



# Intelligent Server for Public Event Detection

## User's Manual



# Foreword

## General






This manual introduces the functions and operations of the Event Detection Intelligent Server (hereinafter referred to as "the Server").

## Models

Device	Model
1U	DH-IVS-IP8000-E-GU1
2U	DH-IVS-IP8000-2E-GU2, DH-IVS-IP8000-3E-GU2, DH-IVS-IP8000-4E-GU2, DH-IVS-IP8000-5E-GU2, and DH-IVS-IP8000-6E-GU2

## Safety Instructions

The following signal words might appear in the manual.

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

## Revision History

Revision Content	Release Time	Revision Content
V1.0.0	First Release.	November 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, comply with the guidelines when using it, and keep the manual safe for future reference.

## Transportation Requirements



Transport the server under allowed humidity and temperature conditions.

## Storage Requirements



Store the server under allowed humidity and temperature conditions.

## Installation Requirements



- 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



- 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



- 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

Foreword .....	I
Important Safeguards and Warnings.....	III
1 Overview .....	1
1.1 Introduction .....	1
1.2 Functions .....	1
1.3 Structure .....	5
1.3.1 1U.....	5
1.3.2 2U.....	7
1.4 Networking Diagram .....	9
2 Cable Connection .....	11
3 Installing Client .....	12
4 Client Operation.....	14
4.1 Logging in to Client .....	14
4.2 System Configuration .....	14
4.3 Device Management .....	15
4.3.1 Adding Devices .....	15
4.3.2 Managing Remote Devices .....	18
4.4 Intelligent Video Analysis .....	21
4.4.1 Enabling Smart Plan .....	21
4.4.2 IVS Rules .....	22
4.4.2.1 Tripwire Detection .....	22
4.4.2.2 Intrusion Detection.....	24
4.4.2.3 Climbing Detection.....	28
4.4.2.4 Getting up Detection .....	29
4.4.2.5 Staying (Loitering) Detection .....	31
4.4.2.6 Sleep Detection.....	33
4.4.2.7 Abnormal Number of People Detection .....	36
4.4.2.8 Abnormal Sound Detection.....	39
4.4.2.9 Fight Detection .....	42
4.4.2.10 Staying Alone Detection.....	44
4.4.2.11 Crowd Gathering Detection.....	46
4.4.2.12 Object Detection.....	48
4.4.2.13 Call Detection.....	51
4.4.2.14 Using Mobile Phone Detection.....	53
4.4.2.15 Fall Detection .....	56

---

4.4.2.16 Running Detection .....	58
4.4.2.17 Smoking Detection.....	60
4.4.2.18 Sleeping with Quilt Covering Head Detection .....	63
4.4.2.19 Posture Detection .....	65
4.4.3 Video Quality Diagnosis.....	67
4.4.4 (Optional) Target Filter .....	68
4.5 Real-time Monitoring .....	70
4.6 Searching for Alarm Information.....	72
Appendix 1 Cybersecurity Recommendations.....	74

# 1 Overview


## 1.1 Introduction

The intelligent event detection server is a device that automatically analyzes video surveillance images and extracts key information from the video source to identify and distinguish objects. It makes judgments based on custom event types and triggers alarms once abnormal behaviors or unexpected events are detected, turning video surveillance from track back after the event to early warning before the event. You can discover potential security hazards in time and effectively avoid property loss and injury to personnel. The device also reduces the work intensity of personnel and surveillance vulnerabilities caused by visual fatigue, allowing personnel to more effectively deal with crises and minimize the generalization of false alarms and missed alarms.

The server fully meets the many requirements of the security system, catering to both indoor and outdoor scenarios. For indoor scenarios, it is applicable to detention centers, interrogation rooms, and more. For outdoor scenarios, it is ideal for use outside the room, around the fence of the detention center, and more.

## 1.2 Functions

Table 1-1 Function description


Functions	Description
Intelligent Analysis	Rule types include the detection of tripwire, intrusion, climbing, getting up, staying (loitering), sleep, abnormal number of people, abnormal sound, fight, staying alone, crowd gathering, object, call, using mobile phone, fall, running, smoking, sleeping with quilt covering head, posture (head on wall), and video quality diagnosis.
Analysis Capability	<ul style="list-style-type: none"> <li>• More analysis cards represent greater video analysis capabilities.</li> <li>• Each channel of video can be configured with up to 10 identical or different AI rules.</li> </ul>  <p>For object detection, each channel supports no more than four AI rules.</p>
Access Ability	<ul style="list-style-type: none"> <li>• Video access analysis of IP cameras through ONVIF, Dahua, and Hikvision protocols.</li> <li>• Video access analysis of IP cameras with H.264, H.265, or MPEG4 stream.</li> </ul>
Batch Import or Export of AI Rules	<ul style="list-style-type: none"> <li>• For typical monitoring scenarios, multiple AI rules can be exported and saved.</li> <li>• Import configured rules into other channels for quick arming.</li> </ul>



Functions	Description
Alarm Information Search	<ul style="list-style-type: none"> <li>• Store alarm information, including monitoring point, time, detection channel, alarm event type, and alarm event snapshot.</li> <li>• Search for alarm information by multiple video channels or periods (closed intervals).</li> <li>• Generate a report on all or a selection of the search results.</li> </ul>

Table 1-2 Description of intelligent analysis

Functions	Description
Tripwire Detection	<ul style="list-style-type: none"> <li>• Set the detection line as a polyline with an arbitrary shape.</li> <li>• Specify the direction of illegal crossing for each detection line.</li> <li>• Set the target trigger position (the upper, lower, left and right sides and center point of the target box. It is set as the center point by default.).</li> <li>• An alarm is triggered when a target crosses the detection line.</li> <li>• The system recognizes the attributes of police uniforms. You can enable intelligent configuration and configure whether to trigger alarm at the client.</li> </ul>
Intrusion Detection	<ul style="list-style-type: none"> <li>• Set the detection area as a polygon with an arbitrary shape.</li> <li>• For each detection area, behavior detection can be set as crossing the area, inside the area or both.</li> <li>• For inside the area detection, the number of targets, minimum duration, and interval between repeated alarms can be set.</li> <li>• For targets crossing the area, the crossing direction can be set as entry, exit, or entry and exit.</li> <li>• An alarm is triggered when a target enters or exits the detection area.</li> <li>• The system recognizes the attributes of police uniforms. You can enable intelligent configuration and configure whether to trigger alarm at the client.</li> </ul>
Climbing Detection	<ul style="list-style-type: none"> <li>• Set the detection line as a polyline with an arbitrary shape.</li> <li>• An alarm is triggered when any part of the body below the head crosses the height detection line.</li> <li>• Set the minimum duration with any value ranging from 0 seconds to 600 seconds.</li> </ul>
Getting up detection	<ul style="list-style-type: none"> <li>• Set a rectangular area for detecting getting up behavior.</li> <li>• Set the detection line and sleep direction line (from head to feet) for each detection area.</li> <li>• Scenario requirement: The bed should be perpendicular to the monitoring direction of the camera.</li> <li>• Only supports single-layer beds. Bunks beds are not supported at this time.</li> <li>• An alarm is triggered when the target gets up during arming.</li> </ul>

Functions	Description
Stay Detection	<ul style="list-style-type: none"> <li>Set the detection area as a polygon with an arbitrary shape.</li> <li>Set the minimum duration and report interval. Minimum duration: 1 s–60 s; report interval: 1 s–600 s.</li> <li>An alarm is triggered when the stay (loitering) duration exceeds the defined time for the specified area.</li> </ul>
Sleep Detection	<ul style="list-style-type: none"> <li>Set the detection area as a polygon with an arbitrary shape.</li> <li>Set the minimum duration and report interval. Minimum duration: 1 s–3600 s; report interval: 1 s–3600 s.</li> <li>An alarm is triggered when an on-duty personnel stays still or lies down on a table for longer than the set time.</li> </ul>
People No. Error Detection	<ul style="list-style-type: none"> <li>Set the detection area as a polygon with an arbitrary shape.</li> <li>Set the minimum duration and report interval. Minimum duration: 1 s–60 s; report interval: 1 s–60 s.</li> <li>Configure detection modes to: 1. Report when people number is equal to, not equal to, greater than or less than the threshold. 2. Report when people number is within the range (including the boundary value) or falls outside the range (excluding the boundary value). 3. Report on the number of people in an area in real-time.</li> </ul>  <p>When the detection mode is reported with the real-time people number in the area, the real-time people number will appear on the left side.</p>
Loudness Detection	<ul style="list-style-type: none"> <li>After configuring this rule, the client displays the decibel value of the sound intensity on the video channel in real-time.</li> <li>Set the decibel value threshold and the duration for triggering alarms.</li> <li>An alarm is triggered when the sound intensity is greater than the defined value (1 dB–150 dB) and the sound lasts for the minimum duration (0 s–30 s).</li> </ul>
Fighting detection	<ul style="list-style-type: none"> <li>Set the detection area to a polygon with an arbitrary shape. You can only set one detection area and one fight rule per video channel.</li> <li>1U server supports 16-channel fight detection analysis, overlaid analysis of fight detection and other rules.</li> <li>Set the detection sensitivity as a value from 1 to 10. It is 7 by default.</li> </ul>
Staying Alone Detection	<ul style="list-style-type: none"> <li>Set the detection area as a polygon with an arbitrary shape.</li> <li>Staying alone alarm can be triggered for each detection area.</li> <li>Set the minimum duration and alarm interval. Duration: 1 s–1,200 s; alarm interval: 1 s–600 s.</li> </ul>
Crowd Gathering Detection	<ul style="list-style-type: none"> <li>An alarm is triggered when the duration of crowd gathering in the detection area exceeds the defined time.</li> <li>Set the detection area as a polygon with an arbitrary shape.</li> <li>Set the minimum duration and alarm interval. Duration: 1 s–300 s; alarm interval: 1 s–300 s.</li> <li>Set the sensitivity from 1 to 10.</li> </ul>


Functions	Description
Object Detection	<ul style="list-style-type: none"> <li>● Set the detection area as a polygon with an arbitrary shape.</li> <li>● An alarm is triggered when suspicious objects are left in key detection areas or are moved for longer than the minimum duration time.</li> <li>● Set the minimum duration time from 6 to 3600 seconds.</li> </ul>
Call Detection	<ul style="list-style-type: none"> <li>● Set the detection area as a polygon with an arbitrary shape.</li> <li>● An alarm is triggered when the behavior is detected to last longer than the defined minimum duration.</li> <li>● Set the minimum duration and alarm interval. Minimum duration: 1 s–600 s; alarm interval: 0 s–600 s.</li> <li>● Set the sensitivity from 1 to 10. It is 5 by default.</li> </ul>
Using Mobile Phone Detection	<ul style="list-style-type: none"> <li>● Set the detection area as a polygon with an arbitrary shape.</li> <li>● An alarm is triggered when the behavior is detected to last longer than the defined minimum duration.</li> <li>● Set the minimum duration and alarm interval. Minimum duration: 1 s–600 s; alarm interval: 0 s–600 s.</li> <li>● Set the sensitivity from 1 to 10. It is 5 by default.</li> </ul>
Fall Detection	<ul style="list-style-type: none"> <li>● Set the detection area as a polygon with an arbitrary shape.</li> <li>● Detect squatting or falling. Falling and squatting are selected by default. The check mark on falling cannot be removed.</li> <li>● Set the minimum duration and alarm interval. Minimum duration: 1 s–600 s; alarm interval: 0 s–600 s.</li> <li>● Set the sensitivity from 1 to 10. It is 5 by default.</li> </ul>
Running Detection	<ul style="list-style-type: none"> <li>● Set the detection area as a polygon with an arbitrary shape.</li> <li>● Set the sensitivity from 1 to 10. It is 5 by default.</li> </ul>
Smoking Detection	<ul style="list-style-type: none"> <li>● Set the detection area as a polygon with an arbitrary shape (only one detection area and one smoking detection rule can be configured).</li> <li>● 1U server supports 16-channel smoking detection analysis, overlaid analysis of smoking detection and other rules.</li> <li>● An alarm is triggered when the behavior is lasted for longer than the defined time.</li> <li>● Set the minimum duration and alarm interval. Minimum duration: 1 s–600 s. It is 30 s by default. Alarm interval ranges from 0 to 600 seconds. It is set as 0 by default.</li> <li>● Set the sensitivity from 1 to 10. It is 5 by default.</li> </ul>
Sleeping with Quilt Covering Head	<ul style="list-style-type: none"> <li>● Set the detection area as a polygon with an arbitrary shape.</li> <li>● An alarm is triggered when the person under supervision is detected to sleep with their head covered for longer than the defined time.</li> <li>● Set the minimum duration and alarm interval. Minimum duration: 1 s–600 s, and it is 10 seconds by default. The alarm interval ranges from 0 to 600 seconds, and it is 0 by default.</li> </ul>

Functions	Description
Posture Detection	<ul style="list-style-type: none"> <li>Set the detection area as a polygon with an arbitrary shape.</li> <li>An alarm is triggered when a person is detected to hit their head on a wall.</li> <li>Set the minimum duration and alarm interval. Minimum duration: 1 s–600 s. It is 5 seconds by default. The alarm interval ranges from 0 to 600 seconds. It is set as 0 by default.</li> </ul>
Video Quality Diagnosis	<ul style="list-style-type: none"> <li>Provides video quality diagnosis and analyzes the duration of each channel with a range of 25 s-60 s. It is 30 s by default.</li> <li>Enables or disables analysis, and analyzes a channel each time.</li> <li>Set the alarm threshold.</li> </ul>

Table 1-3 Description of analysis capacities (1)

Server	Model	Description
1U	DH-IVS-IP8000-E-GU1	<ul style="list-style-type: none"> <li>32-channel 1080p real-time video stream analysis.</li> <li>Each channel of video can be configured with up to 10 identical or different AI rules.</li> </ul>

Table 1-4 Description of analysis capacities (2)

Server	Model	Description
2U	DH-IVS-IP8000-xE-GU2  x = 2, 3, 4, 5, 6	<ul style="list-style-type: none"> <li>32-channel 1080p real-time video stream analysis for each card.</li> <li>Each channel of video can be configured with up to 10 identical or different AI rules.</li> </ul>

## 1.3 Structure

### 1.3.1 1U

#### Front Panel

Figure 1-1 Front Panel



Table 1-5 Front panel description

No.	Port, panel, or slot	Description
1	USB2.0	Connects to external devices such as a mouse and keyboard.

No.	Port, panel, or slot	Description
2	UID switch and indicator	<ul style="list-style-type: none"> <li>● Press to turn on the server and the indicator will switch on. You can quickly locate the server through the indicator.</li> <li>● When the server is enabled, press to disable it.</li> </ul>
3	Reset button	Press and hold it, and the server restores to its factory settings.
4	Network status indicator	<ul style="list-style-type: none"> <li>● Green flashes: Network connected.</li> <li>● Off: Network disconnected.</li> </ul>
5	System status indicator	<ul style="list-style-type: none"> <li>● Indicator is on.                             <ul style="list-style-type: none"> <li>◇ Green indicator flashing: The system runs normally.</li> <li>◇ Red indicator flashing: The system runs with a lower performance level or in the redundant state, and system failure alarms such as redundant power supply or fan failure alarms are triggered.</li> </ul> </li> <li>● Off: The system is not running.</li> </ul>
6	HDD status indicator	<ul style="list-style-type: none"> <li>● Green flashes: HDD is active.</li> <li>● Off: HDD is inactive.</li> </ul>
7	Power switch and indicator	Disconnect or connect the power supply. <ul style="list-style-type: none"> <li>● On: Powered on.</li> <li>● Off: Powered off.</li> </ul>

## Rear Panel

Figure 1-2 Rear Panel

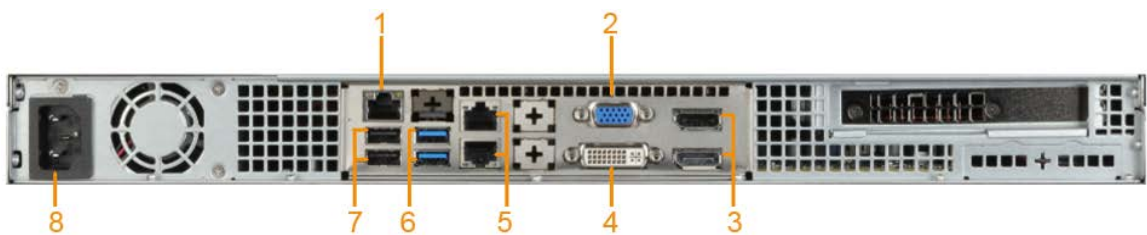


Table 1-6 Rear panel description

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








### 1.3.2 2U

#### Front Panel

Figure 1-3 Front Panel



Table 1-7 Front panel description

No.	Port/Indicator	Description
1	Power button 	Power switch. When the server is on, press and hold this button for longer than 4 seconds to turn it off.
	UID button 	UID button can be used as an indicator for easy positioning of the server. Press this button to turn on or off the indicator. <ul style="list-style-type: none"> <li>Blue indicator is on: The server is being located.</li> <li>Indicator is off: The server is not being located.</li> </ul>  Use the virtual front panel of BMC to remotely turn on or off the indicator. For details, see the instructions.
	Reset button 	Restart the server.
2	Power indicator 	It indicates the power status. <ul style="list-style-type: none"> <li>Blue: The server is powered on.</li> <li>Off: The server is not powered on.</li> </ul>
	System status indicator 	It indicates the running status of the server. <ul style="list-style-type: none"> <li>Green indicator flashing: The server is running.</li> <li>Indicator is off: The server is not running.</li> <li>Red indicator flashing: The server works in the degraded status, such as no fan detected or abnormal operation.</li> </ul>
	Network status indicator 1/2 	It indicates the current network status, corresponding to the left and right Ethernet ports of the rear view. <ul style="list-style-type: none"> <li>Green indicator flashing: Network connected.</li> <li>Indicator is off: The Ethernet port is not in use.</li> </ul>
3	HDD status indicator	It indicates the HDD running status. <ul style="list-style-type: none"> <li>Blue indicator light is on: HDD has been installed.</li> <li>Indicator is off: HDD has not been installed.</li> </ul>

No.	Port/Indicator	Description
	HDD read-write indicator	It indicates the HDD read-write status. <ul style="list-style-type: none"> <li>When a RAID card is not installed:                             <ul style="list-style-type: none"> <li>Green indicator flashing: HDD is in the read-write status.</li> <li>Indicator is off: HDD is not in place or failed.</li> </ul> </li> <li>When a RAID card is installed:                             <ul style="list-style-type: none"> <li>Green indicator flashing: HDD is in the read-write status.</li> <li>Indicator is off: HDD is not in place or failed.</li> </ul> </li> </ul>
	HDD failure/positioning indicator	It indicates HDD failure or HDD positioning. <ul style="list-style-type: none"> <li>The indicator does not take effect when a RAID card is not installed.</li> <li>When a RAID card is installed:                             <ul style="list-style-type: none"> <li>Red indicator is on: HDD failure is detected.</li> <li>Red indicator flashing (at a frequency of 4 Hz): HDD is being located.</li> <li>Red indicator flashing (at a frequency of 1 Hz): RAID is being restructured.</li> <li>Indicator is off: HDD is running normally or is not in the slot.</li> </ul> </li> </ul>
4	VGA port	VGA video output port outputs analog video signals and can be connected to a monitor to view the local interface of the server.
5	USB 3.0 port	Connects a mouse, keyboard, USB storage device, and more.

## Rear Panel

Figure 1-4 Rear Panel

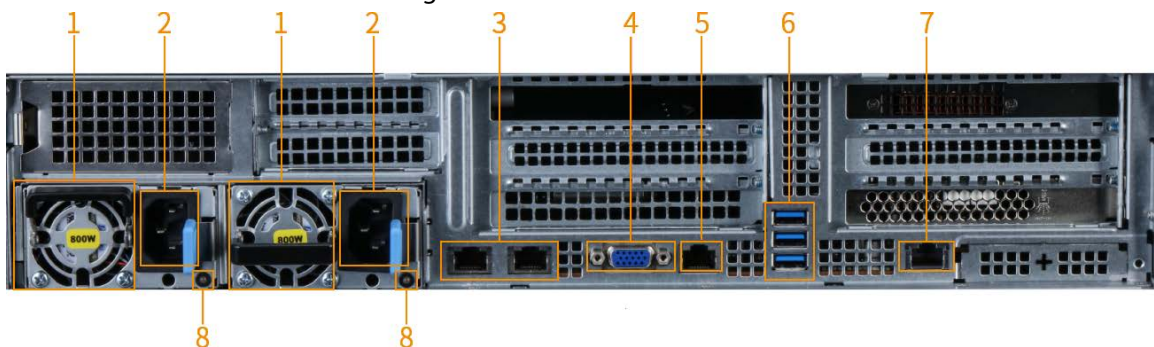




Table 1-8 Rear panel description

No.	Panel/Port/Indicator	Description
1	Fan	Used to cool the server. Fan is automatically started after power-on.
2	Power port	Connects to the power supply.
3	Network port	Two 10 Gbps Ethernet ports are connected with network cables.  The two Ethernet ports can also be used to access the BMC.

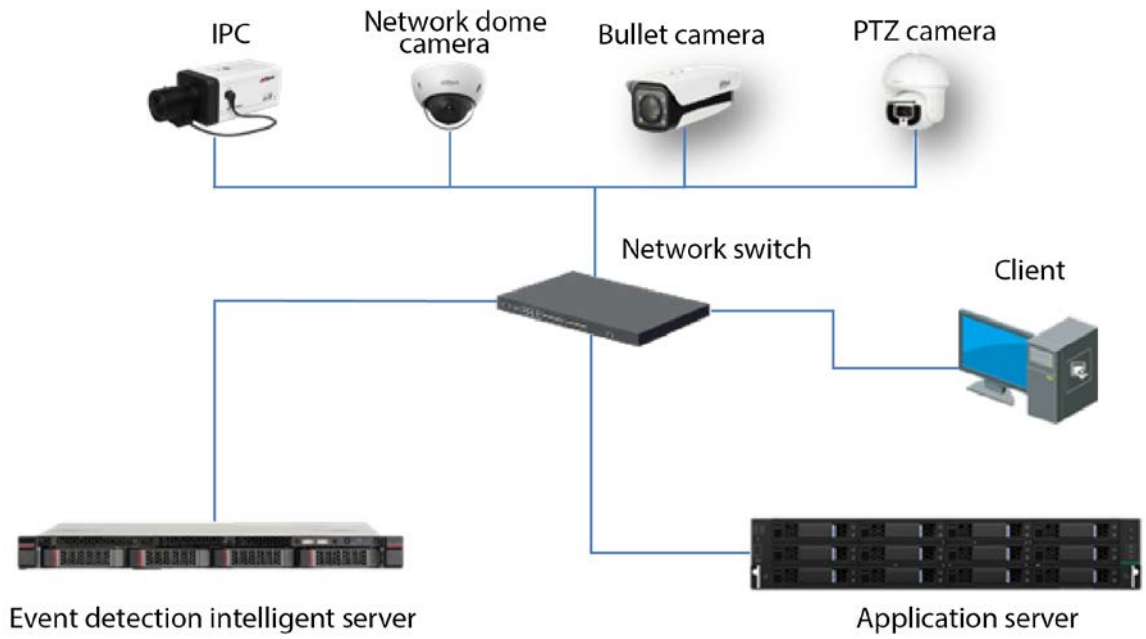
No.	Panel/Port/Indicator	Description
4	VGA port	VGA video output port outputs analog video signals and can be connected to a monitor to view the local interface of the server.
5	Serial port	Connected to the display device for debugging.
6	USB3.0 port	Connects to a mouse, keyboard, USB storage device, and more.
7	BMC management Ethernet port	<p>1000 Mbps/100 Mbps Ethernet port, only for BMC access.</p>  <p>BMC management Ethernet port is only for BMC access and cannot be used as a data Ethernet port.</p>
8	Power indicator	<ul style="list-style-type: none"> <li>Green indicator: An effective power supply has been connected and is running normally.</li> <li>Amber indicator flashing: PSU error.</li> <li>Indicator off: Power supply is not connected.</li> <li>Green indicator flashing: When updating PSU firmware, the green indicator on the PSU handle flashes.</li> <li>Green indicator flashes and then turns off: When hot swapping the PSU, the green indicator on the PSU handle is flashing at a frequency of 4 Hz, then turns off. It means that the efficiency, function group, operating conditions and supported voltages of the PSU are not matched.</li> </ul>

## 1.4 Networking Diagram

- The server is connected to the network through LAN or the Internet. Make sure that the devices in the networking are on the same network.
- The client is used for managing devices, configuring intelligent rules, and viewing alarm details and reports.
- The default IP address is 192.168.1.108, and we recommend you change it after startup. For details, see the Event Detection Intelligent Server Deployment Manual.



Figure 1-5 Typical Networking



## 2 Cable Connection

### Prerequisites

Check the Server and cables to make sure there is no obvious damage before connecting the device. Also, ensure that all cables are connected properly before powering on the Server.

### Procedure

Step 1 Connect the Server with the VGA display.

Step 2 Connect the network cable to the Server.

Step 3 Connect the power supply. You can access the Server through the network after it is powered on.



- It takes about 2 to 3 minutes to turn on the server.
- Change the IP address upon the first startup of the server.

## 3 Installing Client

### Prerequisites

- Windows 7 or Windows 10 is used for software installation.
- The PC resolution must be least 1280 × 800.
- We recommend you disable the computer firewall for normal installation and use of the software.

### Procedure

- Step 1 Double-click **Intelligent Video Analysis Client Software.exe**.  
For example: **General\_IVS-IBC\_Base\_IS\_V1.0.0.378303.R.2021-10-26.exe**.



The name of the installation file and the actual interfaces might differ depending on the version. Please be advised.

- Step 2 Select the language of the installer.  
Step 3 Select **I Agree EULA**.  
Step 4 Click **Custom** to select the installation directory.

Figure 3-1 Start installation



- Step 5 Click **Install**.

Figure 3-2 Installation completed



## 4 Client Operation

### 4.1 Logging in to Client


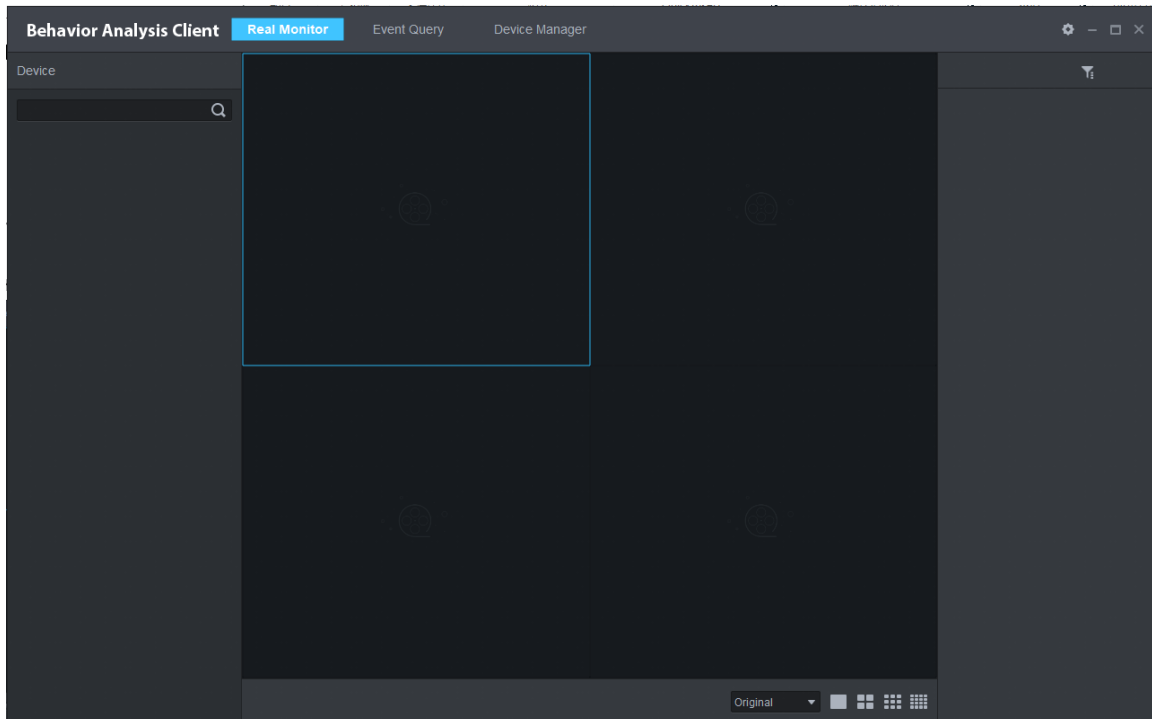
Double-click  on the desktop to open the Behavior Analysis Client.

Figure 4-1 Client homepage



### 4.2 System Configuration

View the version, built date, and the open source statement of the client. Select whether to enable **Filter Uniform Alarm**, which indicates whether uniform alarms are displayed in the real-time alarm column when alarm events occur.


