User Manual for AI Edge Computing Supervisory Device

Copyright Notice

Trademark Notice

Product names mentioned in this manual are used solely for identification purposes. These names may be registered trademarks or copyrights of their respective owners. All other trademarks mentioned are the property of their respective trademark holders. Such trademarks are used for reference only, and the product provider claims no ownership; no exhaustive list of trademark owners is provided.

Product Notice

Functions or performance described in this manual may vary depending on the specific product model, operating environment, or configuration methods. Such variations are considered normal. For any related questions, please consult the technical support personnel of the product provider.

Disclaimer

The product provider and its employees shall not be held liable for any direct or indirect data loss, financial loss, or other damages arising from the use of this manual or any information contained herein.

Usage Instructions

This user manual applies to the AI edge computing supervisory device and its system platform. Please read this manual carefully before using the product. After use, please keep the manual in a safe place for future reference.

User Manual for AI Edge Computing Supervisory Device

Table of Contents

1 Product Overview of Edge Computing Supervisory Device

This product is a low-power, high-performance general-purpose edge AI server, integrating 1 – 16 video channel access, AI snapshot capture, and alarm detection functions. It supports up to 16 channels of 1080P video analytics, suitable for various intelligent vision applications.

Product versions are available in:

Standard Edition (supports up to 8 channels)

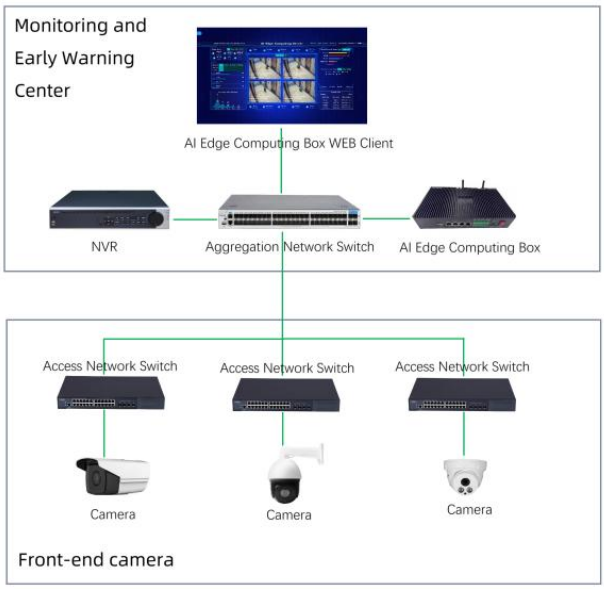
Professional Edition (supports up to 16 channels)

1.1 Product Appearance

Standard Edition Edge Supervisory Device (4 – 8 channels)

Professional Edition Edge Supervisory Device (8 – 16 channels)

2 Hardware Connection and Usage Instructions



Standard Edition Edge Supervisory Device Connection Diagram

Professional Edition Edge Supervisory Device Connection Diagram

3 Advantages of the Embedded System Management Platform

The edge supervisory device features a high-performance embedded system management platform, integrating algorithm execution, video analytics, and local management functions. It supports real-time processing of 1 to 16 video streams. With a lightweight architecture, the platform has low resource consumption and ensures stable operation, enabling independent intelligent detection and alarm response for personnel, vehicles, behaviors, and environmental anomalies directly on the device.

It supports remote configuration and status monitoring, offering excellent compatibility and maintainability. Without relying on a central platform, it enables efficient, low-latency localized intelligent control, making it ideal for distributed deployments and edge-side rapid response scenarios.

4 Management Platform Configuration Guide

This section provides a brief overview of the system platform configuration process:

Server IP address setting, platform login, device network configuration, checking device ID and firmware version, online firmware upgrade, changing website title and logo, camera video stream integration, channel algorithm deployment, and when to restart the AI algorithm.

4.1 Server IP Address Setting

Note: In the current version, for ease of IP configuration, the network interface is managed internally via a dedicated tool. IP settings are configured using this tool. Follow the steps below:

1. Use a Windows PC and run the configuration tool: BMLiteTool.exe

2. Search for and select the device starting with "d8" (Note: If the device is not found, please disable the Windows firewall)

3. The default IP address for the device's WLAN port is 192.168.1.32. This is typically the IP shown in the scan. If there is an IP conflict within the local network, the IP address must be changed accordingly.

