AI Video Surveillance and Analysis Terminal System User Manual

Eight 2025

Copyright notice

Revisions status

Version	Status	Revise content	Compiling personnel	Date Completed	Reviewer	Review Date
V1.0	C	First Draft	Li Dashuai	April 30, 2024		

Remarks: C - Create, A - Add, M - Modify, D - Delete

Contents

1 System Overview

At present, the system has two edge computing all-in-one machines, each of which integrates 22 edge computing server units, which can support up to 352 channels of 1080PAI video analysis and a Haiguang server motherboard. The centralized management platform of the edge all-in-one machine runs on the Haiguang server system, and both servers can be used as the management platform, and we currently choose one of them as the main system to manage all 44 computing units.

To simplify system deployment, the 44 computing units are interconnected via a local area network (LAN) and connected internally to the server system's network interfaces. For external connectivity, another network interface on the server is used to connect to the video network.

1.1 System Positioning and Core Value

The AI Video Surveillance and Analysis Terminal System is an industrial-grade intelligent surveillance solution developed by Shenzhen Benmai Technology Co., Ltd. Integrating edge computing, artificial intelligence, and video analytics technologies, the system serves scenarios such as energy, chemical plants, industrial parks, and security, providing end-to-end management from video access and intelligent analysis to alarm linkage. Through a collaborative architecture combining edge computing integrated appliances with a centralized management platform, the system enables real-time processing and centralized control of massive video streams, significantly improving monitoring efficiency, reducing labor costs, and helping users build intelligent and automated security protection systems.

1.2 System Architecture and Component Functions

1.2.1 Edge Computing Integrated Appliance

Hardware Configuration: A single all-in-one machine integrates 22 edge computing server units and one Haiguang server motherboard, supporting parallel AI analysis of up to 352 channels of 1080P video streams. Each computing unit is equipped with an independent computing module, capable of handling 16 channels of video input, decoding, AI analysis, and data storage.

Network Design: The system employs an internal-external network isolation architecture. The computing units interconnect with the server via a local area network (LAN), while the server connects to the external video network through a dedicated network interface, ensuring secure data transmission.

Core capabilities: Support H.264/RTSP protocol access to mainstream cameras, built-in

46 small model algorithms (covering personnel violations, environmental anomalies, perimeter warnings and other scenarios), and can output structured analysis results (such as face attributes, vehicle number plates, and abnormal behavior types) in real time.

1.2.2 Centralized Management Platform

Deployment Platform: Hosted on the Hygon server system, supporting dual-server hot standby (with switchover between primary and secondary servers), enabling unified management of the 44 computing units within the local area network.

Functional Matrix:

- **Data Visualization:** Real-time display of key metrics—such as snapshot statistics, alarm trends, and device online rate—via dashboard on large screens. Supports multi-dimensional time filtering (Today, Last 7 Days, Last 30 Days).
- **Device Management:** Provides functions such as IP configuration for computing units, channel management, and GB28181 national standard cascading, supporting batch device addition and parameter synchronization.
- **Alarm Management System:** Integrates multiple alarm types—including perimeter intrusion detection, structured video analysis, and facial recognition—enabling secondary validation using large AI models to filter false positives. Alerts can be delivered to third-party platforms via standard protocols such as HTTP and MQTT.
- **System Configuration:** Supports user role and permission management, interface language switching (Chinese/English), personalized settings for LOGO and title, as well as configuration of data synchronization and cleanup policies.

1.3 Core Functional Features

1.3.1 Intelligent Video Analysis

Multi-Algorithm Collaboration: Enables simultaneous execution of multiple algorithms—such as person detection, flame recognition, and license plate identification—on a single video stream, facilitating "multi-detection on a single screen" capabilities.

Dynamic Rule Configuration: Users can customize parameters such as monitoring zones, confidence thresholds (0–100), and dwell time to adapt to diverse operational scenarios. For example, in chemical plant environments, a dual-trigger alarm rule combining "smoke detection" and "unauthorized personnel intrusion" can be configured for tank farm areas.

Large Model Application: Employs advanced large AI models to conduct semantic analysis on alerts generated by smaller models (e.g., verifying the authenticity of images indicating "running, steaming, dripping, or leaking" (RSDL) conditions), effectively minimizing false alarms triggered by environmental factors.

1.3.2 Flexible Integration and Interoperability

Cross-Brand Compatibility: Supports RTSP integration with mainstream cameras from brands such as Hikvision and Dahua, and is compatible with the ONVIF protocol for automatic device discovery. Also adapts to specialized access scenarios, including 4G/RTMP streaming.

Multi-Point Interoperability: Upon alarm triggering, the system synchronously activates local pop-up alerts, on-site voice announcements (requires external speaker configuration), and remote platform notifications. Supports integration with access control and fire protection systems to establish a comprehensive, multi-layered security and safety network.

1.3.3 Data Management and Operations & Maintenance

Storage Strategy: Supports dual storage modes—local storage and centralized synchronized storage. Users can configure alarm-triggered recording duration (default: 20 seconds) and image compression quality. The system automatically purges expired data to release storage space.

Remote Operations & Maintenance: Provides online upgrade, remote firmware push, and log query capabilities. Supports batch configuration of computing unit parameters via the centralized management platform, effectively reducing operational complexity and maintenance overhead.

1.4 Typical Application Scenarios

1.4.1 Industrial Safety Production Monitoring

In high-risk industrial environments such as petrochemical plants and power stations, the system continuously monitors critical safety risks, including personnel PPE compliance (e.g., wearing of safety helmets and protective clothing), equipment abnormalities—such as fluid leaks, vapor emissions, flame ignition, and smoke generation—and unauthorized intrusions into designated zones. Upon detection, the system triggers 联动 actions by activating on-site audible/visual alarms and forwarding alerts to the central control system, achieving the operational objective of "hazard detection within seconds and response initiation within minutes."

1.4.2 Integrated Security System for Smart Parks

Applicable to industrial parks, campuses, and similar environments, the system enhances security efficiency through perimeter intrusion detection, facial recognition access control, and automatic capture of illegally parked vehicles. Integrated with a centralized

visualization dashboard, it provides real-time situational awareness of personnel flow and equipment operational status, supporting emergency command and decision-making.

1.4.3 Behavioral Intelligence in Public Spaces

In public spaces such as shopping malls and transportation hubs, the system detects crowd gatherings, identifies falls, and performs pedestrian flow statistics. This supports optimized crowd guidance and enhanced safety management. It also provides data-driven insights for commercial operations, such as hotspot zone analysis and customer dwell time trends.

1.5 System Advantages

High Performance: The edge computing unit is equipped with a dedicated AI chip, enabling single-stream video analysis with latency of less than 500ms. The system supports 7×24 hours continuous operation, ensuring reliable real-time processing in mission-critical environments.

Easy Deployment: The system features plug-and-play hardware and an intuitive graphical interface, enabling users with no prior experience to quickly set up and operate it.

Scalability: Supports customizable AI algorithms and modular expansion of computing resources, allowing adaptation to diverse industry-specific detection requirements—such as hazardous chemical vehicle identification or defect detection on specialized equipment.

2 Product Form and Design

The product is available in three rack-mountable configurations:

- 1U model：supports up to 96 video channels
- 2U model：supports up to 128 video channels
- 4U model：supports up to 352 video channels

Figure 2-1 1U All-in-One AI Server

Figure 2-2 2U All-in-One AI Server

Figure 2-3 4U All-in-One AI Server

2.1 Hardware Connection Instructions

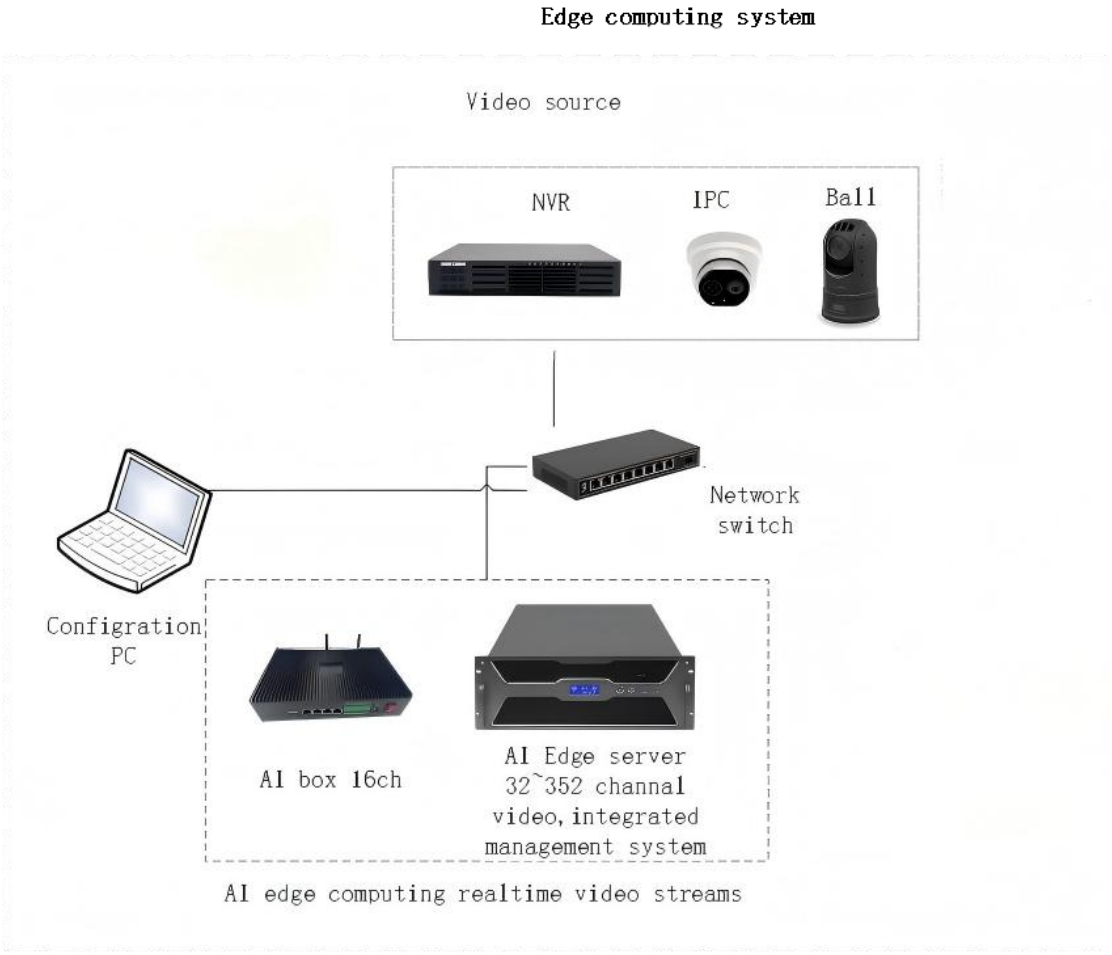


Figure 2-4 Hardware Connection Diagram

Figure 2-5: Connection Method of the 1U AI Edge Server All-in-One

Figure 2-6 Connection Method of the 2U AI Edge Server All-in-One

3 Instructions for Using the Centralized Management Platform

The centralized management platform is primarily designed to manage multiple AI edge computing units or AI boxes within a local area network, facilitating their use in large-scale projects.

3.1 Server IP Address Configuration

Note: In the current version, for ease of IP configuration, the network interface settings are managed internally by dedicated software. You can use the setup tool to search for and configure the IP address. The specific steps are as follows:

1. Find a Windows PC and run the configuration tool，BMLiteTool.exe.
2. Search for and edit the device starting with "a01101" (Note: If the device is not found, please disable the Windows firewall):

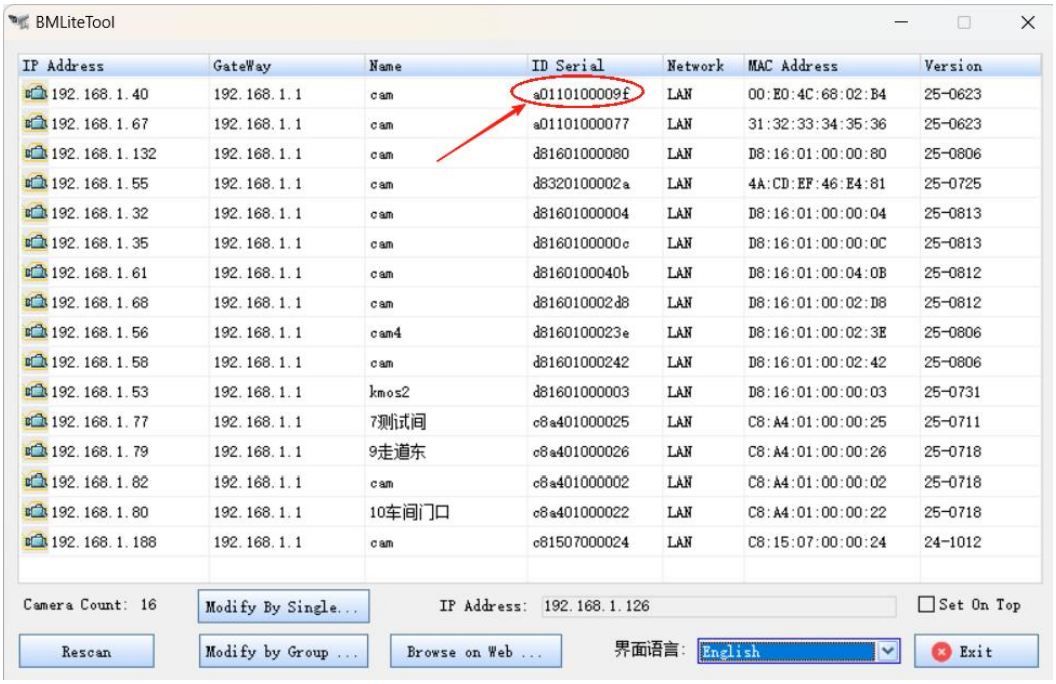


Figure 3-1 Searching for IP Using BMLiteTool.exe

3. Change the IP address to the desired one. Note: The gateway and subnet mask must also be adjusted accordingly.

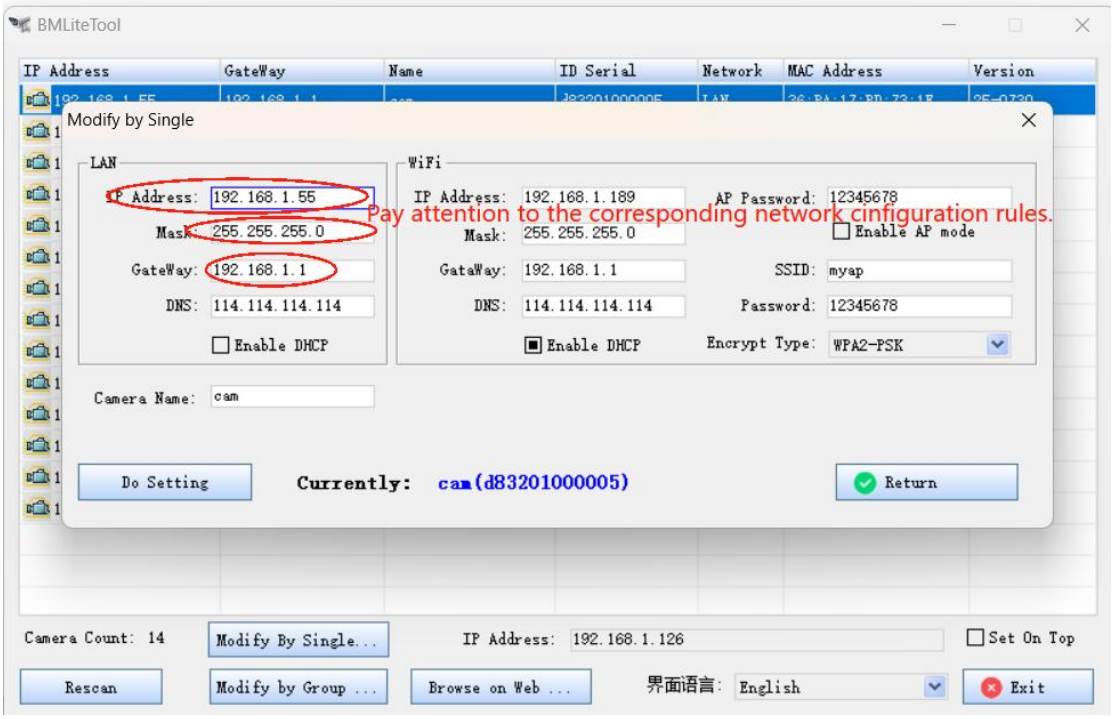


Figure 3-2 Changing IP Using BMLiteTool.exe

4. Once the network parameters are set, you can continue with the next steps based on the configured IP address.

Note: This tutorial is based on the 192.168.1.X IP segment. In your network environment, you will need to modify the settings according to your specific IP segment.

3.2 Introduction to Functional Modules

Local Centralized Management Platform Functions:

The Local Centralized Management Platform provides functions including large-screen data dashboards, maps, workbenches, alarm management, real-time monitoring, and system settings.

3.3 Instructions for using interface functions

3.3.1 Login Interface

1. To log in from the local machine, enter the following URL in the browser: http://127.0.0.1:3000/,

To log in from another computer on the local network, access the IP address of the edge all-in-one machine. For example:http://10.179.232.58:3000/.

2. Default login username: admin , Default login password: 123456

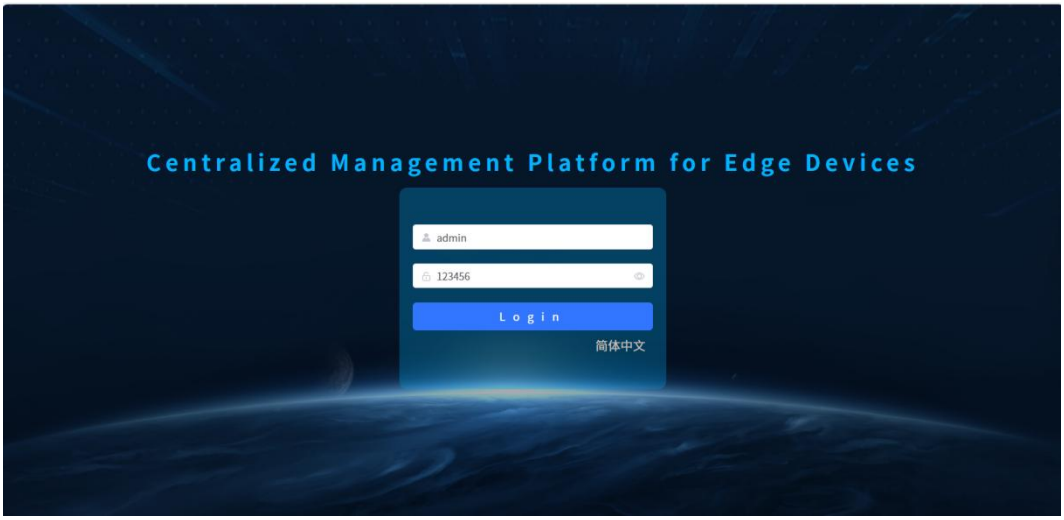


Figure 3-3 Centralized Management Platform Login Page for the AI Edge Server All-in-One

3.3.2 Large Screen Dashboard

The Large Screen Dashboard primarily displays statistical information on captures and alarms from the system. Additionally, it provides pop-up notifications when an alarm is triggered or a capture occurs.

Figure 3-4 Centralized Large Screen Dashboard for the AI Edge Server All-in-One

3.3.3 Workbench

Basic Function Description

The workbench provides a variety of data display for the entire platform, allowing users to intuitively view the current asset status, early warning status, early warning statistics, and message notifications, and quickly enter the computing unit through the workbench, supporting direct deployment and control settings for each channel. At the same time, it provides functions such as GB28181 video access configuration, AI model management, personnel file management, and vehicle file management.

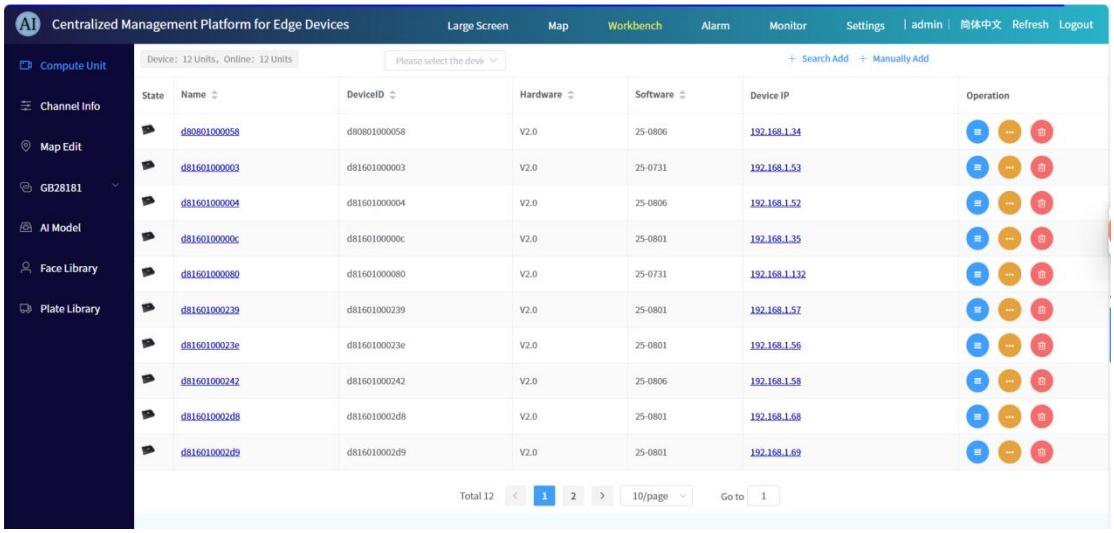


Figure 3-5 Workbench Module Interface for the AI Edge Server All-in-One

Configuration of Computing Units

1. You can add computing units within the local area network (LAN) via search, or manually add a computing unit by entering its IP address into the system.

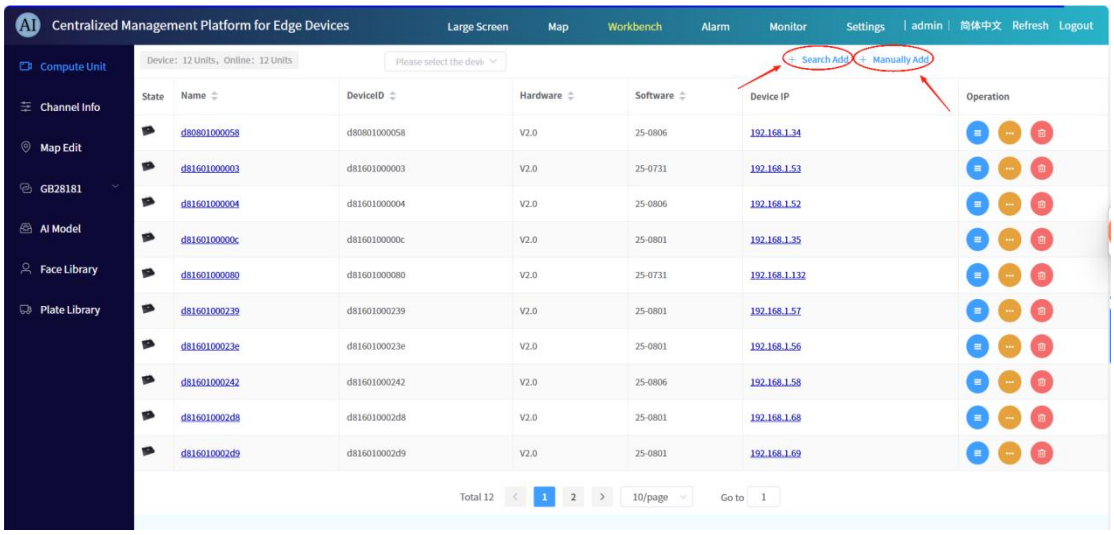
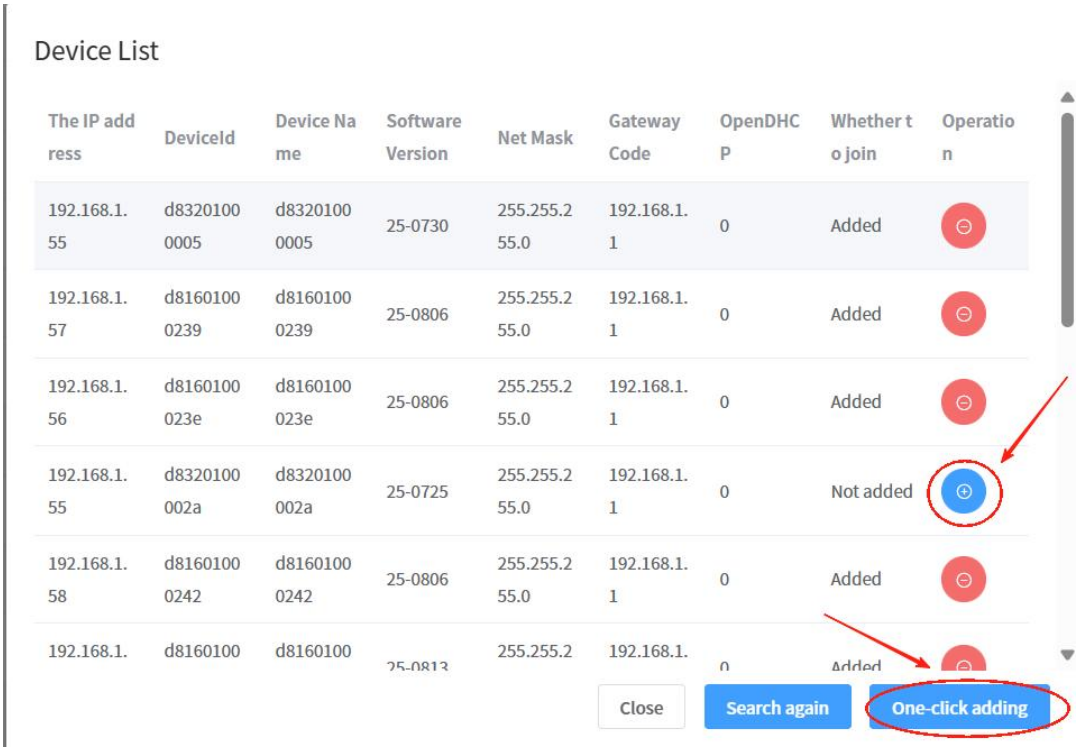


Figure 3-6 Computing Unit Interface for the AI Edge Server All-in-One

2. Click the "Add" button to search for computing units within the local area network (LAN) and add them to the management system.



3-7 Adding Computing Units to the AI Edge Server All-in-One

3. After adding, you can click the "Settings" button to edit the device.

Figure 3-8 Configuring a Computing Unit

4. In the device editing interface, you can directly edit the IP address of the computing unit by using the "Search Device" button, as shown in Figure 2-8.

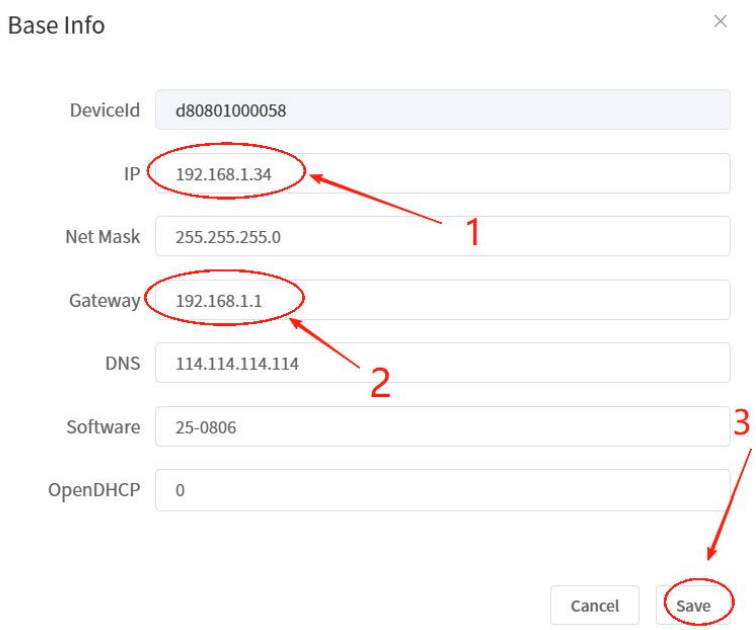


Figure 3-9 IP Address Configuration for Computing Unit

After completing the IP address configuration of the computing unit, you can proceed to configure its channels.