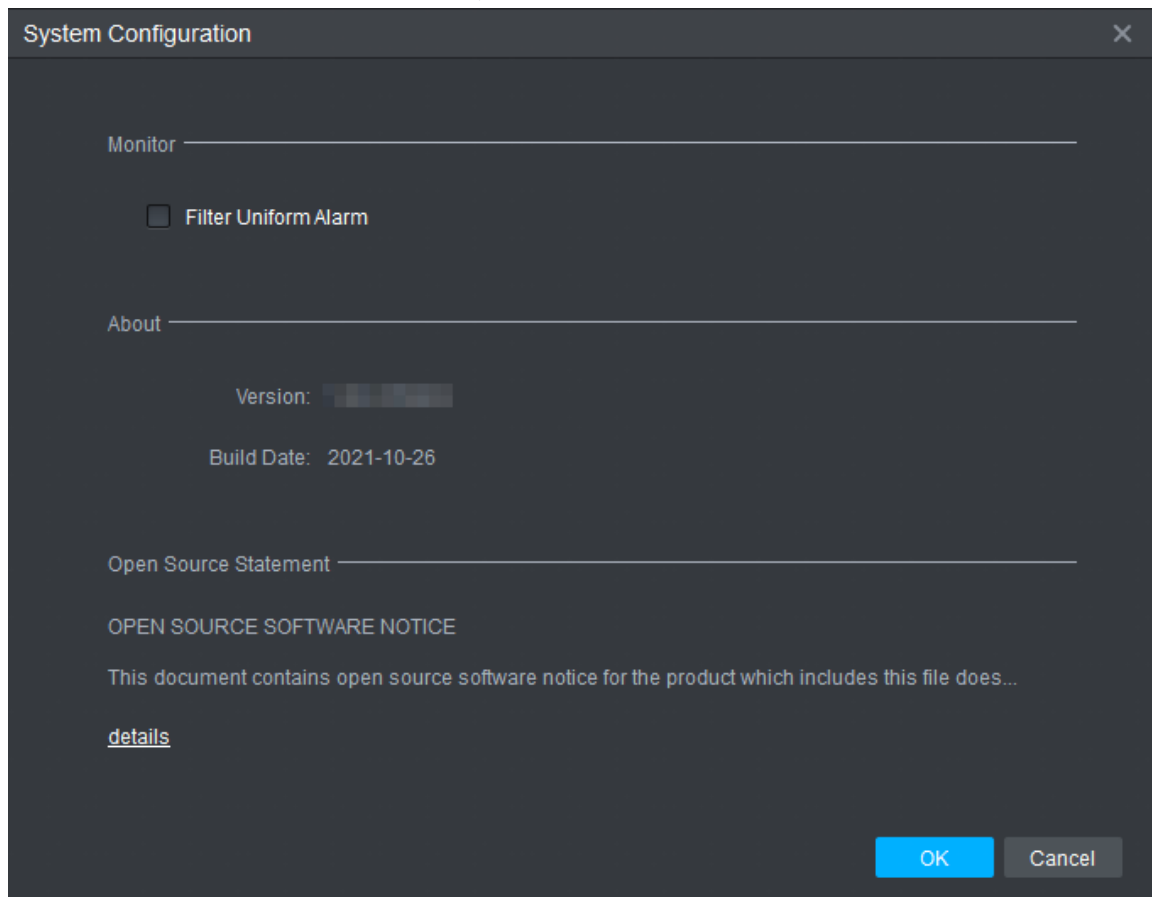
Step 1 Click  at the upper right corner.

Figure 4-2 System configuration



**Step 2** (Optional) Select **Filter Uniform Alarm**.

If **Filter Uniform Alarm** is selected, no alarm is displayed in the real-time alarm column when uniformed personnel are detected. If **Filter Uniform Alarm** is not selected, alarms are displayed in the real-time alarm column when uniformed personnel are detected.

## 4.3 Device Management

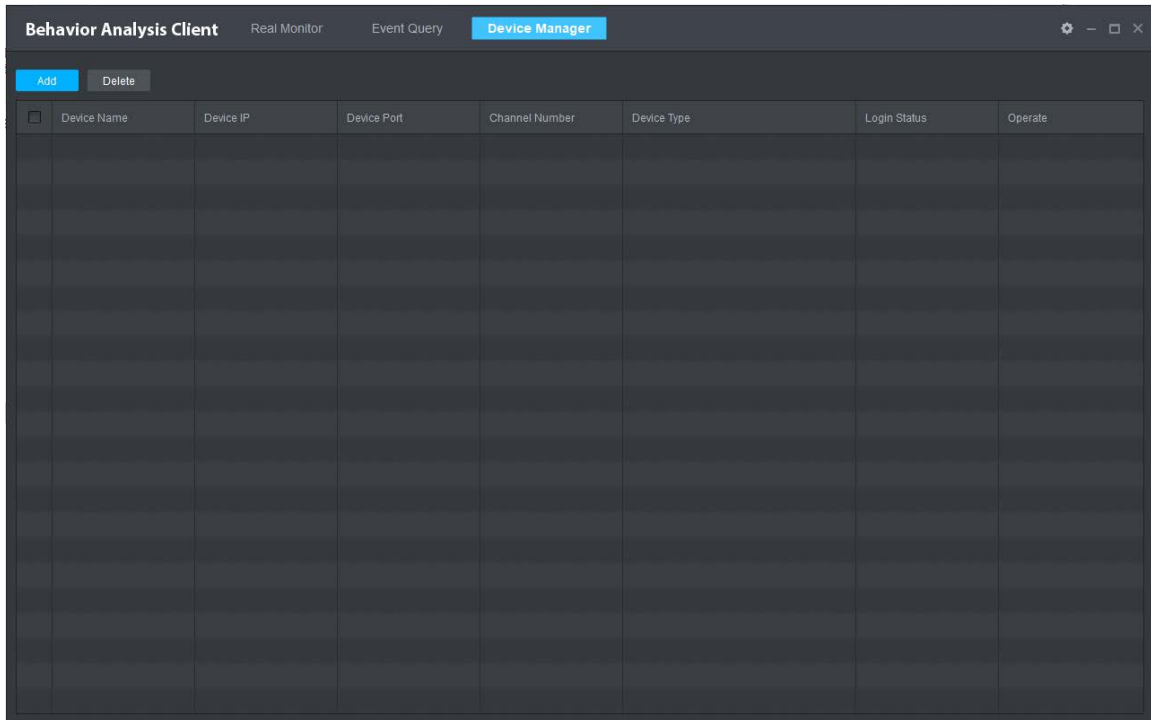
Add the server or other remote devices through the client and configure device information.

### 4.3.1 Adding Devices

#### Procedure

**Step 1** Click **Device Manager**.

Figure 4-3 Manage device



Step 2 Click **Add** to configure the parameters.

Figure 4-4 Add device

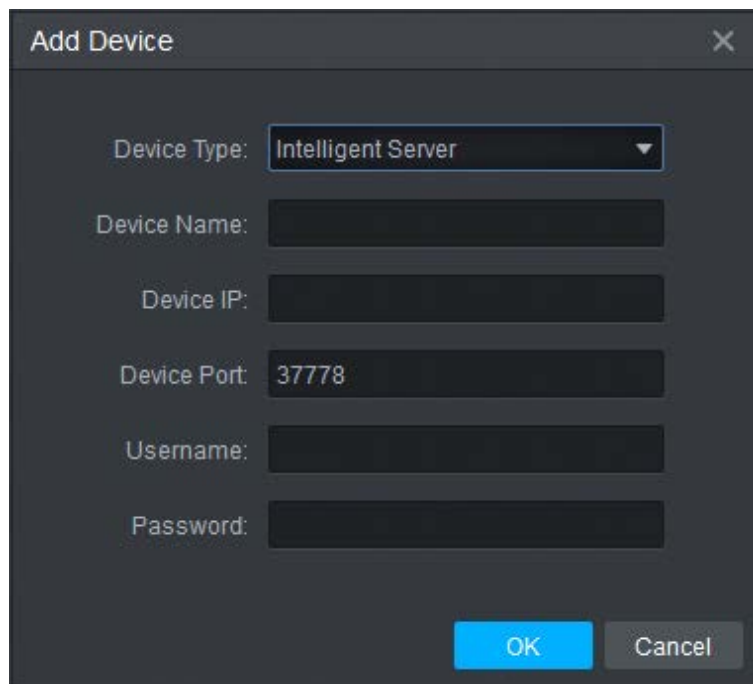


Table 4-1 Description of adding device parameters

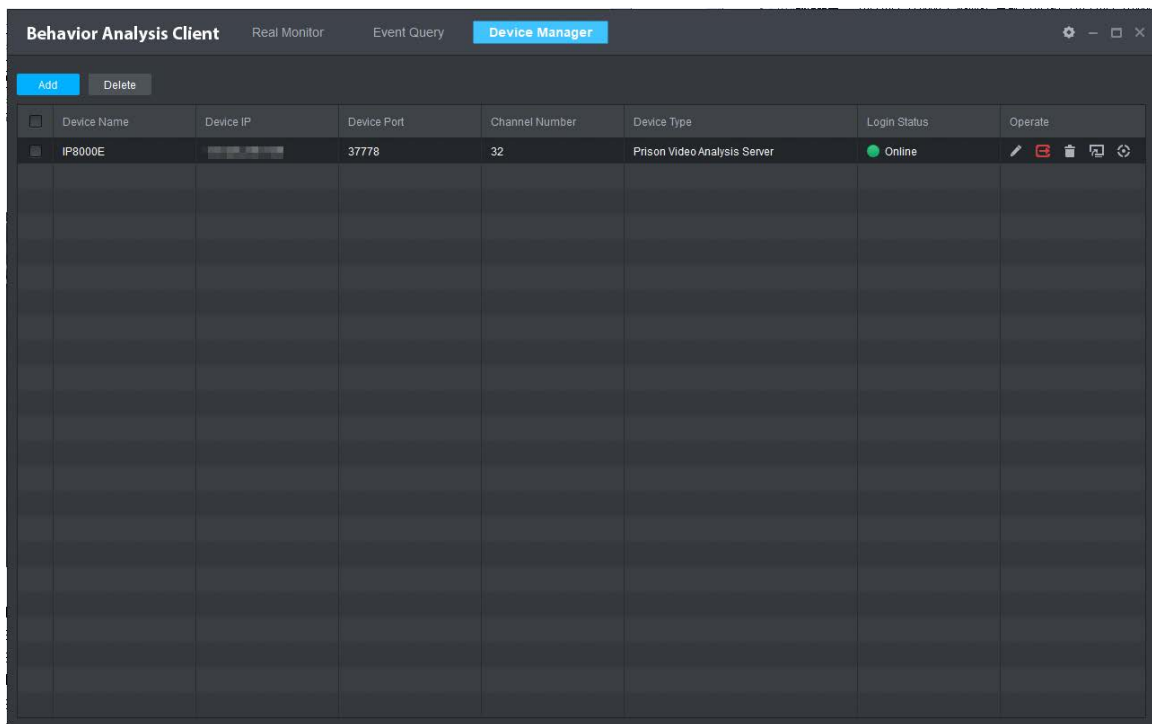
Parameter	Description
Device Type	The type of device to be added.
Device Name	Enter a name for the server to differentiate it from other servers.
Device IP	The IP address of device.
Device Port	Corresponding protocol port number.

Parameter	Description
Username	Username for logging in to the device.
Password	Password for logging in to the device.







**Step 3** Click **OK**.

After the device is added, the client logs in to the device automatically. The login status is **Online** and the device type is **Video Analysis Server**, which means successful login.

Figure 4-5 Add device



## Related Operations

- Log in to the server.
  - ◇ On the **Device Manager** page, when the server is offline, click  to log in to the server.
  - ◇ On the **Real Monitor** page, right-click the device on the device list on the left, and then click **Login** to log in to the server.
- Log out of the server.
  - ◇ On the **Device Manager** page, when the server is online, click  to log out of the server.
  - ◇ On the **Real Monitor** page, right-click the device on the device list on the left, and then click **Logout** to log out of the server.
- Click  to modify device information.
- Delete server.
  - ◇ Delete a server: Click .
  - ◇ Delete servers in batches: Select multiple devices and click **Delete** at the upper-left corner.
- Click  to manage remote devices and channels. For details, see "4.3.2 Managing Remote Devices".
- Click  to configure video quality diagnosis. For details, see "4.4.3 Video Quality Diagnosis".



### 4.3.2 Managing Remote Devices

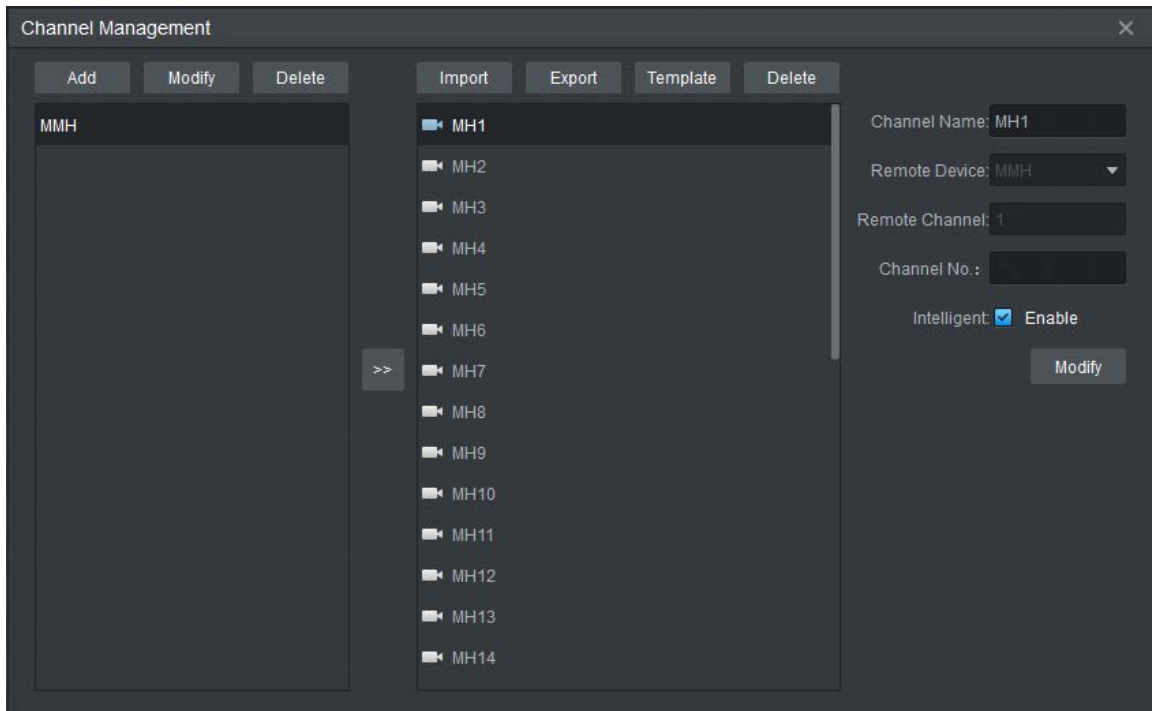
Manage remote devices and channels. If rules are configured after enabling the smart plan, an alarm will be generated once an event that meets the rules occurs.

#### Procedure

**Step 1** Add remote devices.

1. Click  on the **Device Manager** page.

Figure 4-6 Channel management



2. Click **Add**, and then configure the parameters.

Figure 4-7 Add remote device (1)

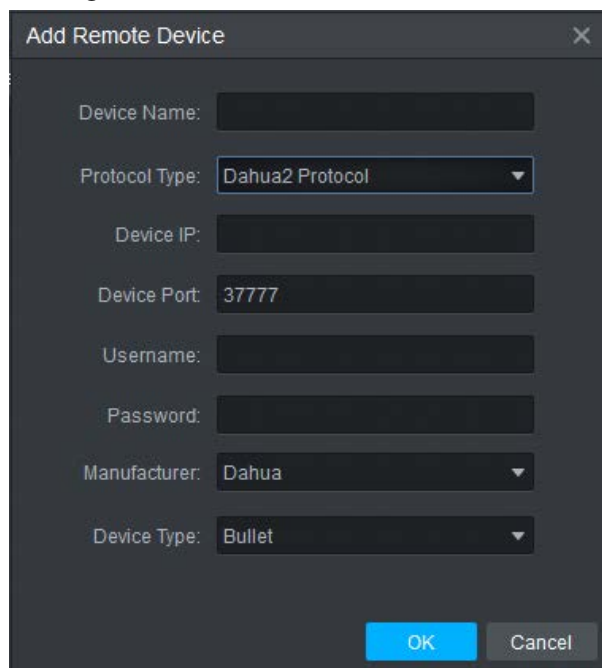
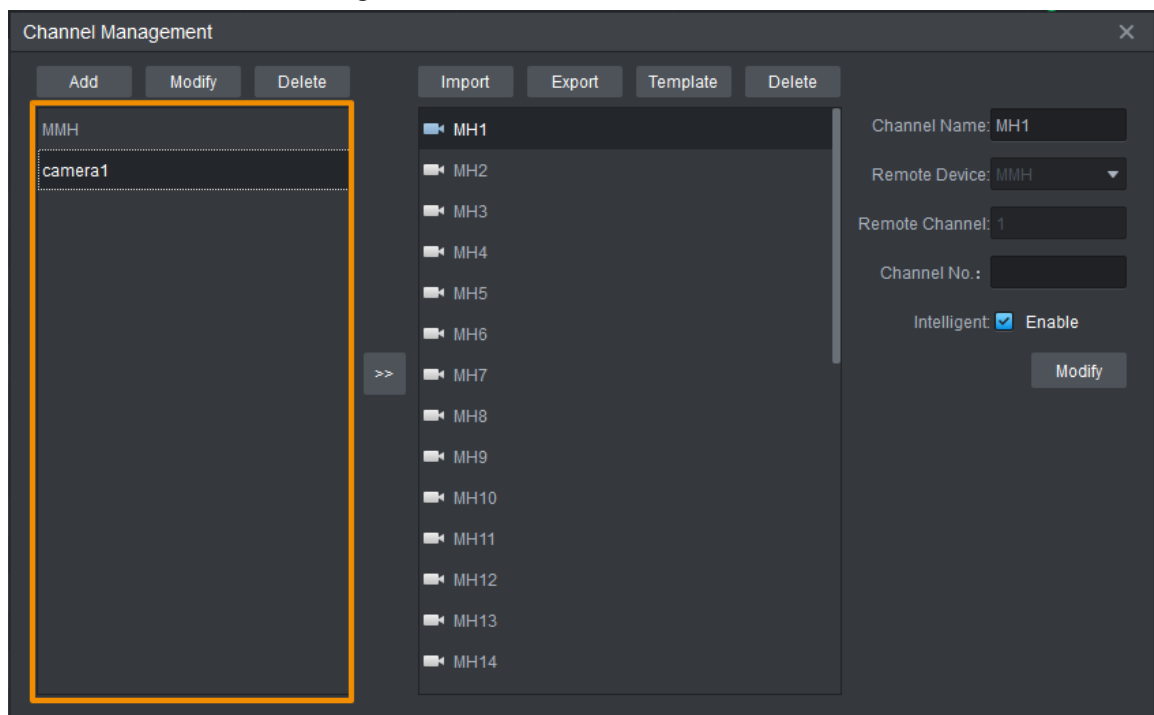


Table 4-2 Parameter description

Parameter	Description
Device Name	The name that differentiates a device.
Device IP	The device IP address.
Device Port	Port number
Username	Username and password for logging in to the remote device.
Password	
Manufacturer	Select device manufacturer.
Device Type	Select the device type depending on the actual remote device. Supported devices include bullet camera, PTZ camera, digital video recorder and network video recorder.

3. Click **OK**.

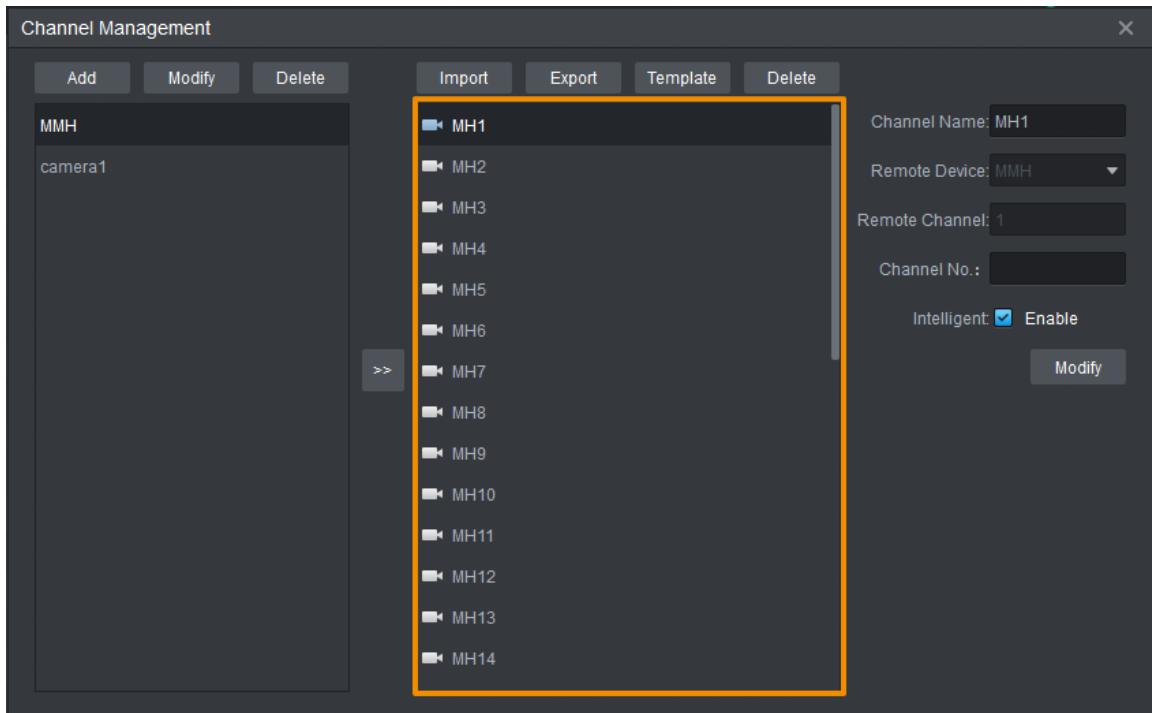
Figure 4-8 Add remote device (2)



**Step 2** Bind channels.

1. Select a remote device.
2. Click **>>** to configure channel information.  
Enter **Channel Name** and set **Remote Channel** as the channel number to be added.  
Enter the channel number, which should start from 1.
3. Click **Modify** on the right side of the page.

Figure 4-9 Channel Information



**Step 3** (Optional) Enable intelligent analysis. For channels added for the first time, **Enable** is selected by default.



If the intelligent analysis is not enabled for the channel, the original video can be played but rule configuration and intelligent analysis are not available.

1. Select channels from the channel list to enable intelligent analysis.
2. Select **Enable**.
3. Click **Modify** to enable intelligent analysis.

## Related Operations

- Modify and delete remote devices.
  - ◇ Select a remote device and click **Modify** at the top of the page to modify its information, and then click **OK**.
  - ◇ Select a remote device and click **Delete**. Click **Yes** in the prompt box.



When a remote device is deleted, all the channels added to it are deleted simultaneously.

- Modify and delete channels.
  - ◇ Select a channel and click **Modify** at the top of the page to modify its information. You can only modify **Channel Name**, **Channel No.** and **Enable**.
  - ◇ Select a channel and click **Delete** to delete it according to the prompts.
- Click **Download Template** to download the remote device table template for adding remote devices in batches.
- Click **Import** to import the remote device table template to the client.
- Click **Export** to export the remote device table template from the client to local.

## 4.4 Intelligent Video Analysis

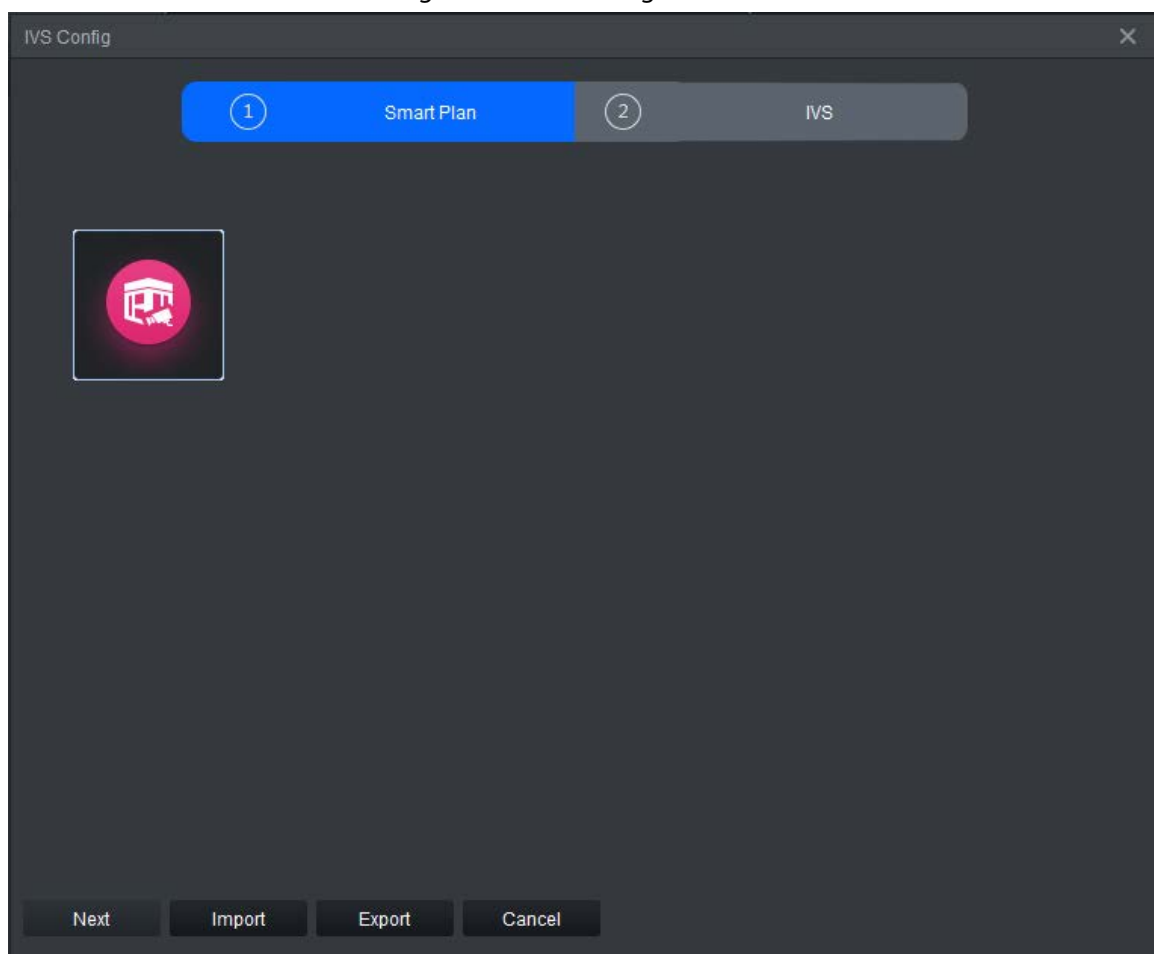
Enable the smart plan and configure rules. You can configure up to 10 AI rules and video quality diagnosis.

### 4.4.1 Enabling Smart Plan



#### Procedure

- Step 1 Click **Real Monitor** on the home page of the client.
- Step 2 Right-click a channel to select **IVS Config**.

Figure 4-10 IVS Config



Step 3 Select the plan.

-  indicates enabled or selected.
-  indicates not enabled or not selected.

Step 4 Click **Next** to go to the rule configuration page.



Click **Previous** to return to the smart plan page.

## Related Operations

- Click **Import** to import the XML file of configured IVS rules.
- Click **Export** to export the XML file of configured IVS rules.

### 4.4.2 IVS Rules

On the **IVS Config** page, you can add multiple alarm rules for each channel. You can set rules for the following detection scenarios: Tripwire, intrusion, climbing, getting up, staying (loitering), sleep, people number exception, loudness, fighting, staying alone, crowd gathering, object, call, using mobile phone, fall, running, smoking, sleeping with quilt covering head, head on wall, and video quality diagnosis. Ten independent detection areas can be set for a scenario.

#### Prerequisites

- The server has been added and is online.
- Intelligent analysis has been enabled. For details , see "4.3.2 Managing Remote Devices".

#### Background Information



You can enable or disable an AI rule, or delete added rules with the rule deletion button.

#### 4.4.2.1 Tripwire Detection

An alarm is triggered when a target crosses the drawn detection line in the same direction that the line was drawn.

Step 1 Click **Real Monitor** on the home page of the client.

Step 2 right-click a channel, and then select **IVS Config**.

Step 3 Select the smart plan, and then click **Next** to go to the IVS page.

Step 4 Click **Add rule**.