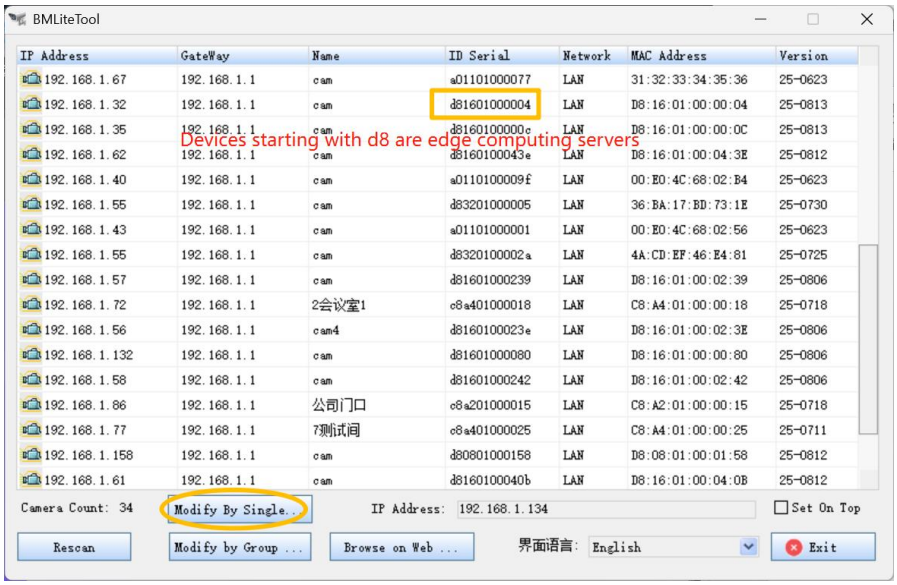


Figure 4.1 Scanning IP Addresses Using the BMLiteTool.exe Tool

4. Modify the IP address, gateway, and subnet mask, then click Save.

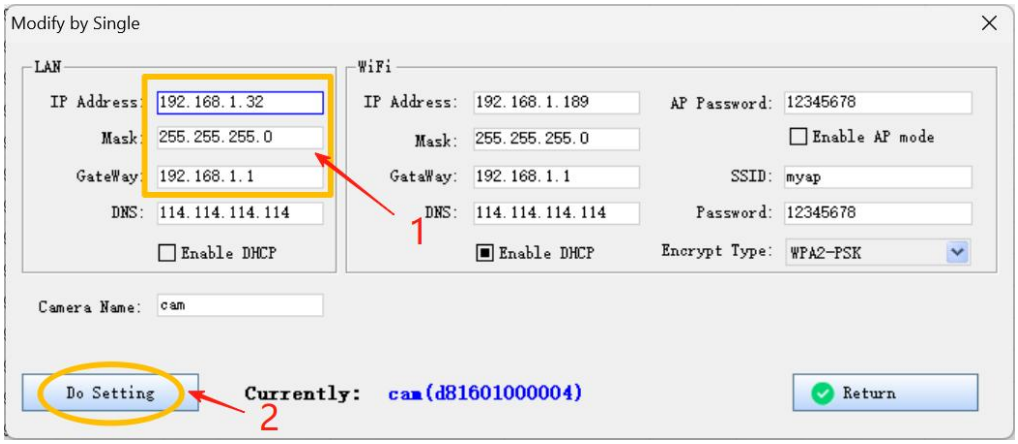


Figure 4.2 Setting Network Parameters

Note: This tutorial is based on the 192.168.1.x subnet. In your actual network environment, you must adjust the settings according to your custom subnet.

After configuring the network parameters, you can proceed with the following tasks using the assigned IP address.

4.2 Platform Interface Login

If the device IP is 192.168.1.32, set your computer's IP address to the same local network segment.

Open Google Chrome or Microsoft Edge browser and enter the URL:

http://192.168.1.32/#/login

Log in using the default credentials:

Username: admin Password: 123456。

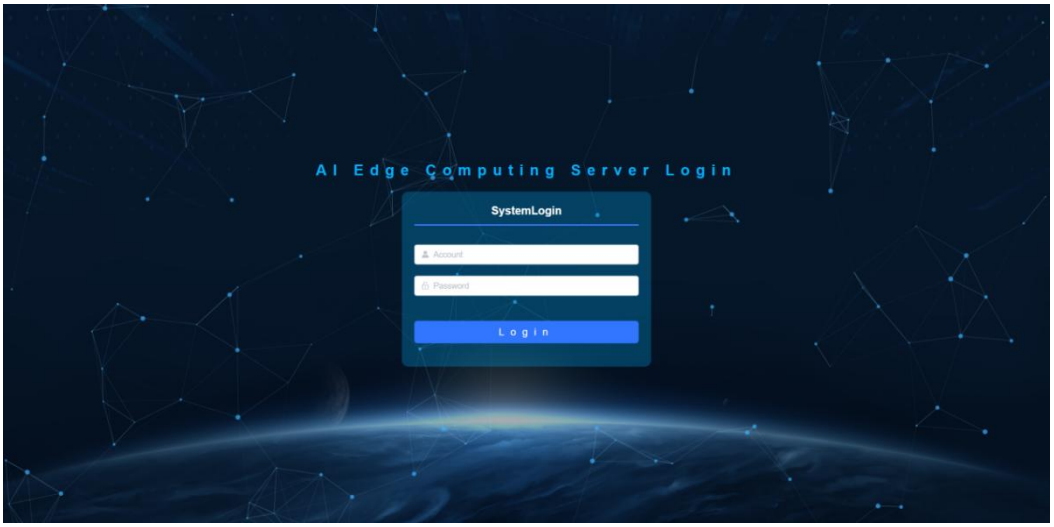


Figure 4.3 Login Interface

After logging in, the intelligent analytics dashboard will be displayed. Click the floating icon in the upper-left corner to show the sidebar main menu. Click it again to hide the menu.

Figure 4.4 Sidebar Main Menu

4.3 Device Network Configuration

Setup steps: Left sidebar → System Management → Network Settings to configure IP addresses.

As shown in the figure:

WAN: Configure the IP of the WLAN port, default is 192.168.1.32

LAN1: Configure the IP of the LAN1 port, default is 192.168.2.101

Note: If you are connected to the LAN1 port, the BMLiteTool.exe tool will still detect the default WLAN IP (192.168.1.32). However, to access the platform, you must use the actual LAN1 IP: 192.168.2.101.

Please ensure that the IP address of the connected device port and your computer are within the same local network segment.