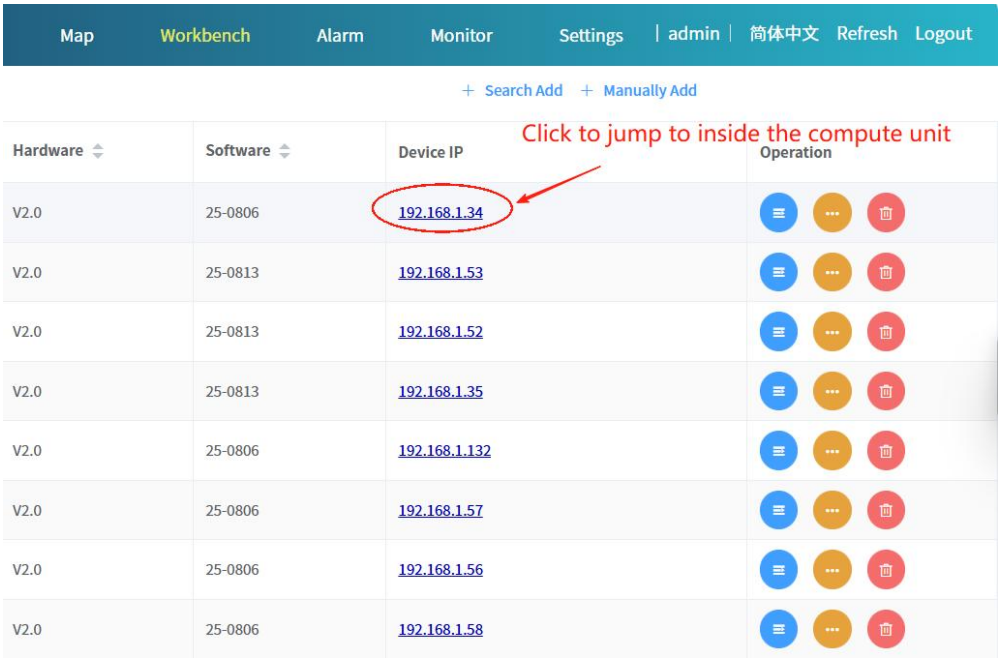


Figure 3-10 Navigating to the Computing Unit Interface

After adding channels and configuring alarm rules, all system alerts can be pushed to third-party platforms, and simultaneously displayed on the centralized management platform. Local and remote operations do not interfere with each other.

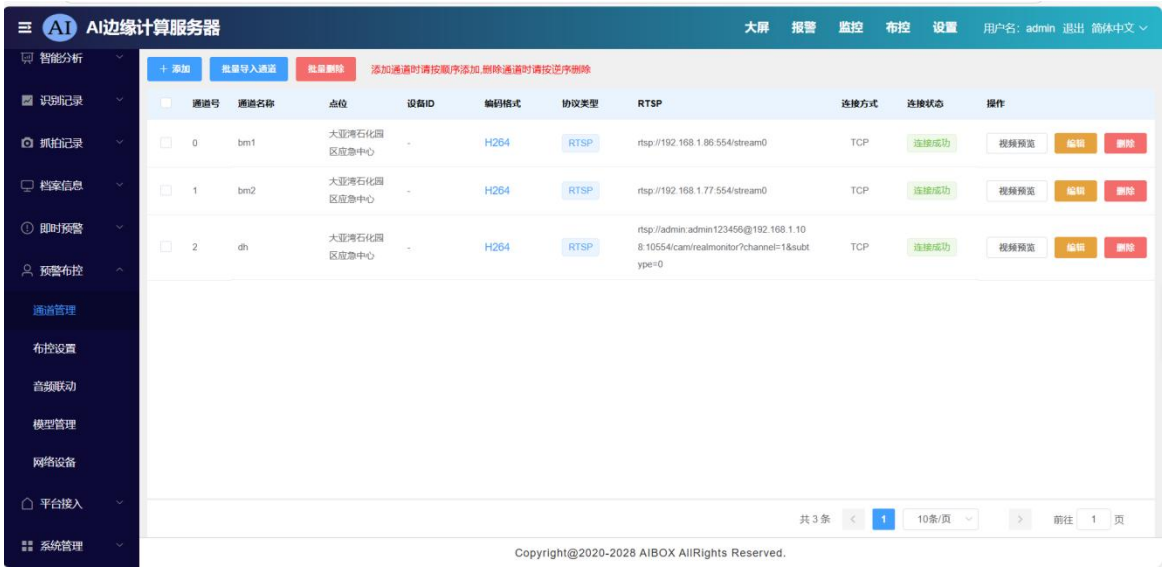


Figure 3-11 Channel Management Interface of the AIBOX

For detailed configuration of computing units, see Chapter 3 for detailed description of AI edge computing server units.

GB28181 Four-Level Cascade

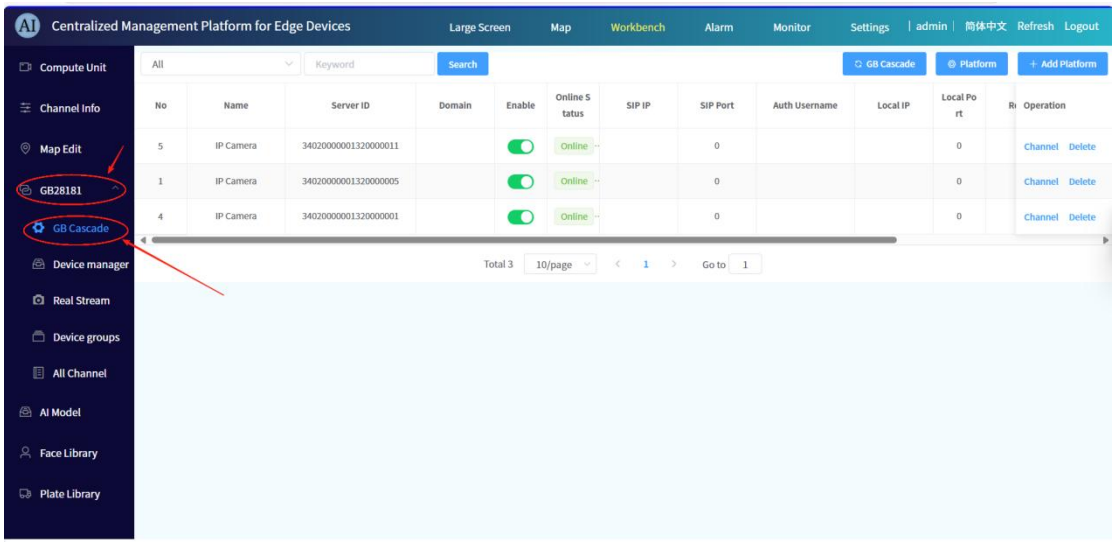


Figure 3-12 GB28181 National Standard Cascade Networking Page

For large-scale projects requiring video streams to be pulled from a video integration platform, GB/T 28181 integration is the most convenient solution. The system provides built-in support for this functionality.

By configuring the national standard (GB28181) parameters, devices can be cascaded into the system.

The configuration steps are as follows:

1. Click Workbench > GBCascade> Platform

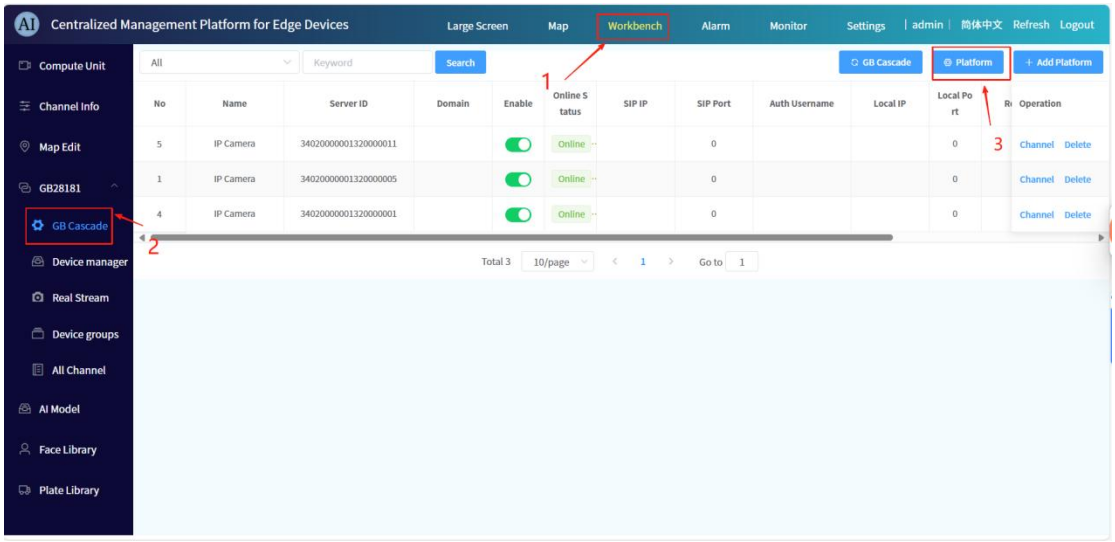


Figure 3-13 Adding a GB28181-Compliant Platform

2. Set Relevant Parameters - Proactive Addition

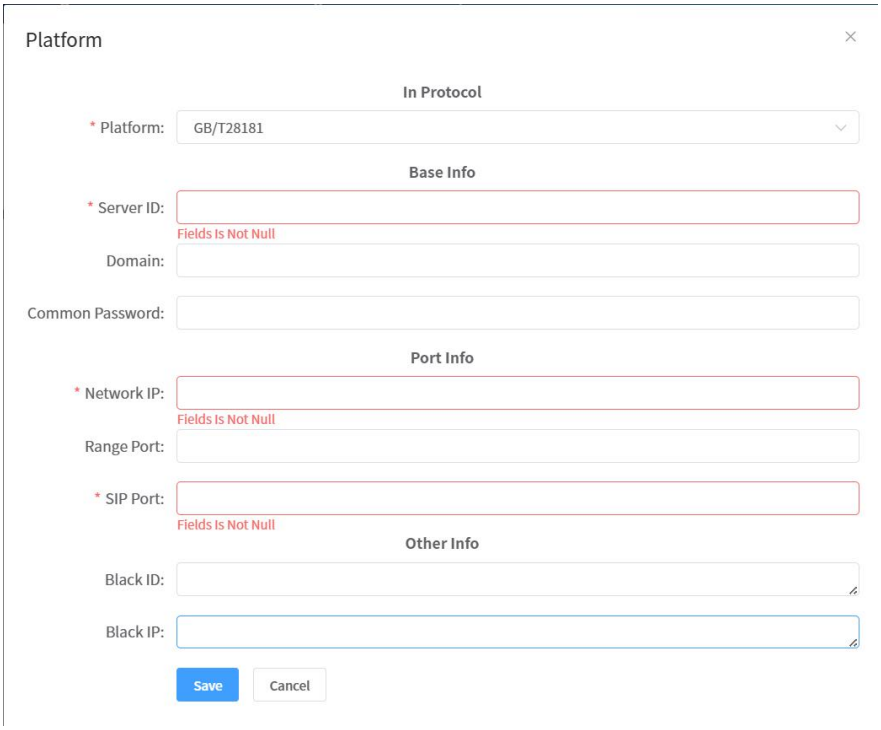


Figure 3-14 GB28181 Platform Access

The all-in-one appliance provides direct connection channels to the video integration platform for multiple external platforms.The configuration steps are as follows:

1. On the video integration platform, configure the following parameters:

External Domain ID	Default 34020000002000000001
IP Address	IPServer IP Address
Signaling Communication Port	5060

Table 2-1 Reference Parameters for Video Integration Platform Configuration

Figure 3-15 Platform Access Prompt

2. Click Workbench > GB28181 > GB Cascade > GB Cascade

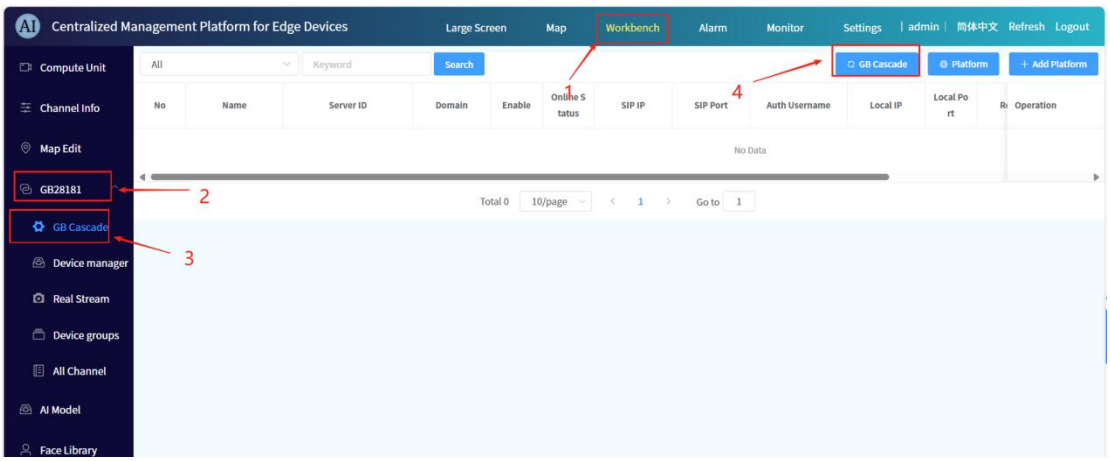


Figure 3-15 National Standard Cascade

3. After the subordinate device directory tree is connected to the GB28181 platform, the platform will automatically generate RTSP URLs. These RTSP URLs can be configured into the channels of the edge computing unit to enable normal operation.

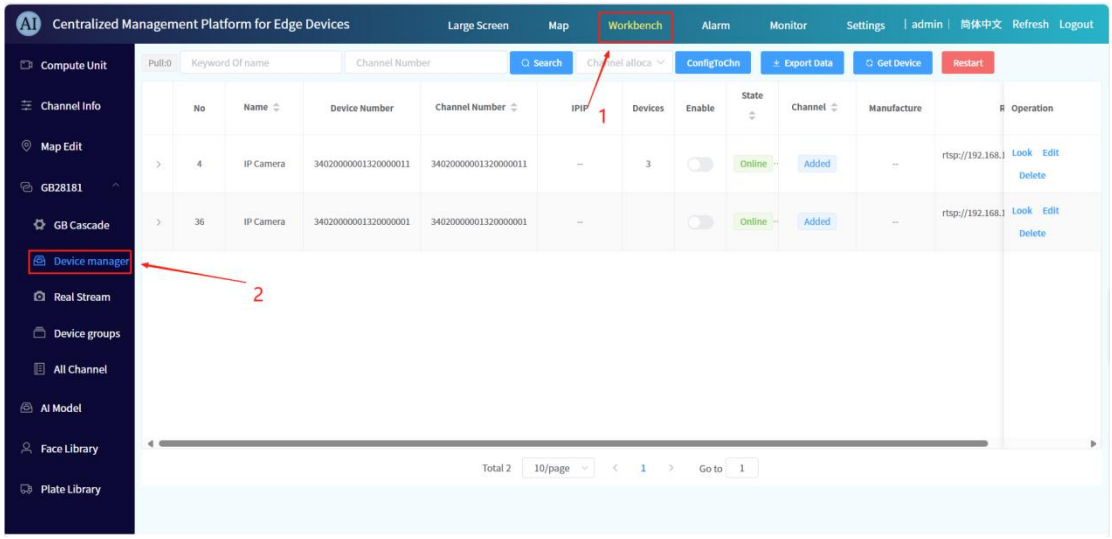


Figure 3-17 Device Management Page

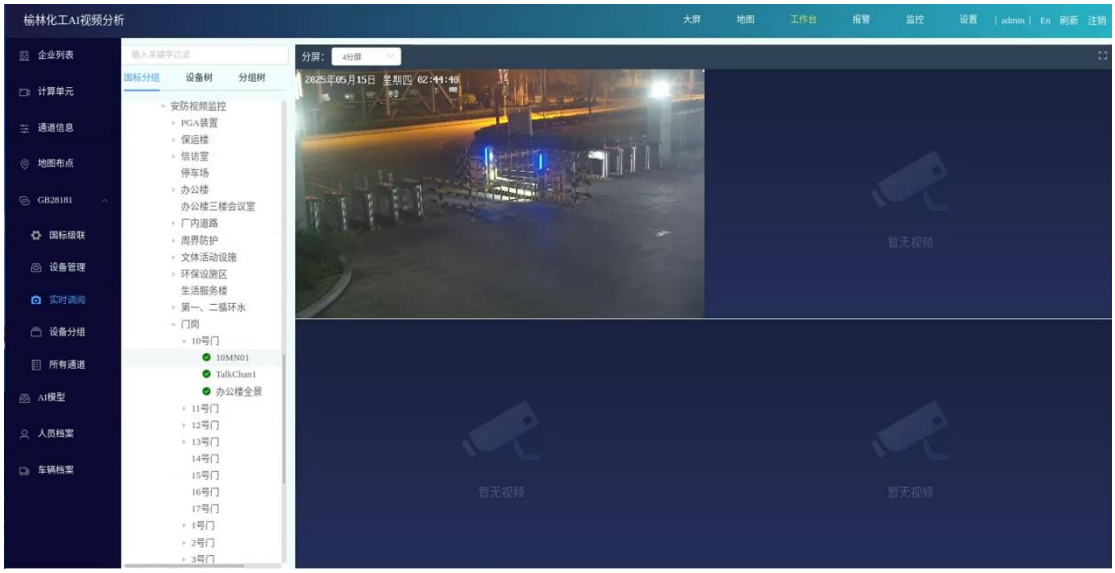


Figure 3-18 Real-Time Video Retrieval Page

Personnel File

Person profiles are used for facial recognition; therefore, the provided photos should preferably be frontal images. The steps to add a profile are as follows:

1. Click Workbench >Face Library > Add.

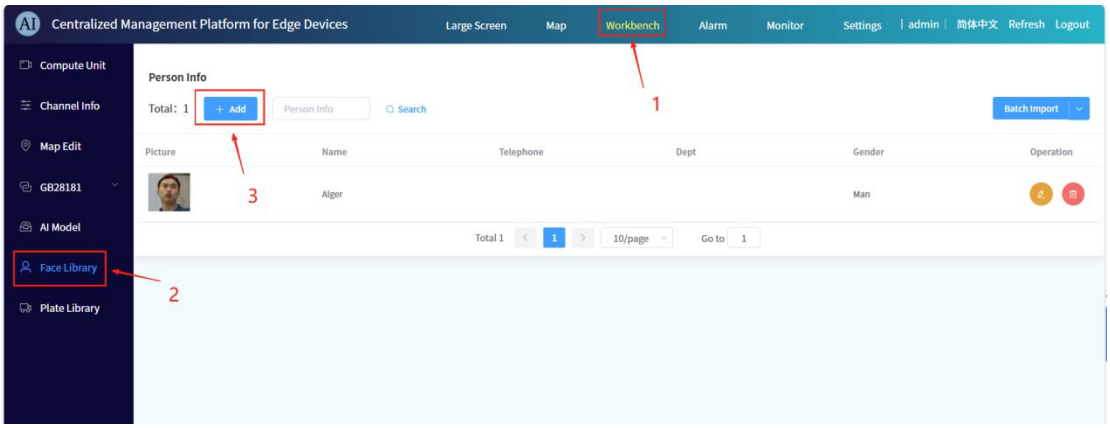


Figure 3-19 Person Profile Page

2. Personnel Profile Addition Module.

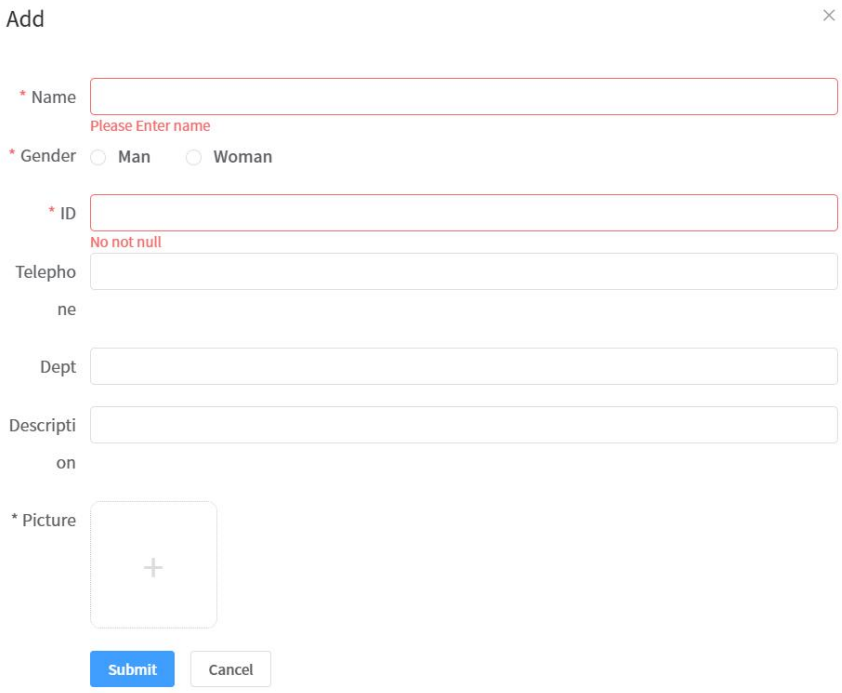


Figure 3-20 Person Profile Addition Settings

When importing data in bulk, please follow the system prompts to complete the import.

3.3.4 Alarm Management

The Alarm Management module provides functions such as intrusion detection with alarm capture, structured data capture, facial recognition, vehicle recognition, and alarm pop-up windows.

Statistical Analysis

The Statistical Analysis module provides visualized statistics of early warning data. It intuitively presents the overall security situation through multi-dimensional analysis, highlights key issues, and improves monitoring efficiency. The module supports data filtering and aggregation across different time periods, as well as export of analysis results.

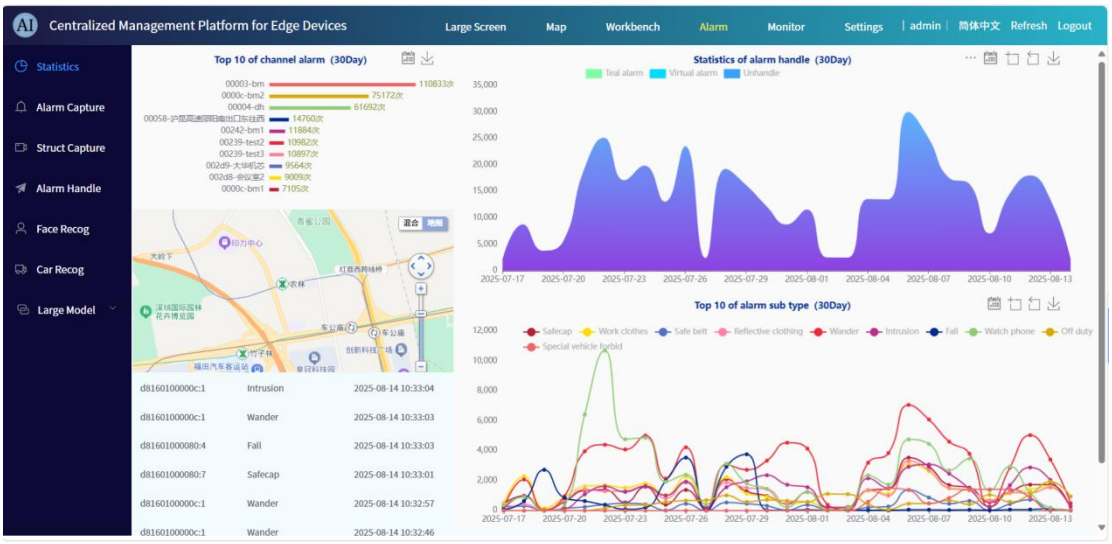


Figure 3-21 Statistical Analysis Page

Alarm Capture

Alarm Capture page provides functionalities to query alarm situations based on time, computing unit, channel, and alarm type, as well as to handle alarms.

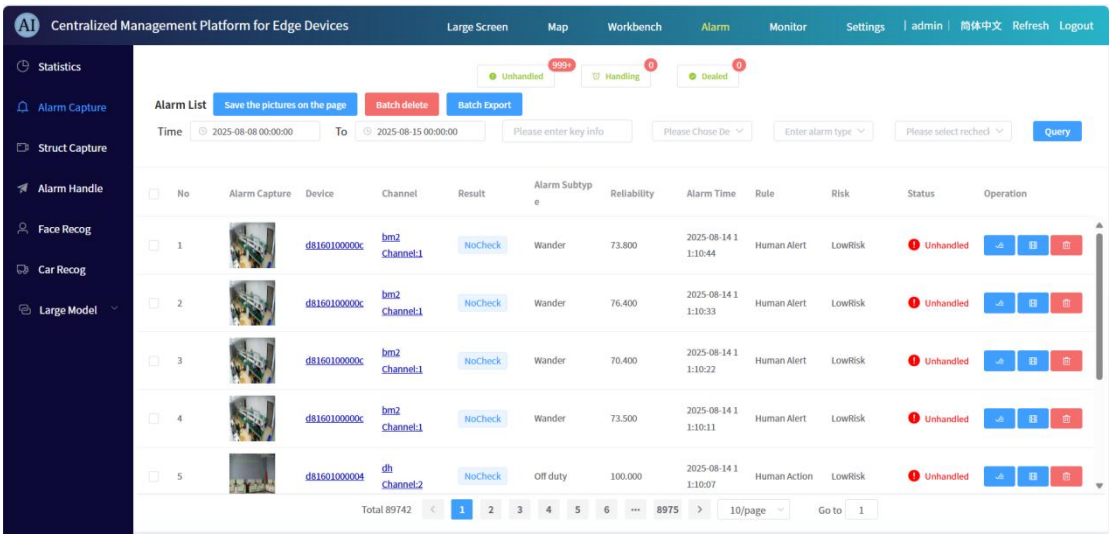


Figure 3-22 Alarm Capture Page

Struct Capture

Structured Capture provides retrieval capabilities for various captured targets, including faces, human figures, motor vehicles, non-motor vehicles, and license plates. It supports image-to-image face search and facial emotion recognition.

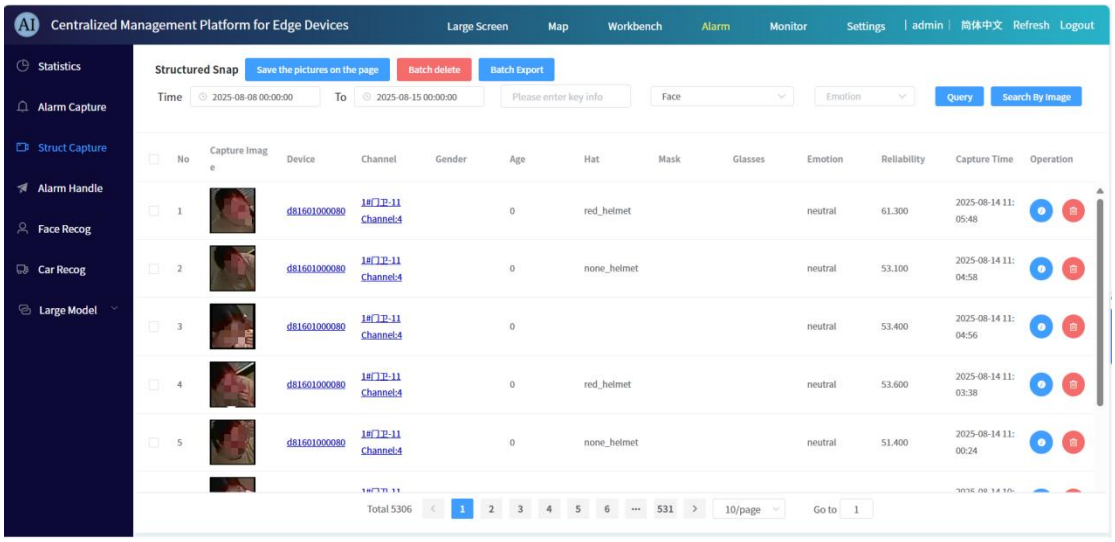


Figure 3-23 Struct Capture Page

Face Recog

Records all captured face images and provides retrieval functionality.

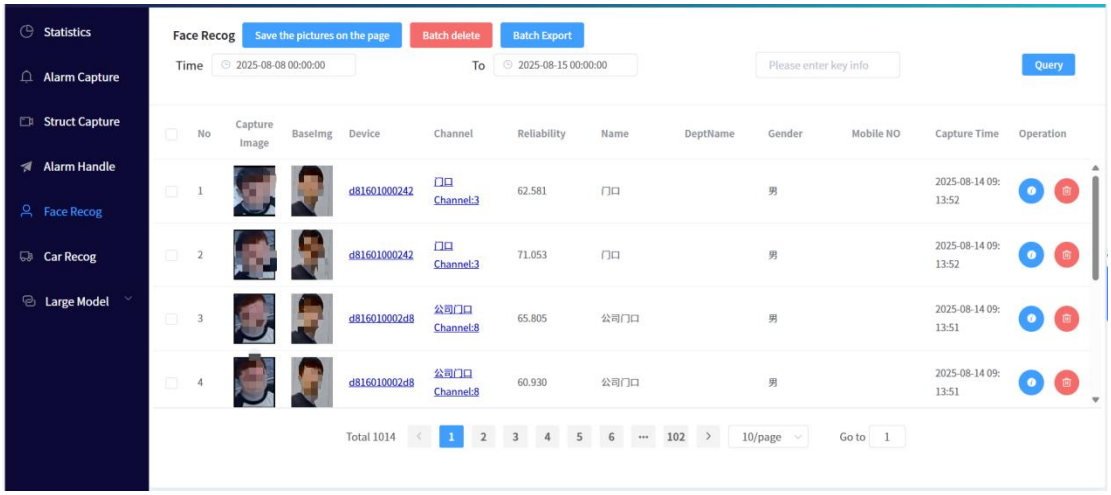


Figure 3-24 Face Recog Page

Face Recog Switch

Set the face recog switch, as well as the thresholds for face recognition and image-to-image search.