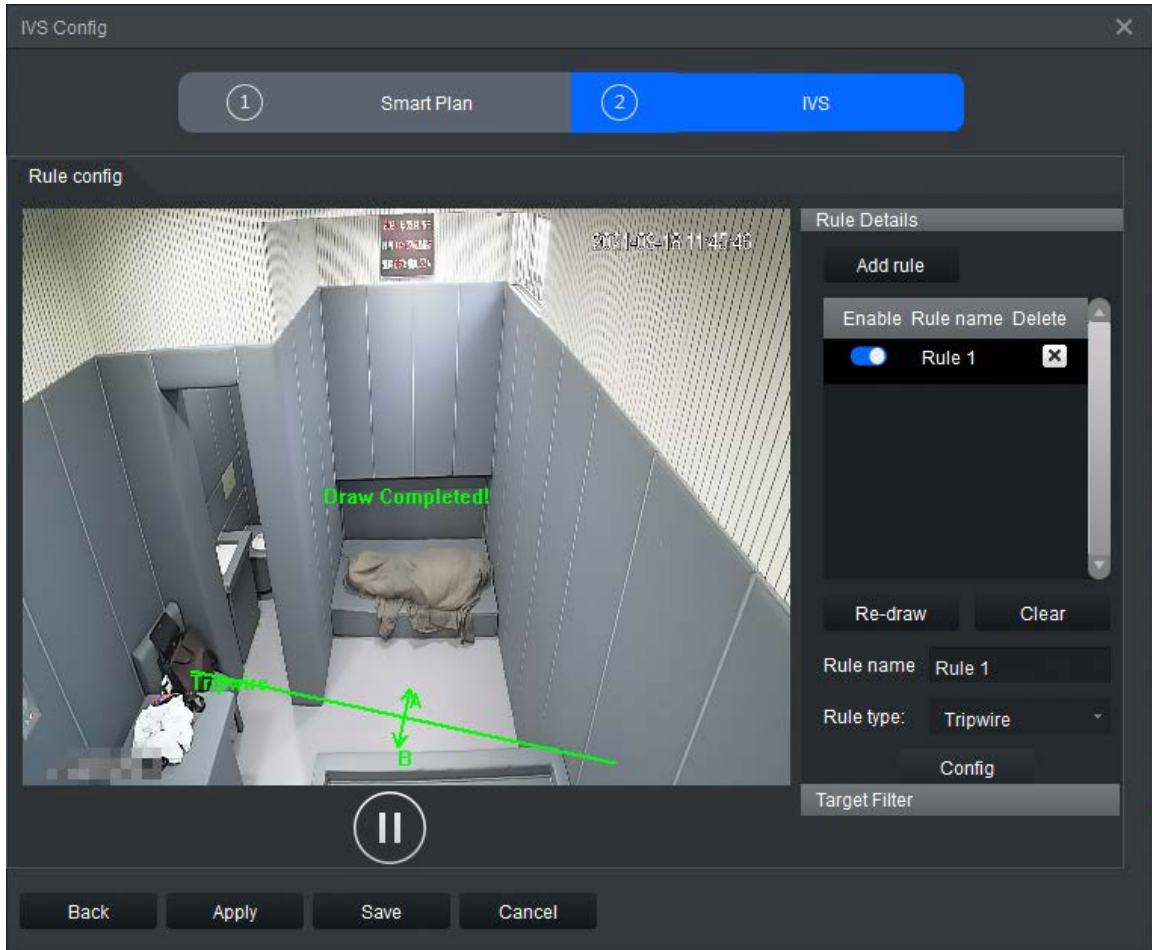
Step 5 Enter a **Rule name** and select **Tripwire** from the rule type.

Step 6 Draw a detection line on the monitoring screen on the left side, and then select **Direction**.



The detection line can be unidirectional or bidirectional.

Figure 4-11 Tripwire



**Step 7** Click **Config** to configure the parameters and the arming schedule.

1. Click **Parameters** to configure the parameters.

Figure 4-12 Tripwire parameter configuration

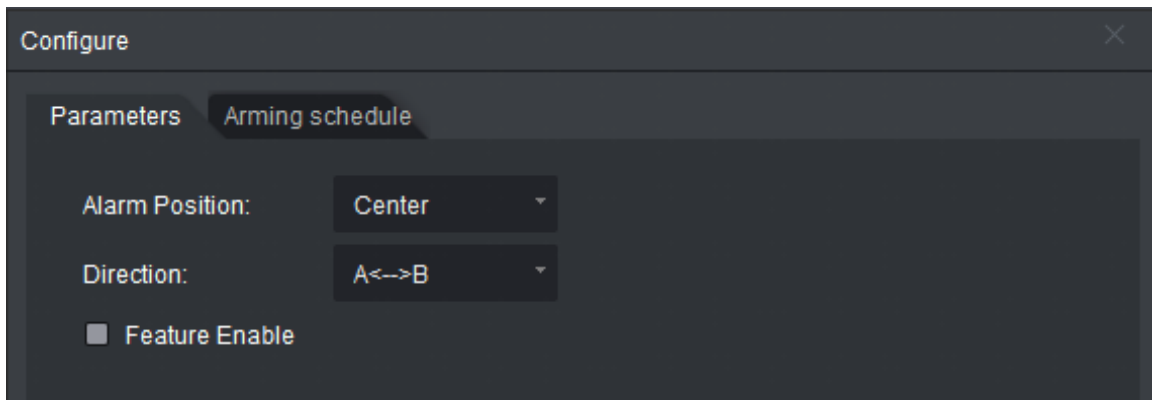


Table 4-3 configure the parameters

Item	Description
Alarm Position	Select the trigger position, including center, left center, top center, right center and bottom center.
Direction	Select direction: <b>A-&gt;B</b> , <b>A&lt;-B</b> or <b>A&lt;--&gt;B</b> .
(Optional) Feature Enable	If selected, uniforms can be recognized.

2. Click **Arming schedule** to change the arming schedule.

- Full-time arming is enabled by default. You can adjust the arming time.
- You can set up to six periods for each day.
- After configuring the arming schedule for one day, you can select other days (one or more) in the **Copy** section, and then click **Copy** to copy the configured arming schedule for other days.

Figure 4-13 Arming schedule



3. Click **Save**.

**Step 8** Save IVS.

- Click **Save** to save the IVS configuration and exit the page.
- Click **Apply** to save the IVS configuration without exiting the page.

#### 4.4.2.2 Intrusion Detection

An alarm is triggered when a target enters or exits the drawn intrusion area or stays in the area.

**Step 1** Click **Real Monitor** on the home page of the client.

**Step 2** right-click a channel, and then select **IVS Config**.

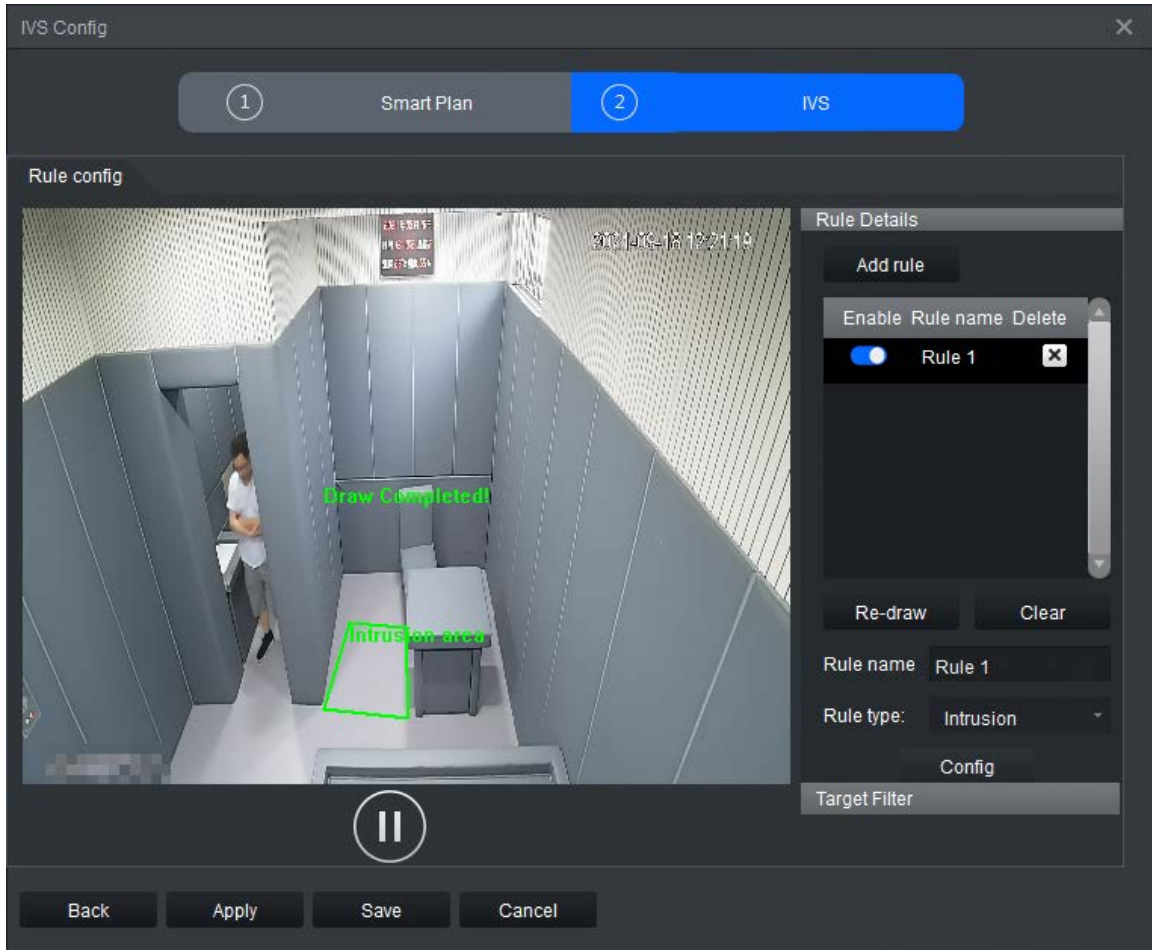
**Step 3** Select the smart plan, and then click **Next** to go to the IVS page.

**Step 4** Click **Add rule**.

**Step 5** Enter a **Rule name** and select **Intrusion** from the rule type.

**Step 6** Draw a detection area on the monitoring screen on the left.

Figure 4-14 Intrusion



**Step 7** Click **Config** to configure the parameters and the arming schedule.

1. Click **Parameters** to configure the parameters.



Figure 4-15 Parameters

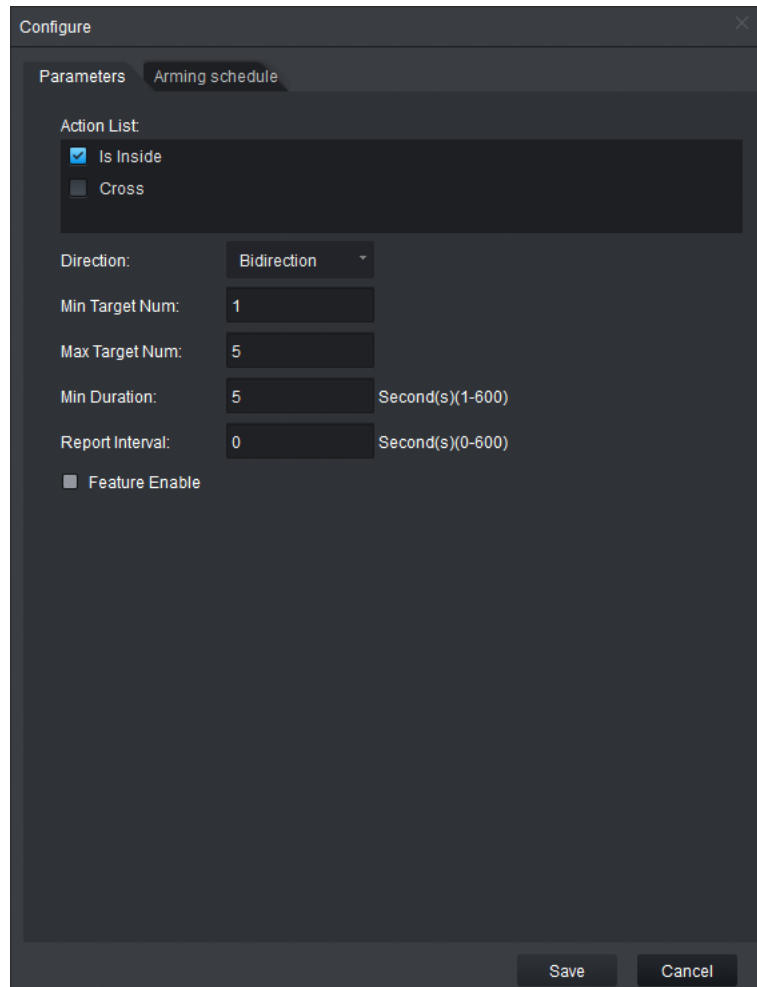



Table 4-4 Parameter description

Parameter		Description
Action List	<b>Is Inside</b>	Select <b>Is Inside</b> for scenarios when the target stays in the area. You need to set minimum target number, maximum target number, minimum duration, and report interval. No need to set direction.
	<b>Cross</b>	Select <b>Cross</b> for scenarios when the target enters or exits the area. <b>Direction</b> can be set as entry, leave, or bidirection. No need to set other parameters.  Bidirection: An alarm is triggered when an object enters or exits the area.
Min Target Num		An alarm is triggered when the number of detected persons is less than the defined value.
Max Target Num		An alarm is triggered when the number of detected persons exceeds the defined value.
Min Duration		An alarm is triggered when a person stays in the detection area for longer than the defined value.

Parameter	Description
Report Interval	When an alarm even occurs, and the target remains in the detection area for longer than the defined interval, another alarm will be triggered and information on the event will be shown on the screen.
(Optional) Feature Enable	Identifies police uniforms and yellow vests.

2. Click **Arming schedule** to change the arming schedule.

- Full-time arming is enabled by default. You can adjust the arming time.
- You can set up to six periods for each day.
- After configuring the arming schedule for one day, you can select other days (one or more) in the **Copy** section, and then click **Copy** to copy the configured arming schedule for other days.

Figure 4-16 Arming schedule

3. Click **Save**.

**Step 8** Save IVS.

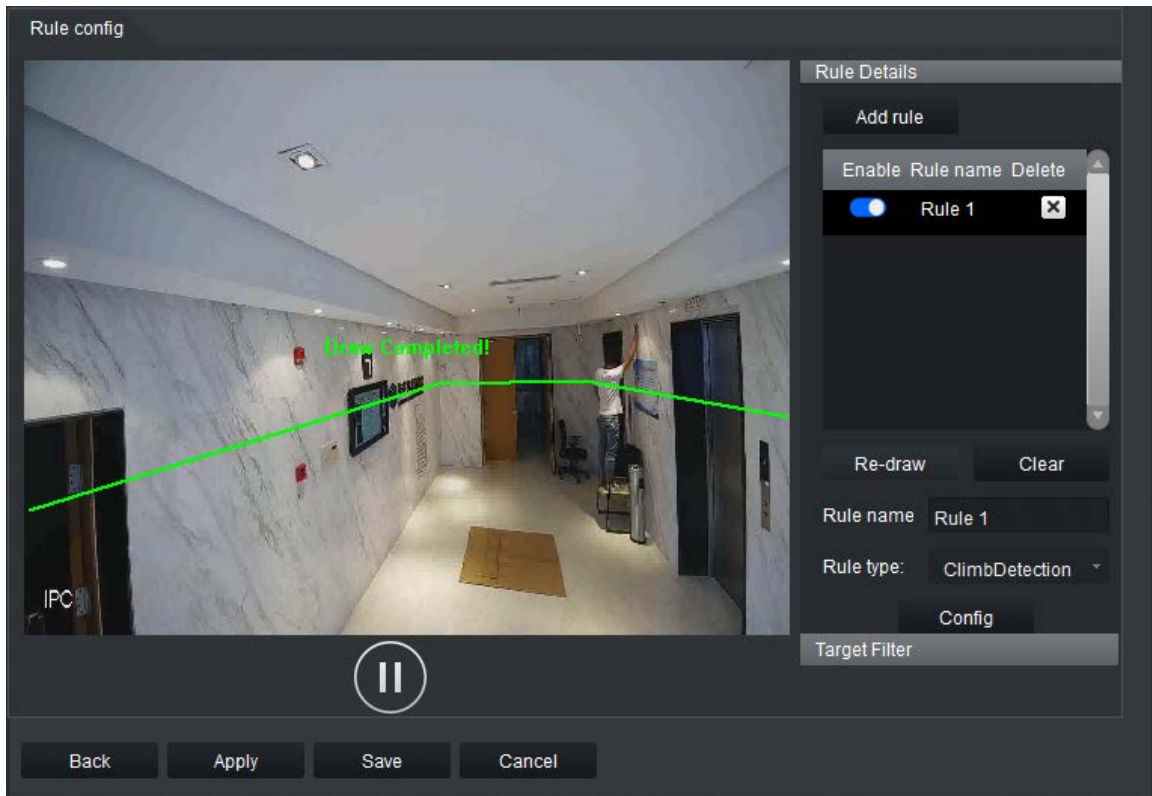
- Click **Save** to save the IVS configuration and exit the page.
- Click **Apply** to save the IVS configuration without exiting the page.

### 4.4.2.3 Climbing Detection

An alarm is triggered when a target climbs up and crosses the drawn climbing line.

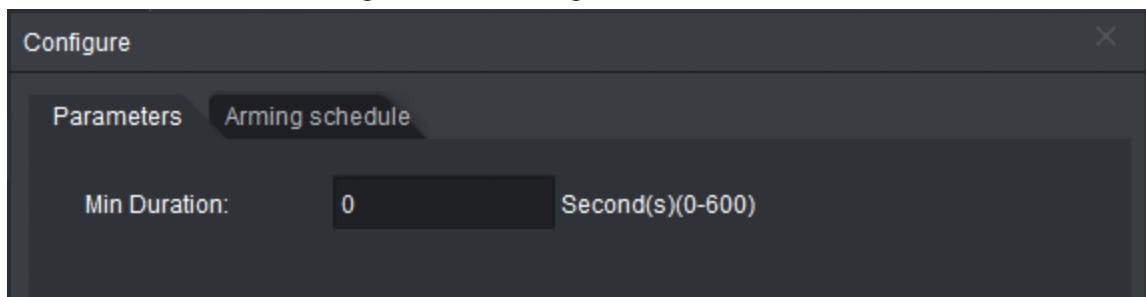
- Step 1** Click **Real Monitor** on the home page of the client.
- Step 2** right-click a channel, and then select **IVS Config**.
- Step 3** Select the smart plan, and then click **Next** to go to the IVS page.
- Step 4** Click **Add rule**.
- Step 5** Enter a **Rule name** and select **ClimbDetection** from the rule type.

Figure 4-17 Climbing detection



- Step 6** Click **Config** to configure the parameters and the arming schedule.
  1. Click **Parameters**.

Figure 4-18 Climbing detection

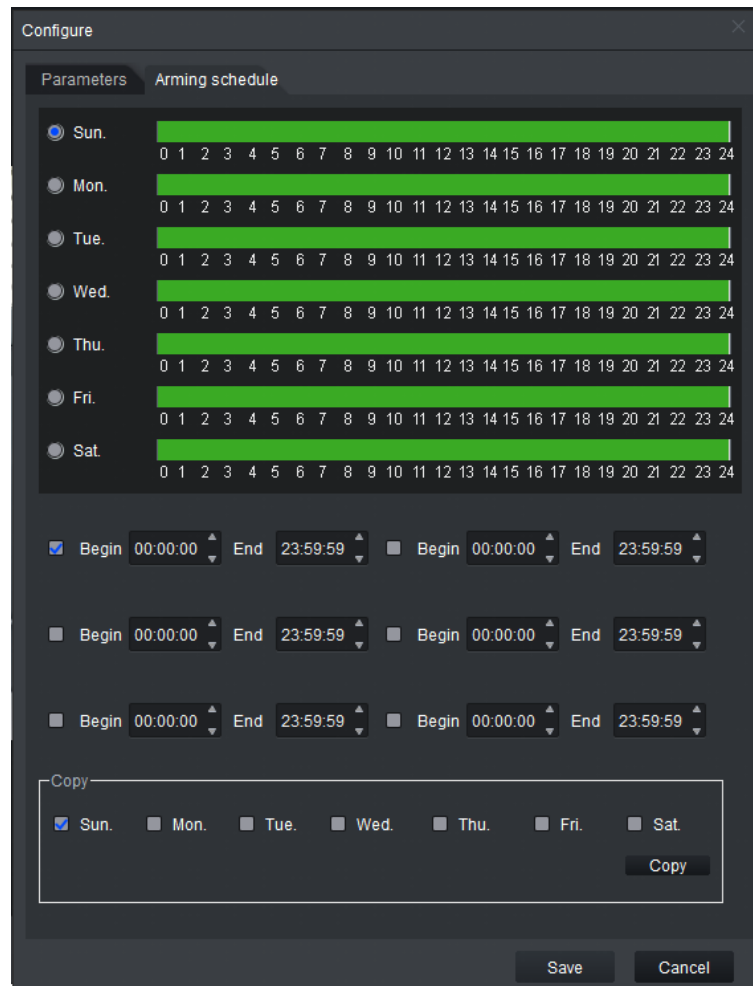


An alarm is triggered when a person is climbing, and their head and shoulders rise above the detection line, and remains above it for longer than the minimum duration time.

2. Click **Arming schedule** to change the arming schedule.
  - Full-time arming is enabled by default. You can adjust the arming time.
  - You can set up to six periods for each day.

- After configuring the arming schedule for one day, you can select other days (one or more) in the **Copy** section, and then click **Copy** to copy the configured arming schedule for other days.

Figure 4-19 Arming schedule



3. Click **Save**.

#### Step 7 Save IVS.

- Click **Save** to save the IVS configuration and exit the page.
- Click **Apply** to save the IVS configuration without exiting the page.

### 4.4.2.4 Getting up Detection

An alarm is triggered when a person rises above the detection line during the scheduled sleep time.



Only supports single-layer beds. Bunk beds are not supported at this time.

**Step 1** Click **Real Monitor** on the home page of the client.

**Step 2** right-click a channel, and then select **IVS Config**.

**Step 3** Select the smart plan, and then click **Next** to go to the IVS page.

**Step 4** Click **Add rule**.

**Step 5** Enter a **Rule name** and select **RiseDetection** from the rule type.

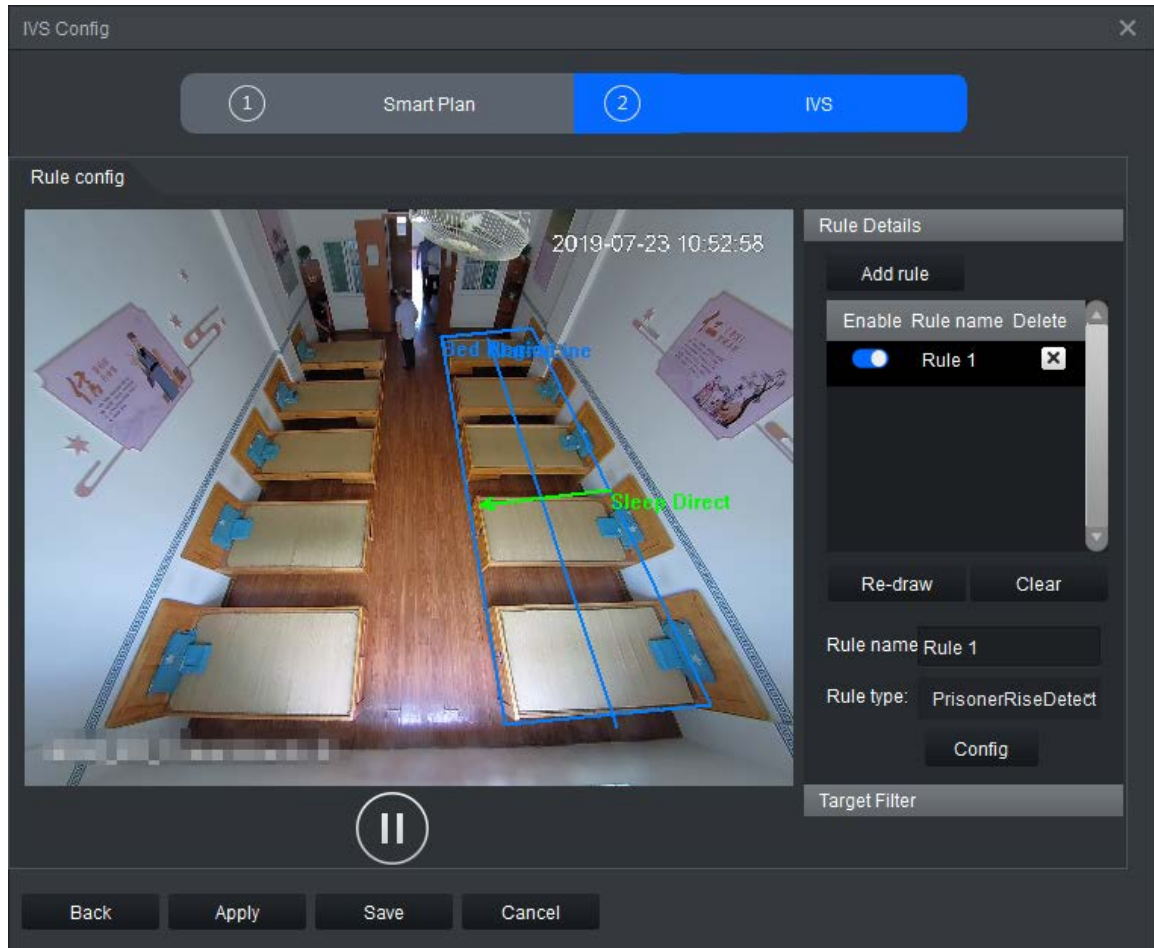
Draw the bed area, detection line and sleep direction on the monitoring screen on the left

according to the prompts.



- You can only draw four points in the bed area.
- The arrow direction of the sleep line is from the head to feet of the target.
- Draw the detection line on the chest of the person.

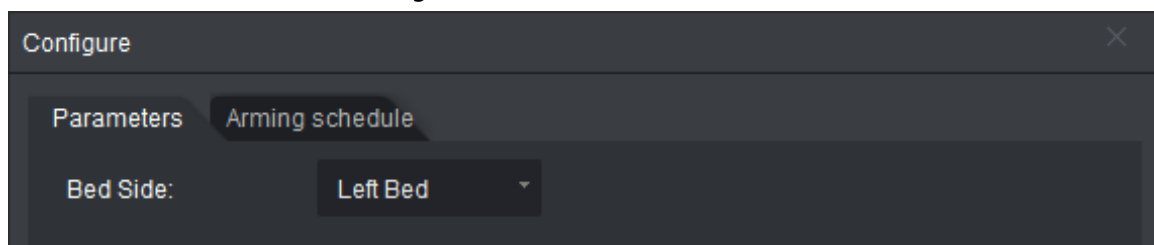
Figure 4-20 Getting up detection



**Step 6** Click **Config** to configure the parameters and the arming schedule.

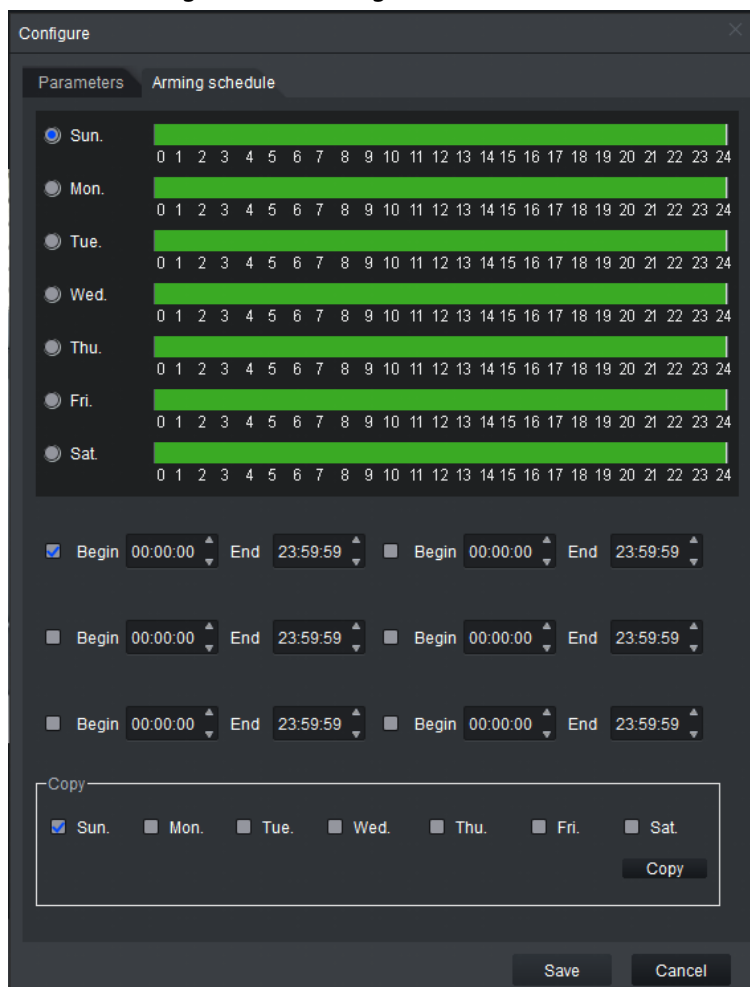
1. Click **Parameters** to configure **Bed Side**, including **Left Bed** and **Right Bed**.

Figure 4-21 Parameters



2. Click **Arming schedule** to change the arming schedule.
  - Full-time arming is enabled by default. You can adjust the arming time.
  - You can set up to six periods for each day.
  - After configuring the arming schedule for one day, you can select other days (one or more) in the **Copy** section, and then click **Copy** to copy the configured arming schedule for other days.

Figure 4-22 Arming schedule



3. Click **Save**.

Step 7 Save IVS.

- Click **Save** to save the IVS configuration and exit the page.
- Click **Apply** to save the IVS configuration without exiting the page.

