User Manual

AI Traffic Video Detector

ClairEye-i

Version: 2.2

TraffiClair Technology Co., Ltd.

Content

1. Background 3
1.1 Business Context 3
1.2 Business Scenarios 3
2. Product Overview 4
2.1 Product Introduction 4
2.2 Product Targets 5
2.3 Product Logic 5
2.4 Product Specifications 6
3. System Introduction 8
3.1 Login 8
3.2 System interface 10
3.3 Video Configuration 12
3.4 Data Analysis 14
3.5 System Settings 16
3.5.1 Parameter Configuration 16
3.5.2 Central Configuration 18
3.5.3 I/O Configuration 19
3.5.4 Password Setting 20
3.5.5 System Tools 21
3.5.6 System Logs 23
3.5.7 Object Portion Settings 23
4. Communication Protocols 25

1. Background

1.1 Business Context

With the rapid advancement of technology, artificial intelligence and machine learning have been widely applied across various industries. In this process, video intelligent recognition devices have emerged as a new focal point in the market. ClairEye-i arises in response to this background, aiming to address the efficient processing and analysis of complex video data.
By efficiently processing and analyzing video data, ClairEye-i provides enterprises and individuals with a new perception of vision and the capability for data insight, thus facilitating the intelligent upgrading and innovative development across various industries.

1.2 Business Scenarios

1. Security Surveillance: In the field of security surveillance, ClairEye-i can be widely applied in public safety, traffic management, the finance industry, commercial premises, and more. By monitoring real-time videos, ClairEye-i can automatically detect abnormal behaviors such as loitering, sudden running, unusual gatherings, etc., and immediately issue alerts, thereby enhancing security capabilities. Additionally, ClairEye-i can perform facial recognition to track the movements of suspects, aiding in criminal investigations.

2. Facial Recognition: ClairEye-i's facial recognition technology can be widely applied in identity authentication, access control systems, payment platforms, and other scenarios. Through facial recognition, users can quickly complete identity authentication, facilitating access control or payment operations. Furthermore, ClairEye-i can play a crucial role in public safety by tracking the movements of suspects or missing persons.

3. Intelligent Traffic: In the field of intelligent traffic, ClairEye-i can achieve automatic identification and tracking of vehicles, providing real-time and accurate data support for traffic management. By analyzing vehicle trajectories and behavior patterns, ClairEye-i can assist traffic management departments in optimizing traffic flow allocation, reducing traffic congestion, and minimizing accident risks. Additionally, ClairEye-i can be applied in smart parking, automatically identifying vacant parking spaces and guiding vehicles to find parking spots.

4. Smart Manufacturing: In the field of smart manufacturing, ClairEye-i can be applied in production line automation, product quality inspection, and other aspects. By automatically identifying and detecting product defects, ClairEye-i can improve production efficiency and product quality while reducing production costs. Moreover, ClairEye-i can intelligently analyze the behavior of employees on the production line, enhancing production safety and management efficiency.

5. Retail Industry: In the retail sector, ClairEye-i can be applied in customer behavior analysis, product recommendations, etc. By analyzing customers' purchasing behaviors and preferences, ClairEye-i can provide personalized product recommendation services, thereby improving sales effectiveness and customer satisfaction. Additionally, ClairEye-i can be used for theft prevention surveillance, automatically identifying abnormal behaviors and issuing alerts.

2. Product Overview

2.1 Product Introduction

ClairEye-i is an advanced video intelligent recognition device that empowers you with a new visual perception through innovative technology and outstanding performance, making real-time video data analysis and processing possible.

The design concept of ClairEye-i stems from the pursuit of deep integration between technology and life. It is powered by cutting-edge AI technology and equipped with powerful video processing capabilities, capable of capturing and analyzing video content in real-time. Whether it's dynamic images, static figures, objects, or even minute details, ClairEye-i can accurately identify them, enabling intelligent and automated information extraction and analysis.

The core technology of ClairEye-i lies in its deep learning algorithm, enabling the device to possess human-like understanding and recognition capabilities when processing video data. Whether it's recognizing faces, objects, or environmental features, ClairEye-i can accurately identify and match them. Furthermore, ClairEye-i excels in real-time processing, capable of analyzing video data within milliseconds.

In terms of application scenarios, ClairEye-i undoubtedly stands out as the most flexible and comprehensive video intelligent recognition solution on the market. Whether in security surveillance, facial recognition, intelligent traffic, smart manufacturing, retail, and various other fields, ClairEye-i can leverage its powerful advantages. For instance, in security surveillance, ClairEye-i can detect abnormal behaviors in real-time, issue early warnings, and enhance security levels. In the domain of intelligent traffic, ClairEye-i can automatically identify and track vehicles, thereby improving traffic management efficiency. In retail, ClairEye-i can analyze customer purchasing behaviors to provide precise product recommendations, boosting sales effectiveness.

ClairEye-i video intelligent recognition device is a powerful and versatile product. With leading-edge technology and outstanding performance, it provides you with a new level of visual perception, making real-time video data analysis and processing possible. In this era full of boundless possibilities, let's embark on a new visual journey with ClairEye-i!

2.2 Product Targets

ClairEye-i video intelligent recognition device is an intelligent analysis device designed for video data, with its core functionality being real-time recognition, analysis, and processing of input video streams. The following are the main product targets of ClairEye-i:

1. Video Data Input: ClairEye-i can receive video streams from various video input sources such as cameras, surveillance recordings, etc. Users can utilize ClairEye-i to perform intelligent analysis on video streams to meet various application scenarios.

2. Video Recognition and Analysis: ClairEye-i employs advanced deep learning algorithms to perform real-time recognition and analysis of input video streams. It can identify information such as people, objects, scenes, etc., within the video and perform analysis and extraction. For example, ClairEye-i can detect abnormal behaviors, perform facial recognition, license plate recognition, etc.

3. Data Output: ClairEye-i can output recognition and analysis results to users, providing precise data support and insight capabilities. Users can apply the results to various scenarios such as security surveillance, facial recognition, intelligent traffic, smart manufacturing, retail, etc., according to their actual needs.

4. User Interface: ClairEye-i is equipped with an intuitive user interface, allowing users to easily configure and manage the device. Users can manage functions such as video stream configuration, adjustment of recognition parameters, result output, etc., through the interface.

5. Scalability: ClairEye-i supports horizontal and vertical scalability, catering to the needs of different scales and application scenarios. Users can increase or decrease the number of devices according to their actual needs to achieve flexible deployment solutions.

2.3 Product Logic

The product logic of ClairEye-i video intelligent recognition device includes video input and preprocessing, video recognition, behavior analysis, data output, user interface, and scalability. Through the combination and coordination of these logics, ClairEye-i can provide efficient video intelligent recognition functionality to meet the needs of various fields.

1. Video Input and Preprocessing: ClairEye-i initially receives video streams from various video input sources such as cameras, surveillance recordings, etc. Subsequently, through the preprocessing stage, the input video stream undergoes necessary formatting, noise reduction, image enhancement, etc., to prepare for subsequent recognition and analysis operations.

2. Video Recognition: ClairEye-i employs deep learning algorithms to recognize preprocessed video frames. It can identify information such as people, objects, scenes, etc., within the video and perform analysis and extraction. For instance, through facial recognition technology, ClairEye-i can detect and identify faces in the video; through object recognition technology, it can detect and identify specific objects within the video.

3. Behavior Analysis: Building upon the recognition of video content, ClairEye-i can conduct behavior analysis. By tracking and analyzing elements such as people and objects within the video, it can detect abnormal behaviors, target tracking, etc. For example, ClairEye-i can detect sudden running, abnormal gatherings, etc., in the video and immediately issue alerts.

4. Data Output: ClairEye-i can output recognition and analysis results to users, providing precise data support and insight capabilities. Users can apply the results to various scenarios such as security surveillance, facial recognition, intelligent traffic, smart manufacturing, retail, etc. For example, in the security surveillance field, ClairEye-i can detect abnormal behaviors in real-time, issue early warnings, and enhance security levels.

5. User Interface: ClairEye-i is equipped with an intuitive user interface, enabling users to easily configure and manage the device. Users can manage functions such as video stream configuration, adjustment of recognition parameters, result output, etc., through the interface. Additionally, the interface provides real-time preview and historical playback functions, allowing users to conveniently view and analyze video content.

6. Scalability: ClairEye-i supports horizontal and vertical scalability, catering to the needs of different scales and application scenarios. Users can increase or decrease the number of devices according to their actual needs to achieve flexible deployment solutions. For example, in large-scale surveillance systems, increasing the number of ClairEye-i devices can expand the system's monitoring range and recognition capabilities.

