



USER MANUAL

AI BOX

4CH / 8CH / 16CH





Copyright

This manual without the manufacturer's approved copy and reprinted partially or in full, or translated into another language is prohibited.

Limitation of Liability

This product is designed to prevent fire and theft is not the main means. We shall not be liable for accidents or damage by using this product can result in liability for accidents or damage.

In order to improve the performance of the product without prior notice to the product may be a firmware upgrade.



1 Overview 06

1. Safety Instruction 06
2. WARNING 08
3. Key features 09

2 Components 09

1. Components 09
2. Names and functions of front panel 09
3. Name and functions of rear panel 10

3 Installation 11

1. Basic connection configuration 11
2. Network setting 11

4 System setting 17

1. Network setting 17
2. Change user password 18
3. Language setting 20
4. Date and Time setting 20
5. Firmware upgrade 21
6. Factory default 23



5 AI Source & Annotated Live Video 24

1. Video Source setting 24
2. AI algorithm 26
3. False detection filter setting 27
4. Face Recognition 28
5. Annotated Live Video 28

6 Action Rules 30

1. Action Rule Overview 30
2. AI Trigger setting 31
3. System Trigger setting 54
4. Schedule setting 55
5. Event Action setting 58

7 Statistics 78

1. Counting 78
2. Report 78

8 AI Marketing 80



9 Other Menu 84

1. Search 84
2. Display 85
3. System 87

10 Face Recognition 89

11 License Plate Recognition 95



1. Safety Instruction

The Company shall not have any responsibility for any accident or damage that may incur during the use of the product. For your safety, we provide a few instructions about installation, manipulation, cleaning, assembly/disassembly of the product as below. So please read carefully and comply with the instructions.

Before installation

Comply with the following instructions to prevent a fire, explosion, system failure or electric shock

- Remove the power supply module before proceeding
- Check the input voltage (AC100V-AC240V) to the power supply module before connecting it
- Keep the product away from excessive humidity (refer to optimal operating temperature indicated in product specification sheet)
- Ensure that all devices connected to the product should be properly earth-grounded

In operation mode

Comply with the following instructions to prevent a fire, explosion, system failure or electric shock

- If in need of disassemble the product for service, please consult with our trained technician before proceeding
- Do not connect multiple devices to a single adapter, Exceeding the capacity may cause abnormal heat generation or fire
- Keep products away from excessive dust or flammable substances (e.g. : propane gas)



- Do not touch it with wet hand while powered on
- Do not insert a conductor the ventilation system
- Do not apply excessive force to unplug the power cord

Disassembly & Cleaning

- When cleaning on the surface, use a dry cloth
- Do not wipe the product using water, paint thinner or organic solvents
- Do never dismantle, repair or modify the product. Without a consulting t rained technician

During installation

To prevent an accident or physical injury and to operate Product p roperly, please comply with the followings:

- Secure at least 18 centimeter of distance between cooling fan and wall f or a proper ventilation
- Install the product on a flat surface
- Keep it away from direct sunlight or excessive heat
- Be sure to use only the standard adapter that is specified in the specif ication sheet. Using any other adapter could cause fire, electrical shoc k, or damage to the product
- Incorrectly connecting the power supply or replacing battery may cause e xplosion, fire, electric shock, or damage to the product

While in use

- Do not apply excessive force to or shake it while in use



- Only use attachments/ accessories specified by the manufacturer

2. WARNING

To reduce the risk of fire or electric shock, do not expose this product to rain or moisture.

To avoid injury, this product must be mounted securely to the floor / wall in accordance with the installation instructions.

- Use only the standard power source specified in the specification. Using a different power source can cause fire, electric shock, or damage to the product.
- Install the product firmly and reliably. Otherwise, the product may fall and personal injury may result.
- Do not block any ventilation openings, Install in accordance with the manufacturer's instructions.
- Do not install near any heat sources such as radiators, heat registers, stoves, or other apparatus (including amplifiers) that produce heat.
- Do not defeat the safety purpose of the polarized or grounding-type plug. A polarized plug has two blades with one wider than the other. A grounding type plug has two blades and a third grounding prong. The wide blade or the third prong are provided for your safety. If the provided plug does not fit into your outlet, consult an electrician for replacement of the obsolete outlet.
- Do not place conductive objects (e.g. screwdrivers, coins, metal parts, etc.) or containers filled with water on top of the camera. Doing so may cause personal injury due to fire, electric shock, or falling objects



- Protect the power cord from being walked on or pinched particularly at plugs, convenience receptacles, and the point where they exit from the apparatus
- Do not install the product where the air conditioner is exposed to direct air. Otherwise, moisture may condense inside the product due to temperature differences inside and outside the product
- Refer all servicing to qualified service personnel. Servicing is required when the apparatus has been damaged in any way, such as power-supply cord or plug is damaged, liquid has been spilled or objects have fallen into the apparatus, the apparatus has been exposed to rain or moisture, does not operate normally, or has been dropped

3. Key features

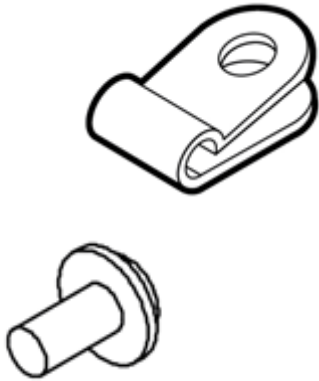
This device is based on the latest deep learning technology of intelligent video analysis which has up to 16 channels network camera video inputs. The features include object identification, object counts and object tracking by AI technology. Also, it allows to configure various trigger rules to ring alarms and can be utilized for various purposes by interworking with external network devices or systems, For example, this product can be interlocked with existing surveillance system and build an intelligent surveillance system such as business intelligence access control. It also can be used as an edge computing based video analysis device that combined with cloud web service.

- The latest deep learning technology of object recognition engine (Human, car and etc)
- Equipped rule engine to detect various situations and actions such as ‘Intrusion’, ‘Occupancy’, ‘Loitering’, ‘Enter/Exit’, ‘Line Crossing’

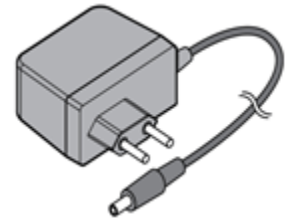


- Counts the number of objects that exist in a specific zone or counts the number of objects that pass through a specific zone
- OSD is displayed on the input image and provided as standard RTSP so that it can be easily linked without major compatibility with existing interlocking systems
- Standard ONVIF protocol support enables easy integration with ONVIF based network cameras and VMS (Video Management System)
- Various I/O supports including Alarm-in, Relay, RS485, USB
- Receive up to 16 channels of network video
- Receive Full HD video up to 30 fps, 4K video up to 30fps

1.Components

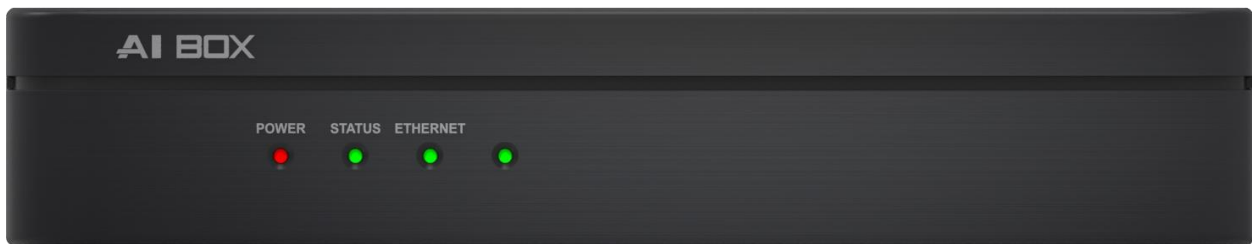



Cable clamp
crew



Adapter S

2.Names and functions of front panel

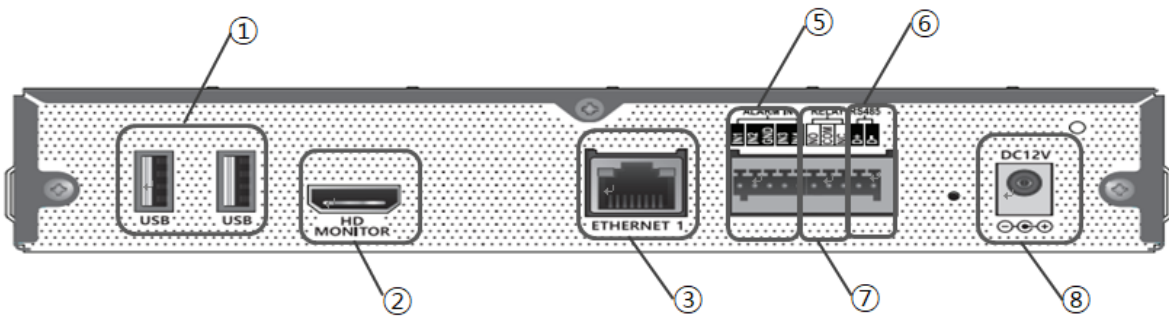


List	Status sign LED	Description
POWER		Red light blinks during the boot phase and green light during operation.

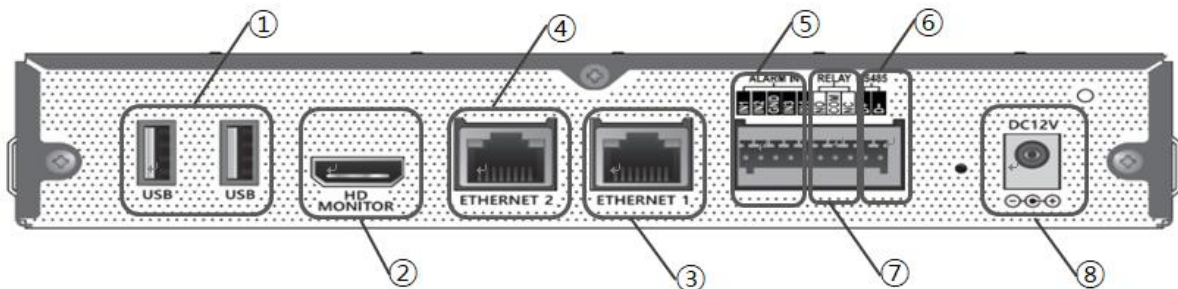
STATUS		Status light blinks when an event occurs after passing the set condition.
ETH1		ETH1 light blinks when communication is take place via the ETH1 port or turns off when communication is not taking place.
ETH2		Headlight turns on when communication is take place via the ETH2 port or turns off when communication is not taking place.

3.Name and functions of rear panel

- 4CH



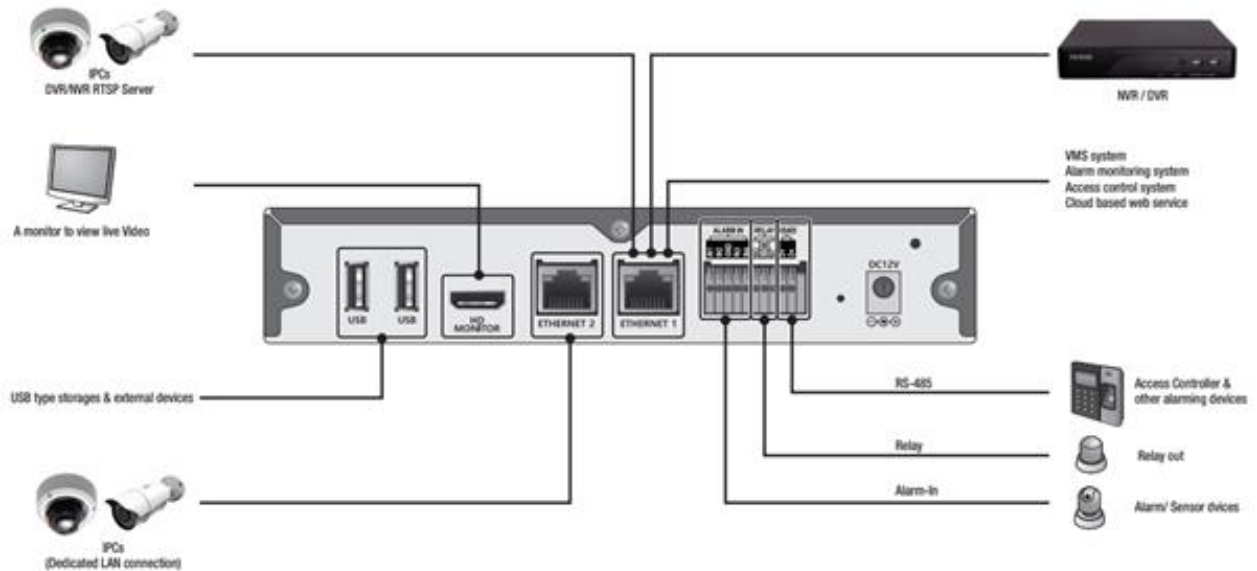
- 8CH / 16CH





No.	Names	Description
①	USB	Universal Serial Bus (USB) ports for additional devices such as USB Mouse.
②	HD MONITOR	For connecting a monitor to view connected cameras. Note, AI Box cannot be configured locally.
③	ETHERNET 1	RJ-45 port for connecting internet and other platforms such as interoperable VMS, recorders and IP cameras.
④	ETHERNET 2	Network port for connecting camera and other through a separate network disconnected from the outside.
⑤	ALARM IN	Alarm input signal line terminal.
⑥	REPLAY	Relay connection terminal.
⑦	RS485	RS485 communication device connection terminal.
⑧	DC12V	12V adapter plug

1. Basic connection configuration



2. Network setting

- Basic requirements of Web

Name	Description
Recommended Browser	Google Chrome, FireFox, MS Edge
OS	Window / Mac / Linux
RAM	≥1GB



- Way to access the Web setting page

1. The factory default network setting is DHCP. Therefore, it is possible to access the IP assigned through the router supported by DHCP (IP can be checked by accessing the Web of the router).

