



Abnormal Event Analysis Server

User Manual

Legal Information

About this Document

- This Document includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only.
- The information contained in the Document is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of the Document at the Hikvision website (<https://www.hikvision.com>). Unless otherwise agreed, Hangzhou Hikvision Digital Technology Co., Ltd. or its affiliates (hereinafter referred to as "Hikvision") makes no warranties, express or implied.
- Please use the Document with the guidance and assistance of professionals trained in supporting the Product.

About this Product

- This product can only enjoy the after-sales service support in the country or region where the purchase is made.
- If the product you choose is a video product, please scan the following QR code to obtain the "Initiatives on the Use of Video Products", and read it carefully.



Acknowledgment of Intellectual Property Rights

- Hikvision owns the copyrights and/or patents related to the technology embodied in the Products described in this Document, which may include licenses obtained from third parties.
- Any part of the Document, including text, pictures, graphics, etc., belongs to Hikvision. No part of this Document may be excerpted, copied, translated, or modified in whole or in part by any means without written permission.
- **HIKVISION** and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.
- Other trademarks and logos mentioned are the properties of their respective owners.
- **HDMI**™ The terms HDMI, HDMI High-Definition Multimedia Interface, HDMI Trade dress and the HDMI Logos are trademarks or registered trademarks of HDMI Licensing Administrator, Inc.
- The following trademark is owned by Access Advance LLC and shall not be used without authorization.



LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.
- YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
- YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.
- IN THE EVENT OF ANY CONFLICTS BETWEEN THIS DOCUMENT AND THE APPLICABLE LAW, THE LATTER PREVAILS.

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

Preface

The purpose of this section is to make sure the user can use the product correctly in this manual to avoid risky operation or property damage. Before using this product, please read the product manual carefully and keep it for future reference.

Overview

This manual describes the instructions for abnormal event detection server and guides you in configuring and operating the server.

Symbol Conventions

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

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

TABLE OF CONTENTS

Chapter 1 Activation and Login	1
1.1 System Requirements	1
1.2 Activate	1
1.2.1 Activate via SADP	1
1.2.2 Activate via Web	2
1.3 Log In.....	2
Chapter 2 Device Access	4
2.1 Add Video Device.....	4
2.2 Group Video Devices.....	4
2.3 Add Video File	5
Chapter 3 Intelligent Application	6
3.1 Application Management	6
3.1.1 Import Application	6
3.2 Allocate Algorithm Resource	7
3.3 Task Management	7
3.3.1 Task Overview	7
3.3.2 Configure Event.....	8
3.3.3 Add Task.....	8
3.4 Description of Drawing Event Rule Areas	10
3.5 Description of Configuring Event Rule Parameters	11
3.5.1 General Parameters	11
3.5.2 Specific Parameters	12
3.6 Examples of Configuring Event Rules.....	15
3.6.1 Trend Analysis Event.....	15
3.6.2 Street Behavior Event	17
3.6.3 Indoor Event	18
3.6.4 Perimeter Protection Event	23
3.7 Description of Configuring Advanced Parameters.....	26
Chapter 4 Intelligent Search	27
Chapter 5 System Configuration	28
5.1 System Settings.....	28
5.1.1 Basic Information	28
5.1.2 Time Configuration	28
5.2 User Management	28
5.2.1 Add/Edit User.....	28
5.2.2 View Online User	28
5.3 Network Configuration	28
5.3.1 Basic Settings	28
5.3.2 Platform Access.....	29
5.3.3 Network Service	30
5.3.4 Alarm Configuration.....	30
Chapter 6 Maintenance and Security	32
6.1 System Maintenance	32
6.1.1 Restart.....	32
6.1.2 Upgrade	32
6.1.3 Backup and Restore	32
6.1.4 Log.....	33
6.1.5 Device Debugging	33
6.2 View Hardware Information	33
6.3 Security Management.....	33
6.4 View Running Information	33

Chapter 7 Account Operation	34
--	-----------

Chapter 1 Activation and Login

1.1 System Requirements

Access the device via browser. The system requirements to access the device are as follows.

Table 1-1 System Requirements

Component Name	Configuration Requirements
Operating System	Microsoft Windows 7/10/11
CPU	Intel Pentium IV 3.0 GHz or above
Memory	1 GB or higher
Resolution	1280 × 768 or higher
Browser	Edge 91+, Chrome 91+

1.2 Activate

1.2.1 Activate via SADP

Before You Start

- You have downloaded the SADP from official website.
- The PC and device are in the same network.

Steps

Step 1 After installing and running the SADP, all online devices in the same LAN will be searched automatically. Information such as device type, IP address, activation status, and device serial No. will be displayed in the list.



Note

Initial device IP address: 192.168.1.64.

Step 2 Select the device to be activated. Set the device password in **Activate Device**, and click **Activate**.



Note

The password set here is the password of admin user.



Note

- Password should contain 8 to 16 characters, including at least 2 of the following types: digits, lowercase letters, uppercase letters, and special characters.
- In order to protect your privacy and corporate data, and avoid network security issues, it is recommended to set strong password in compliance with security requirements.

Step 3 (Optional) Edit device IP address.

- 1) Select the activated device and enter IP address, subnet mask, gateway, etc. in the **Modify Network Parameters** on the right.
- 2) Please enter the password set when activating. Click **Modify**. If “**Network parameters modified.**” is prompted, the settings will take effect.

1.2.2 Activate via Web

The device needs to be activated before it can be used. The default IP address of the device is 192.168.1.64.

Before You Start

The PC and device are in the same network.

Steps

Step 1 Open the browser, enter *https://192.168.1.64* in the address field, and press **Enter**.



Note

Set a strong password according to the prompt. Please save the password.

Step 2 Enter **Password**, **Password Confirm**, and click **OK**.

1.3 Log In

You can log in to the device via web page.

Before You Start

The device is activated and you have obtained its IP address.

Steps

Step 1 Enter *https://192.168.1.64* in the address bar of the web browser and press **Enter**.

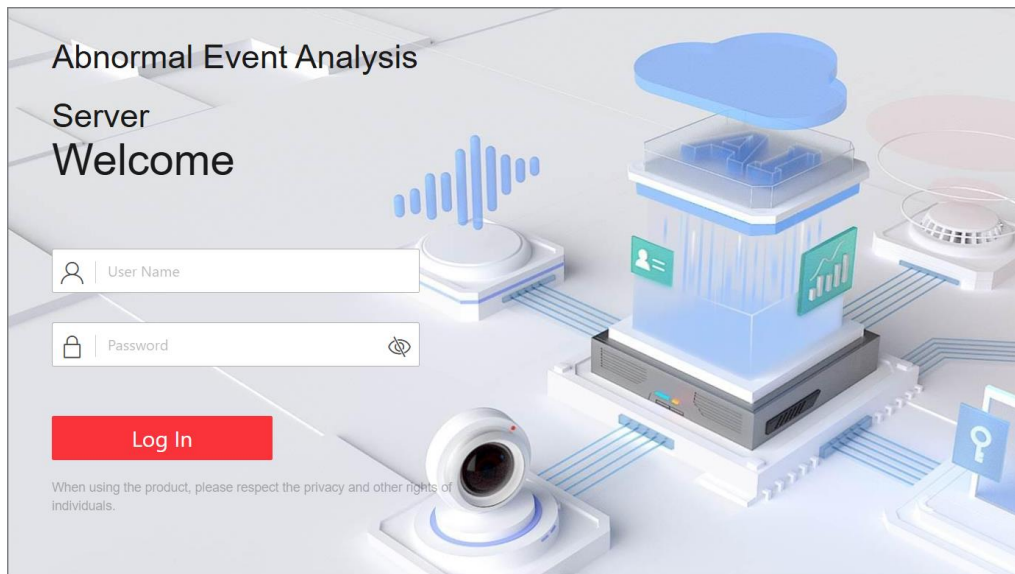


Figure 1-1 Login Page

Step 2 Enter **User Name** and **Password**, and click **Log In**.