2.4 Product Specifications

Detection objectives	• Stop bar vehicle detection • Road users identification • Traffic event identification • Traffic data collection • HD video surveillance
Traffic data output	• Vehicle presence, traffic flow, occupancy, and road user identification • Identification of 80 different targets including truck, car, motorbike, bicycle, pedestrian

	• Event identification like fog, fire, illegal reversing on expressway, road congestion, vehicle abnormal driving event and accident detection	
Video	AI chip	NPU
	Sensor	1/1.8 inch, 5 megapixel large scene coverage
	Resolution	1080P, 1920*1080
	Lens	2.8-12mm
	Frame rate	10-25FPs
	Encoding formats	H.264, H.265
Functional indicators	Detection distance	150m
	Detection zone	Up to 32 detection zones and 32 virtual detectors
	Fill light mode	None
	Installation	Use of the existing pedestrian traffic light poles, vehicle traffic light poles, street light poles and any roadside structures
	Management	Automatic reset, operation status monitoring, embedded logging, remote batch upgrade, etc.
	Communication	RJ45*1, optional I/O*2
	Protocols	UDP/TCP
General features	Power supply	12VDC and POE 802.3af/at (Mode A)
	Power consumption	3W Max
	Operating temperature	-35°C to +74°C

	Operating humidity	0%-95%
	Dimension	85mm*80mm*218mm (W*D*H, including mounting bracket)
	Weight	700g (including mounting bracket)
	IP class	IP67

3. System Introduction

3.1 Login

To log into the system, follow these steps:

1. Open a web browser.
2. The default IP address is 192.168.0.126. Enter the IP address "192.168.0.126" in the address bar.
3. Press Enter to access the home page.
4. The default password is “123456”.
5. Click on the ">" button.

If the provided username and password are correct, you will be successfully logged into the system.

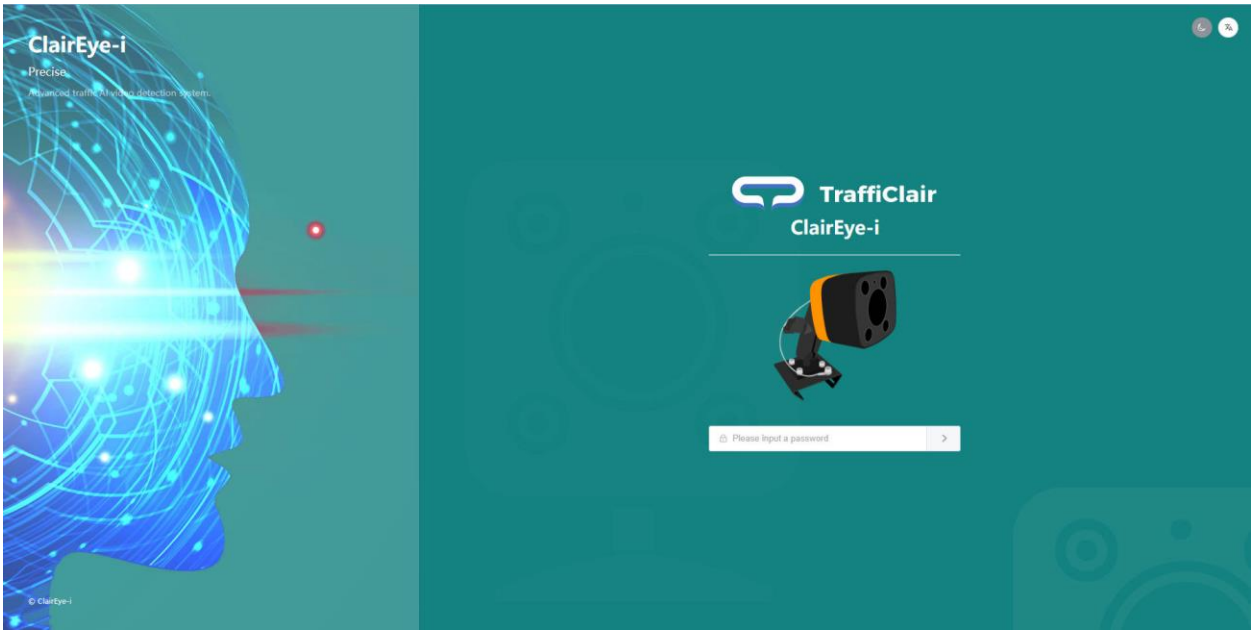


Figure 1: Welcome to the login.

6. The login interface specifically offers a dark mode option for nighttime use scenarios. In dark mode, the interface adopts a dark background with text colors automatically adjusted to light colors, providing a better browsing experience. The toggle button is located at the top right corner of the screen.

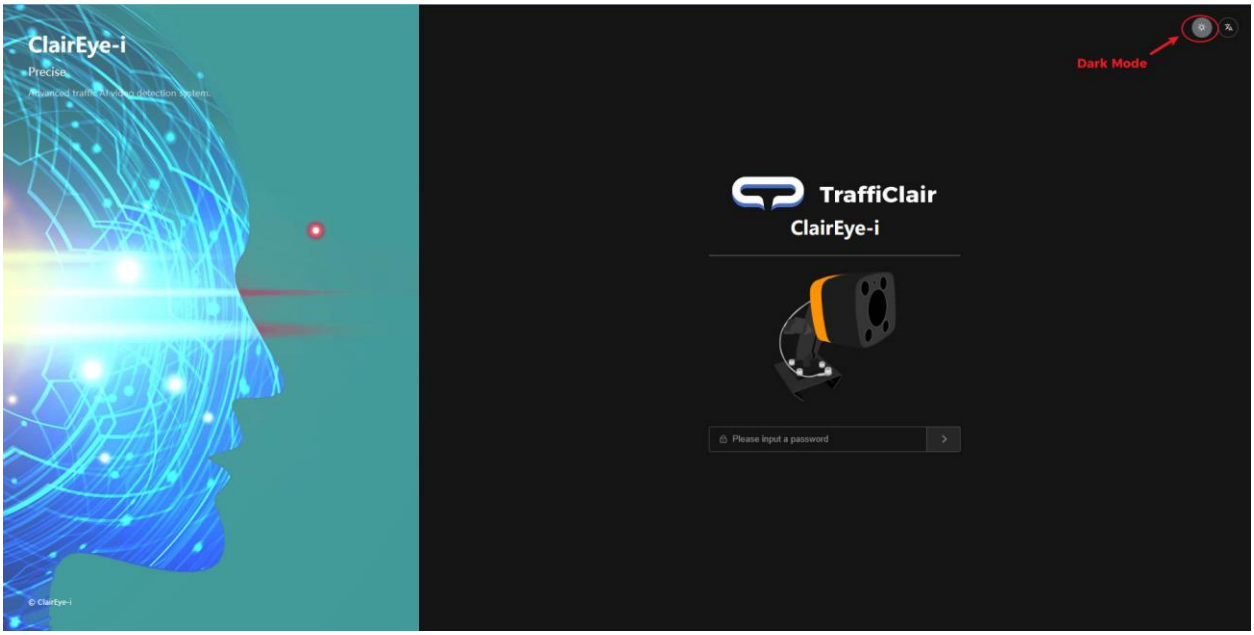


Figure 2: Dark mode toggle button.

7. You may also shift the language if needed with the other toggle button at the top right

corner of the screen.

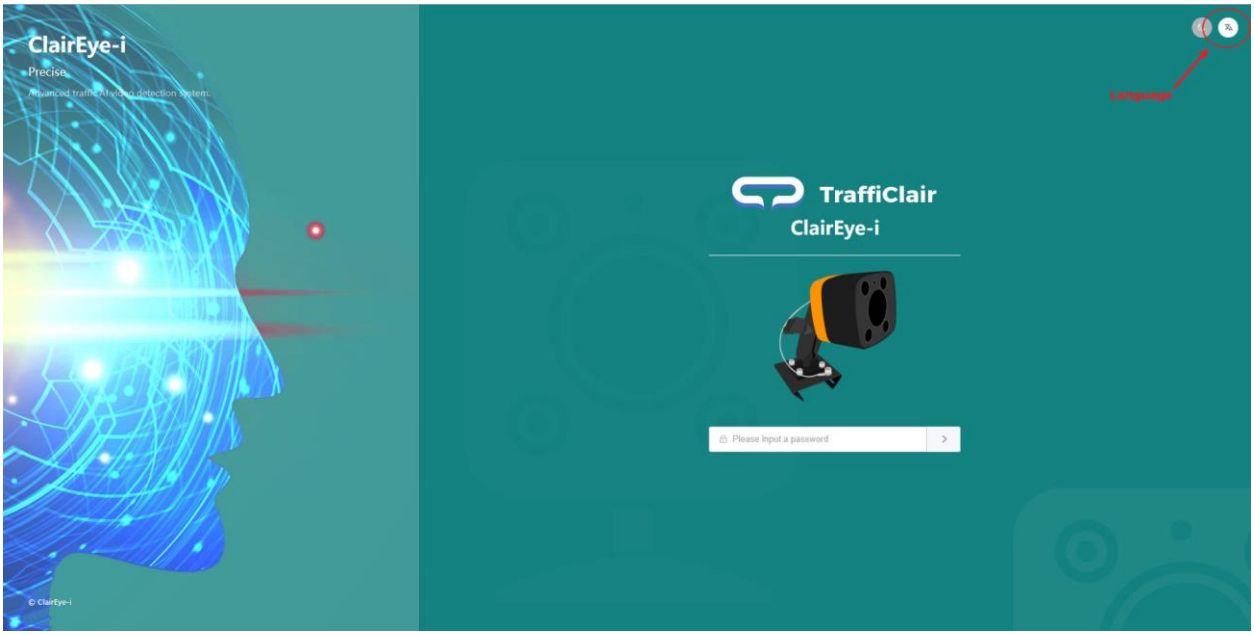


Figure 3: Language toggle button.