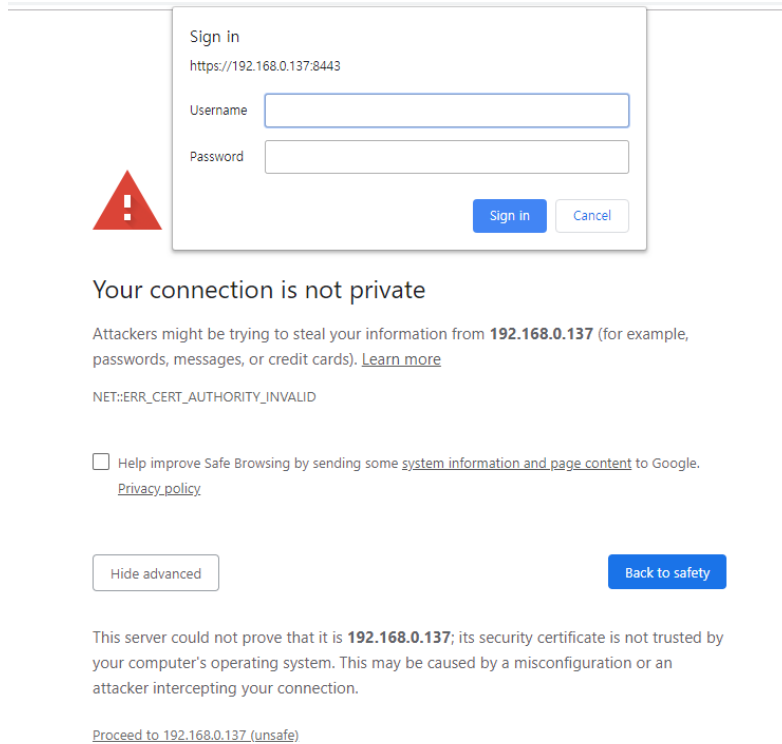
- IP address: `https://<AI Box IP>:8443`

(e. g. : `https://10.10.10.10:8443`)

- ID: ADMIN

- Password: 1234

NOTE: Make sure to use ‘https://’ (Hypertext Transfer Protocol Secure)



2. 'Admin_Tool.exe' allows discover and configure AI BOX in the network. The tool also discovers and configures other devices such as IP cameras, NVR and DVR.

1) Click the 'Search' button to search the AI BOX connection to the network.



Admin Tool V4.13

STEP	MAC Address	Type	IP Address	HTTP Port	Model	SW Ver.	Status	Xid
------	-------------	------	------------	-----------	-------	---------	--------	-----

IP Address: . . DNS1: . . ID:

Subnet Mask: . . DNS2: . . Password:

Gateway: . .

Network Type:

NIC Select:

Set network: Wire Wireless(Wi-Fi)

Ready CAP | NUM

2) The search results are displayed on the screen when search function is completed. You can determine the AI BOX from the model information and click on the product you want to set up in the list.

Admin Tool V4.13

STEP	MAC Address	Type	IP Address	HTTP Port	Model	SW Ver.	Status	Xid
ID/PW MISMATCH	00:11:5F:2A:00:05	STATIC	192.168.200.227	8443	AIBOX-16		Unreachable	0D05002A

IP Address: . . DNS1: . . ID:

Subnet Mask: . . DNS2: . . Password:

Gateway: . .

Network Type:

NIC Select:

Set network: Wire Wireless(Wi-Fi)

Ready CAP | NUM

- 3) Select one of 'DHCP' or 'STATIC' for <Network Type> at the bottom left. Please input the IP Address, Subnet Mask, Gateway, DNS information and click 'APPLY' button.

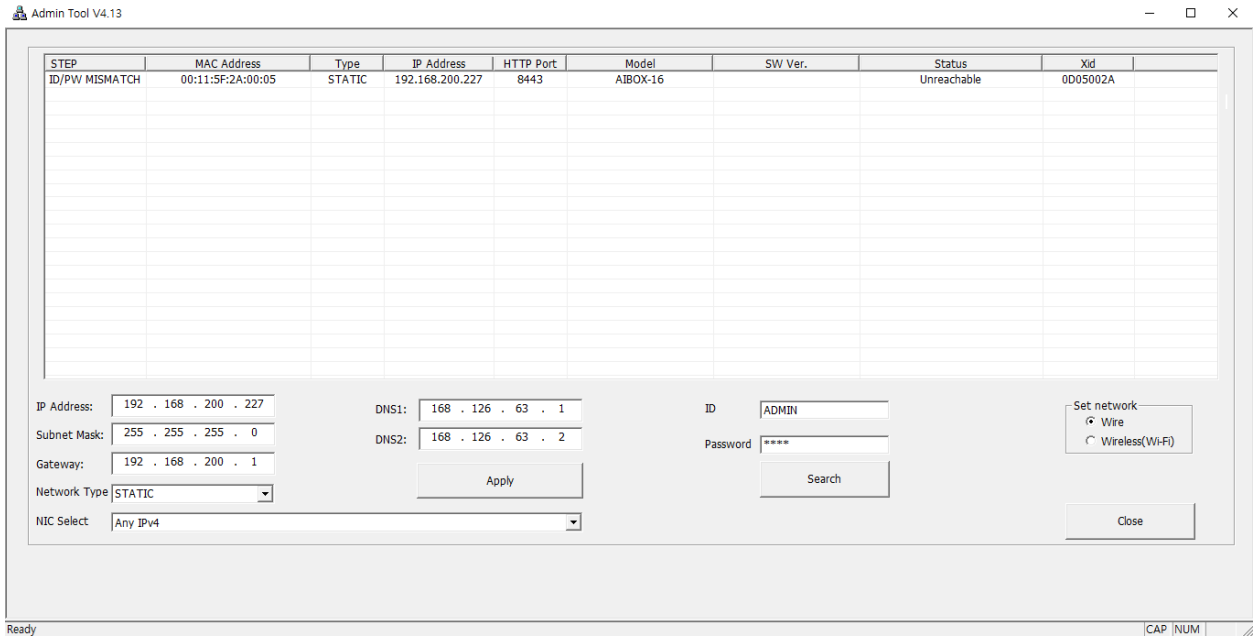
The screenshot shows a window titled "Admin Tool V4.13" with a table and configuration fields. The table has the following data:

STEP	MAC Address	Type	IP Address	HTTP Port	Model	SW Ver.	Status	Xid
ID/PW MISMATCH	00:11:5F:2A:00:05	STATIC	192.168.200.227	8443	AIBOX-16		Unreachable	0D05002A

Below the table are configuration fields:

- IP Address: [. . .]
- Subnet Mask: [. . .]
- Gateway: [. . .]
- DNS1: [. . .]
- DNS2: [. . .]
- Network Type: [DHCP / STATIC]
- NIC Select: [Any IPv4]
- ID: [ADMIN]
- Password: [****]
- Buttons: Apply, Search, Close
- Set network: Wire, Wireless(Wi-Fi)

- 4) After a short period of time, the list will be updated automatically and the network configuration is completed by confirming that the settings are correct.



5) Double click the device information in the list to open the device setting page.

※ Please click ‘Advanced’ button at the bottom and click ‘Go to(unsafe)’ button if you see a security warning as shown below. (Unlike a portal site that uses a public certificate, you may get a warning by using a private certificate) Note: This is a completely safe procedure as the user is only connecting to AI BOX



Your connection is not private

Attackers might be trying to steal your information from **192.168.200.227** (for example, passwords, messages, or credit cards). [Learn more](#)

NET:ERR_CERT_AUTHORITY_INVALID

Help improve Chrome security by sending [URLs of some pages you visit, limited system information, and some page content](#) to Google. [Privacy policy](#)

Advanced

Back to safety



Your connection is not private

Attackers might be trying to steal your information from **192.168.200.227** (for example, passwords, messages, or credit cards). [Learn more](#)

NET:ERR_CERT_AUTHORITY_INVALID

Help improve Chrome security by sending [URLs of some pages you visit, limited system information, and some page content](#) to Google. [Privacy policy](#)

Hide advanced

Back to safety

This server could not prove that it is **192.168.200.227**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

[Proceed to 192.168.200.227 \(unsafe\)](#)

6) Input username and password in the login window

Primary username: ADMIN

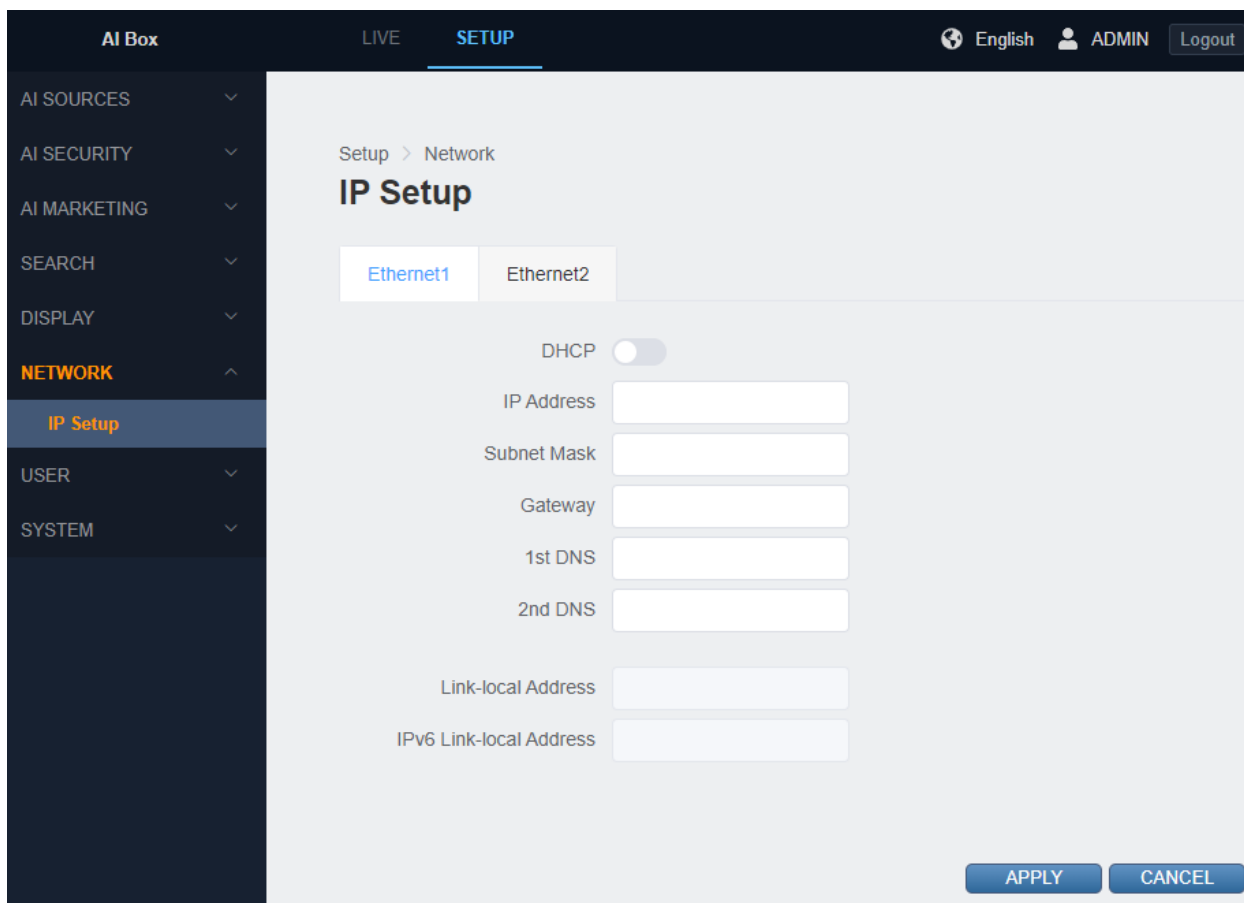
Password: 1234

The image shows a login interface with two input fields. The first field is labeled 'User ID' and the second is labeled 'Password'. Below these fields is a blue button with the text 'LOGIN' in white capital letters.

* It is recommended to change password for safety purposes. To increase security of the device, it is recommended to change to a strong password and reset regularly.

1. Network setting

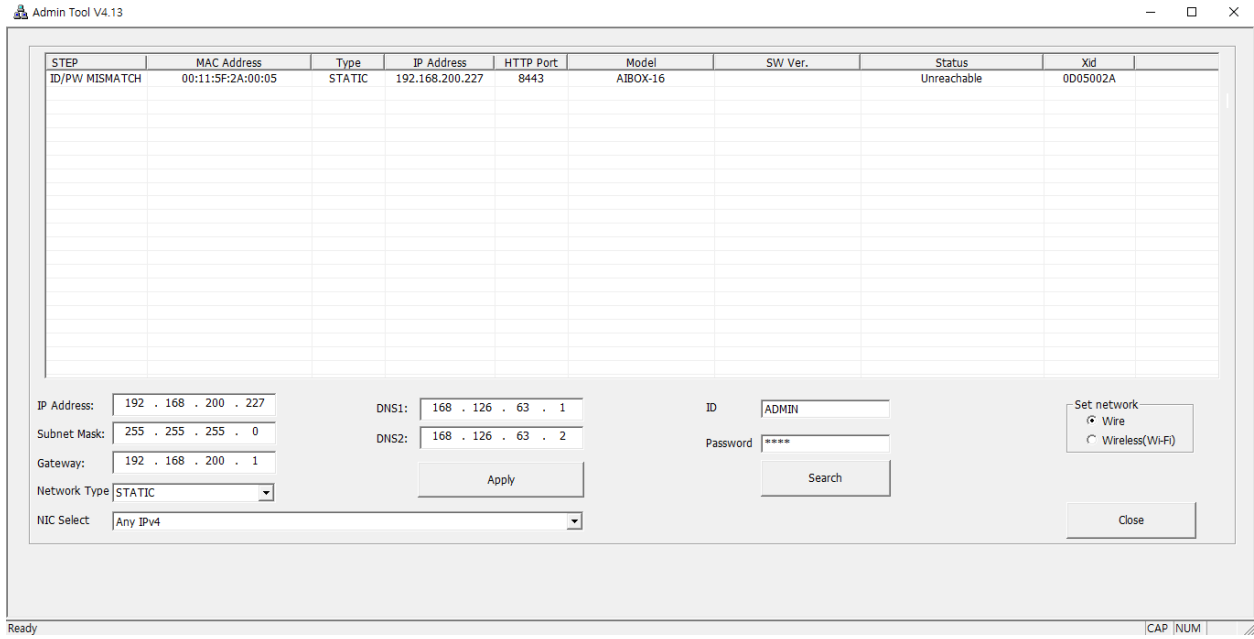
Check and change the network-related settings of the device



Ethernet1, Ethernet2 means Ethernet port on the back of the device to which a network cable is connected

- Automatic IP address allocation

Enable or disable the Dynamic Host Configuration Protocol (DHCP) server. DHCP automatically assigns an IP address to the device if there is a DHCP server on the network.



- Static IP address allocation

Disabling the DHCP settings allows users to manually configure the device's network settings for the network environment.

If DHCP is set to Off, these settings must be manually changed

- IP address: Input your device's IP address.
- Subnet mask: Input the subnet mask value of the device.
- Gateway: Input the gateway value of the device or router that accesses other networks such as Internet/WAN.
- 1st DNS: Input the 1st DNS value of the device.



- 2nd DNS: Input the 2nd DNS value of the device.

- Link local address

It is an IP address automatically assigned to communicate with other devices in the broadcast domain and cannot be changed. NOTE: Link Local Addresses are not supported for DNS.