 Note

Please refer to the actual product interface.

Chapter 2 Device Access

Before starting intelligent analysis, you should add video (real-time video stream or video file from the device) to be analyzed, as well as target library and target pictures for comparison.

2.1 Add Video Device

After adding video device, the real-time video stream of the video device can be analyzed.

Steps

Step 1 Click **Device Access** → **Device** → **Video Device**.

Step 2 Click **Add**.

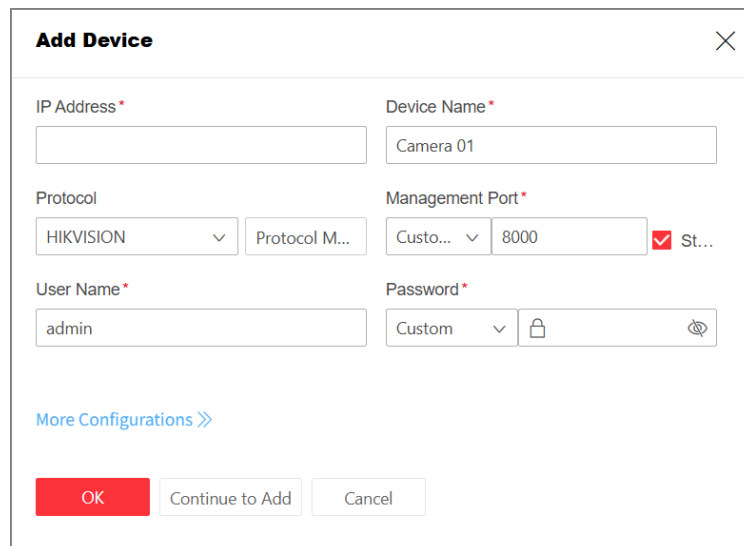


Figure 2-1 Add Video Device

Step 3 Enter the name, IP address, user name, and password of the device to be added.

Step 4 Click **OK** or **Continue to Add**.

Step 5 Perform more operations such as delete and export devices.

2.2 Group Video Devices

You can grouping the added video devices. If many video devices are added, when creating intelligent analysis task and selecting analysis channel, you can quickly find the device by group.

Steps

Step 1 Click **Device Access** → **Device Group**.

Step 2 Click  to add group.

Step 3 Select a group to add the video device.

Step 4 Click **Import**.

Step 5 Select device(s) to be added.

Step 6 (Optional) Click  in the **Operation** column to remove the device from the group.

2.3 Add Video File

You can add video file for analysis.

Steps

Step 1 Click **Device Access** → **Offline Video**.

Step 2 Click **Add Folder** or  to add a folder.

Step 3 Select a folder.

Step 4 Click **Import**.

Step 5 Select the video file(s) from local PC.



Supported formats: ps, ts, mp4, avi, mbf, asf, mkv, h.264, h.265 (HIKVISION), svac, ES. A single video file should not exceed 10 GB, and the total size of the offline video files should be no more than 20 GB.

Step 6 (Optional) Click **Add More** to add more video files.

Step 7 (Optional) Edit the uploading time.



It is recommended to upload video files when the device is idle.

Step 8 Click **Start Uploading**.



You can click  to delete the video.

Chapter 3 Intelligent Application

3.1 Application Management

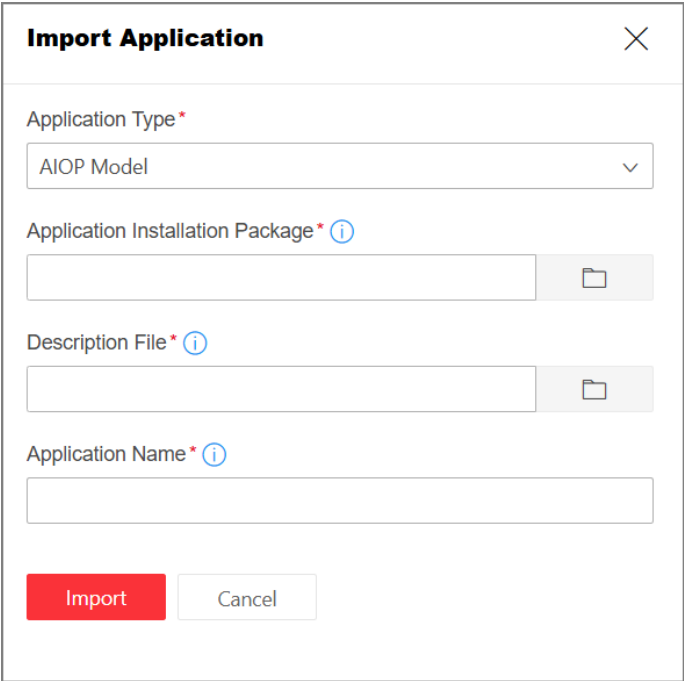
On the Application Management page, you can view the built-in applications (including general algorithms and general ultra-high-precision algorithms) and the imported applications.

3.1.1 Import Application

Steps

Step 1 Click **Intelligent Application** → **Application Management**.

Step 2 Click **Import Application**.



The screenshot shows a modal dialog titled "Import Application". It contains the following fields and controls:

- Application Type***: A dropdown menu with "AIOP Model" selected.
- Application Installation Package***: A text input field followed by a folder icon for file selection.
- Description File***: A text input field followed by a folder icon for file selection.
- Application Name***: A text input field.
- Buttons**: "Import" (red) and "Cancel" (white) buttons at the bottom.

Figure 3-1 Import Application

Step 3 Set the application type, select the application installation package and description file from local PC, and enter the application name.

Step 4 Click **Import**.

Step 5 (Optional) Cursor on the application, and perform more operations.

-  : Upgrade application.
-  : Delete application.
-  : View application details.

-  : Edit application information.

3.2 Allocate Algorithm Resource

You can allocate resources for general algorithms.

Steps

Step 1 Click **Intelligent Application** → **Resource Allocation**.

Step 2 Click  to expand the algorithm details.

Step 3 Click the drop-down list below **Pre-Allocated Cards**, and set the number of cards.