3.2 System interface

The main web interface is displayed once you log in, consisting of three main sections:

Section 1: Top Information

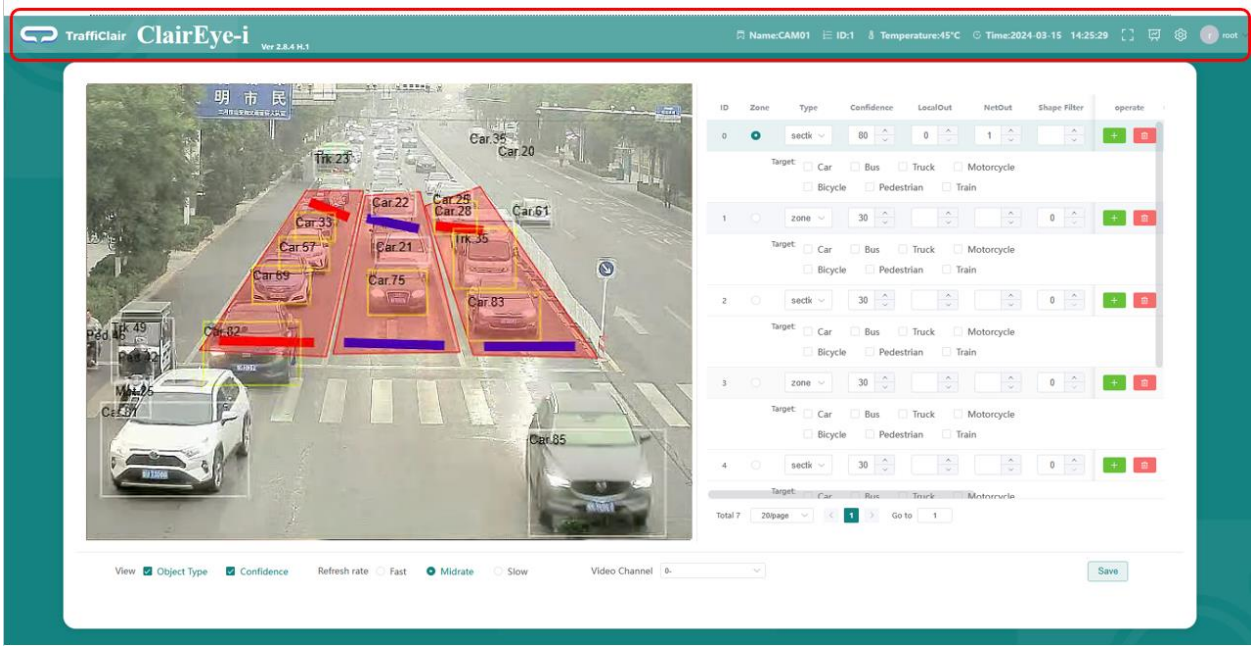


Figure 4: Top information section

At the top of the interface, you will find important details, including:

- System Name: ClairEye-i traffic video detector. Please note that by clicking on this area, which includes the TraffiClair logo and the ClairEye-i system name, you will be able to return to the home page after you finish configuring the system or analyzing data.
- Firmware Version: The current version of the firmware installed on the system.
- Device Name: A name assigned to the device for easy identification.
- Device ID: The unique identification number assigned to the device.
- Current Time: The current time displayed by the device.
- Temperature: The operating temperature of the device.
- Full Screen Button: Click to expand the display to full screen.
- Data Analysis: Navigate to the statistics interface for data analysis.
- System Settings: Access system configurations for setup.
- Login: Clear cache or log out of the system as needed.

Section 2: On the left-hand side is the video display section. In this area, users can select the target type and confidence level for the displayed content, adjust the refresh rate, and switch between video channels. Through these settings, users can customize the accuracy and real-time display of the video according to their preferences and needs.

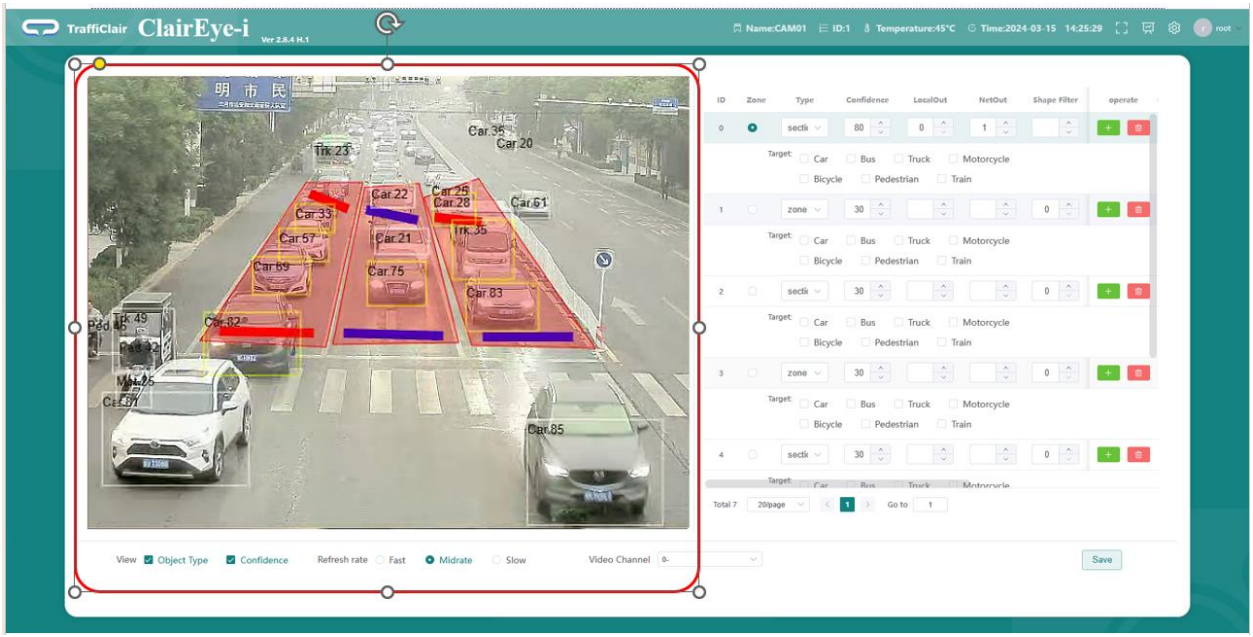


Figure 5: Video display section.

Section 3: On the right-hand side is the video configuration section. This section allows users to

configure the detection area and detection types for the video. The specific configuration options and parameters may vary depending on different application scenarios and requirements, but they are all designed to help users better adjust and apply the various functionalities of the video intelligent recognition device.