2. Change user password

Use the Users & User Management page to create and manage user accounts and to change the way the AI BOX manages the user settings.

The screenshot shows the 'User Management' page in the AI Box interface. The breadcrumb trail is 'Setup > User'. The page title is 'User Management'. Below the title is a 'User List' table with the following data:

User ID	Group	Operation
ADMIN	Administrator	Edit

An 'Add' button is located at the bottom right of the table.

Setup > User

User Management

Edit User

User ID	<input type="text" value="ADMIN"/>
Group	<input type="text" value="Administrator"/>
Old Password	<input type="text"/>
Password	<input type="text"/>
Confirm Password	<input type="text"/>

User accounts are created to limit the permissions of individuals who are logged onto the camera. The User Management page also includes four predefined access level settings that include Administrators, Managers, Operators, and Viewers permissions.

- Edit window of use information will pop-up if you press the 'Edit' button.
- Input your current password and new password then press the 'APPLY' button.
- ✓ Current password: Input the current password for user account
- ✓ New password: Input new password

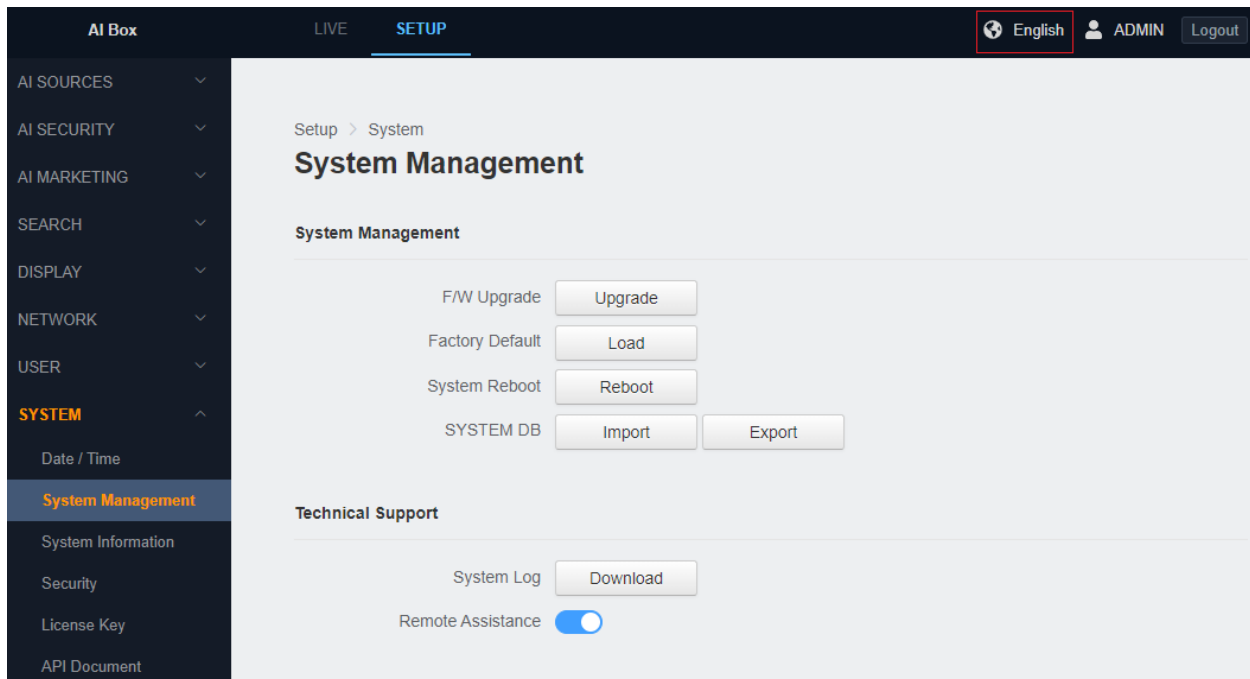


✓ New password Confirm: Input new password once more

- Press the 'APPLY' button to change your password.
- You need to log in again with your new password if you change the password.

3. Language setting

Set the language which will be displayed on the system.





4. Date and Time setting

Set the system date and time.

- **Date / Time**

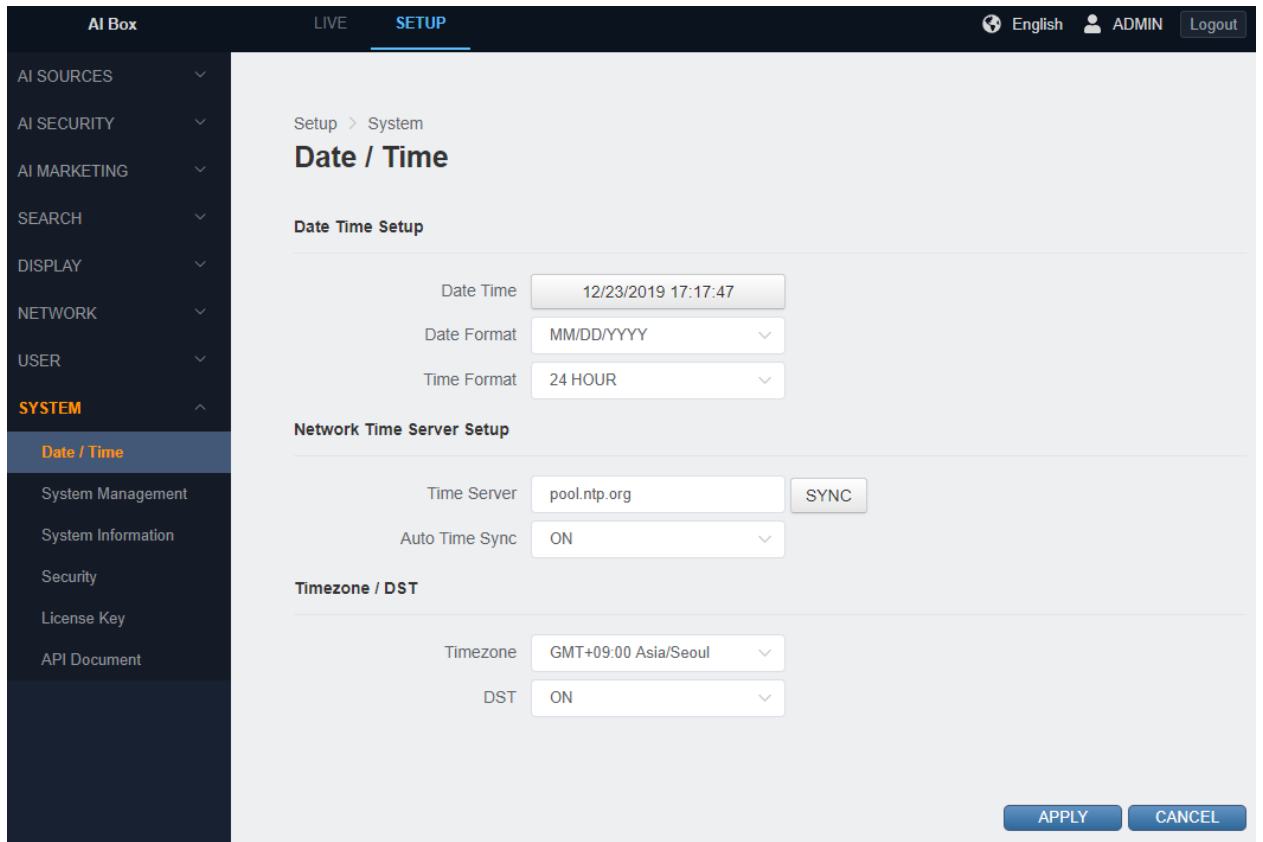
The date and time set on the device are displayed. Change the date and time by pressing the button with the date and time displayed

- **Network Time server setting**

- Time server: Input the address of NTP server. Pressing the 'SYNC' button will communicate with the NTP server information provided to automatically synchronized to change the system date and time.

※ The DNS address of the device must be set correctly if the address of NTP server is a domain.

- Auto Sync: Select whether to synchronize the time periodically through the NTP server.



- Time zone / DST

- Time zone: Select your timezone.
- DST: Choose whether to use daylight saving time.

5.Firmware upgrade

Upgrade device' s firmware.

AI Box LIVE SETUP English ADMIN Logout

AI SOURCES
AI SECURITY
AI MARKETING
SEARCH
DISPLAY
NETWORK
USER
SYSTEM
Date / Time
System Management
System Information
Security
License Key
API Document

Setup > System

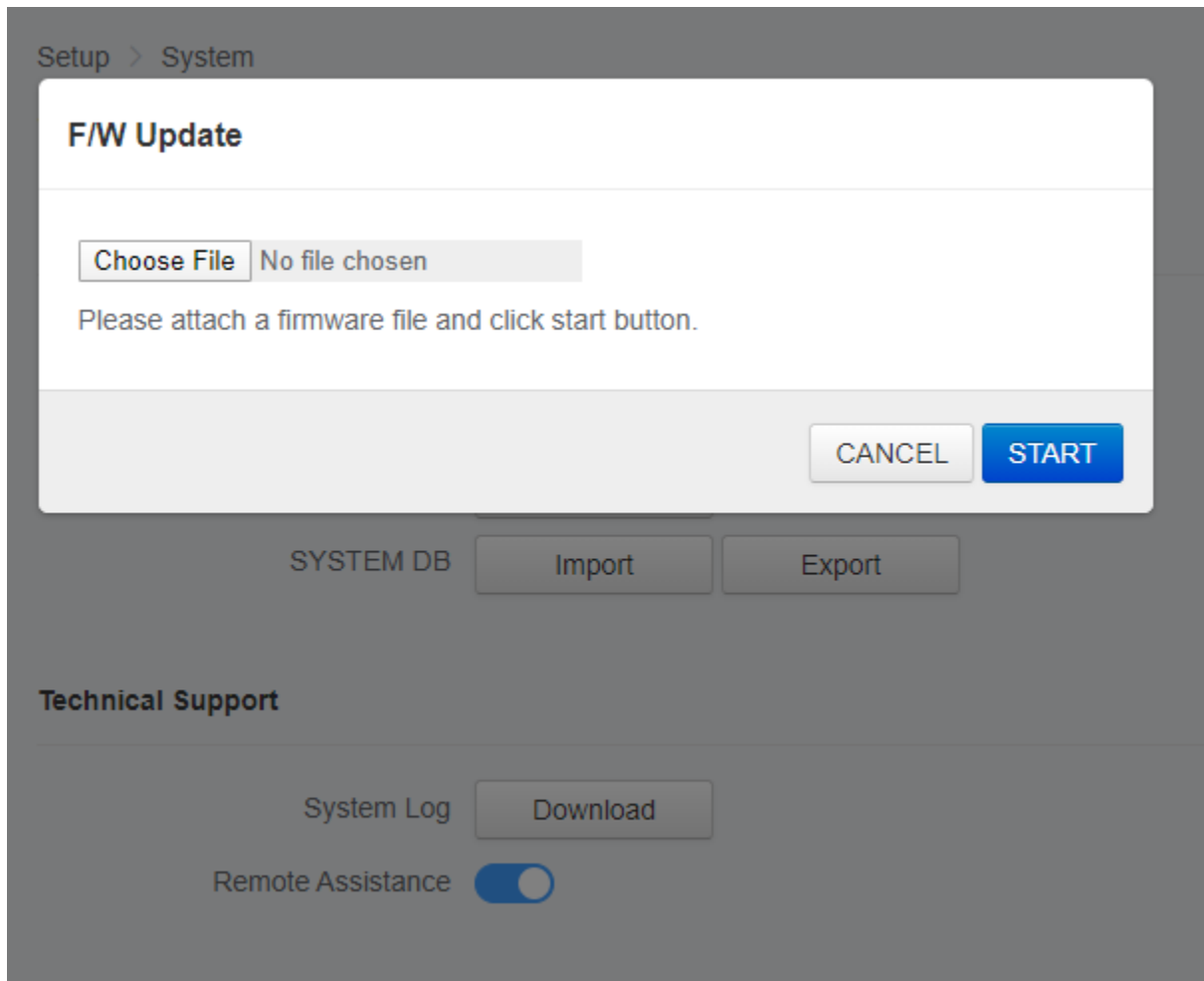
System Management

System Management

F/W Upgrade Upgrade
Factory Default Load
System Reboot Reboot
SYSTEM DB Import Export

Technical Support

System Log Download
Remote Assistance



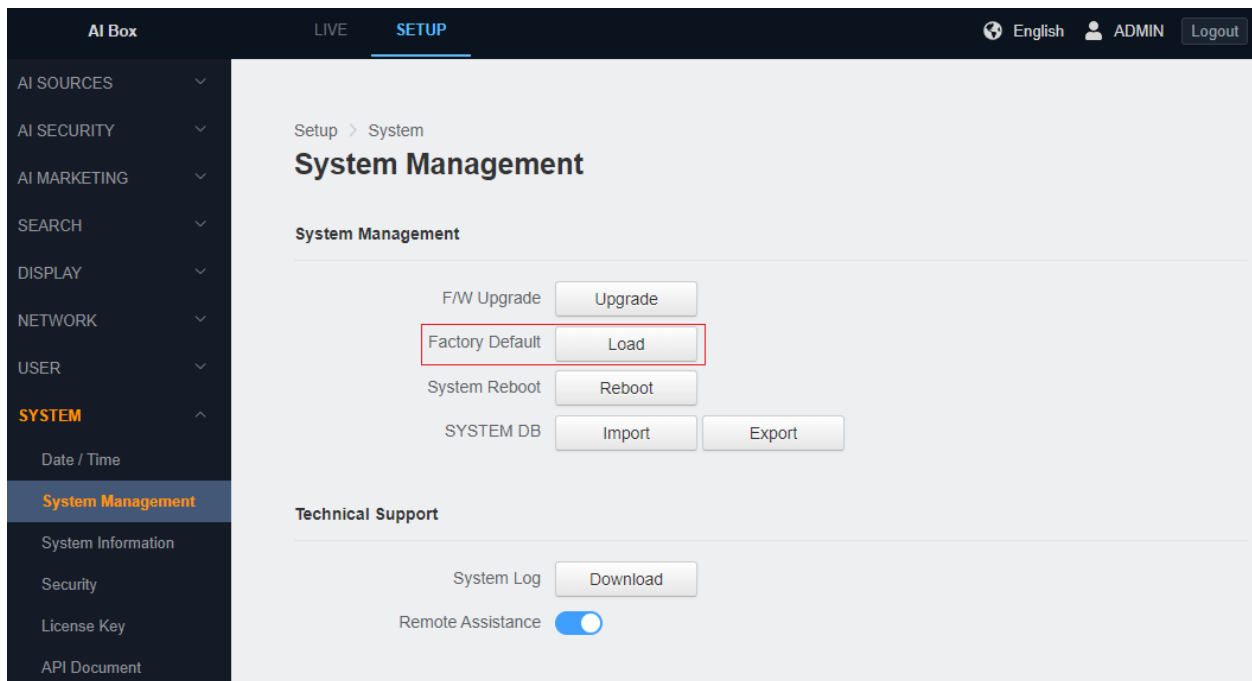
Users can update system firmware if available. All AI BOX functions will shut down during firmware update. Please close any other screens before firmware update. Never disconnect power or LAN cable during the firmware update process. It takes approximately 3-10 minutes for the unit to reboot after firmware update process. NOTE: power cannot be lost when updating firmware since it will cause the update failure and manufacturer maintenance will be required.