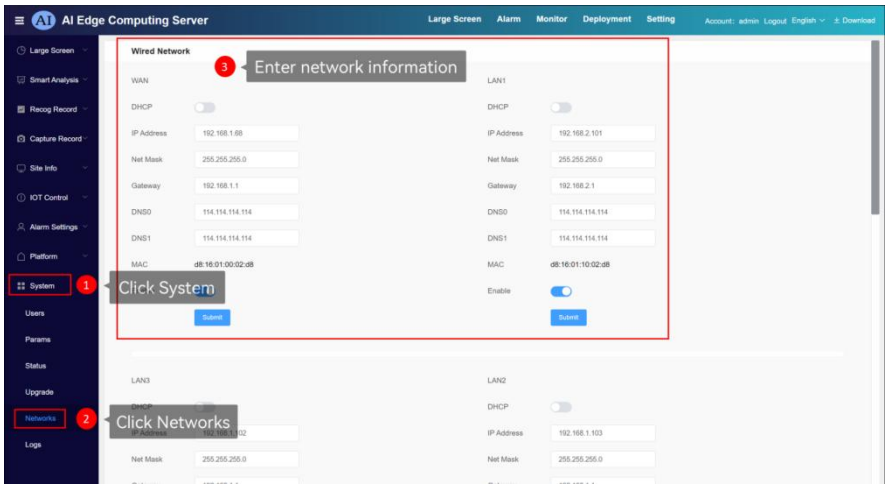


Figure 4.5 Device Network Configuration

4.4 Viewing Device ID and Firmware Version Upgrade

Setup steps: Left sidebar → System → Status → View hardware information / Firmware upgrade.

Here, you can check the device ID and firmware version.

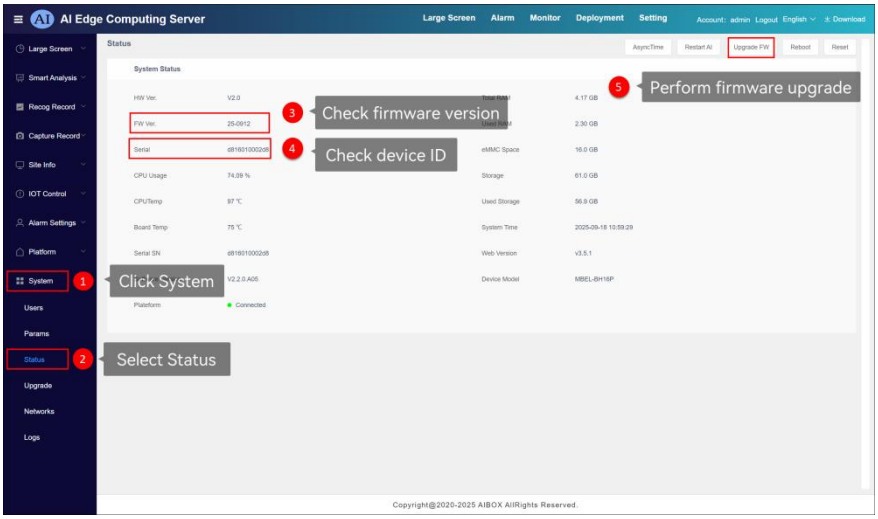


Figure 4.6 Viewing Device ID and Firmware Upgrade

If the firmware version is not the latest, please contact our technical support team to obtain the latest installation package.

Firmware Upgrade Steps:

Firmware Upgrade: Click Upgrade FW, then Click Chose File to upload the upgrade package provided by our technical support team, and then click Upgrade FW to proceed.

Please wait patiently during the upgrade process and do not operate the platform.

4.5 System Online Upgrade and LOGO Replacement

Setup steps: Left sidebar → System → Upgrade → Upgrade/LOGO Replace.

To perform an online upgrade, click “Upgrade”. The system will automatically start the upgrade process. Do not operate the platform during this time.

LOGO Replace steps are as shown in the figure.

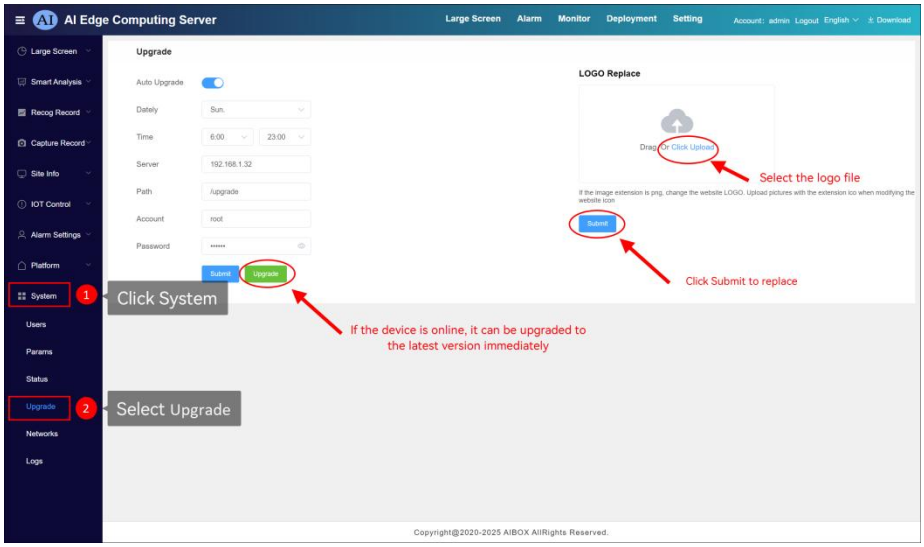


Figure 4.7 Online Upgrade Settings and LOGO Replacement

4.6 Website Title Modification

Setup steps: Left sidebar → System → Params → Modify Website Name.

Enter the system parameters page, locate

, modify the website title text in the input field, and click 

to apply the changes immediately.