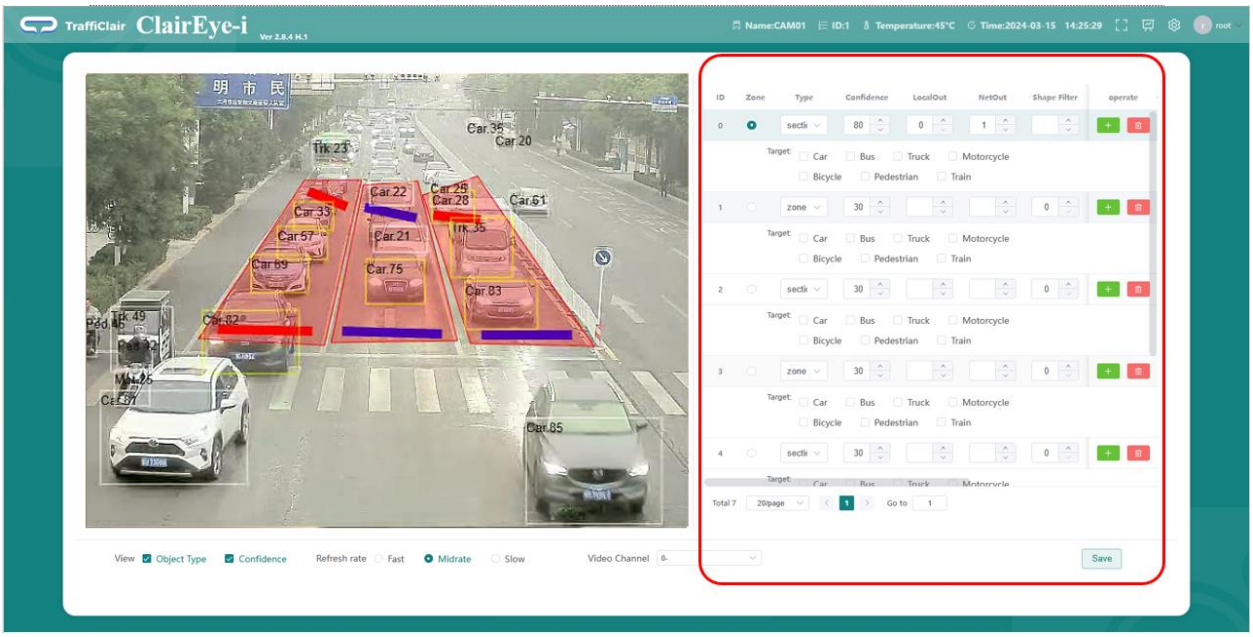


Figure 6: Video configuration section.

3.3 Video Configuration

1. Clicking on the "Zone" radio button in the video configuration section allows you to adjust the desired detection area. The detection area will be displayed in green.
2. Left-clicking on a numerical label enables you to select targets (highlighted in red).
3. By dragging the numerical labels of the detection area with the mouse, you can draw a custom region outline. Left clicking twice will add a new marker point.
4. Right-clicking on the numerical labels of the detection area allows you to delete the current marker point.
5. On the video configuration interface, the "Channel" option is used to switch between different video cameras.

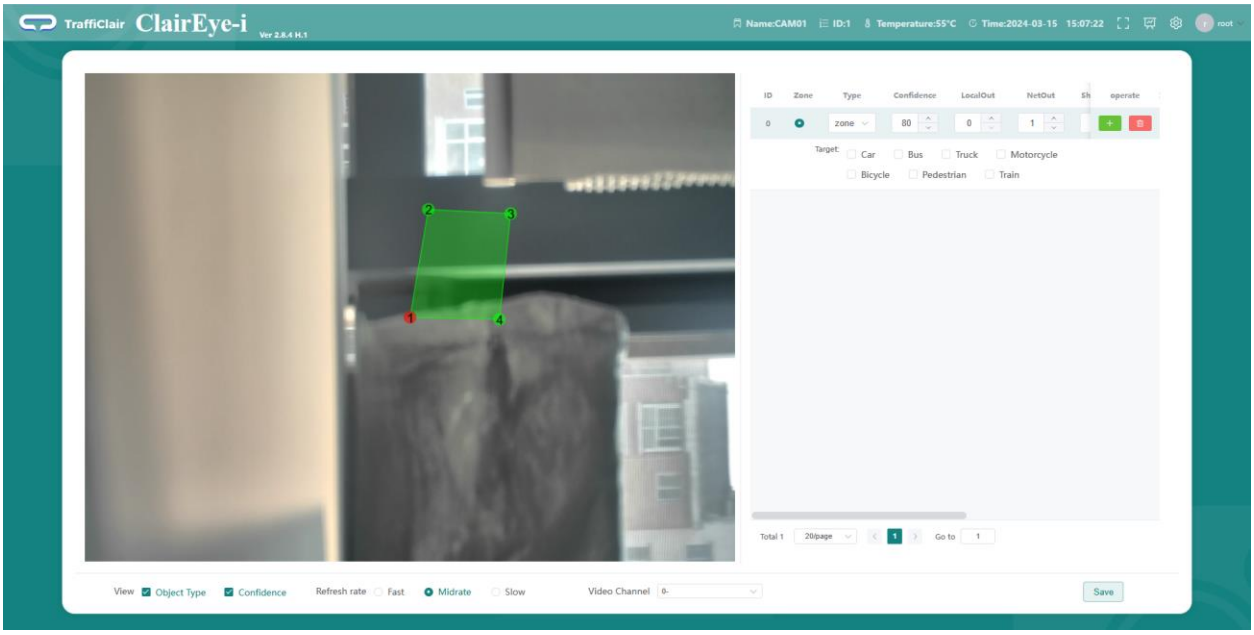


Figure 7: Defining the detection zone.

The video extension configuration interface allows for configuring detection types ("Type"), confidence level ("Confidence"), local output ("LocalOut"), network output ("NetOut"), target outlines ("Shape Filter"), trigger delay ("On Delay (s)"), cancel delay ("Off Delays"), normally open fault ("DFM ON"), normally closed fault ("DMF OFF"), and default status ("Default").

1. Clicking on the plus icon allows you to add new detection areas and configurations.
2. Clicking on the delete icon enables you to remove detection areas and configurations.
3. Below each row of detection configuration, you can select different detection targets, including Car, Bus, Truck, Motorcycle, Bicycles, Pedestrians, and Train (tram).
4. Clicking the save button allows you to save the modifications made to the detection areas and configurations.

The video configuration interface allows you to configure the following settings:

- **Type**: Specify the types of detections to be performed. Zone represents a detection zone, and section represents a detection bar.
- **LocalOut**: Defines the logical output port sequence number that the detection results output to the local area.
- **NetOut**: Defines the detector number that corresponds to the detection result when it is output over the network communication protocol.
- **Confidence**: The filtering criteria define the confidence threshold for detected targets. Detection results with confidence lower than this threshold will be ignored. The value ranges from 0 to 100 and the suggested default value is 30.
- **Shape Filter**: the shape filter is used to filter detected target contours based on their

aspect ratio, with a square having an aspect ratio of 100.

- **On Delay (S)**: Refers to the time duration (in seconds) after which an output of 1 is generated if the detection region remains continuously active (changes from 0 to 1) for that duration.
- **Off Delay (S)**: Refers to the time duration (in seconds) after which an output changes to 0 if the detection region remains continuously inactive (changes from 1 to 0) for that duration.
- **DFM On**: Refers to a malfunction that occurs when the detection region remains continuously in the state of 0 for a specific duration (in minutes).
- **DFM Off**: Refers to a malfunction that occurs when the detection region remains continuously in the state of 1 for a specific duration (in minutes).
- **Default**: Refers to the default value of the output when a fault occurs.

All above parameters are invalid when inputting 0.

By clicking on the "Save" button, you can save the modifications made to the detection regions and their configurations.

3.4 Data Analysis

Clicking on the Data Analysis button in the upper-right corner opens the system's data analysis functionality.



Figure 8: Data analysis

When dealing with key metrics such as traffic flow, occupancy rates, headways, speeds, and others, data analysis provides clear and intuitive visualizations to help us better understand and

utilize this data. In addition to visual data displays, data analysis also offers functionality to export corresponding data and images.

Here are the steps to use the data analysis:

1. Select the statistical date.
2. Choose the statistical time interval [15 minutes, 30 minutes, 1 hour, 1 day].
3. Select the statistical range [the range name can be customized, and the range content is either local output or network output ID number].
4. Click on "Query."