#### 4.4.2.5 Staying (Loitering) Detection

An alarm is triggered when the target stays in the detection area for longer than the defined time.

Step 1 Click **Real Monitor** on the home page of the client.

Step 2 right-click a channel, and then select **IVS Config**.

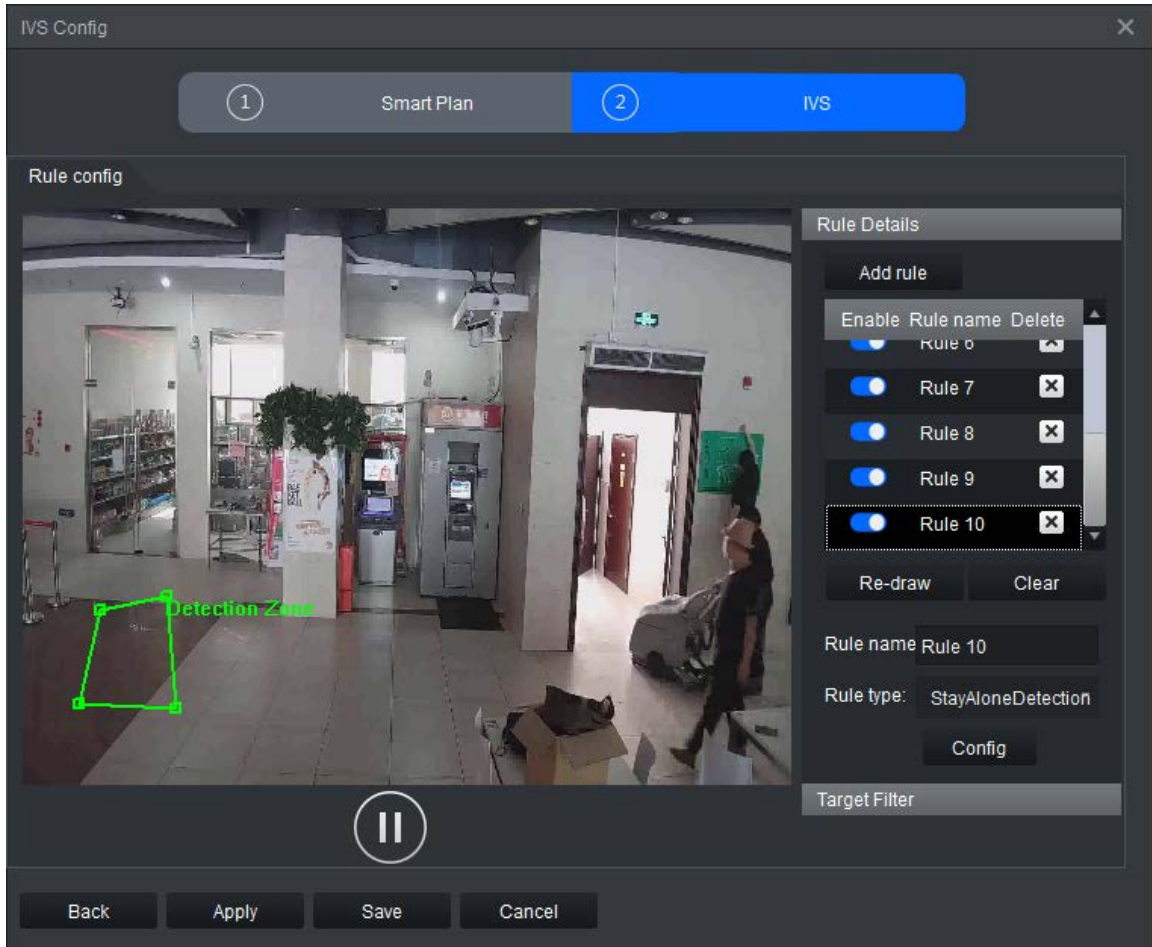
Step 3 Select the smart plan, and then click **Next** to go to the IVS page.

Step 4 Click **Add rule**.

Step 5 Enter a **Rule name** and select **StayDetection** from the rule type.

Draw a detection area on the monitoring screen on the left.

Figure 4-23 Stay Detection

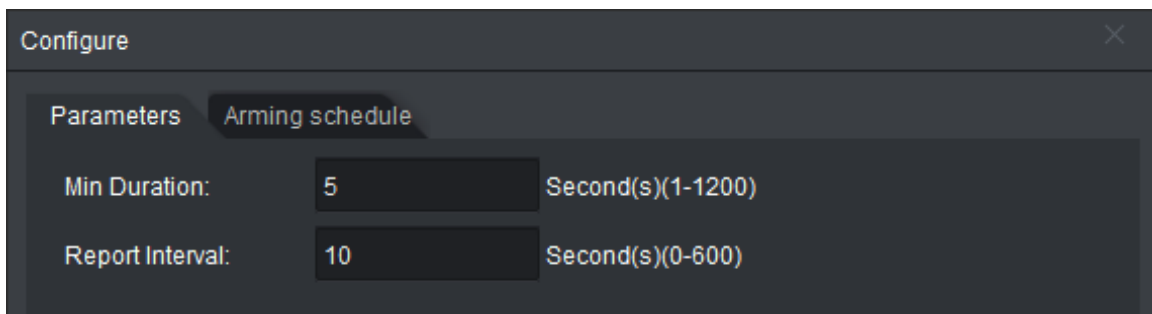


**Step 6** Click **Config** to configure the parameters and the arming schedule.

1. Click **Parameters** to configure the parameters.

- **Min Duration:** An alarm is triggered when a person stays in the detection area for longer than the defined minimum duration.
- **Report Interval:** When an alarm even occurs, and the target remains in the detection area for longer than the defined interval, another alarm will be triggered and information on the event will be shown on the screen.

Figure 4-24 Parameters

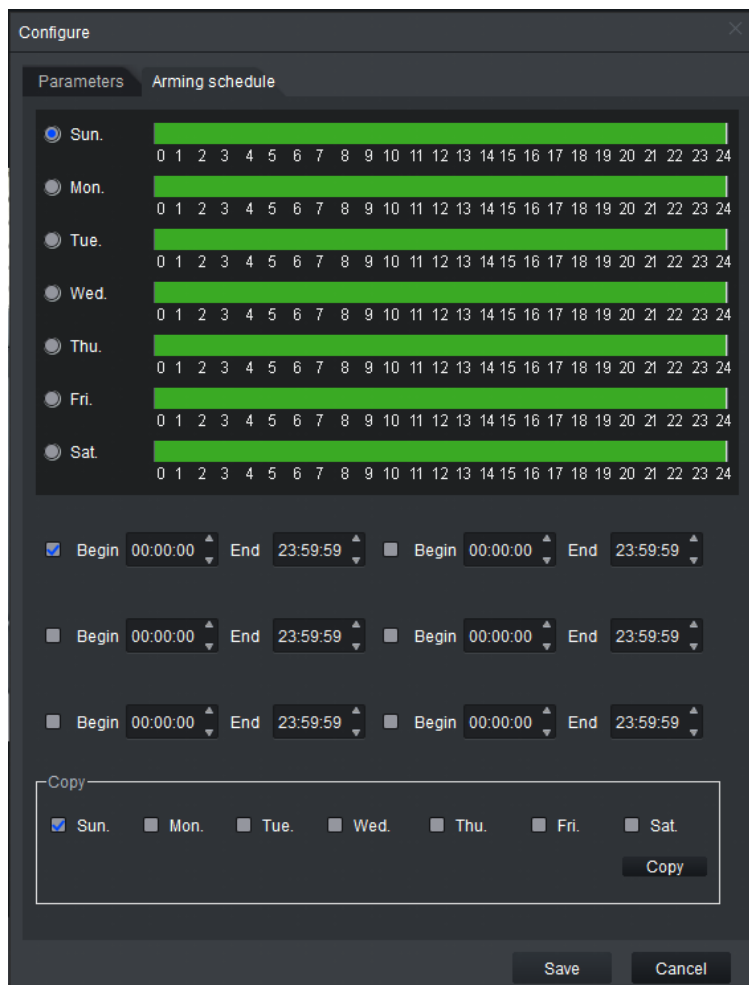


2. Click **Arming schedule** to change the arming schedule.

- Full-time arming is enabled by default. You can adjust the arming time.
- You can set up to six periods for each day.
- After configuring the arming schedule for one day, you can select other days (one or more) in the **Copy** section, and then click **Copy** to copy the configured arming

schedule for other days.

Figure 4-25 Arming schedule



3. Click **Save**.

Step 7 Save IVS.

- Click **Save** to save the IVS configuration and exit the page.
- Click **Apply** to save the IVS configuration without exiting the page.

#### 4.4.2.6 Sleep Detection

An alarm is triggered when a person is detected as staying still or laying down on a table for a long time.

Step 1 Click **Real Monitor** on the home page of the client.

Step 2 right-click a channel, and then select **IVS Config**.

Step 3 Select the smart plan, and then click **Next** to go to the IVS page.

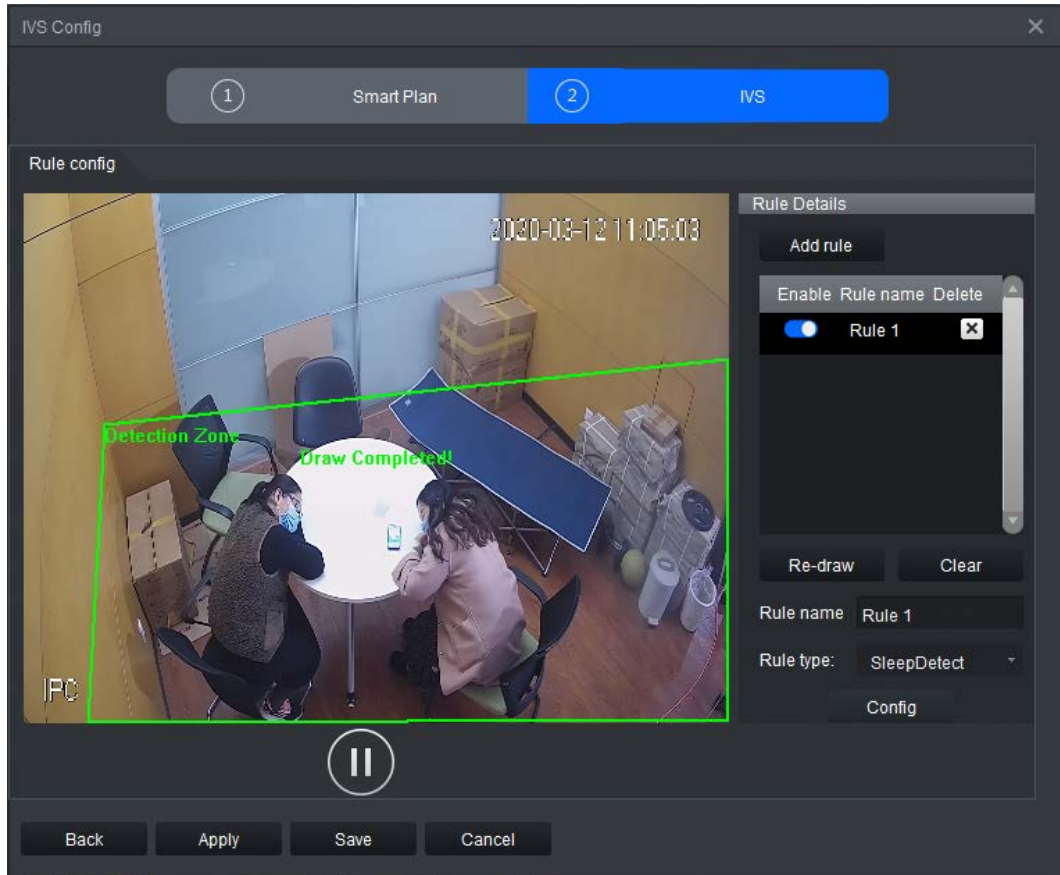
Step 4 Click **Add rule**.

Step 5 Enter a **Rule name** and select **LeaveDetection** from the rule type.

Draw the detection area on the monitoring screen on the left according to the prompts.



Figure 4-26 Sleep detection



- Step 6** Click **Config** to configure the parameters and the arming schedule.
1. Click **Parameters** to configure the parameters.

Figure 4-27 Parameters

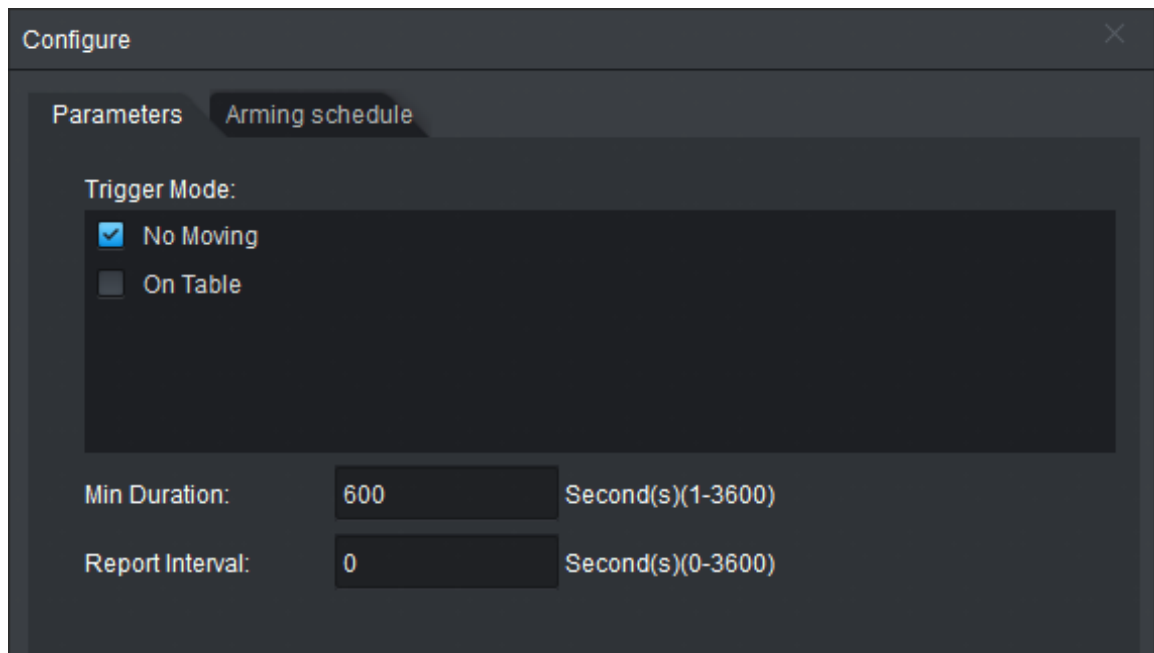



Table 4-5 Parameters for sleep detection

Parameter	Description
Trigger Mode	<ul style="list-style-type: none"> <li>• <b>No Moving:</b> If someone does not move or perform an action in the detection area within the defined period, an alarm will be triggered, and the alarm target will move to the position of the person.</li> <li>• <b>On Table:</b> If someone in the detection area lays down on the table within the defined period, an alarm will be triggered and the alarm target will move to the position of the person.</li> </ul>  <p><b>No Movement</b> is selected by default.</p>
Min Duration	An alarm is triggered when an on-duty person sleeps for longer than the defined value.
Report Interval	When an alarm even occurs, and the target remains in the detection area for longer than the defined interval, another alarm will be triggered and information on the event will be shown on the screen.

2. Click **Arming schedule** to change the arming schedule.

- Full-time arming is enabled by default. You can adjust the arming time.
- You can set up to six periods for each day.
- After configuring the arming schedule for one day, you can select other days (one or more) in the **Copy** section, and then click **Copy** to copy the configured arming schedule for other days.

Figure 4-28 Arming schedule



3. Click **Save**.

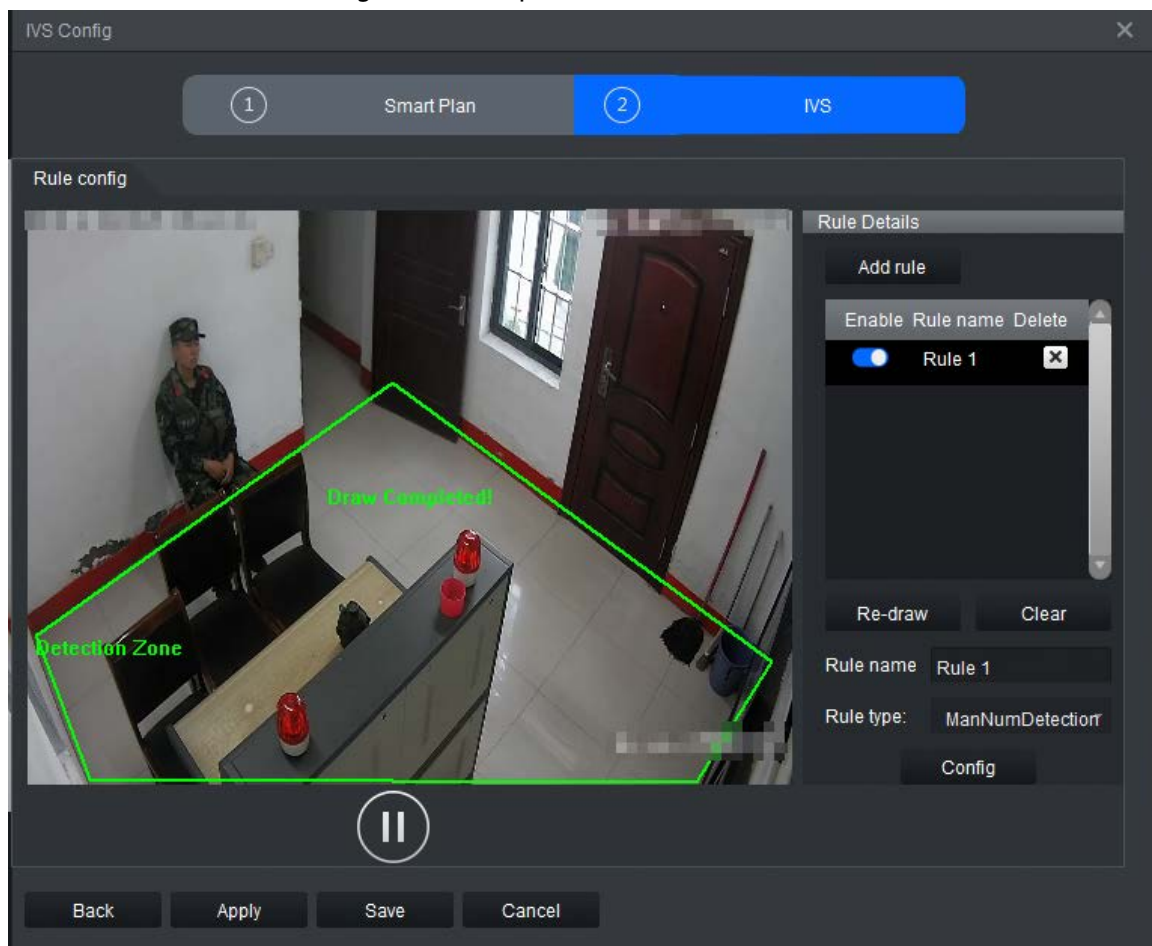
- Step 7** Save IVS.
- Click **Save** to save the IVS configuration and exit the page.
  - Click **Apply** to save the IVS configuration without exiting the page.

#### 4.4.2.7 Abnormal Number of People Detection

Based on the configured rules, an alarm is triggered when the number of people in the detection area does not conform to the configured rules.

- Step 1** Click **Real Monitor** on the home page of the client.
- Step 2** right-click a channel, and then select **IVS Config**.
- Step 3** Select the smart plan, and then click **Next** to go to the IVS page.
- Step 4** Click **Add rule**.
- Step 5** Enter a **Rule name** and select **ManNumDetection** from the rule type.

Figure 4-29 People number error



- Step 6** Click **Config** to configure the parameters and the arming time.
1. Click **Parameters** to configure the parameters.

Figure 4-30 Parameter configuration

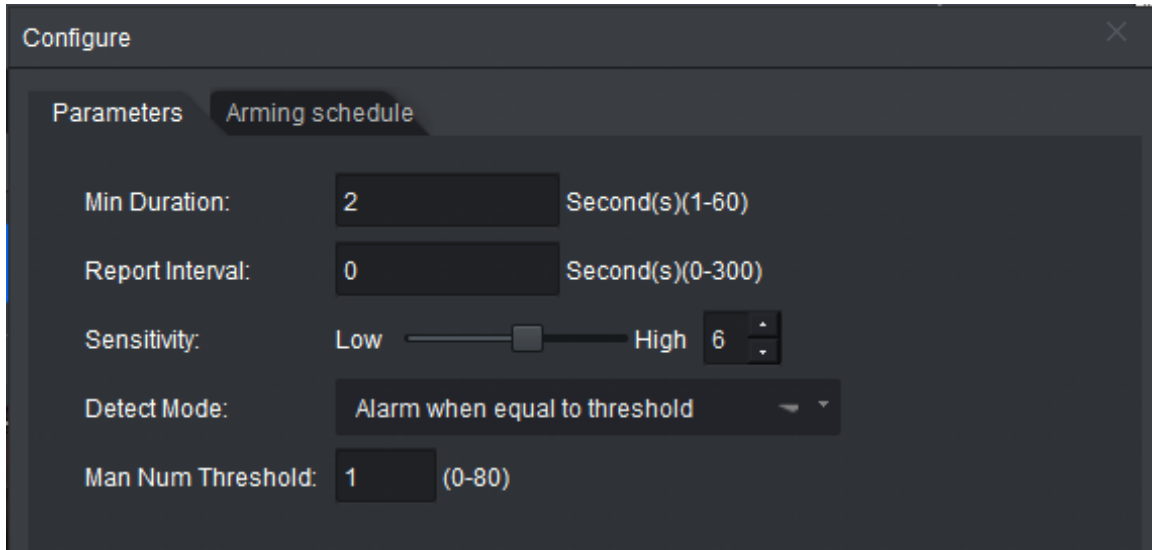




Table 4-6 Parameter configuration

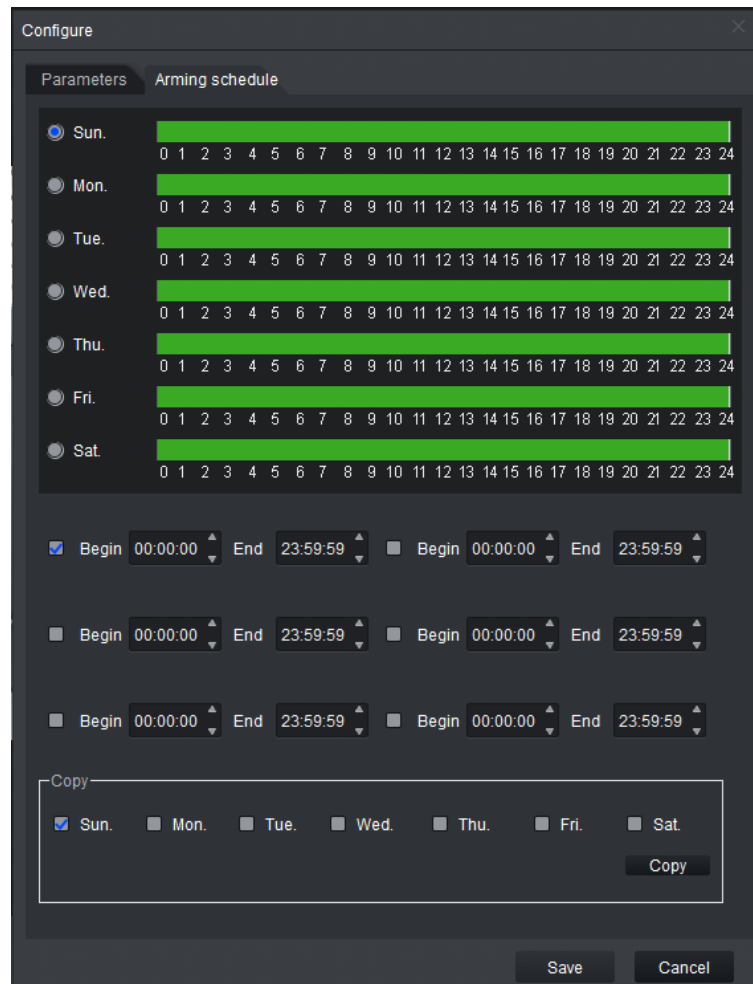
Parameter	Description
Minimum Duration	An alarm is triggered when the number of people in the detection area does not conform to the defined value and lasts longer than the minimum duration.
Report Interval	When an alarm even occurs, and the target remains in the detection area for longer than the defined interval, another alarm will be triggered and information on the event will be shown on the screen.
Sensitivity	Set the sensitivity value as needed. The higher the sensitivity, the easier the alarm is triggered.  The sensitivity range is 1 to 10. It is 7 by default.

Parameter	Description
Detect Mode	<ul style="list-style-type: none"> <li>● <b>Alarm when equal to threshold:</b> An alarm is triggered when the number of people in the detection area equals to the configured threshold.</li> <li>● <b>Alarm when not equal to threshold:</b> An alarm is triggered when the number of people in the detection area does not equal to the configured threshold (it is either higher or lower than the threshold). For example, if the threshold is set to be 1, an alarm will be triggered when there is no one present or when there is more than one persons present.</li> <li>● <b>Alarm when greater than threshold:</b> An alarm is triggered when the number of people in the detection area is higher than the threshold. For example, if the threshold is set to be 2, an alarm will be triggered when there are more than two people present.</li> <li>● <b>Alarm when less than to threshold:</b> An alarm is triggered when the number of people in the detection area is less than the threshold. For example, if the threshold is set as 2, an alarm will be triggered when only one person or no one is present.</li> <li>● <b>Alarm when is of section(Include boundary):</b> An alarm is triggered when the number of people in the detection area is within the configured range (boundary value included). For example, if the configured range is set as 1 to 2, an alarm will be triggered when one or two people are present.</li> <li>● <b>Alarm when out of boundary(No boundary):</b> An alarm is triggered when the number of people in the detection area is higher than the configured range (the boundary value is excluded). For example, if the configured range is set as 1 to 2, an alarm will be triggered when no one is present or when more than 2 people are present.</li> <li>● <b>Real time number of people in the area:</b> The number of people is displayed in real-time in the upper left corner of the live video.</li> </ul>
Man Num Threshold/ PersonNum	<p>Configure the threshold for the number of people in the detection area.</p>  <ul style="list-style-type: none"> <li>● When the detection mode is <b>Alarm when is of section(Include boundary)</b> or <b>Alarm when out of boundary(No boundary)</b>, <b>Man Num Threshold</b> changes to <b>PersonNum</b>.</li> <li>● The range is 0 to 80 when the detection mode is <b>Alarm when equal to threshold</b>, <b>Alarm when not equal to threshold</b>, or <b>Alarm when greater than threshold</b>.</li> <li>● The range is 1 to 80 when the detection mode is <b>Alarm when less than to threshold</b>.</li> <li>● The range is 1 to 80 when the detection mode is <b>Alarm when is of section(Include boundary)</b> or <b>Alarm when out of boundary(No boundary)</b>.</li> </ul>

2. Click **Arming schedule** to change the arming schedule.

- Full-time arming is enabled by default. You can adjust the arming time.
- You can set up to six periods for each day.
- After configuring the arming schedule for one day, you can select other days (one or more) in the **Copy** section, and then click **Copy** to copy the configured arming schedule for other days.

Figure 4-31 Arming schedule



3. Click **Save**.

**Step 7** Save IVS.

- Click **Save** to save the IVS configuration and exit the page.
- Click **Apply** to save the IVS configuration without exiting the page.

#### 4.4.2.8 Abnormal Sound Detection

An alarm is triggered when the sound intensity exceeds the defined threshold, and the sound lasts longer than the defined period.