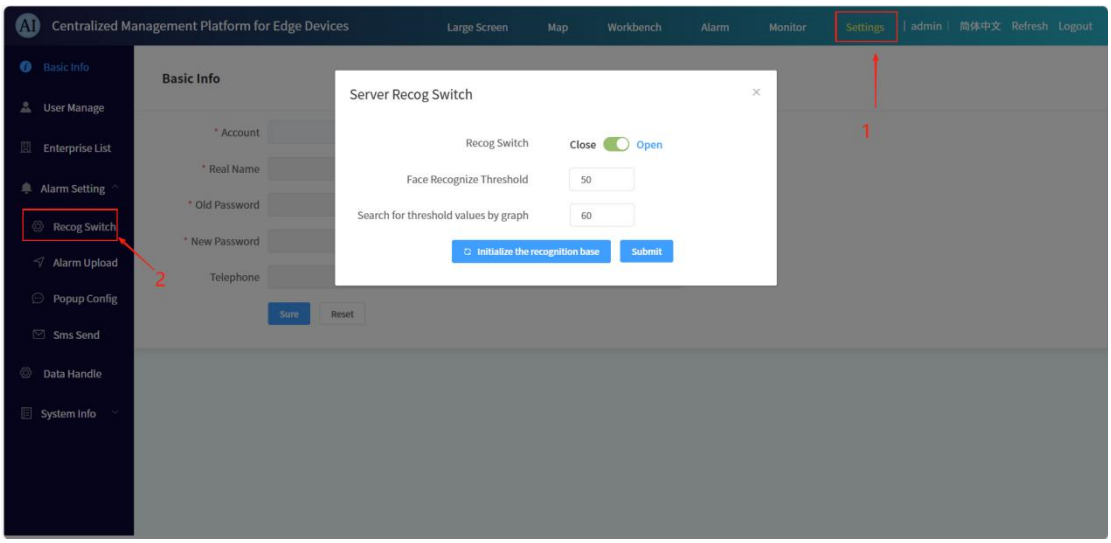


Figure 3-25 Face Recog Switch

Alarm Upload

Configure whether face recognition results are reported as alerts, whether large model analysis results are reported, and the server address for alert reporting.

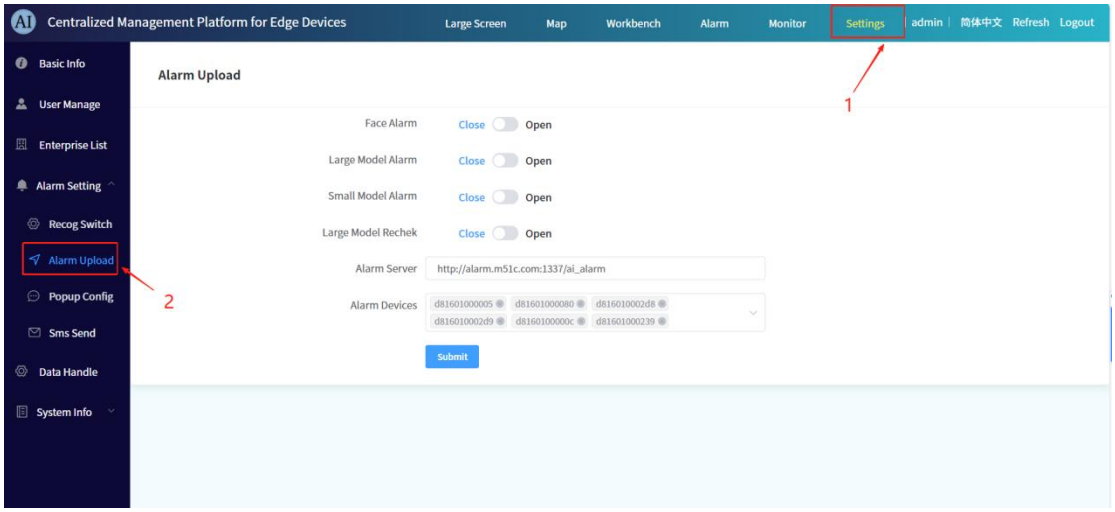


Figure 3-26 Alarm Upload Page

Large Model

This module primarily supports two key functions: Large Model-based Alert Orchestration and Large Model Re-inspection of Alert Information.

1) Large Model-based Alert Orchestration

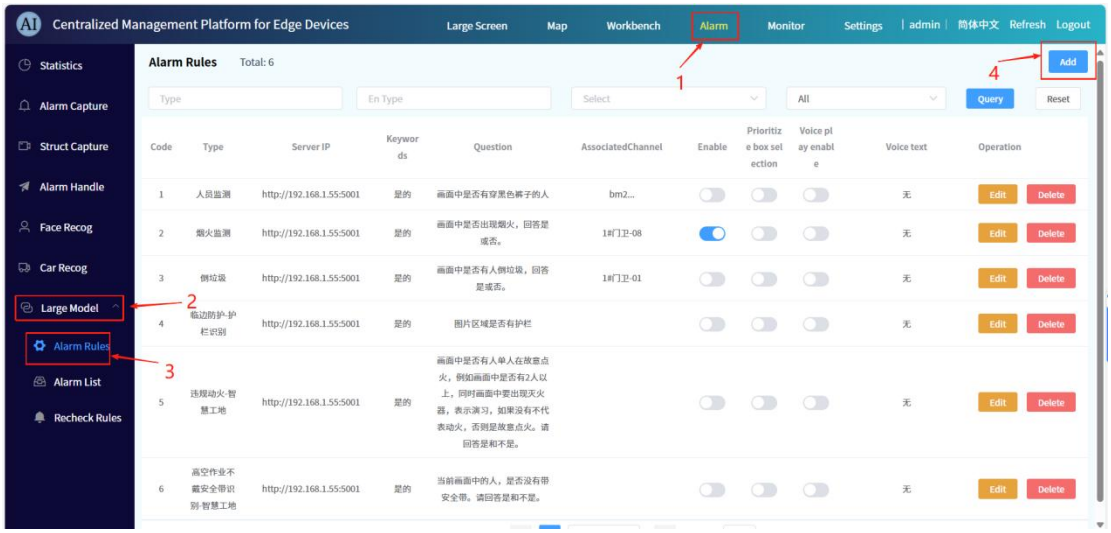


Figure3-27 Large model application module

Add or edit large model queries, and associate them with video channels. The system will use the captured images as input to the large model, which can then trigger a secondary alert based on its analysis.

Parameter settings are as follows:

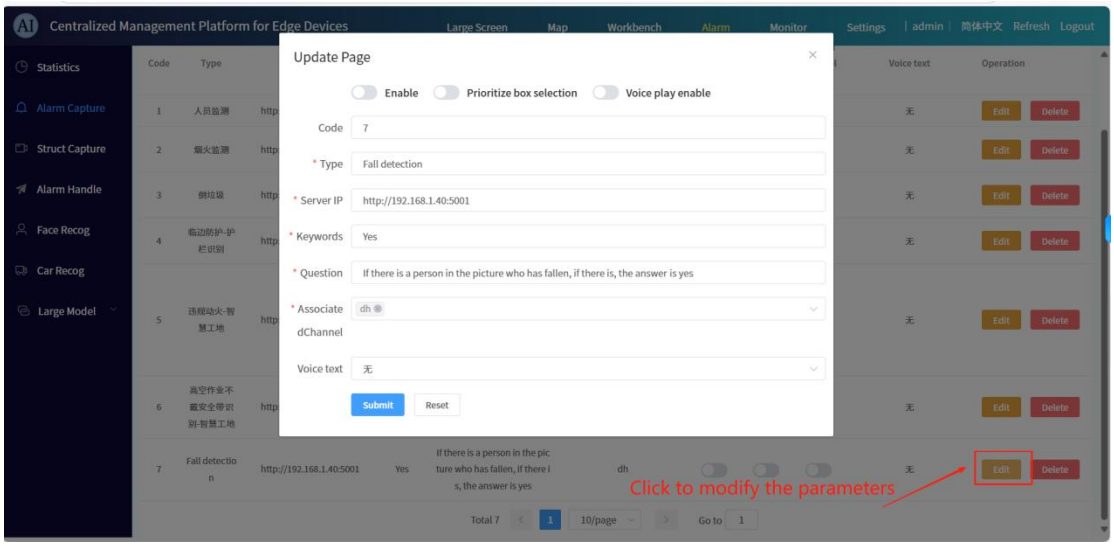


Figure 3-28 Reference Parameters for Large Models

For reference on the type parameters, see Section 3.2, Algorithm Table.

The alert results are shown in the figure below:

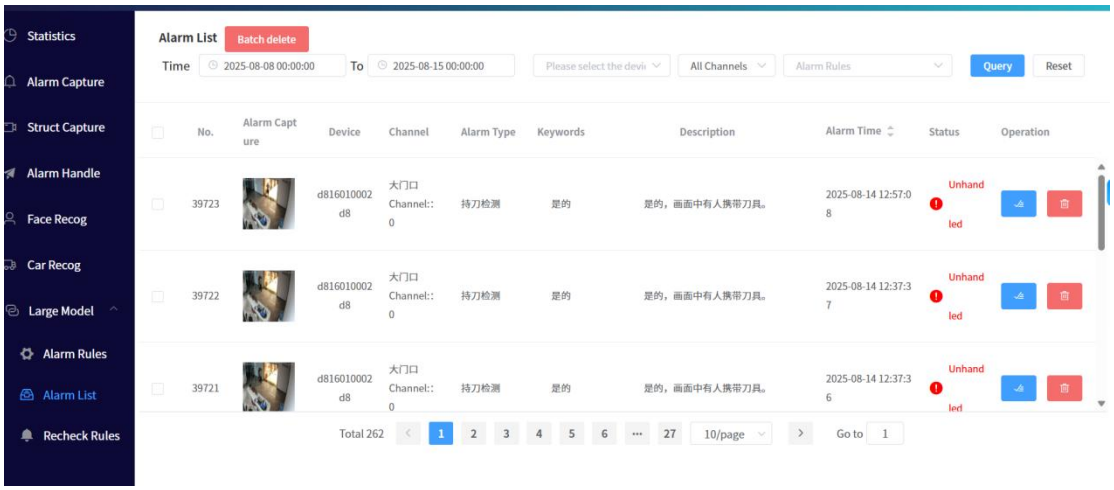


Figure 3-29 Alert List Page

1) Large Model Alert Re-inspection

Since alerts generated by small models may have limited accuracy and contain false positives, performing a secondary review on certain alert data can help filter out incorrect alarms. To enable this function, orchestrate the corresponding query and activate the rule. The configuration module is shown below:

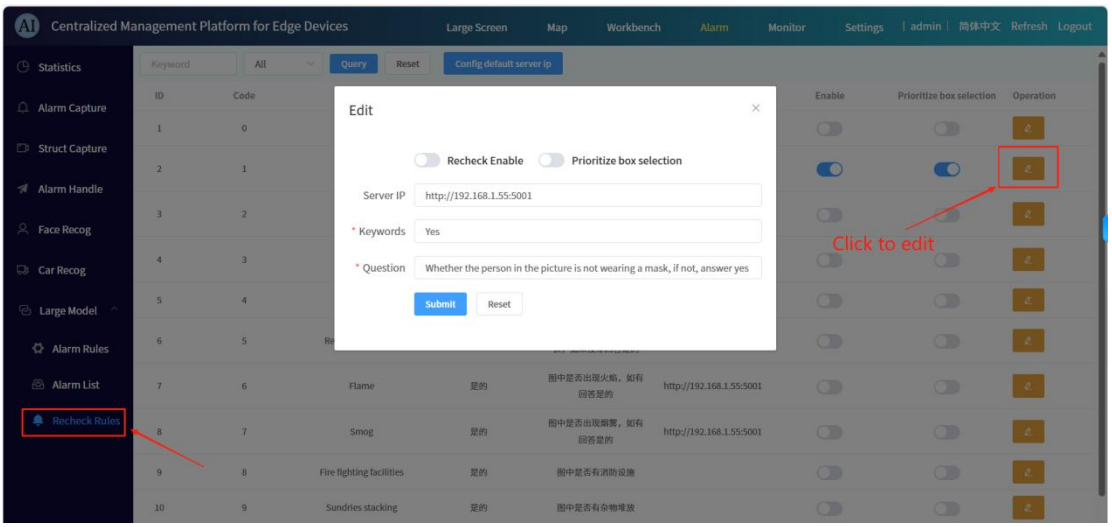


Figure 3-30 Recheck Rules

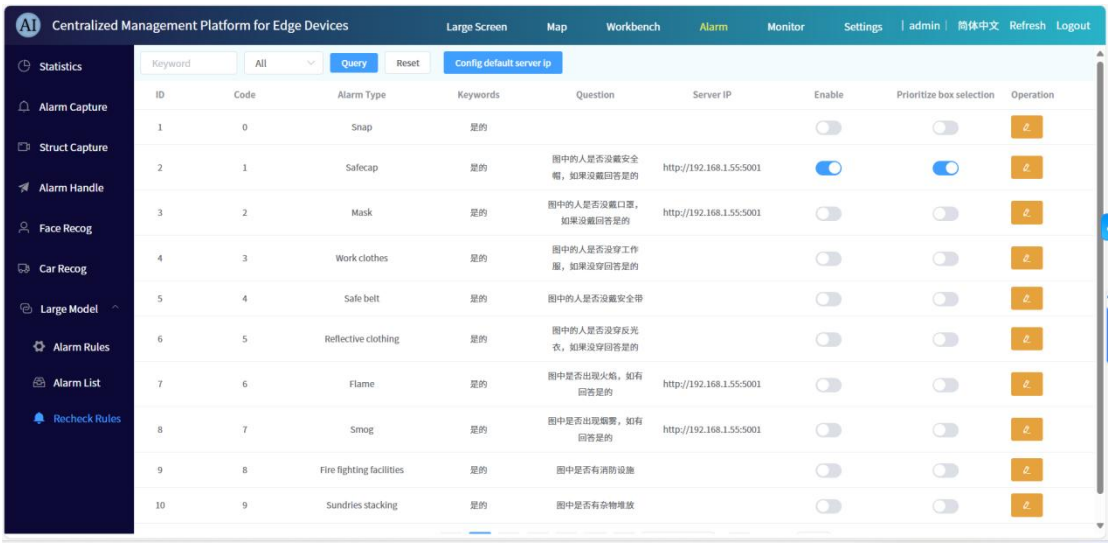


Figure 3-30 Recheck Rules Page

3.3.5 Real-time Monitoring

The Real-time Monitoring module serves as the primary interface for monitoring daily production processes. It enables continuous scene surveillance and supports switching between single-screen and multi-screen display modes. The interface also supports AI-enhanced video streams and allows users to search for alert-triggered recordings and images across all video channels.

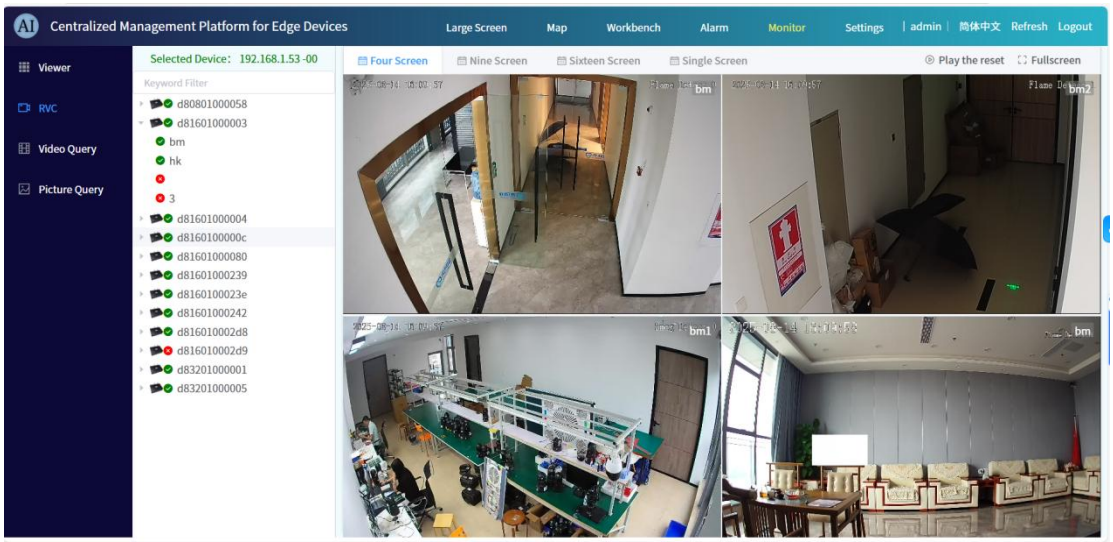


Figure 3-32 RVC Page

3.3.6 System Settings

Basic info Settings

You can change passwords and other information.

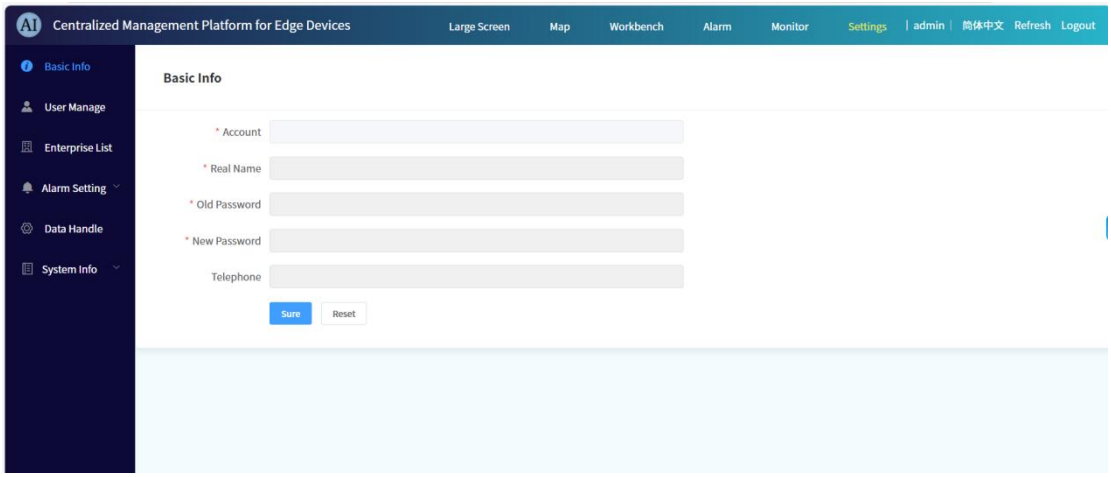


Figure 3-33 Basic info Page

User Manage

Users can be added, removed, granted or modified in terms of permissions, and have their passwords set or reset.

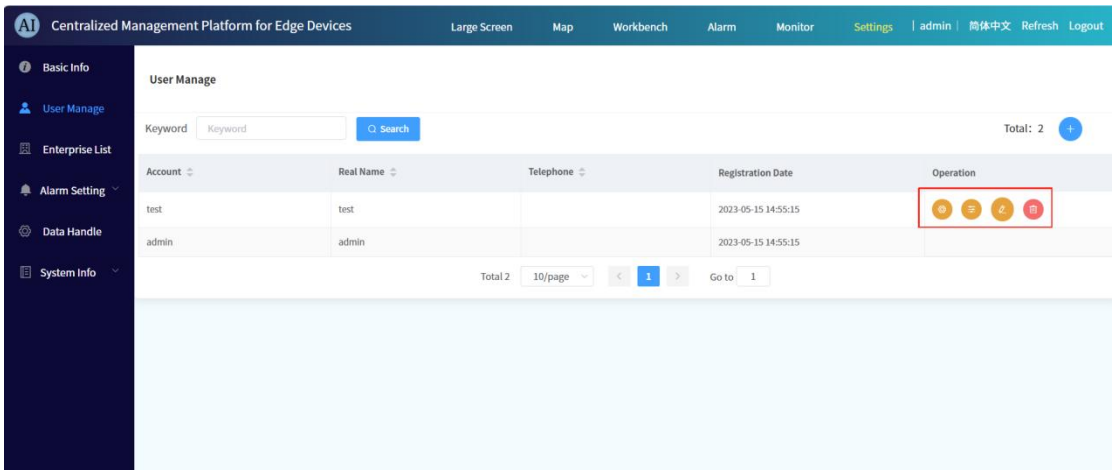


Figure3-34 User Manage Page

Popup Config

Allows users to enable or disable alert, recognition, and capture pop-ups, and configure the pages on which they appear.

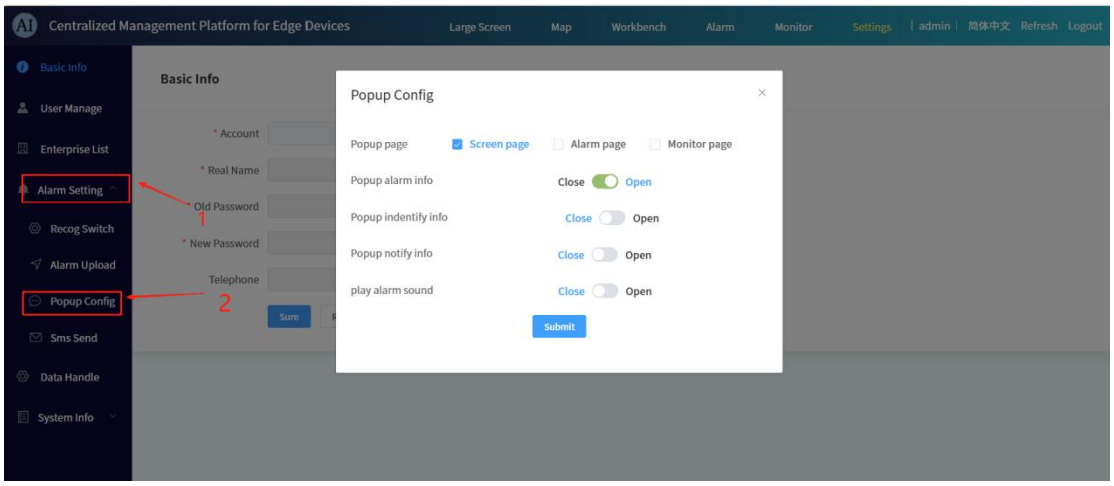


Figure 3-35 Pop-up Toggle Module

Soft Config

The system name and logo can be customized based on actual requirements.

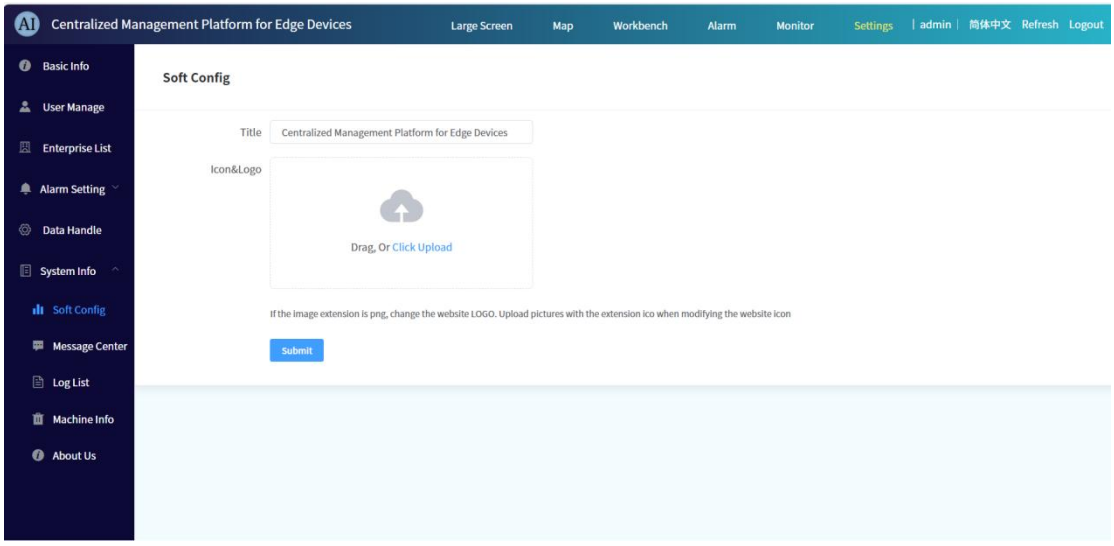


Figure3-36 Soft Config Page

Sync Storage

Provides an option to synchronize image and video data from the computing unit to the management platform, and includes functions to clean up:Uploaded images、Alert-triggered recordings、Raw images、Synchronized files

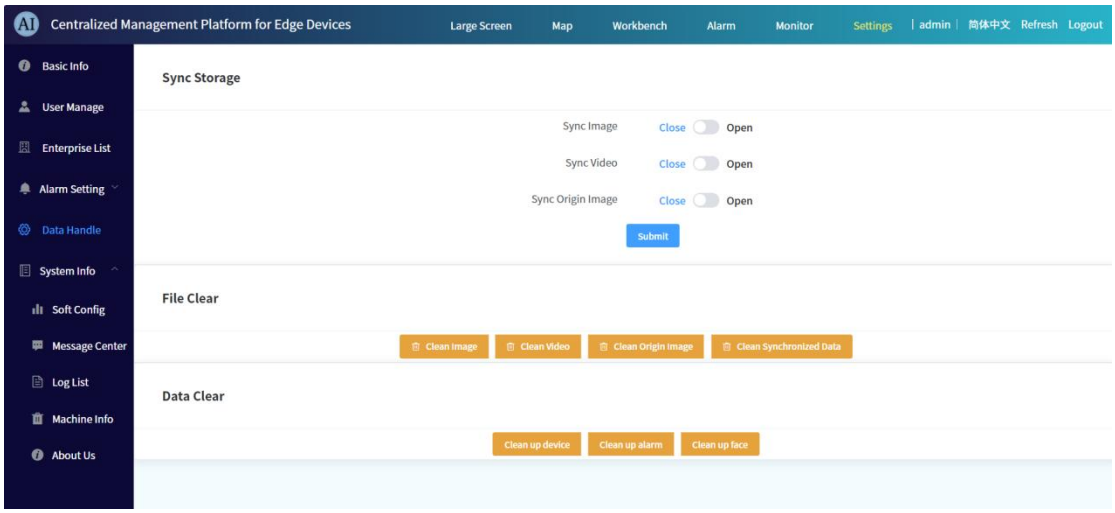


Figure3-37 Sync Storage Page

System Info

The system information module includes software configuration, message center, log list, local information, about and other information.