4.7 Camera Video Stream Integration

Setup steps: Left sidebar → Alarm Settings → Channels → Add camera / Edit existing camera, as shown in the figure:

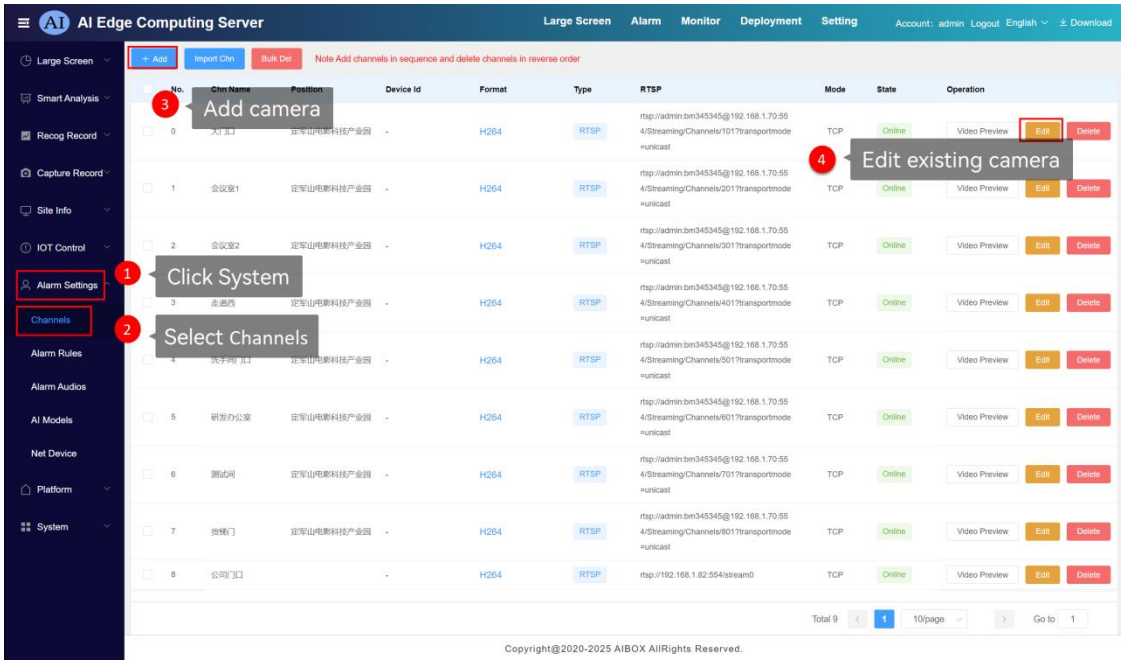


Figure 4.8 Adding/Editing Camera Channels

Note: The edge supervisory device supports cameras with resolutions up to 8 megapixels. 1080P resolution with H.264 RTSP video stream is recommended. All channels must be added sequentially from 0 to 15. Skipping numbers in the sequence may cause AI recognition to malfunction.

4.7.1 Special Notes on Camera Integration

4.7.1.1 Adding Ordinary Cameras to the Edge-Side Supervision Device

For cameras that support ONVIF discovery, the RTSP address can be obtained via ONVIF search; if the RTSP address is already known, enter it directly. As shown in the figure below, fill in the required information according to the page prompts, then follow the steps accordingly.

The RTSP address format for our company's cameras is:

rtsp://192.168.1.31:554/stream0

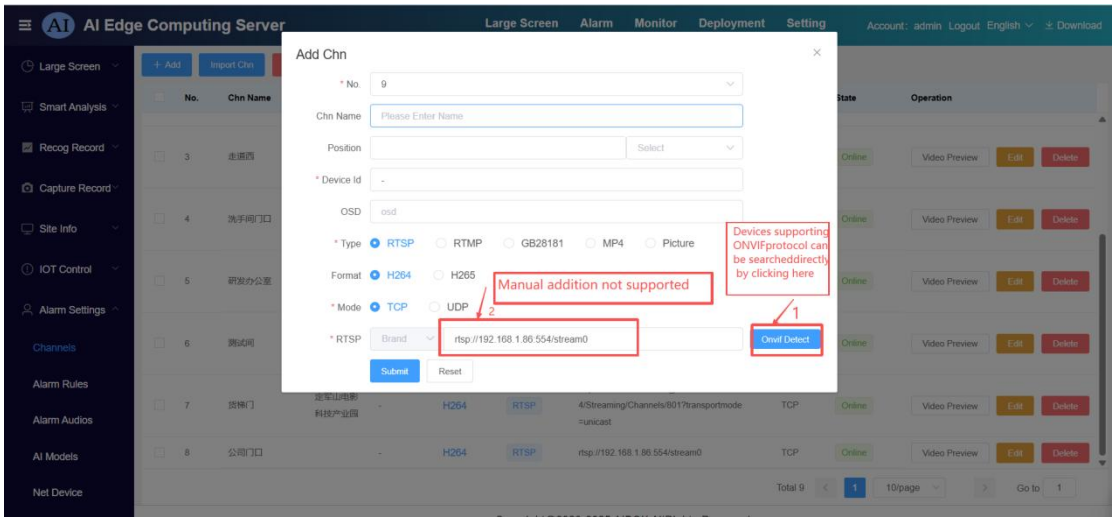


Figure 4.9 Edit Channel Settings Page

If multiple cameras need to be integrated, use our company's 4gcms software to verify the RTSP addresses of the cameras. During this process, please note:

Identifiers starting with "d8" represent the AI box, while those starting with "c8" represent the camera ID.

Note: When entering RTSP/RTMP URLs in the channel configuration interface of the device, users should first verify the video stream using VLC media player to ensure the stream can be successfully read. Only after confirming that the IP address, username, and password are correct should the camera be added to the web-based channel settings of this product.