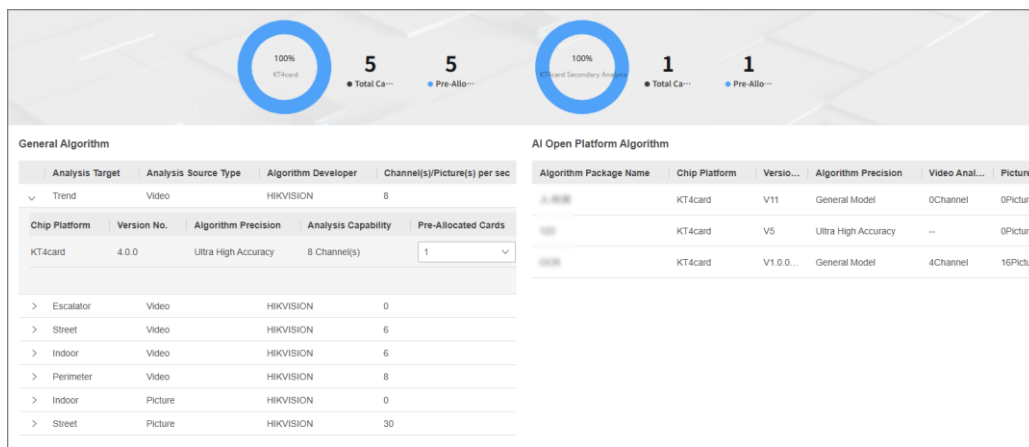


Figure 3-2 Algorithm Resource Pre-Allocation



Note

The above figure is for reference only. Please refer to the actual interface.

3.3 Task Management

3.3.1 Task Overview

The Task Overview page allows you to view the details of the created tasks such as execution status and estimated end time.

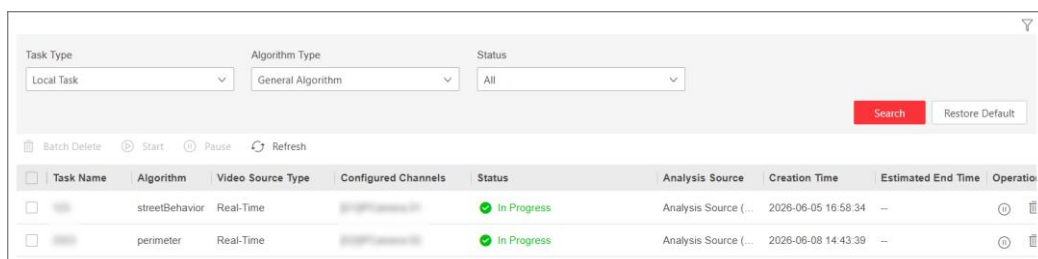


Figure 3-3 Task Overview

You can filter tasks by task type, algorithm type, or status.

Perform the following operations if needed.

-  : Start executing the task(s).
-  : Pause executing the task(s).
-  : Delete the task(s).
-  : Refresh the task execution status.

3.3.2 Configure Event

You should configure events before configuring tasks.

Steps

Step 1 Click **Intelligent Application** → **Application Management** → **Behavior Event Configuration**.

Step 2 Select scene type.

Step 3 Enable the event to be used.

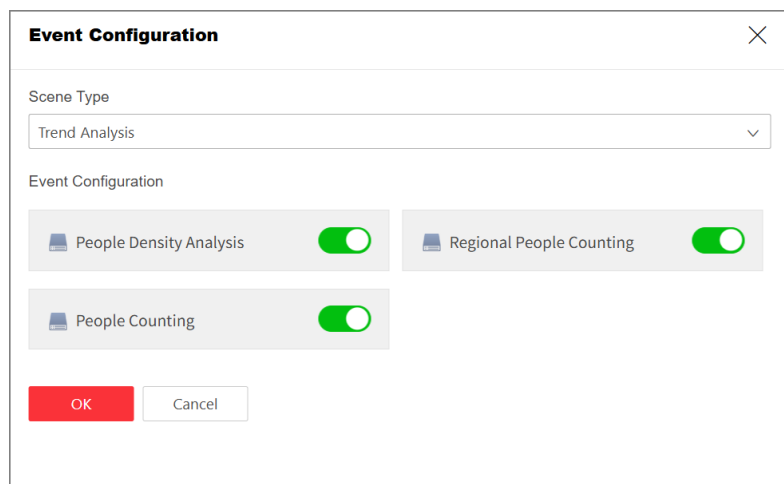


Figure 3-4 Enable Event

Step 4 Click **OK**.

3.3.3 Add Task

You can add tasks to analyze corresponding events in the video.

Steps

Step 1 Click **Intelligent Application** → **Application Management**.

Step 2 Select an application.

Step 3 Click **Video Analysis**.

Step 4 Click **Add** or **Add Task**.

Step 5 Enter task information and click **Next**.

Figure 3-5 Task Information

Step 6 Configure the rule.

- 1) Enter rule name.
- 2) Select event type.
- 3) Configure the time schedule.
- 4) Draw rule area and (optional) size filter area. Please refer to “3.4 Description of Drawing Event Rule Areas” for drawing instructions of different rule areas.
- 5) (Optional) Enable size filter and select drawn size filter area.
- 6) Configure event parameters.
- 7) (Optional) Add the next event rule.

Figure 3-6 Rule Setting Flow

- 8) Click **Advanced Configuration** to configure advanced parameters.
- 9) Click **Scheduled Task** to draw analysis schedule.
- 10) Configure the parameters of the next channel to be analyzed. Refer to “3.5 Description of Configuring Event Rule” for details about the parameter configurations of different events.

Step 7 Click **Save** to save the above settings and finish creating the task.

Step 8 (Optional) Perform more operations in the task list.

- Click  to edit the task.
- Click **Delete** to delete a single task or click **Batch Delete** to delete all tasks.

3.4 Description of Drawing Event Rule Areas

Table 3-1 Description of Drawing Event Rule Areas

Rule Area Name	Icon	Description
Detection Area		Click the button to start drawing. Click to set a vertex on the video image and right-click to finish drawing. After drawing, click the drawn area, click and hold to drag the drawn polygon.
		Click the button to draw a full-screen detection area. After drawing, click the drawn area, click and hold the area vertex to adjust the shape.
Detection Line		Click the button to draw a detection line automatically on the video, click the detection line, click and hold to drag the endpoint position.
Polyline		Click the button to start drawing. Click to set a turning point on the video and right click to finish drawing. Click the drawn line, click and hold to drag the line.
Size Filter Area		Click the button to start drawing. Hold the left mouse button on the video and drag to draw the maximum size frame. Click to drag the vertex of the area and adjust the drawn rectangle. Targets larger than the maximum size will be filtered and excluded from the analysis results.
		Click the button to start drawing. Click and hold to drag the minimum size frame. Click to drag the vertex of the area and adjust the drawn rectangle. Targets smaller than the minimum size will be filtered and excluded from the analysis results.

