



User's Manual

AI Surveillance Station

▶ AIS-1000



Copyright

Copyright © 2026 by PLANET Technology Corp. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written permission of PLANET.

PLANET makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not PLANET, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, PLANET reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

All brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.

EU Representative

PLANET Technology Europe B.V.

Address: Posthoornstraat 11, 3011 WD Rotterdam, NL

Email: eu_rep@planet.com.tw

URL: www.planet.com.tw

FCC Caution

To assure continued compliance, use only shielded interface cables when connecting to computer or peripheral devices. Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Federal Communication Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20 cm (8 inches) during normal operation.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

CE Mark Warning

This device is compliant with Class A of CISPR 32. In a residential environment this equipment may cause radio interference.

WEEE Regulation

To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste and have to collect such WEEE separately.

Energy Saving Note of the Device

This power required device does not support Standby mode operation.

For energy saving, please remove the AC-plug to disconnect the device from the power circuit.

Without remove the AC-plug or switch off the device, the devices will still be consuming power from the power circuit.

In the view of Saving the Energy and reduce the unnecessary power consuming, it is strongly suggested to switch off or remove the DC-plug for the device if this device is not intended to be active.

Revision

User's Manual of PLANET AI Surveillance Station

Model: AIS-1000

Rev: 1.0 (April, 2026)

Part No. EM-AIS-1000_v1.0

Declaration

Copyright ©2026. All rights reserved.

Without the written permission of the company, any company or individual should not extract, duplicate part of or all of contents of this manual and no spreading in any form.

As the upgrade of the products or other reason, the contents of manual will be upgraded periodically. Unless otherwise stipulated, the manual is used as a NOTE. All statements, information and suggestions of the manual do not constitute any ostensive or implied guarantee.

Photographs, graphics, charts, and illustrations provided in the manual are for explanation and illustration purposes only, and may differ from specific products. Please prevail in kind.

Safety Precautions



CAUTION

- Please do not place and install equipment directly under the sunlight or near heating device.
- Please do not install equipment at moist place or place with dust or soot.
- Please keep equipment installed horizontally, or install equipment in a stable place, avoid the equipment falling down.
- Please avoid liquid dropping on the equipment, make sure no objects filled (eg cups) with liquid on the equipment and prevent liquid from leaking.
- Please install the device in a well-ventilated place, do not block the vents of the equipment.
- Please only use equipment within rated input/output.
- Please do not disassemble at liberty.
- Please transport, use and reserve the equipment within allowing humidity (10%~90%) and temperature (0°C ~50°C).
- When cleaning the device, unplug the power cord and completely shut off the power.
- The dust on the circuit board inside the AI box may cause a short circuit after being exposed to moisture. Regularly clean the circuit board, connectors, chassis, and chassis fan with a soft brush. If dirt is difficult to remove, wipe it off with a neutral detergent diluted in water and wipe it dry.
- Do not use volatile solvents such as alcohol, benzene, or thinner when cleaning the device. Do not use strong or abrasive cleaning agents. This can damage the surface coating.
- Please purchase the AI box dedicated hard drive recommended by the equipment manufacturer from the formal channels to ensure the quality and usage requirements of the hard drive.
- Make sure that there is no threat due to uneven mechanical load.



WARNING

- Please do use recommended cord sets (power cords), do use within the rated specifications.
- If you connect the product to the Internet at your own risk, including but not limited to products that may be subject to cyber-attacks, hacking attacks, virus infections, etc., the company will not be responsible for product abnormality, information leakage, etc., but the company will timely to provide you with product-related technical support.

Contents

Chapter 1 Product Introduction	7
1.1 Product Overview	7
1.2 Features.....	11
1.3 Product Specifications	12
1.4 Package Contents	14
Chapter 2 Hardware Description	15
2.1 Front Panel	15
2.2 Rear Panel.....	15
2.3 Side Panel	16
Chapter 3 Getting Started	17
3.1 System Requirements	17
3.2 Discover Device (IP Address Detection).....	17
3.3 Login Procedure	18
Chapter 4 System Configuration.....	19
4.1 Dashboard	19
4.2 Settings.....	20
4.2.1 General Settings.....	20
4.2.2 Time Zone Settings	23
4.2.3 Certificate Download	24
4.2.4 License Update	25
4.2.5 Update Model	26
4.2.6 Software Update.....	27
4.3 Network Settings.....	30
4.4 Media Settings	32
4.4.1 NVR Settings	32
4.4.2 Camera Settings.....	34
4.4.3 Camera Management.....	38
4.4.4 Camera AI Settings	40
4.5 AI Settings.....	43
4.6 Notification Settings	45
4.6.1 Email Settings.....	45
4.6.2 Webhook Settings	46
4.6.3 On-Screen Notification Settings	47
4.6.4 Event Notification Settings	47
4.7 List Settings	49
4.8 Health Status	50
4.8.1 Monitoring Items	50
4.9 User Management	51
4.9.1 User Roles.....	51
4.9.2 Add a New User	51
4.9.3 Edit and Delete Users	51
4.9.4 User Permissions	52
Chapter 5 Web Interface Overview.....	55
5.1 Dashboard	55

5.2 Events	58
5.2.1 Page Overview	58
5.2.2 Event Filtering and Search	58
5.3. Live View	60
5.3.1 Page Overview	60
5.4 Smart Playback.....	61
5.4.1 Search Criteria.....	61
5.5 AI Chatbot	62
5.6 Health Status	63
5.6.1 Monitoring Metrics	63
5.6.2 Interpretation Guidelines	63
5.6.3 Best Practice	63
5.7 Report	65

Chapter 1 Product Introduction

1.1 Product Overview

Empowering Existing Surveillance with AI Intelligence

PLANET AI Surveillance Station is designed to seamlessly enhance existing surveillance infrastructures by introducing intelligent video analytics at the edge. While preserving existing surveillance infrastructure, it enables organizations to upgrade traditional surveillance into a smarter, more responsive security framework. By integrating directly into existing network environments, businesses can simplify deployment and improve operational efficiency.



Real-Time AI Detection for Smarter Security Operations

Equipped with advanced AI capabilities, the system delivers real-time detection across a wide range of scenarios, including:

- Illegal vehicle entry detection
- Vehicle timeout / stay detection
- Line-crossing detection
- Area intrusion detection
- Crowd counting detection
- Loitering time detection
- Cat and dog detection
- Whitelist/blacklist face recognition
- Helmet and safety vest detection
- Fire and smoke detection



It enabling comprehensive situational awareness across diverse environments such as factories, campuses, and commercial spaces. These AI-driven insights help security teams respond faster and operate more efficiently.

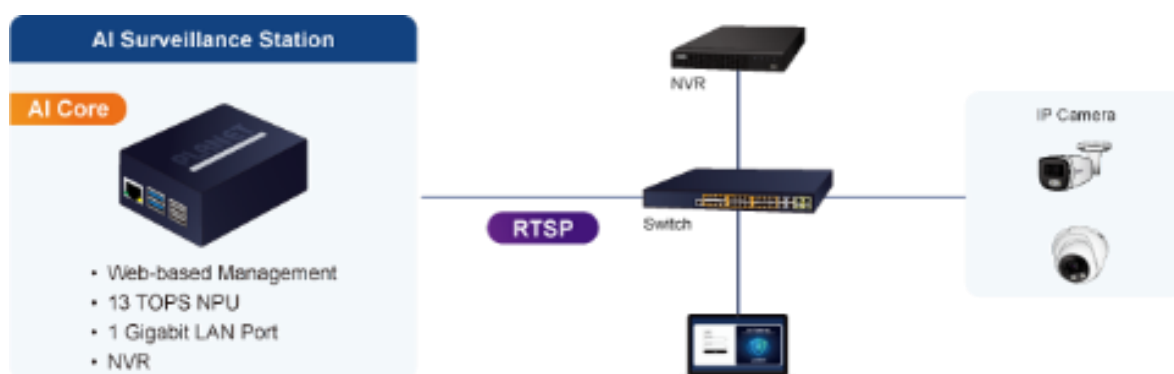


Centralized AI Event Hub for Efficient Management

At the core of the system is a centralized management platform that consolidates all AI detection results into a unified event hub. Through an intuitive dashboard, users can monitor live video streams, review recent events, and manage alerts in real time. The platform enables efficient event handling, allowing operators to quickly identify critical incidents and take action with improved operational visibility.

Centralized AI Surveillance Management

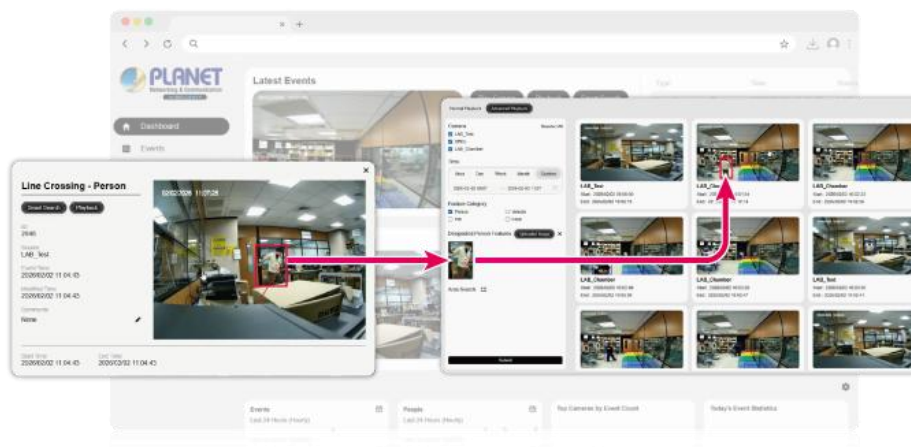
Unified Platform · Easy Deployment · Real-Time Insights



Streamlined Investigation with Intelligent Playback and Search

The AI Surveillance Station enhances video investigation workflows by enabling event-based playback, object tracking, and attribute filtering. Users can quickly locate relevant footage through structured filtering methods such as human detection, region-based search, and feature matching. This significantly reduces the time required for incident investigation while improving search accuracy and usability.

Object Tracking in Playback



Flexible Deployment with Edge AI Architecture

Built on an edge AI architecture, the system performs video analysis locally, reducing bandwidth consumption and alleviating the need for centralized computing resources. It can operate as a standalone AI node or be deployed across distributed environments, providing flexibility for different scales of surveillance applications. This modular approach allows organizations to expand their AI capabilities gradually as needs evolve.

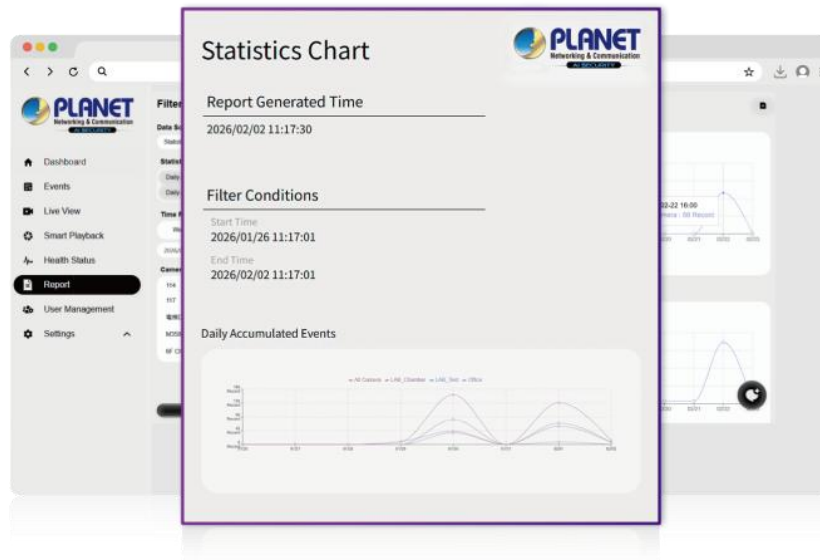
Advanced Automation and Integrated Security Applications

Beyond detection and monitoring, the system supports advanced automation capabilities such as virtual patrol and intelligent video playback analysis. It can also be integrated with access control systems, enabling integration with external access control systems, to enhance overall security management. These capabilities extend the value of surveillance systems from passive monitoring to proactive security operations.

Enhancing Legacy Systems with Future-Ready AI

By bridging traditional surveillance systems with modern AI technologies, PLANET AI Surveillance Station transforms legacy infrastructure into an intelligent security solution. Organizations can extend system lifespan, improve operational efficiency, and gain deeper insights from video data—all while preparing for future smart security applications.

Auto Report Generation



1.2 Features

Hardware

- High-performance 64-bit quad-core CPU for real-time AI video analytics
- Built-in 13 TOPS AI acceleration engine for real-time edge AI inference
- 1TB NVMe SSD storage for high-speed storage of video metadata and event records
- 1 × Gigabit Ethernet interface for high-bandwidth video transmission
- Ultra-compact device size (88.7 × 68.2 × 41 mm) for flexible installation in limited spaces
- Operating temperature range 0 ~ 50°C suitable for various indoor monitoring environments
- Low-power edge AI device suitable for continuous surveillance operation

AI Video Analytics

- Real-time object detection and behavior analysis through edge AI inference
- Supports intelligent event detection including intrusion detection, line-crossing detection and loitering detection
- AI visual recognition capabilities including helmet, reflective vest, mask detection
- Supports smoke and fire detection for early hazard identification
- Built-in pet recognition (cat and dog detection) for specialized monitoring scenarios
- Simultaneous analysis of multiple video streams for improved surveillance coverage

Intelligent Video Search

- Supports efficient video search through structured filtering and event-based queries
- Enhances video investigation efficiency compared with manual timeline browsing
- Enables rapid retrieval of relevant video segments based on detected events and attributes

System Integration

- Compatible with RTSP IP cameras from various manufacturers
- Supports integration with existing IP surveillance systems
- Enables cost-effective upgrade of conventional surveillance systems to AI-powered monitoring

Management and Deployment

- Web-based management interface for system configuration and monitoring
- Designed for flexible edge deployment in distributed surveillance environments
- Supports centralized monitoring and intelligent event management (AI Event Hub)
- Compact edge AI platform suitable for industrial, retail, campus and smart city applications

1.3 Product Specifications

Product	AIS-1000
Hardware Specifications	
CPU	64-bit Quad-core ARM Cortex-A76 @ 2.4GHz
AI Accelerator	Hailo-8L (13 TOPS)
GPU	Broadcom VideoCore VII
Internal Storage	1TB NVMe SSD
Memory	8GB SDRAM
Networking Interface	1 × 10/100/1000T Gigabit Ethernet (RJ45)
Button	> 10 sec: system shutdown
USB Port	2 x USB 3.0 ports 2 x USB 2.0 ports
Operating Temperature	0 to 50 degrees C
Power Interface	USB Type-C power input
Power Input	5V/5A DC via USB Type-C power connector
Power Consumption	Max. 27W
Enclosure	Metal enclosure
Installation	Desktop and wall-mount
Dimensions (W × D × H)	88.7 × 68.2 × 41 mm
Weight	0.287 kg
Camera and NVR Compatibility	
Camera Compatibility	RTSP IP camera support
Max. Channels	8-channel IP cameras
NVR	Built-in video recording capability
AI Function	
Parking Detection	Illegal Vehicle Intrusion / Idle Timeout Detection
Human Detection	Line Crossing / Area Intrusion / Crowd Counting
Pet Detection	Cats & Dogs
Face Recognition	Whitelist / Blacklist
Industrial Safety Detection	Helmet / Vest
Fire & Smoke Detection	Fire & Smoke
Smart Search System	Object Filtering / Area Detection / Feature Matching (Human / Vehicle / Pet) / Vehicle Attribute Search (e.g., color, type) / Interactive Search Enhancement (LLM-based concept)
Management Functions	
Management Interface	HTTP
System Management	AI parameter configuration Camera IP/device name configuration Camera event parameter configuration

	Firmware upgrade by HTTP protocol through Ethernet network Configuration upload/download through HTTP NTP System reboot
System Monitoring	CPU/RAM/GPU utilization monitoring Export logs and error reports
AI Model Management	AI model upload/update interface Model version rollback
Event Management	Event/alarm condition configuration Trigger actions (notification/recording)
Real-time Display	Homepage real-time event display Event details with live video stream Incident processing record window
Playback	Event log playback Event replay
Monitoring View	Multi-camera NVR-style interface Multi-screen / single-screen switching Historical person-fragment search
Intelligent Platform	Search-based playback query interface Integrated homepage search optimization
Historical Data	Historical event record query Report generation
User Management	Permission control
Video Compression	H.264 / H.265 H.264+ / H.265+
Video Streaming	RTSP (Sub-stream only)* Resolution: Up to 704 × 576 (D1) Frame Rate: Up to 10 fps Compression: H.264 / H.265 / H.265+ (H.265+ supported for optimized streaming)
Recording Performance	8-channel simultaneous recording Up to 1080P Full HD recording @ 25/30 fps (per channel) Supports 960P / 720P / D1
Security Management	Secure Web Access via HTTPS (TLS 1.3 encryption) Service Port Control (only essential services enabled)

1.4 Package Contents

Please verify the contents inside the package box.

