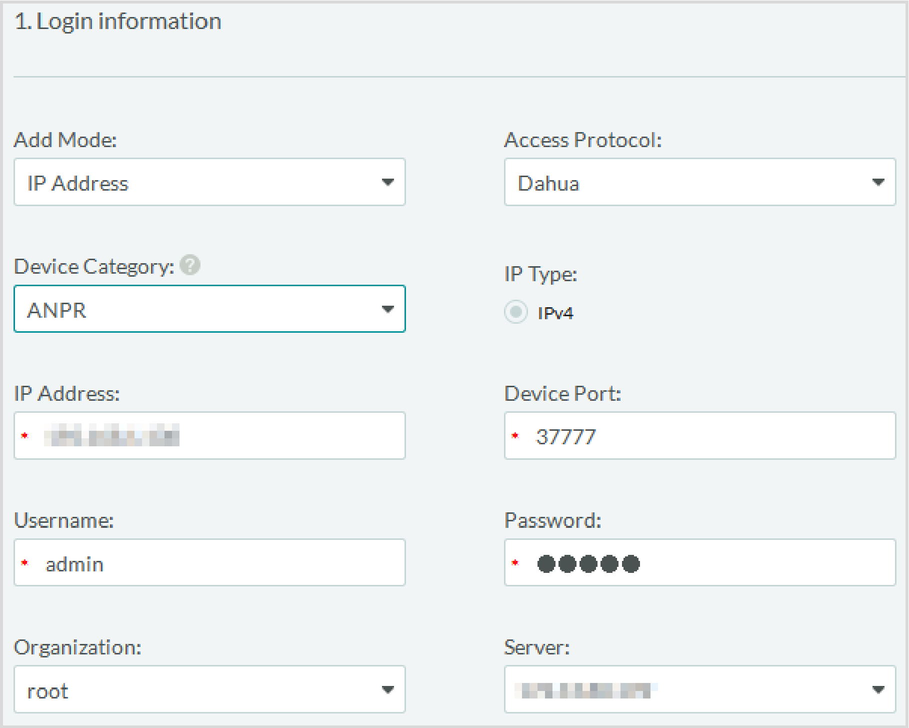
Step 3 Click **Log in**.

Step 4 On home page, select **Configuration** > **Device**, click **Add** to add TB8000-E to the platform.

1) Enter the login information, and then click **Add**.

- **Device Category**: Select ANPR.
- **IP Address**: The IP address of TB8000-E.
- **Username** and **Password**: The username and password of TB8000-E.

Figure 7-1 Login information



1. Login information

Add Mode: IP Address

Access Protocol: Dahua

Device Category: ANPR

IP Type: ● IPv4

IP Address: * [redacted]

Device Port: * 37777

Username: * admin

Password: * ●●●●●

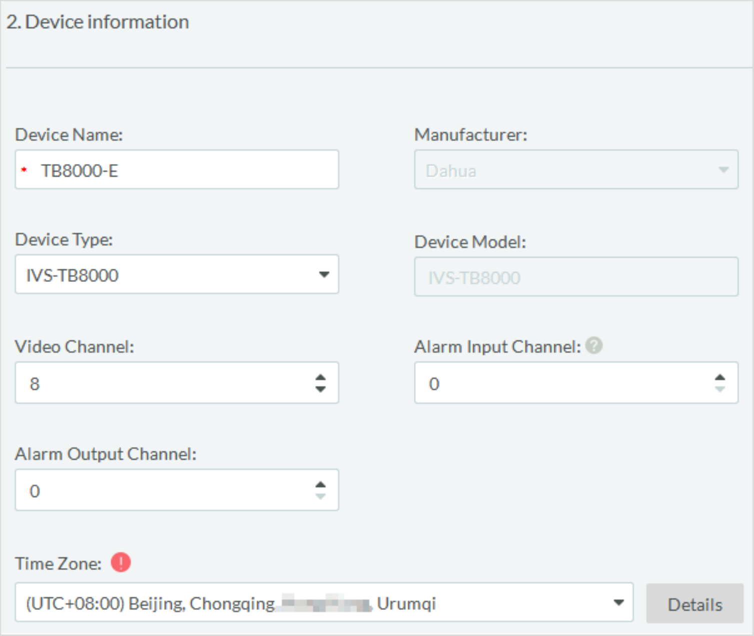
Organization: root

Server: [redacted]

2) Enter the device information, and then click **OK**.