- Press the 'Upgrade' button and a firmware upgrade popup will appear
- Attach the firmware file (*.bin) to upgrade
- Press the 'Start' button to start the firmware upgrade
- The device will reboot when the firmware upgrade is complete

※ Please do not operate the device during the firmware upgrade.

6.Factory default

Reset your device' s settings to factory default settings.



- Press the 'OK' button to bring up the factory reset popup.
- The network-related settings will not be reset if you select the 'Network settings remain current' option.
- Click 'OK' button to start factory default.
- The device will reboot when the factory default is complete.

[CAUTION] If the AI BOX is not connected to a Dynamic Host Configuration Protocol (DHCP) network, the IP address settings for the AI BOX will be lost and the server will not recognize the camera. DHCP On is the default setting for the AI BOX IP address





1.Video Source setting

Connect video from a server or device that supports IP cameras or RTSP streaming and configure the default AI algorithm to assign to each video channel

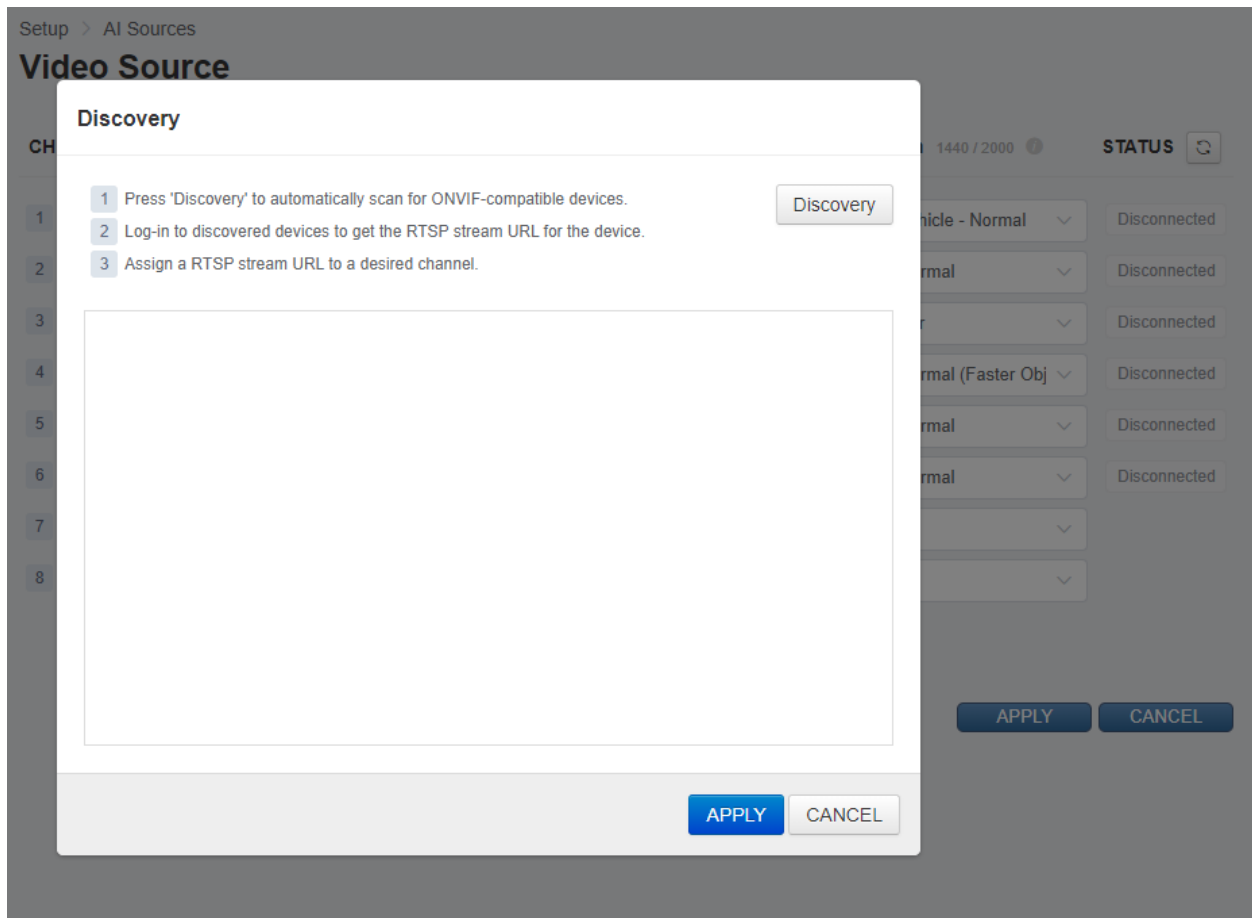
[CAUTION] Video resolution can be connected up to a maximum channel of 2M pixels 30 fps. In other words, you should connect the cable at a lower fps to 7 fps or less to connect all channels when connecting a 4K camera.

The screenshot shows the 'AI SOURCES' configuration page in the GANZ AI Box interface. The page is titled 'Video Source' and is part of the 'SETUP' menu. It features a table with 16 channels, each with a 'NAME', 'URL', 'Discovery' button, 'AI Algorithm', and resolution '480 / 2000'. Channel 1 is pre-filled with '1' and a specific RTSP URL. Channels 2-16 are empty, with their URLs masked as 'rtsp://username:password@ip.port/url'. The 'AI Algorithm' dropdown for channel 1 is set to 'Human / Vehicle - Normal (F)', while others are set to 'None'. The interface includes a sidebar with navigation options like 'AI SECURITY', 'AI MARKETING', 'SEARCH', 'DISPLAY', 'NETWORK', 'USER', and 'SYSTEM'. At the bottom right, there are 'APPLY' and 'CANCEL' buttons.

CH	NAME	URL	Discovery	AI Algorithm	480 / 2000
1	1	rtsp://ADMIN:*****@192.168.200.226:554/live/ma		Human / Vehicle - Normal (F)	
2		rtsp://username:password@ip.port/url		None	
3		rtsp://username:password@ip.port/url		None	
4		rtsp://username:password@ip.port/url		None	
5		rtsp://username:password@ip.port/url		None	
6		rtsp://username:password@ip.port/url		None	
7		rtsp://username:password@ip.port/url		None	
8		rtsp://username:password@ip.port/url		None	
9		rtsp://username:password@ip.port/url		None	
10		rtsp://username:password@ip.port/url		None	
11		rtsp://username:password@ip.port/url		None	
12		rtsp://username:password@ip.port/url		None	
13		rtsp://username:password@ip.port/url		None	
14		rtsp://username:password@ip.port/url		None	
15		rtsp://username:password@ip.port/url		None	
16		rtsp://username:password@ip.port/url		None	

- IP camera / DVR / NVR connection using ONVIF discovery protocol

Video stream address can be configured by searching ONVIF devices connected to the local network.



- Press the 'Discovery' button and the ONVIF Discovery popup will appear.
- Press the 'Discovery' button to search ONVIF devices connected to the local network.
- Input the account information of the device found and press the <Login> button to view the video stream address.



- Assign the video stream address of the ONVIF device to a specific channel.
- The video stream address is inputted in the URL field of the assigned channel when you press the 'APPLY' button.

- **Connection via manual entry of RTSP address**

Connection can be made by directly entering the RTSP address of a device or server that supports standard TCP based RTSP.

- **DVR / NVR auto connection through Plug & Play**

By using a dedicated DVR / NVR supports AI Box Plug & Play, you can connect AI Box automatically through the menu of DVR / NVR without device setting through AI Box's Web UI. (Please refer to the dedicated DVR / NVR user guide for details.)

2. AI algorithm

Set a basic AI algorithm for each video source analysis. Various algorithms can be selected according to the object, distance and purpose to be analyzed. Choosing a particular algorithm can be reduced the number of channels you can support because each algorithm has a different throughput. For example, selecting AI algorithm that requires higher resources from AI BOX, the maximum channel will be reduced.

The default installed algorithm is as follows:

- **Human / Vehicle - Mid**

The algorithm detects medium distance of people and vehicle.



- Human / Vehicle - Far

The algorithm is optimized to distinguish people and object in the far distance.

- Human / Vehicle - Mid (High Speed)

The algorithm is optimized to track fast moving people and vehicle. It can be used when you want to detect fast moving objects more accurately through rules such as 'Line Crossing' or 'Enter / Exit'.

The minimum object recognition size compared to the input screen for each algorithm is as follows:

✓ Minimum detectable object size of Intrusion and Occupancy.

	Person		Vehicle	
	width	height	width	height
Human/Vehicle Far	1.00%	3.00%	2.00%	1.50%
Human/Vehicle Mid	1.25%	4.50%	3.00%	2.25%

✓ Minimum detectable object size of Loitering, Enter / Exit and Line Crossing

	Person		Vehicle	
	width	height	width	height

Human/Vehicle Far	1.25%	5.00%	3.00%	2.50%
Human/Vehicle Mid	2.00%	6.00%	7.00%	6.00%

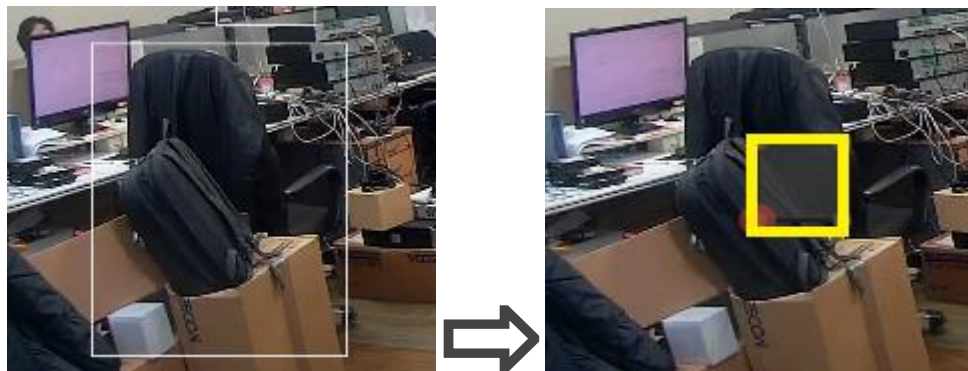
3. False detection filter setting

- Static Object Exclusion Zone

It is possible to specify the area to force exclusion by randomly processing static objects that are erroneous. For example, if a mannequin or a container box is known as a person or a car to be detected, this function can be forcibly excluded.

[Caution] The judgment of whether the object to be detected is within the static object exclusion area is based on the object's center coordinate. Therefore, specifying only the smallest size of the excluded area (as much as it covers the center of the object you want to exclude) can reduce the error that excludes even the actual object to be detected.

(In order to exclude the detected box as follows, only the center of the object should be minimized, not covering the entire box.)



4. Face Recognition

See P.00 for more information on face detection settings.

5. Annotated Live Video

- Live screen composition

- Go to the live or setting page.
- Select multi-view or a specific channel (Multi-view is the same as the H DMI output screen).
- Annotated video stream of the selected channel is played.
- The Annotated video stream address (RTSP URL) of the selected channel is displayed. You can view videos with information drawn directly in standard RTSP viewers such as VLC players.

- ✂ What is Annotated video stream?

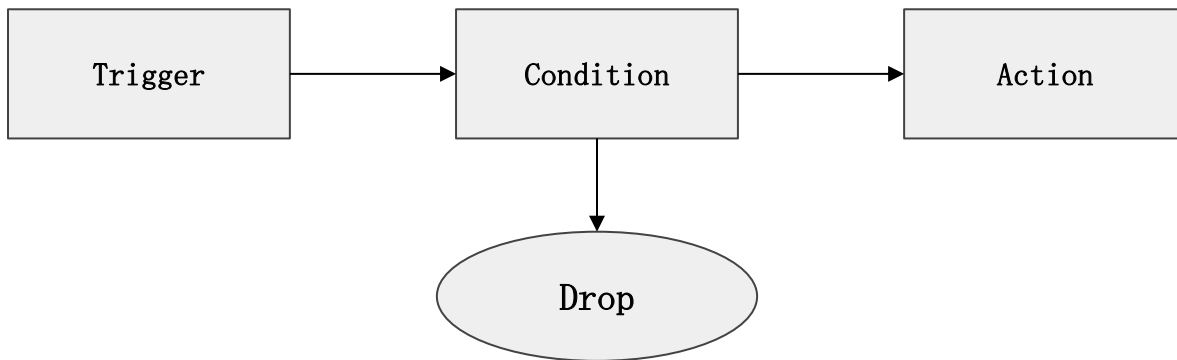
Video stream with tracked object detection box, set zone and AI trigger widget on OSD.

- Show object bounding box

- Grey: Objects in a static state.
- White: Objects in dynamic state.
- Purple: The object where the event occurred. (Appears for a few seconds after the event)

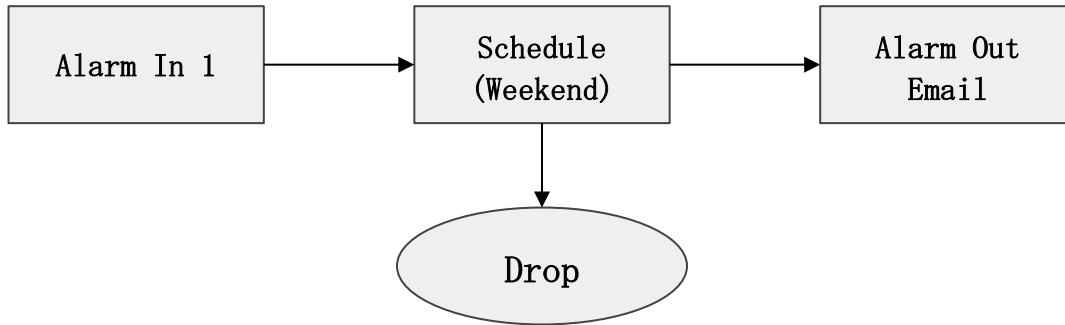
1. Action Rule Overview

Action Rule is composed of Trigger, Condition and Action. After Action Rule is set, it operates by checking Condition when Trigger occurs and performing Action if satisfied.