- AIS-1000
- QR code sheet
- Type-C Power Adapter



Note

If any of the above items are missing, please contact your dealer immediately.

Chapter 2 Hardware Description

2.1 Front Panel



No.	Name	Description
A	RJ45 Ethernet Port	10/100/1000BASE-T Gigabit Ethernet port for network connection
B	USB 3.0 Port *2	USB 3.0 ports for connecting USB storage devices or supported USB peripherals
C	USB 2.0 Port *2	USB 2.0 ports for connecting keyboard, mouse, or supported USB devices

2.2 Rear Panel



No.	Name	Description
D	Recessed Power Button	Used to turn the device ON or OFF. Insert a pointed object (such as a pin) into the hole to press the button.
E	Power LED (PWR)	Indicates power status • ON: Device is powered on • OFF: No power input

2.3 Side Panel



No.	Name	Description
F	Power Input (USB Type-C)	USB Type-C port for DC power input
G	Reserved Interface	Reserved for future use (no function by default)



CAUTION

For optimal performance and reliability, please use the **power adapter provided with the device**.

The use of non-certified or incompatible power adapters may cause system instability, abnormal operation, or potential hardware issues.

Chapter 3 Getting Started

3.1 System Requirements

To ensure optimal performance of the AIS-1000 system and a better user experience, it is recommended to access the system using the following software environment:

- **Supported Web Browsers:**
Google Chrome (recommended), Mozilla Firefox, Microsoft Edge (Chromium-based)
Please ensure your browser is updated to the latest version.
- **Recommended Resolution:**
1920 × 1080 (Full HD) or higher

3.2 Discover Device (IP Address Detection)

If the IP address of the AIS-1000 is unknown, especially when operating in DHCP mode, you can use a device discovery tool to locate the system on the network.

The following steps guide you through using the IP Discovery Tool:

Step 1:

Download and install the IP Discovery Tool on your PC.

Step 2:

Run the utility. The main interface will appear, displaying available network interfaces.

Step 3:

Select the correct network adapter connected to the same LAN as the AIS-1000, then click **“Refresh”** to scan for devices.

Step 4:

Locate the AIS-1000 in the device list based on its **Device Name**, or **IP Address**.

Step 5:

Click **“Connect to Device”** to open the web login page of the AIS-1000.

Note

- The AIS-1000 may obtain an IP address automatically from a DHCP server.
If the IP address is unknown, the Planet Smart Discovery Utility can be used to identify the device on the network.
- Ensure that your PC and the AIS-1000 are connected to the same network segment.
- Disable firewall or security software temporarily if the device cannot be discovered.

3.3 Login Procedure

Please follow the steps below to log in to the system:

Step 1: Open a web browser (Google Chrome is recommended), and enter the system IP address in the address bar.

For example: `https://192.168.0.20`

Step 2: After accessing the login page, enter the username in the “**Username**” field.

(Default username: admin / password: admin)

For first-time login, the system will require you to change the password.

The new password must contain 8 to 31 characters, including uppercase letters, lowercase letters, numbers, and symbols. Spaces are not allowed.

Step 3: After confirming that the username and password are correct, click the “Login” button.

Step 4: Once authentication is successful, the system will automatically redirect to the dashboard page.

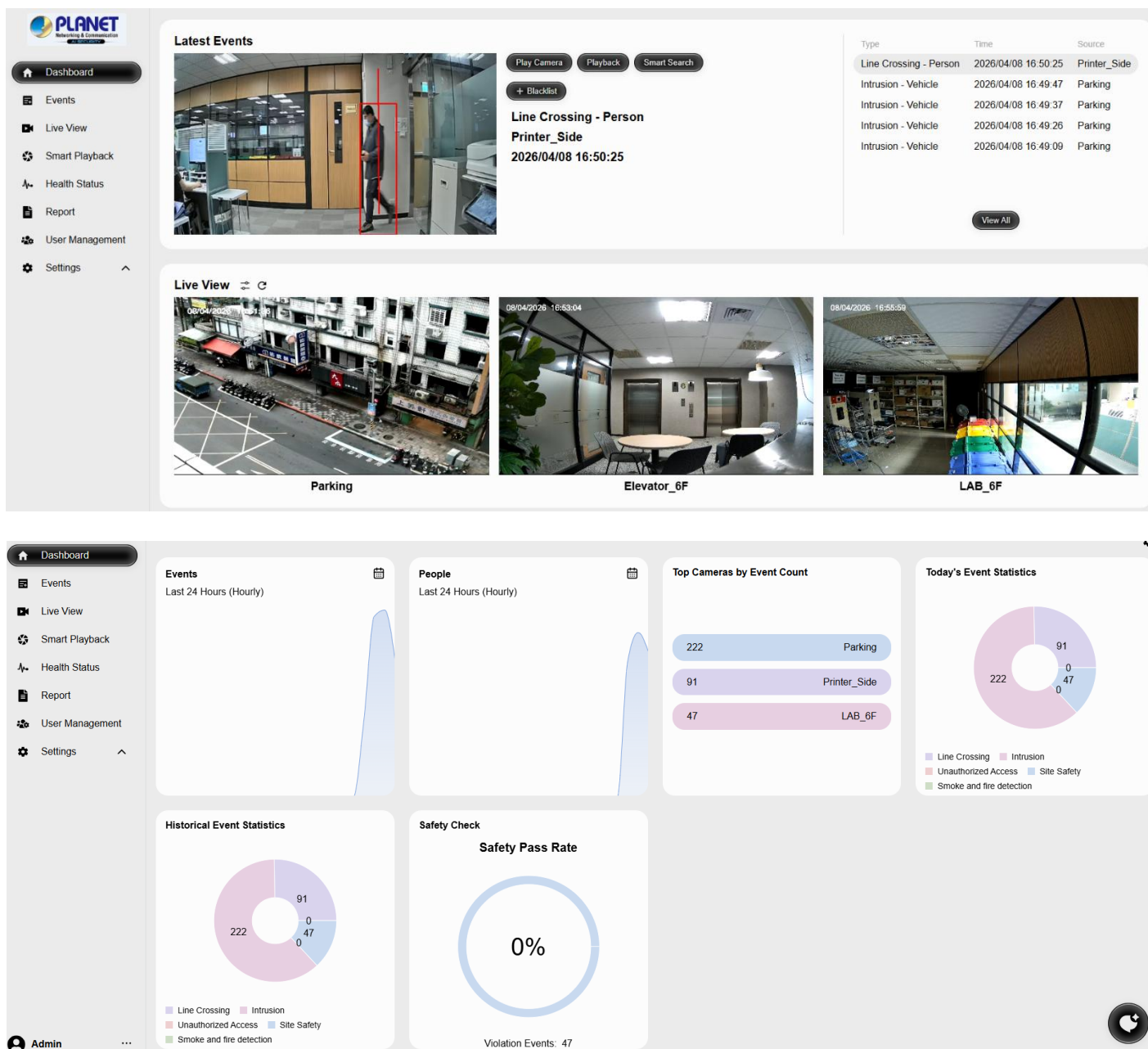
Chapter 4 System Configuration

This chapter describes system configuration and administrative settings.

4.1 Dashboard

The Dashboard provides an overview of system status, including latest events, live view, and system resources.

For detailed descriptions of each widget, please refer to Chapter 5.1 Dashboard.



4.2 Settings

The Settings module allows system administrators to configure global system parameters.

After entering this page, a submenu will be displayed on the left side, including options such as **General Settings**, **AI Settings**, and **Media Settings**.

4.2.1 General Settings

The General Settings page provides access to various system configuration modules.

Users can navigate through different setting categories using the tabs at the top of the page.

The available configuration tabs are described as follows:

System Settings

Allows users to configure system-level functions such as automatic restart, system reboot, and restoring factory default settings.

Network Settings

Used to configure network parameters, including IP address, subnet mask, gateway, and DNS settings.

License Update

Allows users to verify and update the system license to ensure all features are properly activated.

Software Update

Provides options to update the system firmware to enhance performance, stability, and functionality.

Update Model

Used to update the AI recognition model to improve detection accuracy and system performance.

Time Zone Settings

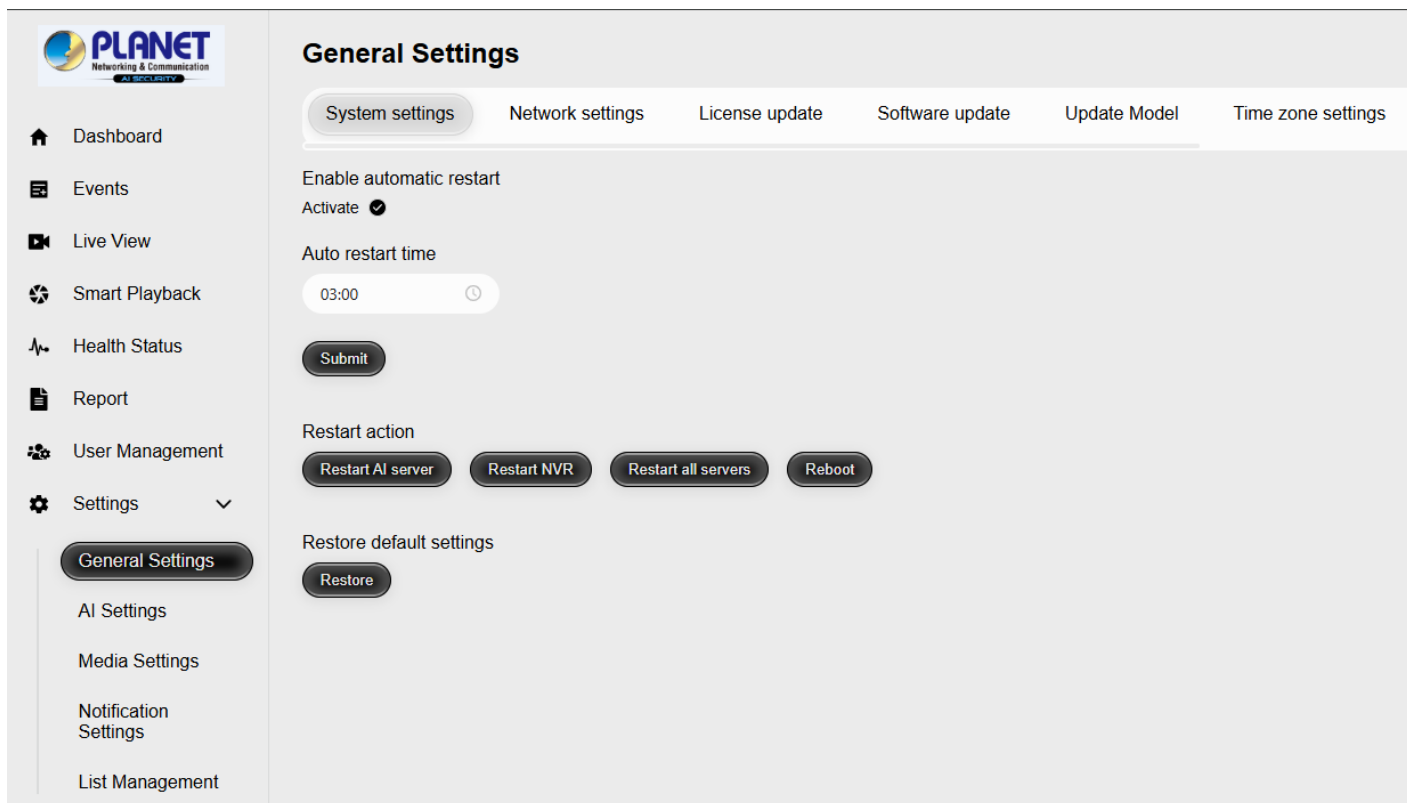
Allows users to configure system time, synchronization methods, and time zone settings.

Certificate Download

Provides the system SSL certificate for secure HTTPS access and allows users to install it on client devices.

Logs (if available)

Displays system logs for monitoring system activity and troubleshooting issues.



4.2.1.1 System Settings

The **System Settings** page allows users to configure system maintenance options, including automatic restart, manual restart functions, and restoring the system to default settings.

Configuration Items

- **Enable Automatic Restart**
Enable or disable the automatic system restart function.
When activated, the system will reboot at the scheduled time daily.
- **Auto Restart Time**
Set the time for automatic restart (24-hour format).
Example: 03:00

Restart Actions

The system provides several manual restart options:

- **Restart AI Server**
Restarts the AI processing service without affecting the entire system.
- **Restart NVR**
Restarts the video recording service.
- **Restart All Servers**
Restarts all system services.
- **Reboot**
Restarts the entire device.

Restore Default Settings

- **Restore**

Resets the system to factory default settings.