- **Device Name**: Enter the device name to differentiate it from others.
- **Device Type**: Select IVS-TB8000.
- Enter the number of video channel.
- Select the **Time Zone**.

Figure 7-2 Device Information



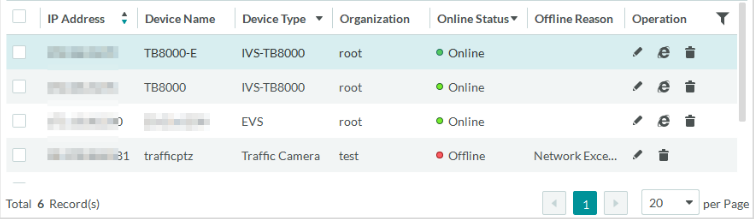
2. Device information

Device Name: * TB8000-E	Manufacturer: Dahua
Device Type: IVS-TB8000	Device Model: IVS-TB8000
Video Channel: 8	Alarm Input Channel: 0
Alarm Output Channel: 0	

Time Zone: (UTC+08:00) Beijing, Chongqing [redacted] Urumqi

If the added device displays online, it means that the device is added successfully.

Figure 7-3 Added successfully



□	IP Address	Device Name	Device Type	Organization	Online Status	Offline Reason	Operation
□	[redacted]	TB8000-E	IVS-TB8000	root	● Online		
□	[redacted]	TB8000	IVS-TB8000	root	● Online		
□	[redacted]0	[redacted]	EVS	root	● Online		
□	[redacted]31	trafficptz	Traffic Camera	test	● Offline	Network Exce...	

Total 6 Record(s)

Step 5 View alarm information.

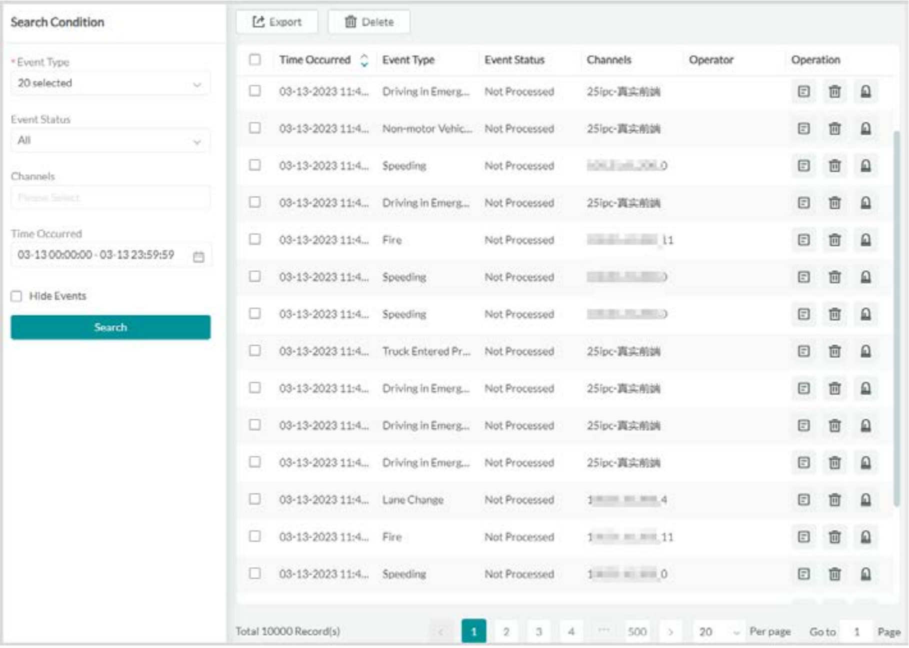
1) On home page, select **Application** > **Road Event**.

2) Set search conditions, and then click **Search**.

Select **Hide Events** to display the hidden events.

The results will be displayed on the left and you can view the detailed information, delete the records or export the alarm records. For details, see the Cyber City user's manual.