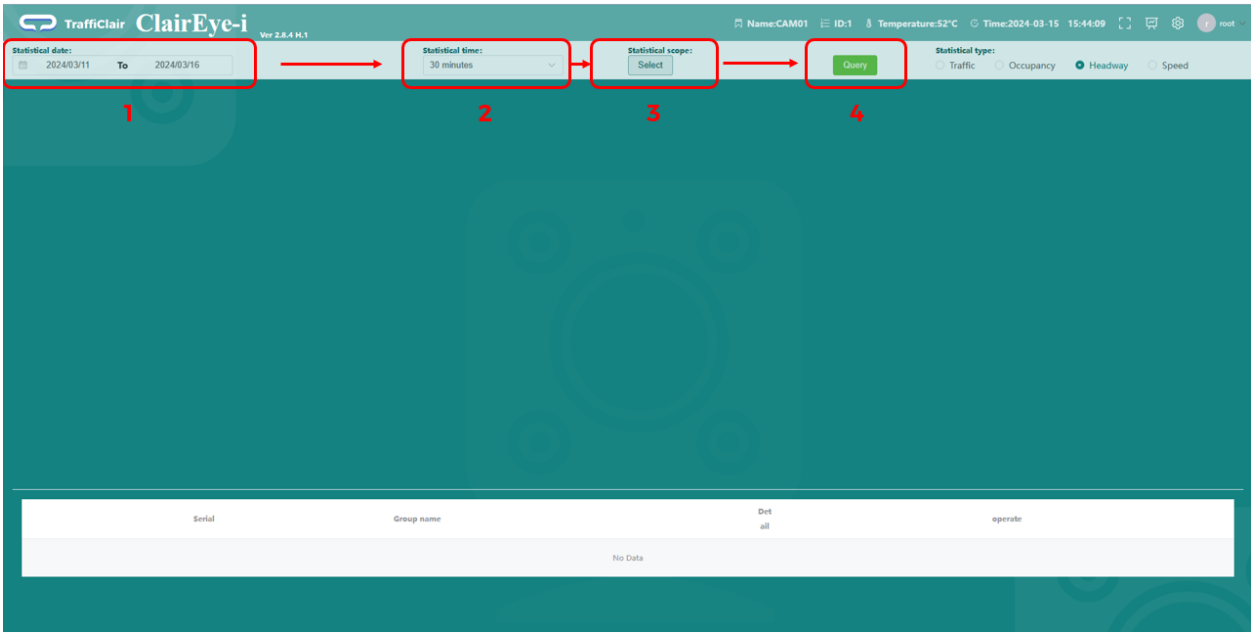


Figure 9: Query steps.

When selecting the range, you can add a template for direct selection next time.

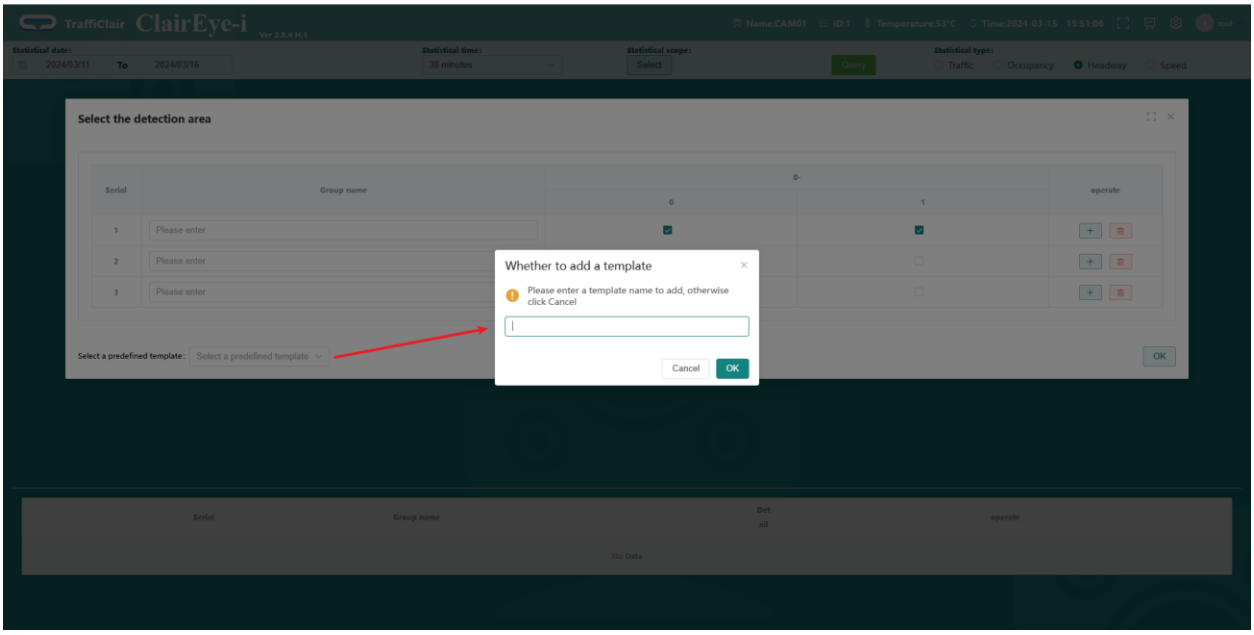


Figure 10: Add a template for the query.

3.5 System Settings

Clicking on the settings button in the upper-right corner opens the system configuration functionality.

3.5.1 Parameter Configuration

Parameter configuration allows users to adjust and configure various device parameters in detail. Through parameter configuration, device's normal operation can be ensured, and its performance can be optimized to adapt to specific application scenarios.

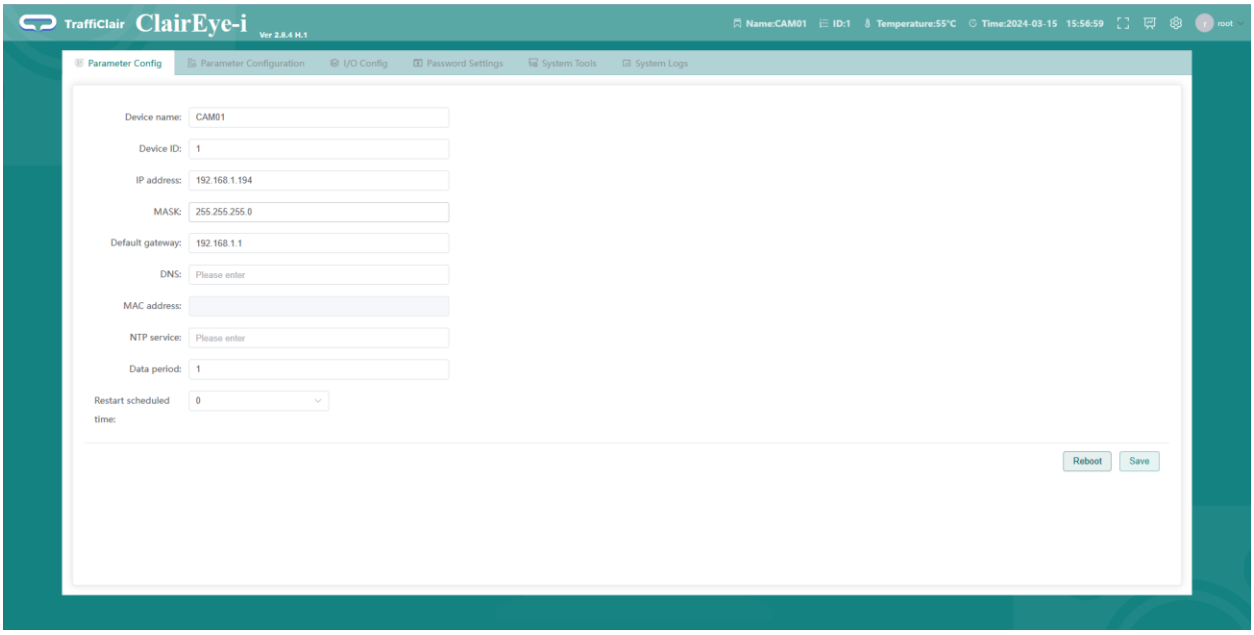


Figure 11: Parameter configuration.

Here are the main components and functionalities of parameter configuration:

1. Device Name: Users can assign a unique name to the device for identification and management within the system. The name can be customized according to user preferences.

2. Device ID: Each device has a unique identifier used for identification and tracking within the system. Users can assign a number to the device as needed.

3. IP Address: The IP address is a unique identifier for the device in the network, used for communication with other devices. Users need to assign a valid IP address to the device to ensure normal network communication.

4. Subnet Mask: The subnet mask is used to determine the subnet to which the device belongs and to identify hosts and routers in the network. Properly setting the subnet mask ensures that the device communicates with other devices in the same subnet.

5. Default Gateway: The default gateway is the router used by the device to access other networks. By setting the default gateway, the device can communicate with other networks.

6. DNS: The DNS is used to map the device's IP address to the corresponding domain name for easier access and management of the device.

7. MAC Address: The device's physical address is typically a unique MAC address used to identify

the device in the network. Users can set the device's physical address to ensure correct communication with other devices. By default, this item is not allowed to set.

8. NTP Service: The NTP service is used to synchronize the device's clock with the time of other network time servers. By enabling the NTP service, the device's time can be kept consistent with other network devices.

9. Data Period: The data period refers to the frequency or period at which the device transmits data. Users can set the data cycle as needed to better control the device's performance and data transmission rate.

10. Scheduled Restart: The scheduled restart feature allows users to set the device's restart time for regular system maintenance and updates. This helps maintain the device's performance and stability.

Upon completion of the above configuration modifications, saving will automatically restart the system to apply the changes.