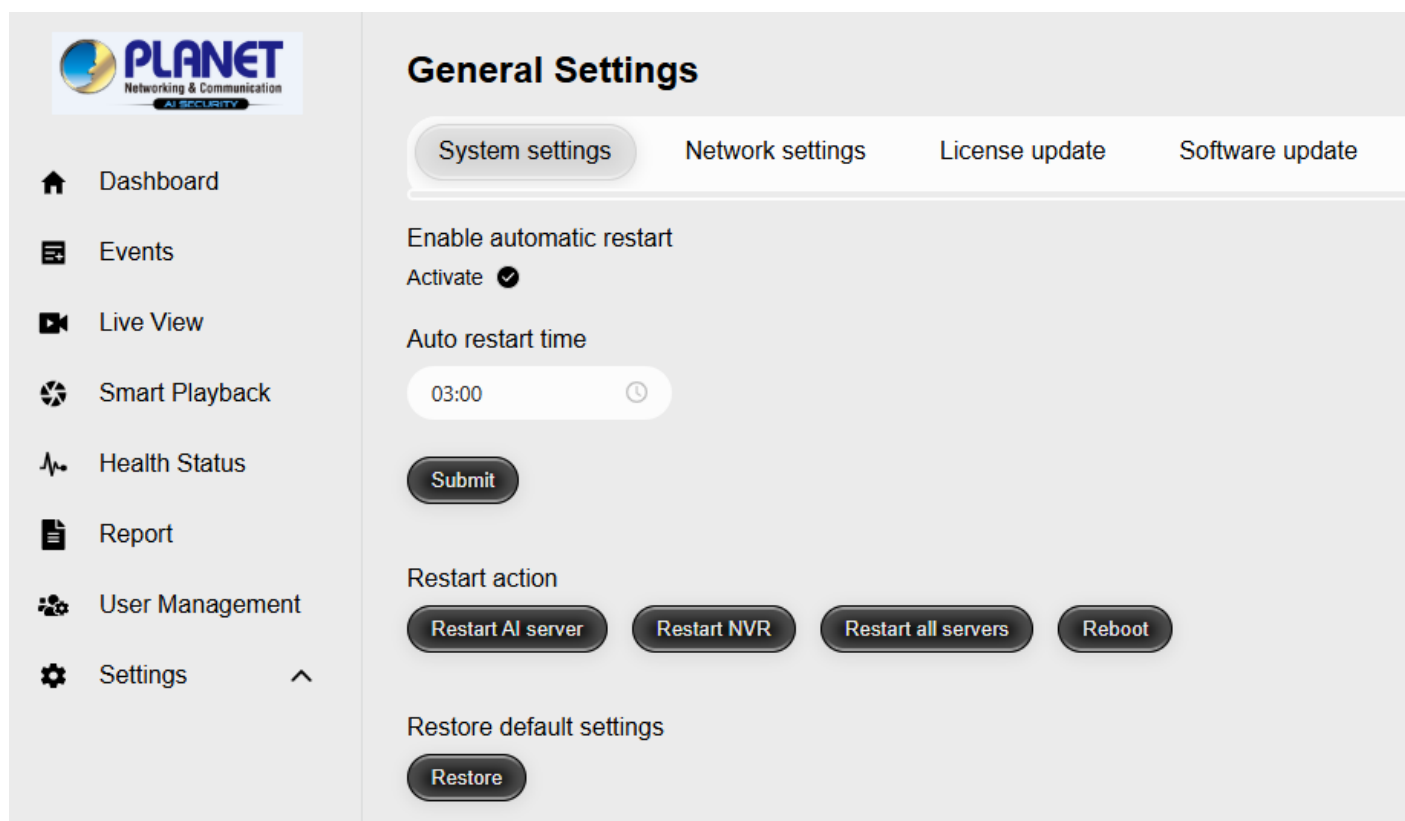
All configurations will be erased and restored to the original state.

Configuration Steps

1. Go to **Settings > General Settings > System settings**.
2. Enable **Automatic Restart** if required.
3. Set the desired **Auto Restart Time**.
4. Click **Submit** to apply the settings.
5. (Optional) Use **Restart Actions** for manual system control.
6. (Optional) Click **Restore** to reset the system to factory defaults.

Note

- It is recommended to schedule automatic restart during off-peak hours to minimize service interruption.
- Restarting services may temporarily interrupt AI detection or video recording.
- Do not power off the device during a reboot or restore process.
- Restoring to factory default will erase all configurations, including network settings, user accounts, and AI configurations.



The screenshot shows the 'General Settings' page of the PLANET AI Surveillance Station. The left sidebar contains a navigation menu with icons and labels for Dashboard, Events, Live View, Smart Playback, Health Status, Report, User Management, and Settings. The main content area is titled 'General Settings' and has four tabs: 'System settings' (active), 'Network settings', 'License update', and 'Software update'. Under 'System settings', there are three sections: 1. 'Enable automatic restart' with an 'Activate' checkbox that is checked. 2. 'Auto restart time' with a time picker set to '03:00'. 3. 'Restart action' with four buttons: 'Restart AI server', 'Restart NVR', 'Restart all servers', and 'Reboot'. 4. 'Restore default settings' with a 'Restore' button.

4.2.2 Time Zone Settings

The **Time Zone Settings** page allows users to configure the system time, synchronization method, and time zone to ensure accurate timekeeping for system logs and events.

Configuration Items

- **System Time**

Displays the current system date and time.

- **Sync with computer time**

When enabled, the system time will automatically synchronize with the local computer time.

- **Synchronization Method**

Select how the system time is updated:

- **Automatic (sync from time server):** Synchronizes with an NTP (Network Time Protocol) server.
 - (If applicable) Manual configuration.

- **Date Format**

Select the preferred date display format (e.g., DD/MM/YYYY or YYYY/MM/DD).

- **Time Zone**

Select the appropriate time zone based on the system location.

Example: *Asia/Taipei (GMT+08:00)*

- **Time Server**

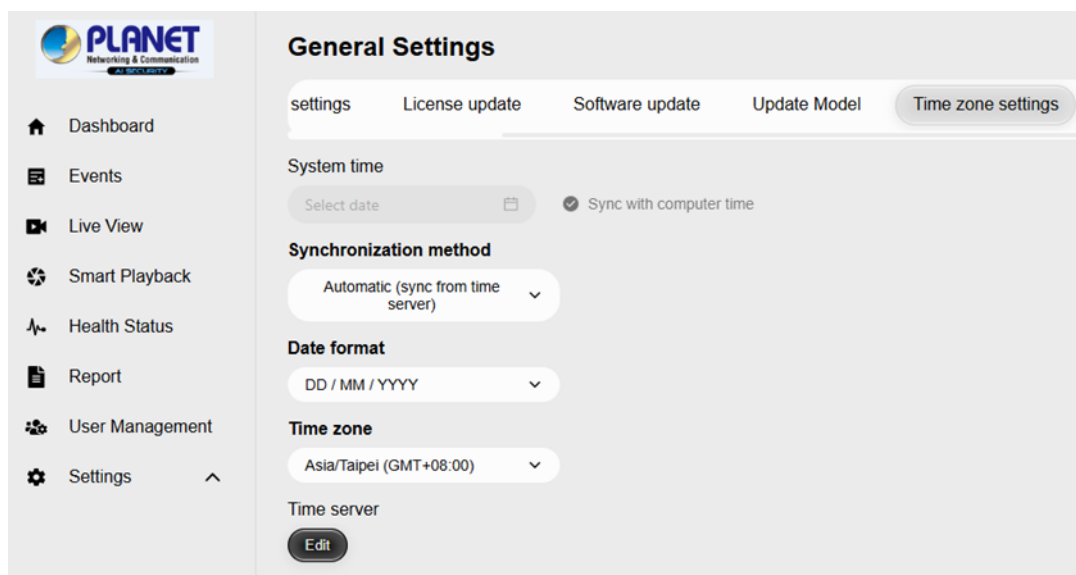
Configure the NTP server used for automatic time synchronization.

Configuration Steps

1. Go to **Settings > General Settings > Time zone settings**.
2. (Optional) Enable **Sync with computer time** to automatically match the local PC time.
3. Select the desired **Synchronization Method**.
4. Choose the appropriate **Date Format**.
5. Select the correct **Time Zone** for your location.
6. Click **Edit** to configure the **Time Server** if required.
7. Click **Submit** to apply the settings.

Note

- It is recommended to use **Automatic synchronization (NTP)** to ensure accurate system time.
- Incorrect time settings may affect:
 - Event logs
 - Video timestamps
 - AI detection records
- Ensure the time zone and system time are correctly configured before using AI and recording functions.



4.2.3 Certificate Download

The General Settings page includes several sub-tabs. The **Certificate Download** tab provides instructions for downloading and installing the system's SSL certificate.

After installing the certificate, the browser will no longer display the “Not Secure” warning, improving the security and reliability of system access.

Installation Steps (macOS Example)

1. Click the “**Certificate Download**” tab in the menu.
2. Click the download button to save the certificate file to your local device.

Open the **Keychain Access** application on macOS, and import the certificate into the **System** keychain.

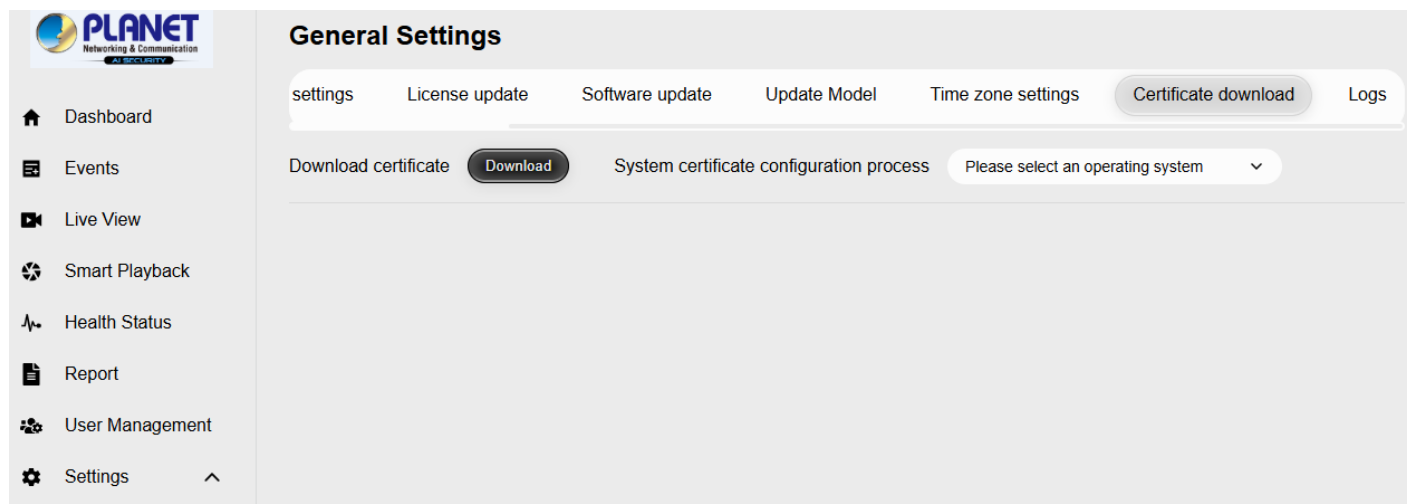
Double-click the imported certificate, expand the **Trust** section, and set “**When using this certificate**” to “**Always Trust.**”

Close the settings window and enter the macOS administrator password to confirm.

Note

Windows users can open the **Certificate Manager** and import the certificate into the **Trusted Root Certification Authorities** store.

The procedure is slightly different



4.2.4 License Update

The **License Update** page allows users to verify and update the system license to ensure all features are properly activated.

Update Method

Users can select one of the following license update methods:

- **Auto Update**

The system will automatically verify and update the license via the Internet.

An active Internet connection is required.

- **Manual Update**

Allows users to manually upload a license file.

The license file must be obtained from **PLANET support or your authorized distributor**.

Configuration Steps

Go to **Settings > General Settings > License update**.

Select the desired **Update Method**:

Choose **Auto Update** to verify the license automatically (Internet required).

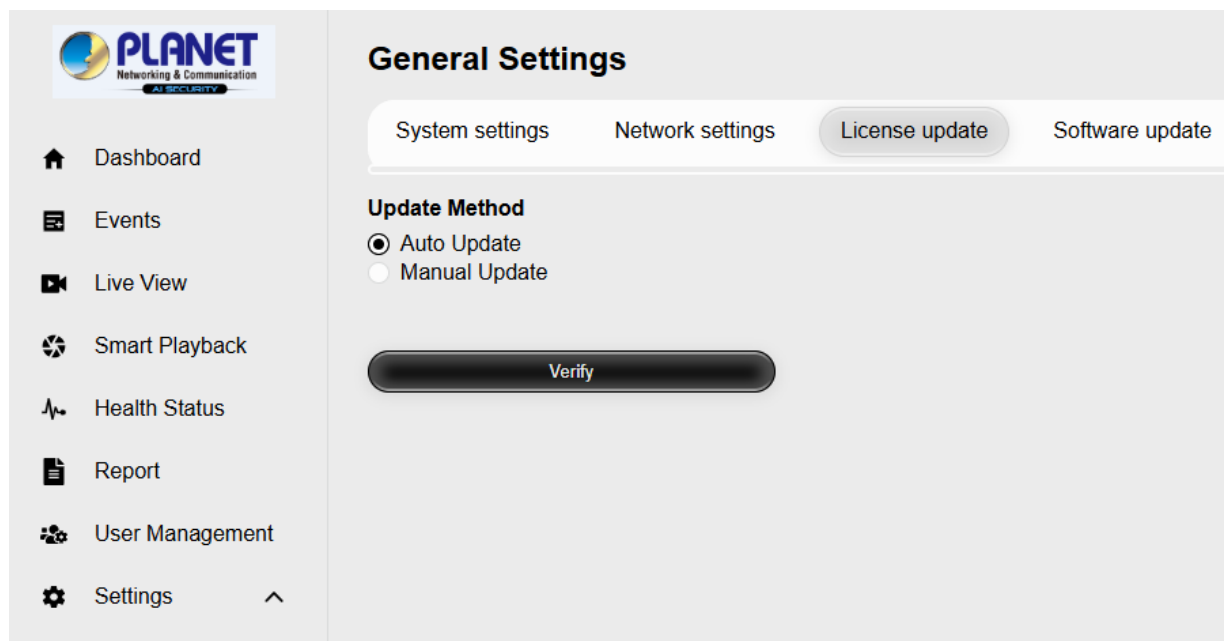
Choose **Manual Update** if a license file has been provided.

Click the **Verify** button to start the license validation process.

1. Wait for the system to complete the verification.

Note

- The device is preloaded with a valid license before shipment.
- If the internal storage (e.g., SSD) is replaced, a new license must be requested and installed.
- For **Manual Update**, please contact **PLANET support or your distributor** to obtain the license file.
- Without a valid license, login or system functions may be restricted.
- Ensure network connectivity when using **Auto Update**.
- Internet access must not be blocked by firewall or network restrictions when using Auto Update.



4.2.5 Update Model

The **Update Model** page allows users to update the AI recognition model used by the system to ensure optimal detection performance and accuracy.

Update Method

Users can select one of the following model update methods:

- **Auto Update**
The system will automatically check for available AI model updates via the Internet.
An active Internet connection is required.
- **Manual Update**
Allows users to manually upload an AI model file.
The model file must be obtained from **PLANET support or your authorized distributor.**

Configuration Steps

Go to **Settings > General Settings > Update Model**.

Select the desired **Update Method**:

Choose **Auto Update** to check and update the model automatically (Internet required).

Choose **Manual Update** if a model file has been provided.

1. The system will display the update status:

If no update is available, a message such as **“No updates available”** will be shown.