Figure 7-4 Search results



Search Condition

* Event Type

20 selected

Event Status

All

Channels

Please Select

Time Occurred

03-13 00:00:00 - 03-13 23:59:59

□ Hide Events

Search

Export   Delete

□	Time Occurred	Event Type	Event Status	Channels	Operator	Operation
□	03-13-2023 11:4...	Driving in Emerg...	Not Processed	25ipc-真实前端		
□	03-13-2023 11:4...	Non-motor Vehic...	Not Processed	25ipc-真实前端		
□	03-13-2023 11:4...	Speeding	Not Processed	[redacted]0		
□	03-13-2023 11:4...	Driving in Emerg...	Not Processed	25ipc-真实前端		
□	03-13-2023 11:4...	Fire	Not Processed	[redacted]11		
□	03-13-2023 11:4...	Speeding	Not Processed	[redacted])		
□	03-13-2023 11:4...	Speeding	Not Processed	[redacted])		
□	03-13-2023 11:4...	Truck Entered Pr...	Not Processed	25ipc-真实前端		
□	03-13-2023 11:4...	Driving in Emerg...	Not Processed	25ipc-真实前端		
□	03-13-2023 11:4...	Driving in Emerg...	Not Processed	25ipc-真实前端		
□	03-13-2023 11:4...	Driving in Emerg...	Not Processed	25ipc-真实前端		
□	03-13-2023 11:4...	Lane Change	Not Processed	1[redacted]4		
□	03-13-2023 11:4...	Fire	Not Processed	1[redacted]11		
□	03-13-2023 11:4...	Speeding	Not Processed	1[redacted]0		

Total 10000 Record(s)   < 1 2 3 4 ··· 500 >   20 Per page   Go to 1 Page

Appendix 1 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations from Dahua on how to create a more secured security system.

Mandatory actions to be taken for basic device network security:

1. **Use Strong Passwords**

   Please refer to the following suggestions to set passwords:

   - The length should not be less than 8 characters.
   - Include at least two types of characters; character types include upper and lower case letters, numbers and symbols.
   - Do not contain the account name or the account name in reverse order.
   - Do not use continuous characters, such as 123, abc, etc.
   - Do not use overlapped characters, such as 111, aaa, etc.

2. **Update Firmware and Client Software in Time**

   - According to the standard procedure in Tech-industry, we recommend to keep your device (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the device is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
   - We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your device network security:

1. **Physical Protection**

   We suggest that you perform physical protection to device, especially storage devices. For example, place the device in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable device (such as USB flash disk, serial port), etc.

2. **Change Passwords Regularly**

   We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. **Set and Update Passwords Reset Information Timely**

   The device supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4. **Enable Account Lock**

   The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

5. **Change Default HTTP and Other Service Ports**

   We suggest you to change default HTTP and other service ports into any set of numbers between

1024–65535, reducing the risk of outsiders being able to guess which ports you are using.

6. **Enable HTTPS**

   We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. **MAC Address Binding**

   We recommend you to bind the IP and MAC address of the gateway to the device, thus reducing the risk of ARP spoofing.

8. **Assign Accounts and Privileges Reasonably**

   According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

9. **Disable Unnecessary Services and Choose Secure Modes**

   If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

   If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:

   - SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
   - SMTP: Choose TLS to access mailbox server.
   - FTP: Choose SFTP, and set up strong passwords.
   - AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

10. **Audio and Video Encrypted Transmission**

    If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

    Reminder: encrypted transmission will cause some loss in transmission efficiency.

11. **Secure Auditing**

    - Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
    - Check device log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

12. **Network Log**

    Due to the limited storage capacity of the device, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

13. **Construct a Safe Network Environment**

    In order to better ensure the safety of device and reduce potential cyber risks, we recommend:

    - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
    - The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
    - Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
    - Enable IP/MAC address filtering function to limit the range of hosts allowed to access the

device.

More information

Please visit Dahua official website security emergency response center for security announcements and the latest security recommendations.

ENABLING A SAFER SOCIETY AND SMARTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.
Address: No. 1399, Binxing Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053
Email: dhoverseas@dhvisiontech.com | Tel: +86-571-87688888 28933188