4.7.1.2 Adding Hikvision Cameras to the Edge-Side Supervision Device

For Hikvision cameras, ONVIF discovery may fail to detect them, and some models have RTSP disabled by default. You must manually enable the RTSP function on the Hikvision camera. The RTSP address format is as follows:

rtsp://admin:woxi123456@192.168.1.64:554/h264/ch1/main/av_stream

Manually enter this address into the RTSP address field in the figure above.

Important Notes: It is recommended to set the encoding format of Hikvision cameras to H.264. The interface for setting H.264 encoding is shown in the figure below. H.265 is also supported, but real-time video playback in the browser may be slightly slower.

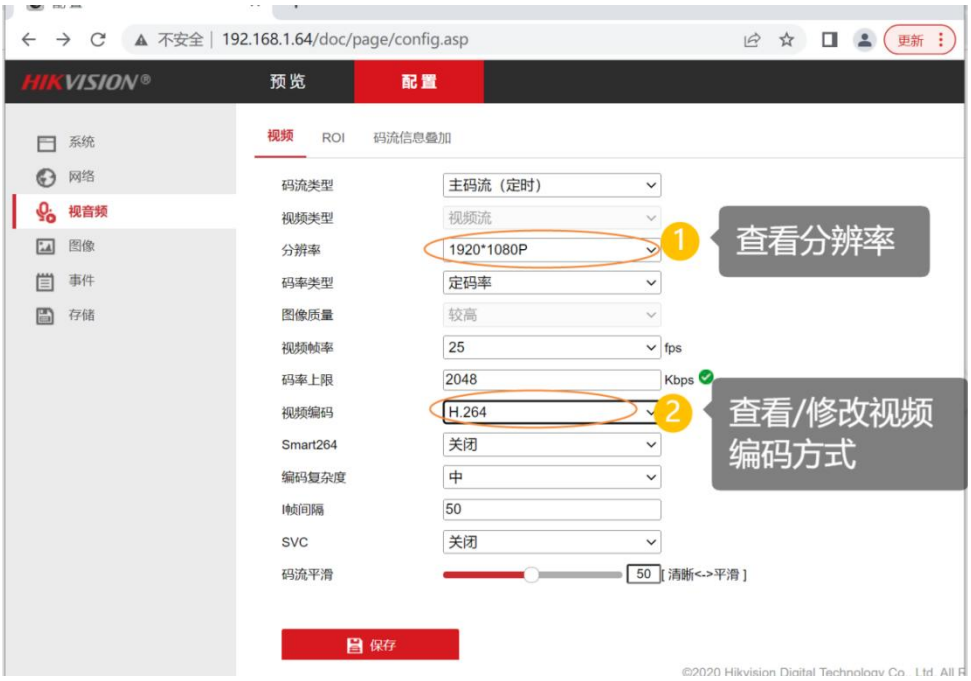


Figure 4.10 Hikvision Camera Encoding Settings Page

4.7.1.3 For Hikvision NVRs to directly stream RTSP to the Edge-Side Supervision Device

Hikvision NVR, take iDS-8632NX-I8/FA as an example:

Figure 4.11 Hikvision NVR System Settings Page

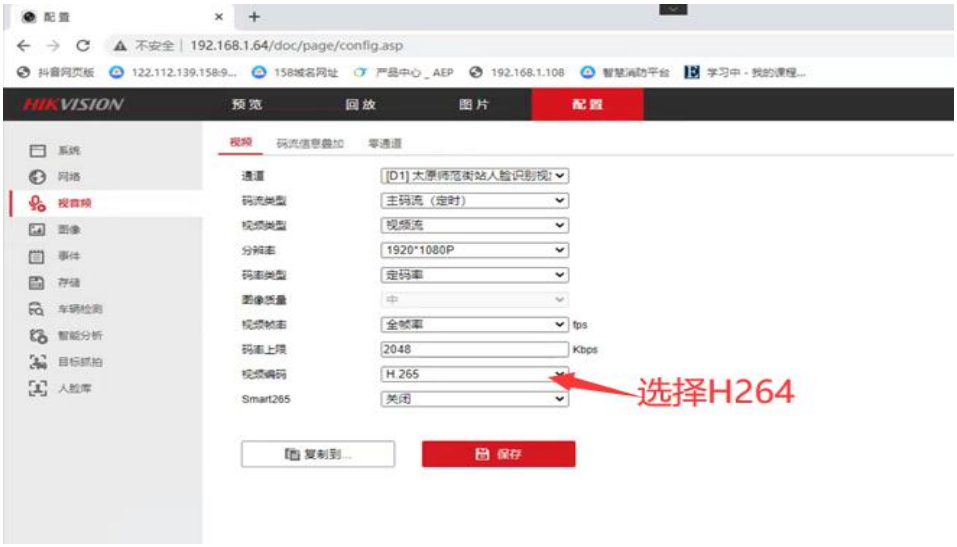


Figure 4.12 Video Encoding Viewing and Modification Page

rtsp://admin:ty080910@192.168.1.88:554/Streaming/Channels/701?transportmode=unicast

rtsp://admin:ty080910@192.168.1.88:554/Streaming/Channels/1201?transportmode=unicast

rtsp://admin:ty36zhan@192.168.1.64:554/Streaming/Channels/201?transportmode=unicast

Note: For Hikvision NVRs, H.265 is generally supported without issues. In "701", "7" represents the channel number, "1" indicates the main stream (high bitrate), and setting it to "2" will output the sub-stream (low bitrate).