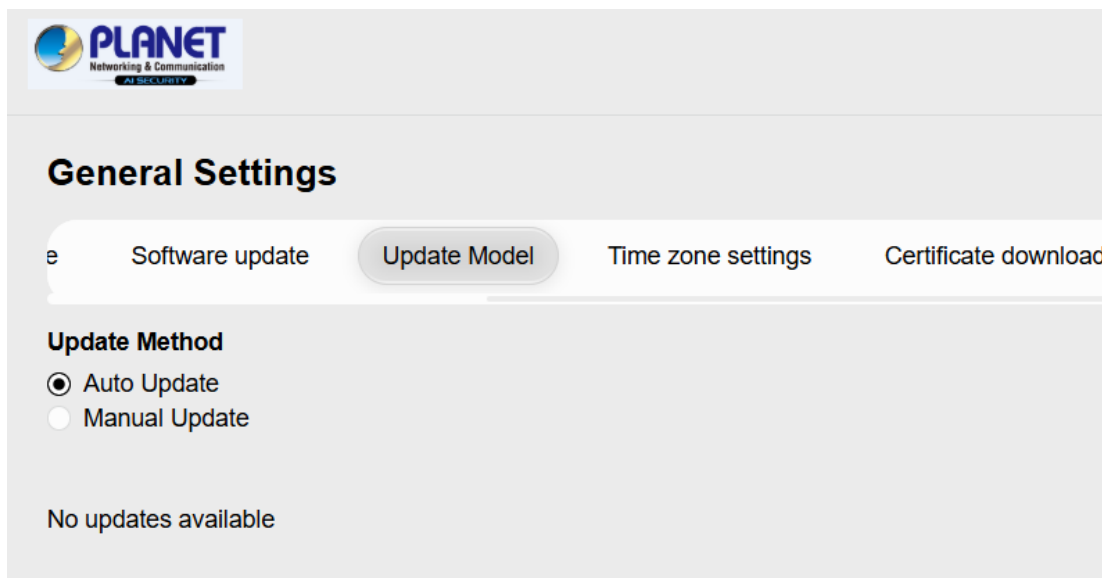
Follow on-screen instructions if an update is available.

Note

Ensure the device is connected to the Internet when using **Auto Update**.

For **Manual Update**, please contact **PLANET support or your distributor** to obtain the correct model file.

- Do not power off the device during the update process to avoid system malfunction.
- Updating the AI model may improve detection accuracy and system performance.
- The system will use the latest compatible AI model version after a successful update.



4.2.6 Software Update

The Software Update function allows users to upgrade the system firmware.

Two update methods are supported:

- **Online Update**

The system connects to the update server to download and install the latest firmware automatically.

- **Manual Update**

Users can upload a firmware file or license file provided by the vendor.

Steps:

1. Go to Settings > System > Software Update
2. Select Online Update or Manual Update
3. Click "Check for updates" or upload the file
4. Confirm and start update
5. The system will reboot after completion

Note:

- Do not power off during update
- Internet connection is required for online update
- License file may be required for customized firmware

The **Software Update** page allows users to update the system firmware to enhance functionality, improve system stability, and fix known issues.

Update Method

Users can select one of the following software update methods:

- **Auto Update**

The system will automatically check for available firmware updates via the Internet.

An active Internet connection is required.

- **Manual Update**

Allows users to manually upload a firmware file.

The firmware file must be obtained from **PLANET support or your authorized distributor**.

Configuration Steps

Go to **Settings > General Settings > Software update**.

Select the desired **Update Method**:

Choose **Auto Update** to check and update firmware automatically (Internet required).

Choose **Manual Update** if a firmware file has been provided.

1. Follow the on-screen instructions to proceed with the update.
2. Wait for the system to complete the update process.

The system may automatically reboot after the update is completed.

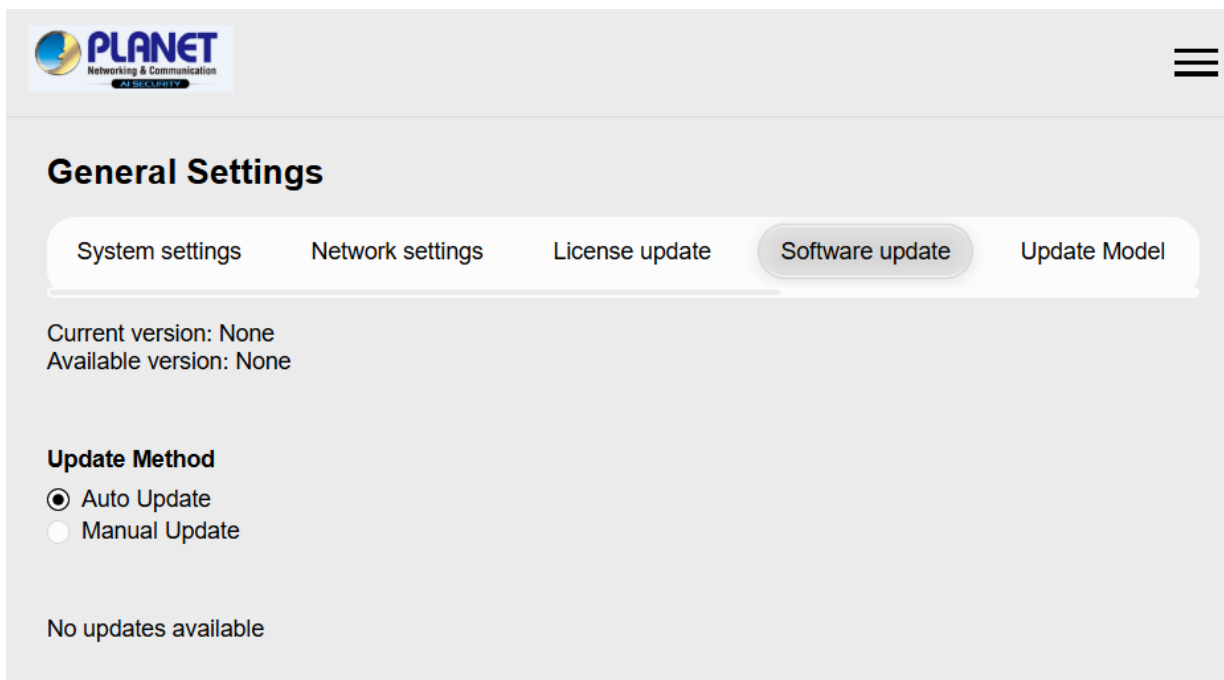
Note

Ensure the device is connected to the Internet when using **Auto Update**.

For **Manual Update**, please contact **PLANET support or your distributor** to obtain the correct firmware file.

- Do not power off the device during the update process to avoid system damage or failure.
- It is recommended to back up important configurations before performing a software update.
- System functions and interface may change after updating to a newer version.

- After the update, please log in to the system again and verify that all functions are operating normally.



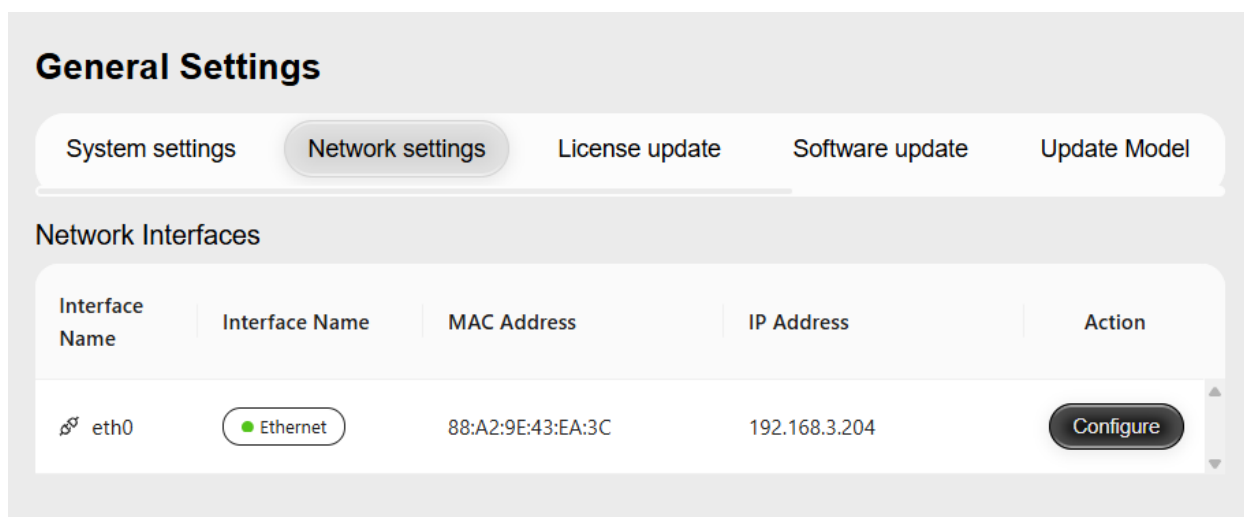
4.3 Network Settings

The Network Settings page allows users to configure the network parameters of the device, including IP address, subnet mask, gateway, and DNS settings.

Users can manage available network interfaces and modify their configurations based on the network environment.

Network Interfaces

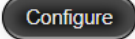
The system displays available network interfaces with the following information:



General Settings

System settings **Network settings** License update Software update Update Model

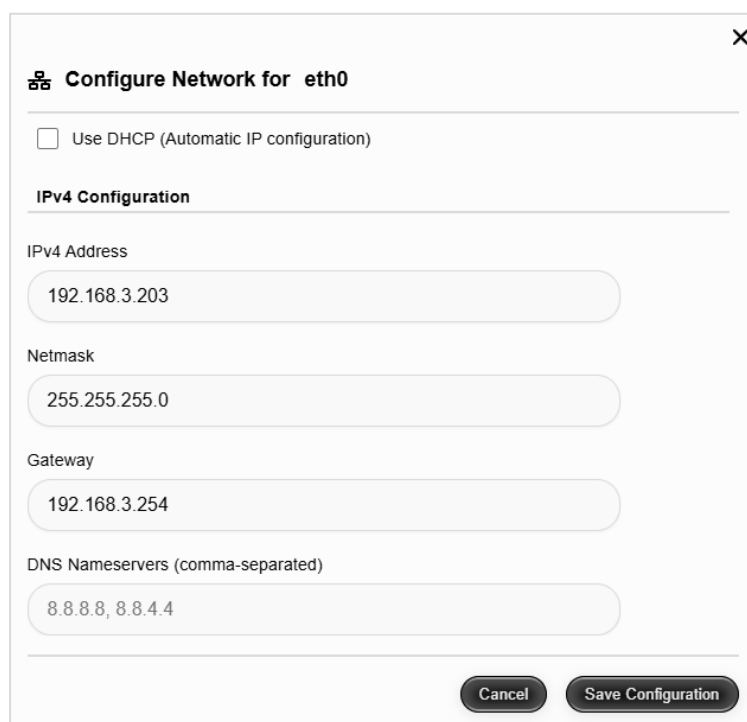
Network Interfaces

Interface Name	Interface Name	MAC Address	IP Address	Action
 eth0	 Ethernet	88:A2:9E:43:EA:3C	192.168.3.204	

- **Interface Name:** The name of the network interface (eth0) , Connection type (Ethernet only)
- **MAC Address:** Unique hardware address of the interface
- **IP Address:** Current assigned IP address
- **Action:** Click **Configure** to modify network settings

Configure Network Interface

Click the **Configure** button to open the network configuration window.



 **Configure Network for eth0** ✕

☐ Use DHCP (Automatic IP configuration)

IPv4 Configuration

IPv4 Address
192.168.3.203

Netmask
255.255.255.0

Gateway
192.168.3.254

DNS Nameservers (comma-separated)
8.8.8.8, 8.8.4.4

Available Settings:

- **Use DHCP (Automatic IP configuration)**
Enable this option to automatically obtain an IP address from a DHCP server.
- **IPv4 Address**
Manually assign an IP address when DHCP is disabled.
- **Netmask**
Define the subnet mask of the network.
- **Gateway**
Specify the default gateway for external network access.
- **DNS Nameservers**
Enter DNS server addresses (comma-separated).

Operation

1. Click **Configure** on the desired interface
2. Select **DHCP** or manually enter network parameters
3. Click **Save Configuration** to apply settings

Note

- Incorrect network settings may cause loss of connection to the device.
- It is recommended to record the current IP address before making changes.
- If DHCP is enabled, the IP address may change automatically.
- Use PLANET IP Discovery Tool to identify the device IP if needed.

4.4 Media Settings

The **Media Settings** page allows users to configure video recording parameters and manage connected cameras. This section includes **NVR settings** and **Camera settings**, providing control over storage behavior and camera connections.

4.4.1 NVR Settings

The **NVR Settings** tab allows users to configure video storage and recording policies.

Configuration Items

- **NVR Type**
Built-in NVR only.
- **Storage Type**
Select the storage location for recorded video.
 - Example: Internal Storage or External Storage (USB)

⚠ Switching the storage location will cause existing recorded video data to become inaccessible.
- **Video Retention Days**
Specifies how many days recorded video will be retained.
Older recordings will be automatically deleted after the specified period.
- **Minimum Storage Remaining**
Defines the minimum amount of storage space to be reserved.
When storage usage reaches this threshold, the system may overwrite older recordings.
 - When using internal storage, this value is automatically set to **10% of total capacity**.

Configuration Steps

1. Go to **Settings > Media Settings > NVR settings**.
2. Set the **Video Retention Days**.
3. Configure the **Minimum Storage Remaining** if applicable.
4. Click **Save** to apply the settings.

Note

- Changing the storage type may result in loss of access to existing recordings.
- It is recommended to configure retention days based on storage capacity and usage requirements.
- Ensure sufficient storage space is available for continuous recording.

Media Settings

NVR settings

NVR Type

Built-in NVR



Built-in NVR Settings

Storage Type ⓘ

Internal Storage



Switching storage location will cause existing video data to be inaccessible.

Video Retention Days

7

days

Minimum Storage Remaining

0

GB / 0 GB

When using internal storage, minimum storage remaining is automatically set to 10% of total storage.

4.4.2 Camera Settings

Protocol Description

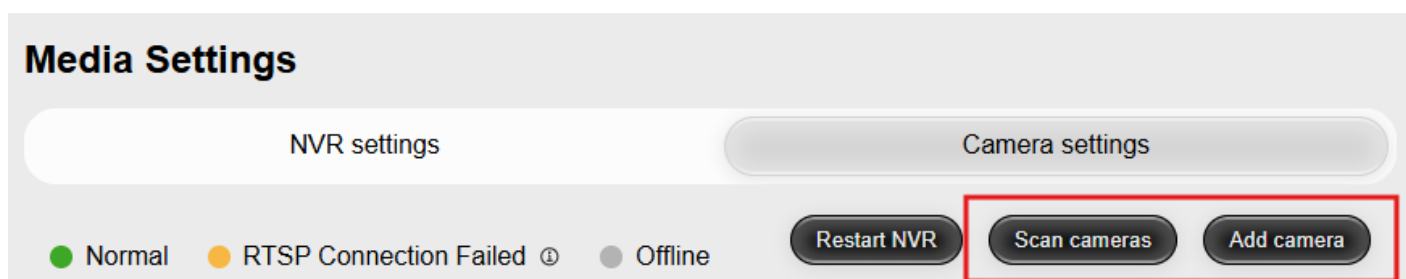
The AIS-1000 uses the following protocols:

- RTSP: Used for video streaming
- ONVIF: Used for camera discovery

Cameras supporting RTSP can be added manually even without ONVIF.