**Step 1** Click **Real Monitor** on the home page of the client.

**Step 2** right-click a channel, and then select **IVS Config**.

**Step 3** Select the smart plan, and then click **Next** to go to the IVS page.

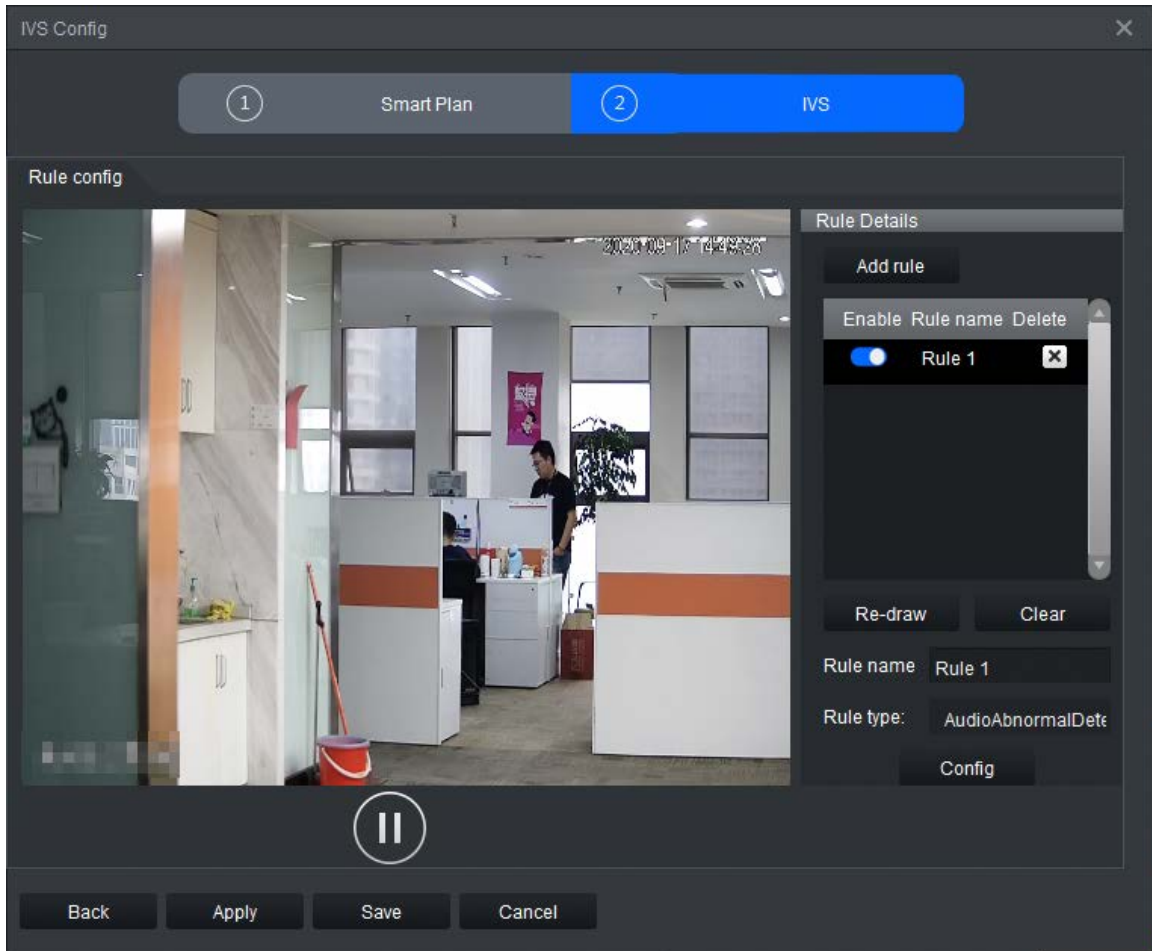
**Step 4** Click **Add rule**.

**Step 5** Enter a **Rule name** and select **AudioAbnormalDetection** from the rule type.



Only one abnormal sound detection rule can be configured for each channel.

Figure 4-32 Abnormal Sound Detection



**Step 6** Click **Config** to configure the parameters and the arming schedule.

1. Click **Parameters** to configure the parameters.

Figure 4-33 Parameters

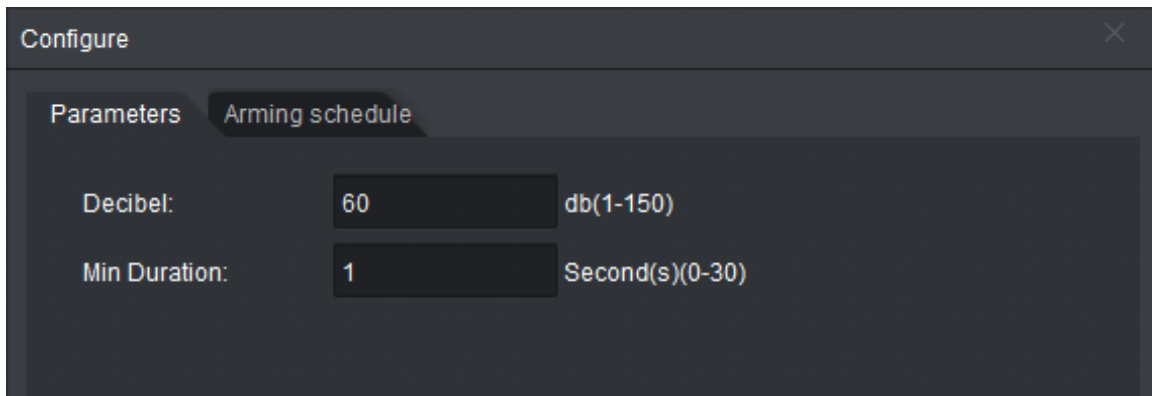


Table 4-7 Parameter description

Item	Description
Decibel	An alarm is triggered when the sound intensity is higher than the defined decibel for longer than the defined time. It is 60 by default.
Duration	

2. Click **Arming schedule** to change the arming schedule.

- Full-time arming is enabled by default. You can adjust the arming time.
- You can set up to six periods for each day.
- After configuring the arming schedule for one day, you can select other days (one or more) in the **Copy** section, and then click **Copy** to copy the configured arming schedule for other days.

Figure 4-34 Arming schedule

3. Click **Save**.

Step 7 Save IVS.

- Click **Save** to save the IVS configuration and exit the page.
- Click **Apply** to save the IVS configuration without exiting the page.



### 4.4.2.9 Fight Detection

An alarm is triggered when people are detected to be fighting.

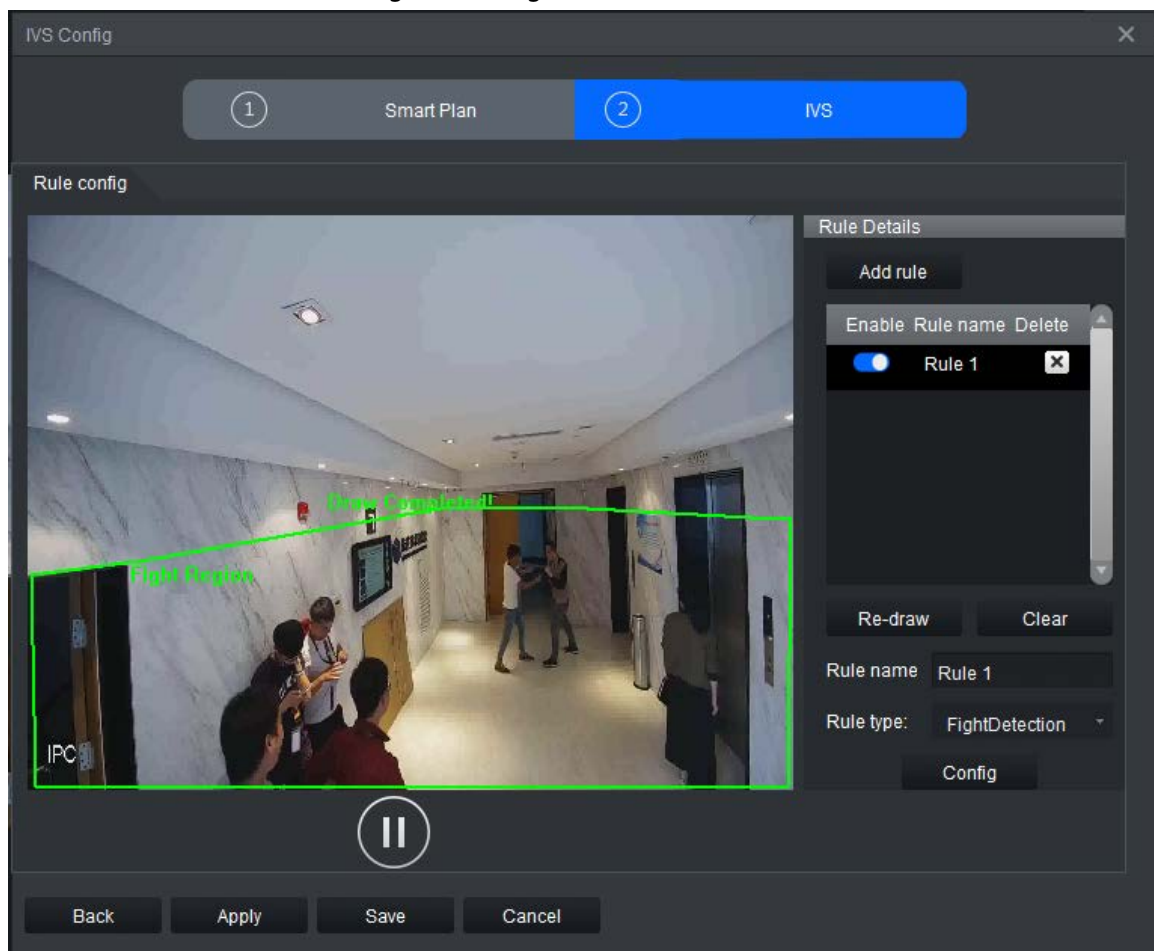


- Fight detection is performance intensive, so make sure to correctly outline the detection area. This will increase its efficiency.
- Fight detection can be used with other rules.
- A maximum of 16 channels can be set with the fight detection rule.
- Only one detection area and one fight detection rule can be set for each channel.
- For the 1U server, only 16 channels can be set with the fight detection rule.

#### Procedure

- Step 1** Click **Real Monitor** on the home page of the client.
- Step 2** right-click a channel, and then select **IVS Config**.
- Step 3** Select the smart plan, and then click **Next** to go to the IVS page.
- Step 4** Click **Add rule**.
- Step 5** Enter a **Rule name** and select **FightDetection** from the rule type.  
Draw a detection area on the monitoring screen on the left.

Figure 4-35 Fight detection



- Step 6** Click **Config** to configure the parameters and the arming schedule.

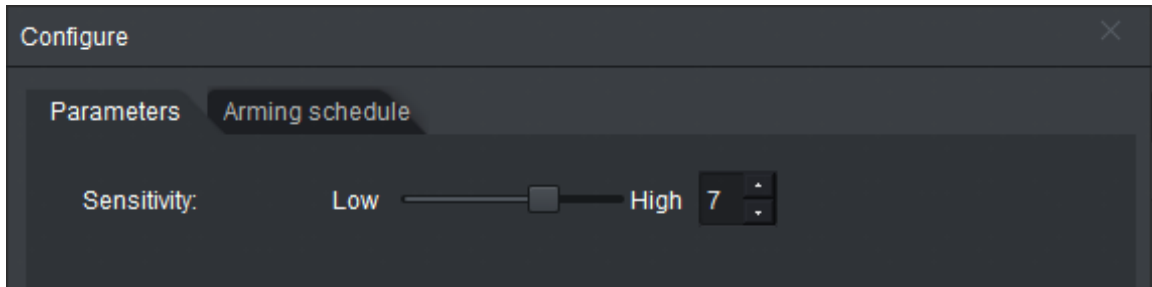
1. Select **Parameters**, and then drag the slider or enter a number in to adjust the

sensitivity. The higher the sensitivity, the easier it is for the alarms to be triggered. The false alarm rate will also increase.



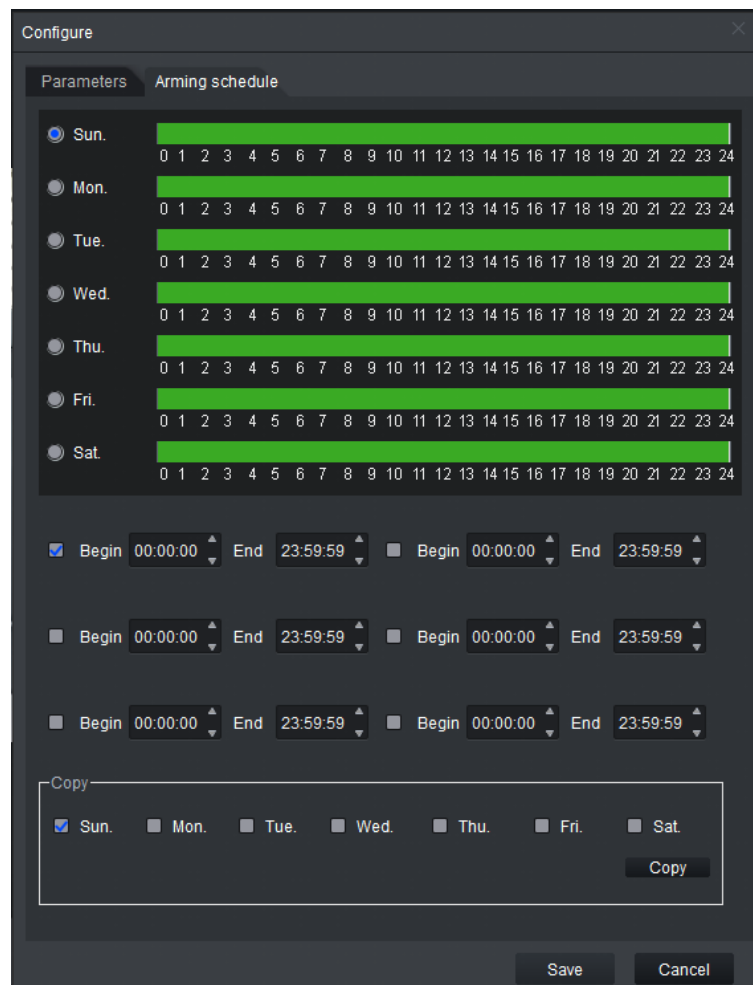
The sensitivity range is 1 to 10. It is 7 by default.

Figure 4-36 Fight detection



2. Click **Arming schedule** to change the arming schedule.
  - Full-time arming is enabled by default. You can adjust the arming time.
  - You can set up to six periods for each day.
  - After configuring the arming schedule for one day, you can select other days (one or more) in the **Copy** section, and then click **Copy** to copy the configured arming schedule for other days.

Figure 4-37 Arming schedule



3. Click **Save**.

- Step 7 Save IVS.
- Click **Save** to save the IVS configuration and exit the page.
  - Click **Apply** to save the IVS configuration without exiting the page.

#### 4.4.2.10 Staying Alone Detection

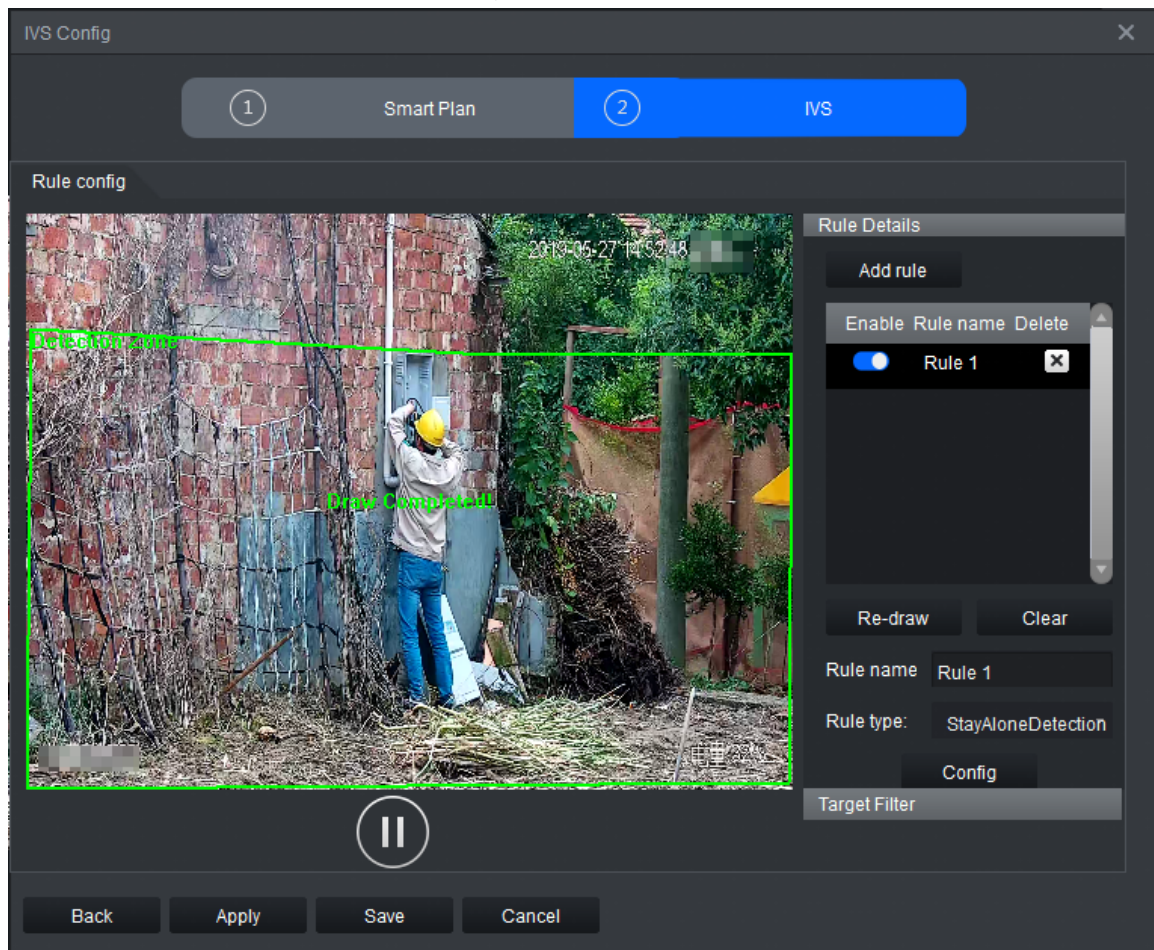
An alarm is triggered when a person is alone in the detection area for longer than the defined time.

- Step 1 Click **Real Monitor** on the home page of the client.
- Step 2 right-click a channel, and then select **IVS Config**.
- Step 3 Select the smart plan, and then click **Next** to go to the IVS page.
- Step 4 Click **Add rule**.
- Step 5 Enter a **Rule name** and select **StayAloneDetection** from the rule type.



Alarms are not triggered when more than one person is present in the detection area.

Figure 4-38 Staying alone detection



- Step 6 Click **Config** to configure the parameters and the arming schedule.
1. Click **Parameters** to configure the parameters.

Figure 4-39 Parameters

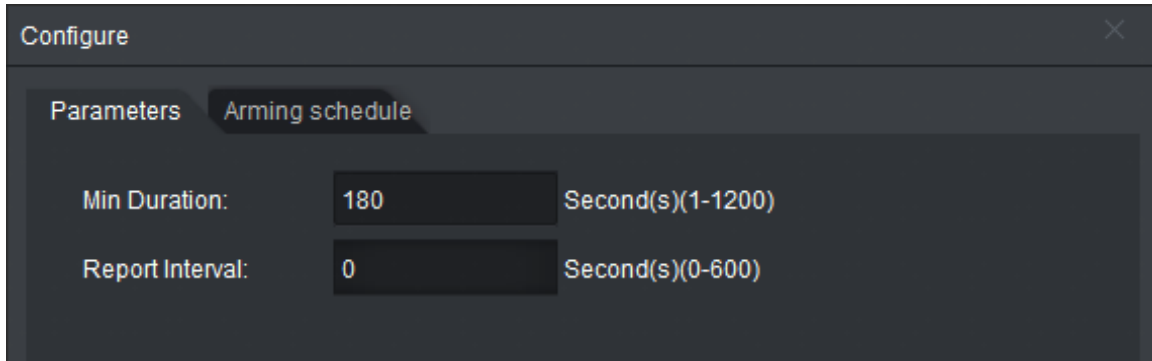
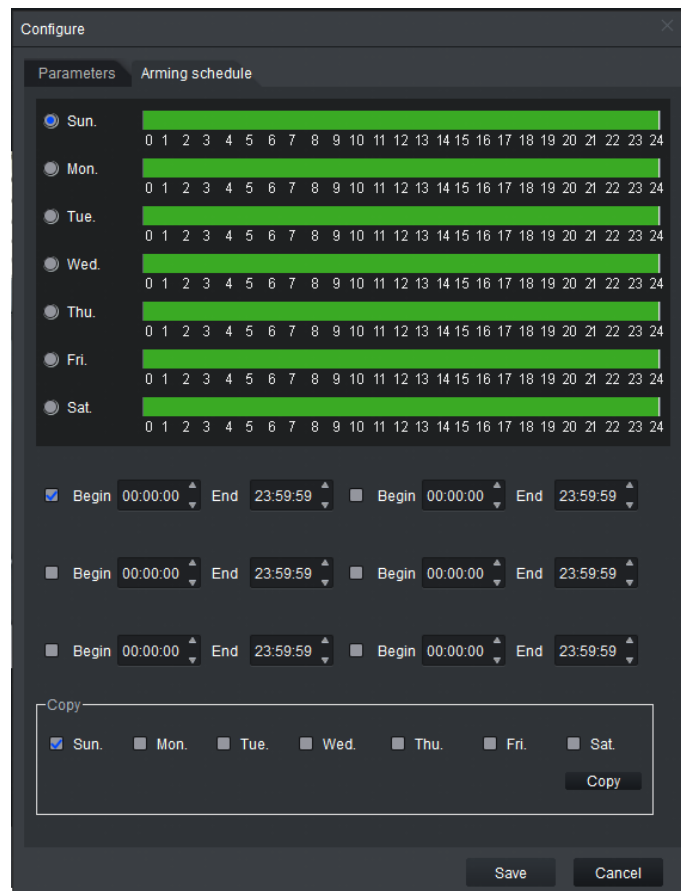


Table 4-8 Parameters

Item	Description
Min Duration	An alarm will be triggered if a person is staying alone in a detection area for longer than the defined value.
Report Interval	When an alarm even occurs, and the target remains in the detection area for longer than the defined interval, another alarm will be triggered and information on the event will be shown on the screen.

2. Click **Arming schedule** to change the arming schedule.
  - Full-time arming is enabled by default. You can adjust the arming time.
  - You can set up to six periods for each day.
  - After configuring the arming schedule for one day, you can select other days (one or more) in the **Copy** section, and then click **Copy** to copy the configured arming schedule for other days.

Figure 4-40 Arming schedule



3. Click **Save**.

Step 7 Save IVS.

- Click **Save** to save the IVS configuration and exit the page.
- Click **Apply** to save the IVS configuration without exiting the page.

#### 4.4.2.11 Crowd Gathering Detection

An alarm is triggered when four or more people gather and stay for longer than the defined time in the detection area.

Step 1 Click **Real Monitor** on the home page of the client.

Step 2 right-click a channel, and then select **IVS Config**.

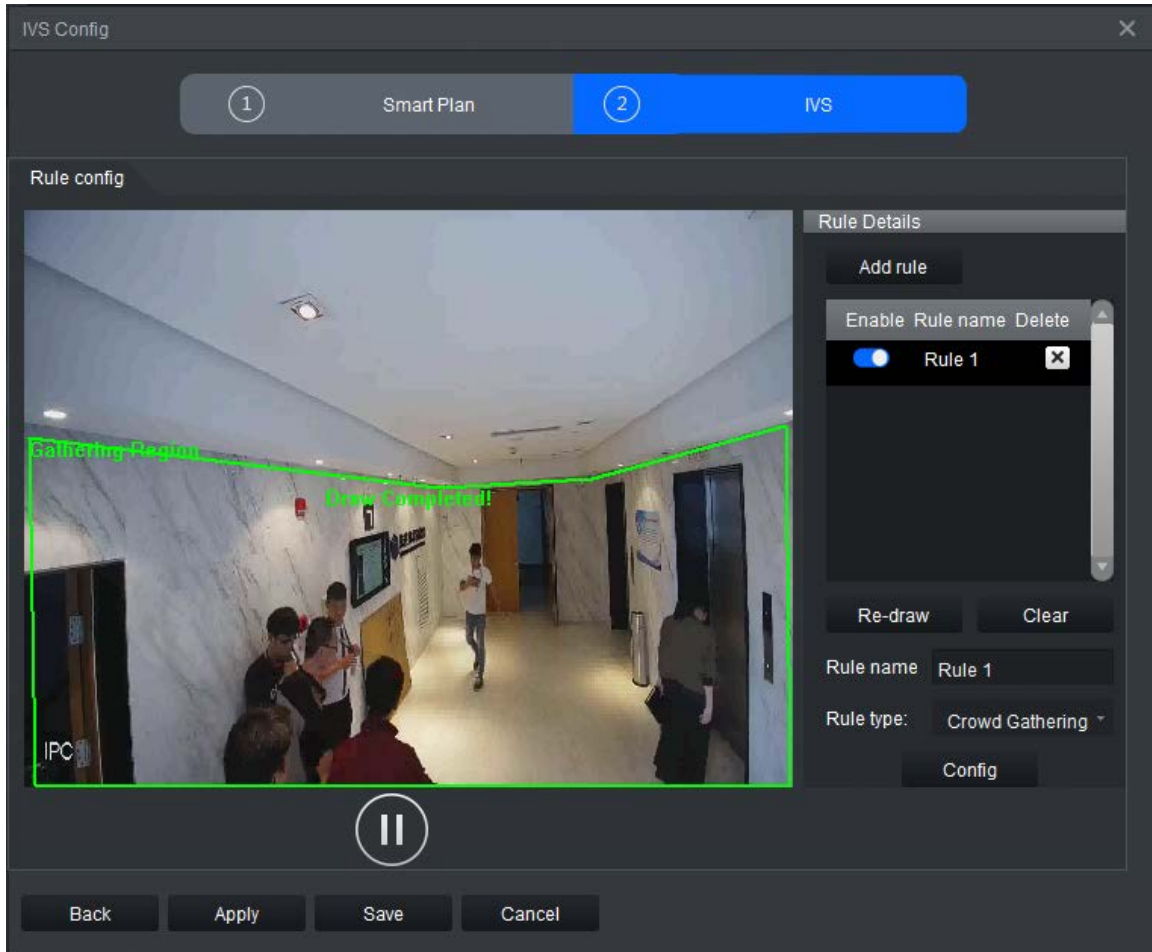
Step 3 Select the smart plan, and then click **Next** to go to the IVS page.

Step 4 Click **Add rule**.

Step 5 Enter a **Rule name** and select **Crowd Gathering** from the rule type.

Draw a detection area on the monitoring screen on the left.

Figure 4-41 Crowd gathering detection



**Step 6** Click **Config** to configure the parameters and the arming schedule.

1. Click **Parameters** to configure the parameters.

Figure 4-42 Parameters

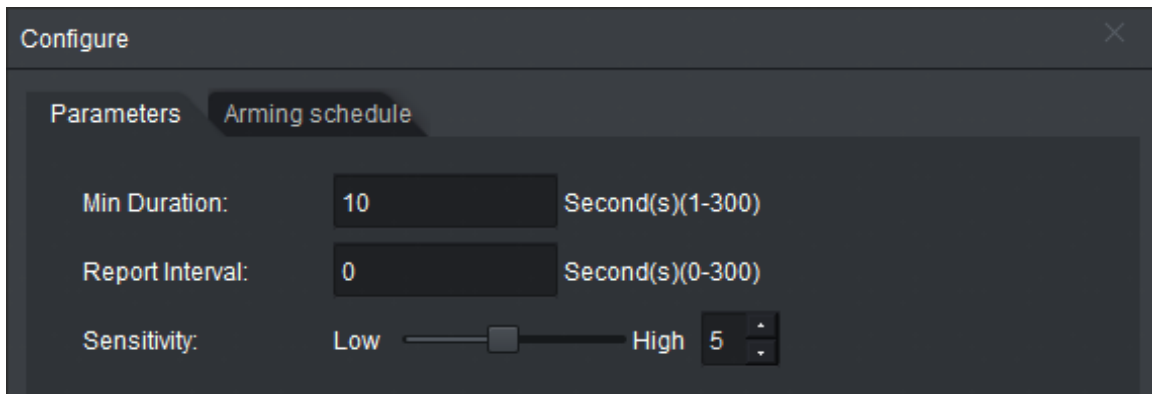



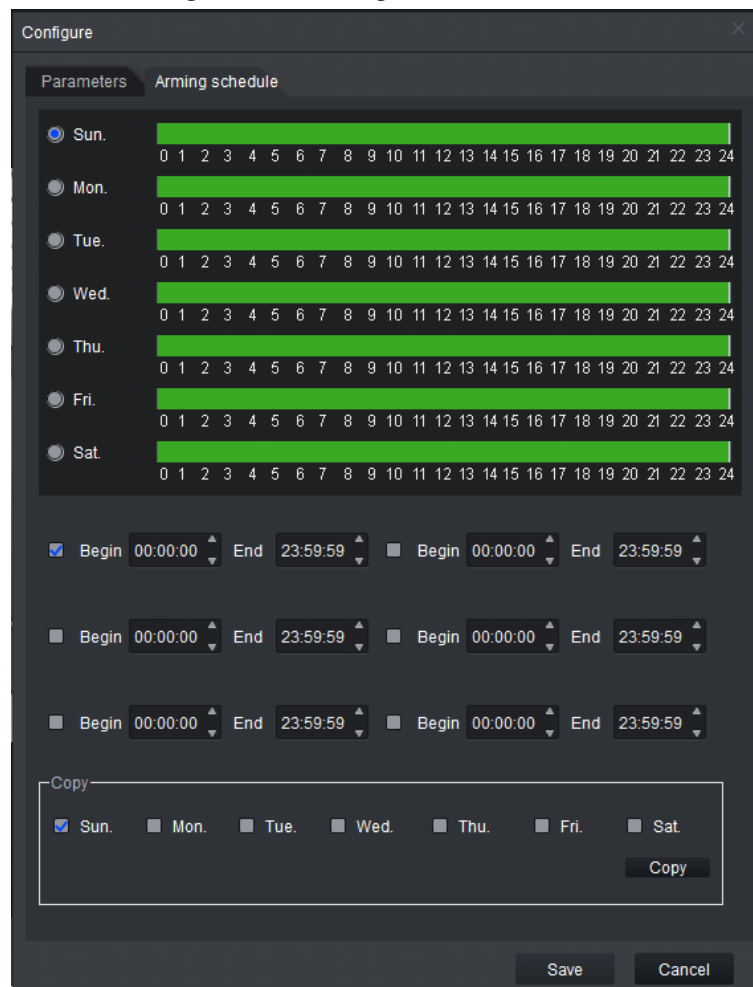
Table 4-9 Parameters

Item	Description
Min Duration	An alarm is triggered when a person stays in the detection area for longer than the defined value.
Report Interval	When an alarm even occurs, and the target remains in the detection area for longer than the defined interval, another alarm will be triggered and information on the event will be shown on the screen.