< Action Rule composition >

- There are 2 types of trigger, AI Trigger and System Trigger. An event discovered by AI in AI Box generates an AI Trigger. Events detected by system sensors such as sensor state changes trigger a System Trigger. Both kinds of triggers can be triggers for Action Rules.
- Condition is the filter component for the trigger. Typically, Schedule condition is to set filter condition by time component.
- The Action defines the action to be performed when Trigger event occurs and Condition is met. It can define and perform various types of actions, including exporting alarm outputs or sending their events to the ONVIF Metadata Stream.

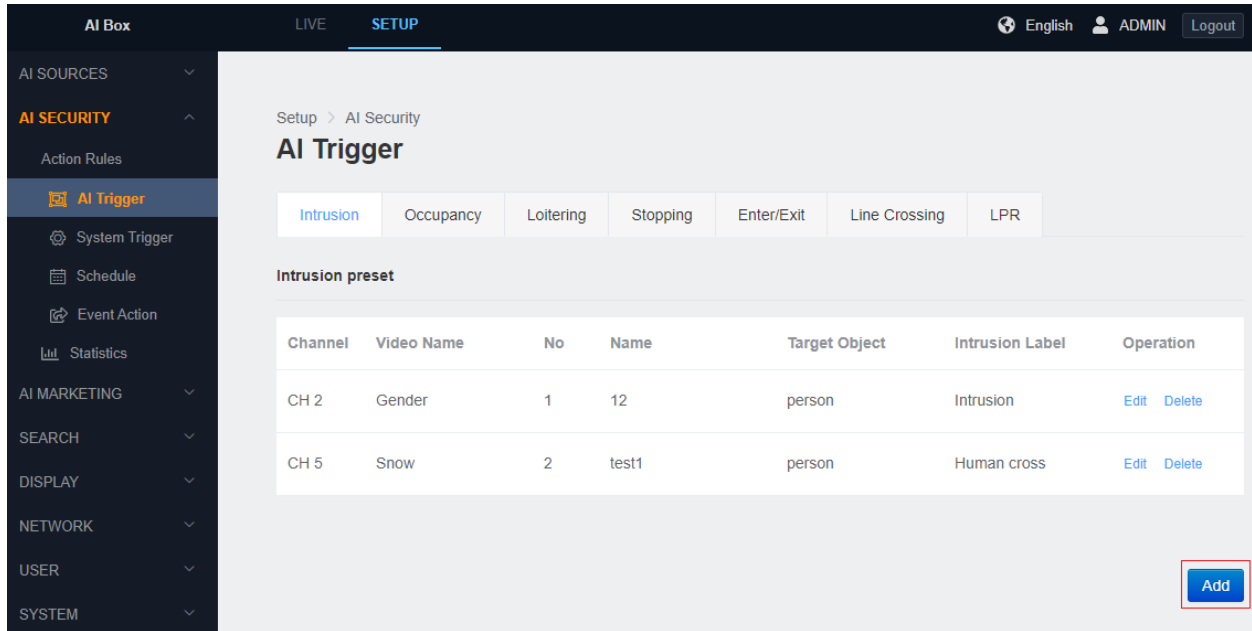


< Action Rule example >

2. AI Trigger setting

- Intrusion

Intrusion is a function that is triggered when a new target appears in the area from the ROI set zone on the screen ([Caution] The determination of whether an object is inside a section is based on the center coordinates of the object .)



- 1) In the SETUP application tab, enter the AI Trigger menu under the 'Action Rules' menu.
- 2) Click the Intrusion tab.
- 3) Click the 'Add' button at the bottom.

Setup > AI Security

AI Trigger

Intrusion | Occupancy | Loitering | Stopping | Enter/Exit | Line Crossing | LPR

Intrusion preset

Name

Video Source

Target Object

Ignore Duplicate Event

Sends intrusion events for each objects.

Advanced Setup

- 4) Input a Trigger preset name.
- 5) Select 'Video Source' .
- 6) Select the discovery target class.

It is possible to select multiple objects for detection.

The detection target may vary depending on the algorithm setting of the selected 'Video Source' .

- 7) Ignore Duplicate Events is an option to ignore event occurrences when an intrusion of another object following an intrusion state occurs.

When the 'check' is enabled, only the first object that breaks into the zone will raise an event. (Intrusion must occur again when all objects are disappeared in a zone before new events occur.)

- 8) The reminder alarm interval is an event frequency setting to remind the user again if the intrusion continues. (Only works when Ignore Duplicate Event is activated)
- 9) Checking the Advanced Settings displays additional setting items.

- 10) Intrusion Label entry allows you to set the counter name of the widget.
- 11) Counter Reset lets you set the time to reset the widget's counter.

You can also reset manually by pressing the Reset button.

12) It will ignore objects that are not moving if the Ignore Static Object is enabled.

(An event may occur if there is no movement and then you move again.)

13) Set ROI zone

Move the entire ROI by dragging its zone.

Move the edge by dragging the edge of the ROI.

Click on the line of the ROI to create a new edge.

Right click the edge of ROI to delete the edge.

14) Drag the Widget rectangle in the upper right corner to set where the widget will appear.



- 15) Click the 'APPLY' button at the bottom to save.
- 16) The Widget will display properly if the trigger is added.
- 17) After confirming the settings, click the 'CLOSE' button at the bottom to check the list.

- **Occupancy**

Occupancy is an item that is triggered when you set an area on the screen and the number of detection targets in the area is out of the specified range. For example, an alarm can be triggered if a car that must be parked in a designated area has disappeared, or if more than two people are entering an area that can only accommodate two people.

[Caution] The determination of whether an object is inside a section is based on the center coordinates of the object.

The screenshot shows the 'AI Box' interface in 'SETUP' mode. The left sidebar contains a navigation menu with categories like AI SOURCES, AI SECURITY, AI MARKETING, SEARCH, DISPLAY, NETWORK, USER, and SYSTEM. Under AI SECURITY, 'AI Trigger' is selected. The main content area shows the 'AI Trigger' configuration page with tabs for Intrusion, Occupancy, Loitering, Stopping, Enter/Exit, Line Crossing, and LPR. The 'Occupancy preset' section contains a table with columns: Channel, Video Name, No, Name, Target Object, Count, and Operation. The table is currently empty, displaying 'No Data'. A blue 'Add' button is located at the bottom right of the table area.



- 1) In the 'SETUP' application tab, enter the AI Trigger menu under the 'Action Rules' menu.
- 2) Click the 'Occupancy' tab.
- 3) Click the 'Add' button at the bottom.

- 4) Input a Trigger preset name.
- 5) Select 'Video Source'.
- 6) Select the discovery target class.

It is possible to select multiple objects for detection.



The detection target may vary depending on the algorithm setting of the selected 'Video Source' .

- 7) Set the 'More than' . It will trigger when the number of detection targets exceeds the set number.
- 8) After the 'Fewer than' is set, it will trigger if the number of targets to be detected is less than the set number.
- 9) Show additional settings when you check for the 'Advanced Setup' .

Setup > AI Security

AI Trigger

Intrusion **Occupancy** Loitering Stopping Enter/Exit Line Crossing LPR

Occupancy preset

Name

Video Source

Target Object

Trigger Method

Fewer than

More than

Trigger an event when the number of objects over or under the limits.

Advanced Setup

Num Objects Label

Fewer Than Label

More Than Label

Count Reset

Ignore Static Object

- 10) 'Count Reset' allows you to set the time to reset the widget's count. You can also reset manually by pressing the 'RESET' button.
- 11) It will ignore objects that are not moving if the 'Ignore Static Object' is enabled. (Only objects that are currently moving are included in the count.)



12) Set ROI zone

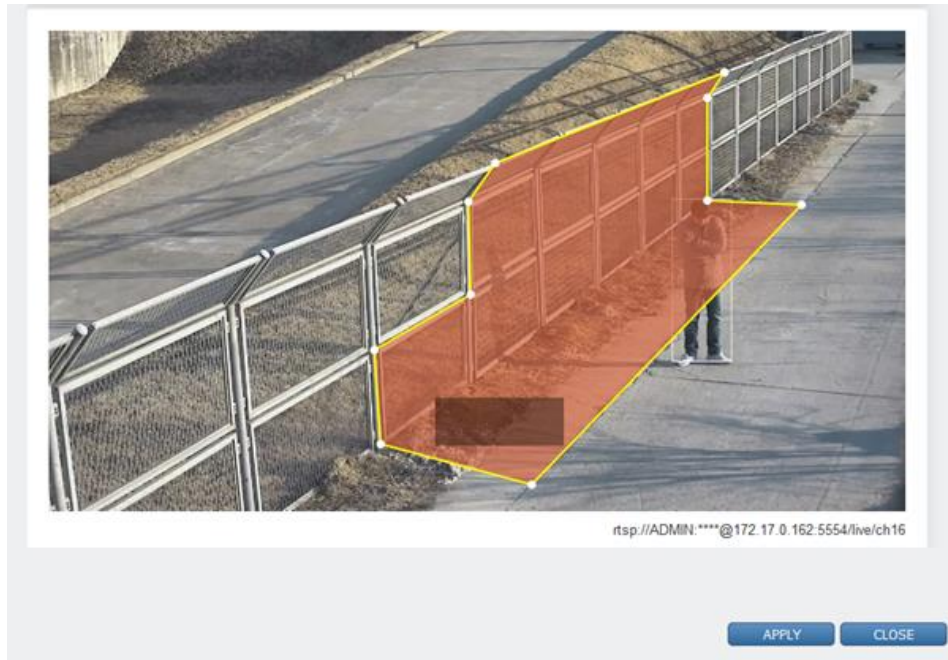
Move the entire ROI by dragging its zone.

Move the edge by dragging the edge of the ROI.

Click on the line of the ROI to create a new edge.

Right click the edge of ROI to delete the edge.

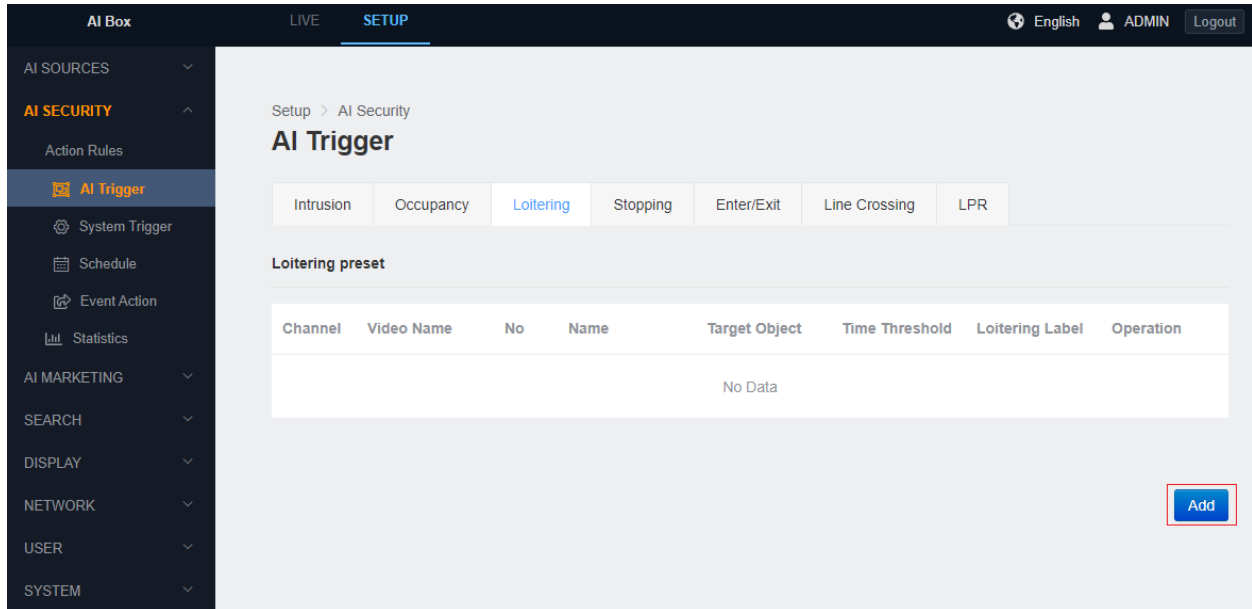
- 13) Drag the Widget rectangle in the upper right corner to set where the widget will appear.



- 14) Click the 'APPLY' button at the bottom to save.
- 15) The Widget will display properly if the trigger is added.
- 16) After confirming the settings, click the 'CLOSE' button at the bottom to check the list.

- **Loitering**

Loitering is a function that is triggered when the detection target stays in the area for a certain period of time from the ROI set zone on the screen. For example, triggers an event when a person has been hanging around in a certain area for the preset period of time. ([Caution] The determination of whether an object is inside a section is based on the center coordinates of the object.)



- 1) In the 'SETUP' application tab, enter the AI Triger menu under the 'Action Rules' menu.
- 2) Click Loitering tab.
- 3) Click the 'Add' button at the bottom.

Setup > AI Security

AI Trigger

Intrusion | Occupancy | **Loitering** | Stopping | Enter/Exit | Line Crossing | LPR

Loitering preset

Name

Video Source

Target Object

Dwell Time second(s)

Maximum time threshold to judge

Advanced Setup

- 4) Input a Trigger preset name.
- 5) Select 'Video Source' .
- 6) Select the discovery target class.

It is possible to select multiple objects for detection.

The detection target may vary depending on the algorithm setting of the selected 'Video Source' .

- 7) Set the 'Dwell Time' . Triggered when detection target stays longer than set time.
- 8) Show additional settings when you check for the 'Advanced Setup' .

Setup > AI Security

AI Trigger

Intrusion | Occupancy | **Loitering** | Stopping | Enter/Exit | Line Crossing | LPR

Loitering preset

Name

Video Source

Target Object

Dwell Time second(s)

Maximum time threshold to judge

Advanced Setup

Loitering Label

Count Reset

- 9) 'Loitering Label' allows you to set the count name of the widget.
- 10) 'Count Reset' allows you to set the time to reset the widget's count. You can also reset manually by pressing the 'RESET' button.
- 11) It will ignore objects that are not moving if the 'Ignore Static Object' is enabled.



12) Set ROI zone.