3.5.2 Central Configuration

Central configuration allows users to adjust and configure various parameters related to the central server in detail. Through central configuration, stable communication and data transmission with the central server can be ensured to meet the system's requirements.

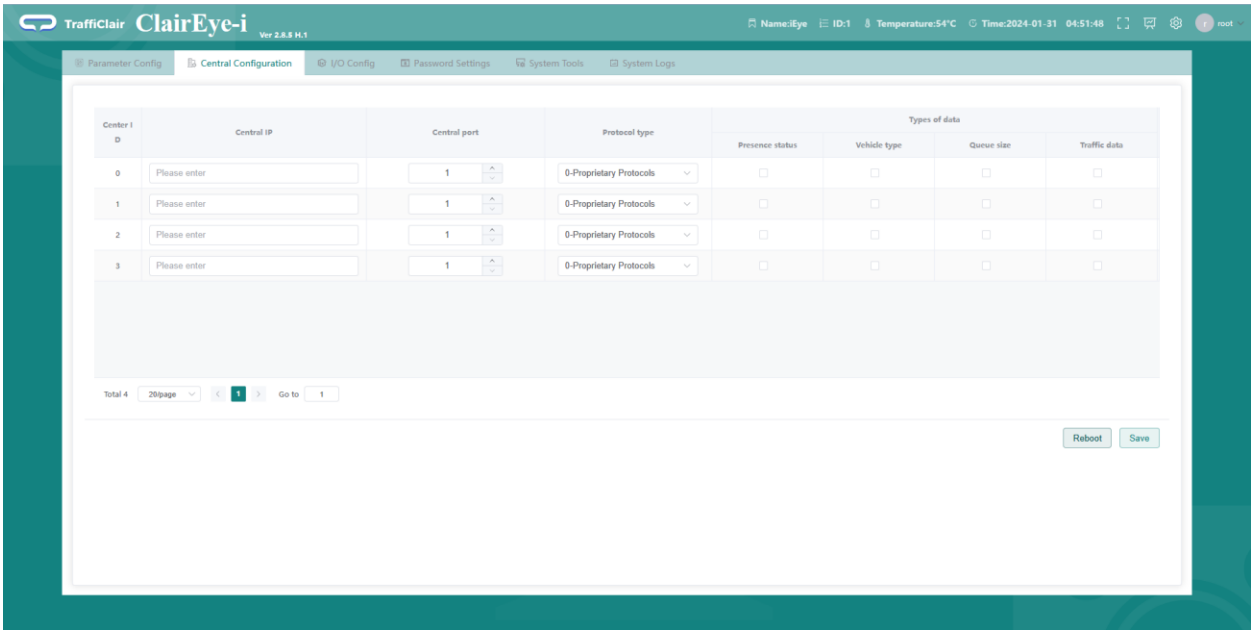


Figure 12: Central configuration

Here are the main components and functionalities of central configuration:

1. Central IP: Users need to provide the IP address of the central server to establish a network connection with it. Users can input the IP address into the configuration option, ensuring that the entered IP address is correct.

2. Central Port: Ports are protocol ports used by specific applications or services running on the server. In central configuration, users need to specify the port number used for communication with the central server. Ensure that the entered port number is correct to avoid communication errors.

3. Protocol Type: Protocols are standards or rules in network communication that specify how computers exchange information. In central configuration, users need to select the protocol type used for communication with the central server. Common protocol types include TCP, UDP, etc. Selecting the appropriate protocol type ensures stable communication with the central server.

4. Types of Data: Users can select the types of data to be reported in central configuration, including presence status, vehicle types, queue size, traffic data, etc. These data types can be selected and configured according to actual needs to meet the system's requirements for data collection and analysis.

Upon completion of the above configuration modifications, saving will automatically restart the system to apply the changes.

3.5.3 I/O Configuration

I/O configuration is a crucial aspect of system configuration, allowing users to adjust and configure various parameters related to I/O (Input/Output) based on their actual needs. These parameters include I/O ID (Input/Output Identifier) and IP addresses. By precisely configuring these parameters, stable communication and data transmission with I/O devices can be ensured, meeting the operational requirements of the entire system.

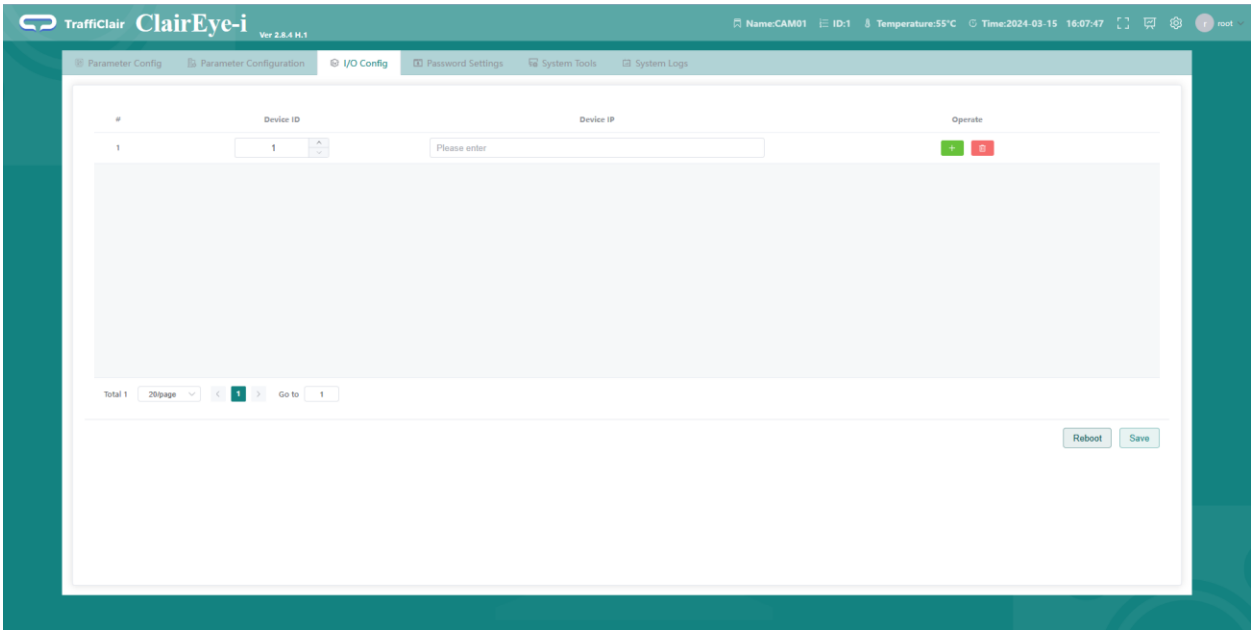


Figure 13: I/O configuration.

Here are the main components and functionalities of I/O configuration:

1. I/O ID Configuration:
   - Unique Identification: Each I/O device or interface requires a unique I/O ID to enable accurate recognition and communication by the system.
   - Configuration Flexibility: Users can assign I/O IDs based on the device's physical location, function type, or logical grouping to enhance configuration flexibility and manageability.

2. IP Address Configuration:
   - Static and Dynamic Allocation: IP addresses can be set as static or dynamically allocated. Static IP addresses are suitable for I/O devices requiring fixed addresses, while dynamic allocation is applicable to temporary connections or devices with high mobility.
   - Subnet Division: Depending on the system's scale and complexity, users may need to divide IP addresses into subnets to manage network traffic and security more effectively.

Upon completion of the above configuration modifications, saving will automatically restart the system to apply the changes.

3.5.4 Password Setting

Password setting allows for the protection of critical system information and data from

unauthorized access or tampering.

In the password setting, users need to input a password and confirm it. The system will verify the inputted password, and if it meets the security requirements, it will save and activate the password.