Item	Description
Sensitivity	Enter sensitivity. The higher the sensitivity, the easier the alarm is to be triggered.  The sensitivity range is from 1 to 10. It is 5 by default.

- Click **Arming schedule** to change the arming schedule.
  - Full-time arming is enabled by default. You can adjust the arming time.
  - You can set up to six periods for each day.
  - After configuring the arming schedule for one day, you can select other days (one or more) in the **Copy** section, and then click **Copy** to copy the configured arming schedule for other days.

Figure 4-43 Arming schedule



- Click **Save**.

#### Step 7 Save IVS.

- Click **Save** to save the IVS configuration and exit the page.
- Click **Apply** to save the IVS configuration without exiting the page.

### 4.4.2.12 Object Detection

An alarm is triggered when an object is left in or moved from the detection area for longer than the

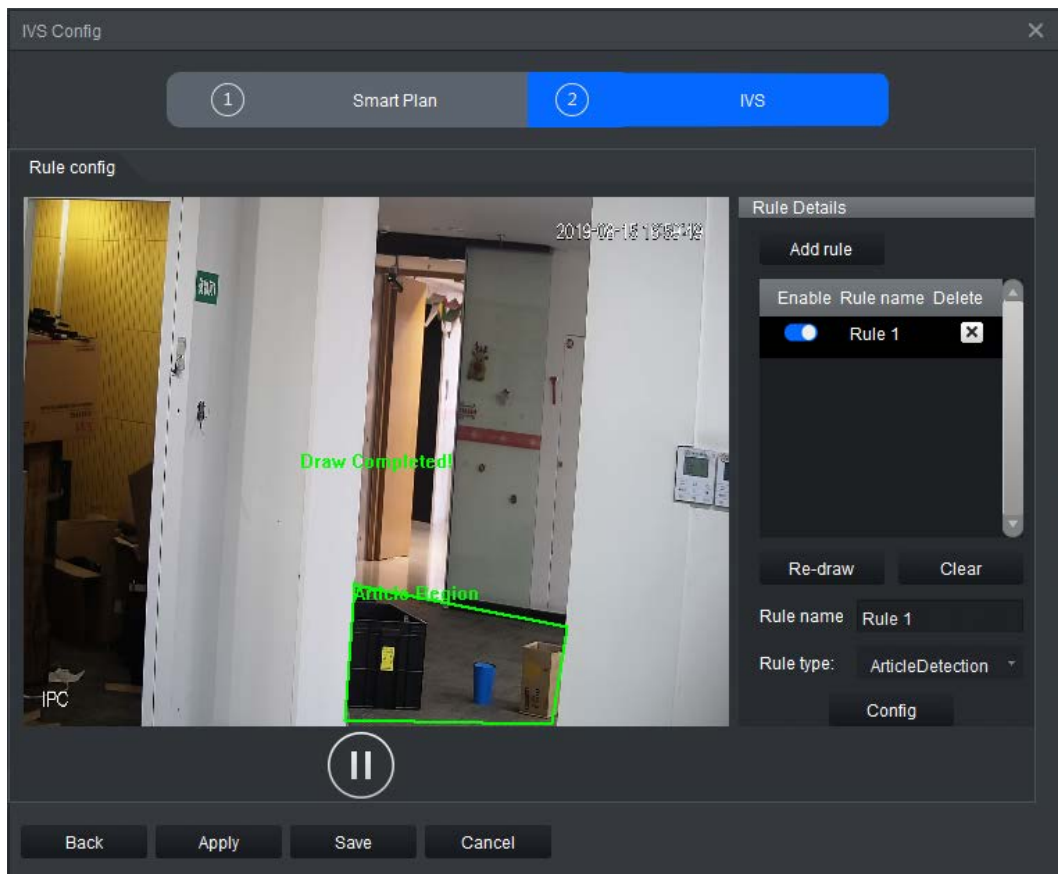
defined period.

- Step 1 Click **Real Monitor** on the home page of the client.
- Step 2 right-click a channel, and then select **IVS Config**.
- Step 3 Select the smart plan, and then click **Next** to go to the IVS page.
- Step 4 Click **Add rule**.
- Step 5 Enter a **Rule name** and select **ArticleDetection** from the rule type.



No more than four AI rules can be configured for each channel.

Figure 4-44 Object detection



- Step 6 Click **Config** to configure the parameters and the arming schedule.
  1. Click the **Parameters** to configure the parameters.



Figure 4-45 Parameters

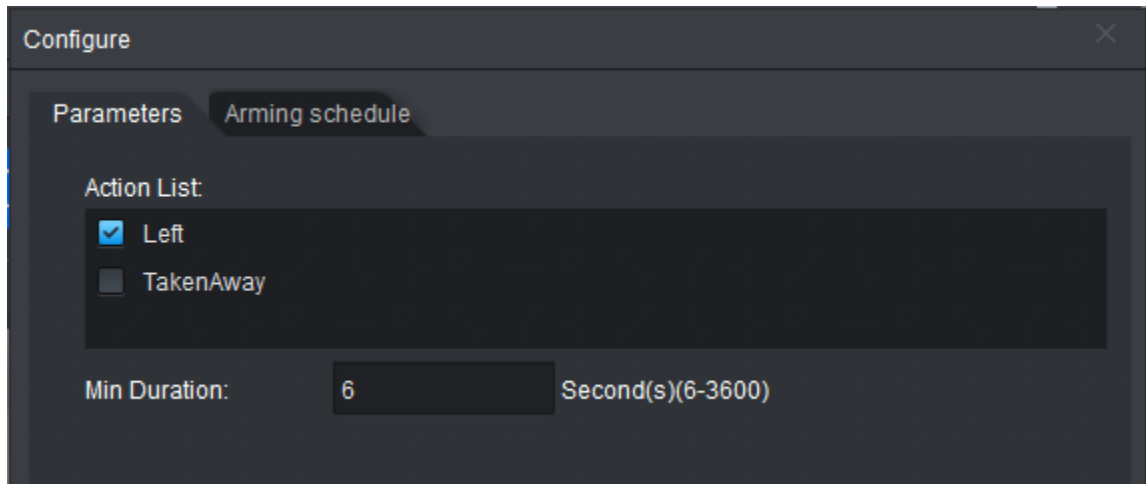


Table 4-10 Parameters

Parameter	Description
Action List	<ul style="list-style-type: none"> <li>• <b>Left:</b> an alarm is triggered when an object is left in the detection area for longer than the defined time.</li> <li>• <b>TakenAway:</b> an object detection alarm is triggered when an object is moved from the detection area and is not moved back within the defined time.</li> </ul>
Min Duration	An alarm is triggered when an object is left in or moved away from the detection area for longer than defined value.

2. Click **Arming schedule** to change the arming schedule.
  - Full-time arming is enabled by default. You can adjust the arming time.
  - You can set up to six periods for each day.
  - After configuring the arming schedule for one day, you can select other days (one or more) in the **Copy** section, and then click **Copy** to copy the configured arming schedule for other days.

Figure 4-46 Arming schedule

The screenshot shows a 'Configure' dialog box with the following elements:

- Parameters:** Arming schedule
- Days and Time Ranges:**
  - Sun. (Selected): 00:00:00 to 23:59:59
  - Mon.: 00:00:00 to 23:59:59
  - Tue.: 00:00:00 to 23:59:59
  - Wed.: 00:00:00 to 23:59:59
  - Thu.: 00:00:00 to 23:59:59
  - Fri.: 00:00:00 to 23:59:59
  - Sat.: 00:00:00 to 23:59:59
- Copy Section:**
  - Copy
  - Sun.  Mon.  Tue.  Wed.  Thu.  Fri.  Sat.
  - Copy
- Buttons:** Save, Cancel

3. Click **Save**.

Step 7 Save IVS.

- Click **Save** to save the IVS configuration and exit the page.
- Click **Apply** to save the IVS configuration without exiting the page.

#### 4.4.2.13 Call Detection

An alarm is triggered when a person makes a phone call in the detection area, and remains on the phone for longer than the defined period.

Step 1 Click **Real Monitor** on the home page of the client.

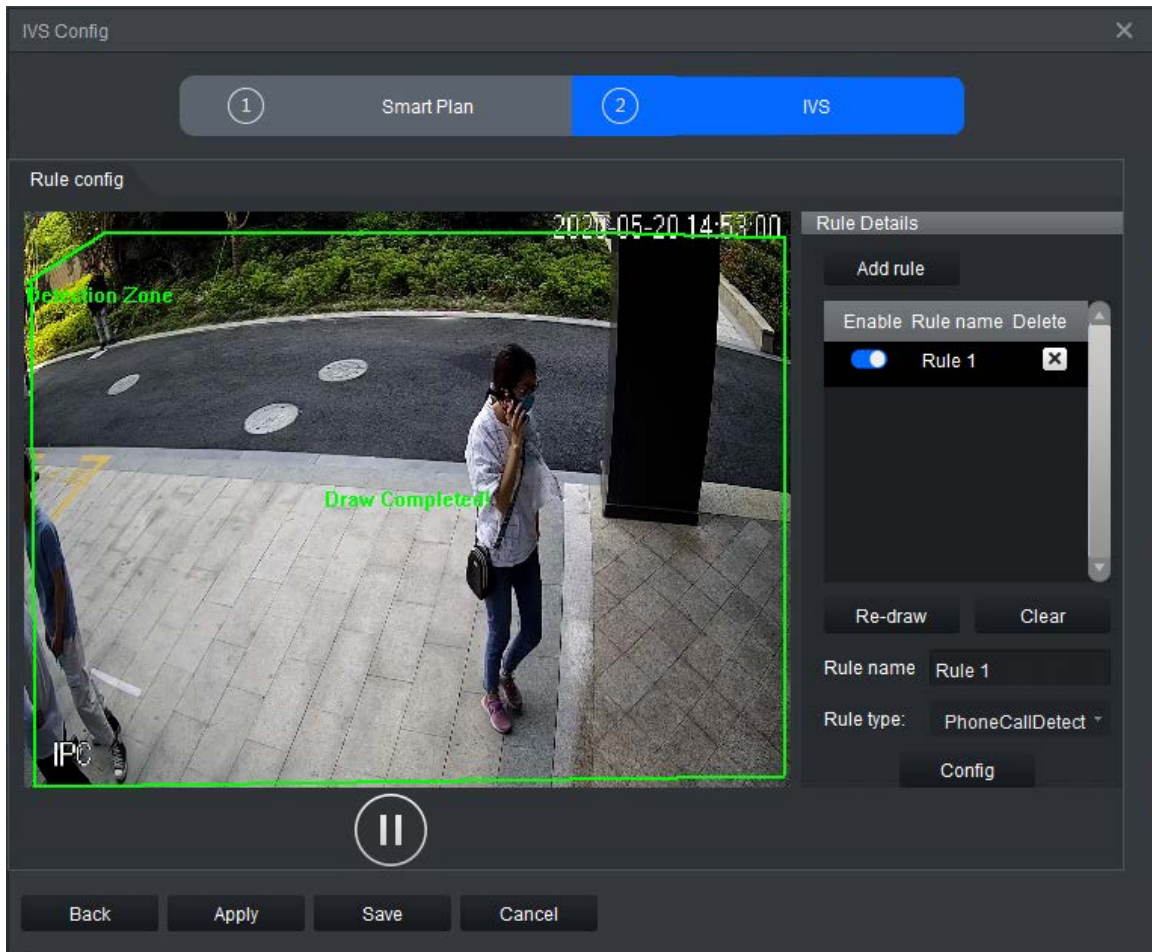
Step 2 right-click a channel, and then select **IVS Config**.

Step 3 Select the smart plan, and then click **Next** to go to the IVS page.

Step 4 Click **Add rule**.

Step 5 Enter a **Rule name** and select **PhoneCallDetect** from the rule type.

Figure 4-47 Call detection



- Step 6** Click **Config** to configure the parameters and the arming schedule.
1. Click **Parameters** to configure the parameters.

Figure 4-48 Parameters

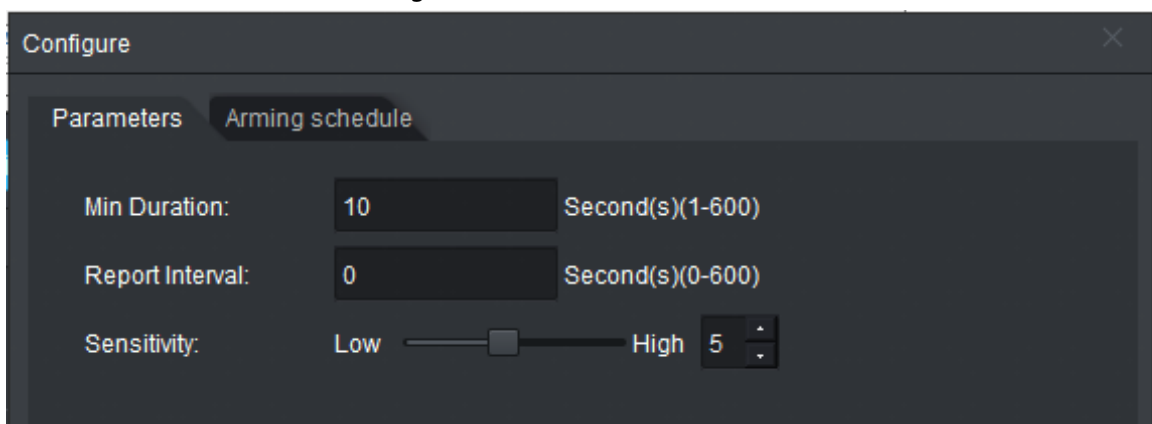



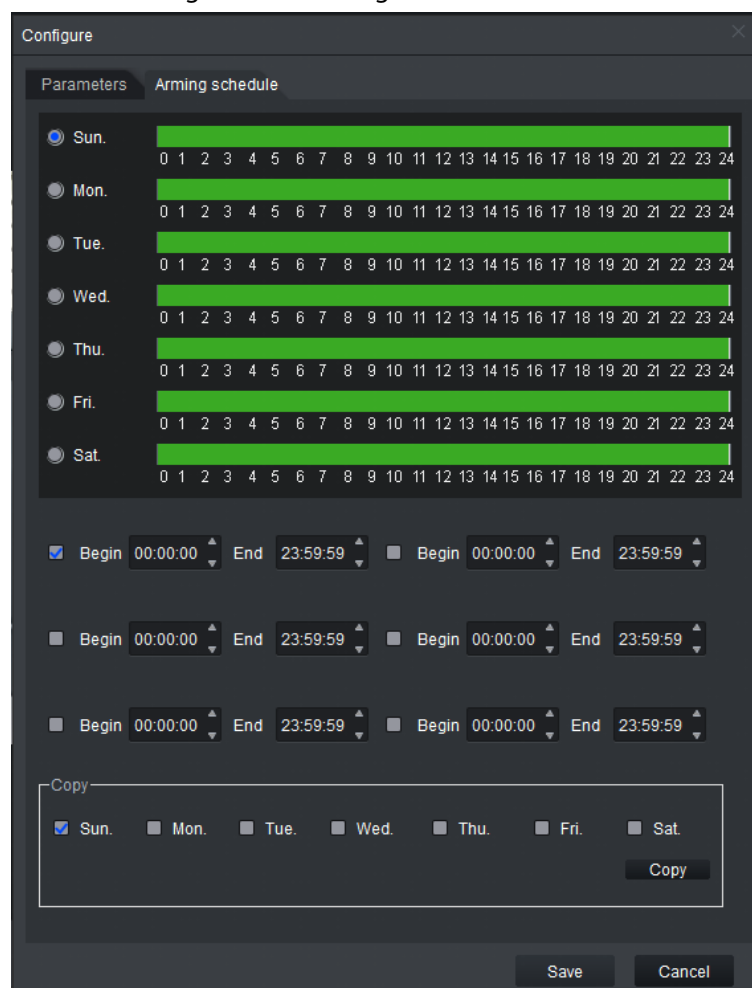
Table 4-11 Parameters

Parameter	Description
Min Duration	An alarm is triggered when a person makes a phone call in the detection area and remains on the phone for longer than the defined time.
Report Interval	When an alarm even occurs, and the target remains in the detection area for longer than the defined interval, another alarm will be triggered and information on the event will be shown on the screen.

Parameter	Description
Sensitivity	Set the sensitivity as needed. The higher the sensitivity, the easier it is for the alarm to be triggered.  The sensitivity range is 1 to 10, with 5 by default.

- Click **Arming schedule** to change the arming schedule.
  - Full-time arming is enabled by default. You can adjust the arming time.
  - You can set up to six periods for each day.
  - After configuring the arming schedule for one day, you can select other days (one or more) in the **Copy** section, and then click **Copy** to copy the configured arming schedule for other days.

Figure 4-49 Arming schedule



- Click **Save**.

#### Step 7 Save IVS.

- Click **Save** to save the IVS configuration and exit the page.
- Click **Apply** to save the IVS configuration without exiting the page.

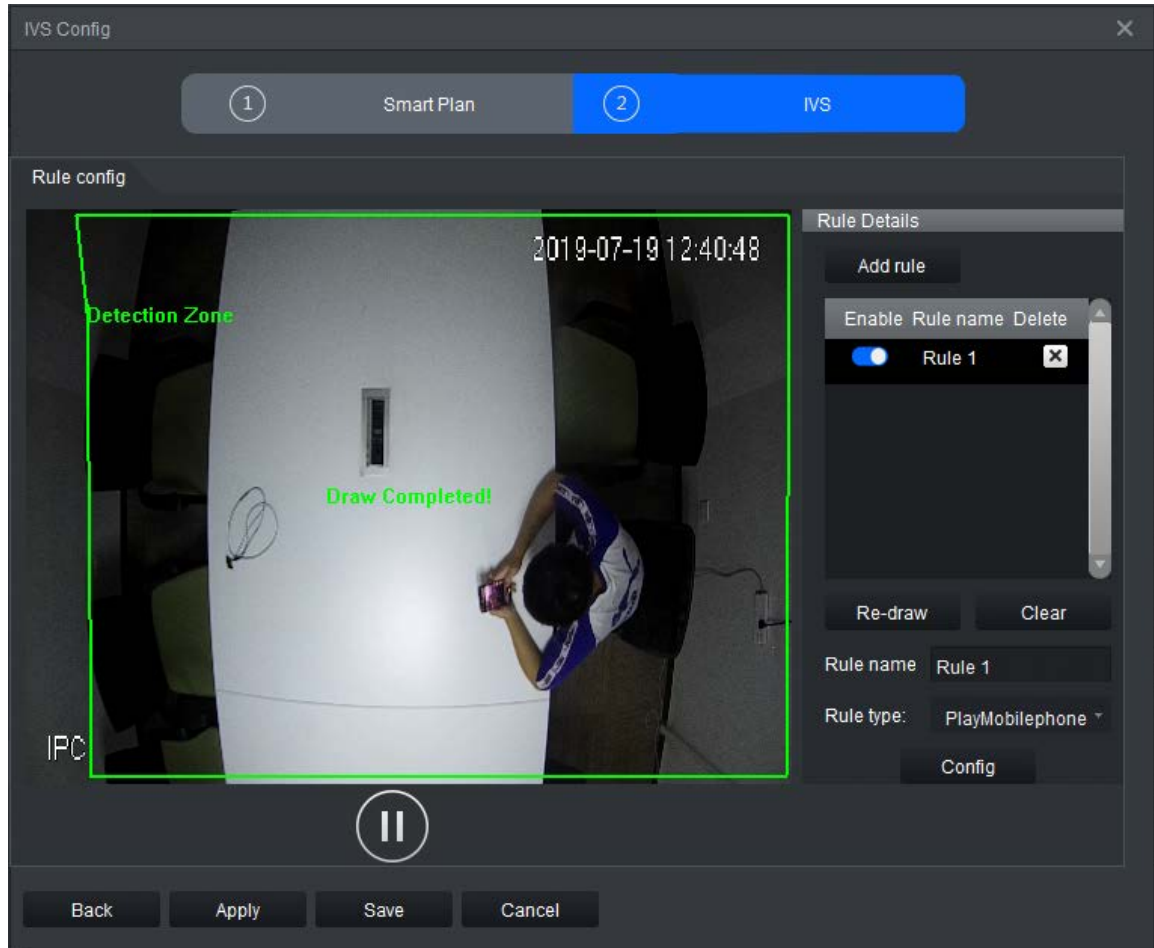
### 4.4.2.14 Using Mobile Phone Detection

An alarm is triggered when a person uses their phone in the detection area for longer than the

defined time.

- Step 1** Click **Real Monitor** on the home page of the client.
- Step 2** right-click a channel, and then select **IVS Config**.
- Step 3** Select the smart plan, and then click **Next** to go to the IVS page.
- Step 4** Click **Add rule**.
- Step 5** Enter the **Rule name** and select **PlayMobilePhone** from the rule type.

Figure 4-50 Using mobile phone detection



- Step 6** Click **Config** to configure the parameters and the arming schedule.
  1. Click **Parameters** to configure the parameters.

Figure 4-51 Parameters

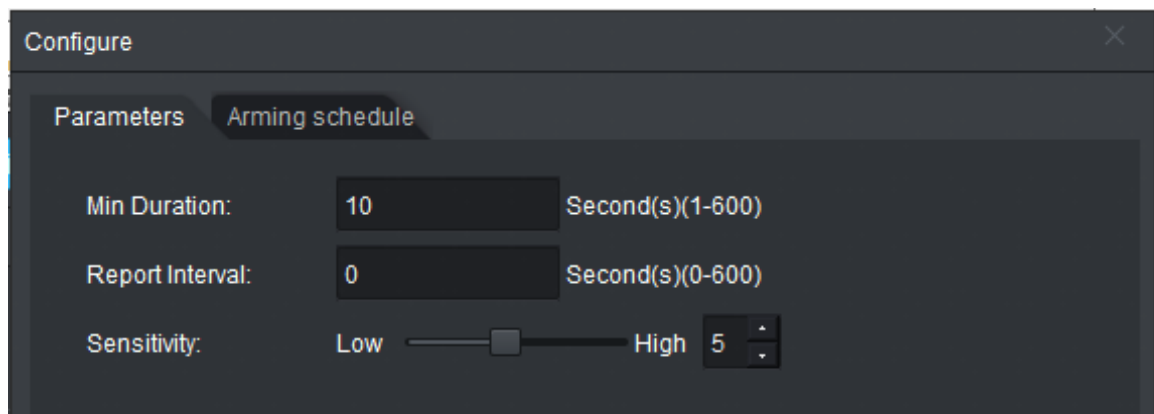



Table 4-12 Parameters

Parameter	Description
Min Duration	An alarm is triggered when a person uses their phone in the detection area for longer than the defined time.
Report Interval	When an alarm even occurs, and the target remains in the detection area for longer than the defined interval, another alarm will be triggered and information on the event will be shown on the screen.
Sensitivity	Set sensitivity as needed. The higher the sensitivity, the easier it is for the alarm to be triggered.  The sensitivity range is from 1 to 10. It is 5 by default.

2. Click **Arming schedule** to change the arming schedule.

- Full-time arming is enabled by default. You can adjust the arming time.
- You can set up to six periods for each day.
- After configuring the arming schedule for one day, you can select other days (one or more) in the **Copy** section, and then click **Copy** to copy the configured arming schedule for other days.

Figure 4-52 Arming schedule

3. Click **Save**.

**Step 7** Save IVS.

- Click **Save** to save the IVS configuration and exit the page.

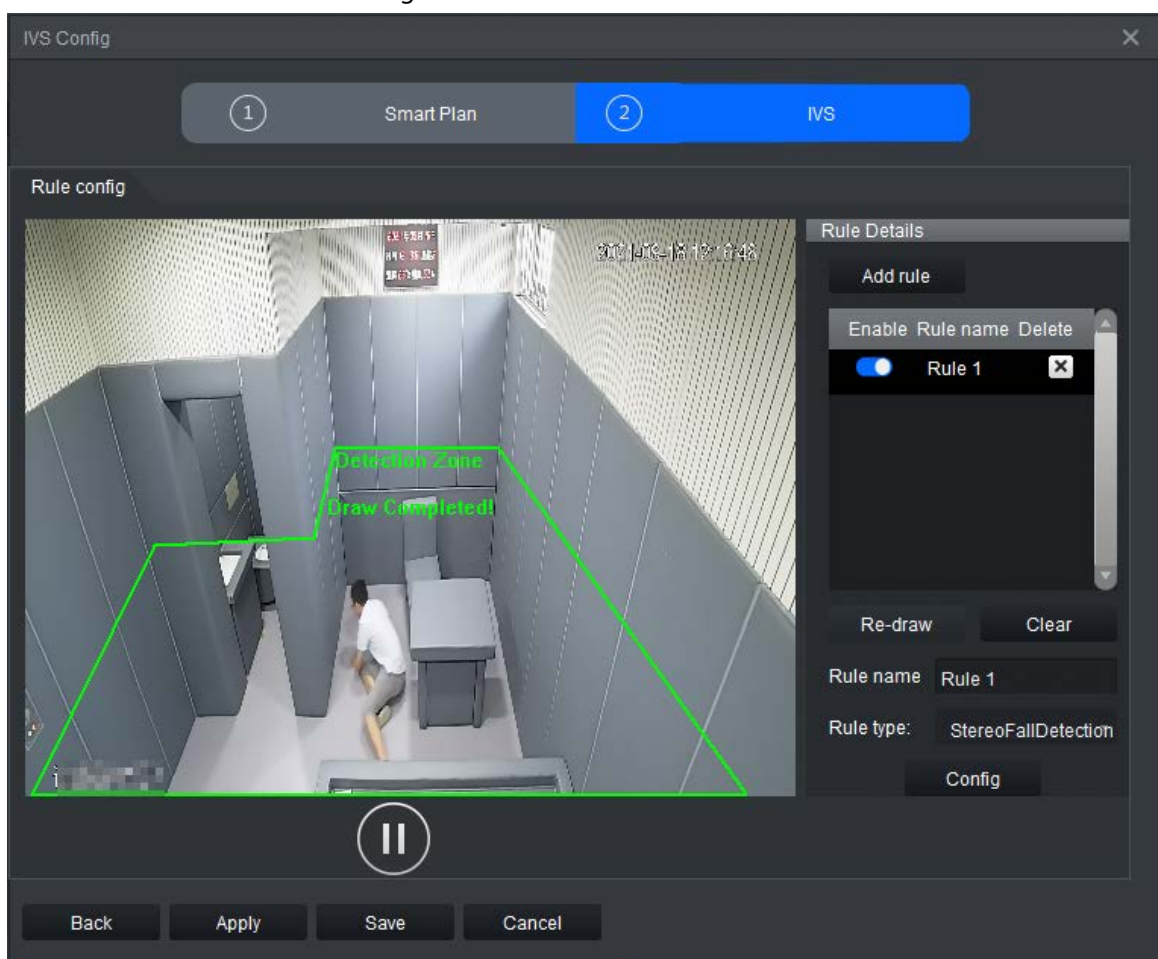
- Click **Apply** to save the IVS configuration without exiting the page.

#### 4.4.2.15 Fall Detection

An alarm is triggered when a person falls down or squats in the detection area for longer than the defined time.

- Step 1** Click **Real Monitor** on the home page of the client.
- Step 2** right-click a channel, and then select **IVS Config**.
- Step 3** Select the smart plan, and then click **Next** to go to the IVS page.
- Step 4** Click **Add rule**.
- Step 5** Enter the **Rule name** and select **StereoFallDetection** from the rule type.
- Step 6** Draw the detection area on the monitoring screen on the left.

Figure 4-53 Fall detection



- Step 7** Click **Config** to configure the parameters and arming schedule.
1. Click **Parameters** to configure the parameters.

Figure 4-54 Parameters

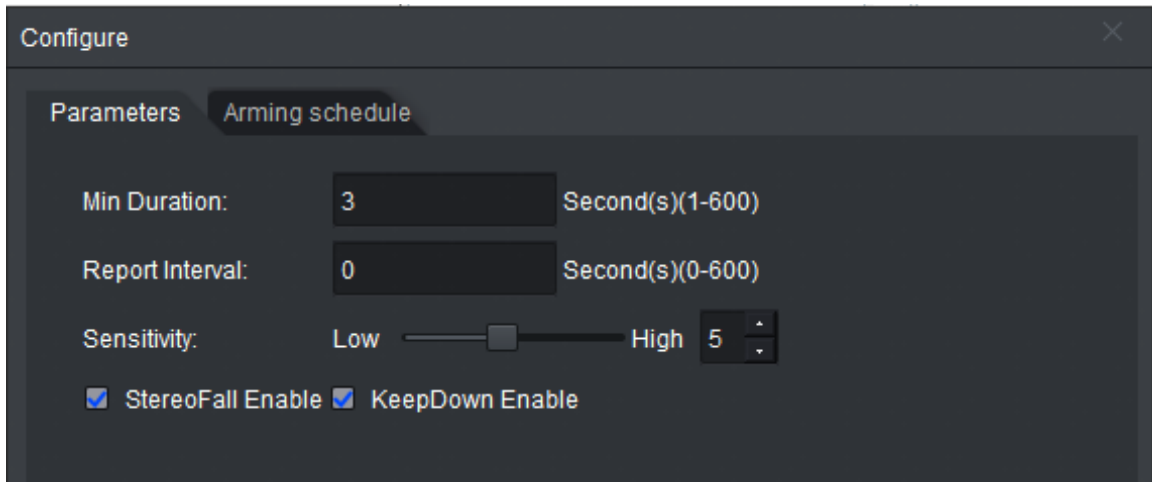




Table 4-13 Parameters

Parameter	Description
Min Duration	An alarm is triggered when a person falls down or squats in the detection area for longer than the defined time.
Report Interval	When an alarm even occurs, and the target remains in the detection area for longer than the defined interval, another alarm will be triggered and information on the event will be shown on the screen.
Sensitivity	Set the sensitivity as needed. The higher the sensitivity, the easier it is for the alarm to be triggered.  The sensitivity range is from 1 to 10. It is 5 by default.
Detection Type	<b>StereoFall Enable</b> detects people falling down and <b>KeepDown Enable</b> detects people squatting. Both are selected by default.  StereoFall Enable cannot be unselected.