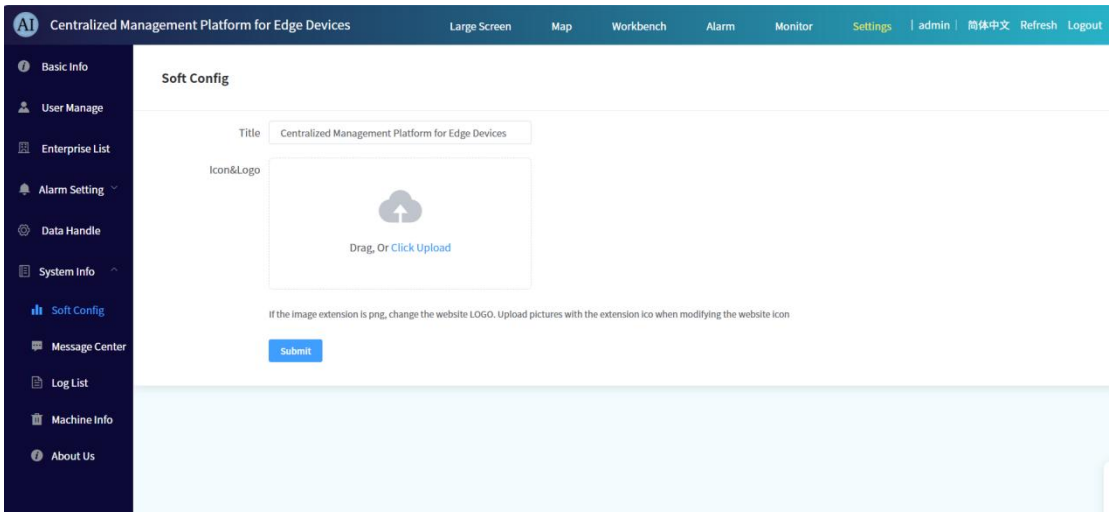


Figure3-38 Soft Config Page

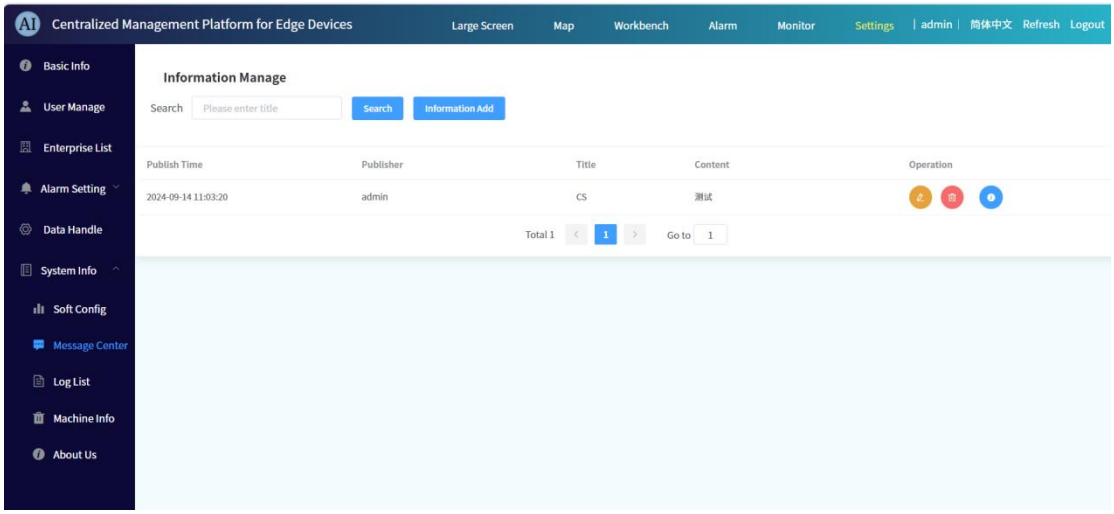


Figure3-39 Message Center Page

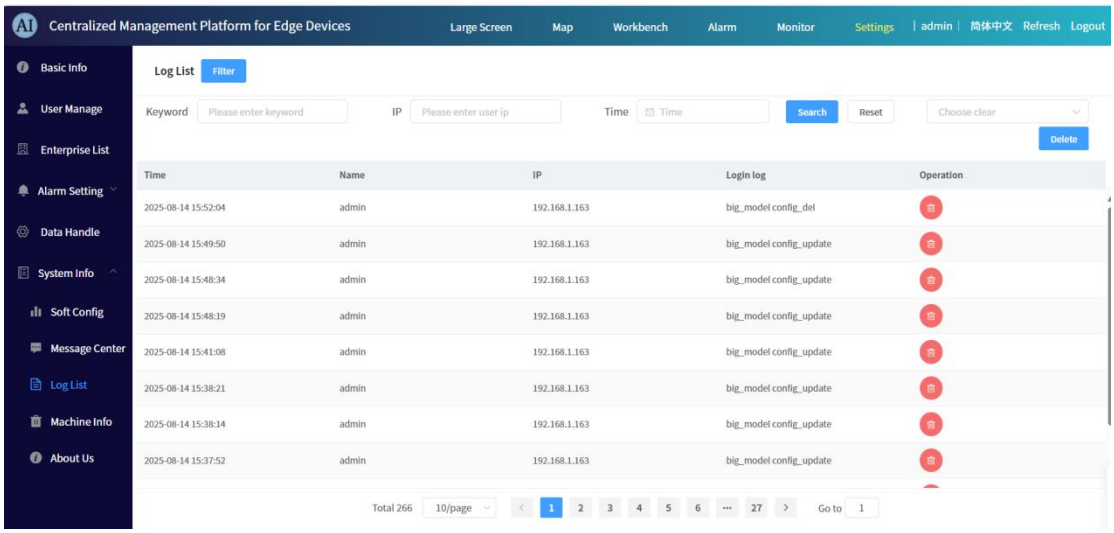


Figure3-40 Log List Page

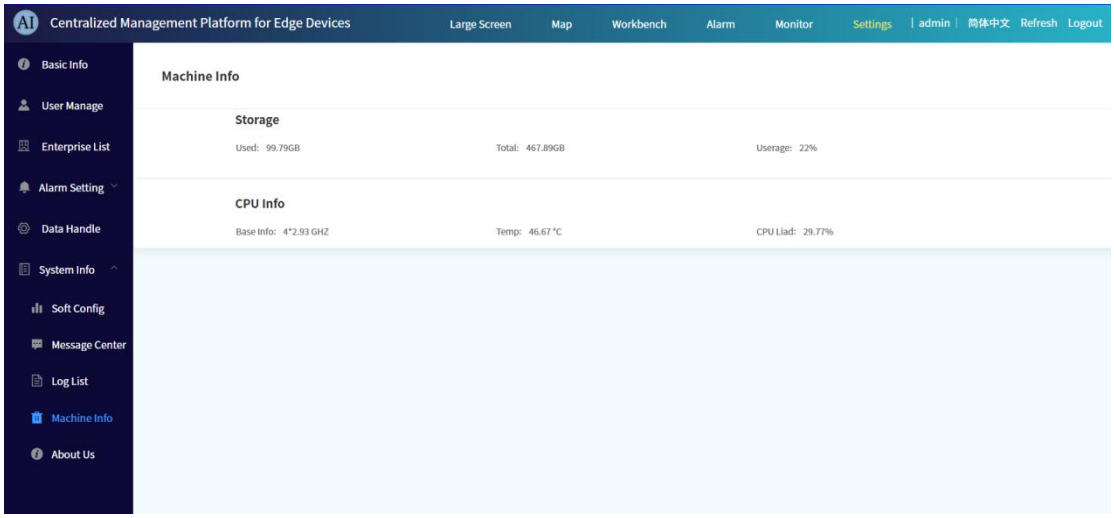


Figure3-41 Machine Info Page

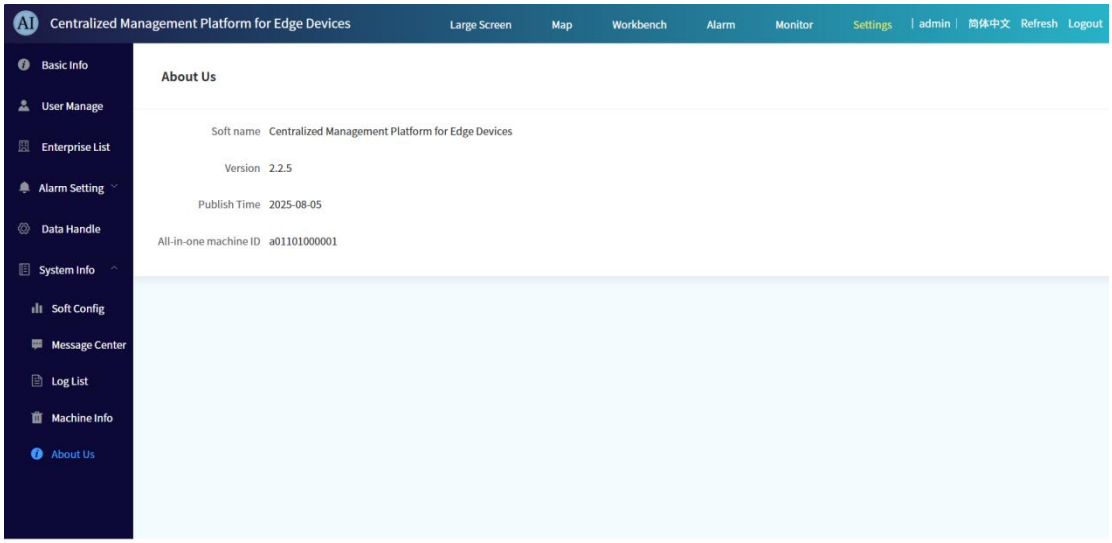


Figure3-42 About Us

4 AI Edge Computing Server Unit Detailed Setup Instructions

4.1 Basic Function Description

The edge computing unit is a relatively independent and self-contained management system, integrating video access, AI snapshot capture, and alarm detection in one. Its functions include: support for up to 16 channels of 1080P video input, video decoding, AI analysis, alarm-triggered snapshot capture, face recognition, license plate recognition, and video encoding storage.

4.2 Small-model algorithms have been implemented.

AI algorithms have been implemented as listed below. More algorithms can be customized upon request. The currently implemented algorithms are as follows:

Table 3-1 AI Algorithm Implementation List

id	Alarm Type Name	Algorithm Type ID	Algorithm Type Name
1	Not Wearing Safety Helmet Alarm	3	Personnel Violation
2	Not Wearing Face Mask Alarm	3	Personnel Violation
3	Not Wearing Work Uniform Alarm	3	Personnel Violation
4	Not Wearing Seatbelt Alarm	3	Personnel Violation
5	Not Wearing Reflective Vest Alarm	3	Personnel Violation
6	Flame Detection Alarm	3	Environmental

			Anomaly
7	Smoke Detection Alarm	3	Environmental Anomaly
8	Fire Safety Equipment Detection	3	Environmental Anomaly
9	Clutter Piling	4	Environmental Anomaly
10	Vehicle No-Parking Violation	5	Perimeter Monitoring
11	Vehicle Departure	5	Perimeter Monitoring
12	Personnel Loitering	5	Perimeter Monitoring
13	Wall Climbing Detection	5	Perimeter Monitoring
14	Intrusion Alarm	5	Perimeter Monitoring
15	Boundary Crossing	5	Perimeter Monitoring
16	Fall Detection	6	Behavioral Alert
17	Smoking Detection	6	Behavioral Alert
18	Phone Call Detection	6	Behavioral Alert
19	Mobile Phone Usage Detection	6	Behavioral Alert
20	Personnel Running	6	Behavioral Alert
21	Sleeping on Duty Detection	6	Behavioral Alert
22	Leaving Post Detection	6	Behavioral Alert
23	Crowd Gathering Detection	6	Behavioral Alert
24	Fighting Detection	6	Behavioral Alert
25	Face Detection	2	Full Structured Analysis
26	Human Shape Detection	2	Full Structured Analysis
27	Motor Vehicle Detection	2	Full Structured Analysis
28	Non-Motor Vehicle Detection	2	Full Structured Analysis
29	License Plate Detection	2	Full Structured Analysis
30	Face Recognition Comparison	1	Face-Human Binding and Recognition
31	License Plate Recognition Comparison	1	Face-Human Binding and Recognition
32	Overcrowding	5	Perimeter Monitoring
33	Understaffed	5	Perimeter Monitoring
34	Personnel Departure	5	Perimeter Monitoring
35	Non-Motor Vehicle No-Parking Violation	5	Perimeter Monitoring
36	Non-Motor Vehicle Departure	5	Perimeter Monitoring
37	Rider Not Wearing Helmet	3	Personnel Violation
38	Motor Vehicle Count Exceeded	5	Perimeter Monitoring
39	Motor Vehicle Count Below Minimum	5	Perimeter Monitoring
40	Hazardous Materials Vehicle Entry Prohibited	5	Perimeter Monitoring

41	Motorcycle Entering Gas Station	3	Personnel Violation
42	Unstandardized Oil Unloading Process	5	Perimeter Monitoring
43	Signage Recognition	5	Perimeter Monitoring
44	Personnel Lingering	6	Behavioral Alert
45	Hand-Raising for Help	6	Behavioral Alert
46	Face Recognition Alarm	1	Face-Human Binding and Recognition
47	Camera Obstruction	3	Environmental Anomaly
48	Camera Displacement	3	Environmental Anomaly
49	Leak and Spill Detection	3	Environmental Anomaly
50	Fatigue Driving Detection	6	Behavioral Alert

4.3 Camera Access Configuration

4.3.1 Camera Channel Setup

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

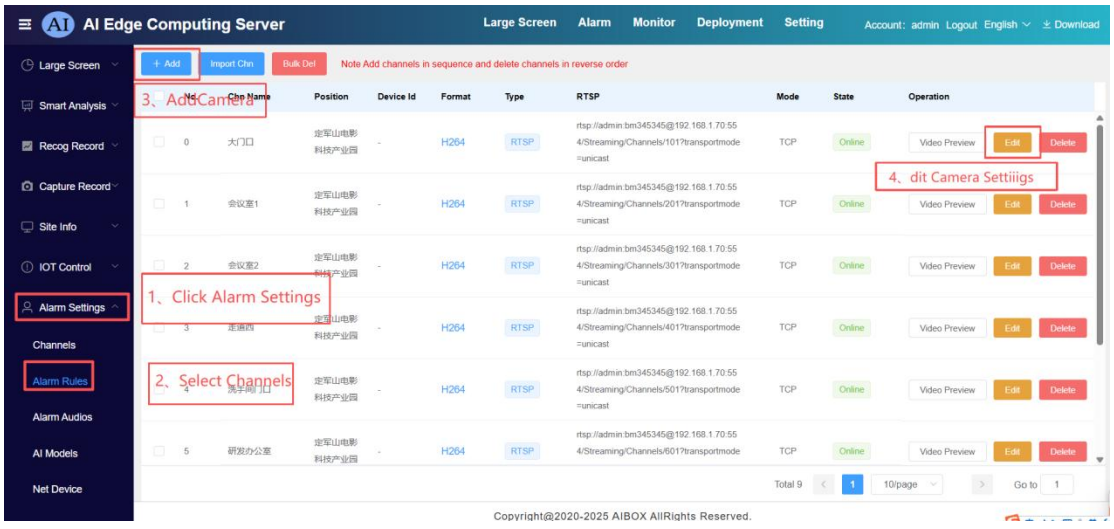


Figure 4-1 Camera Channel Setup Steps

Important Notes：：The edge-side supervision device supports cameras 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 may cause AI recognition issues.

4.3.2 Special Instructions for Camera Integration

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.

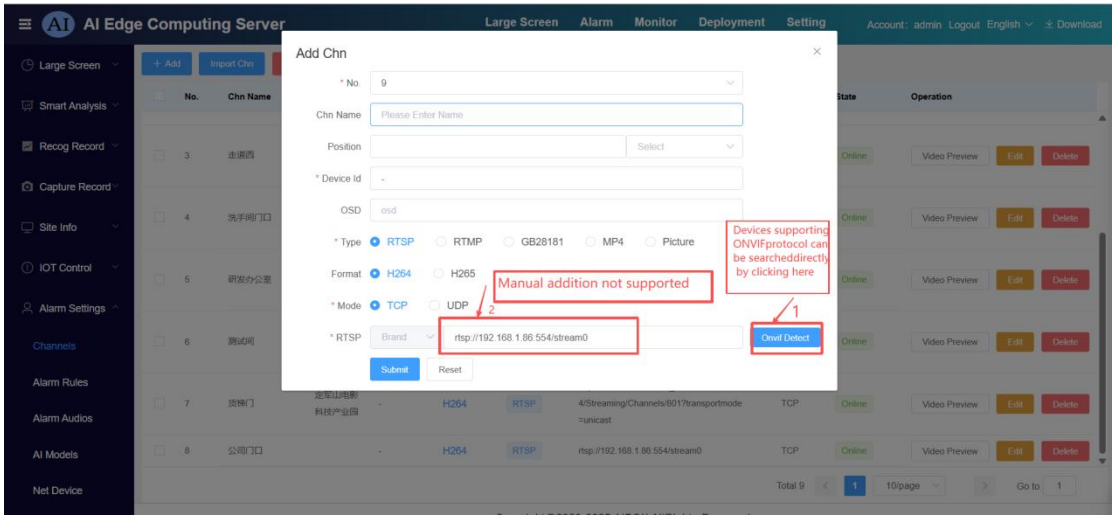


Figure 4-2 Edit Channel Settings Page

If multiple cameras need to be connected, you can use the 4gcms software provided by our company to verify the RTSP addresses of the cameras. During this process, please note that identifiers starting with "d8" represent the AI box, while those starting with "c8" represent the camera ID.

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. If issues occur when using H.265, perform operations on the video preview interface to resolve them.

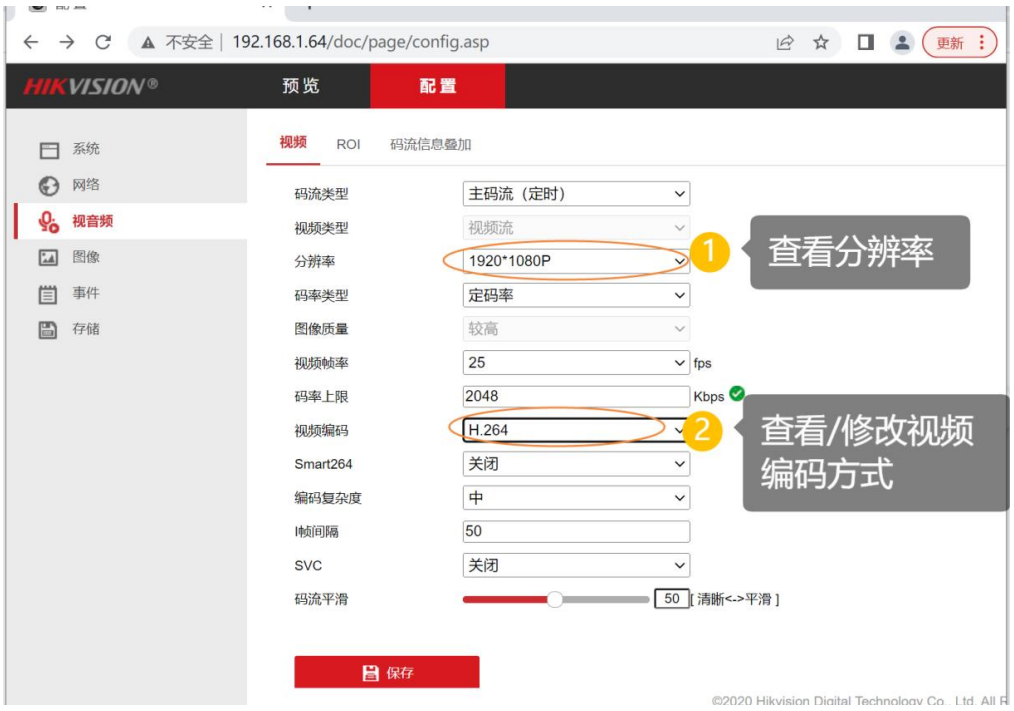


Figure 4-3 Hikvision Camera Encoding Settings Page

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

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

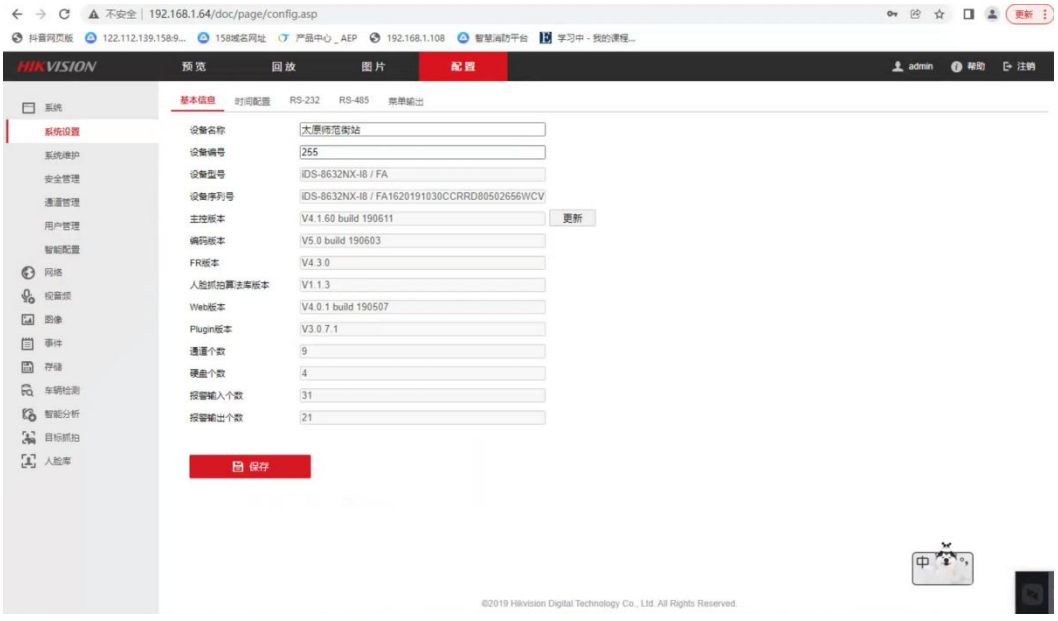


Figure 4-4 Hikvision NVR System Settings Page

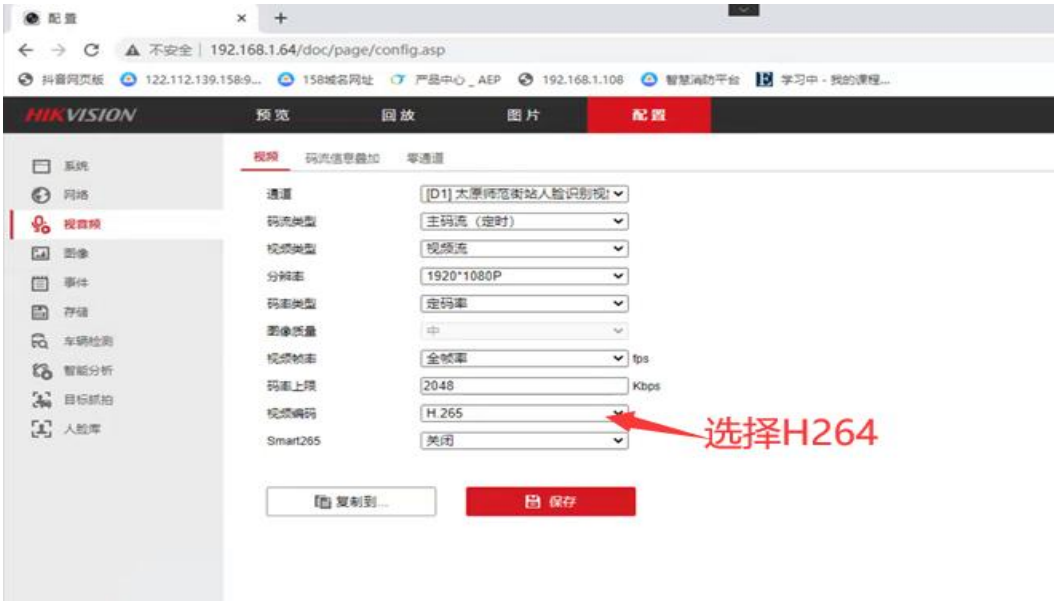


Figure 4-5 Video Encoding Viewing and Modification Page

Hikvision RTSP streaming URL example:

rtsp://admin:ty080910@192.168.1.88:554/Streaming/Channels/701?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).

For Dahua cameras connecting to the Edge-Side Supervision Device

he RTSP format for Dahua cameras is as follows:

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

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

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

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

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.

RTMP Video Access

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

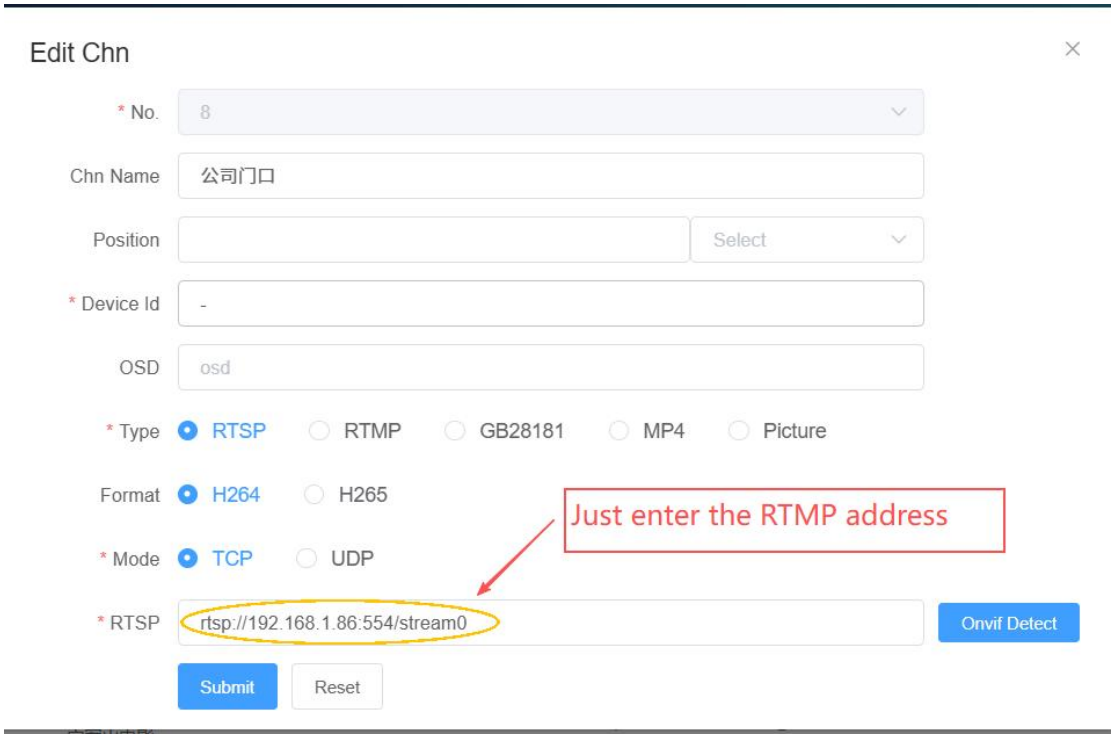


Figure 4-6 Location to Enter RTMP Address

Note: When adding RTSP/RTMP URLs in the device's channel interface, please use “VLC media player” to verify whether the RTSP/RTMP video stream can be successfully accessed. Ensure that the IP address, username, and password are all correct before adding the stream to the web channel interface of this product.

4.4 Edge Computing Unit Surveillance Setup

Configuration Steps: Left sidebar—Alarm Settings—Alarm Rules, as shown in the figure below: edit the alarm rules for the channel.

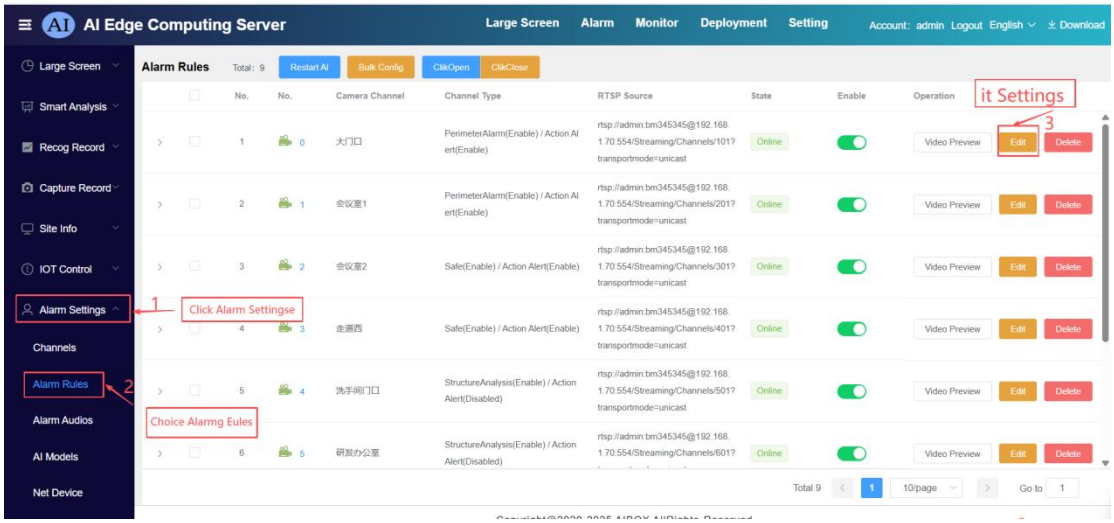


Figure 4-7 Alarm Rules Page

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.

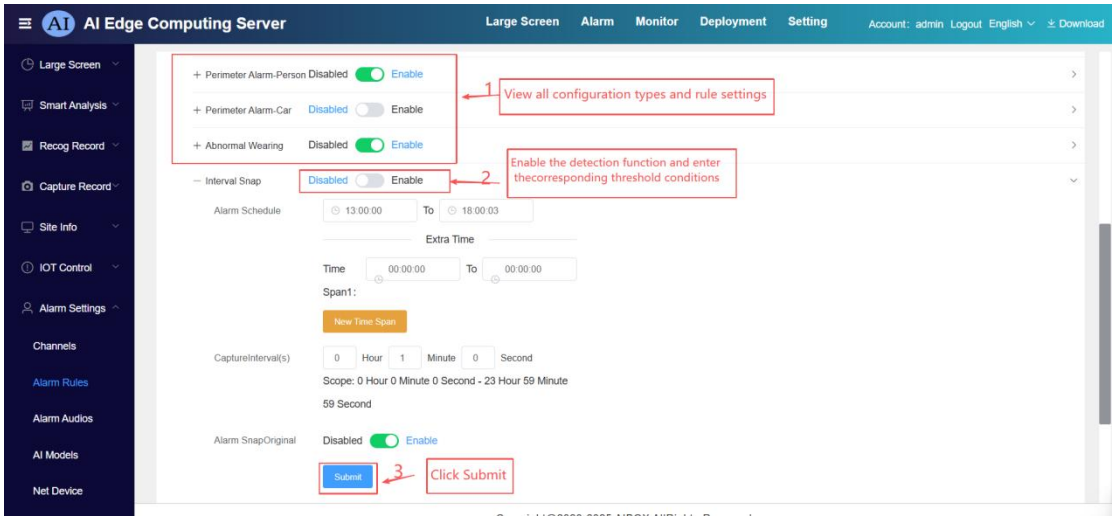


Figure 4-8 Alarm Rules Edit Page

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.

4.4.1 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.

4.4.2 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:

Configuration Steps: Left Sidebar — System — Status — Restart AI.

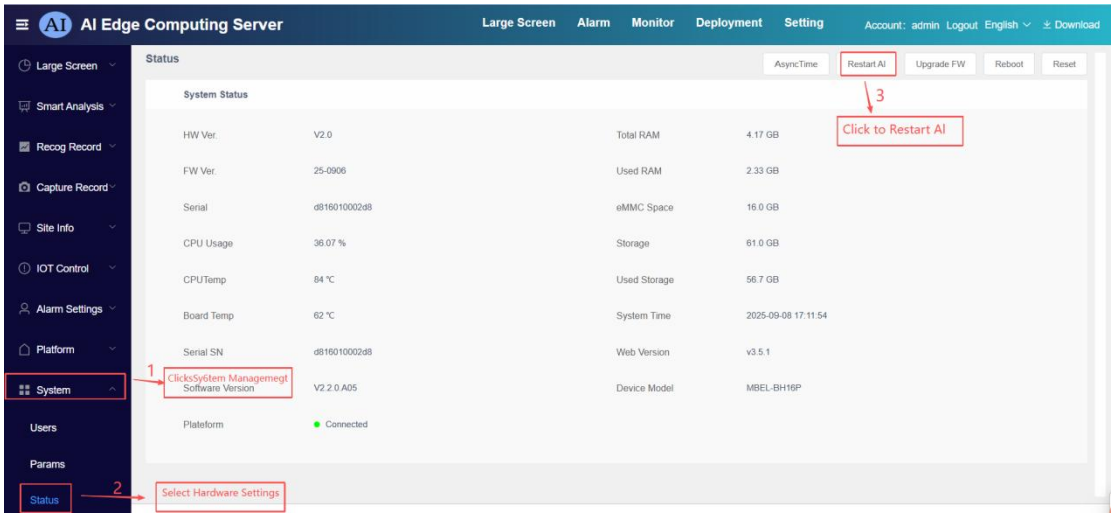


Figure 4-9 Guidance on Restart Procedure

4.4.3 Special Notes on Smoke and Flame Detection

The impact of ambient light on smoke and flame detection is unavoidable in certain scenarios. Configuring additional dynamic detection parameters can effectively reduce the false alarm rate. This becomes particularly critical when severe lighting interference is present in real-world applications.