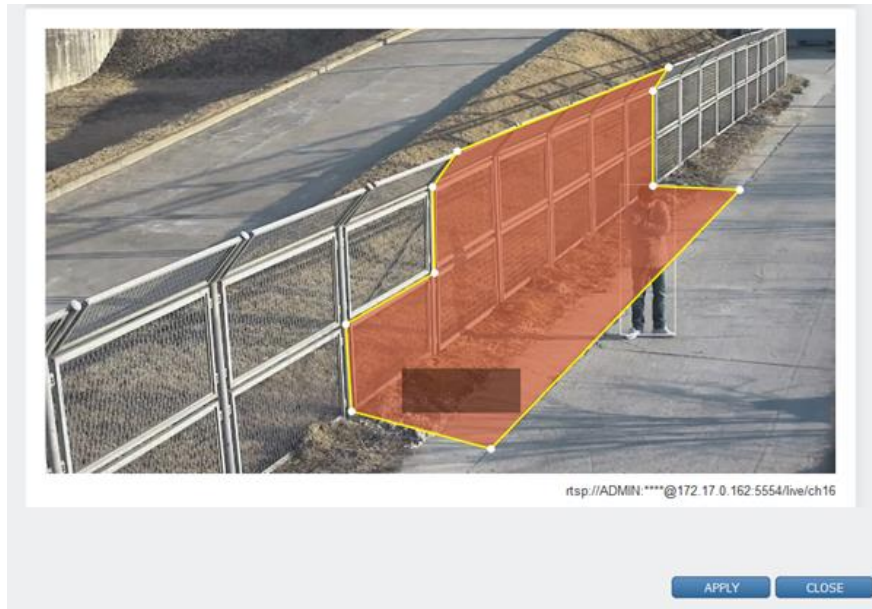
Move the entire ROI by dragging its zone.

Move the edge by dragging the edge of the ROI.

Click on the line of the ROI to create a new edge.

Right click the edge of ROI to delete the edge.

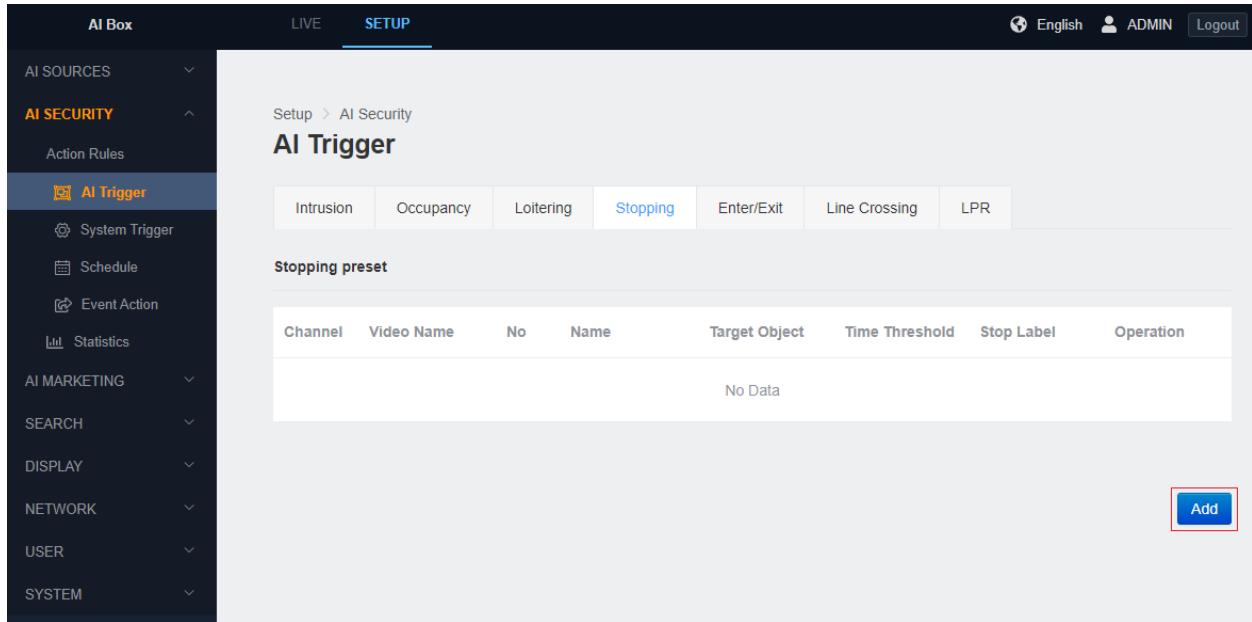
13) Drag the Widget rectangle in the upper right corner to set where the widget will appear.



- 14) Click the 'APPLY' button at the bottom to save
- 15) The Widget will display properly if the trigger is added
- 16) After confirming the settings, click the 'CLOSE' button at the bottom to check the list.

- **Stopping**

Stopping is a function that is triggered when the object stays in the area without movement on the ROI set zone on the screen. For example, it can be used to trigger an event when a car has been parked for a certain time in a certain area. ([Caution] The determination of whether an object is inside a section is based on the center coordinates of the object.)



- 1) In the 'SETUP' application tab, enter the 'AI Trigger' menu under the 'Action Rules' menu.
- 2) Click 'Stopping' tab.
- 3) Click the 'Add' button at the bottom.

Setup > AI Security

AI Trigger

Intrusion | Occupancy | Loitering | **Stopping** | Enter/Exit | Line Crossing | LPR

Stopping preset

Name

Video Source

Target Object

Dwell Time second(s)

Maximum time threshold to judge

Advanced Setup

- 4) Input a Trigger preset name.
- 5) Select 'Video Source' .
- 6) Select the discovery target class

It is possible to select multiple objects for detection.

The detection target may vary depending on the algorithm setting of the selected 'Video Source' .

- 7) Set the 'Dwell Time' . Triggered when detection target stays longer than set time.
- 8) Show additional settings when you check for the 'Advanced Setup' .

Setup > AI Security

AI Trigger

Intrusion | Occupancy | Loitering | **Stopping** | Enter/Exit | Line Crossing | LPR

Stopping preset

Name

Video Source

Target Object

Dwell Time second(s)
Maximum time threshold to judge

Advanced Setup

Stop Label

Count Reset

- 9) 'Stop Label' allows you to set the count name of the widget.
- 10) 'Count Reset' allows you to set the time to reset the widget's count. You can also reset manually by pressing the 'RESET' button.



rtsp://ADMIN.****@172.17.0.162:5554/live/ch16

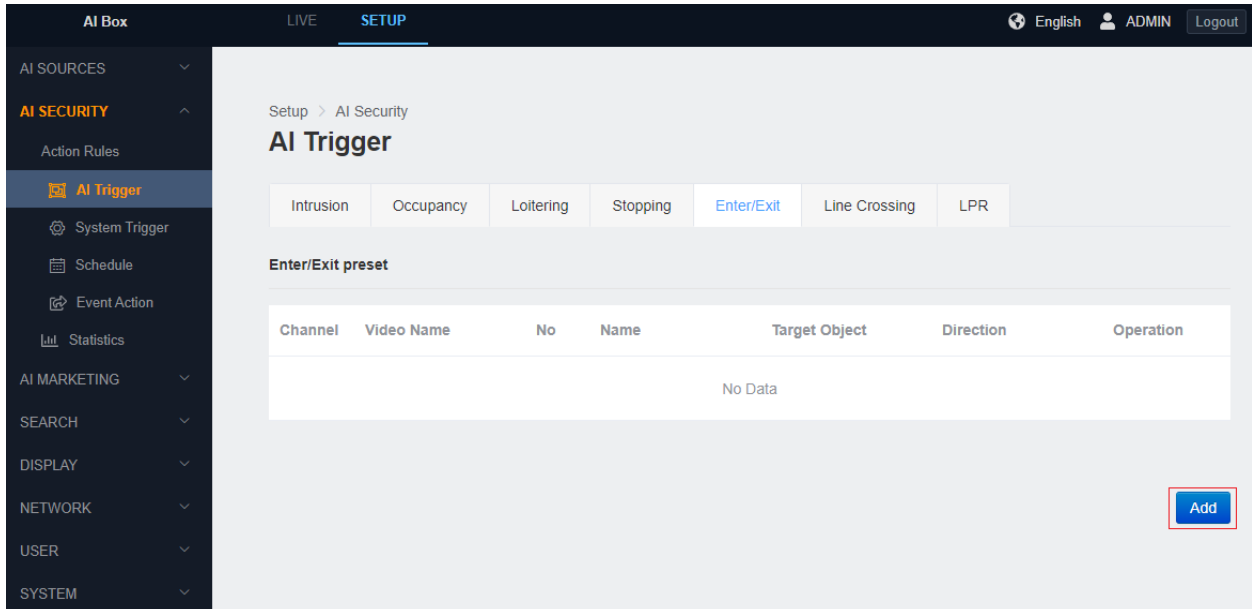
- 11) It will ignore objects that are not moving if the 'Ignore Static Object' is enabled.
- 12) Set ROI zone
 - Move the entire ROI by dragging its zone.
 - Move the edge by dragging the edge of the ROI.
 - Click on the line of the ROI to create a new edge.
 - Right click the edge of ROI to delete the edge.
- 13) Drag the Widget rectangle in the upper right corner to set where the widget will appear.



- 14) Click the 'APPLY' button at the bottom to save.
- 15) The Widget will display properly if the trigger is added.
- 16) After confirming the settings, click the 'CLOSE' button at the bottom to check the list.

- **Enter/Exit**

Enter/Exit is a function that is triggered when the detection target enters or exits based on the boundary of the area on the ROI set zone on the screen. ([Caution] Judging whether an object has entered the zone is based on when the object's center coordinates span the boundary line. The center coordinates can be seen by activating the Object Trajectory option in the DISPLAY-> OSD item.)



- 1) In the 'SETUP' application tab, enter the 'AI Trigger' menu under the 'Action Rules' menu.
- 2) Click 'Enter/Exit' tab.
- 3) Click the 'Add' button at the bottom.

Setup > AI Security

AI Trigger

Intrusion Occupancy Loitering Stopping **Enter/Exit** Line Crossing LPR

Enter/Exit preset

Name

Video Source

Target Object

Direction

Advanced Setup

APPLY **CLOSE**

- 4) Input a Trigger preset name.
- 5) Select 'Video Source' .
- 6) Select the discovery target class.

It is possible to select multiple objects for detection.

The detection target may vary depending on the algorithm setting of the selected 'Video Source' .

- 7) Set 'Direction'

enter - detect the target enters the zone.

exit - detect the target goes out of the zone.

both - detect both directions.

- 8) Show additional settings when you check for the 'Advanced Setup' .

Setup > AI Security

AI Trigger

Intrusion | Occupancy | Loitering | Stopping | **Enter/Exit** | Line Crossing | LPR

Enter/Exit preset

Name

Video Source

Target Object

Direction

Advanced Setup

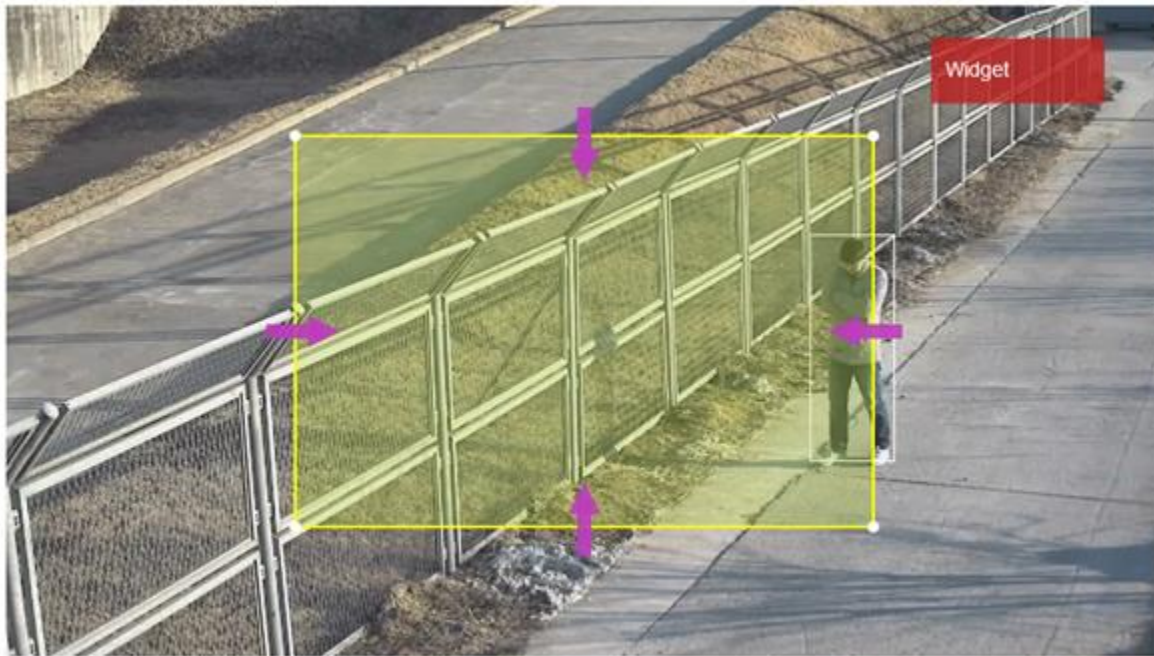
Crossing count
Triggerred at every 1 time(s) of line crossing detected.

Enter Direction Label

Exit Direction Label

Count Reset

- 9) Crossing count function sets how many times an event will occur when an object crossing the area boundary is detected.
- 10) 'Enter/Exit' Direction Label set the label name of the widget count.
- 11) 'Count Reset' allows you to set the time to reset the widget's count. You can also reset manually by pressing the 'RESET' button.



rtsp://ADMIN:****@172.17.0.162:5554/live/ch16

12) Set ROI zone.

Move the entire ROI by dragging its zone.

Move the edge by dragging the edge of the ROI.

Click on the line of the ROI to create a new edge.

Right click the edge of ROI to delete the edge.

13) Drag the Widget rectangle in the upper right corner to set where the widget will appear.

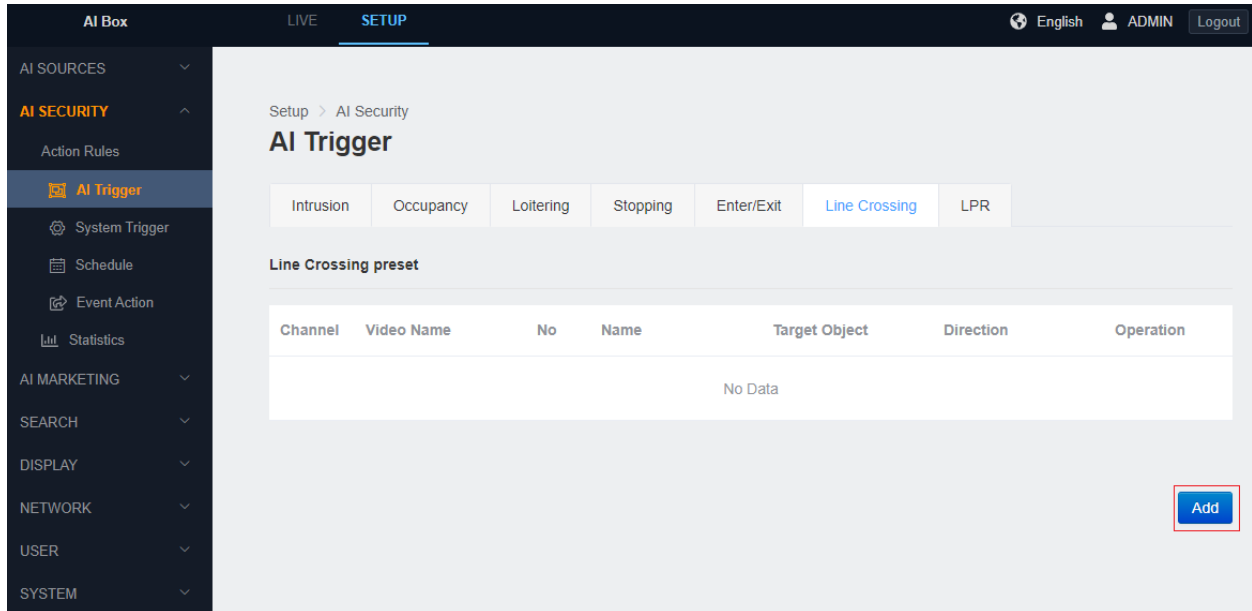


14) Click the 'APPLY' button at the bottom to save.