Rule Area Name	Icon	Description
Bed Area		Click the button to start drawing. Click to set a vertex on the video and right click to finish drawing. After drawing, click and hold the area vertex to drag the drawn polygon.
Escalator Area		Click the button to start drawing. Click to set a vertex on the video and right click to finish drawing. After drawing, click and hold the area vertex to drag the drawn polygon.
Shielded Area		Click the button to start drawing. Click to set a vertex on the video and right click to finish drawing. After drawing, click and hold the area vertex to drag the drawn polygon. The shielded area will be excluded from smart analysis.

Note

- You can click  to clear all the rule areas.
- Rule areas are different with different event types. Please refer to the actual interface.
- The above table is for reference by general algorithms only.

3.5 Description of Configuring Event Rule Parameters

3.5.1 General Parameters

Table 3-2 Parameter Description

Parameter	Description
Time Schedule	The time of video intelligent analysis of the channel according to current rule. If the scheduled task time is different from the schedule, the current rule will analyze the intersection time of the two time configurations.
Size Filter	After drawing the max./min. size frame and enabling size filtering, targets larger than the max. size and smaller than the min. size will be filtered, and the analysis results will be excluded from the filtered targets.
Sensitivity	The larger the value, the more sensitive the event to be detected will be, and false alarm may occur. It is recommended to keep the default value. If the result is poor, debug it in the actual scene.
Target Type	Only the analysis result of the selected target type will be output. The selected target type will be filtered, and the analysis results will be excluded from the filtered targets.

Parameter	Description
Duration (s)	Alarm will be triggered when the detected event in the video persists until the configured time.
Alarm Interval (s)	Time interval for generating 2 alarm messages. If there are too many alarms for the same event, the value can be increased. If the generated alarm messages are insufficient, the value can be decreased.
Alarm Reporting Mode	Select Interval if there are too many alarms. Select Single if the generated alarm messages are insufficient.
Analysis Reporting Interval	The time interval for uploading analysis information.

 Note

- The parameters are different with different event types. Please refer to the actual interface.
- The above table is for reference by general algorithms only.

3.5.2 Specific Parameters

Table 3-3 Parameter Configuration

Parameter	Event	Description
Getting Up Mode	Indoor—Getting Up Detection	Select the getting up mode according to the scene. When you select the Wide Bed Mode , you need to draw a rule area of wide bed for detection.
Out of Bed Duration	Indoor—Getting Up Detection	Alarm will be triggered when the detected event in the video persists until the configured time.
Human Body Center Detection Configuration	Indoor—Climbing Detection	It is recommended to keep the default.
Configuration Mode	Indoor—Absence Detection	Select configuration mode according to the actual scene.
Alarm Time When Nobody Detected (sec)	Indoor—Absence Detection	Alarm will be triggered when the detected event in the video persists until the configured time.
Person On Duty	Indoor—Absence Detection	Select according to actual on-duty schedule.
Detection Mode	Indoor—Detection for Sudden Change of Sound Intensity	● Sensitivity Detection: Detects sound from multiple aspects. Alarm will be triggered if there is abnormal sound in the monitoring area, such as screaming, quarreling, etc. You can adjust sensitivity value according to actual situations. ● Decibel Threshold Detection: Detects the audio volume in the video. Alarm will be triggered if the volume is larger than the decibel threshold.
Decibel Threshold (dB)	Indoor—Detection for Sudden Change of Sound Intensity	When the detection mode is selected as the Detection Threshold , alarm will be triggered when the volume in the video is larger than the detection threshold.

Table 3-3 Parameter Configuration

Triggering Time (s)	Indoor—Number of People Exception	Alarm will be triggered when the detected event in the video persists until the configured time.
Number of People Threshold and Detection Type	Indoor—Number of People Exception	• More Than: Alarm will be triggered when the people count exceeds the threshold. • Less Than: Alarm will be triggered if the count remains below the threshold for the specified duration. • Equal To: Alarm will be triggered if the count matches the threshold for the specified duration. • Not Equal To: Alarm will be triggered if the count differs from the threshold for the specified duration.
Alarm Reporting Interval	Trend—Crowd Trend Analysis	The time interval for uploading alarm information of trend analysis.
Low/Medium/High Alarm Threshold	Trend—Crowd Trend Analysis	Low/medium/high-level alarm will be triggered when the number of people detected in the video reaches the configured value.
Low/Medium/High-Level Alarm Name	Trend—Crowd Trend Analysis	Custom name.

 Note

- The parameters vary with different event types. Please refer to the above table according to actual needs.
- This description is for behavior task reference only. Algorithm task parameters of the AI open platform are subject to specific algorithm.

3.6 Examples of Configuring Event Rules



All the examples and parameters in this chapter are for reference only. Please adjust parameters according to your actual situation.

3.6.1 Trend Analysis Event



All the examples and parameters in this chapter are for reference only. Please adjust parameters according to your actual situation, or contact technical support if necessary.

Table 3-4 Event Rule Configuration

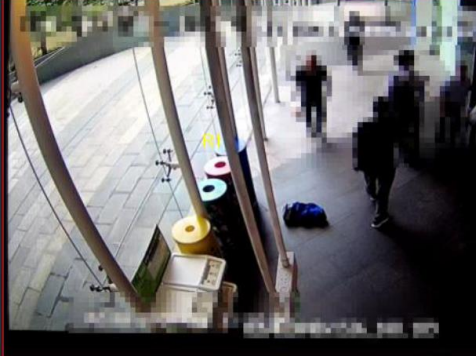
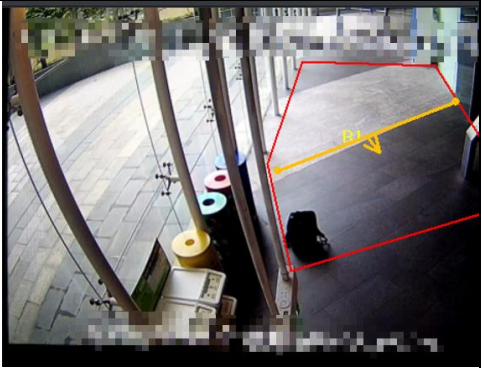
Event Type	Parameter Description	Rule Area Example
People Density Analysis	● Crowd Density Detection Mode -Default Mode: Applicable to large sized areas such as squares. -Detection Mode: Applicable to moderately large sized areas such as supermarkets. -Density Mode: Applicable to compact spaces such as conference rooms. ● Analysis Reporting Interval (s): The time interval for uploading people density data. ● Alarm Reporting Interval (s): The time interval for uploading the people density alarm. ● Low Alarm Threshold: The minimum number of people generating a low-level alarm for people density. ● Medium Alarm Threshold: The minimum number of people generating a medium-level alarm for people density. ● High Alarm Threshold: The minimum number of people generating high-level alarm for people density.	
Regional People Counting	Analysis Reporting Interval (s): The time interval between two consecutive reports of the number of people in a region.	

Table 3-4 Event Rule Configuration

People Counting	● Analysis Reporting Interval (s): The time interval between two consecutive reports of people counting. ● Statistics Mode Accumulate: The people counting results will be accumulated and not cleared. Reset Every Day: Reset the people counting from the previous day at midnight. Reset by Interval Time: Supports configuring the resetting interval.	
-----------------	--	--

3.6.2 Street Behavior Event



Note

All the examples and parameters in this chapter are for reference only. Please adjust parameters according to your actual situation, or contact technical support if necessary.