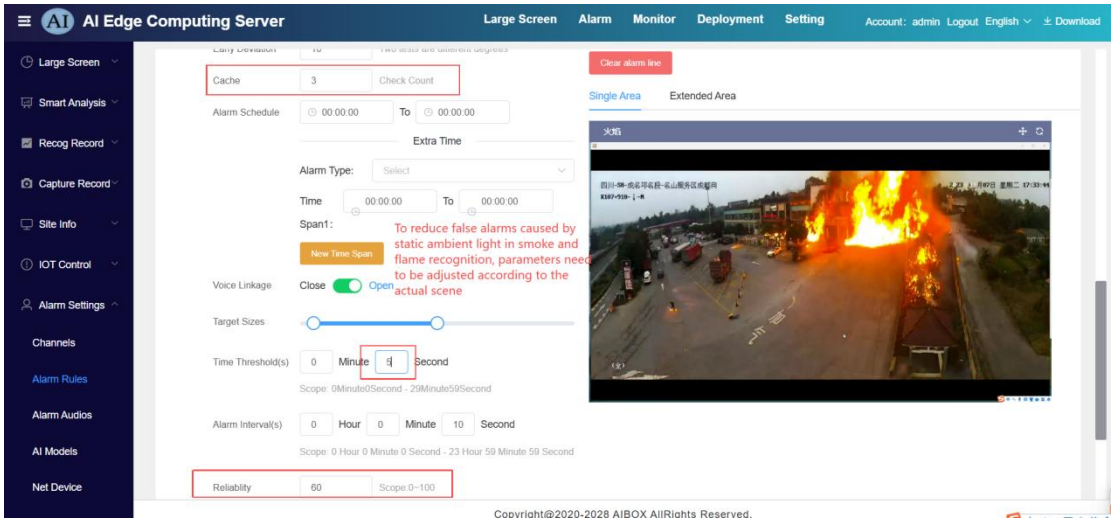


Figure 4-10 Flame Alarm Setting Instructions

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.

4.5 Introduction to the Edge Computing Unit System Function Menu

4.5.1 Intelligent Statistical Analysis Dashboard Interface

To meet the visualization requirements for statistical analysis in small and medium-sized projects, a data statistics dashboard display function has been specially developed. The dashboard interface is primarily designed for supervisors to monitor operations in real time, filter and display valid alarm information, and summarize alarm types for efficient oversight and decision-making.

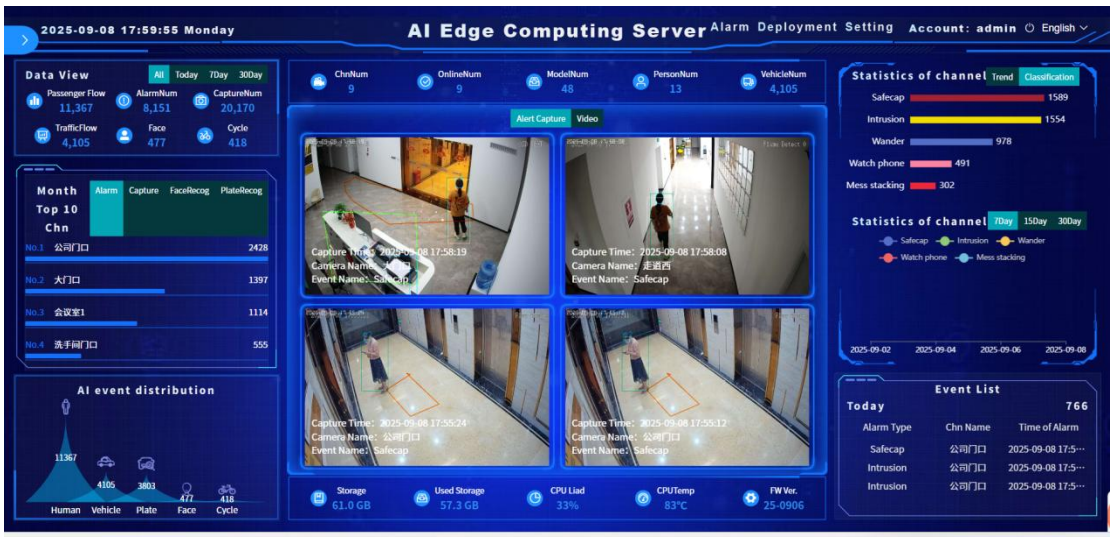


Figure 4-11 Intelligent Statistical Analysis Dashboard Interface

The header section of the dashboard displays, on the left, the time, date, and day of the week; in the center is the system title; and on the right are interactive shortcut buttons. Next to the username is the "Log Out" button, and at the far right is a dropdown box for language switching. Regarding theshortcuts: clicking Alarm one redirects to the alert snapshot page, clicking Deployment another goes to the surveillance setup page, and clicking the Setting navigates to the system parameter settings page.

The dashboard displays statistical data, divided into seven sections in total.

1. Data View

Data View: This section shows the number of channels (the number of added channels on the edge monitoring device), online count (the number of online channels among added ones), model count (the number of alarm types), personnel database (the number of personnel records), vehicle database (the number of vehicle records), pedestrian flow (the number of face recognitions), alarm count (the total number of all alarm types), and snapshot count (the number of snapshots including faces, human figures, motor vehicles, non-motor vehicles, and license plates).

2. Top 10 Channels by Alarm Count This Month

This section displays the top 10 channels with the highest number of alarms in the current month, showing the proportion and total count of alarm-triggering channels in a progress bar format. By default, the top 10 channels by total alarms are displayed. Users can click to All Today 7Day 30Day select and view the top 10 channels for different alarm types.

3. AI Event Distribution

This section displays the distribution of AI event types, including human body, face, motor vehicle, non-motor vehicle, and license plate. Clicking on a field with a non-zero count allows users to view detailed snapshot information.

4. Alert Snapshots / Video

The alert snapshot section displays the four most recent alert images. Each image shows, in the lower-left corner, data such as the event name, surveillance name, and capture time. Clicking an image opens a detailed view: the left side shows the captured image and a 20-second video clip (before and after the capture), while the right side displays detailed event information. In the video section, users can select video channels to display, and perform operations such as stretching, recording, snapshot capture, and full-screen playback.

5. System Status Bar

This section displays the system's total and used storage space, CPU utilization, CPU temperature, and firmware version.

6. Alarm Trend Analysis

This includes two parts: trend analysis and type distribution. The trend graph (line chart) and alarm type distribution (pie chart) default to showing today's data. Users can 

select different time ranges. Hovering over the pie chart displays the count for that category; hovering over a point on the line chart shows the count at that time. The details section shows bar and line charts for alarm classification statistics, defaulting to a 7-day view,can click to 

select data within the time range for viewing.

7. Event List

This section displays the distribution of AI event types, including human body, face, motor vehicle, non-motor vehicle, and license plate. Clicking on a field with a non-zero count allows users to view detailed snapshot information.

4.5.2 Main Menu Bar

Click the floating icon in the upper-left corner to open the side main menu bar; click again to hide it. Clicking an item in the menu navigates to the corresponding page. At this point, the floating icon is hidden and the main menu remains displayed on the left. To return to the dashboard page, simply click the dashboard menu item.

Figure 4-12 Dashboard Interface Showing the Main Menu Bar

4.5.3 Intelligent Analysis

This option includes: Real-time Video and AI Video.

Real-time Video: Displays the live video stream directly from the cameras.

AI Video: Shows the camera's preset virtual fence (electronic perimeter), where detection results from the configured AI algorithms (such as intrusion, behavior analysis, etc.) are overlaid and displayed on the video feed.

Real-time Video

The upper-middle-left area of the interface includes the following:

（1）Preview Channel Selection Area: Checkboxes to select which camera channels to preview.

（2）Split-screen Control Area: Allows setting the number of viewing panes—1, 4, 9, or 16—for multi-channel monitoring

（3）Full-screen Icon: Click to expand the current preview to full screen.

（4）Video Analysis Mode Selection Area: Choose from the following analysis modes: ① Face-Person Binding and Recognition .② Full Structural Analysis .③ Alert Snapshot Capture

（5）Alarm Log Display Area: Click to view detailed information for a specific alarm. Click "View Large Image" to enlarge the alarm snapshot, and watch the 15-second video clip before and after the alarm event.

（6）Note: The real-time video is decoded by the computer’s browser. If the computer’s hardware configuration is insufficient, the video may lag or fail to load. This is not due to

the edge computing device (the "box") itself.

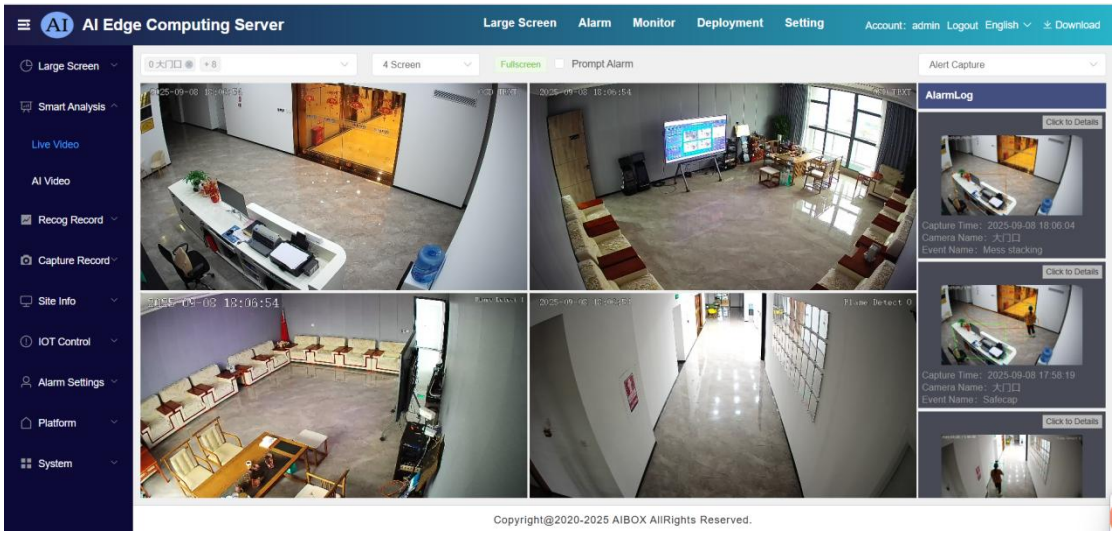


Figure 4-13 Real-time Video Page

Note：Some operations on the Configuration Management page require technical expertise. It is recommended to perform these tasks under the guidance of the manufacturer's technical personnel!

AI Video

The "AI Video" interface is consistent with the "Real-time Video" interface. However, on the AI video channel view, additional information related to the AI algorithms (such as detection results, alarm types, and recognition data) will be overlaid and displayed. Users can click the Monitor button in the page header to quickly navigate to the AI Video page.

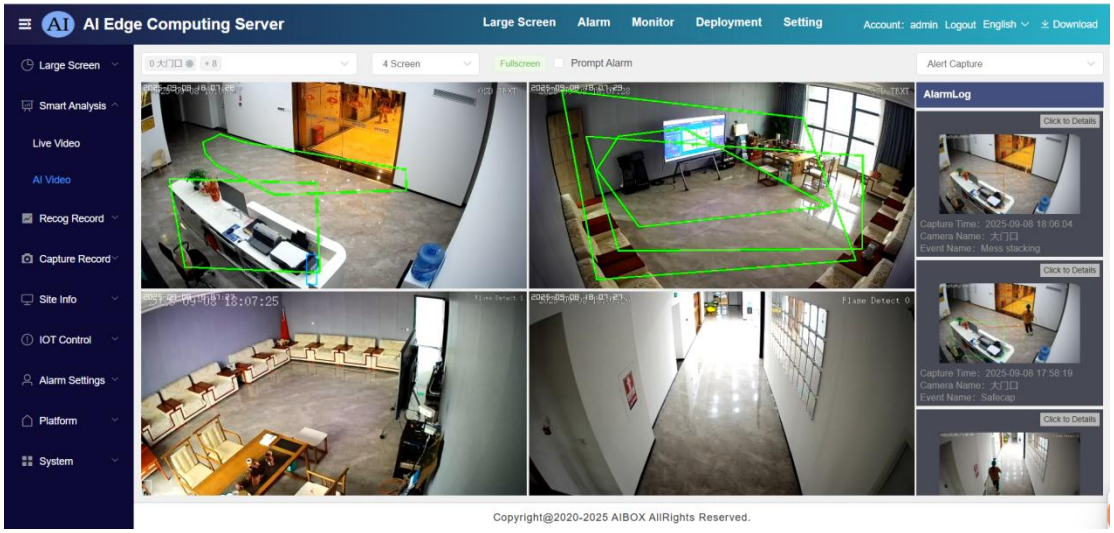


Figure 4-14 AI Video Display

Note：: AI video is primarily used to display the results of AI processing. Frame

sampling and reduced frame rate are applied to optimize performance, so occasional choppiness or lag is normal and expected.

4.5.4 Recognition Records

The system automatically categorizes recognition records into: Face Recognition and Vehicle Recognition.

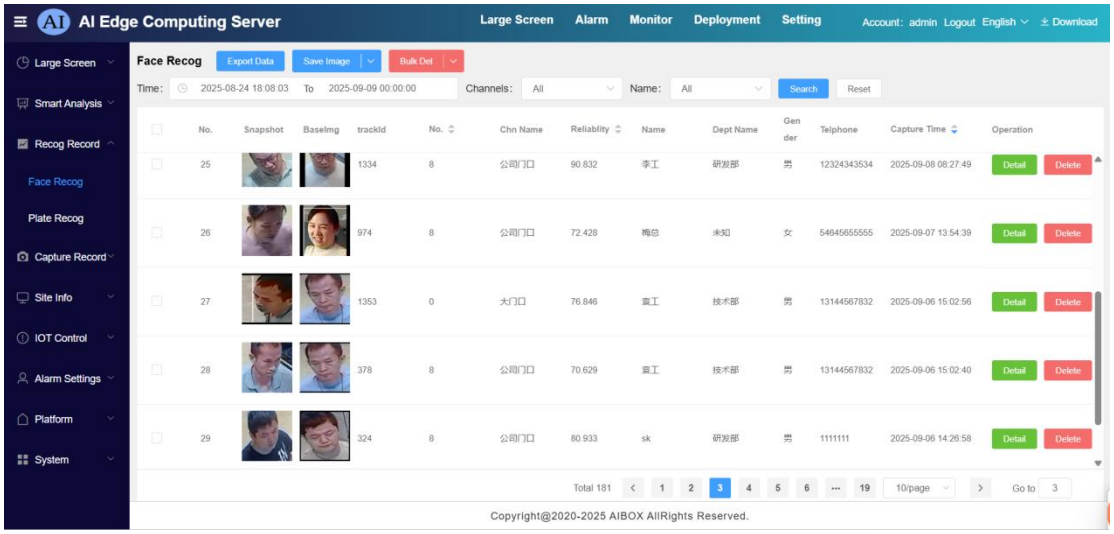


Figure 4-15 Face Recognition Page

Face Recog

Detected face information is displayed on this page. At the top of the interface, functional options such as "Export Data", "Save Images", "Batch Delete", "Time", "Channel", and "Name" are provided, allowing users to further process and manage the recognition results. Additionally, face recognition records can be searched and filtered by criteria including time period, alert channel, and personnel database, enabling efficient data retrieval and analysis.

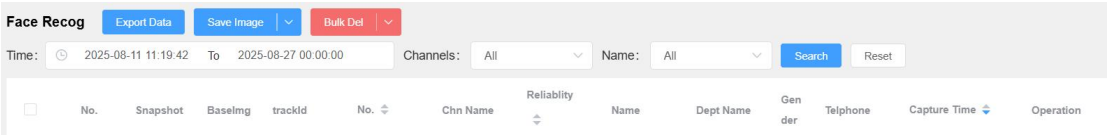


Figure 4-16 Face Recognition Information Panel Interface

To export data from face recognition or vehicle recognition, click the "Export Data"button to open the export dialog. In the dialog box, you can select the export scope and export fields.

The export items include exporting the current page, exporting selected items, or exporting all data.Exporting the current page means exporting the data displayed on the current page, with the number of records varying according to the user's settings; the default

options for records per page are 10, 20, 50, 100, or 200 per page.

Exporting selected items refers to exporting the data selected by the user, allowing cross-page selection.

Exporting all will export all recognition data. Export fields are all selected by default, but users can choose specific fields they want to export. After selecting the export items and fields, click the "Export Data to Excel" button to export the data into an Excel file and download it.

The "Save Images" button allows downloading the selected data or all data, with the downloaded format being a compressed .zip file. Hovering the mouse over the dropdown icon to the right of the save button reveals save options: "Export Selected" and "Export All," with the number following the dropdown indicating the quantity to be exported.

The "Batch Delete" button works similarly: it allows deleting selected or all data — please proceed with caution. After clicking the delete option, the system will prompt the user to confirm the deletion, and the data will be deleted only after confirmation.

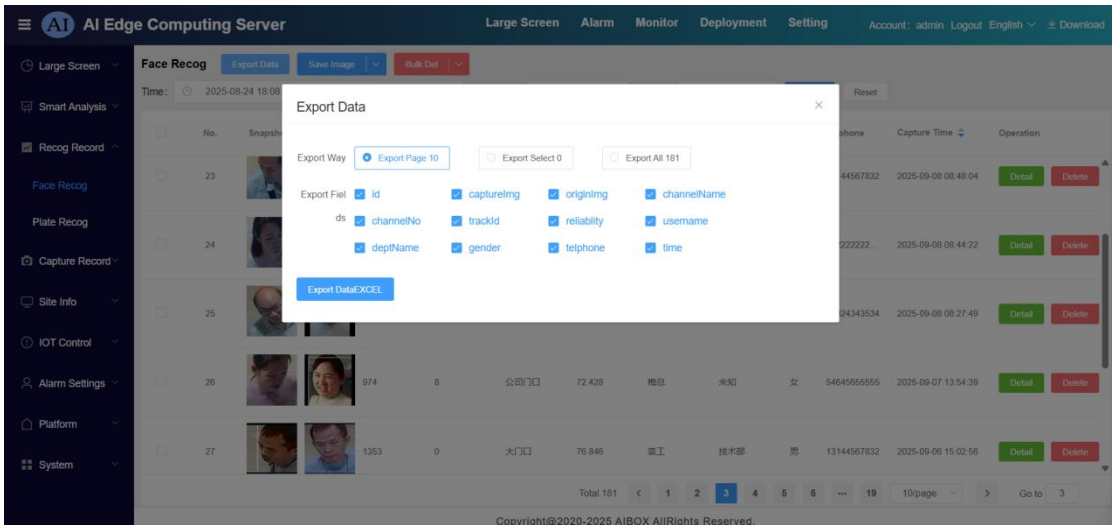


Figure 4-17 Face Image Export Page

Vehicle Recognition

Detected vehicle information is displayed here, and the specific functional options are the same as those described for face recognition.

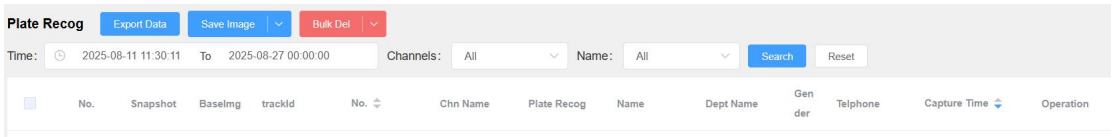


Figure 4-18 Vehicle Recognition Information Panel Interface

4.5.5 Snapshot Records

Snapshot records are divided into: Structured Snapshots, Alert Snapshots, and Video Playback.

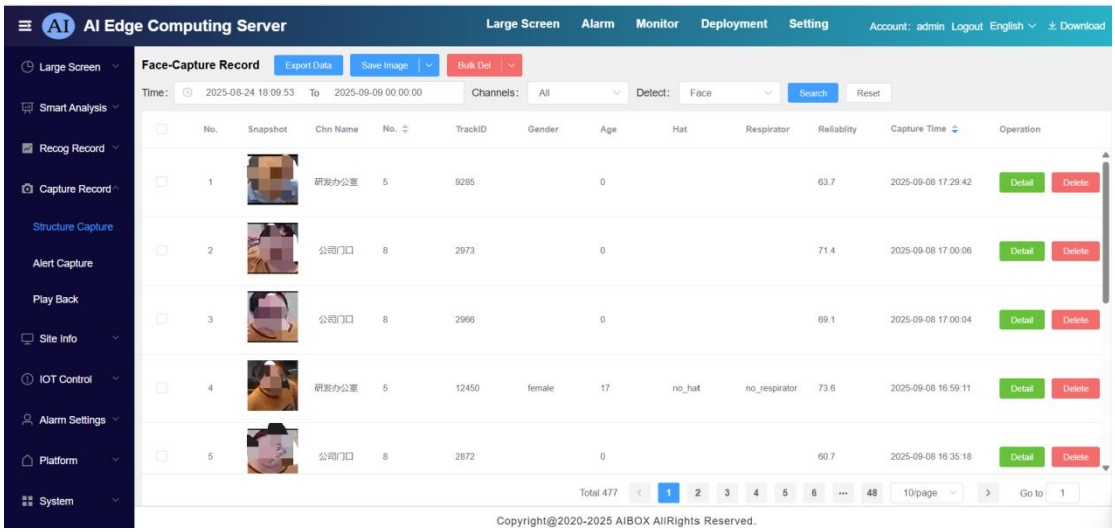


Figure 4-19 Snapshot Records Page

Structured Snapshot Records

Displays AI recognition information captured according to the configured surveillance strategies. The functional area at the top allows filtering by specific channel, date, and time period. Users can click to view the details of each alarm record or delete it.

Alert Snapshots

Captures and stores snapshots for perimeter intrusions (e.g., person, vehicle) and personnel violations, displaying AI recognition information. The top functional area enables search by channel, date, and time range. Users can click to view detailed alarm information or delete records. As shown in the figure, alarm types can be filtered for easier navigation.

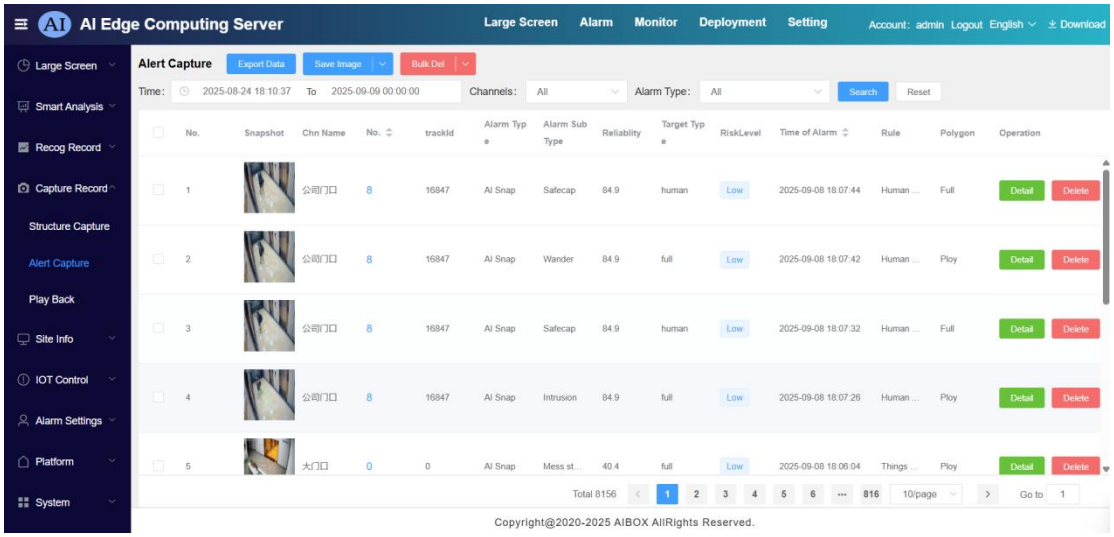


Figure 4-20 Alert Snapshot Filtering Settings

Video Playback

Allows playback of video and images from the selected channel. The functional area at the top enables searching by specific date and time period.

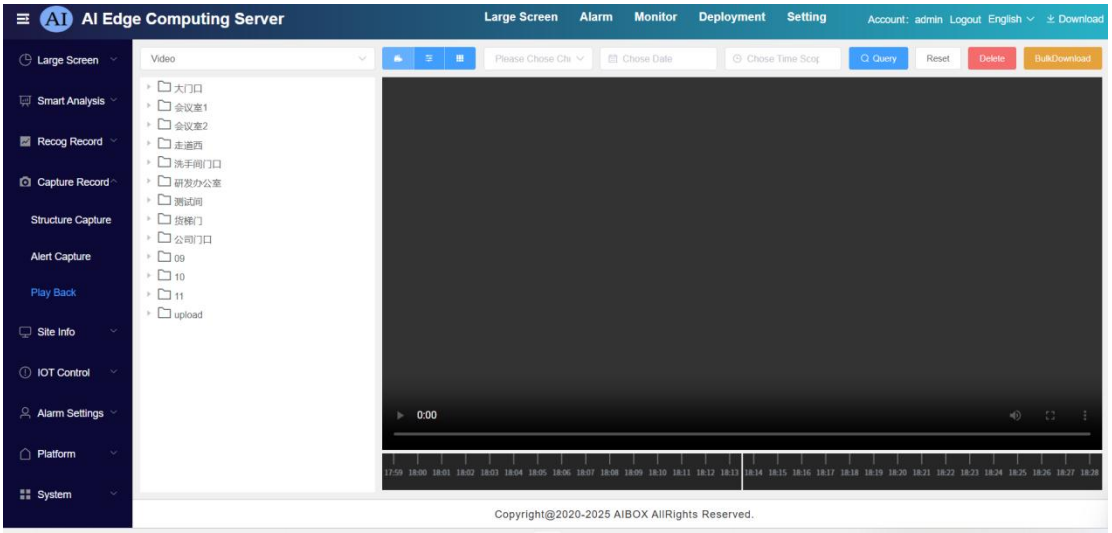


Figure 4-21 Video Playback Page

The content area on the left displays a directory tree of saved channels. The dropdown list at the top allows users to choose between viewing videos or images, with videos being the default option.

If a channel has a name, it will be displayed as the channel name; otherwise, it will be shown as a numeric identifier.

To view data from a specific channel, click on the channel. Clicking on a channel reveals a second-level directory, which consists of dates. Users can select a date to view the corresponding day's data.The third-level directory is composed of both the date and time. Clicking on a directory that combines date and time will display the list of video data.

Video data filenames are structured as Year+Month+Day+Hour+Minute+Second_

VideoSeconds. Clicking on a video filename and then pressing the play button in the video playback area will start the video.When clicking on items in the left-hand directory tree, the search criteria will update accordingly to reflect the selected channel and time period.

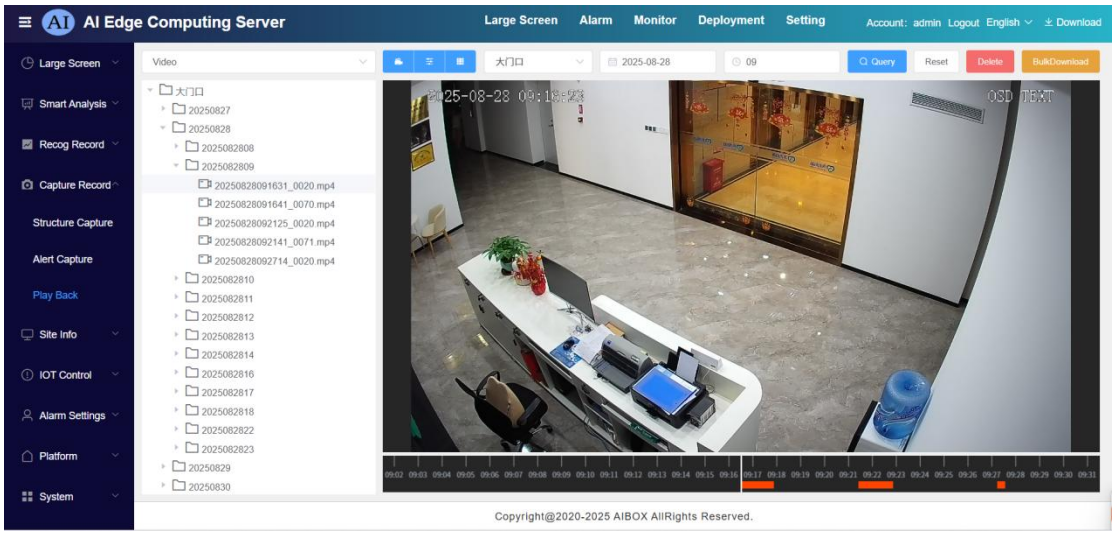


Figure 4-22 Video Playback Page

To display all video data in thumbnail mode, click the button to switch to thumbnail view. Thumbnail mode displays 12 video clips by default, and users can navigate between pages using the pagination buttons. Automatic playback is disabled by default; users must manually click the play button to start playback. To view detailed video information in list format, click the list button to switch views. To return to single-video playback mode, click the video playback button, then directly select the desired video from the left-side directory tree.