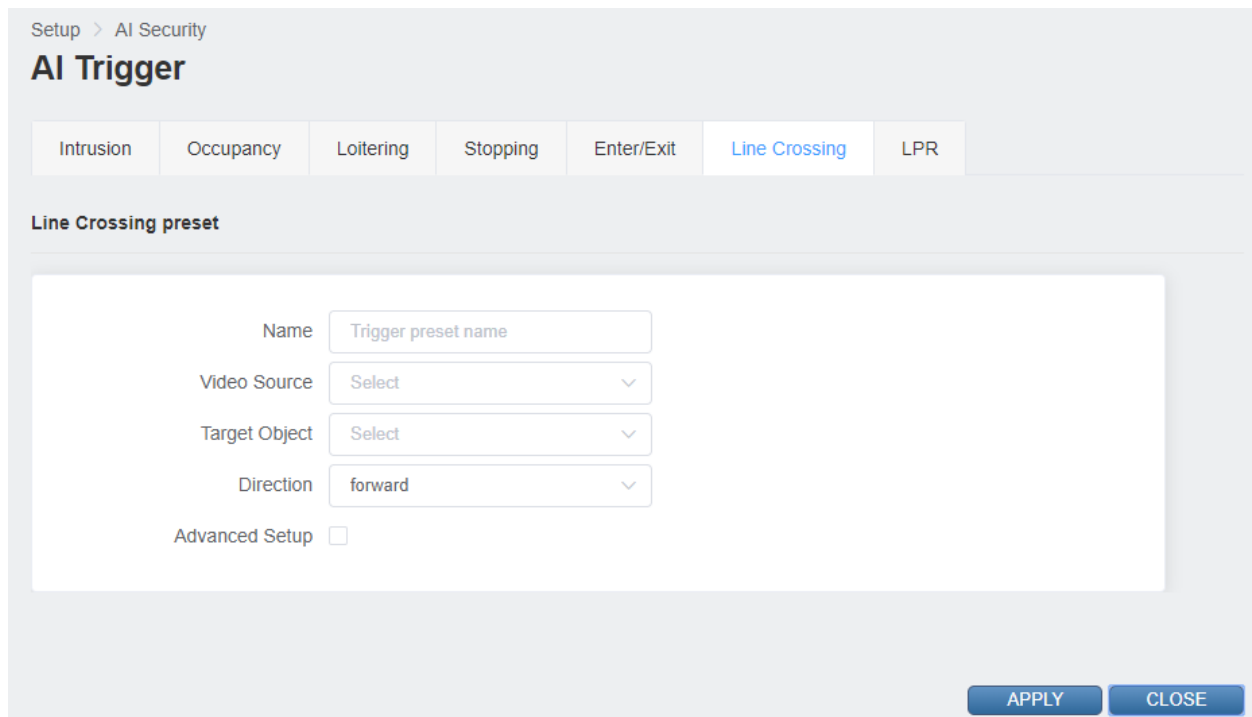
15) The Widget will display properly if the trigger is added.

- **Line Crossing**

Line Crossing is a function set polyline on the screen and it triggered when the detected object crosses the line. ([Caution] Judging whether an object has entered the zone is based on when the object's center coordinates span the boundary line. The center coordinates can be seen by activating the Object Trajectory option in the DISPLAY-> OSD item.)



- 1) In the 'SETUP' application tab, enter the AI Trigger menu under the 'Action Rules' menu.
- 2) Click Line 'Crossing tab'.
- 3) Click the 'Add' button at the bottom.





- 4) Input a Trigger preset name.
- 5) Select 'Video Source' .
- 6) Select the discovery target class.

It is possible to select multiple objects for detection.

The detection target may vary depending on the algorithm setting of the selected 'Video Source' .

- 7) Set Direction.

'forward' -Detects the direction of the green arrow.

'reverse' - Detects the direction of the purple arrow.

'both' -Detects both directions.

- 8) Show additional settings when you check for the 'Advanced Setup' .

Setup > AI Security

AI Trigger

Intrusion | Occupancy | Loitering | Stopping | Enter/Exit | **Line Crossing** | LPR

Line Crossing preset

Name

Video Source

Target Object

Direction

Advanced Setup

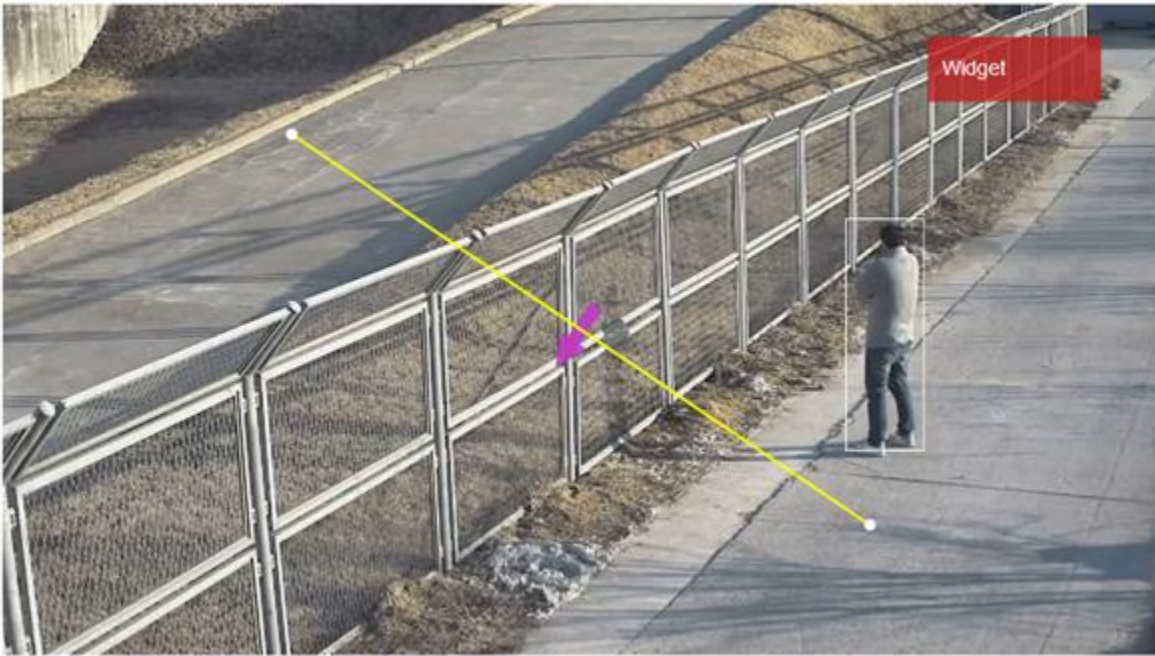
Crossing count
Triggerred at every 1 time(s) of line crossing detected.

Forward Direction Label

Reverse Direction Label

Count Reset

- 9) 'Crossing count' function sets how many times an event will occur when an object crossing the area boundary is detected.
- 10) 'Forward/Reverse Direction Label' sets the label name of the widget counter.
- 11) 'Count Reset' allows you to set the time to reset the widget's count. You can also reset manually by pressing the 'RESET' button.



12) Set 'Polyline' .

Move the edge by dragging the edge of the 'Polyline' .

Click on the line of the 'Polyline' to create a new edge.

Right click the edge of 'Polyline' to delete the edge.

13) Drag the Widget rectangle in the upper right corner to set where the widget will appear.



- 14) Click the 'APPLY' button at the bottom to save.
- 15) The Widget will display properly if the trigger is added.
- 16) After confirming the settings, click the 'CLOSE' button at the bottom to check the list.

3. System Trigger setting

- Alarm In

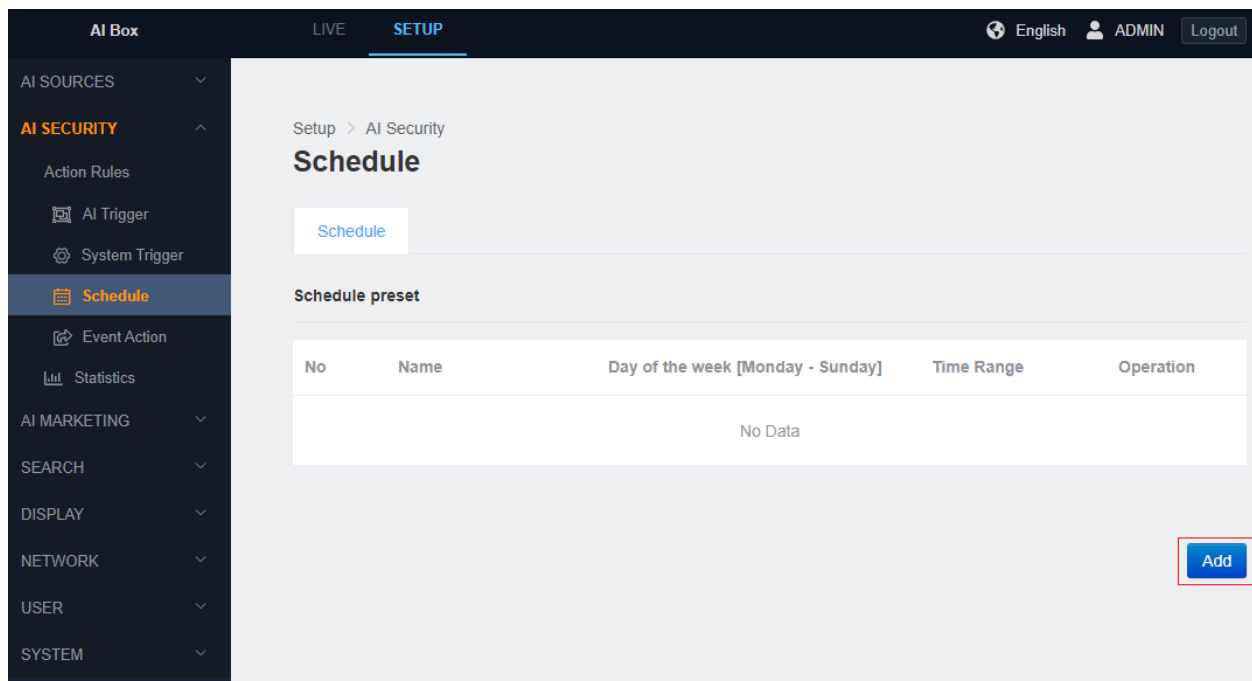
Alarm In does not require a separate preset setting. Alarm In can be added directly in Action Rule setting.

- Recurrence

Create a Recurrence preset.

It is possible to add the Preset name and pattern(time).

4. Schedule setting



- 1) In the 'SETUP' application tab, enter the Schedule menu under the 'Action Rules' menu.
- 2) Click the 'Add' button at the bottom.

Setup > AI Security

Schedule

Schedule

Schedule preset

Name	<input type="text" value="Schedule preset name"/>
Day of the week	<input type="text" value="Select"/>
Time Range	<input type="text" value="00:00"/> ~ <input type="text" value="00:00"/>

APPLY CLOSE

- 3) Input the schedule preset name.
- 4) Select the day.
- 5) Select the start time and end time of the schedule.
- 6) Click the 'APPLY' button at the bottom to save.

Setup > AI Security

Schedule

Schedule

Schedule preset

No	Name	Day of the week [Monday - Sunday]	Time Range	Operation
1	test	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	01:00 ~ 23:00	Edit Delete

Add

7) Check the schedule preset added from the list.

※ All 24 hours will be included in the schedule if you set the same start and end time.

Name

Day of the week

Time Range ~

<Weekend 24 hours setup example>

※ Please set it up like as follows if you need a schedule beyond midnight.

Setup > AI Security

Schedule

Schedule

Schedule preset

Name

Day of the week + 4

Time Range ~

APPLY CLOSE

<Weekday non-working time settings example>

It will be included in the schedule until the end time of the next day of the set day if the Time Range set pass the midnight, In the example above, Monday and Friday are set so the actual schedule is valid until 9:00 AM on Saturday.

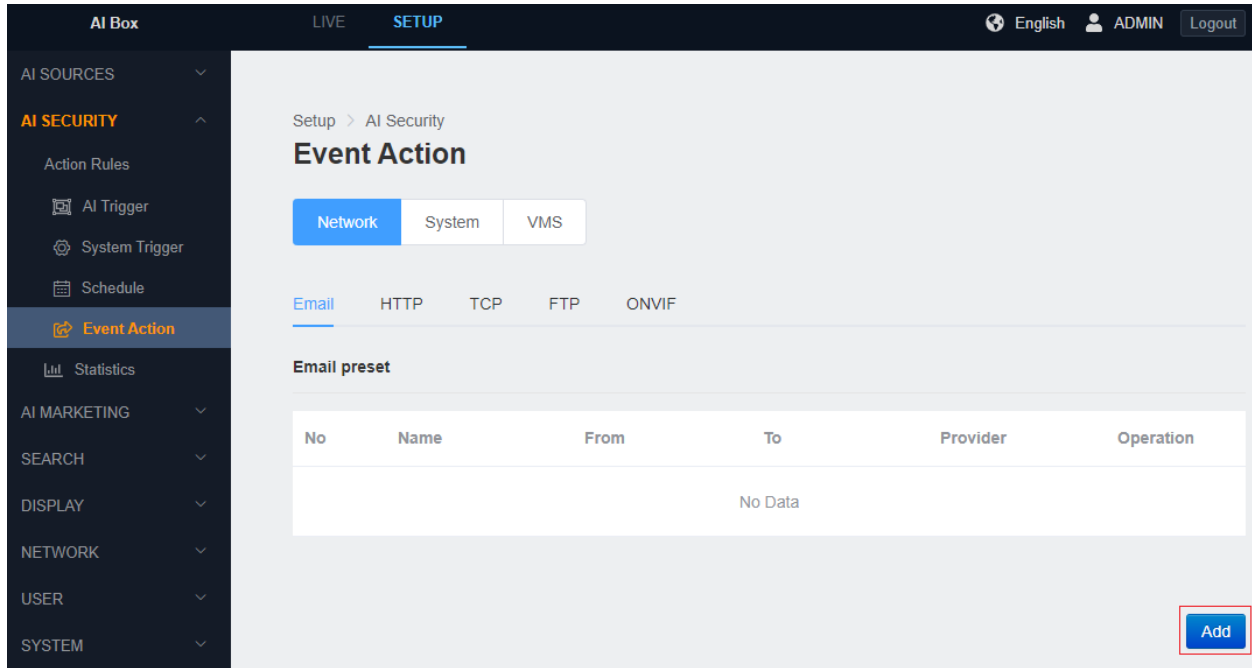
5. Event Action setting

Event actions are classified into three categories: Network, System, and VMS.