DS-9632N-ST IP channel 01 main stream:

rtsp://admin:12345@172.6.22.234:554/Streaming/Channels/101?transportmode=unicast

DS-9016HF-ST IP channel 01 main stream:

rtsp://admin:12345@172.6.22.106:554/Streaming/Channels/1701?transportmode=unicast

Note: The password for cameras and NVRs must not contain special characters, otherwise the RTSP URL cannot be parsed.

Example of incorrect RTSP for NVR:

rtsp://admin:Scfb2025#@192.168.9.100:554/Streaming/Channels/101?transportmode=unicast

Example of incorrect RTSP for NVR:

rtsp://admin:Scfb2025#@192.168.9.21:554/h264/ch0/main/av_stream

Corrected version:

rtsp://admin:Scfb2025@192.168.9.100:554/Streaming/Channels/101?transportmode=unicast

rtsp://admin:Scfb2025@192.168.9.21:554/h264/ch0/main/av_stream

Remove the "#" character from the password.

4.7.1.4 For Dahua cameras connecting to the Edge-Side Supervision Device

The RTSP format for Dahua cameras and NVRs is as follows:

rtsp://username:password@ip:port/cam/realmonitor?channel=1&subtype=0

For example, to request sub-stream 1 of channel 1 from a camera device, the URL is:

rtsp://admin:admin123456@192.168.1.108:10554/cam/realmonitor?channel=1&subtype=0

For example, to request sub-stream 1 of channel 2 from an NVR device, the URL is:

rtsp://admin:admin@192.168.1.112:554/cam/realmonitor?channel=2&subtype=1

Important Notes: When connecting Dahua cameras to the edge-side supervision device, please generally keep the camera bitstream no higher than 2 Mbps.

4.7.1.5 5.2.5.RTMP Video Access

For cases where RTSP video streams need to be accessed, simply add the RTMP address in the channel management section.

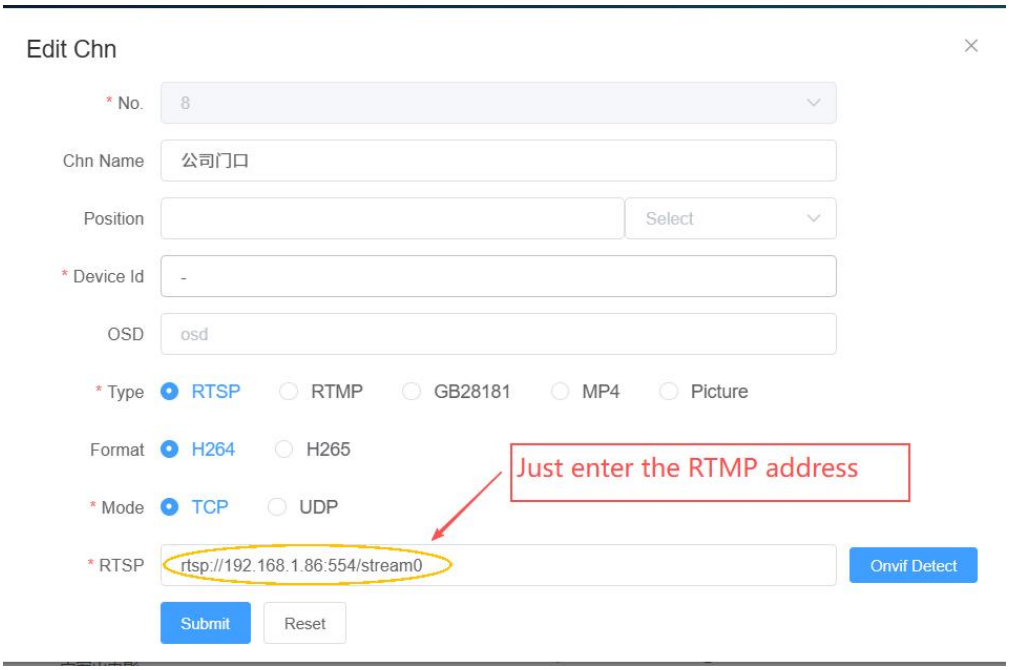


Figure 4.13 RTMP Location to Enter RTMP Address

4.8 AI Algorithm Deployment

Setup steps: Left sidebar → Alarm Settings → Alarm Rules, as shown in the figure: edit the alarm rules for the channel.

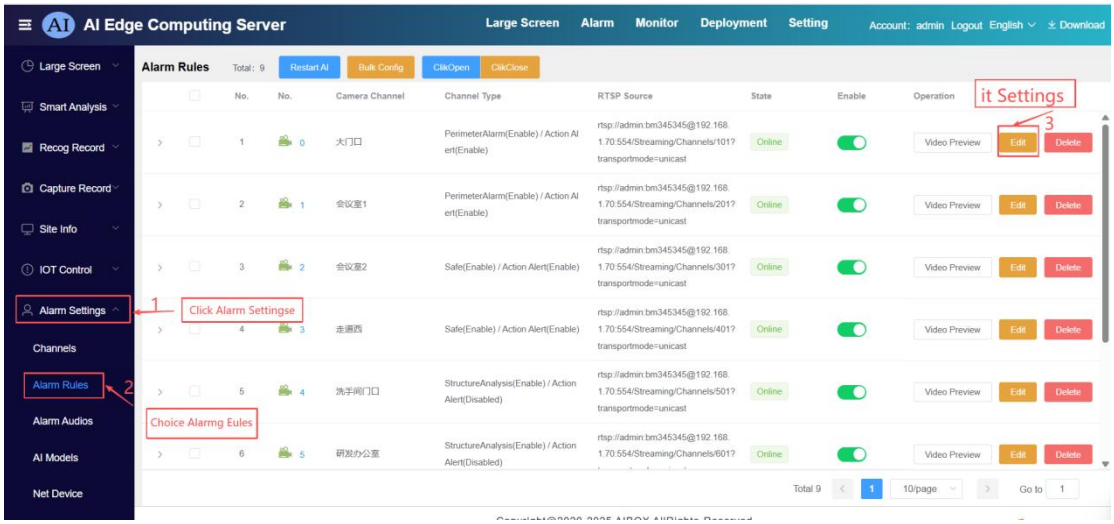


Figure 4.14 Alarm Rules Page

By editing the AI configuration of the channel, different alarm algorithms can be applied. For each rule configuration, click the "+" on the left to perform detailed settings. After completing the configuration, submit the settings.