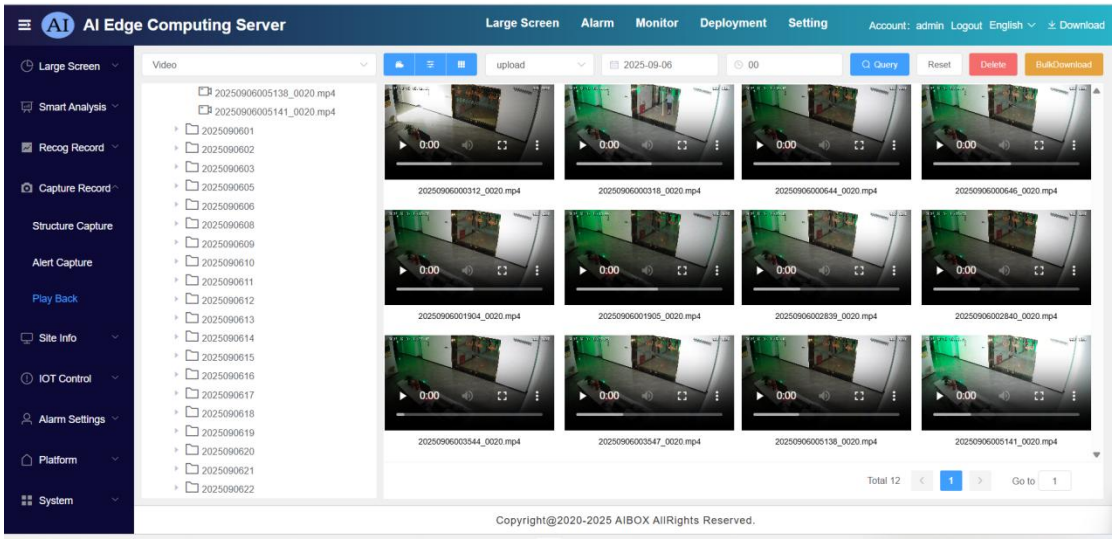


Figure 4-23 Video Playback Thumbnail Page

In video playback, users can drag the time scroll bar located below the video area to quickly locate and play specific segments.

The white vertical line in the middle indicates the current playback time. By dragging this line left or right, users can browse and play video data within the selected time range.

When the mouse is hovered over the time scroll bar, the exact time at the mouse position is displayed.

Figure 4-24 Display of Specific Time Below Video Playback

The operation for querying image data is the same as for video data. The only difference is that when displaying images in list mode, the data is presented in a tabular format, allowing users to click and view or download individual images.

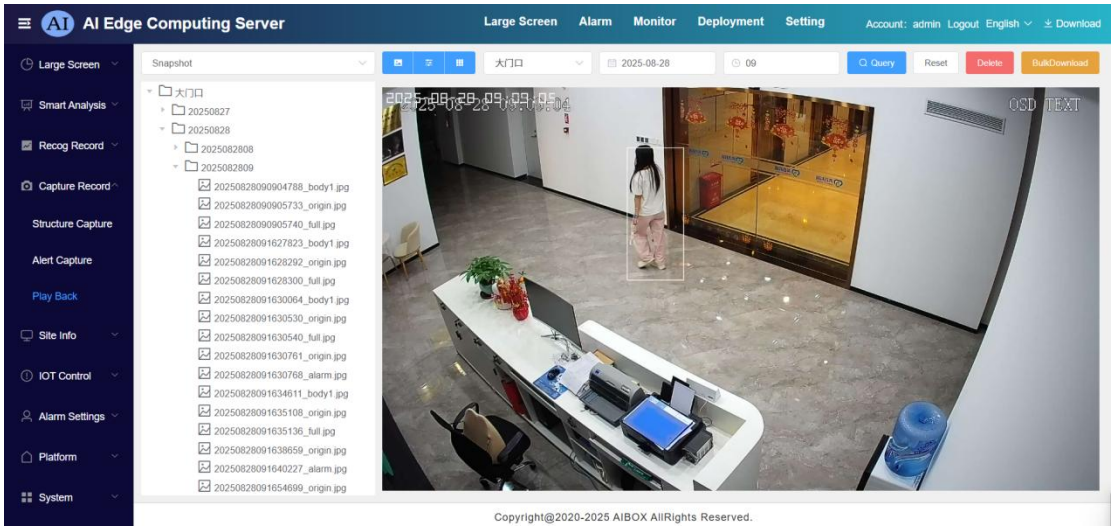


Figure 4-25 Video Playback Snapshot Image Page

4.5.6 Archive Information

Includes: Point Information, Park/Enterprise Archives, Personnel Archives, and Vehicle Archives.

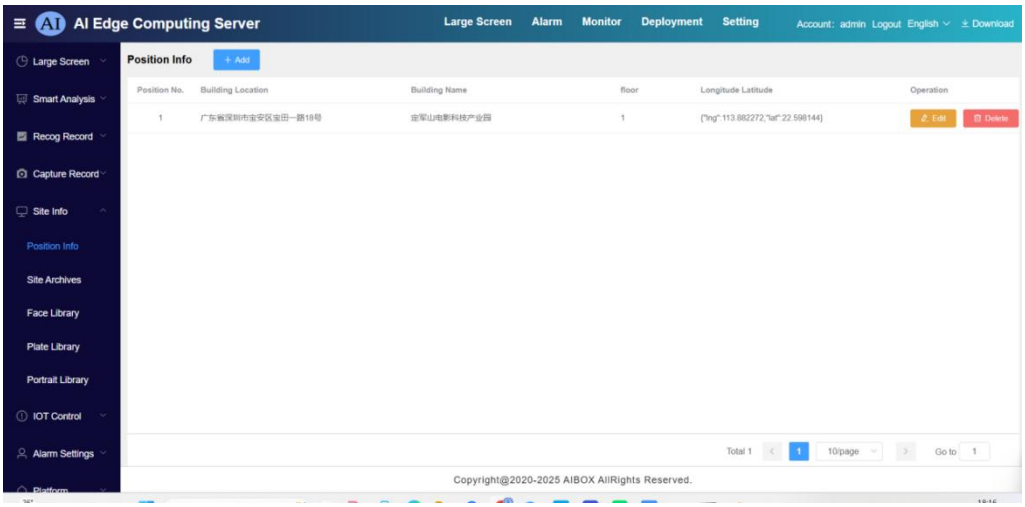


Figure 4-26 Archive Information Page

Point Information

Click + Add to add the specific location where the device is installed. By default, the current geolocation information is displayed. Once the map acquires the location, it will automatically populate the corresponding form fields. If the automatic positioning is inaccurate, users can delete the current location, enter a keyword to search for the desired location, and select one from the dropdown list—the point name will then be automatically filled in.

Alternatively, users can also drag the map to the desired location and click to select the point information directly.

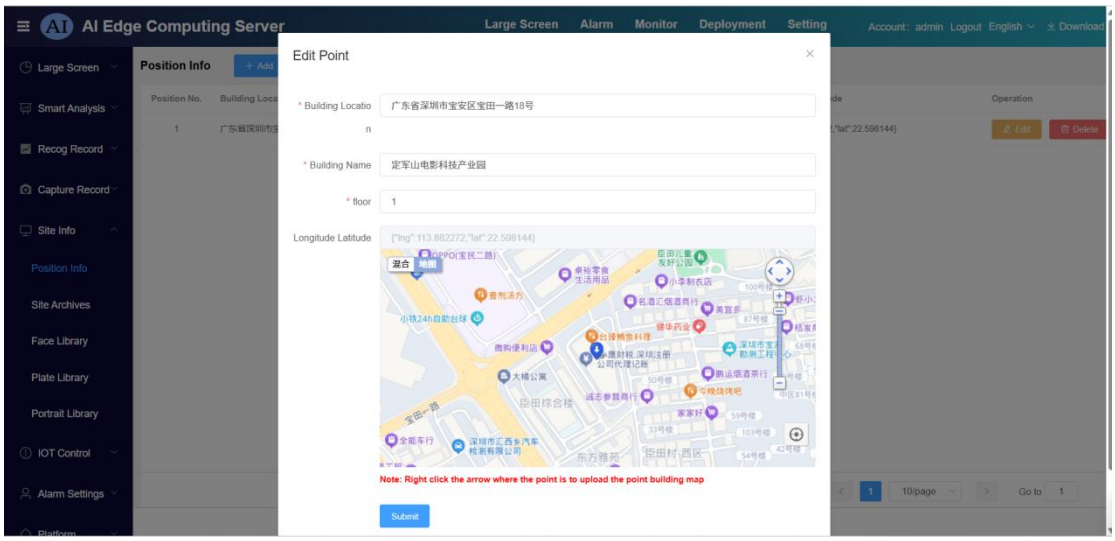


Figure 4-27 Location Information Selection Page

Click Edit to modify the specific point information that has already been added.

Park/Enterprise Archive

Click + Add to add the park/enterprise name, social credit code, and Submit remarks.

Click to LookDept view the department details of the current park/enterprise. To add a department, click New Dept , enter the department name in the list input box, and click to confirm the addition, or click to cancel the addition.

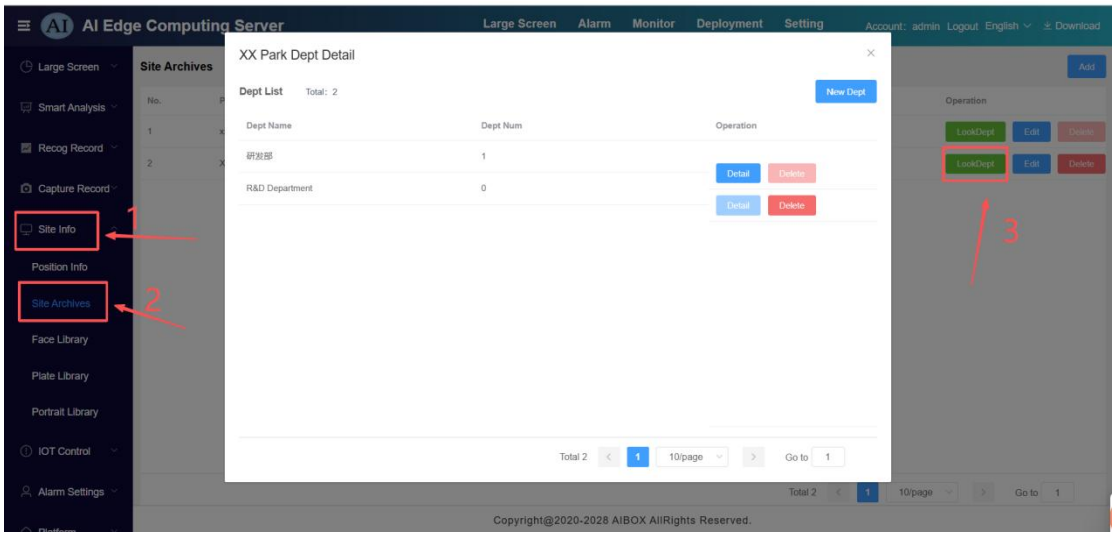


Figure 4-28 Park/Enterprise Addition Interface

In the department list, if the number of departments is 0, the Detail status is grayed out and non-operational. If the number of departments is greater than 0, users can view the personnel information of the current department. At this point, the delete function is disabled; users can directly use the unbind function to remove personnel from the department.

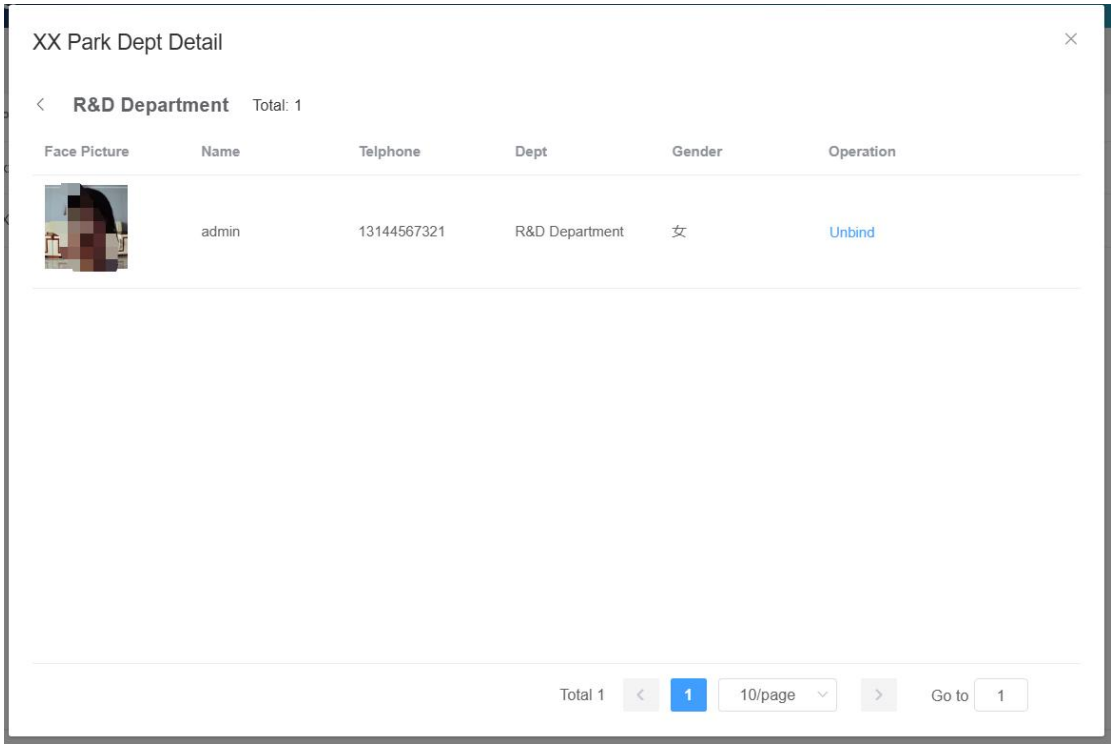


Figure 4-29 Department List Display Page

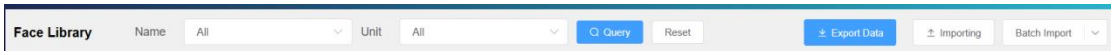
Click Edit to modify the already added park/enterprise archive.

Click Delete to delete an added park/enterprise; if the Delete button is grayed out,

it indicates that the operation is currently unavailable — only parks/enterprises with zero departments can be deleted.

Personnel Archive

On the personnel archive page, you can click the search button to query by name and organization. To clear and reset the search criteria, click the reset button.



To add personnel records, you can choose either single entry or batch entry. Click Importing to proceed, and enter the required information as prompted by the interface. The department dropdown menu is disabled by default and can only be selected after an organization has been chosen. After completing the information, click Submit Entry to complete the process.

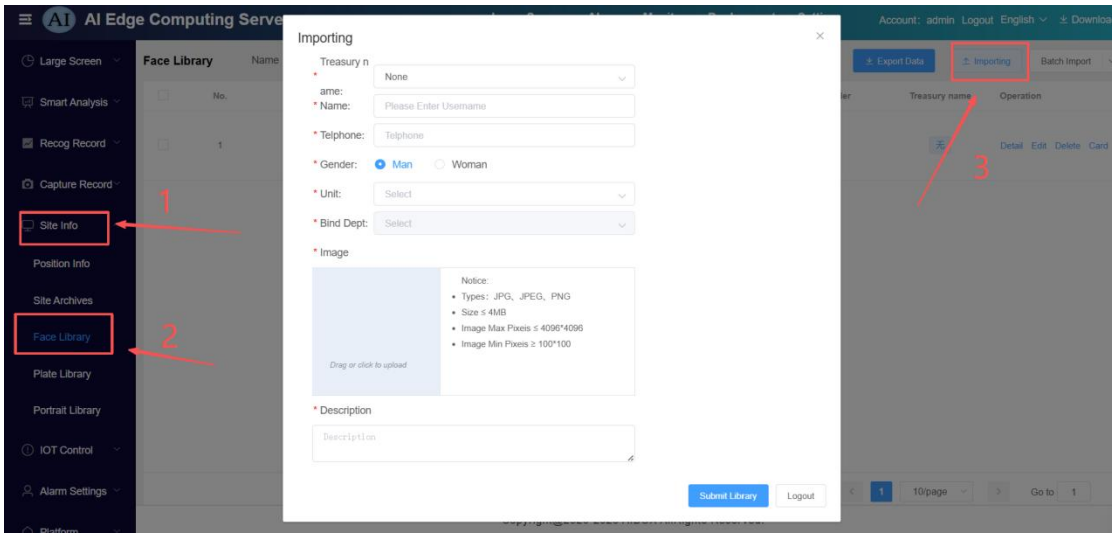


Figure 4-30 Personnel Archive Entry Page

Batch entry allows adding multiple personnel records at once, but the data must follow the specified format. Hover over the dropdown icon next to "Batch Entry" and select folder. A batch import dialog box will pop up. From this dialog, select the folder to upload, then choose the organization and department, and click Batch Import to confirm. Required image naming format:`Name-Gender-Phone-PersonnelDatabaseName.FileType`

Vehicle Archive

The process for vehicle registration is the same as for personnel registration.

4.5.7 Instant Alert

Instant alert mainly includes: alert data, gateway information, and Modbus.

4.5.8 Alarm Settings

Alarm Settings mainly includes: Channel Management, Surveillance Settings, Audio Linkage, Model Management, and Network Devices.

- Channel Management: Refer to Section 5.

- Surveillance Settings: Refer to Section 6.

Alarm Audios

The alarm audios page allows you to modify audio files. Setup steps: Left sidebar — Alert and Surveillance Configuration — Audio Linkage — Upload File — Confirm.

If audio format conversion is required, you can install our company's dedicated audio converter to perform the conversion.

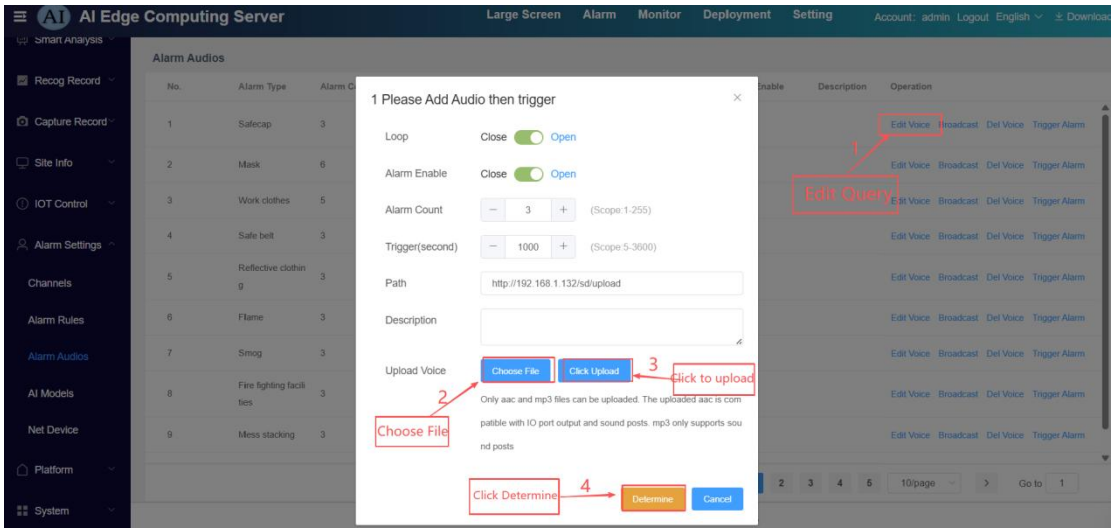


Figure 4-31 Audio Linkage Page

Note: When connecting a speaker to the AIBOX device.For active speakers, connect to the **SPK+** and **GND** terminals. For passive speakers, connect to the **SPK+** and **SPK-** terminals.

Model Management

The model management page allows users to view and edit the alert information for each AI detection model.

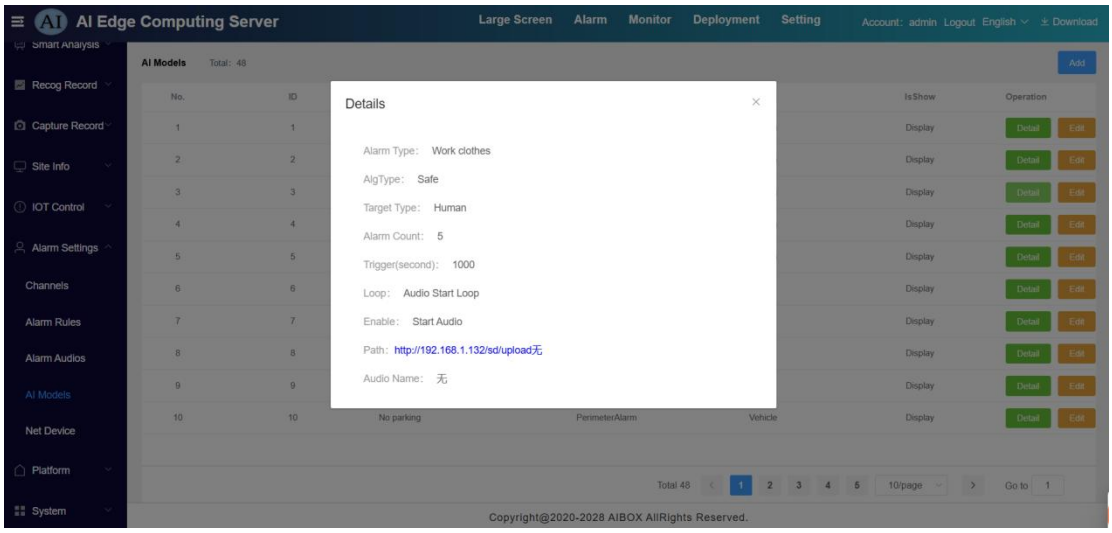


Figure4-32Model Management Page

Network Deveice

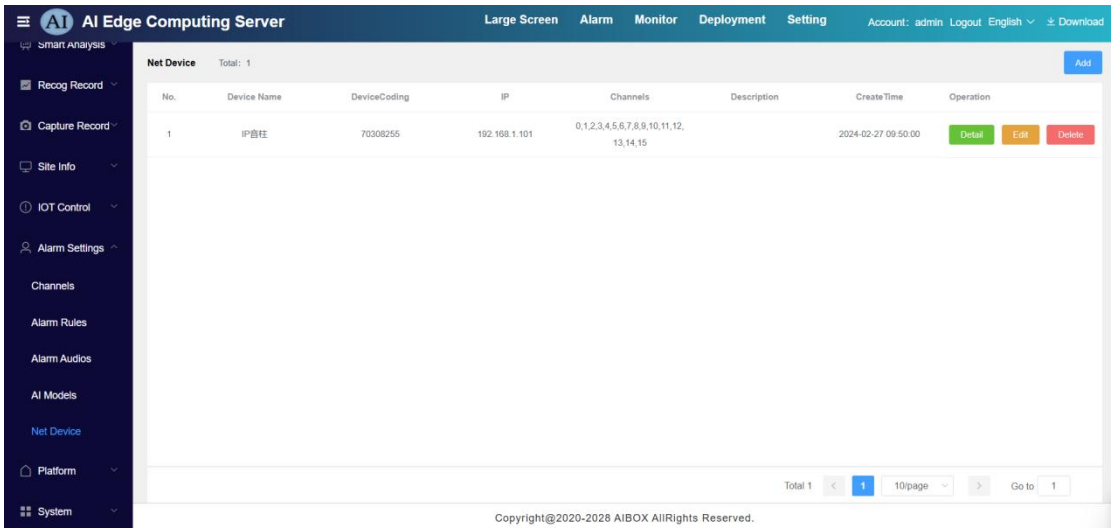


Figure 4-33 Net Deveice Page

The network devices section includes management of IP loudspeakers. By adding IP loudspeaker devices, audio playback can be achieved at locations distant from the edge computing box. On this page, you can configure the IP address of the loudspeaker and specify which channel plays which audio file.

4.5.9 Platform Integration

Platform integration includes: GB28181 Configuration, GA/T 1400, Server Settings, and Report. The most commonly used function currently is HTTP POST integration with alarm platforms.

HTTP Protocol Reporting Results

The system currently supports pushing AI detection results to four addresses—two for the primary server and two for the secondary server. If two addresses need to be entered in a single field, they should be separated by a semicolon (";").

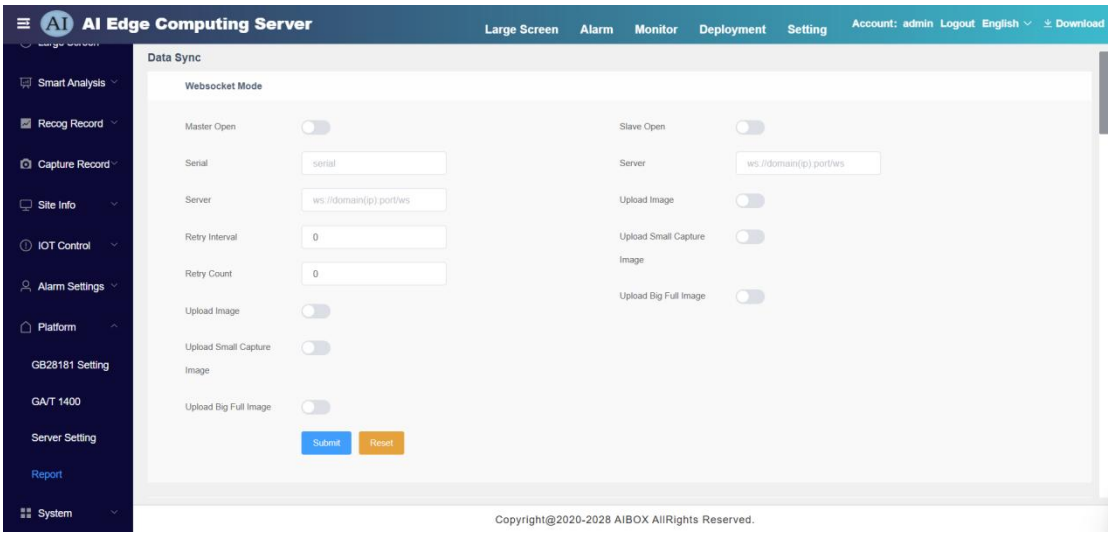


Figure 4-34 HTTP Post Platform Integration Page

Reporting Results via MQTT Protocol

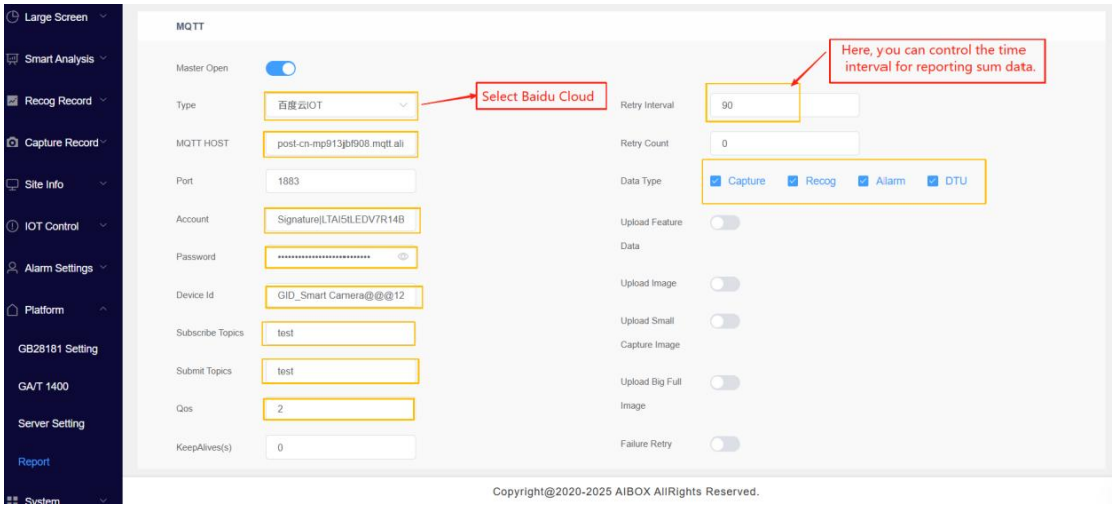


Figure 4-35 MQTT Platform Integration Page

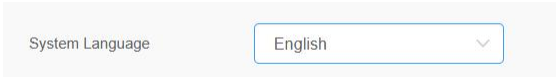
4.5.10 System Management

System management includes: system parameter settings, hardware parameters, online upgrades, and network settings.

System Parameters

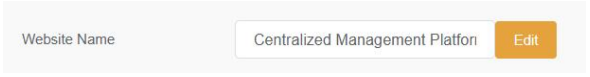
System parameters include:System Configuration、 Global Algorithm Settings、 Access Authentication、M51CConnect。

System configuration:



The system language can be modified to Chinese or English.

The target credibility threshold can be adjusted accordingly, usually set to 10~50, which is the confidence level of all models detecting targets.



The website title can be modified to change the current page title. Enter the desired information and click 

to take effect.

Other settings, please operate according to the prompts on the page.

Global Algorithm Settings:

Modify according to the page instructions; generally, modifications are not recommended.

Hardware Settings:

Displays the current system configuration. The functional area in the upper-right corner includes: Restart AI, Last Upgrade Status, Firmware Upgrade, Device Restart, and Reset.