Table 3-6 Event Rule Configuration

Event Type	Parameter Description	Rule Area Example
Sudden Falling Down	Sensitivity: The higher the sensitivity, the easier it is to trigger an alarm.	
Fast Moving Detection	Sensitivity: The higher the sensitivity, the easier it is to trigger an alarm.	
Physical Conflict (Street)	Sensitivity: The higher the sensitivity, the easier it is to trigger an alarm.	
People Gathering Detection	● Sensitivity: The higher the sensitivity, the easier it is to trigger an alarm. ● Min. People: The minimum number of gathering people to trigger an alarm.	

3.6.3 Indoor Event

Note

The examples and parameters in this chapter are for reference only. Please adjust the parameters according to your actual situation, or contact technical support if necessary.

Table 3-7 Event Rule Configuration

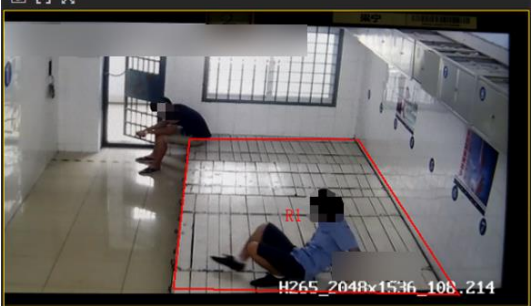
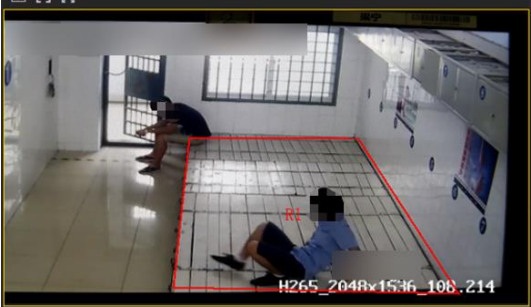
Event Type	Parameter Example	Rule Area Example
Physical Conflict (Indoor)	● Sensitivity: 75 ● Duration (s): 3 ● Alarm Interval (s): 30	
Getting Up Detection (Bunk Bed Mode)	● Sensitivity: 60 ● Duration (s): 3 ● Alarm Interval (s): 30 ● Out of Bed Duration (s): 0	
Getting Up Detection (Wide Bed Mode)	● Sensitivity: 60 ● Duration (s): 3 ● Alarm Interval (s): 30 ● Out of Bed Duration (s): 0	
Getting Up Detection (Sitting and Getting Up Mode)	● Sensitivity: 60 ● Duration (s): 3 ● Alarm Interval (s): 30 ● Out of Bed Duration (s): 0	

Table 3-7 Event Rule Configuration

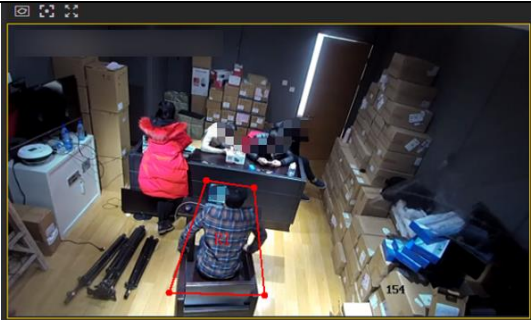
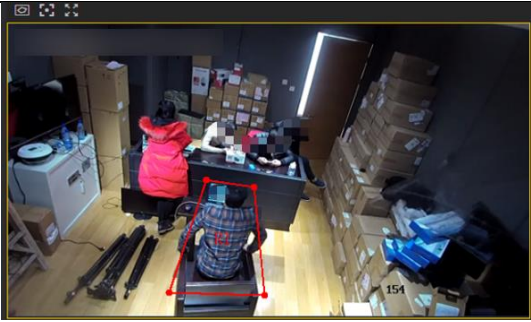
Absence Detection (On And Leave Position)	● Configuration Mode: On And Leave Position ● Alarm Time When Nobody Detected (s): 120 ● Person On Duty: Two Persons ● Sensitivity: 20 ● Alarm Upload Mode: Once ● Alarm Interval (s) 325	
Absence Detection (Absence)	● Configuration Mode: Absence ● Alarm Time When Nobody Detected (s): 120 ● Person On Duty: Two Persons ● Sensitivity: 4 ● Alarm Upload Mode: Once ● Alarm Interval (s) 325	
Absence Detection (Sleep On Duty)	● Configuration Mode: Sleep On Duty ● Alarm Time When Nobody Detected (s): 120 ● Person On Duty: Two Persons ● Sensitivity: 4 ● Alarm Upload Mode: Once ● Alarm Interval (s): 325	

Table 3-7 Event Rule Configuration

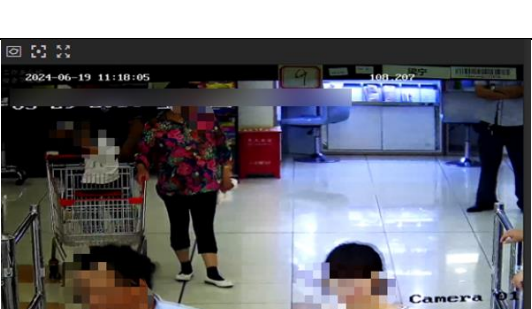
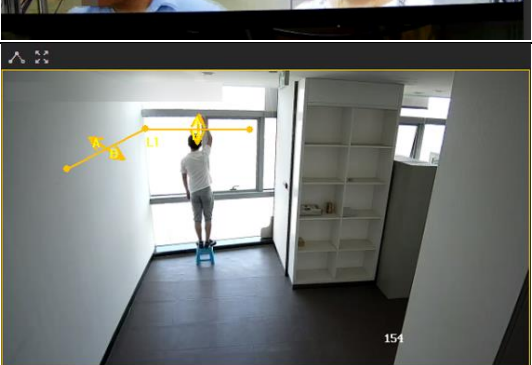
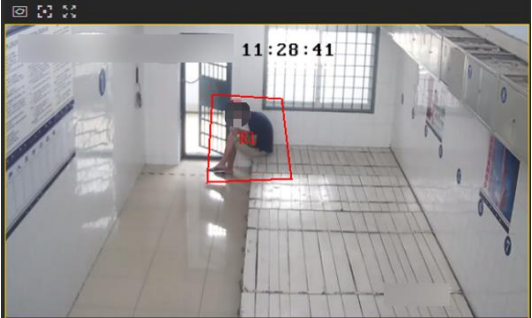
Standing Detection	Up	● Sensitivity: 60	
Sudden Change of Sound Intensity Detection (Decibel Threshold Detection)		● Detection Mode: Decibel Threshold Detection ● Decibel Threshold (dB): 70 ● Sensitivity: 40	
Sudden Change of Sound Intensity Detection (Sensitivity Detection)		● Detection Mode: Sensitivity Detection ● Decibel Threshold (dB): 70 ● Sensitivity: 40	
Climbing Detection		● Sensitivity: 70 ● Duration (s): 1 ● Alarm Interval (s): 10	
Staying Overtime		● Duration (s): 60 ● Alarm Upload Mode: Interval ● Alarm Interval (s): 300	