The Camera Settings page allows users to add, configure, and monitor IP cameras connected to the AIS-1000 system. Two methods are supported:

- Scan Cameras (Automatic Discovery)
- Add Camera (Manual Configuration)



Typical setup process:

- Ensure camera and AIS-1000 are in the same network
- Add camera (Scan or Manual)
- Verify camera connection status
- View live stream
- Enable AI detection

■ Scan Cameras (Automatic Discovery)

The Scan Cameras function automatically searches for available IP cameras within the same network.

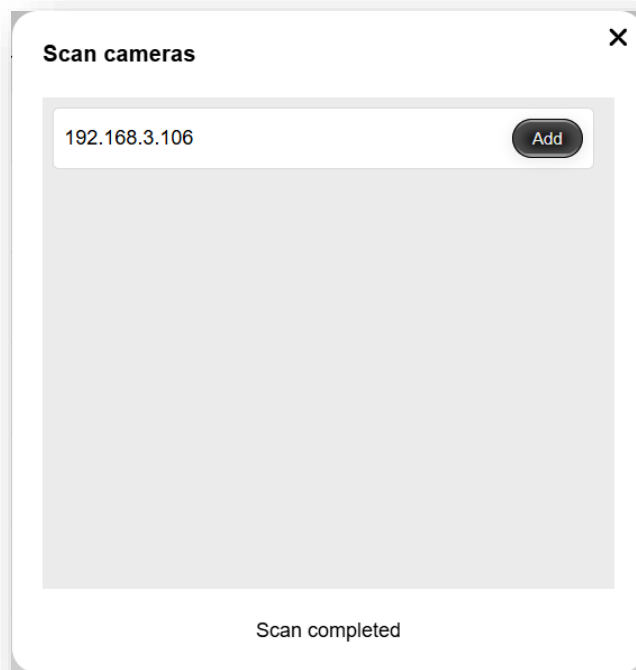
Steps:

1. Click **Scan Cameras**
2. Wait for system to discover devices
3. Select camera(s) from the list
4. Click **Add** to import cameras

Note:

- Cameras must support **ONVIF protocol** for automatic discovery
- Camera and AIS-1000 must be in the **same subnet**

- Ensure camera is powered on



■ Add Camera (Manual Configuration)

If a camera cannot be detected automatically, it can be added manually.

Steps:

1. Click **Add Camera**
2. Enter required information:
 - Camera Name
 - Camera IP Address
 - Camera Type
 - RTSP Username / Password
 - Select Stream
3. Click **Submit**

Add camera ✕

Camera name *

Camera IP address *

Camera type *

Please select a camera type ▼

RTSP username

RTSP password

RTSP stream selection

☐ Main stream only ☐ Sub stream only
☒ Both main and sub streams

Notes

Submit

RTSP Connection Concept

The system retrieves video streams using RTSP.

Typical RTSP URL format:

`rtsp://username:password@camera_ip:port/stream_path`

Troubleshooting – RTSP Connection Issues

If the camera cannot be connected, please check:

1. RTSP Port
 - Default is 554
2. RTSP Path
 - Varies by camera brand
3. Test with VLC Media Player
 - Verify RTSP stream
4. Camera Settings
 - Ensure RTSP is enabled
 - Check username/password

Camera Status Indicators

The system displays real-time connection status:

- Connected
- Disconnected
- RTSP Connection Failed

Media Settings

NVR settings
Camera settings

● Normal
● RTSP Connection Failed ⓘ
● Offline
Restart NVR
Scan cameras
Add camera

Camera name	Camera IP address	Camera type	Connection status	Notes	Actions
Elevator_6F	192.168.3.108	IPCAM	●	ICA-M4580P	...
Kent_side	192.168.3.21	IPCAM	●	ICA-M3580P	...
LAB_6F	192.168.3.101	IPCAM	●	ICA-M3580P	...
Parking	192.168.3.105	IPCAM	●	ICA-M3580P	...
Printer_Side	192.168.3.176	IPCAM	●	ICA-3880	...

< 1 >

4.4.3 Camera Management

In the camera list, click the “...” (**More Options**) icon under the **Actions** column to open the operation menu for each camera.

The following functions are available:

Available Functions

- **Edit Camera**

Modify camera settings, including **camera name**, **IP address**, **RTSP account/password**, and **stream configuration**.

- **AI Parameter Settings**

Configure individual AI detection functions for the selected camera, such as **line crossing detection**, **people tracking**, and **face recognition**.

- **Delete Camera**

Remove the selected camera from the system.

This action is irreversible. Please proceed with caution.

The figure below shows the location of the “...” (**More Options**) icon on the right side of the camera list. Clicking this icon will display the available operation menu.

Camera name	Camera IP address	Camera type	Connection status	Notes	Actions
Elevator_6F	192.168.3.108	IPCAM	●	ICA-M4580P	...
Kent_side	192.168.3.21	IPCAM	●		...
LAB_6F	192.168.3.101	IPCAM	●	ICA-M3580P	...

Edit camera
AI parameter settings
Delete camera

Edit camera ✕

Camera name *

Camera IP address *

Camera type *

RTSP username

RTSP password

RTSP stream selection
☐ Main stream only ☒ Sub stream only
☐ Both main and sub streams

Notes

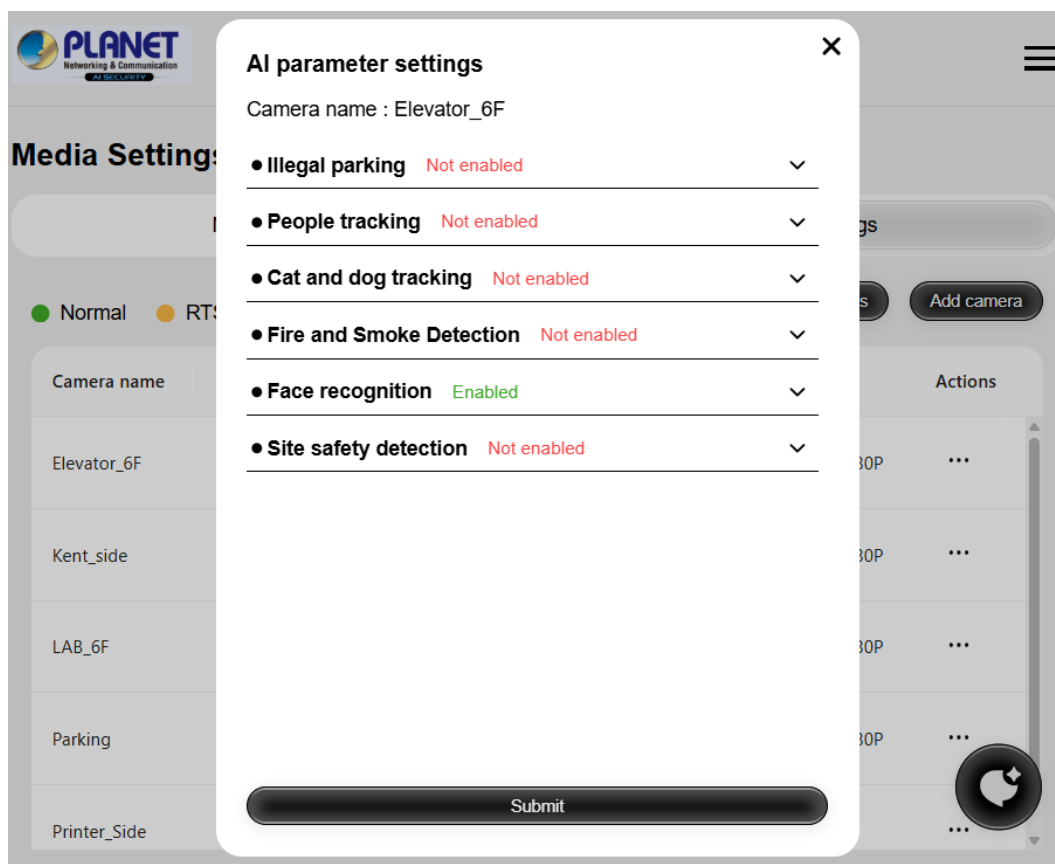
Submit

Note

- Ensure cameras are properly connected to the same network as the system.
- RTSP connection failure may be caused by incorrect credentials or network issues.
- It is recommended to assign static IP addresses to cameras for stable operation.
- AI-related settings for each camera can be configured via the Camera Settings page.

4.4.4 Camera AI Settings

The **Camera AI Settings** allow users to configure AI detection behavior individually for each camera.



Function Description

Each camera can have its own AI detection configuration, allowing flexible deployment based on different monitoring scenarios.

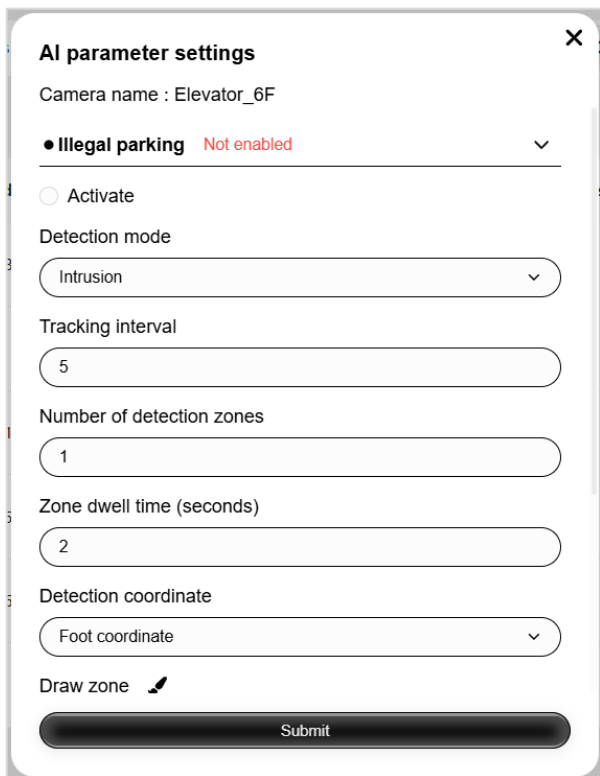
Users can enable or disable specific AI functions per camera, such as:

- Illegal Parking Detection
- People Tracking
- Cat and Dog Tracking
- Fire and Smoke Detection
- Face Recognition
- Site Safety Detection



Configuration Steps

1. Go to **Settings > Media Settings**.
2. Select a camera from the camera list.
3. Click the **AI parameter settings** button.
4. In the pop-up window, configure the AI functions for the selected camera:
 - Enable or disable specific detection features.



AI parameter settings X

Camera name : Elevator_6F

● **Illegal parking** Not enabled

☐ Activate

Detection mode

Intrusion

Tracking interval

5

Number of detection zones

1

Zone dwell time (seconds)

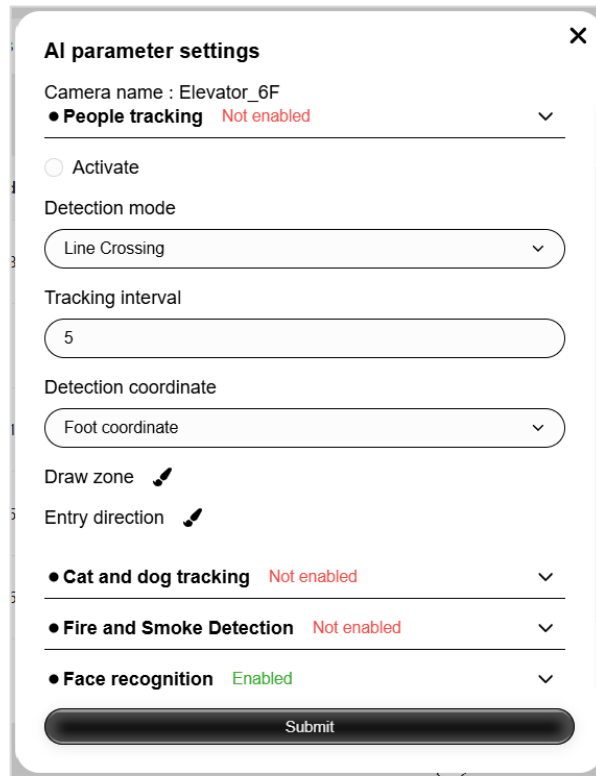
2

Detection coordinate

Foot coordinate

Draw zone

Submit



AI parameter settings X

Camera name : Elevator_6F

● **People tracking** Not enabled

☐ Activate

Detection mode

Line Crossing

Tracking interval

5

Detection coordinate

Foot coordinate

Draw zone

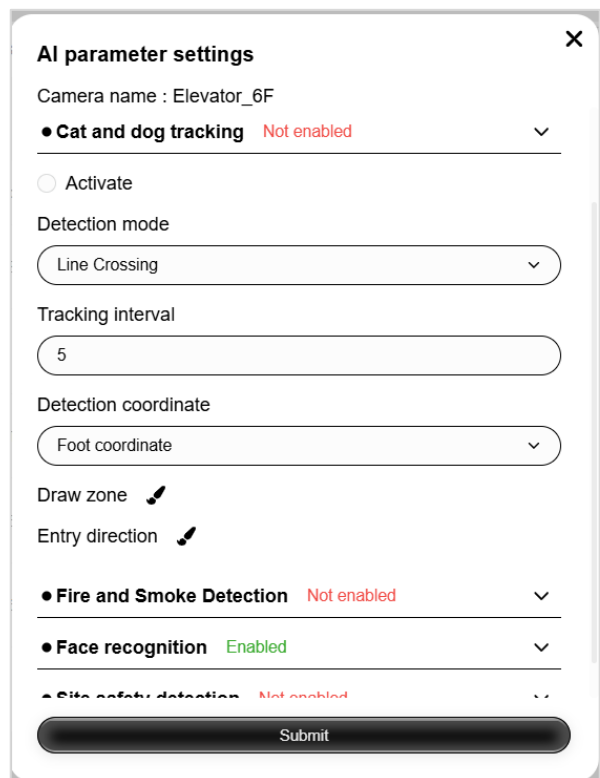
Entry direction

● **Cat and dog tracking** Not enabled

● **Fire and Smoke Detection** Not enabled

● **Face recognition** Enabled

Submit



AI parameter settings X

Camera name : Elevator_6F

● **Cat and dog tracking** Not enabled

☐ Activate

Detection mode

Line Crossing

Tracking interval

5

Detection coordinate

Foot coordinate

Draw zone

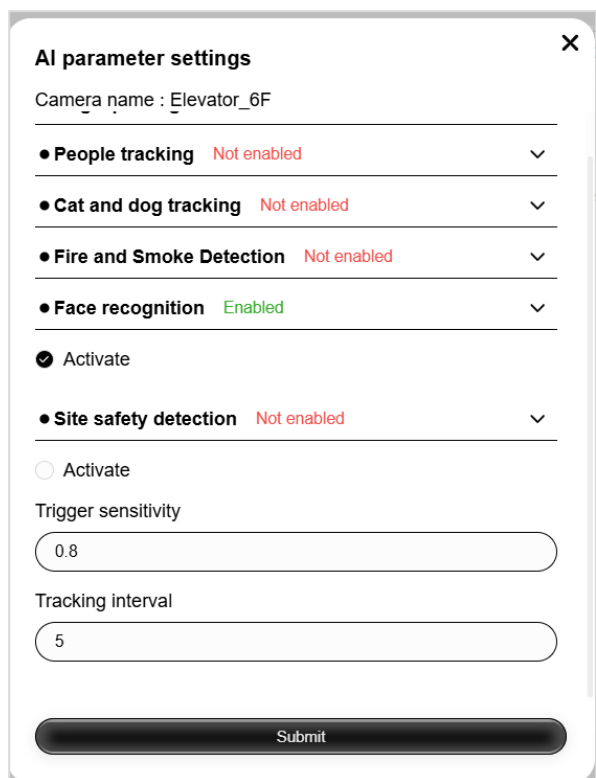
Entry direction

● **Fire and Smoke Detection** Not enabled

● **Face recognition** Enabled

● **Site safety detection** Not enabled

Submit



AI parameter settings X

Camera name : Elevator_6F

● **People tracking** Not enabled

● **Cat and dog tracking** Not enabled

● **Fire and Smoke Detection** Not enabled

● **Face recognition** Enabled

☒ Activate

● **Site safety detection** Not enabled

☐ Activate

Trigger sensitivity

0.8

Tracking interval

5

Submit

5. Click **Submit** to apply the settings.

Note

- Camera AI settings override or refine the global AI behavior for individual cameras.
- It is recommended to enable only the required AI functions per camera to optimize performance.
- Enabling multiple AI functions on multiple cameras may increase system resource usage.
- Detection accuracy may vary depending on camera position, lighting, and environment.
- Global AI settings define system-wide behavior, while camera AI settings allow fine-tuning for individual camera scenarios.