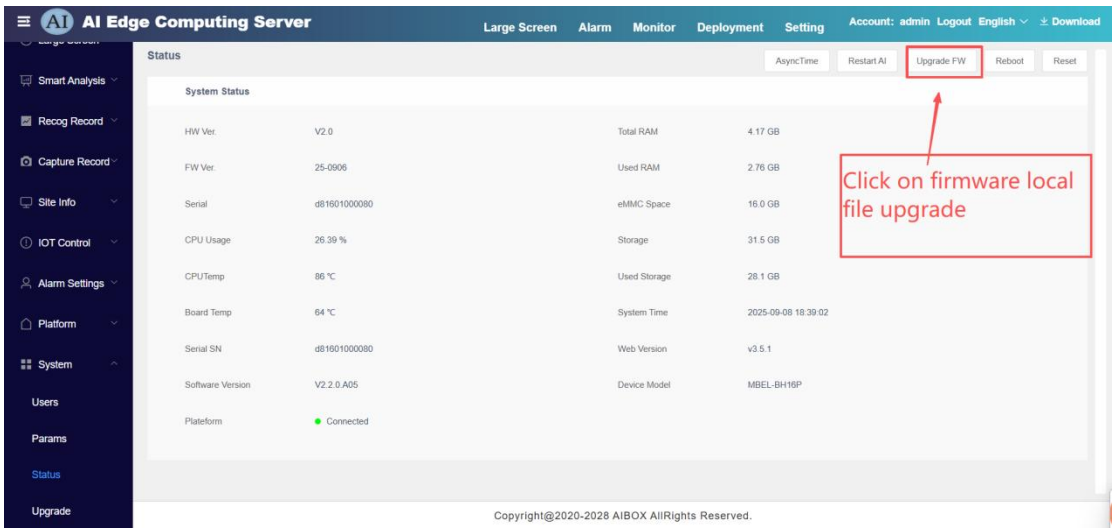


Figure 4-36 Hardware Settings Page

Firmware Upgrade： Click Upgrade FW , then click Chose File to upload the upgrade package provided by our technical personnel, and then click Upgrade FW to start the upgrade process.

Online Upgrade Settings

Online upgrade includes: online upgrade configuration and LOGO replacement.

Online Upgrade: Set according to the on-screen instructions. Generally, it is not recommended to make changes.

LOGO Replacement: Click Click Upload , select the LOGO file you wish to replace, and click "Open" to enter the file selection interface. The selected LOGO file will be displayed in the designated area. Then click Submit to complete the replacement. If the uploaded image file has a **.png** extension, it will replace the website LOGO. If the uploaded image file has a **.ico** extension, it will replace the website icon (favicon).

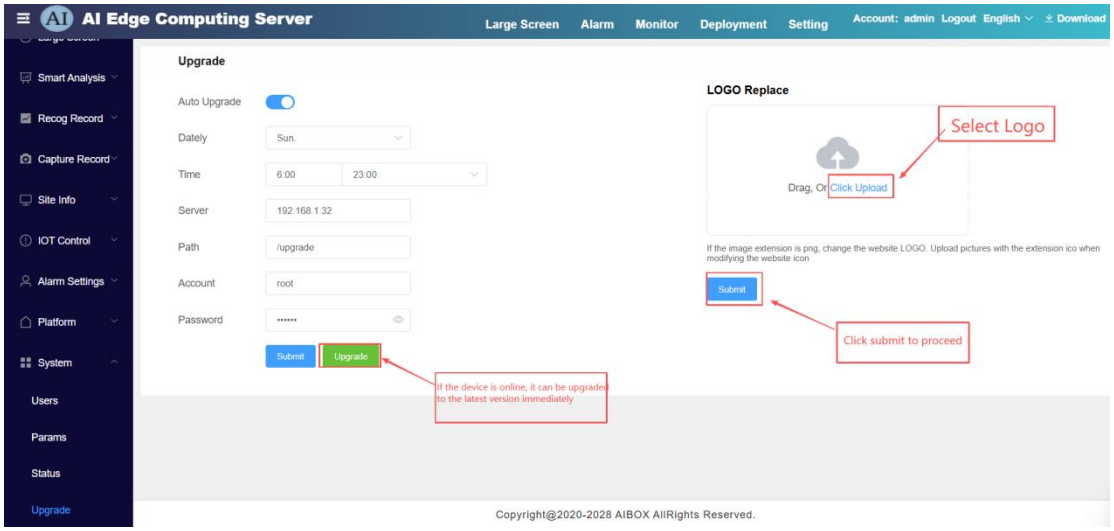


Figure 4-37 Online Upgrade and Logo Replacement Page

Network Settings

You can configure the wired network, wireless network, 4G network, and other LAN port networks for the AIBOX. Simply enter the corresponding information as prompted by the interface.

1. It is recommended to use 4gcms.exe for network configuration. Follow the steps below:

2. Open 4gcms.exe and click Device Scan to enter the device scanning module.

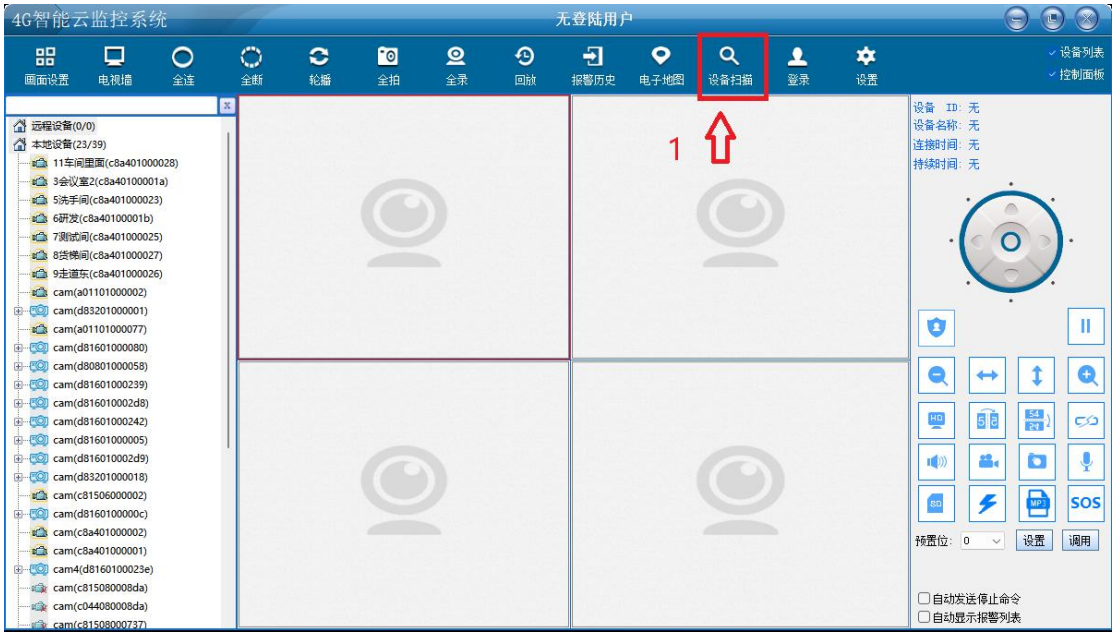


Figure 4-384gcm.exe Click on Device Scan

3. The device scanning module finds the IP address corresponding to AIBOX and enters the editing page.

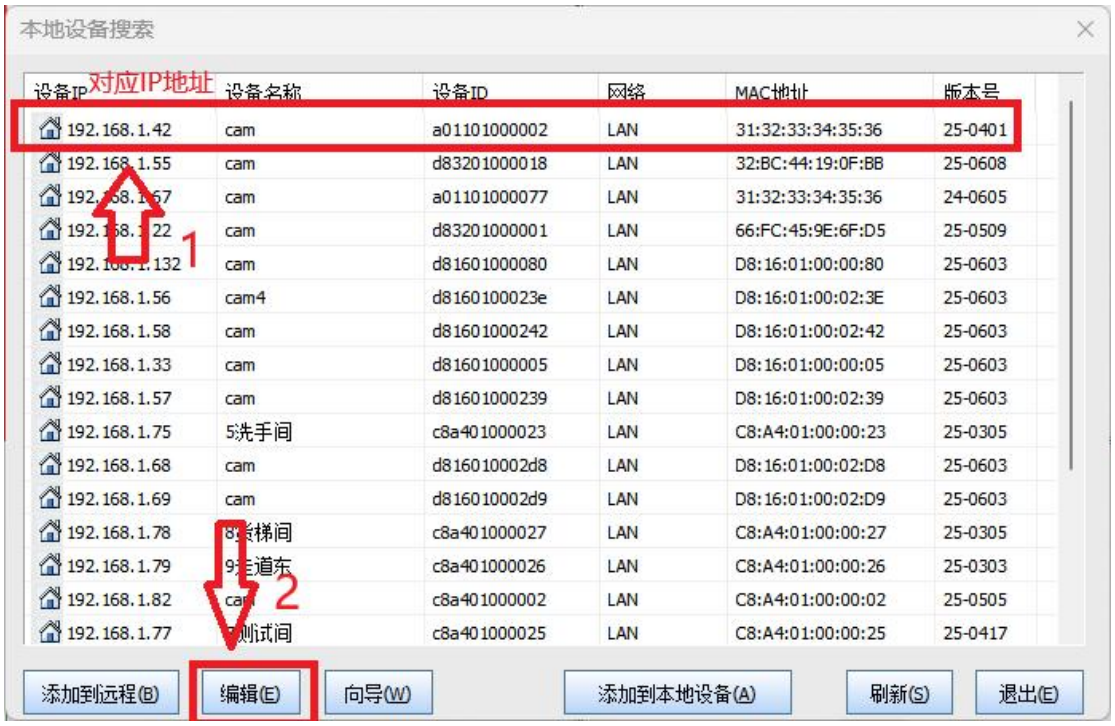


Figure 4-39 Enter Edit Page for Corresponding IP

4. Modify the corresponding IP address, subnet mask, gateway, and other network parameters as needed.

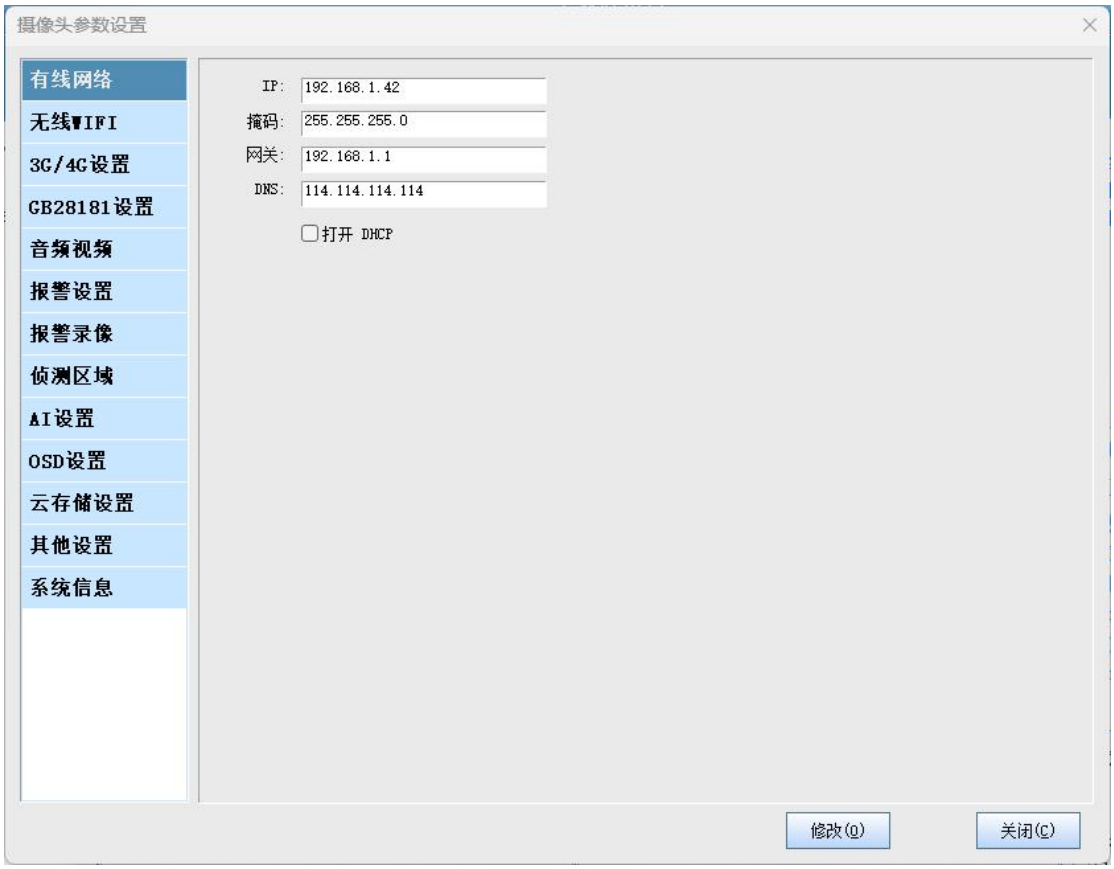


Figure 4-40 Network Modification Parameters

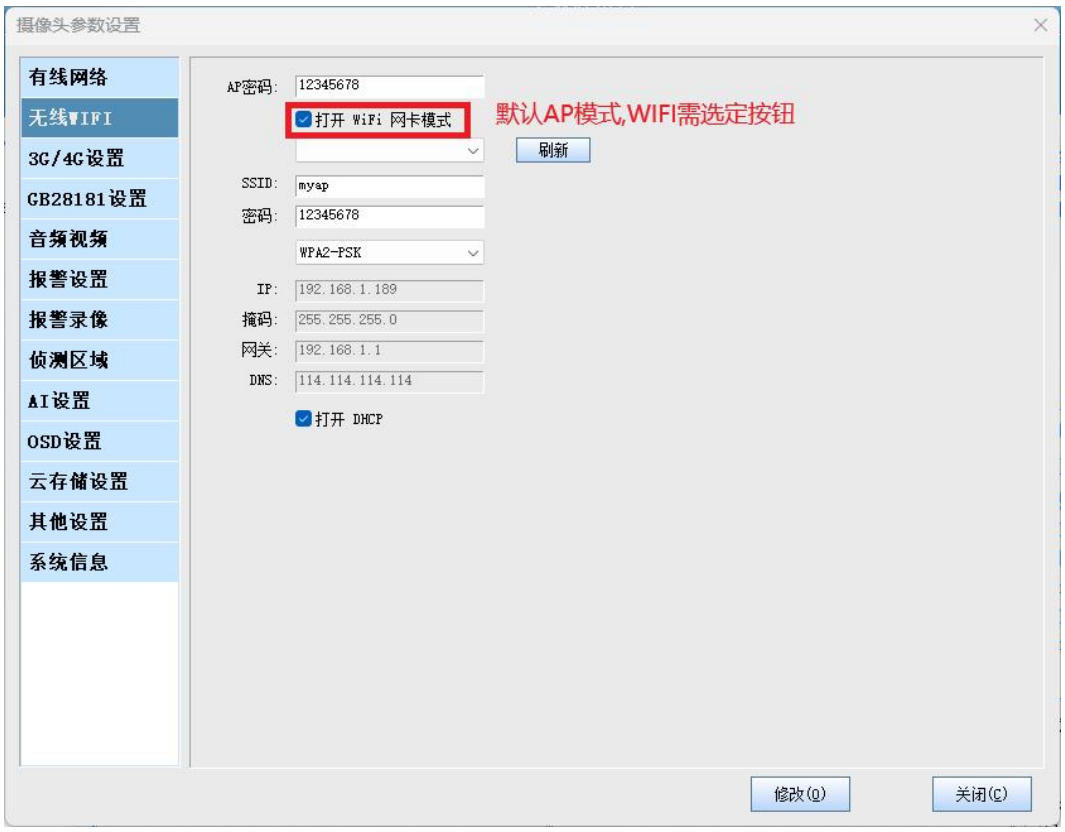


Figure 4-41 WIFI Settings

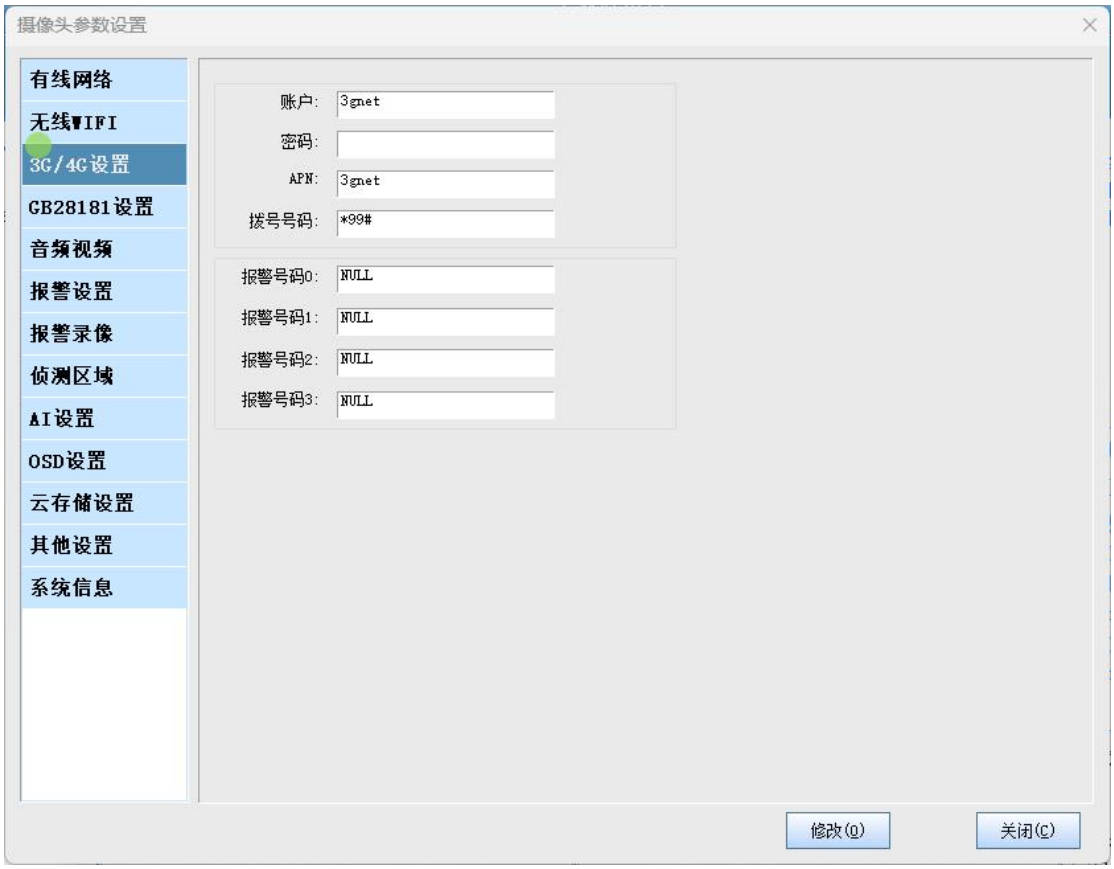


Figure 4-442G setting

Please refer to the user manual of 4ccm.exe for specific parameter settings.

4.6 Frequently Asked Questions (FAQ)

4.6.1 Basic Configuration Logic

1) "Person Leaving" refers to triggering one alarm when a person exits the monitored area.

2) "Person Out of Post" refers to the situation where there is no personnel on duty within the monitored area.

3) "Vehicle Leaving" and "Non-Motorized Vehicle Leaving" each trigger only one alarm.

4) Fire extinguisher detection may fail due to insufficient training images; further optimization is required.

5) Due to limited system resources, the total number of enabled channels for motor vehicle / non-motor vehicle / pedestrian detection must not exceed 15. If the previous channels have already used up the limit, subsequent channels will not function properly.

6) Action recognition detects the duration of an action. For higher sensitivity, set the

duration threshold to a shorter time.

7) If alarms are set but not responding, go to System Management → System Configuration and check the volume settings.

8) If alarm accuracy is poor, go to System Management and adjust the confidence threshold. Refer to Section 7 for detailed threshold ranges. Also, verify whether the alarm zone/line is correctly positioned over the intended detection area.

9) It is currently recommended to use HTTP mode to upload information to the cloud.

10) In channel management, if a camera connection fails, for non-Hikvision cameras, try using VLC software to connect to the network stream to rule out camera issues. For Hikvision cameras, use their official testing software for diagnostics.

4.6.2 Channel Issues

All channels must be added sequentially from 0 to 15. Skipping numbers in the sequence may cause AI recognition issues.

4.6.3 Page Personalization Settings Issues

Title Replacement

To replace the LOGO, refer to section 4.5.10, Online Upgrade Settings.

Title replacement, including the column title and the footer copyright information, can be personalized according to your needs. System Management - System Settings procedure: Left sidebar — System Management — Parameter Settings — Modify Website Title/Permission Information — Refresh the webpage.

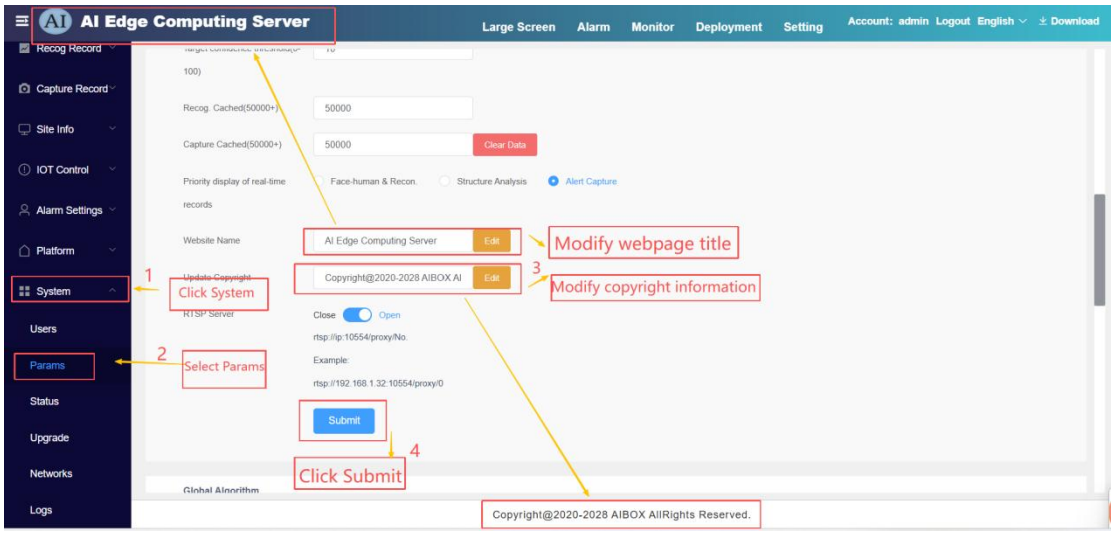


Figure 4-43Title replacement page

Language Settings

If you have requirements to modify the language, you can change the corresponding content as needed. If you need to add other languages, please contact our technical support personnel.

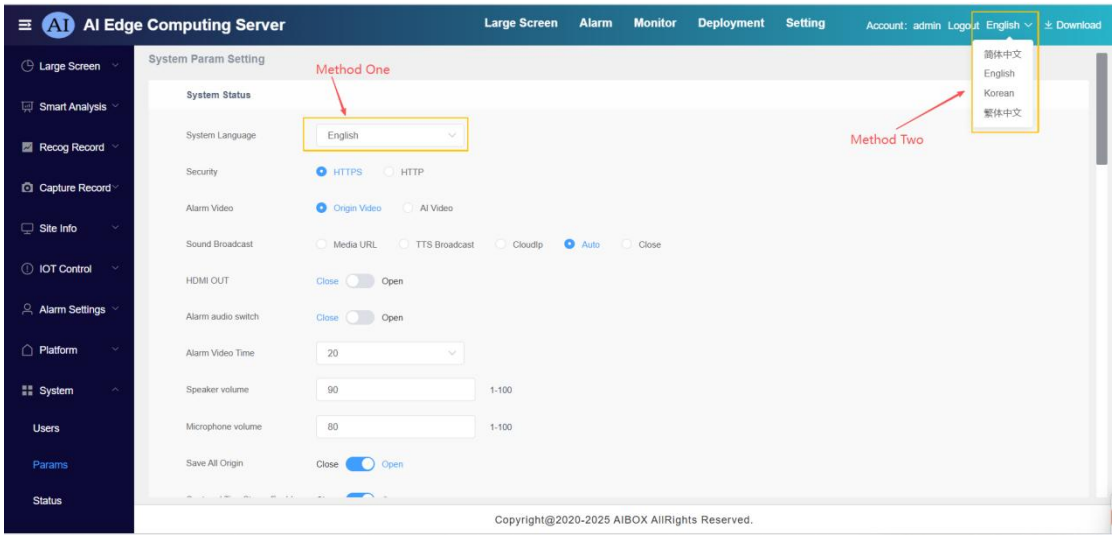


Figure 4-44 Language Settings Location

Note: After switching the language, it is recommended to go to Server Settings to adjust the time information.

Setup Steps: Left sidebar — Platform Access — Server Settings — Select Time Zone / Manually enter Current Time — Click Submit — Refresh the webpage.

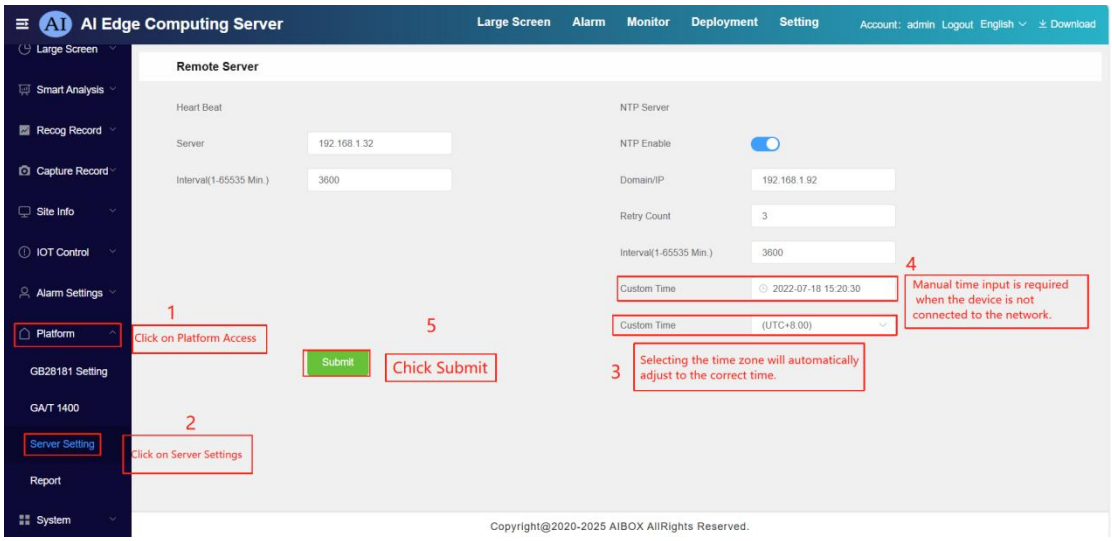


Figure 4-45 Time Zone Modification Steps

5 AI Server Algorithm Advanced Applications

To achieve broader applicability across different scenarios, various functions are realized through AI model configuration. Note: This requires using software version 25-0805 or later.

5.1 Model Changes for Different Algorithms

5.1.1 Camera cover Algorithm Function Configuration

Chinese: 摄像头遮挡　　English: Cameracover

The algorithm uses the serial number:45 ,ID:52 to modify the model

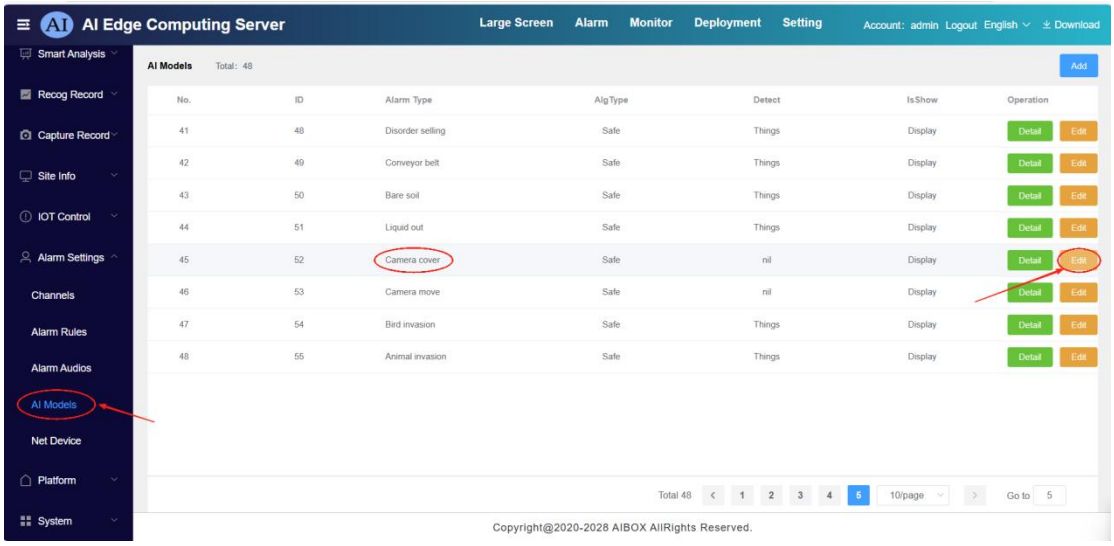


Figure 5-1 Camera cover Algorithm Function Configuration Page

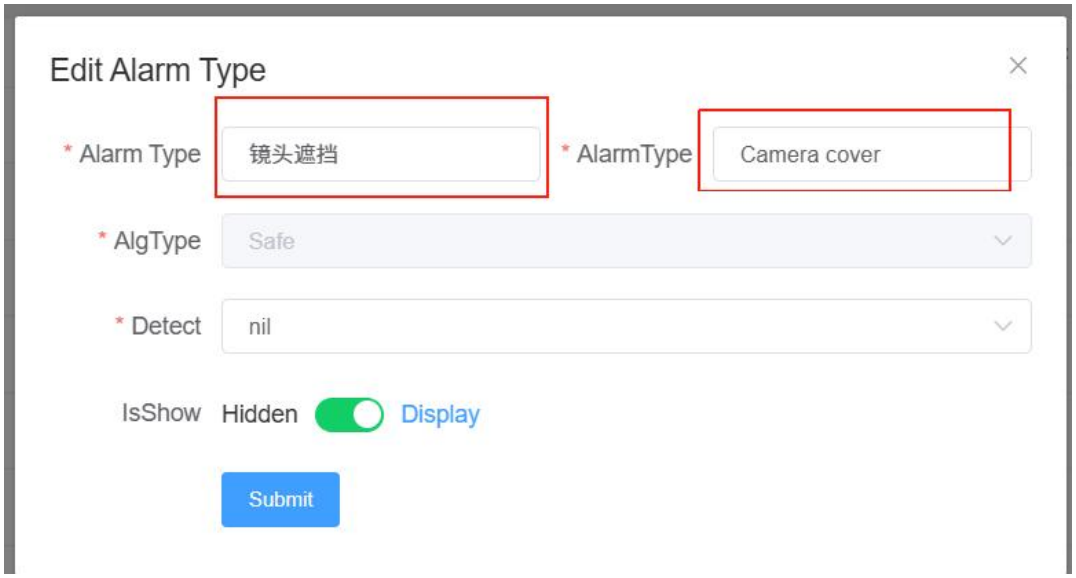


Figure 5-2 Camera occlusion algorithm alarm type editing page

Note: Make sure to follow the steps shown in the figure when making modifications. After modification, the messages pushed by the algorithm will reflect the changes, but the subtype of the push notifications will remain unchanged from before. Be sure to take this into account when applying the modifications.