Table 3-7 Event Rule Configuration

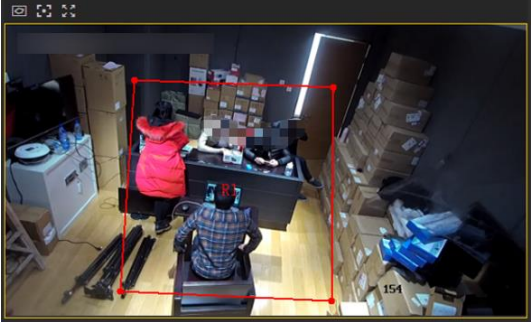
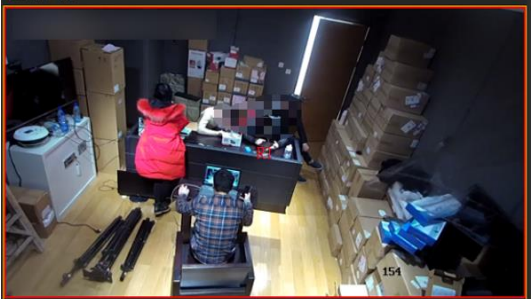
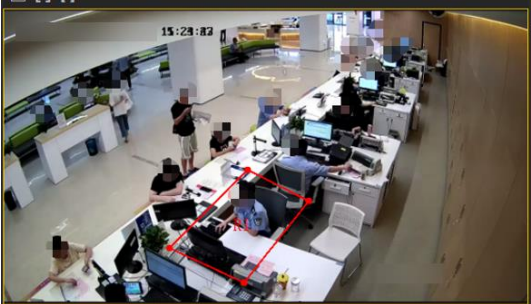
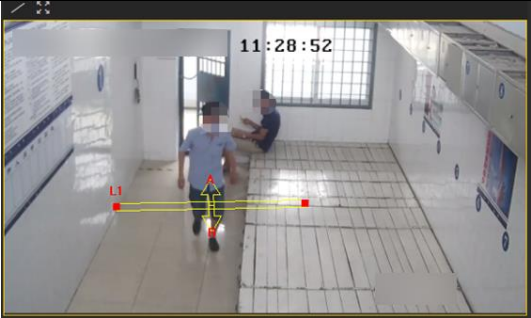
Abnormal Number of People	● Triggering Time (s): 60 ● Number of People Threshold: 5 ● Detection Type: Less Than ● Alarm Upload Mode: Interval ● Alarm Interval (s): 180	
Sitting Detection	● Duration (s): 3000	
Person Counting (Indoor)	● Alarm Interval (s): 120	
Using Mobile Phone	● Duration (s): 5 ● Alarm Interval (s): 30 ● Sensitivity: 70	

Table 3-7 Event Rule Configuration

Falling Down	●Duration (s): 2 ●Sensitivity: 60 ●Alarm Interval (s): 30	
Line Crossing Detection (Indoor)	●Crossing Direction: Bidirectional ●Sensitivity: 50	

3.6.4 Perimeter Protection Event

Note

All the examples and parameters in this chapter are for reference only. Please adjust parameters according to your actual situation, or contact technical support if necessary.

Table 3-8 Event Rule Configuration

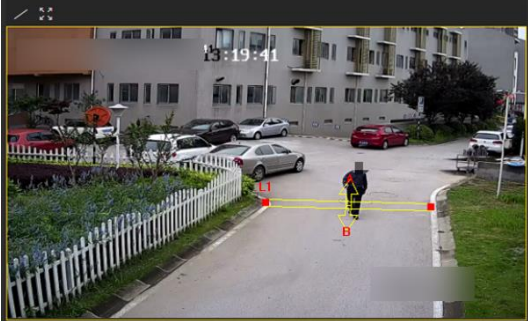
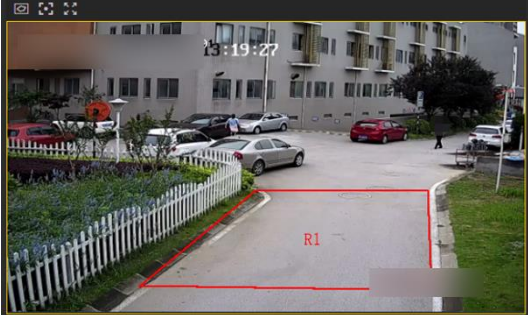
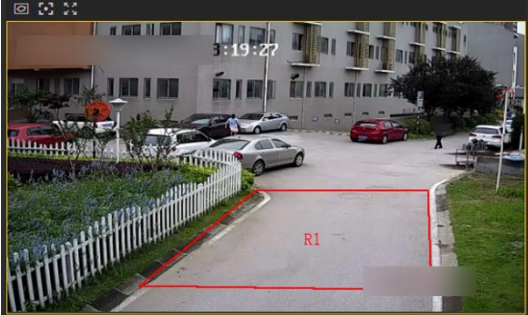
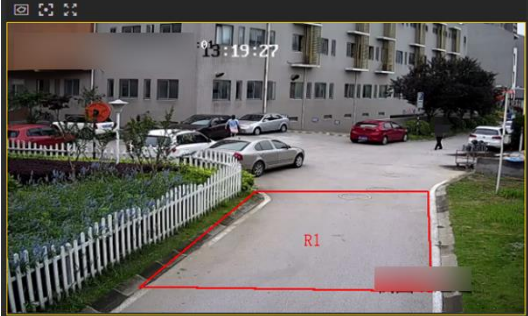
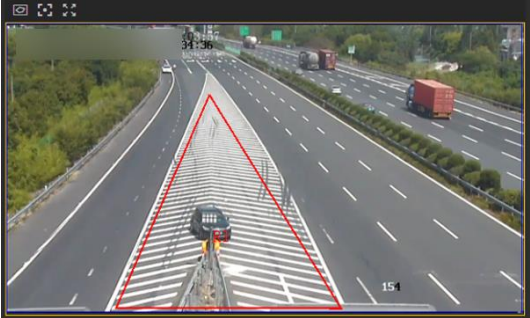
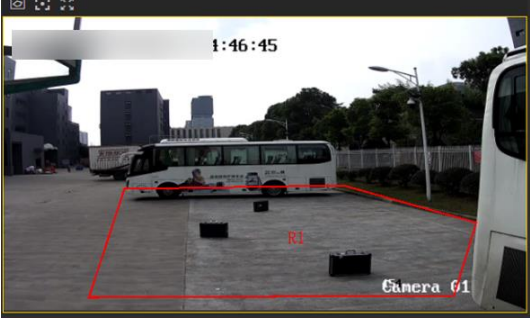
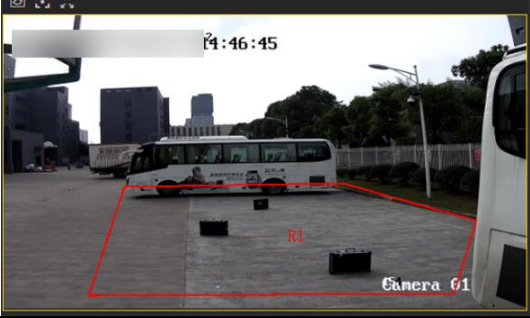
Event Type	Parameter Example	Rule Area Example
Crossing Line Detection	● Crossing Line Direction: Bidirectional ● Sensitivity: 50 ● Target Type: All	 A surveillance camera view of a residential area with a paved path and a white picket fence. A yellow line is drawn across the path, and a person is walking across it. The timestamp is 13:19:41.
Region Entrance Detection	● Target Type: All	 A surveillance camera view of the same residential area. A red rectangular region labeled 'R1' is marked on the path. The timestamp is 13:19:27.
Region Exiting Detection	● Target Type: All	 A surveillance camera view of the same residential area. A red rectangular region labeled 'R1' is marked on the path. The timestamp is 13:19:27.
Intrusion Detection	● Duration (s): 10 ● Target Type: All ● Sensitivity: 50	 A surveillance camera view of the same residential area. A red rectangular region labeled 'R1' is marked on the path. The timestamp is 13:19:27.
Loitering Detection	● Duration (s): 10	 A surveillance camera view of a paved path with a person standing in the middle. A red rectangular region labeled 'R1' is marked around the person. The timestamp is 13:19:57.