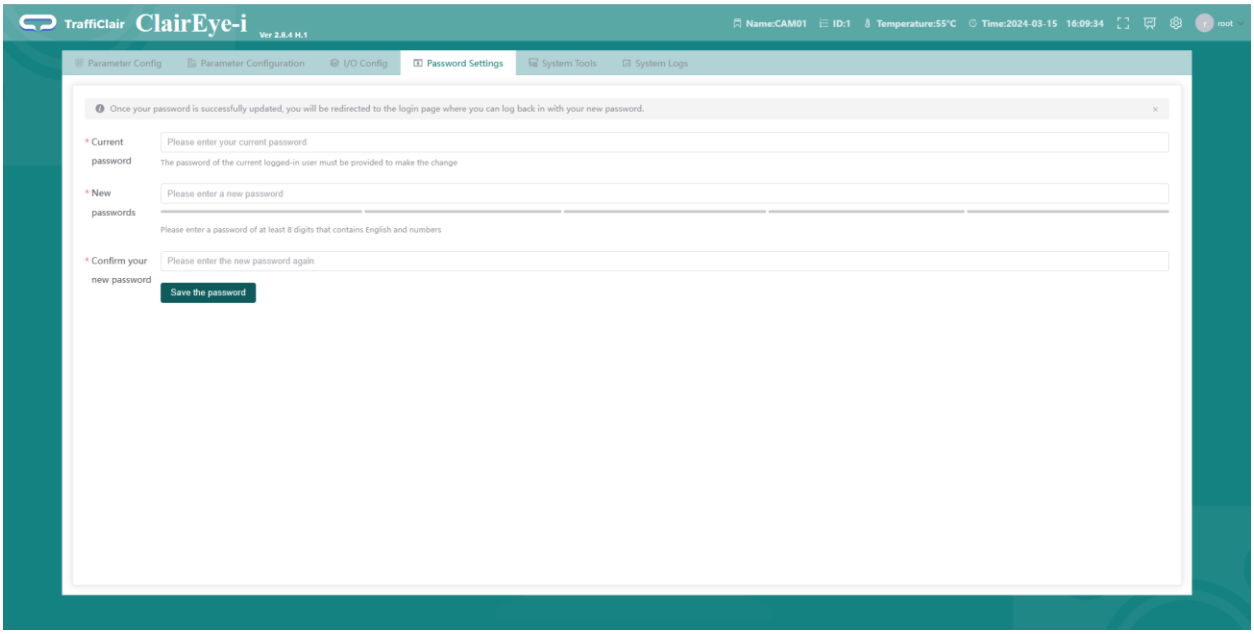


Figure 14: Password settings.

The functionalities of password setting include:

1. Password Strength Verification: The system will verify the strength of the inputted password to ensure it is sufficiently secure. Password strength typically includes requirements for password length, character types, and the presence of special characters.

2. Duplicate Password Verification: The system will verify whether the inputted password duplicates any previous passwords. If it does, the system will prompt the user to input a new password.

Upon completion of the password setting, saving will ensure that the password is effective and active.

3.5.5 System Tools

The system offers various functionalities, including factory reset, system upgrade, and ping

function. These features enable users to better manage and maintain the system, ensuring its stable operation and optimal performance.

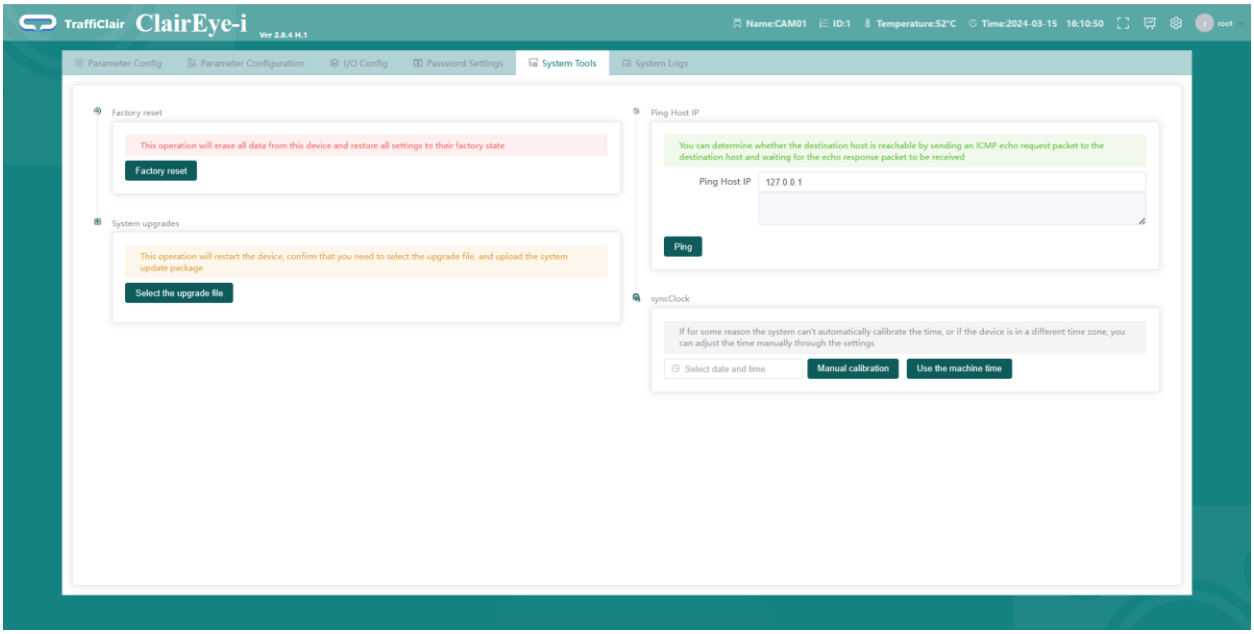


Figure 15: System tools.

1. Factory Reset:
Factory reset is a crucial option in the system's functionality, allowing the system to be restored to its default settings as it was when initially manufactured. This function is useful in case of system malfunctions or when users wish to reset the system. Factory reset clears all user data and configuration settings, resetting the system parameters to their default values. This feature helps restore the stability and normal operation of the system while also safeguarding user privacy and data security.

2. System Upgrade:
The system upgrade function enables users to update and upgrade the system to obtain better performance and additional features. Through system upgrade, users can acquire the latest software versions, fix potential vulnerabilities and errors, and add new functionalities and features. System upgrade helps improve the stability and reliability of the system while also meeting users' requirements for system performance.

3. Ping Function:
The ping function is one of the network diagnostic tools used to test the normality of network connections. Through the ping function, users can send ICMP echo request messages to the target host and wait for their ICMP echo reply messages. This function helps detect network connectivity, determine network latency, and packet loss situations. The ping function is highly useful in network management and troubleshooting, helping users diagnose network issues and

take appropriate measures.

4. Manual Time Calibration:
The manual time calibration function allows users to directly manipulate the system's clock settings, adjusting hours, minutes, seconds, and other time units precisely. In the system's settings interface, within the clock management module, users can perform these operations through a graphical interface.

3.5.6 System Logs

System logs are records of information regarding hardware, software, and system issues within the system, while also serving to monitor events occurring within the system. By querying system logs, users can investigate the causes of errors that occur.

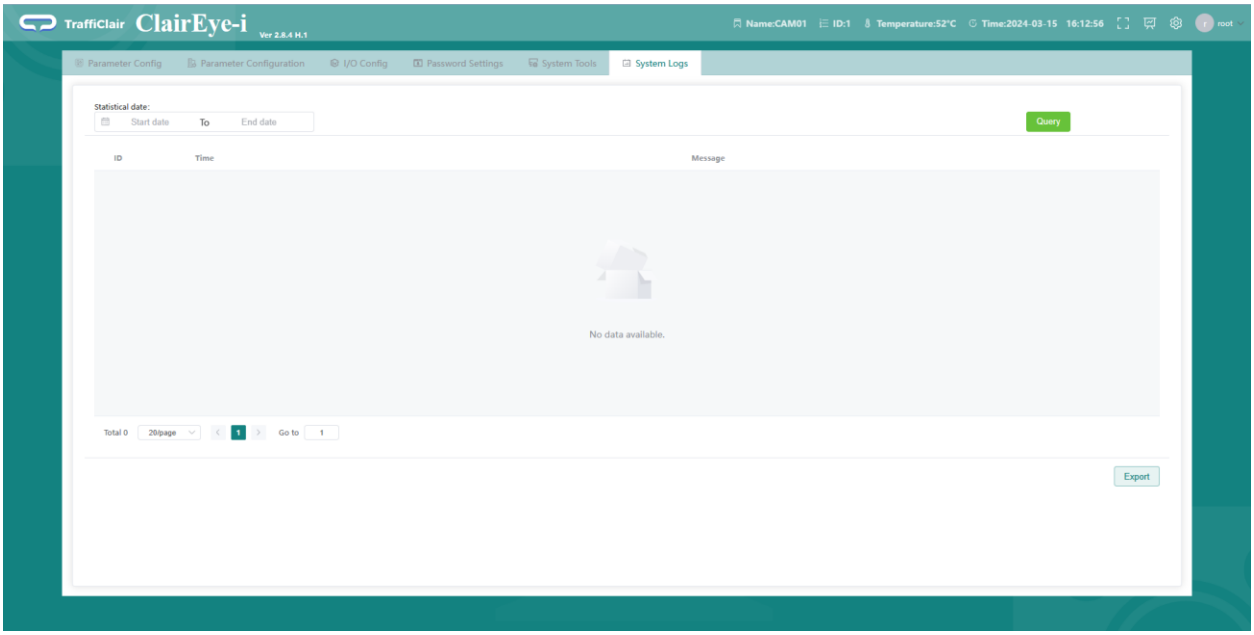


Figure 16: System logs.