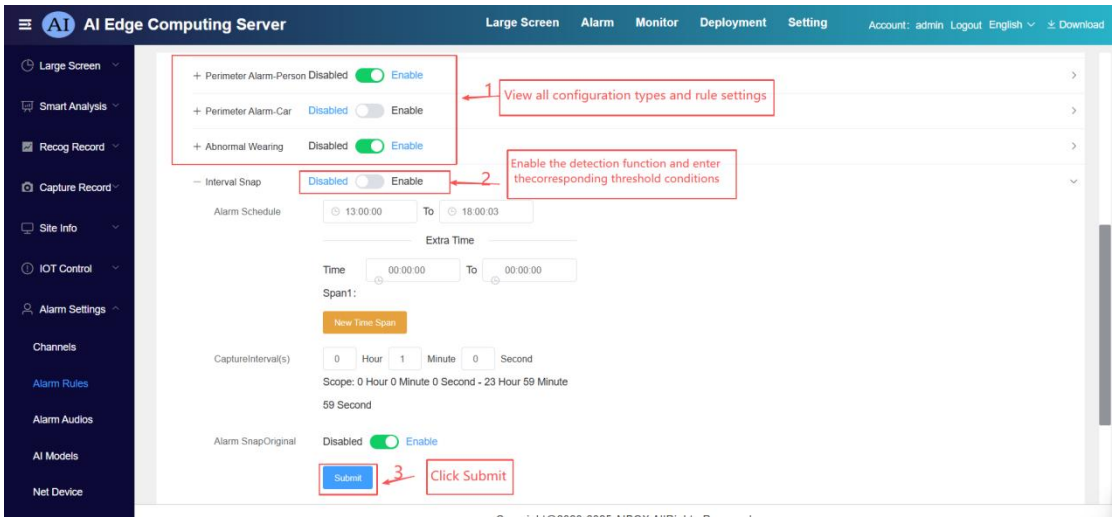


Figure 4.15 Alarm Rules Edit Page

Important Notes💣:

If the overall detection and alarm system performs poorly, appropriately lower the confidence threshold and check the position of the alert zone (bounding box or line). The default detection area is inside the alert bounding box.

If the detection and alarm system produces inaccurate alerts or false positives, pay attention to the Time Threshold(s) (minimum duration for event detection, e.g., how long a person must be

absent before triggering a leaving-post alert) and Alarm Interval(s) (minimum time between consecutive alarms of the same type) in the alarm settings.

If detection results are generated but the speaker does not sound the alarm, check whether the Voice Linkage option is enabled; there may also be errors in related audio settings. Please verify that the audio content has been properly configured. For related settings, refer to Section 7.

When using Personnel Leaving Post detection in Action Alert, it must be used in conjunction with the absence duration setting — that is, an alarm will be triggered after a person has been away from the post for a specified period.

4.8.1 6.1.Alarm Basic Rules Logic

Currently, the system is divided into three main categories of AI functions:

（1） Capture and attribute analysis of motor vehicles, non-motor vehicles, faces, human shapes, and license plates.

（2） Object detection, including smoke, flame, fire safety equipment, etc.

（3）Personnel behavior detection — pay special attention to the loitering duration setting.。

Important Notes: Due to system resource limitations, the total number of channels with rule (1) or rule (3) enabled must not exceed 15. If the previous channel configurations have already reached this limit, subsequent channel configurations will be invalid.

On the configuration page, commonly used rules are already listed. You can enable or disable them as needed and adjust corresponding settings. After completing the configuration, restart the algorithm module for the changes to take effect.

4.8.2 Deployment Configuration Completion and Activation

After completing the deployment configuration, the AI algorithm module must be reloaded. Therefore, restart the algorithm module. The operation steps are shown in the figure below:

Setup steps: Left sidebar → System → Status → Restart AI

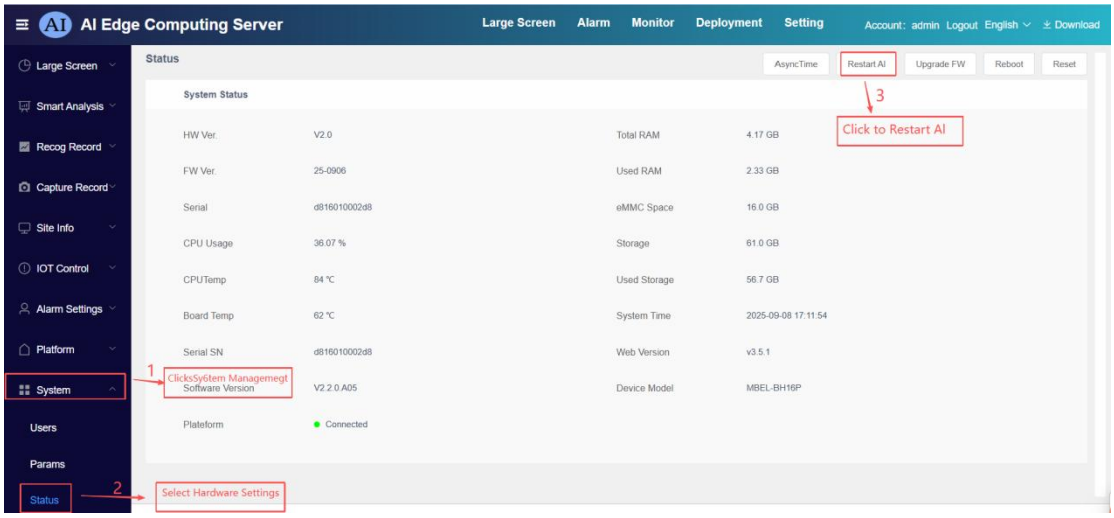


Figure 4.16 Guidance on Restart Procedure

Important Notes💣:

After configuring the "Structure Analysis Rule Set" and "Action Alert Rule Set" master switches, you must restart the AI.

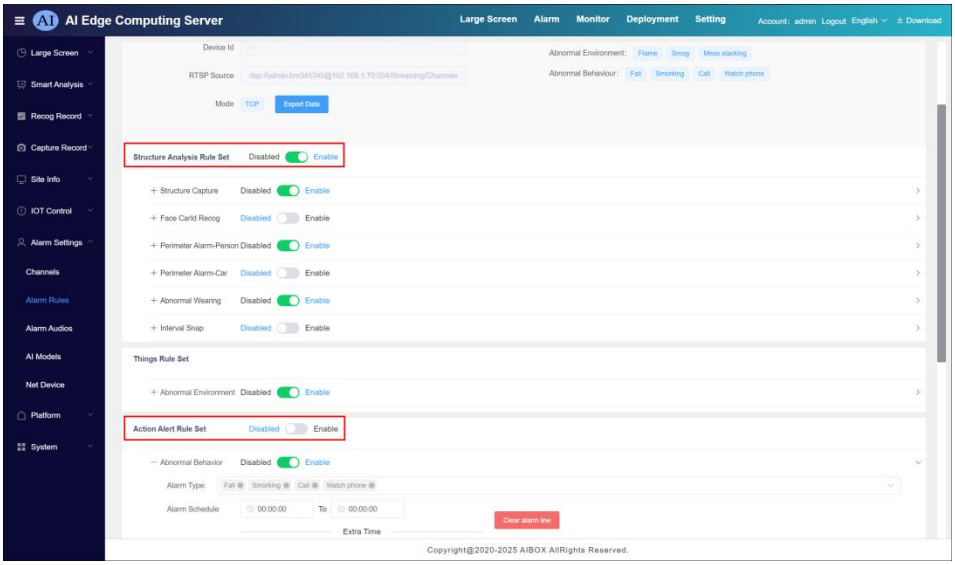


Figure 4.17 Restart AI after enabling these two switchesl

4.8.3 Special Notes on Smoke and Flame Detection

Environmental lighting can affect smoke and flame detection, and in some scenarios, such interference is unavoidable. Adjusting dynamic detection parameters helps reduce false alarms, which is especially important when severe light interference occurs in practical applications.

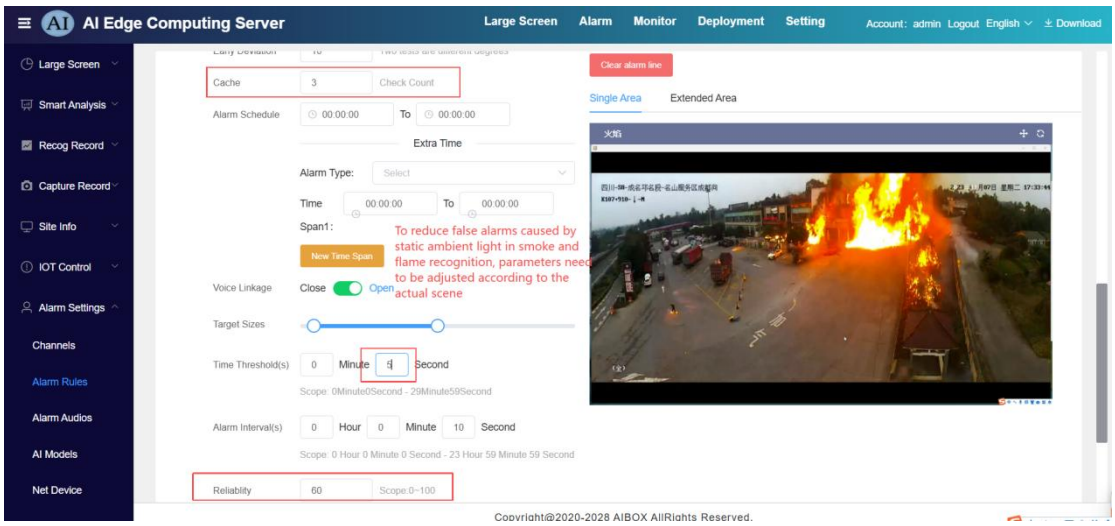


Figure 4.18 Flame Alarm Configuration Instructions

About Early Deviation:

This parameter sets the threshold for how much the position or state of a suspected fire source object can change across consecutive frames. The system will only trigger an alarm when the detected change exceeds this threshold. For easier testing, you can set this value slightly lower.

About Cache:

Set to 0: Detection runs at the fastest speed, suitable for quick algorithm testing.

Set to 1–3: Speed is moderate, suitable for typical scenarios.

Set to 4 or higher (values greater than 3): Detection accuracy improves, but CPU usage increases and processing speed slows down.

For testing purposes, you can also lower the Time Threshold, Alarm Interval, and Reliability parameters appropriately.