Table 3-8 Event Rule Configuration

Parking Detection		● Sensitivity: 50 ● Duration (s): 100	
Object Detection	Removal	● Sensitivity: 50 ● Duration (s): 2	
Unattended Detection	Baggage	● Sensitivity: 50 ● Duration (s): 2	

3.7 Description of Configuring Advanced Parameters

Figure 3-9 Configure Advanced Parameters

Advanced Parameters	Parameter Description
Target Generation Speed	The larger the value, the faster the generation speed. It is recommended to keep the default setting.
Human Body Center Detection Configuration	It is recommended to keep the default setting.
Overlay Target Box.	When enabled, the detected target box is displayed in the alarm picture.
Overlay Rule Information	When enabled, the configured event rule information is displayed in the alarm picture.
Custom Parameter	Custom parameters are supported for indoor events.

 Note

- Advanced parameters are different with different event types. Please refer to the actual interface.
- The above table is for reference by general algorithms only.

Chapter 4 Intelligent Search

After creating intelligent analysis task, you can search for analysis results.

Before You Start

Intelligent analysis task created.

Steps

Step 1 Click **Intelligent Search**.

Step 2 Select search type, scene, event type, time, etc.

Step 3 Click **Search** to search for events that meet the requirements.

Step 4 (Optional) Click a result in the search result list to view the enlarged picture on the right side of the page.

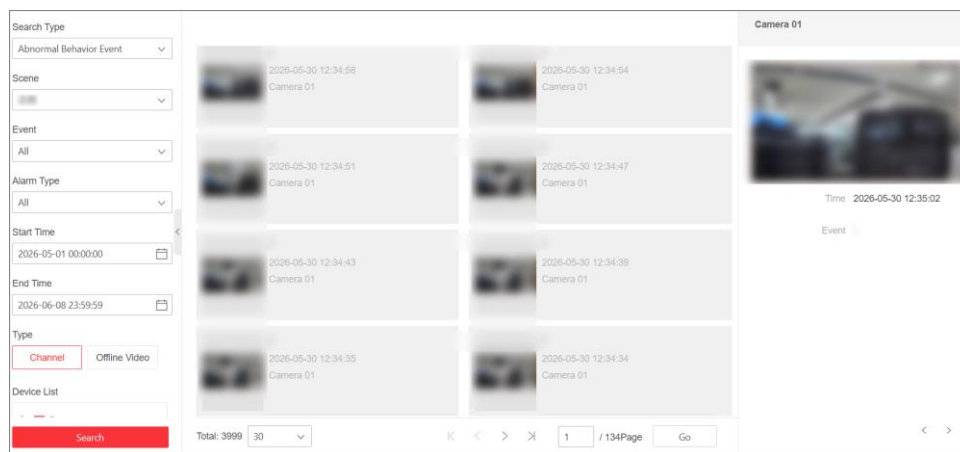


Figure 4-1 Intelligent Search Page



Note

This example is for reference only. Please refer to the actual interface.

Chapter 5 System Configuration

5.1 System Settings

5.1.1 Basic Information

Click **System Configuration** → **System Configuration** → **Basic Information** to view basic device information.

5.1.2 Time Configuration

If the device time is incorrect, please synchronize the time. Two methods are supported: NTP time synchronization and manual time synchronization. Get NTP server IP address and port information first when selecting NTP time synchronization.

Go to **System Configuration** → **System Configuration** → **Time Configuration**.

5.2 User Management

The system predefines an administrator user named “admin”. Only administrator user can add user, delete user, and change user password.

Operators and normal users can only change their own passwords. No more than 32 users (admin included) are allowed in the system.

5.2.1 Add/Edit User

Add and edit non-administrator users.

Go to **System Configuration** → **User Management** → **User Management**.

Add User: Click **Add**.

Edit User: Click .

5.2.2 View Online User

Go to **System Configuration** → **User Management** → **Online User**.

5.3 Network Configuration

5.3.1 Basic Settings

Before connecting the device to the network, you need to configure the device's network parameters.

Steps

Step 1 Click **System Configuration** → **Network Configuration** → **Network Parameter** → **TCP/IP**.

Step 2 Set network parameters.

Auto: If the device is connected to a router or switch with DHCP server enabled, the DHCP server will automatically assign IP address after enabling Auto-Get. If there is no DHCP, please keep disabled. Enter IPv4 address, IPv4 subnet mask, and IPv4 default gateway parameter information manually.

MTU: The maximum transmission unit refers to the size of the max. data packet in TCP/UDP protocol network transmission.

The screenshot shows the TCP/IP configuration page. It includes a title bar 'TCP/IP' in red. Below it, there are several configuration options: 'Working Mode' is a dropdown menu set to 'Net Fault-Tolerance'; 'NIC Type' is a dropdown menu set to 'Auto'; 'DHCP' is a toggle switch that is currently turned off; there are three input fields for IPv4 configuration: '* Device IPv4 Address', '* IPv4 Subnet Mask', and 'IPv4 Default Gateway'; 'IPv6 Mode' has three radio button options: 'Manual', 'DHCP', and 'Route Advertisement' (which is selected), with a 'View' link next to it; there are three input fields for IPv6 configuration: 'Device IPv6 Address', 'Subnet Prefix Length', and 'IPv6 Default Gateway'; and 'MAC Address' is displayed as 'dc:07:f8:81:70:cf'. At the bottom right, there is a red 'Save' button.

Figure 5-1 TCP/IP Configuration

Step 3 Click **Save**.

5.3.2 Platform Access

You can upload device logs to a log server.

Steps

Step 1 Go to **System Configuration** > **Network Configuration** > **Platform Access**.

Step 2 Enable the function and configure the required parameters.