4.5 AI Settings

The **AI Settings** section allows users to configure both global AI parameters and per-camera AI detection settings. These settings determine how the system performs object detection, recognition, and event analysis.

4.5.1 AI Global Settings

The **AI Global Settings** define the overall behavior of AI detection across the system.

Parameter Settings

- **Maximum Detection Count**
Specifies the maximum number of objects that can be detected in a single camera view.
Increasing this value allows more objects to be detected but may affect system performance.
- **Feature Recognition Sensitivity**
Defines the similarity threshold used for feature-based recognition (e.g., face recognition).
 - Higher sensitivity: Only highly similar matches are recognized.
 - Lower sensitivity: More matches may be detected, but accuracy may decrease.
- **AI Active Time**
Defines the time period during which AI detection is active.
AI detection will be automatically disabled outside this time range.

Detection Items

Select the types of objects that the AI will detect globally:

- Face Detection
- Vehicle Detection
- Cat and Dog Detection
- People Detection
- Site Safety Detection
- Fire and Smoke Detection

Restore Default Settings

- **Restore**
Resets all AI global settings to default values.
Custom configurations will be removed.

Configuration Steps

1. Go to **Settings > AI Settings**.
2. Configure the **Parameter Settings**.
3. Enable or disable the desired **Detection Items**.
4. Click **Submit** (if applicable) to apply the settings.
5. (Optional) Click **Restore** to reset settings.

AI Settings

Parameter settings

Maximum detection count

The maximum number of objects that can be detected by AI in a single camera view

— 50 +

Feature recognition sensitivity

The similarity threshold for a specified person's features in smart search. Increasing this value means only persons with higher similarity will be matched.

Medium ▼

AI active time

Specify the time period during which AI detection is enabled. Detection will be automatically disabled outside this period

00:00 → 23:59 ⌚

Detection items

Select the objects that the AI will detect and recognize

Face Detection**Vehicle Detection****Cat and dog Detection****People Detection****Site safety Detection****Fire and Smoke Detection**

Restore default settings

Restore AI settings to their default values. Custom settings will not be preserved

Restore

4.6 Notification Settings

The **Notification Settings** page allows users to configure how the system sends alerts and notifications when events are triggered.

Notifications can be delivered via **on-screen display, email, or webhook**.

4.6.1 Email Settings

Configure email notifications for system events.

Configuration Items

- **Sender Email Address**
The email address used by the system to send notifications.
Recipients will see this address as the sender.
- **Sender Email App Password**
The application-specific password used for email authentication.
⚠ Do not enter your main email account password.
- **Email Language**
Select the language used in system-generated email notifications.
- **Email Sending Time**
Define the time period during which emails will be sent.
Email notifications will be disabled outside this time range.
- **Recipient Email Address**
Specify the email addresses that will receive notifications.
 - Maximum number of recipients: **10**

Note

- Ensure the email account supports SMTP and allows application access.
- Incorrect email settings may result in notification delivery failure.

Notification Settings

Email Settings

Sender email address

The email address used by the system to send emails. Recipients will see this address as the sender

Sender email app password

Enter the application password generated by your Google account for email authentication.
※ Do not enter your main Google account password.

Email language

Set the language used in system-generated email notifications

Email sending time

Emails will only be sent during the specified time period and will be disabled outside this period

Recipient email address

The email address that receives system notifications and messages
Maximum number of recipients: 10

繁體中文

00:00

→ 23:59

Enter an email address and press En

4.6.2 Webhook Settings

Configure webhook notifications to send event data to external systems.

Configuration Items

- **Webhook Format**
Defines the format of the webhook message payload.
- **Webhook List**
Add the destination URLs to receive notifications.
 - Maximum number of webhooks: **3**
- **Webhook Sending Time**
Define the time period during which webhook notifications will be sent.

Note

- Ensure the destination server is reachable from the system.
- Verify that the webhook URL is correctly configured to receive data.

Webhook Settings

Webhook Format

[View](#)

Webhook List

The system will send notifications to the specified URLs
Maximum number of webhooks:3

Enter a URL and press Enter to add

Webhook sending time

Webhook will only be sent during the specified time period and will be disabled outside this period

00:00 → 23:59 

4.6.3 On-Screen Notification Settings

Configure how notifications are displayed on the system interface.

Configuration Items

- **Display Duration**
Specifies how long notifications remain visible before automatically closing.

On-Screen Notifications Settings

Display duration
Set how long notifications remain visible before automatically closing

—

5

+

4.6.4 Event Notification Settings

Define which notification methods are triggered for specific AI events.

Supported Events

- Line Crossing Detection
- Intrusion Detection
- Site Safety Detection
- Face Recognition Detection
- Fire and Smoke Detection

Notification Methods

Each event supports the following notification options:

- **On-Screen Notifications**
Displays alerts directly on the system interface.
- **Email**
Sends notification emails to configured recipients.
- **Webhook**
Sends event data to external systems via webhook.

Configuration Steps

1. Go to **Settings > Notification Settings**.
2. Configure **Email Settings** if email notifications are required.
3. Configure **Webhook Settings** if integration with external systems is needed.
4. Set the **Display Duration** for on-screen notifications.
5. In **Event Notification Settings**, enable or disable notification methods for each event type.

Note

- Multiple notification methods can be enabled simultaneously for each event.
- Notification delivery depends on correct configuration of email or webhook settings.
- Excessive notifications may impact system performance or user experience.
- It is recommended to enable only necessary event notifications.
- Notification settings are triggered based on AI detection events configured in the AI Settings.

Event Settings

Configure how notifications are sent when events occur

Line Crossing Detection

On-Screen Notifications ☒

Email ☐

Webhook ☐

Intrusion Detection

On-Screen Notifications ☒

Email ☐

Webhook ☐

Site Safety Detection

On-Screen Notifications ☒

Email ☐

Webhook ☐

Face Recognition Detection

On-Screen Notifications ☒

Email ☐

Webhook ☐

Fire and Smoke Detection

On-Screen Notifications ☐

Email ☒

Webhook ☒

4.7 List Settings

This section is used to manage **blacklists**, and **whitelists** for AI recognition and matching. Users can manually add new entries or import personnel data in bulk via a CSV file.

Note:

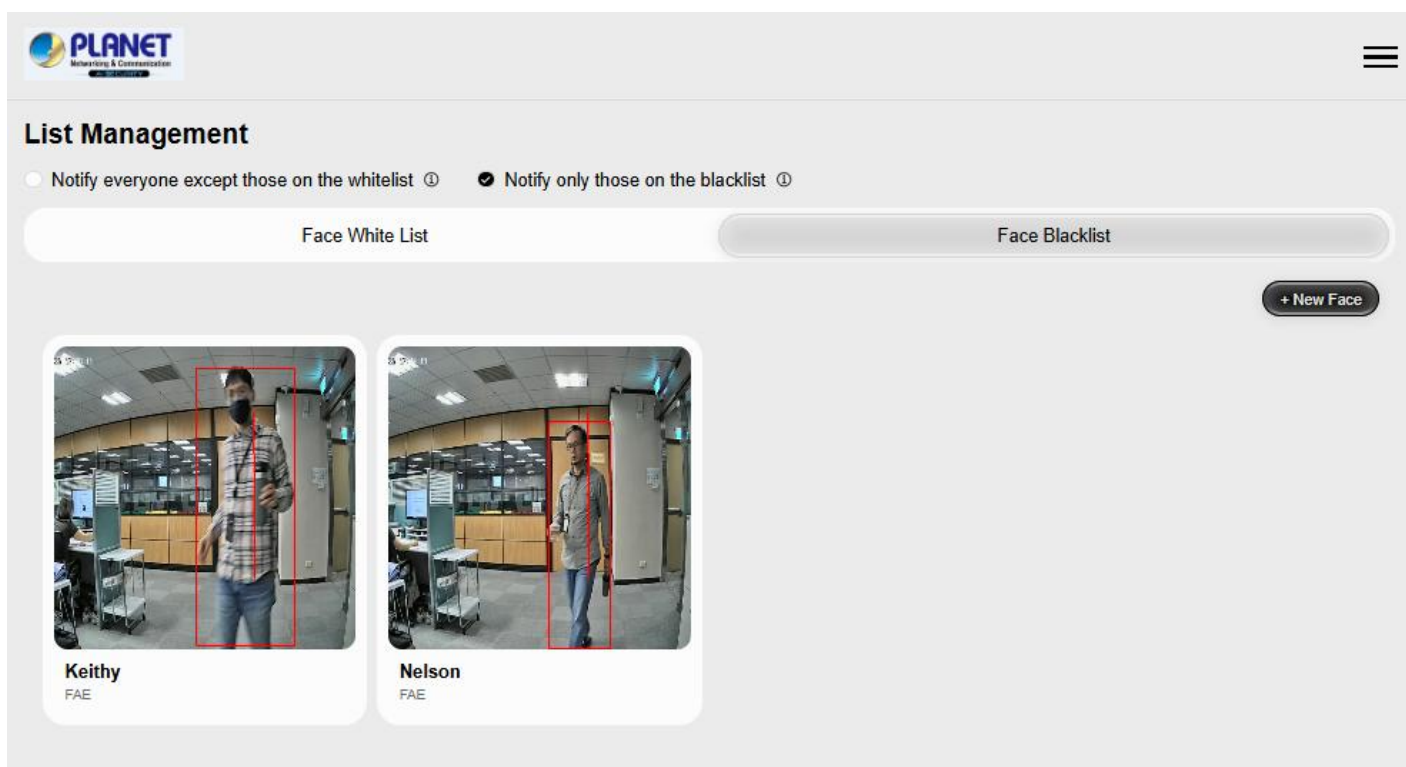
The blacklist and whitelist function currently supports recognition from one camera only.

List Types

- **Whitelist**
For authorized personnel.
No alerts will be generated when they are recognized.
- **Blacklist**
For restricted individuals.
Recognition will immediately trigger high-priority alerts.

Add New Entry

1. Click the “+ Add Person” button in the upper-right corner.
2. In the pop-up window, enter the **name**, and upload a **face image**.
(A clear, front-facing photo is recommended.)
3. Fill in comment (such as **title** and **department**), then click “**Submit**” to complete the entry.



The screenshot shows the 'List Management' section of the AI Surveillance Station interface. At the top left is the PLANET logo. On the right is a hamburger menu icon. Below the title, there are two radio buttons: 'Notify everyone except those on the whitelist' (unselected) and 'Notify only those on the blacklist' (selected). Below these are two tabs: 'Face White List' and 'Face Blacklist'. In the top right corner of the list area is a '+ New Face' button. The list contains two entries, each with a camera feed image of a person and their name and department below it. The first entry is 'Keithy' with department 'FAE'. The second entry is 'Nelson' with department 'FAE'. Both images show a person in a plaid shirt and jeans walking in a hallway, with a red bounding box around their face.

4.8 Health Status

The Health Status page provides real-time monitoring of system hardware resources, including CPU usage, memory usage, and disk information.

It helps administrators quickly identify potential performance bottlenecks or system issues, ensuring stable operation.

4.8.1 Monitoring Items

The page displays three main monitoring indicators in a list format on the left panel.

Each item includes an icon and a “**View**” option for detailed information:

Monitoring Parameters

- **CPU Usage**

Displays the current processor utilization percentage.

If usage consistently exceeds **80%**, it is recommended to reduce AI processing load or limit the number of simultaneous detection tasks.

- **Memory Usage**

Shows current system memory utilization.

It is recommended to maintain at least **20% free memory** for optimal performance.

- **Disk Information**

Displays storage usage and available disk space for recording.

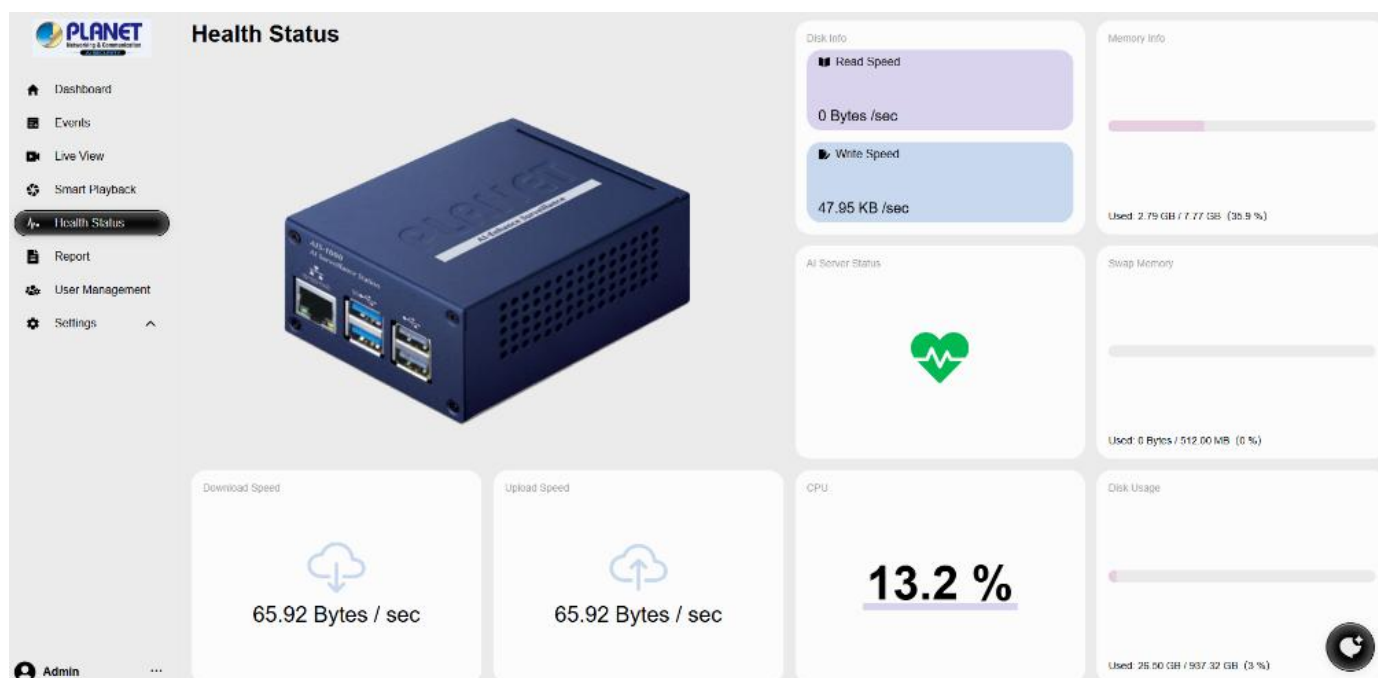
When the remaining space falls below the configured threshold, the system will generate an alert.