5.1.2 Camera move Algorithm Configuration

Chinese: 摄像头偏移　　English: Camera move

The algorithm uses the serial number :46,ID:53 to modify the model

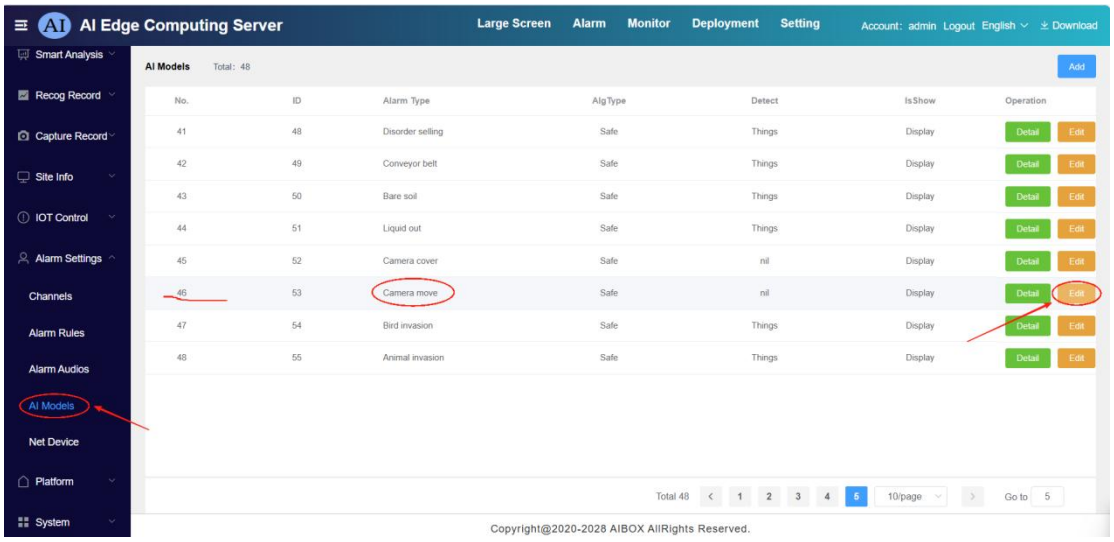


Figure 5-3 Camera offset algorithm editing steps

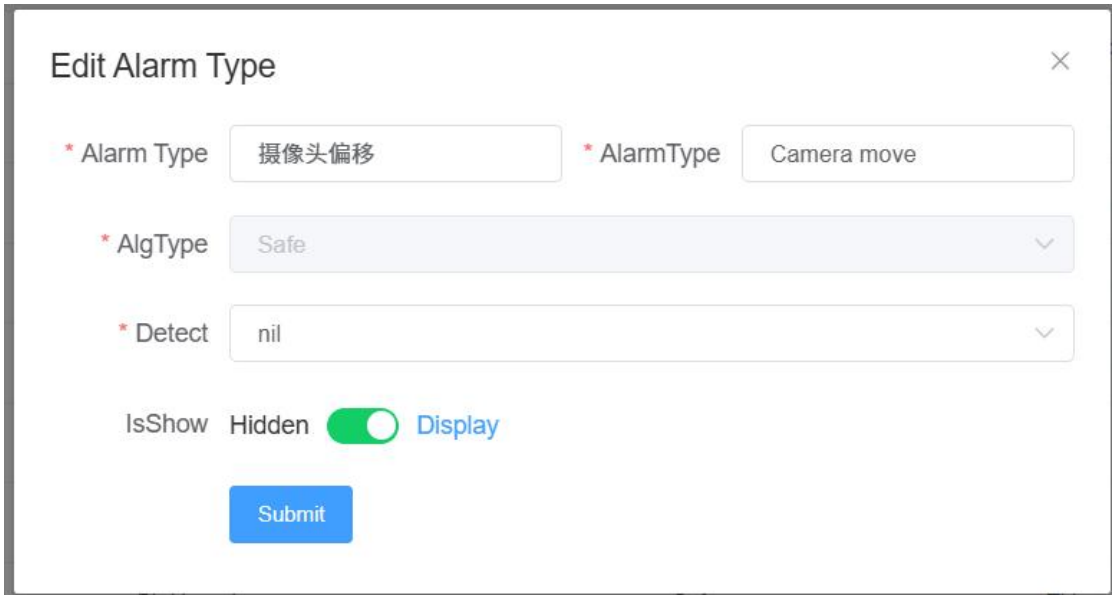


Figure 5-4 Camera offset algorithm alarm type editing page

5.1.3 Ultra high and Over limit Algorithm

Chinese: 物品遗留　　English：Overhigh

This algorithm shares the serial number :47,ID:54 with bird invasion, modify the model

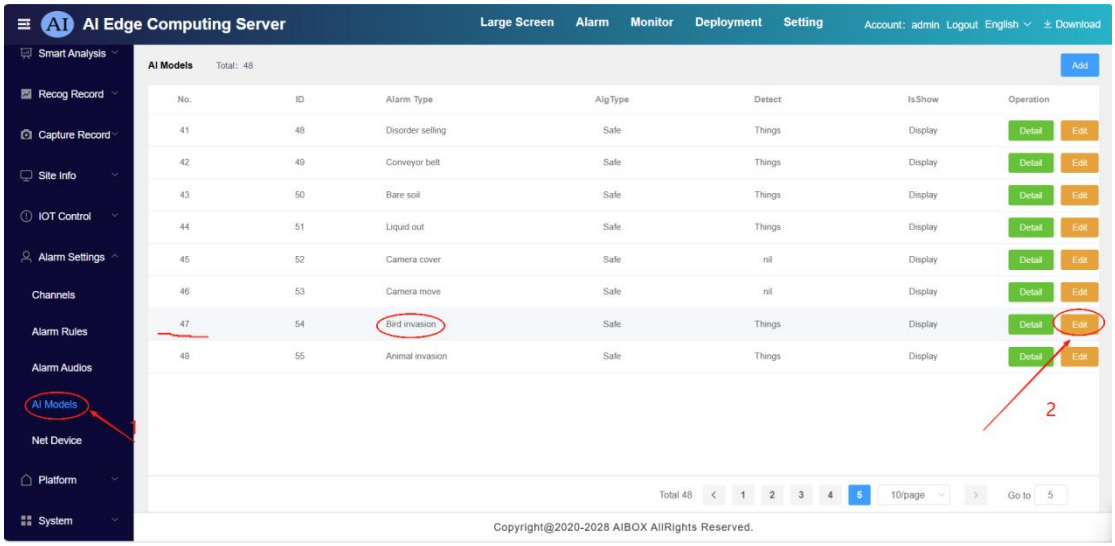


Figure 5-5 Editing steps for ultra-high and over limit algorithm

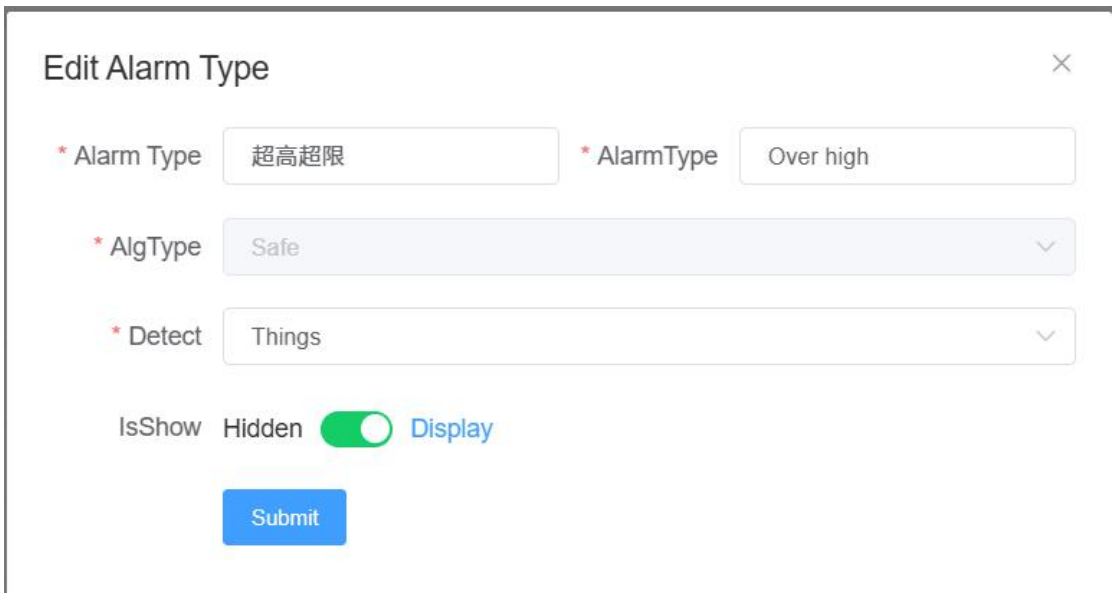


Figure 5-6　Editing page for alarm types of ultra-high and over limit algorithms

When configuring the channel algorithm, it is necessary to draw an extended area and associate it with the overheight/oversize detection rule; otherwise, the algorithm will not take effect.

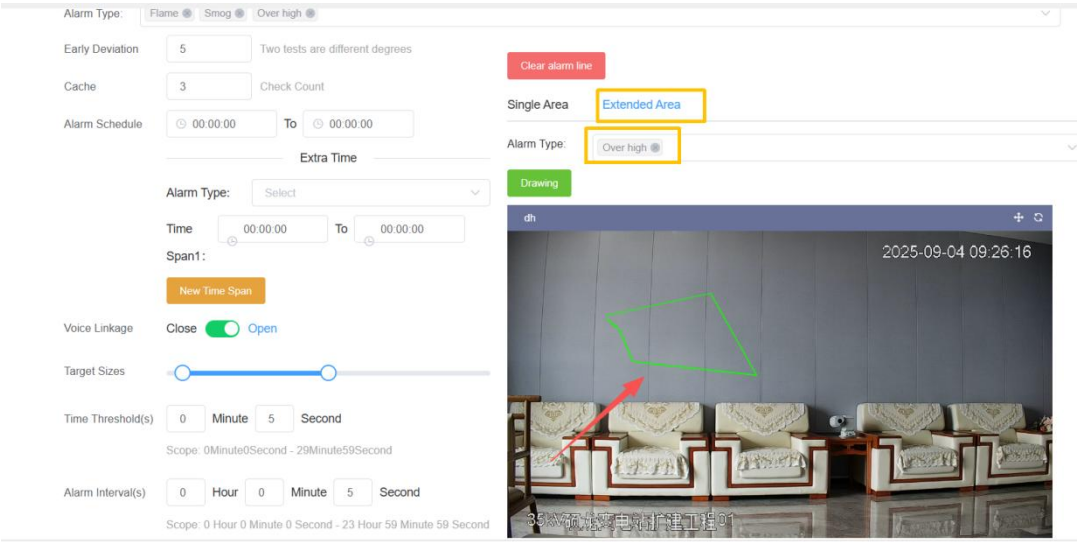


Figure 5-7 Steps for Drawing Extended Areas

5.1.4 Algorithm configuration for leaving and taking away items

Chinese：物品遗留 英文：Thingsmove

This algorithm shares the serial number :48,ID:55 with animal invasion, modify the model

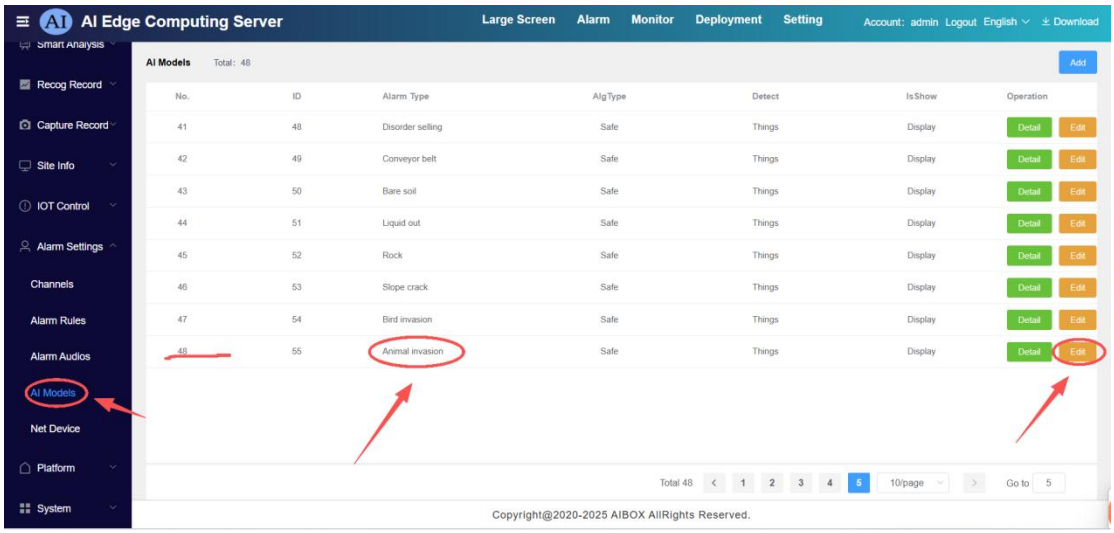


Figure 5-8 Editing steps for the algorithm for leaving and taking away items

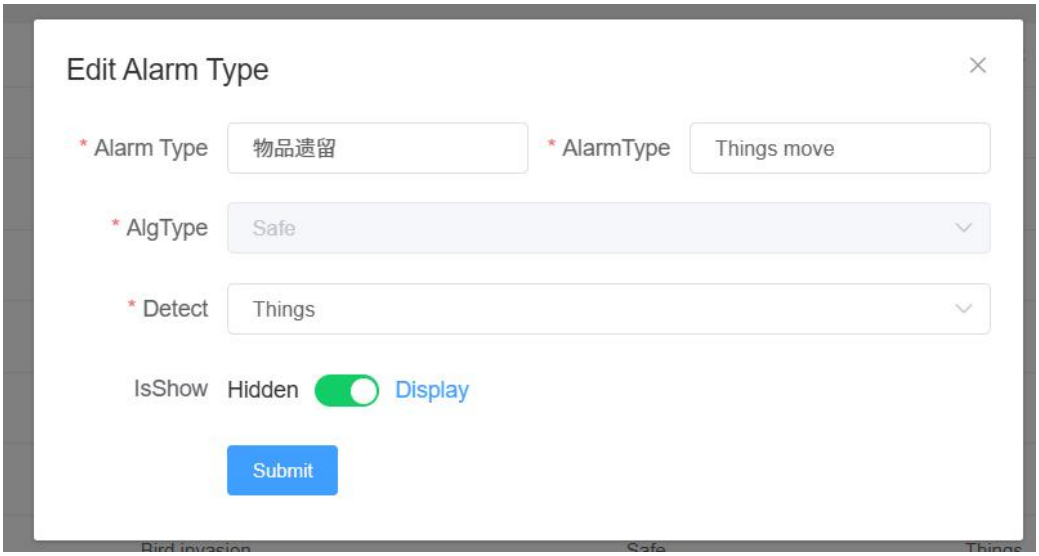


Figure 5-9 Editing page for alarm types of algorithms for leaving and taking away items

5.1.5 Fatigue driving

Modify the 40th model in model management.
Chinese: 疲劳驾驶 English: Fatigue Driving
Implemented detection of closed eyes and yawning.

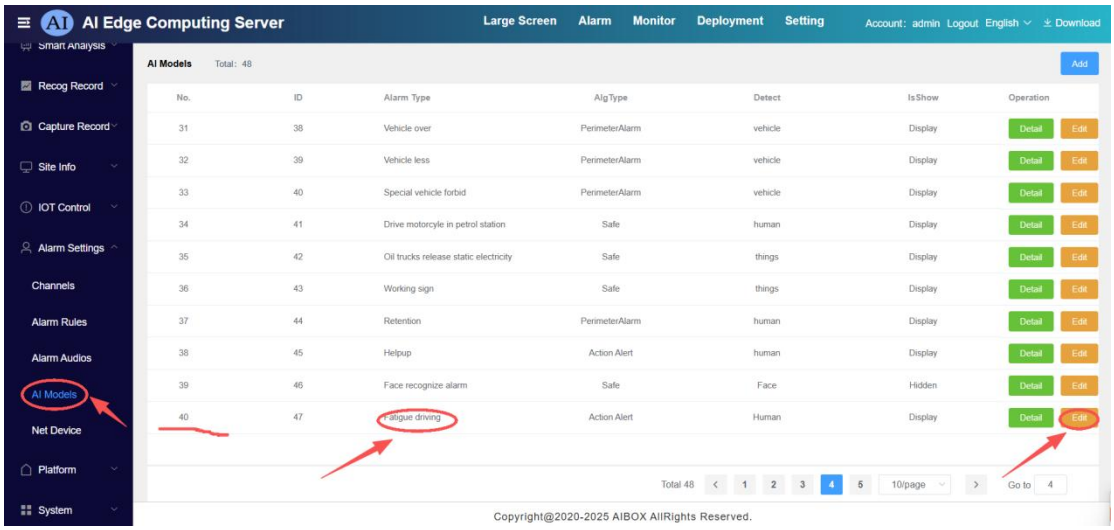


Figure 5-10 Steps for Editing Fatigue Driving Algorithm

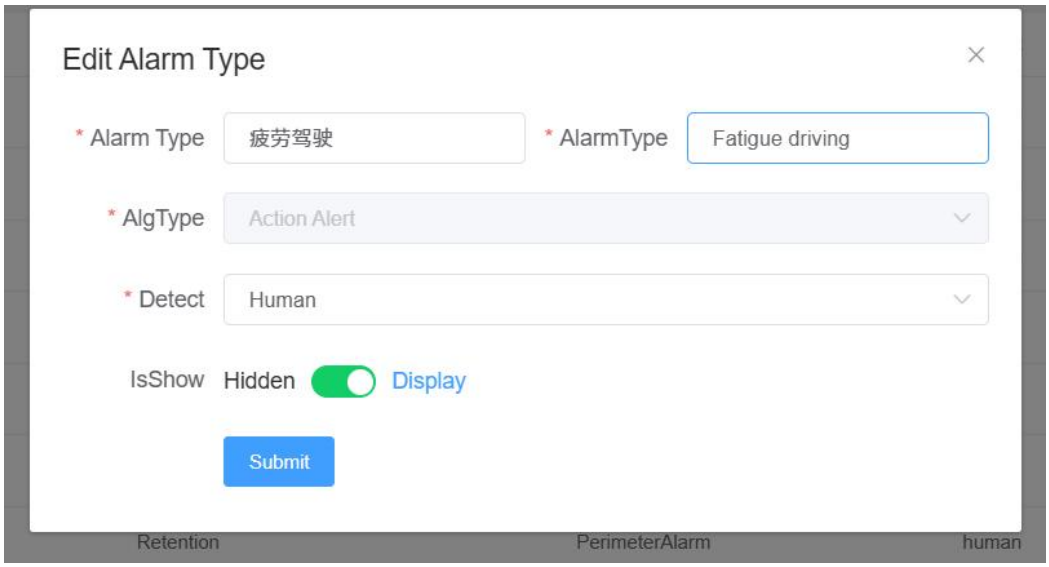


Figure 5-11 Fatigue Driving Algorithm Alarm Type Editing Page

Fatigue driving detection requires the camera to face the person and only detect more than one-third of the human body. Yawning continuously for 5 times within 3 minutes triggers an alarm, with the duration of eye closure linked to the duration of the alarm.

5.2 Advanced Applications of Personnel Counting and Overstaffing Algorithms

In order to achieve the function of gathering people from multiple camera perspectives, the system has implemented the function of counting the number of people from a single camera and all cameras.

5.2.1 Reporting of Number Statistics

Enable the DTU reporting option, as shown in the following figure:

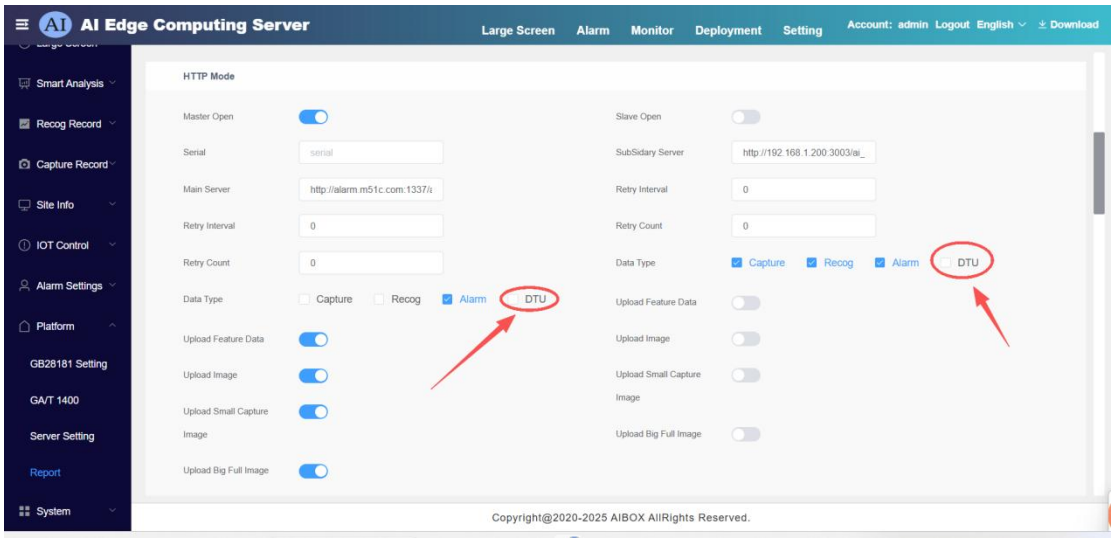


Figure 5-12 Configuration steps for reporting headcount statistics

If the DTU option is enabled, httppost and mqttpost will report data according to the interval. The format is as follows:

```
#definePOST_Sum_DATA"{"    \
"\"devId\":\"%s\","    \
"\"devSn\":\"%s\","   \
"\"ch\":\"%02d\","    \
"\"chId\":\"%s\","     \
"\"chName\":\"%s\","     \
"\"msgType\":\"%s\","     \
"\"msgSource\":\"%s\","  \
"\"aiType\":\"%s\","  \
"\"msgDisc\":\"%s\","     \
"\"trackIDFace\":\"%d\",\"\
"\"trackIDHuman\":\"%d\","   \
"\"trackIDCycle\":\"%d\","     \
"\"trackIDVehicle\":\"%d\","   \
"\"trackIDPlate\":\"%d\","     \
"\"snapedFace\":\"%d\",\"\
"\"snapedHuman\":\"%d\","   \
"\"snapedCycle\":\"%d\","     \
"\"snapedVehicle\":\"%d\","   \
"\"snapedPlate\":\"%d\","     \
"\"currentFace\":\"%d\","     \
"\"currentHuman\":\"%d\","   \
"\"currentCycle\":\"%d\","     \
"\"currentVehicle\":\"%d\","   \
"\"currentPlate\":\"%d\","     \
"\"currentHumanGlobal\":\"%d\","     \
```

```
"\"currentCycleGlobal\":\"%d\","  \
"\"currentVehicleGlobal\":\"%d\","      \
"\"currentPlateGlobal\":\"%d\","  \
"\"time\":\"%d\","     \
"\"img_str_s\":\"%s\","    \
"\"img_str\":\"%s\"" \
"}"
```

5.2.2 Global correlation of overcrowding

If global overcrowding is required as shown in the following figure, select the global option. Please note that the switch for global statistics is as described in the previous section. Enable the DTU option on the report interface, otherwise global statistics will not work.

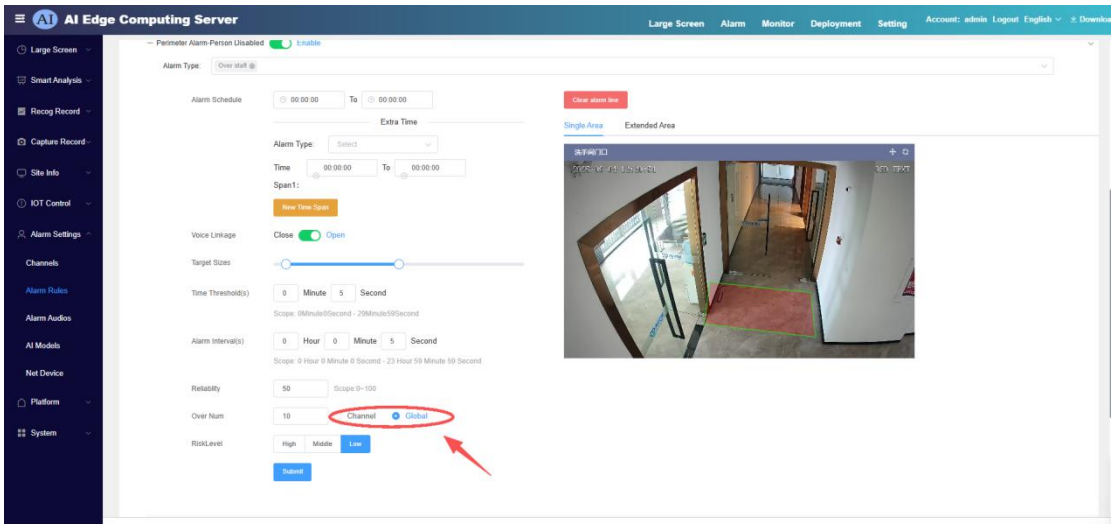


Figure 5-13 Global Association Configuration Steps for Overstaffing Number

In the overbooking alarm, the trackId field is not very useful, and the current number of people is filled in this field.

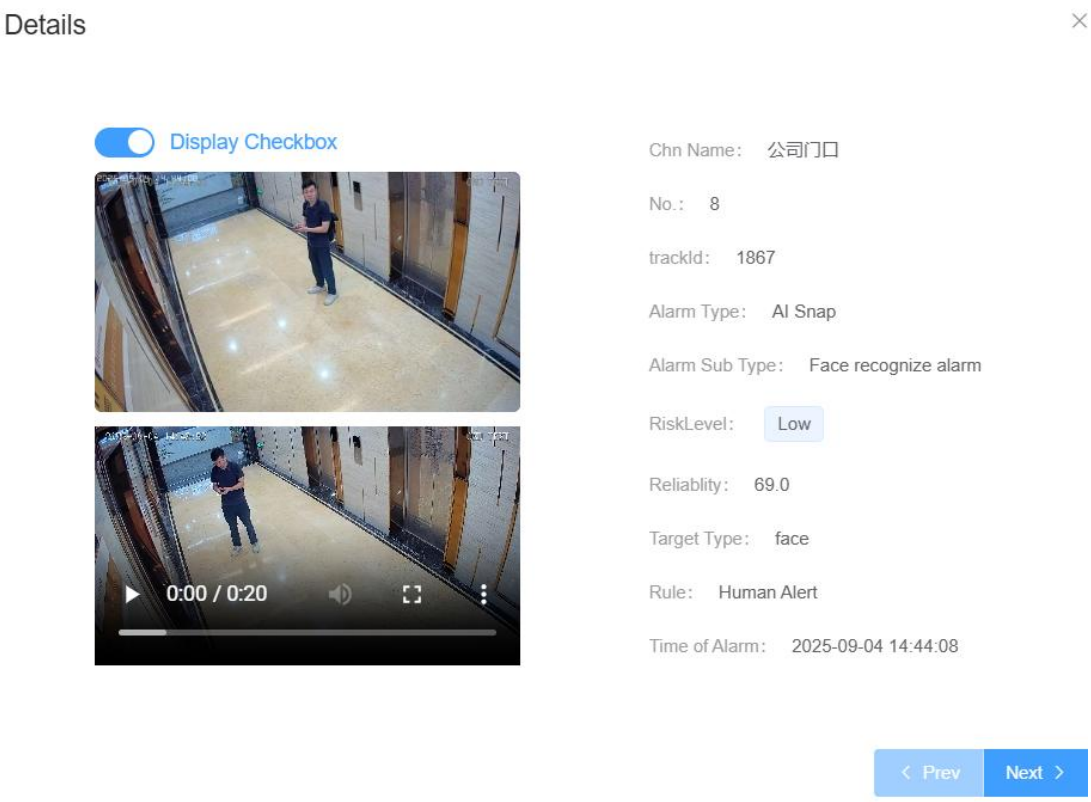


Figure 5-14 TrackId Field