2. Click **Arming schedule** to change the arming schedule.
  - Full-time arming is enabled by default. You can adjust the arming time.
  - You can set up to six periods for each day.
  - After configuring the arming schedule for one day, you can select other days (one or more) in the **Copy** section, and then click **Copy** to copy the configured arming schedule for other days.



Figure 4-55 Arming schedule

The screenshot shows a 'Configure' dialog box with the following elements:

- Parameters:** Arming schedule
- Days:** Sun. (selected), Mon., Tue., Wed., Thu., Fri., Sat.
- Time Slots:**
  - ☑ Begin 00:00:00 End 23:59:59
  - ☐ Begin 00:00:00 End 23:59:59
  - ☐ Begin 00:00:00 End 23:59:59
  - ☐ Begin 00:00:00 End 23:59:59
- Copy:**
  - ☑ Sun. ☐ Mon. ☐ Tue. ☐ Wed. ☐ Thu. ☐ Fri. ☐ Sat.
  - Copy
- Buttons:** Save, Cancel

3. Click **Save**.

**Step 8** Save IVS.

- Click **Save** to save the IVS configuration and exit the page.
- Click **Apply** to save the IVS configuration without exiting the page.

#### 4.4.2.16 Running Detection

An alarm is triggered when a person runs fast in the detection area.

**Step 1** Click **Real Monitor** on the home page of the client.

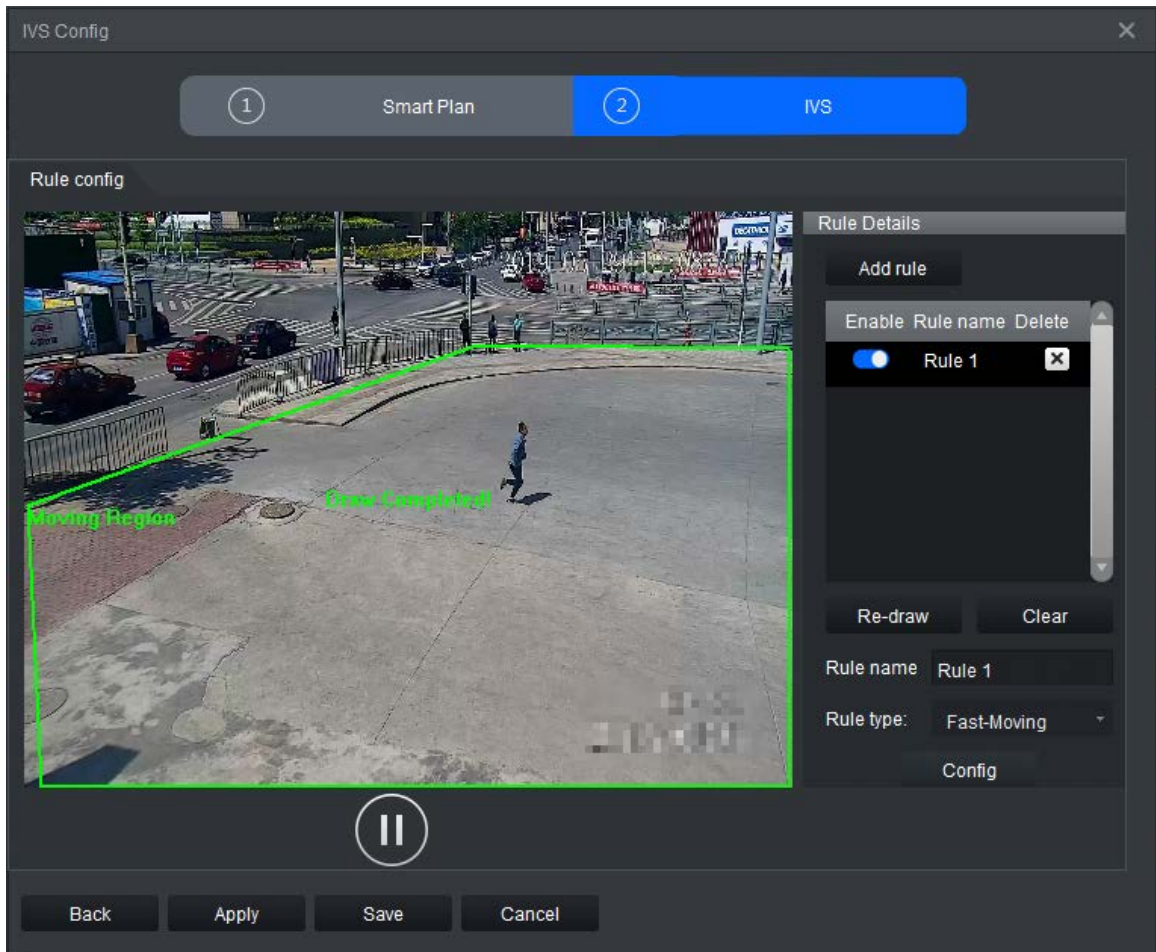
**Step 2** right-click a channel, and then select **IVS Config**.

**Step 3** Select the smart plan, and then click **Next** to go to the IVS page.

**Step 4** Click **Add rule**.

**Step 5** Enter a **Rule name** and select **Fast-moving** from the rule type.

Figure 4-56 Fast run



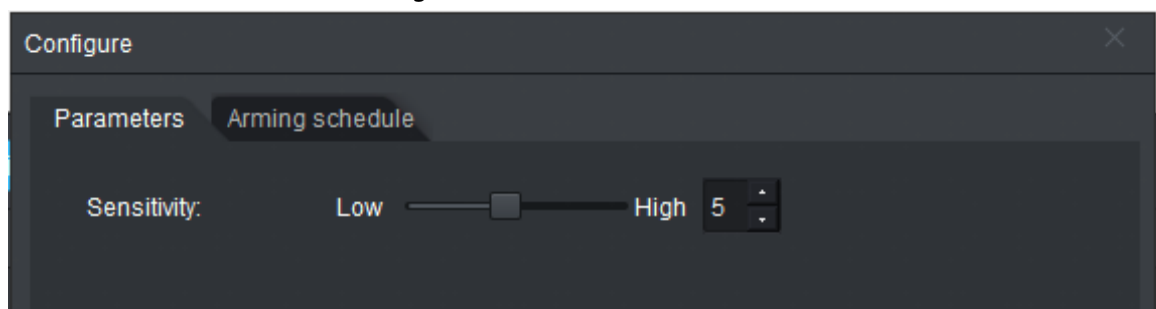
**Step 6** Click **Config** to configure the parameters and the arming schedule.

1. Click **Parameters** to set the sensitivity as needed. The higher the sensitivity, the easier it is for an alarm to be triggered.



The sensitivity range is from 1 to 10. It is 5 by default.

Figure 4-57 Parameters



2. Click **Arming schedule** to change the arming schedule.
  - Full-time arming is enabled by default. You can adjust the arming time.
  - You can set up to six periods for each day.
  - After configuring the arming schedule for one day, you can select other days (one or more) in the **Copy** section, and then click **Copy** to copy the configured arming schedule for other days.

Figure 4-58 Arming schedule

The screenshot shows a 'Configure' dialog box with the following elements:

- Parameters:** Arming schedule
- Days:** Sun. (selected), Mon., Tue., Wed., Thu., Fri., Sat.
- Time Slots:** Each day has a 24-hour bar (0-24) with a green segment indicating the arming period. Below each bar are 'Begin' and 'End' time pickers.
- Copy Section:** A box containing radio buttons for Sun. (checked), Mon., Tue., Wed., Thu., Fri., and Sat., with a 'Copy' button.
- Buttons:** 'Save' and 'Cancel' at the bottom right.

3. Click **Save**.

Step 7 Save IVS.

- Click **Save** to save the IVS configuration and exit the page.
- Click **Apply** to save the IVS configuration without exiting the page.

#### 4.4.2.17 Smoking Detection

An alarm is triggered when a person smokes in the detection area for longer than the defined time.

Step 1 Click **Real Monitor** on the home page of the client.

Step 2 right-click a channel, and then select **IVS Config**.

Step 3 Select the smart plan, and then click **Next** to go to the IVS page.

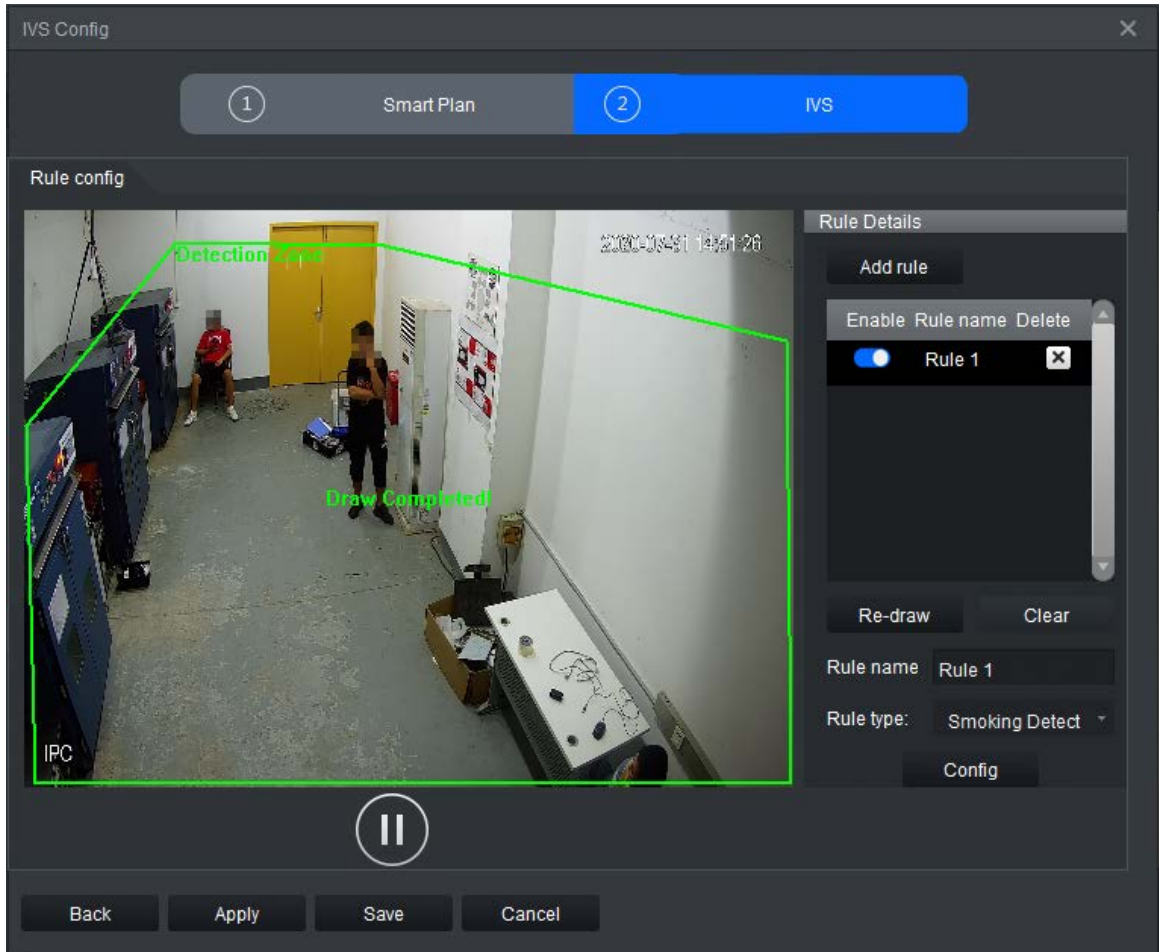
Step 4 Click **Add rule**.

Step 5 Enter the **Rule name** and select **Smoking Detect** from the rule type.



A maximum of 16 channels can be configured with the smoking detection rule.

Figure 4-59 Smoking detection



**Step 6** Click **Config** to configure the parameters and arming schedule.

1. Click **Parameters** to configure the parameters.

Figure 4-60 Parameters

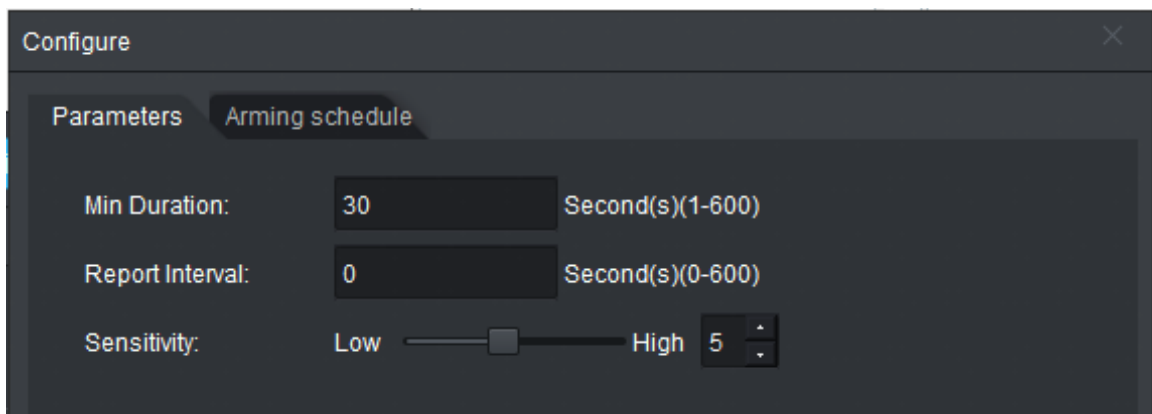



Table 4-14 Parameters

Parameter	Description
Min Duration	An alarm is triggered when a person smokes in the detection area for longer than the minimum duration.
Report Interval	When an alarm even occurs, and the target remains in the detection area for longer than the defined interval, another alarm will be triggered and information on the event will be shown on the screen.

Parameter	Description
Sensitivity	Set the sensitivity as needed. The higher the sensitivity, the easier it is for the alarm to be triggered.  The sensitivity range is from 1 to 10. It is 5 by default.

2. Click **Arming schedule** to change the arming schedule.
  - Full-time arming is enabled by default. You can adjust the arming time.
  - You can set up to six periods for each day.
  - After configuring the arming schedule for one day, you can select other days (one or more) in the **Copy** section, and then click **Copy** to copy the configured arming schedule for other days.

Figure 4-61 Arming schedule



3. Click **Save**.

#### Step 7 Save IVS.

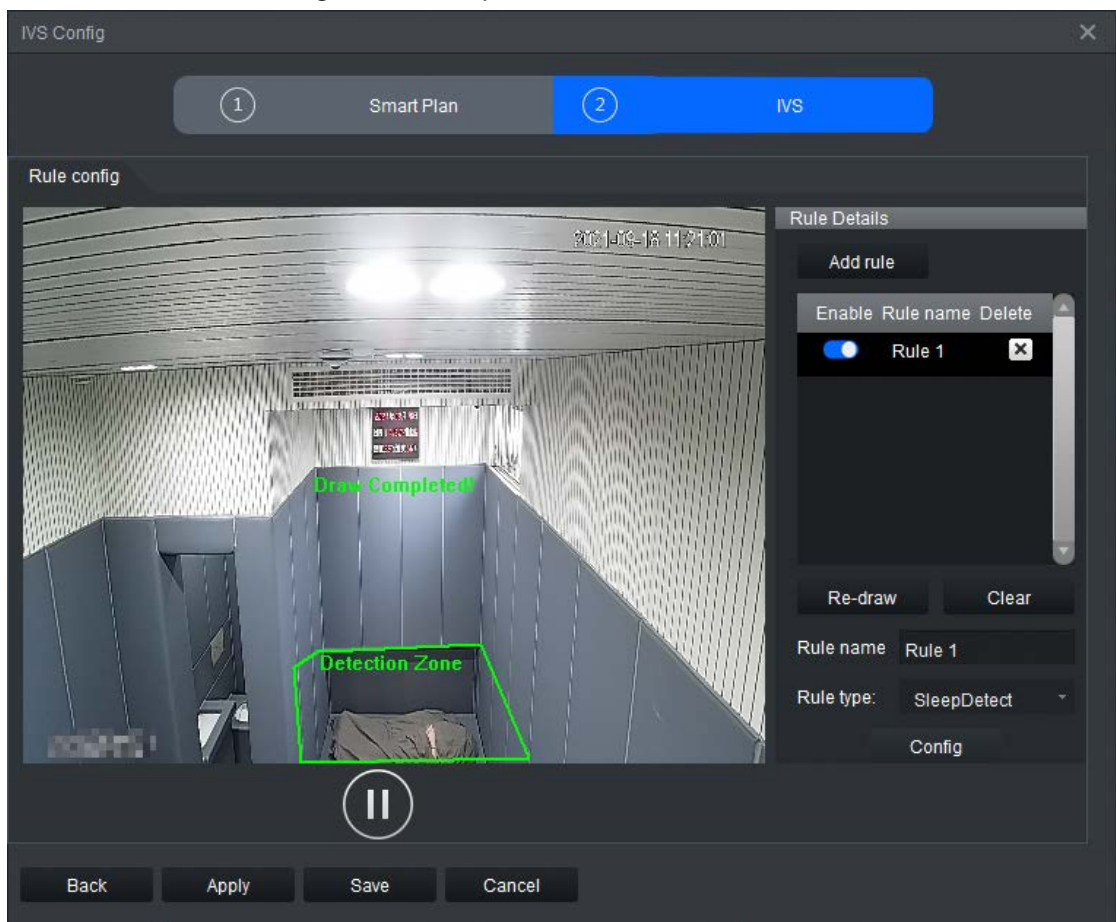
- Click **Save** to save the IVS configuration and exit the page.
- Click **Apply** to save the IVS configuration without exiting the page.

#### 4.4.2.18 Sleeping with Quilt Covering Head Detection

An alarm is triggered when a person sleeps with their head covered for longer than the defined time.

- Step 1 Click **Real Monitor** on the home page of the client.
- Step 2 right-click a channel, and then select **IVS Config**.
- Step 3 Select the smart plan, and then click **Next** to go to the IVS page.
- Step 4 Click **Add rule**.
- Step 5 Enter the **Rule name** and select **SleepDetect** from the rule type.  
Draw a detection area on the monitoring screen on the left.

Figure 4-62 Sleep with head covered



- Step 6 Click **Config** to configure the parameters and the arming schedule.
  1. Click **Parameters** to configure the parameters.

Figure 4-63 Parameters

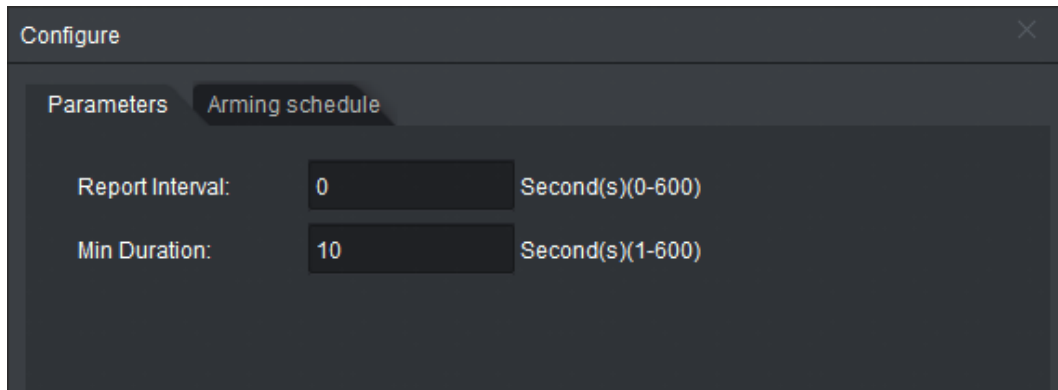
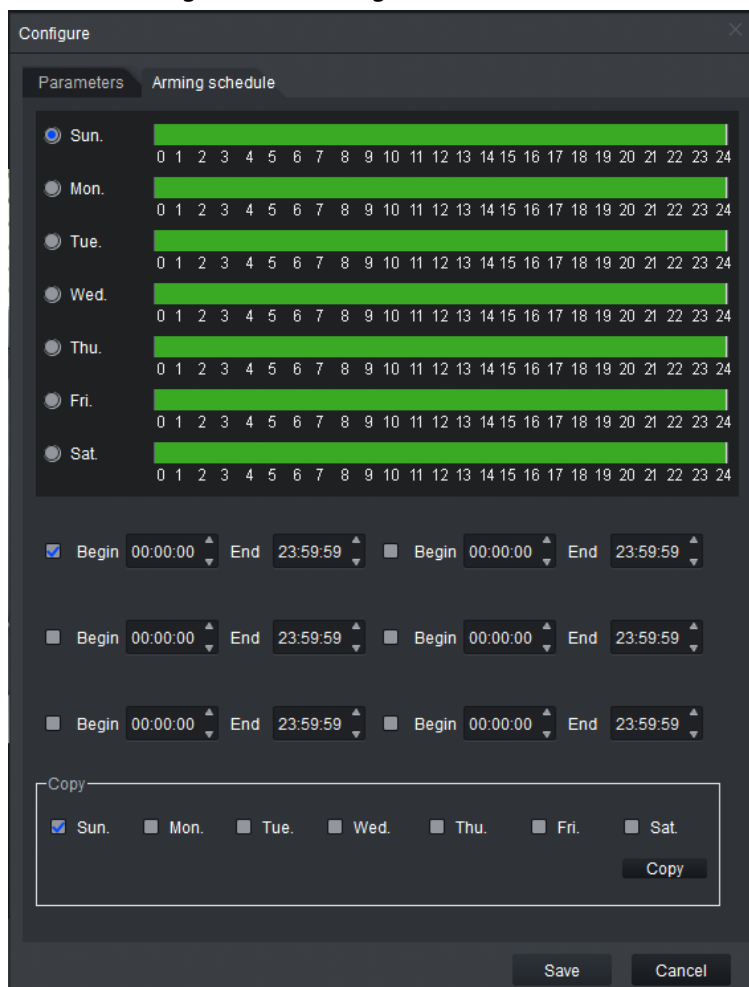


Table 4-15 Parameters

Parameter	Description
Min Duration	An alarm is triggered when a person sleeps with their head covered for longer than the minimum duration.
Report Interval	When an alarm even occurs, and the target remains in the detection area for longer than the defined interval, another alarm will be triggered and information on the event will be shown on the screen.

2. Click **Arming schedule** to change the arming schedule.
  - Full-time arming is enabled by default. You can adjust the arming time.
  - You can set up to six periods for each day.
  - After configuring the arming schedule for one day, you can select other days (one or more) in the **Copy** section, and then click **Copy** to copy the configured arming schedule for other days.

Figure 4-64 Arming schedule



3. Click **Save**.

Step 7 Save IVS.

- Click **Save** to save the IVS configuration and exit the page.
- Click **Apply** to save the IVS configuration without exiting the page.

#### 4.4.2.19 Posture Detection

An alarm is triggered when a person hits the wall repeatedly for longer than the defined time.

Step 1 Click **Real Monitor** on the home page of the client.

Step 2 right-click a channel, and then select **IVS Config**.

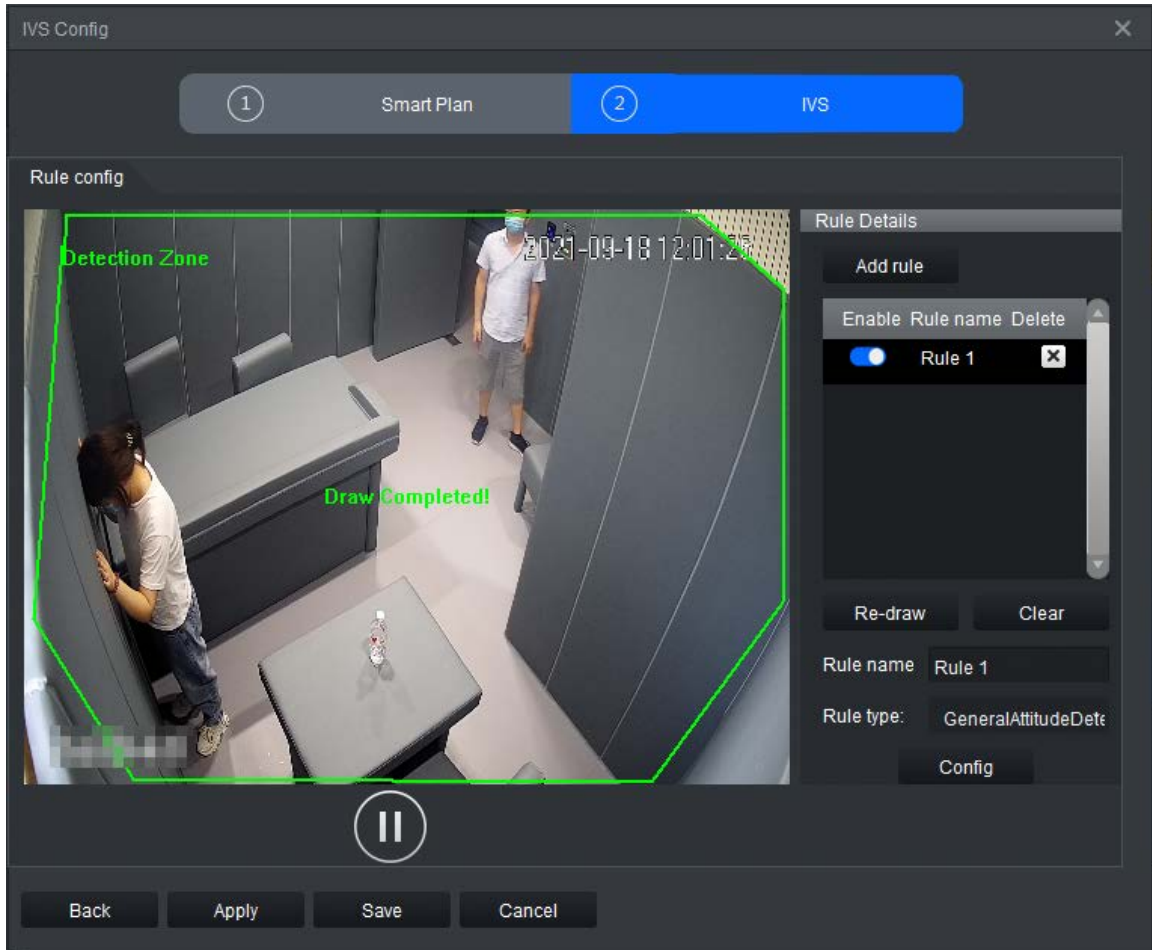
Step 3 Select the smart plan, and then click **Next** to go to the IVS page.

Step 4 Click **Add rule**.

Step 5 Enter a **Rule name** and select **GeneralAttitudeDetection** from the rule type.