Caution

If the available disk space is insufficient, the system will automatically overwrite the oldest recordings to free up space, based on the retention settings configured under **Media Settings**.

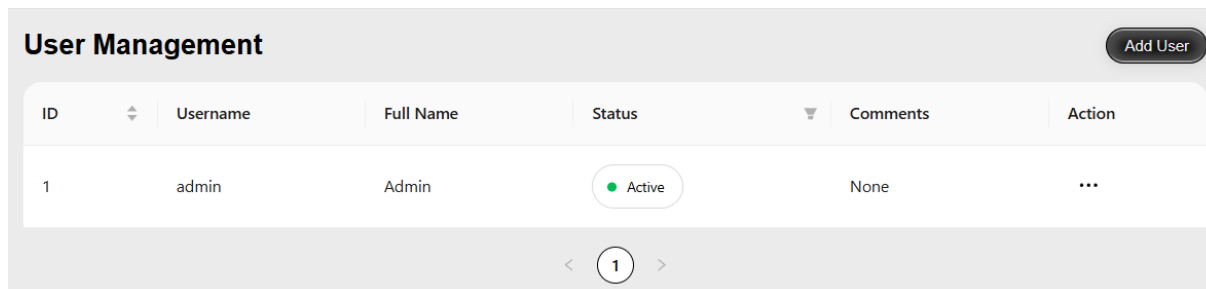
Note

It is recommended to regularly check the disk status on this page to ensure proper system operation.



4.9 User Management

The User Management page allows administrators to create, edit, or delete user accounts, and assign role-based permissions. This ensures secure system access and enables operation traceability.



ID	Username	Full Name	Status	Comments	Action
1	admin	Admin	Active	None	...

4.9.1 User Roles

The system provides two primary user roles:

- Super Administrator (Super Admin)**
 Has full access to all system functions, including user management and system configuration.
 The default account “**admin**” is assigned to this role.
- General User**
 Has access to basic functions such as live monitoring and event viewing, but is not permitted to modify system settings or manage user accounts.

Security Recommendation

It is strongly recommended to change default passwords regularly and avoid sharing accounts among multiple users. This helps ensure accountability and improves system security by maintaining traceable operation records.

4.9.2 Add a New User

Follow the steps below to create a new user account:

- Navigate to **User Management** from the left-side menu.
- Click the “**+ Add User**” button at the top of the page to open the user creation dialog.
- Enter the required information, including **Username** and **Password**, and confirm the password.
- Click the **Settings (⚙️)** icon next to *Permission* to select the appropriate user role. (Refer to Section 4.10.4)
- After verifying the information, click **Submit** to create the user account.

4.9.3 Edit and Delete Users

- Edit**
 Click the “**Edit**” icon next to the target user in the user list.
 You can modify the **username**, **password**, and **user role**.
- Delete**
 Click the “**Delete**” icon and confirm the action in the dialog box to remove the user account.

Warning

Deleting a user account is **irreversible**. Please confirm before proceeding.

The system requires at least one **Super Administrator** account.

It is not possible to delete all administrator accounts.

User Management

Add User

ID	Username	Full Name	Status	Comments	Action
1	admin	Admin	Active	None	...

< 1 >

Edit

Delete

Reset Password

Inactive user

4.9.4 User Permissions

The system allows administrators to assign different access permissions to each user.

Permissions are grouped into the following categories:

- **Dashboard**

View system statistics and overview information

- **Events**

Access, review, and download event records

- **Live View**

View real-time camera streams

- **Smart Playback**

Review and download recorded video

- **System Health**

Monitor system status and resource usage

- **Reports**

View and export system reports

- **User Management**

Manage user accounts and access rights

- **General Settings**

Configure system, network, time, and update settings

- **AI Settings**

View and configure AI-related parameters

- **Media Settings**

Manage NVR and camera configurations

- **Notification Settings**

Configure alert and notification rules

- **Whitelist Settings**

Manage whitelist entries

Note:

Available permissions may vary depending on user roles and system configuration.

Permission



Dashboard

Select All

☐ Statistics

Events

Select All

- ☐ Events: View
- ☐ Events: Edit Notes
- ☐ Events: Replay Download
- ☐ Events: Report Download

Live View

Select All

☐ Live View

Smart Playback

Select All

- ☐ Playback: View
- ☐ Playback: Download
- ☐ Advanced Playback: View
- ☐ Advanced Playback: Download

System Health

Select All

4.10 License Activation

This system requires a valid license file for full functionality.

Steps:

1. Go to Settings > License
2. Select Manual Update
3. Upload the license file provided for this device
4. Click Apply

Note:

- Each device requires a unique license file
- License is bound to hardware (CPU / SSD)

Chapter 5 Web Interface Overview

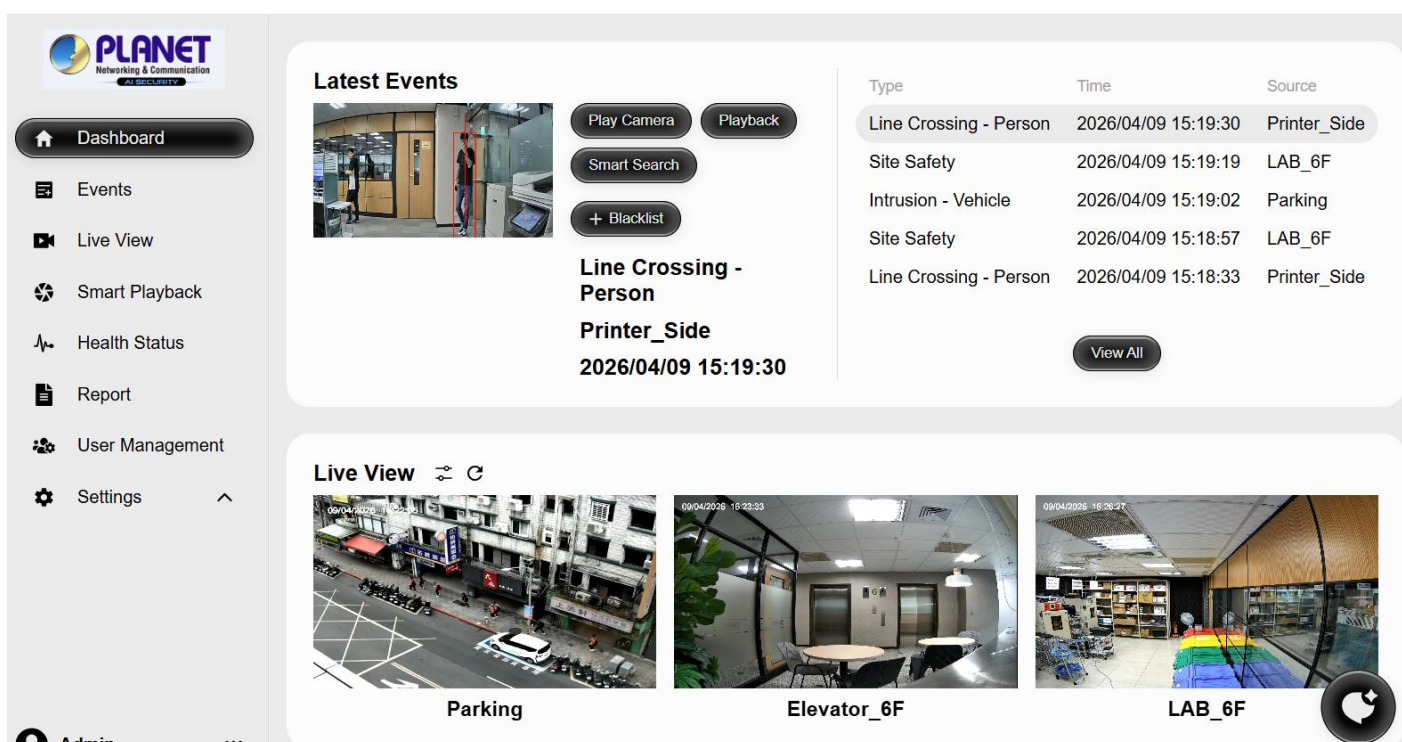
This chapter describes system monitoring and operational interfaces.

5.1 Dashboard

The Dashboard provides a real-time overview of system status, camera monitoring, and AI event statistics. It allows users to quickly understand current system conditions and recent activities.

Dashboard Layout Overview

The Dashboard is divided into the following sections:



The dashboard interface includes a left sidebar with navigation options: Dashboard, Events, Live View, Smart Playback, Health Status, Report, User Management, and Settings. The main content area is divided into two primary sections: Latest Events and Live View.

Latest Events Section:

- Includes a video preview of an event.
- Buttons: Play Camera, Playback, Smart Search, + Blacklist.
- Event details: **Line Crossing - Person**, **Printer_Side**, **2026/04/09 15:19:30**.
- Table of recent events:

Type	Time	Source
Line Crossing - Person	2026/04/09 15:19:30	Printer_Side
Site Safety	2026/04/09 15:19:19	LAB_6F
Intrusion - Vehicle	2026/04/09 15:19:02	Parking
Site Safety	2026/04/09 15:18:57	LAB_6F
Line Crossing - Person	2026/04/09 15:18:33	Printer_Side

A "View All" button is located at the bottom right of the table.

Live View Section:

- Includes three live camera feeds:
 - Parking:** Outdoor street view.
 - Elevator_6F:** Indoor elevator lobby.
 - LAB_6F:** Indoor laboratory setting.
- Each feed has a timestamp in the top left corner (e.g., 09/04/2026 16:28:33).
- A circular icon with a speech bubble is in the bottom right corner.

1. Latest Events

Displays the most recent detected events.

- Shows event preview (image/video snapshot)
- Includes event information such as:
 - Type
 - Time
 - Source
- Click **"View All"** to open the full Events page

Purpose:

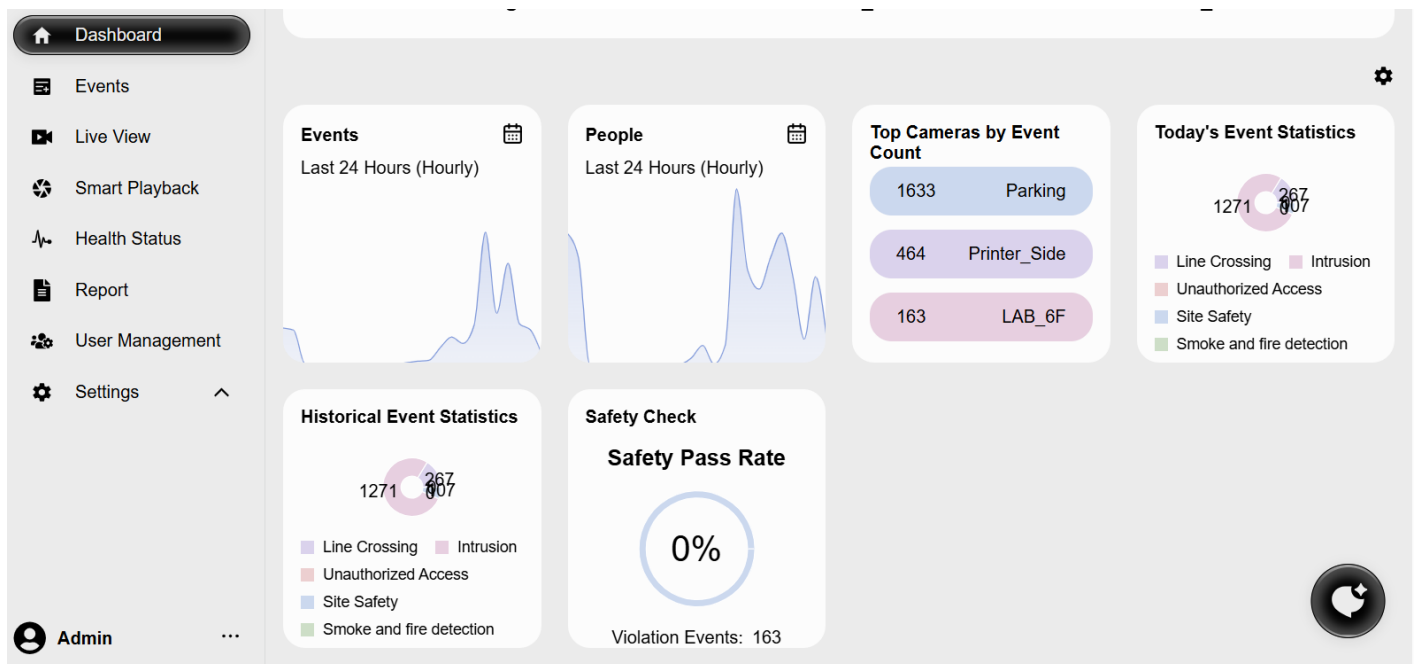
Quickly review the latest AI detections without entering the Events page

2. Live View

Displays real-time video streams from connected cameras.

- Supports multiple camera views
- Empty channels will show *“Please click to Select Camera”*
- Users can select cameras to display live footage

Purpose:



Monitor current on-site conditions instantly

3. Event Statistics (Last 24 Hours)

Includes:

- **Events (Hourly)**
- **People (Hourly)**

Displays hourly trends of detected events and people count

Purpose:

Quickly understand activity patterns within the last 24 hours

4. Top Cameras by Event Count

Shows ranking of cameras based on number of detected events.

Purpose:

Identify high-risk or high-activity areas

5. Today's Event Statistics

Displays categorized AI event types, such as:

- Line Crossing
- Intrusion
- Unauthorized Access
- Site Safety
- Smoke and Fire Detection

Purpose:

Understand distribution of event types for the current day

6. Historical Event Statistics

Displays long-term event trends.

Purpose:

Analyze historical data for behavior patterns and system performance

7. Safety Check

Displays overall safety status.