The screenshot shows a configuration window with the following elements:

- An **Enable** toggle switch, currently turned on (green).
- Three required input fields:
 - *Log Server Address**: An empty text box.
 - *Log Server Port**: A text box containing the value `5555`.
 - *Upload Time Interval**: A text box containing the value `1`, with a unit selector set to `h` (hours).
- A **Test** button located below the input fields.
- A section titled **Client Certificate** containing:
 - A **Create Certificate Request** button with a **Create** sub-button.
 - An **Install Generated Certificate** section with a file selection button (folder icon) and an **Install** button.
- A section titled **CA Certificate** containing:
 - An **Install Generated Certificate** section with a file selection button (folder icon) and an **Install** button.
- A large red **Save** button at the bottom center.

Figure 5-2 Configure Parameters

5.3.3 Network Service

Configure network service. HTTP(S) port is used for browser access.

Configure Entrance: **System Configuration** → **Network Configuration** → **Network Service**.

- **Authentication mode**: When the digest mode is selected, only the IP address with the digest authentication request can access data stream through protocol. For security reasons, it is generally recommended to select the digest authentication mode.
- **Digest algorithm**: The digest algorithm is used for encryption transmission between device and platform. The default is MD5. If the platform supports SHA256, you can also select it.

5.3.4 Alarm Configuration

Add the URL of the alarm analysis device. You can upload the task analysis results of the selected event type to the alarm analysis device (only the task created by the analysis device web page is supported).

The system allows you to set a maximum number of alarms to be cached. If a burst of alarms exceeds the system's real-time processing capacity for ultra-high accuracy analysis, subsequent alarms will be temporarily cached. These cached alarms will be re-analyzed (using the high-accuracy model) when the system load decreases and the number of pending items falls below the cache limit.

Go to **System Configuration** → **Network Configuration** → **Alarm Receiving Address** to add alarm receiving addresses.

Go to **System Configuration** → **Event** → **Alarm Setting** → **Cache Alarm** to configure the number of cached alarms.

Chapter 6 Maintenance and Security

6.1 System Maintenance

6.1.1 Restart

Go to **Maintenance and Security** → **System Maintenance** → **Restart** to restart the device.

6.1.2 Upgrade

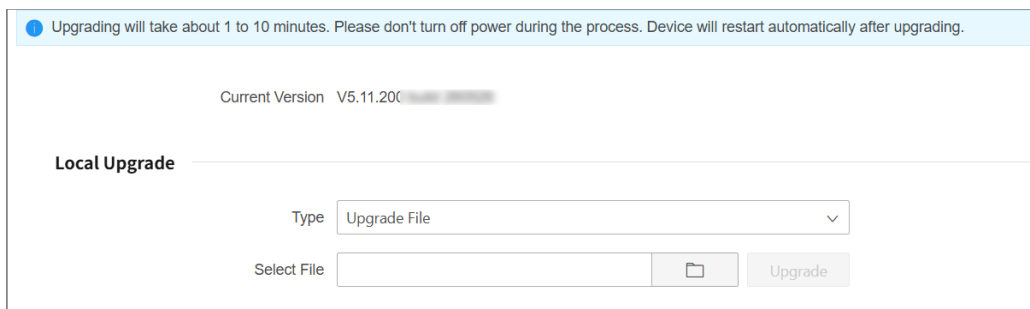
Upgrade device through web page.

Before You Start

Make sure the device is online and you have prepared the upgrade file.

Steps

Step 1 Click **Maintenance and Security** → **System Maintenance** → **Upgrade**.



The screenshot shows a web interface for upgrading the device. At the top, a blue banner contains the text: "Upgrading will take about 1 to 10 minutes. Please don't turn off power during the process. Device will restart automatically after upgrading." Below this, the "Current Version" is displayed as "V5.11.200" next to a progress bar. The "Local Upgrade" section is active, showing a "Type" dropdown menu set to "Upgrade File". Below this is a "Select File" input field with a folder icon button and an "Upgrade" button.

Figure 6-1 Upgrade

Step 2 Click  to select the upgrade file.

Step 3 Click **Upgrade** to start upgrading. Once completed, the device will restart automatically.

6.1.3 Backup and Restore

Go to **Maintenance and Security** → **System Maintenance** → **Back Up and Restore**.

Restore to Default Settings

All device parameters except the device IP address will be restored to default settings. The data files (video data, picture data, structured data and algorithm package, including built-in and user uploaded) will be kept.

Restore to Factory Settings

All functions and parameters will be restored to factory settings. All data will be cleared. You need to activate the system again, set and save the IP address, etc.

Format Disk for Picture Storage

Formatting will permanently erase all picture data. This operation is primarily intended as a last resort to resolve critical errors, such as splitting errors during smart search. Before formatting, please attempt other troubleshooting methods and ensure all important data is backed up.

6.1.4 Log

View and export system logs.

Go to **Maintenance and Security** → **System Maintenance** → **Log**.

View Log: Select major type, subtype, and time, and click **Search**.

Export Log: Click **Export**, set the file type, and click **OK** to export all logs.

The screenshot shows the Log interface with the following components:

- Search Filters:** Major Type (All Types), Subtype (All Types), and Select Time (2026-06-12 00:00:00 - 2026-06-12 23:59:59). A red Search button is on the right.
- Export:** An Export button is located below the search filters.
- Table:** A table with 7 columns: No., Time, Major Type, Minor type, Channel No., Local/Remote User, and Remote Host IP Address. It contains 3 rows of log entries.

No.	Time	Major Type	Minor type	Channel No.	Local/Remote User	Remote Host IP Address
1	2026-06-12 00:06:05	Information	System Running Status Information	--	--	--
2	2026-06-12 00:06:05	Information	System Running Status Information	--	--	--
3	2026-06-12 00:06:05	Information	System Running Status Information	--	--	--

Figure 6-2 Log

6.1.5 Device Debugging

After enabling SSH, you can use SSH protocol for remote control. If there is no debugging need, it is recommended to disable SSH to improve security.

Go to **Maintenance and Security** → **System Maintenance** → **Device Debugging**.

6.2 View Hardware Information

You can view device information such as CPU, memory, and other hardware information.

Go to **Maintenance and Security** → **Hardware Information**.

6.3 Security Management

You can enable picture URL digest authentication to improve security.

Go to **Maintenance and Security** → **Security** → **Security Service**.

6.4 View Running Information

You can view running information, target data synchronization status, etc.

Go to **Maintenance and Security** → **Running Information**.

Chapter 7 Account Operation

Click the user name to change user password or log out.

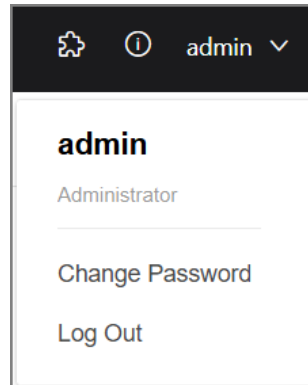
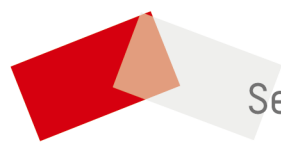


Figure 7-1 Account Operation



See Far, Go Further