3.5.7 Object Portion Settings

Certain firmware versions support object portion settings, which can significantly enhance detection accuracy, especially for pedestrian detection. By configuring the portion of the object to focus on, you can optimize performance. For instance, focusing on a pedestrian's foot can

improve accuracy by ensuring detection occurs precisely when the foot enters the detection zone.

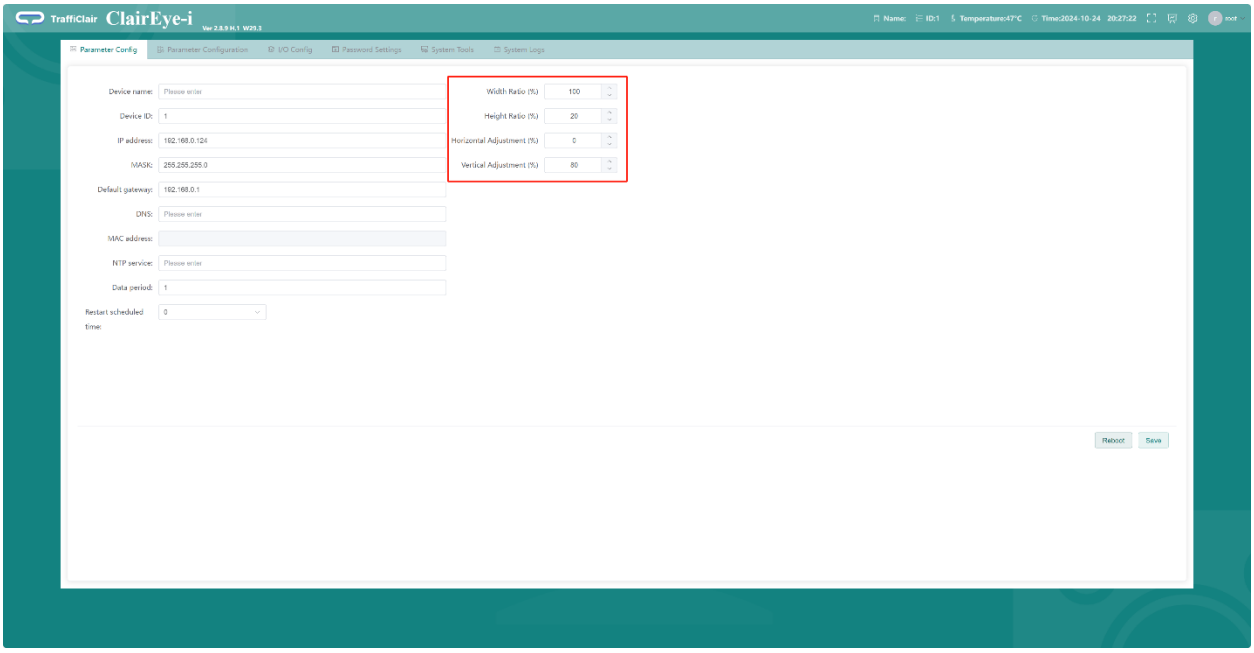
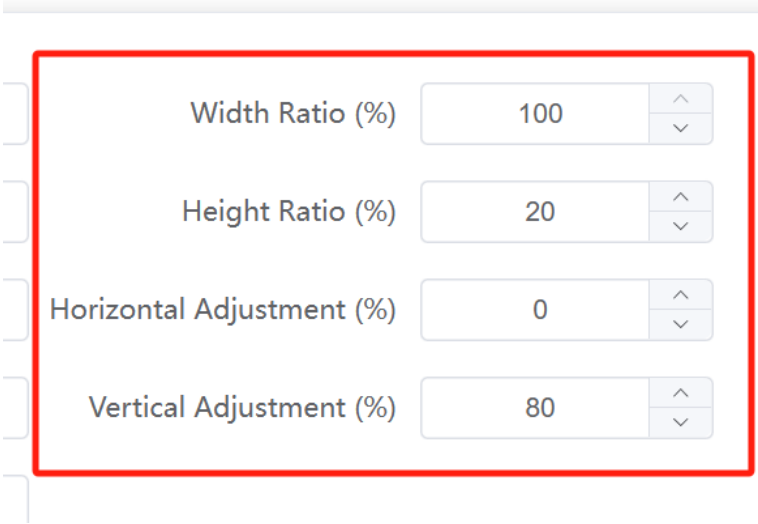


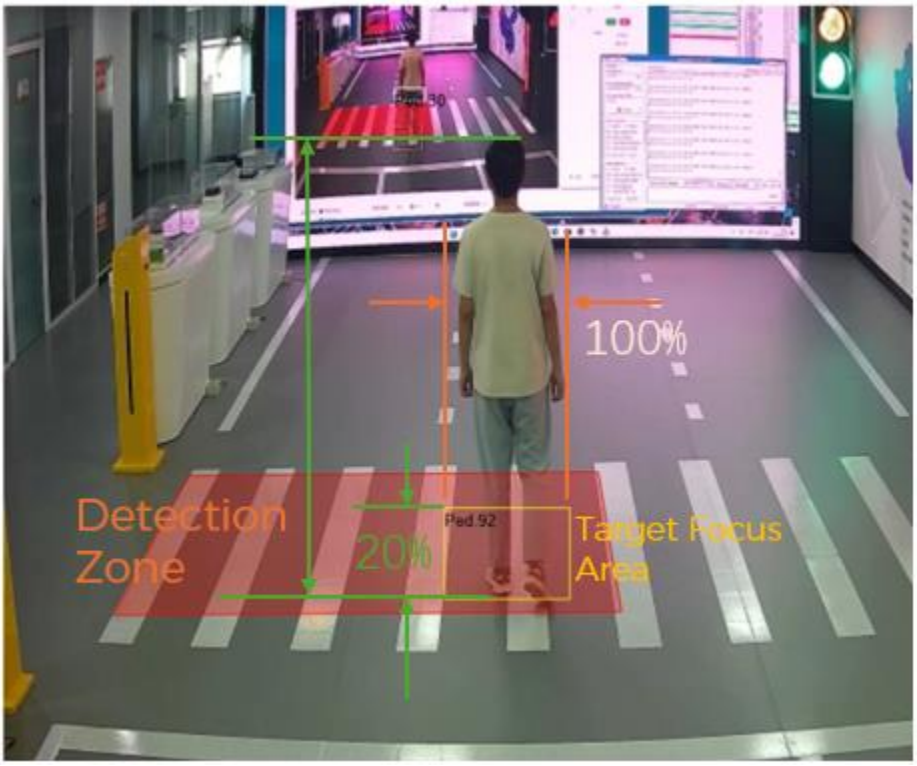
Figure 17: Object portion settings.



In above settings:

- The target focus area occupies 100% of the object's total width, and 20% of the object's total height.
- The horizontal adjustment for the target focus area is set to 0, starting from the left edge and extending to the right.
- The vertical adjustment for the target focus area is set to 80%, starting from the top and extending downward.

-



4. Communication Protocols

- Basic protocol: UDP
- Communication method: active upload
- Configuration information: IP address of the signal controller, data port of the signal controller
- Datagram format

Byte sequence number	Length	Content	Description
0	1	0xFE	Header flag
1	1	2	Detector type: 1- loops 2- video 3- geomagnetic 4- radar 5- ultrasonic 6- infrared
2	1	DataType	Data type:

			0- presence state 1- car type 2- queue 3- traffic data
3	2	Hbyte*127+Lbyte	Data length *
5	1	Num	The number of detectors that the data body contains
6	1	No	Detector numbering
7	1	State	Detector data, which expresses different meanings depending on the type of data. 0- presence 1byte: Less than 32 indicates the detector's status in the past second; greater than or equal to 32 indicates a fault; greater than or equal to 64 indicates no video. 1-car type:1byte 2-queue:1byte 3-traffic data: 2byte volume + 1byte occupancy + 1byte headway + 1byte speed
...			
5+2*Num	1	0xff	End flag

The datagram uses 7-bit format except for the first and last bytes, that is, all byte values are less than or equal to 0x7F.

- Datagram example

Byte sequence number	Length	Content	Description
0	1	0xFE	Header flag
1	1	2	Detector type: 2-Video
2	1	0	Detector presence status
3	2	0x00 0x5	Data length 6 bytes
4	1	2	Detector number: 2
5	1	1	Detector numbering: 1

6	1	1	Detector status: 1
7	1	2	Detector numbering: 2
8	1	0	Detector status: 0
9	1	0xff	End flag