- **Safety Pass Rate (%)**
- Number of violation events

Example:

- Safety Pass Rate: 0%
- Violation Events: 0

Purpose:

Quickly evaluate compliance and safety conditions

Usage Notes

- The Dashboard is designed for monitoring only; configuration settings are available in the **Settings** menu
- Data displayed depends on connected cameras and enabled AI features
- If no data is shown, please check:
 - Camera connection status
 - AI settings configuration
 - Network connectivity

5.2 Events

The Events page records all alerts triggered by the AI detection engine.

Users can filter events based on specific conditions, view snapshots and detailed information, and export data for further analysis or archiving.

5.2.1 Page Overview

The Events page includes three main tabs:

- **Event List**
Displays all AI-triggered events, including **event time**, **camera name**, **event type**, and **snapshot**.
- **Smart Event List**
Categorizes events based on specific AI detection types (e.g., line-crossing detection).
- **Access Control Records**
Displays entry and exit records triggered by AI face recognition.

5.2.2 Event Filtering and Search

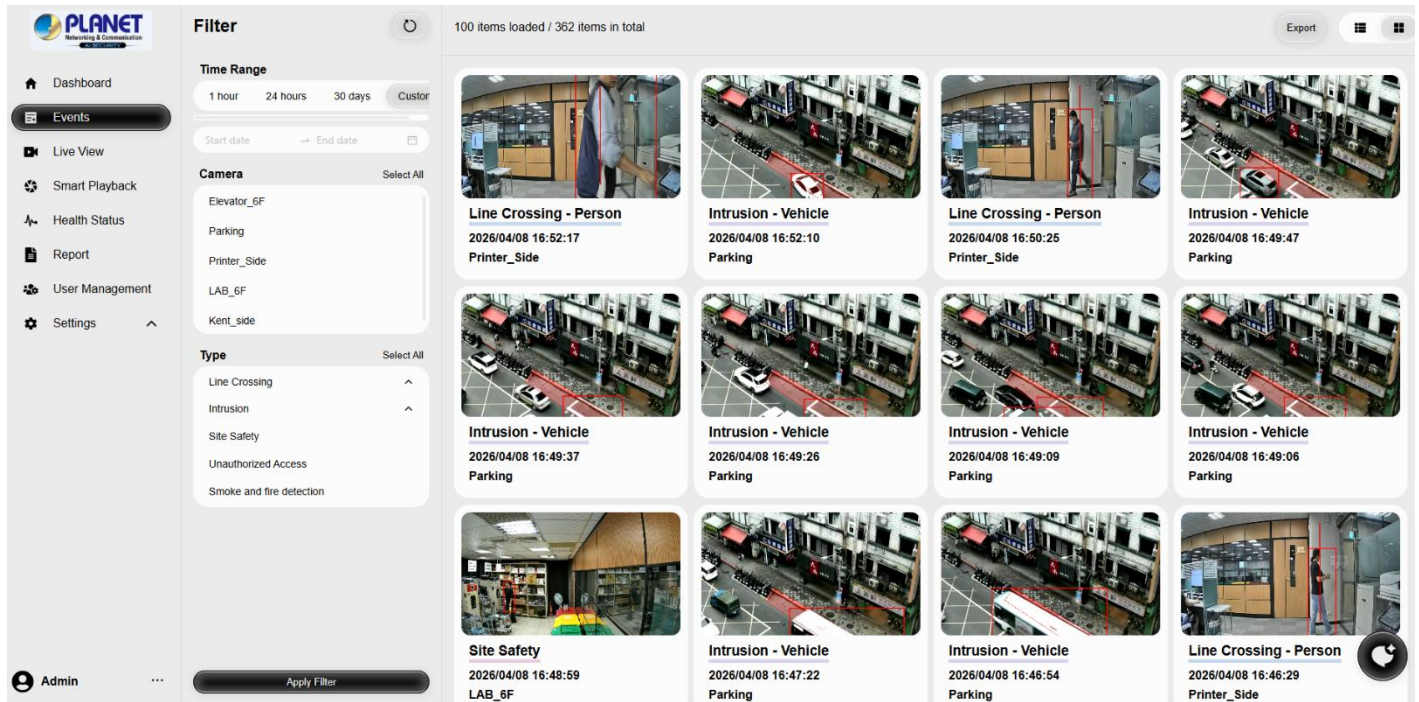
Multiple filtering options are available at the top of the event list:

- **Start Time / End Time**
Define a time range to filter events within a specific period.
- **Event Type**
Select event categories from the dropdown menu (e.g., **Intrusion Detection**, **Face Recognition**).
- **Search Button**
Click to apply the selected filters and display results.
- **Export Button**
Export the filtered results as a **CSV** or **Excel** file.

Caution

If the event snapshot displays “**No Image Available**”, it may be due to insufficient storage space or the camera being offline during that time period.

Please verify the storage configuration under **Settings > Media Settings**.



The screenshot displays the PLANET AI Surveillance Station AIS-1000 interface. On the left is a sidebar menu with options: Dashboard, Events (selected), Live View, Smart Playback, Health Status, Report, User Management, and Settings. The main area shows a list of events with filters on the left and a grid of event snapshots on the right.

Filter Panel:

- Time Range:** 1 hour, 24 hours, 30 days, Custom (selected)
- Start date:** → **End date:** →
- Camera:** Select All, Elevator_6F, Parking, Printer_Side, LAB_6F, Kent_side
- Type:** Select All, Line Crossing, Intrusion, Site Safety, Unauthorized Access, Smoke and fire detection

Event List (100 items loaded / 362 items in total):

Event Type	Timestamp	Camera
Line Crossing - Person	2026/04/08 16:52:17	Printer_Side
Intrusion - Vehicle	2026/04/08 16:52:10	Parking
Line Crossing - Person	2026/04/08 16:50:25	Printer_Side
Intrusion - Vehicle	2026/04/08 16:49:47	Parking
Intrusion - Vehicle	2026/04/08 16:49:37	Parking
Intrusion - Vehicle	2026/04/08 16:49:26	Parking
Intrusion - Vehicle	2026/04/08 16:49:09	Parking
Intrusion - Vehicle	2026/04/08 16:49:06	Parking
Site Safety	2026/04/08 16:48:59	LAB_6F
Intrusion - Vehicle	2026/04/08 16:47:22	Parking
Intrusion - Vehicle	2026/04/08 16:46:54	Parking
Line Crossing - Person	2026/04/08 16:46:29	Printer_Side

5.3. Live View

The Live Video page allows users to monitor real-time video streams from all connected cameras.

It supports multi-channel display and integrates AI analysis overlays, enabling administrators to quickly understand on-site conditions.

5.3.1 Page Overview

After entering the Live Video page, camera feeds are displayed in a grid layout.

Each video panel provides the following quick control buttons in the lower-right corner:

Available Controls

- **Play / Pause (▶)**
Control the playback or pause of the video stream.
- **AI Overlay**
Toggle the display of AI detection bounding boxes and analysis results.
- **Camera Information**
Quickly view camera-related information.
- **Full Screen**
Switch the selected camera view to full-screen mode.

Caution

If the camera view appears black with a play button displayed, it indicates that the camera is currently offline or the stream connection has been interrupted.

Please verify the connection status under **Settings > Media Settings > Camera Settings**.

5.4 Smart Playback

The Smart Playback function allows users to search historical recordings based on specific conditions, such as **persons** or **vehicles**.

By leveraging AI detection results for indexing, the system significantly reduces the time required to locate relevant footage and enables efficient video retrieval.

5.4.1 Search Criteria

Before using Smart Playback, configure the search filters at the top of the page:

Search Parameters

- **Camera**
Select the camera source for the search.
You can choose all cameras or specific ones.
- **Start Time / End Time**
Define the time range for the search.
- **Category**
Switch between different detection types, such as **Person** or **Vehicle**.
- **Search Button**
Click to apply the selected criteria and execute the search.

5.5 AI Chatbot

An AI chatbot is available via the floating button at the bottom-right corner of the interface.

This feature assists users in quickly retrieving system information, camera status, event records, and operational guidance through natural language queries.

How to Use

1. Click the blue floating button at the bottom-right corner to open the chatbot window.
2. Enter your question in the input field.

For example:

“What is the current camera connection status?”

3. The system will return relevant information and suggested actions based on your query.

Supported Query Types

The AI Chatbot supports system-related queries, including:

- **Event Search**
Query event records by time range, camera, and event type (e.g., intrusion, line-crossing, fire detection).
- **Playback Search**
Retrieve and play back recorded video by specifying time, camera, or detected objects.
- **Report Access**
Display statistical reports based on selected time periods and event categories.
- **Camera Information**
Query camera status, names, and IP addresses.
- **AI Settings Query and Modification**
Check or adjust AI-related parameters, such as detection thresholds and enabled functions.
- **Feature Guidance**
Provide explanations of system functions and usage instructions.

Limitations

The AI Chatbot is designed for **interactive system query and operation assistance**.

Its responses are based on predefined system data and supported command scope.

The chatbot may not support:

- General knowledge or open-domain questions
- Unrelated conversational queries
- Requests outside the system's supported functions

Note

For best results, use clear and specific queries, including conditions such as **time**, **camera name**, or **event type**.

5.6 Health Status

This page provides real-time monitoring information and does not allow configuration changes.

The figure below shows the Health Status page.

System resource information is displayed in a card-based layout, presenting real-time values for each monitoring item. At the center of the page, a 3D device model is displayed, while monitoring indicator cards are arranged around it to provide an intuitive overview of system performance.

5.6.1 Monitoring Metrics

The table below describes each monitoring metric displayed on the Health Status page, along with recommended thresholds for maintaining optimal system performance.

Monitoring Metrics Overview

Item	Description	Recommended Threshold
CPU Usage	Indicates the current processor utilization percentage.	Recommended to remain below 80%
Memory Usage	Displays used RAM versus total available memory (e.g., 3.12 GB / 7.77 GB).	Maintain at least 20% free memory
Disk Space	Shows used storage capacity versus total capacity (e.g., 40.70 GB / 56.46 GB).	Ensure available space remains above the configured minimum threshold
Disk Read/Write Speed	Displays real-time disk read/write speed (KB/s).	Check disk health if abnormal performance is observed
AI Service Status	Indicates the operational status of the AI engine. • Green heartbeat icon: Normal • No icon or red indicator: Abnormal	System should remain in normal (green) status

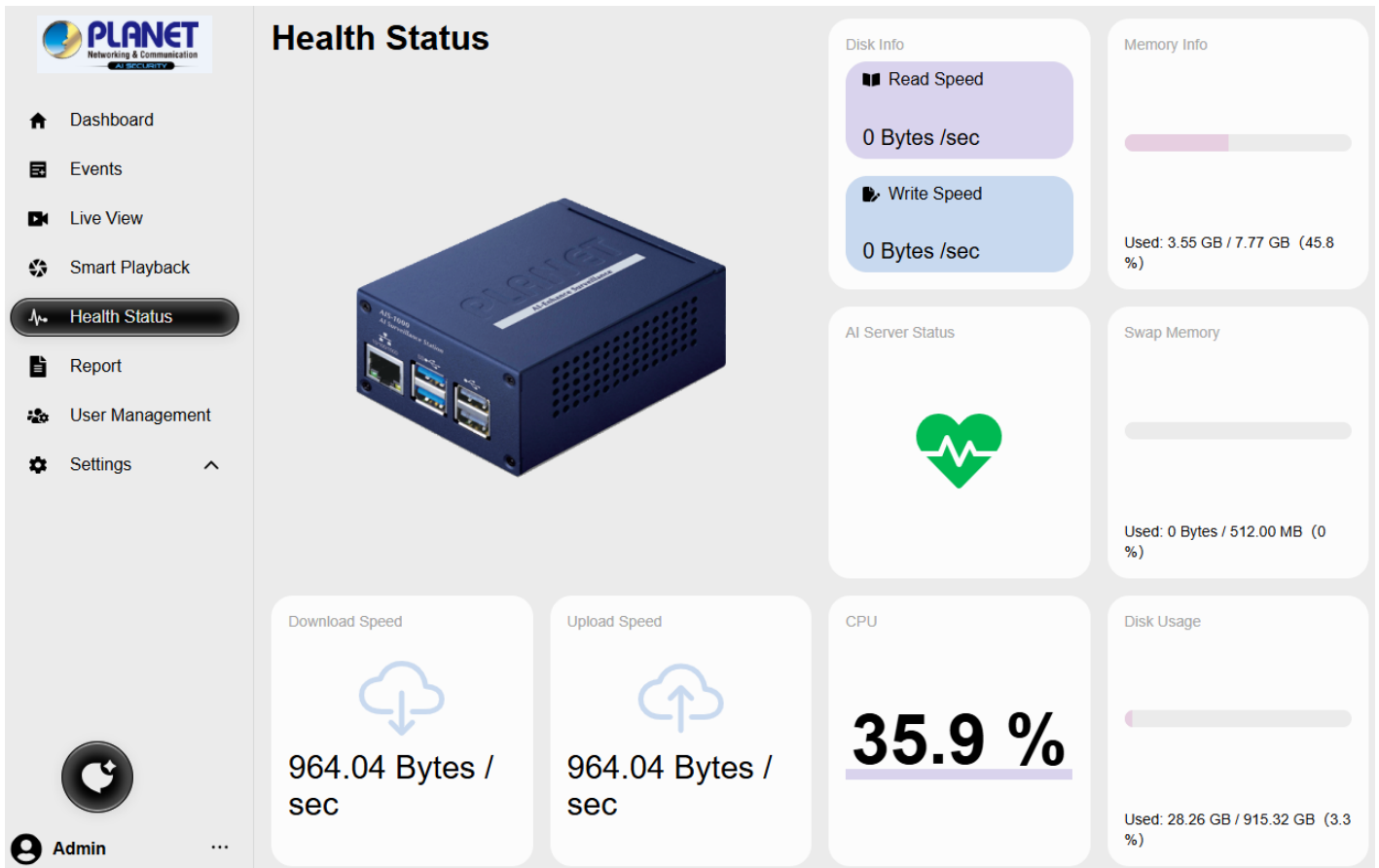
5.6.2 Interpretation Guidelines

To maintain stable system operation, refer to the following guidelines:

- Sustained high **CPU usage** may impact AI detection performance and system responsiveness.
- Low available **memory** may cause system slowdown or instability.
- Insufficient **disk space** may trigger automatic overwriting of older recordings.
- Abnormal **disk read/write speed** may indicate potential storage issues.
- If the **AI service status** is abnormal, AI detection functions may not operate correctly.

5.6.3 Best Practice

- Regularly monitor system resource usage via the Health Status page
- Adjust AI settings if CPU usage is consistently high
- Ensure sufficient storage space for recording retention
- Investigate abnormal indicators promptly to prevent system issues



5.7 Report

The Report Management page provides the following report categories:

- **Face Recognition Report**
Provides statistical analysis of face recognition events within a selected time range, including event count and distribution.
Reports can be further categorized by list types such as whitelist, and blacklist.
- **Person Counting Report**
Displays the number of people detected by each camera, suitable for traffic flow analysis.
- **Peak Hour Analysis**
Analyzes event frequency across different time periods to identify peak activity hours.

Important Notice

The whitelist/blacklist management interface is available for configuration.

However, actual face recognition matching results depend on AI engine support and system deployment conditions.

If no recognition results are generated, related reports will not display data.