Figure 4-65 Posture detection



**Step 6** Click **Config** to configure the parameters and the arming schedule.

1. Click **Parameters** to configure the parameters.

Figure 4-66 Parameters

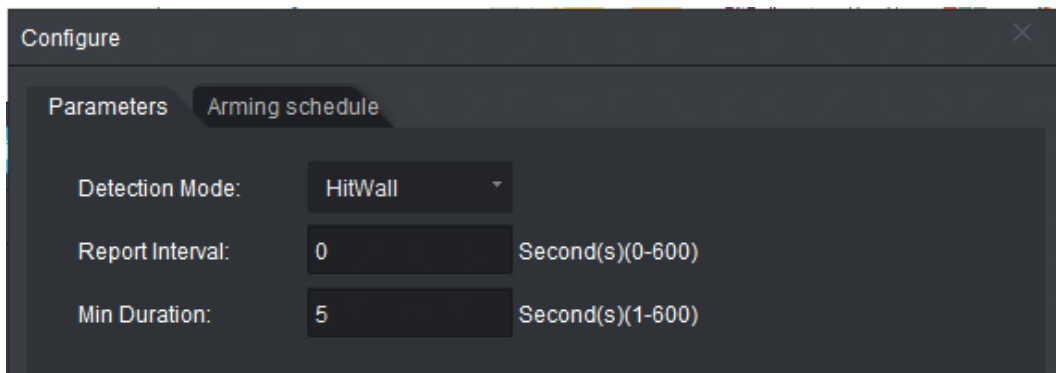



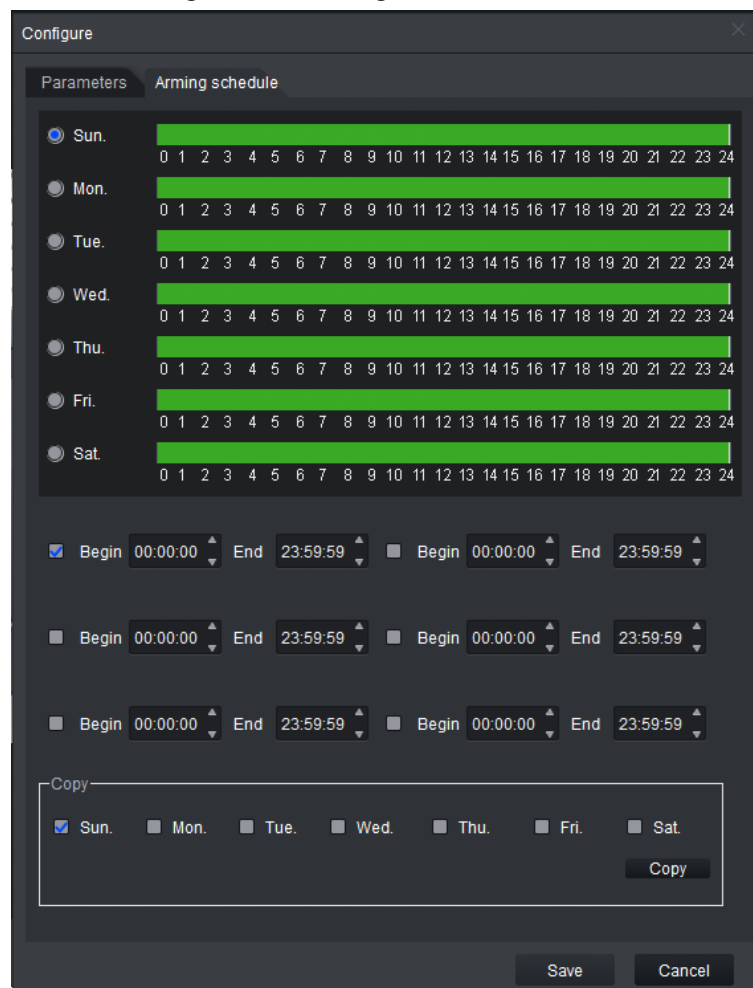
Table 4-16 Parameters

Parameter	Description
Detection Mode	Select <b>HitWall</b> .  Standing up and running into a wall is included in fast run detection.
Min Duration	An alarm is triggered when a person hits the wall repeatedly for longer than the minimum duration.

Parameter	Description
Report Interval	When an alarm even occurs, and the target remains in the detection area for longer than the defined interval, another alarm will be triggered and information on the event will be shown on the screen.

- Click **Arming schedule** to change the arming schedule.
  - Full-time arming is enabled by default. You can adjust the arming time.
  - You can set up to six periods for each day.
  - After configuring the arming schedule for one day, you can select other days (one or more) in the **Copy** section, and then click **Copy** to copy the configured arming schedule for other days.

Figure 4-67 Arming schedule



- Click **Save**.

#### Step 7 Save IVS.

- Click **Save** to save the IVS configuration and exit the page.
- Click **Apply** to save the IVS configuration without exiting the page.

### 4.4.3 Video Quality Diagnosis

Video quality diagnosis includes detection of video loss, overly dim images, overly bright images, color cast, blurred images, B/W images, dithering video, frozen images, tampering video, and scene change. An alarm is triggered when any of the values for the video quality diagnosis rules is

exceeded in the video.

## Prerequisites

Server has been added. For details, see "4.3.1 Adding Devices".

## Procedure


- Step 1 On the home page of the client, click **Device Manager** > .
- Step 2 Select **Enable** to enable video quality diagnosis.
- Step 3 Configure the parameters.

Figure 4-68 Video Quality Diagnosis

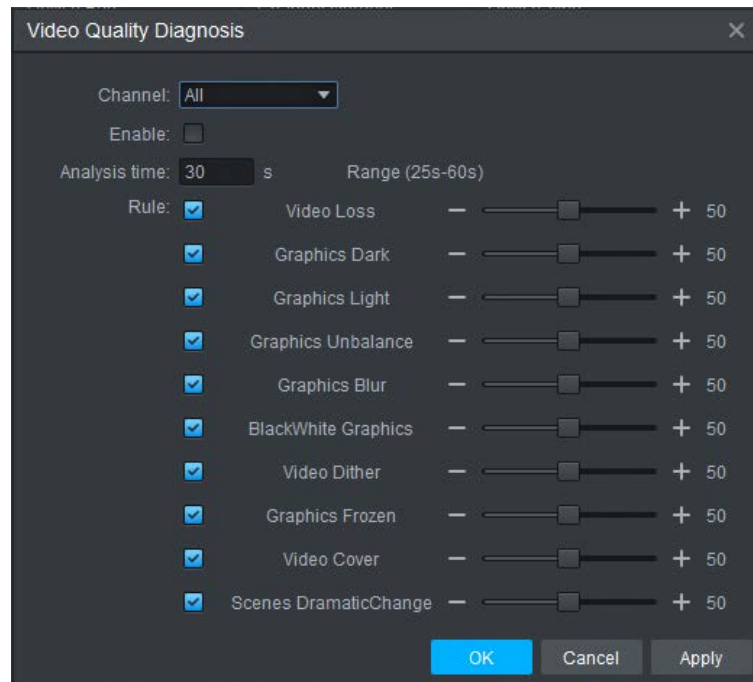



Table 4-17 Parameter description

Item	Description
Channel	Select all the channels.
Analysis time	Select the range for the video analysis duration from 25 s to 60 s.  It is 30 s by default.
Rule	Select required diagnosis rules, and then drag the slider to configure the value, which ranges from 1 to 100.

- Step 4 Click **OK**.

## 4.4.4 (Optional) Target Filter

Target filter is used to customize the size of the target and to keep targets within range. It can be to

filter out targets that are too small or too large.



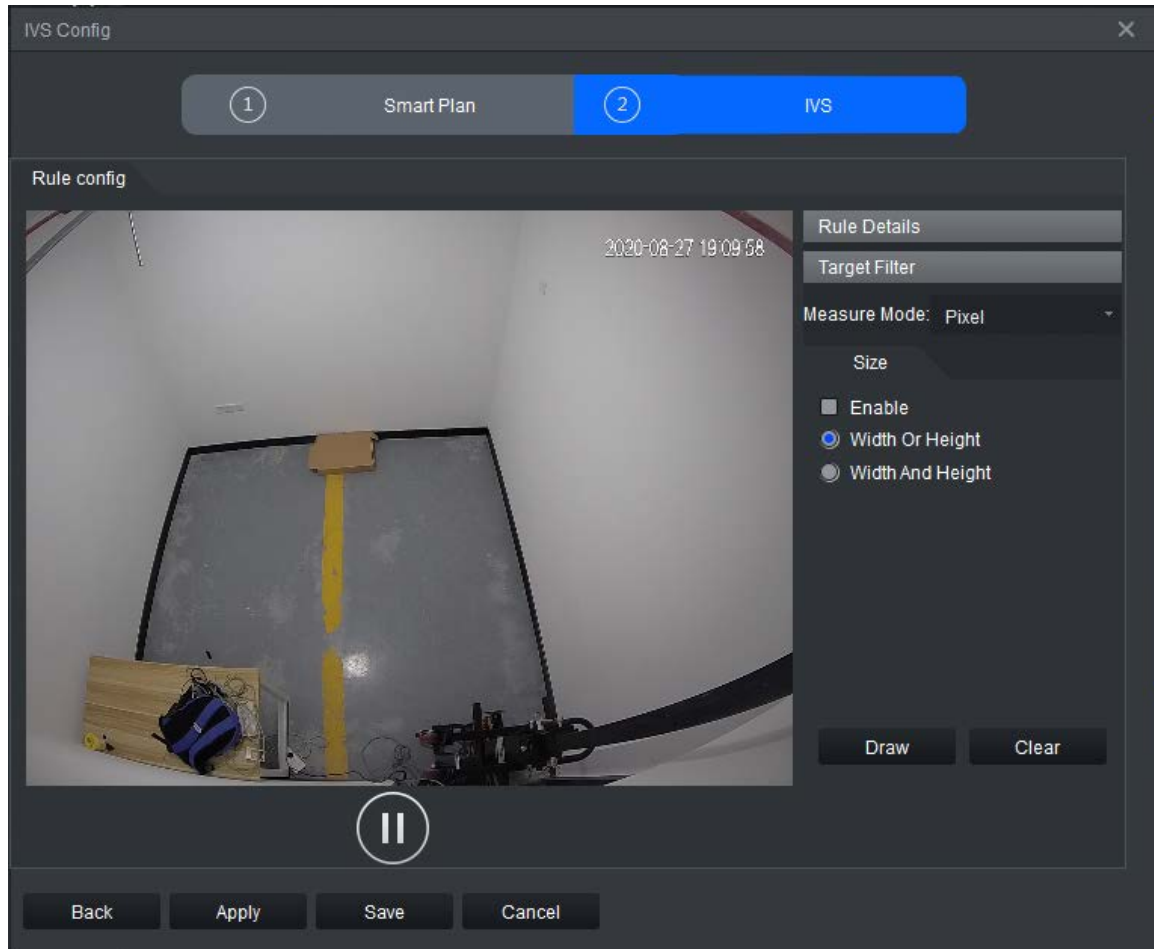
Target filter is available for tripwire, intrusion, climbing detection, getting up detection, sleep detection, and staying alone detection.

**Step 1** Click **Real Monitor** on the home page.

**Step 2** right-click a channel, and then select **IVS Config**.

**Step 3** Click **Target Filter**.

Figure 4-69 Target filter



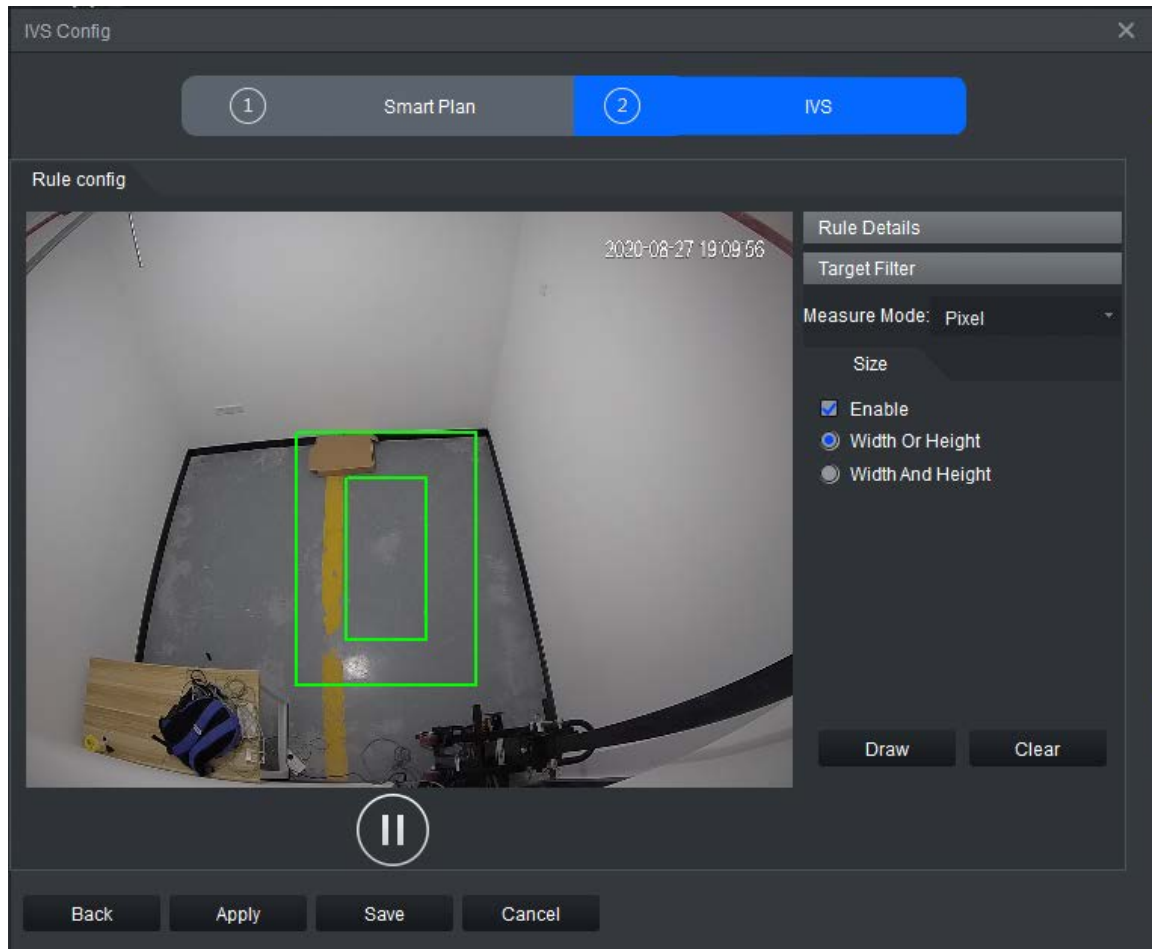
**Step 4** Select **Enable**, and then select **Width Or Height** or **Width And Height** as the filter mode.



**Width And Height** means that both width and height should be met; **Width Or Height** means that either width or height should be met.

**Step 5** Click **Draw** to draw a filter, and then adjust the size of the outer box and inner box separately.

Figure 4-70 Draw filter boxes



**Step 6** Save IVS.

- Click **Save** to save the IVS configuration and exit the page.
- Click **Apply** to save the IVS configuration without exiting the page.

## 4.5 Real-time Monitoring

Log in to the server remotely at the client to view the real-time monitoring image.

**Step 1** Click **Real Monitor** on the home page.



View the server list on the left side.

- indicates that the server is offline. right-click a server and then click **Login** to log in to the server.
- indicates that the server is online. right-click a server and then click **Logout** to log out of the server.

**Step 2** (Optional) Click the drop-down box, and then select the display scale of the video image. Click and select window layout.

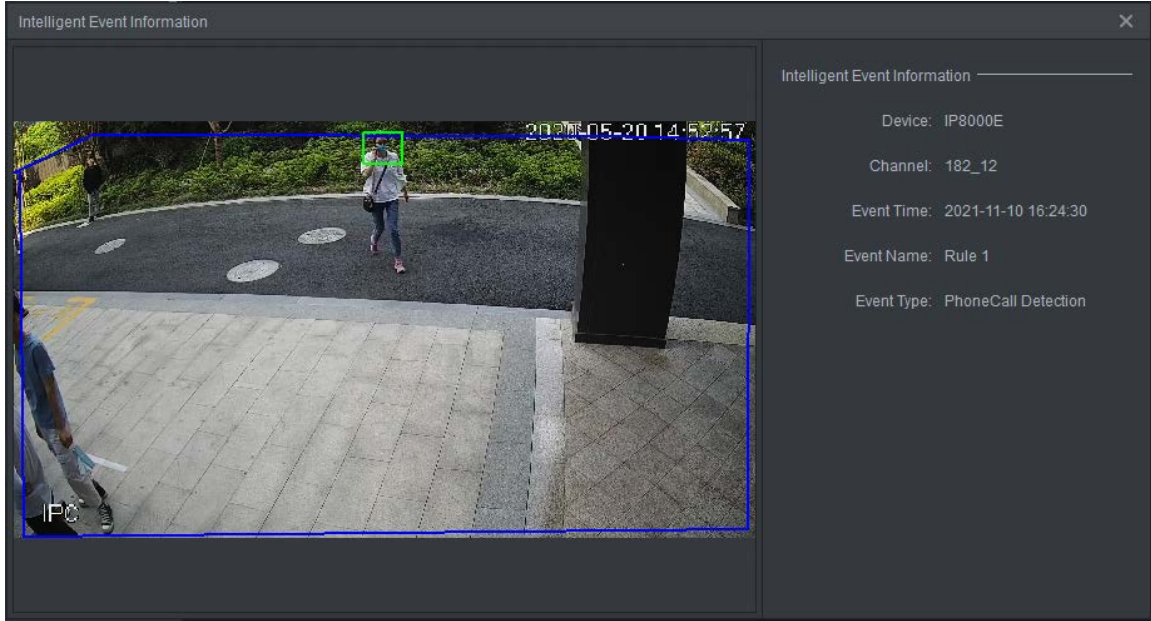
**Step 3** Enable real-time channel monitoring.

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

**Monitoring.**  indicates that the channel is in live view.  indicates that the live view of the channel is not enabled.

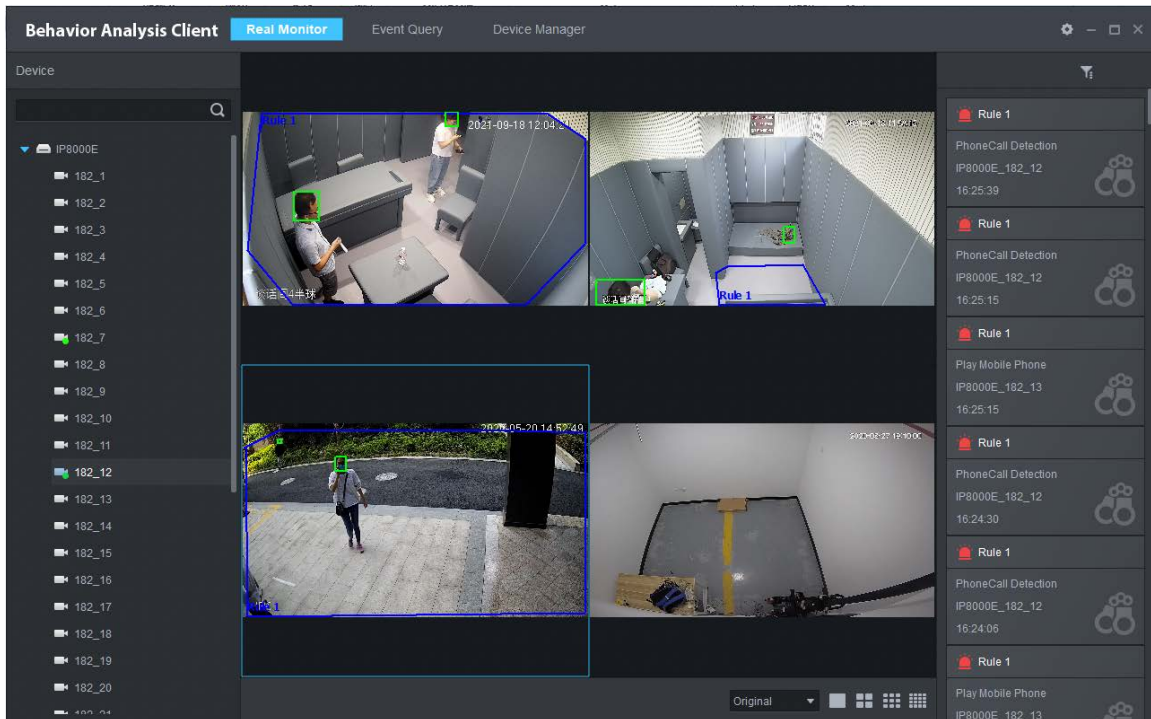
Intelligent event alarm information is displayed on the right side. Double-click the alarm information to view details.

Figure 4-71 Alarm details



Right-click a channel and then select **IVS Config** to enter the IVS page.

Figure 4-72 Real-time monitoring



## 4.6 Searching for Alarm Information

Search for the alarm event information of channels that are on the event detection server within the defined time.

### Procedure


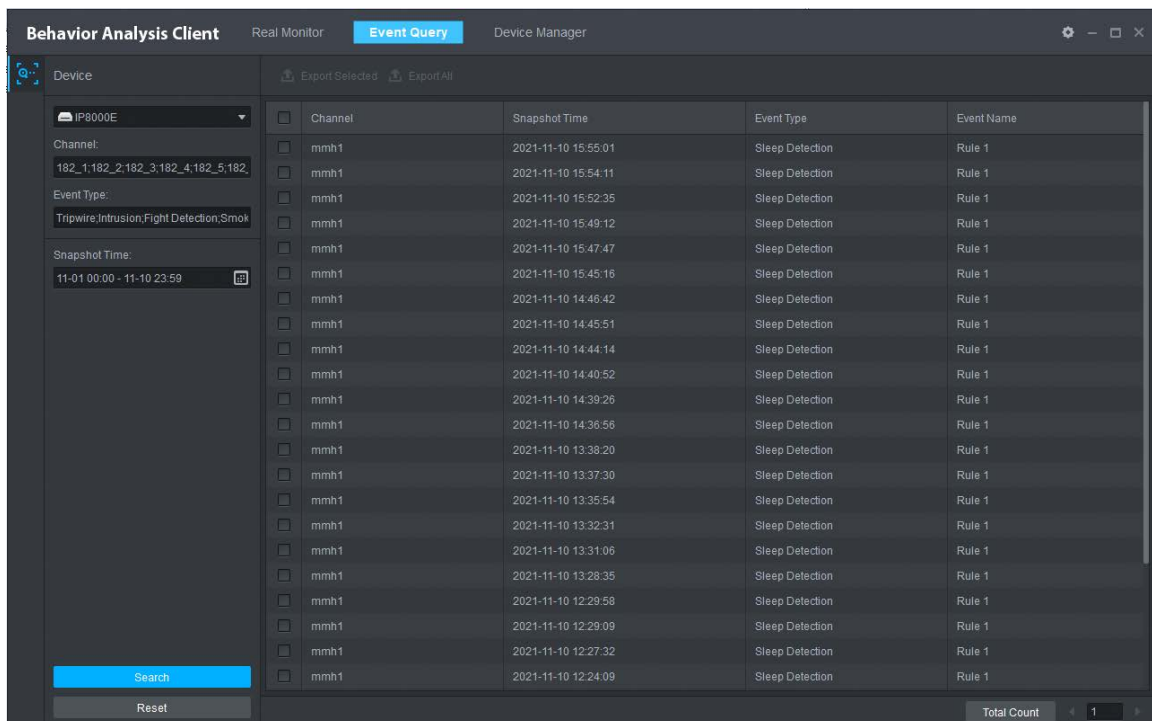
- Step 1** Select **Event Query** > .
- Step 2** Select a server and channels under it.
- Step 3** Select **Event Type**.
- Step 4** Set **Snapshot Time**.
- Step 5** Click **Search**.  
Click **Total Count** at the lower-right corner, and the records are displayed.

Figure 4-73 Select event time



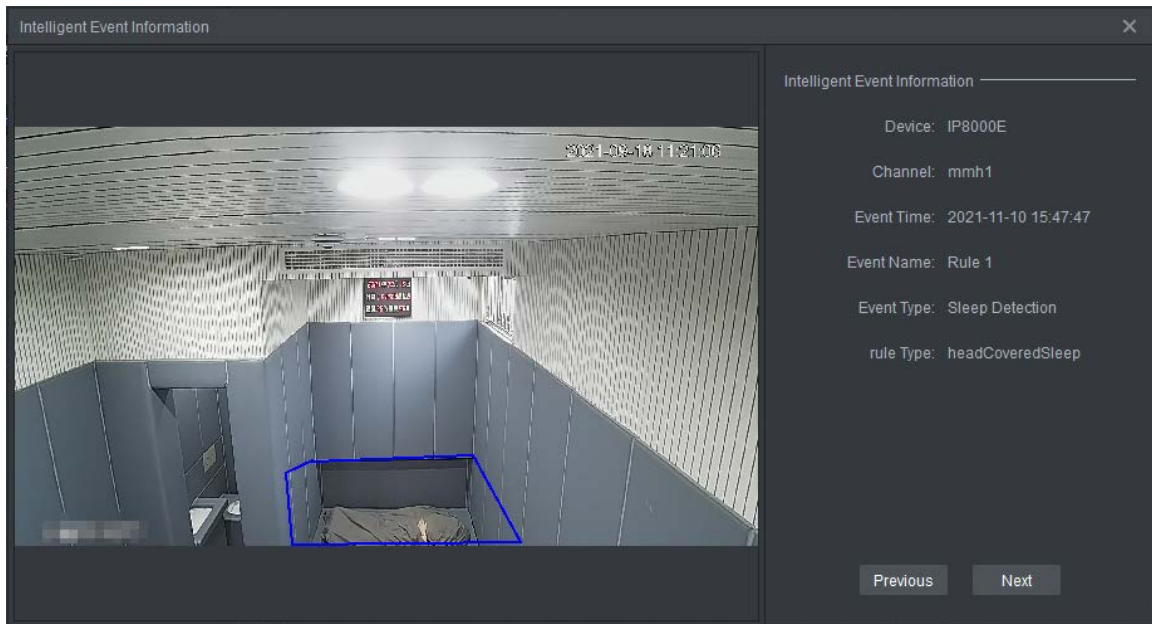
The screenshot shows the 'Behavior Analysis Client' interface with the 'Event Query' tab selected. The left sidebar contains filters for 'Device' (IP8000E), 'Channel' (182\_1;182\_2;182\_3;182\_4;182\_5;182), 'Event Type' (Tripwire,Intrusion,Fight Detection,Smok), and 'Snapshot Time' (11-01 00:00 - 11-10 23:59). The main area displays a table of search results.

Channel	Snapshot Time	Event Type	Event Name
<input type="checkbox"/> mhm1	2021-11-10 15:55:01	Sleep Detection	Rule 1
<input type="checkbox"/> mhm1	2021-11-10 15:54:11	Sleep Detection	Rule 1
<input type="checkbox"/> mhm1	2021-11-10 15:52:35	Sleep Detection	Rule 1
<input type="checkbox"/> mhm1	2021-11-10 15:49:12	Sleep Detection	Rule 1
<input type="checkbox"/> mhm1	2021-11-10 15:47:47	Sleep Detection	Rule 1
<input type="checkbox"/> mhm1	2021-11-10 15:45:16	Sleep Detection	Rule 1
<input type="checkbox"/> mhm1	2021-11-10 14:46:42	Sleep Detection	Rule 1
<input type="checkbox"/> mhm1	2021-11-10 14:45:51	Sleep Detection	Rule 1
<input type="checkbox"/> mhm1	2021-11-10 14:44:14	Sleep Detection	Rule 1
<input type="checkbox"/> mhm1	2021-11-10 14:40:52	Sleep Detection	Rule 1
<input type="checkbox"/> mhm1	2021-11-10 14:39:26	Sleep Detection	Rule 1
<input type="checkbox"/> mhm1	2021-11-10 14:36:56	Sleep Detection	Rule 1
<input type="checkbox"/> mhm1	2021-11-10 13:38:20	Sleep Detection	Rule 1
<input type="checkbox"/> mhm1	2021-11-10 13:37:30	Sleep Detection	Rule 1
<input type="checkbox"/> mhm1	2021-11-10 13:35:54	Sleep Detection	Rule 1
<input type="checkbox"/> mhm1	2021-11-10 13:32:31	Sleep Detection	Rule 1
<input type="checkbox"/> mhm1	2021-11-10 13:31:06	Sleep Detection	Rule 1
<input type="checkbox"/> mhm1	2021-11-10 13:28:35	Sleep Detection	Rule 1
<input type="checkbox"/> mhm1	2021-11-10 12:29:58	Sleep Detection	Rule 1
<input type="checkbox"/> mhm1	2021-11-10 12:29:09	Sleep Detection	Rule 1
<input type="checkbox"/> mhm1	2021-11-10 12:27:32	Sleep Detection	Rule 1
<input type="checkbox"/> mhm1	2021-11-10 12:24:09	Sleep Detection	Rule 1

At the bottom right, the 'Total Count' is displayed as 1.

- Step 6** Double-click the alarm event record to view the alarm event. Click **Previous** or **Next** to view details on other intelligent events.

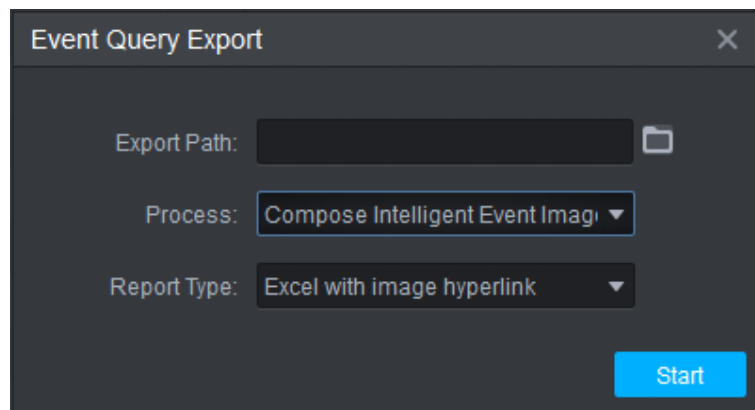
Figure 4-74 Intelligent event details



### Related Operations

- Select the alarm records as needed, and then click **Export Selected** to export them to your computer in CSV, Excel or TXT format.

Figure 4-75 Alarm



- Click **Total Count** at the lower-right corner, and then click **Export All** to export all alarm records to your computer in CSV, Excel or TXT format.



# 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 equipment 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 equipment (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 equipment 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 equipment network security:**

### **1. Physical Protection**

We suggest that you perform physical protection to equipment, especially storage devices. For example, place the equipment 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 equipment (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 equipment 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 equipment, 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 equipment 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 equipment, 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 equipment 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](http://www.dahuasecurity.com) | Postcode: 310053

Email: [dhoverseas@dhvisiontech.com](mailto:dhoverseas@dhvisiontech.com) | Tel: +86-571-87688888 28933188