- Network Action Event

■ Email

Set Email preset in the Email menu. In the Email preset, set the necessary value for sending email such as SMTP server information. You can also send a test email to confirm that your settings are correct.



- 1) In the 'SETUP' application tab, enter the Action menu below the 'Action Rules' menu.
- 2) Click the 'Email' tab to enter the Email preset list and click the 'Add' button.



Setup > AI Security

Event Action

Network System VMS

Email HTTP TCP FTP ONVIF

Email preset

Name

To

Multiple names separated by commas(,)

Attach Snapshot

- 3) Input a name for the Email preset in Name tab
- 4) Input the email address you want to receive in 'TO'
- 5) Check the 'Attach Snapshot' to display the Snapshot transfer sub-settings.

Name

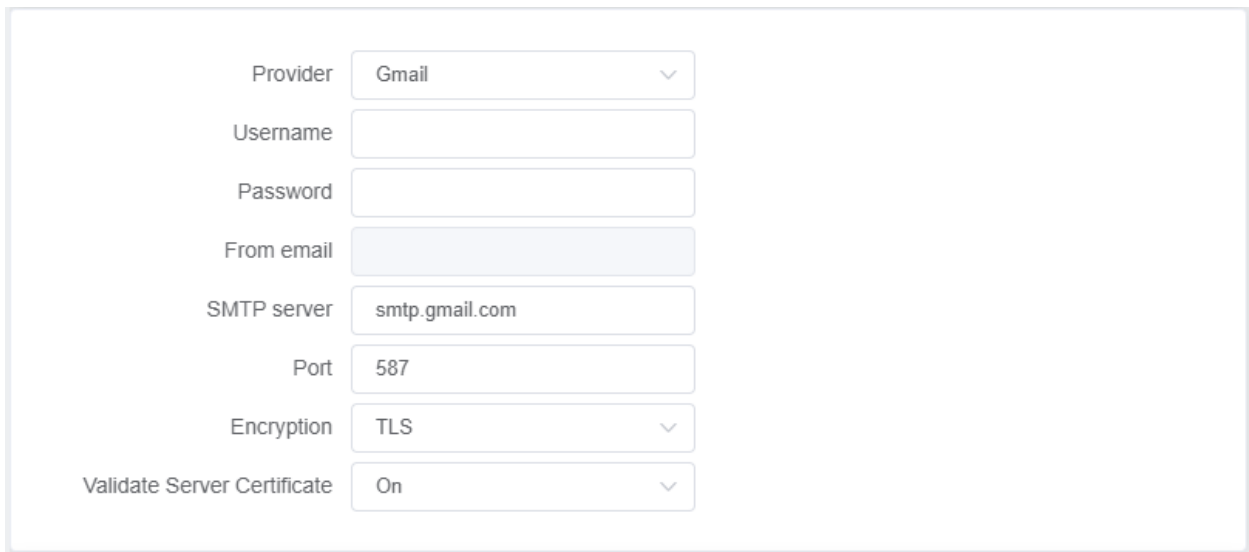
To

Multiple names separated by commas(,)

Attach Snapshot

Snapshot Time Range

- 6) Snapshots occur approximately once every second. Set the time range for the snapshots you want to receive by email.
- 7) Select a service provider in the Provider tab. Please select the 'Custom' if the service provider you want to use is not listed.



The image shows a screenshot of an email configuration interface. It contains several input fields and dropdown menus:

- Provider:** A dropdown menu with 'Gmail' selected.
- Username:** An empty text input field.
- Password:** An empty text input field.
- From email:** A text input field with a light blue background.
- SMTP server:** A text input field containing 'smtp.gmail.com'.
- Port:** A text input field containing '587'.
- Encryption:** A dropdown menu with 'TLS' selected.
- Validate Server Certificate:** A dropdown menu with 'On' selected.

- 8) Input a user name and password that can authenticate with the Email service provider.
- 9) Input the SMTP server address and port number.
- 10) Select Encryption type.
- 11) Select the certificate validation option for the SMTP server.

The screenshot shows a configuration interface for an Event Action Message. It includes a dropdown menu set to 'Use template' with a 'Use' button, another dropdown menu set to 'Select to add tokens' with an 'Add' button, an empty 'Editable Box' for text input, and a 'Message Example' section with a light blue background.

12) Edit the Email action message. You can configure the message by using a template or by including an event attribute token.

Message Example

```
1
My AI Trigger
Enter/Exit
3
00115F2A0096
1561961100.123000
2000-07-01T00:00:00.012345+00:00
```

13) Check the Message Example for an example of the actual message being sent.

14) Click the 'TEST' button to confirm that the receiving test Email's settings are correct.



15) Click the 'APPLY' button at the bottom to save.

16) Check the Email preset section you added in the list.

Setup > AI Security

Event Action

Network System VMS

Email HTTP TCP FTP ONVIF

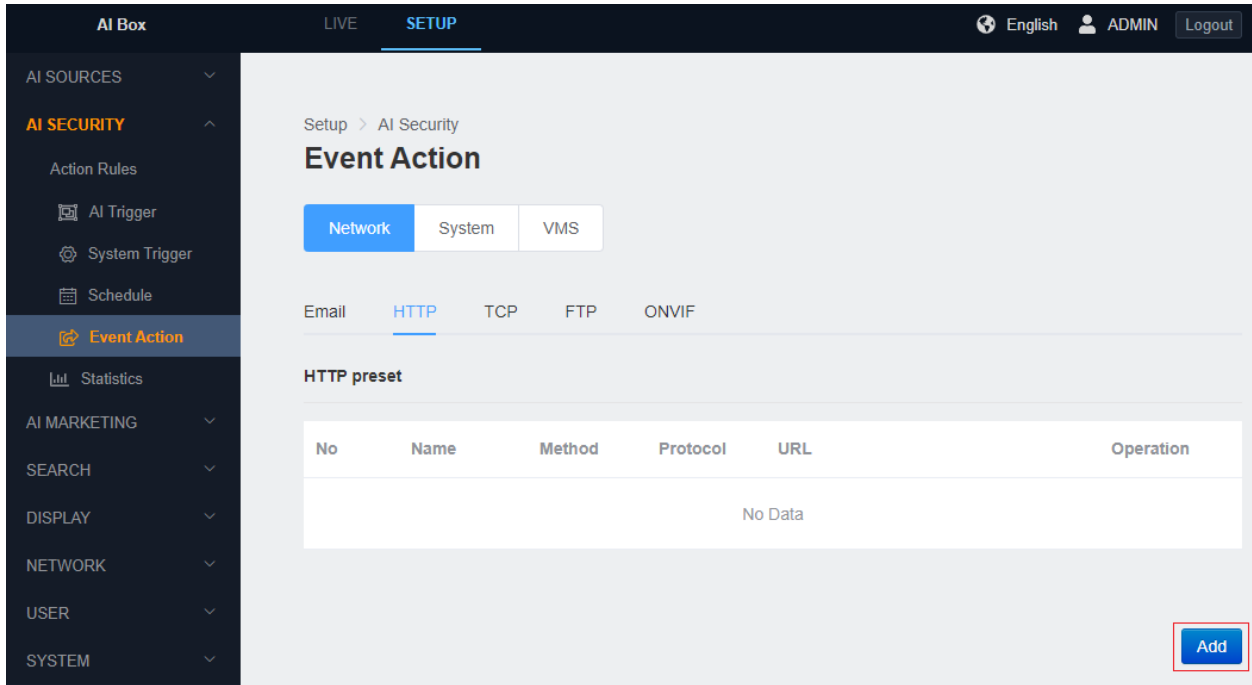
Email preset

No	Name	From	To	Provider	Operation
1	TEST	USER	test@test.com	Gmail	Edit Delete

Add

■ HTTP

You can set the HTTP callback preset in the HTTP tab. In the HTTP preset, set server address and authentication information for receiving the message. In addition, the data format to be transmitted when an event occurs can be set using the event property value token. You can also send a test message to check if the settings are correct.



- 1) In the 'SETUP' tab, enter the 'Event Action' menu under the 'Action Rules' menu.
- 2) Click the HTTP Tab to enter the list of HTTP callback presets and click the 'Add' button.

Setup > AI Security

Event Action

Network System VMS

Email HTTP TCP FTP ONVIF

HTTP preset

Name	<input type="text" value="Action preset name"/>
Protocol	<input type="text" value="HTTP"/>
URL	<input type="text" value="http:// your-domain-name.com/path"/>
Authentication	<input type="text" value="None"/>
Method	<input type="text" value="POST"/>
Content-Type	<input type="text" value="multipart/form-data"/>
Attach Snapshot	<input type="checkbox"/>

- 3) Type the name of the HTTP callback preset in the Name section.
- 4) Select HTTP/HTTPS protocol.
- 5) Input the URL of the server.
- 6) Check the Attach Snapshot to display the Snapshot transfer sub-settings.

Name	<input type="text" value="Action preset name"/>
Protocol	<input type="text" value="HTTP"/>
URL	<input type="text" value="http:// your-domain-name.com/path"/>
Authentication	<input type="text" value="None"/>
Method	<input type="text" value="POST"/>
Content-Type	<input type="text" value="multipart/form-data"/>
Attach Snapshot	<input type="checkbox"/>

7) Snapshots occur approximately once every second. Set the time range for the snapshot to attach.

Event Action Message	<input type="text" value="Use template"/>	<input type="button" value="Use"/>
	<input type="text" value="Select to add tokens"/>	<input type="button" value="Add"/>
Editable Box	<input type="text"/>	
Message Example	<input type="text"/>	

8) Edit the HTTP action message. You can configure the message by using a template or by including an event attribute token.



Message Example

```
1
My AI Trigger
Enter/Exit
3
00115F2A0096
1561961100.123000
2000-07-01T00:00:00.012345+00:00
```

- 9) Check the Message Example for an example of the actual message being sent
- 10) Click the 'TEST' button to confirm that the receiving test Email's settings are correct
- 11) Click the 'APPLY' button at the bottom to save

Setup > AI Security

Event Action

Network System VMS

Email HTTP TCP FTP ONVIF

HTTP preset

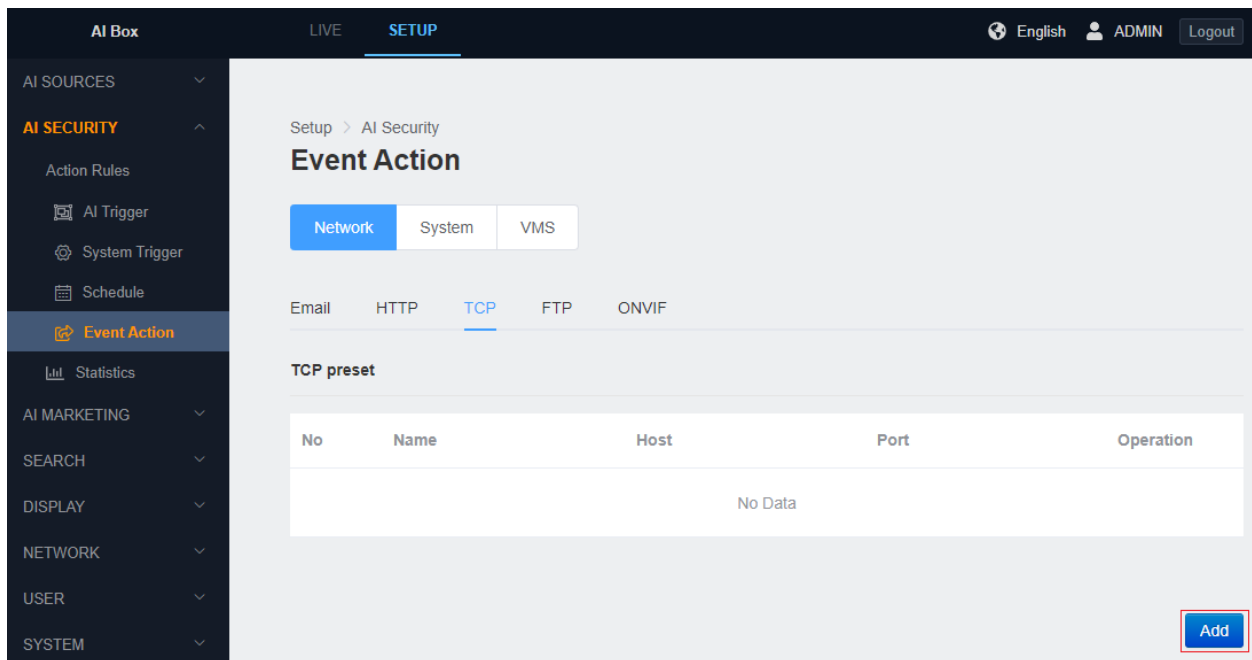
No	Name	Method	Protocol	URL	Operation
1	test	POST	HTTP	http://test.com	Edit Delete

Add

- 12) Check the HTTP preset section you added in the list.

■ TCP

You can set the TCP callback preset in the TCP section. The TCP preset sets the server address and port information for receiving messages. In addition, the message format to be sent when an event occurs can be set using the event property value token. You can also send a test message to confirm that the settings are correct.



The screenshot shows the GANZ AI Security Setup interface. The top navigation bar includes 'AI Box', 'LIVE', and 'SETUP'. The left sidebar lists various menu items, with 'Event Action' highlighted. The main content area is titled 'Event Action' and has tabs for 'Network', 'System', and 'VMS'. Under the 'Network' tab, there are sub-tabs for 'Email', 'HTTP', 'TCP', 'FTP', and 'ONVIF'. The 'TCP' sub-tab is selected, showing a 'TCP preset' section with a table. The table has columns for 'No', 'Name', 'Host', 'Port', and 'Operation', and currently contains no data. An 'Add' button is located at the bottom right of the table area.

- 1) In the 'SETUP' tab, enter the 'Event Action' menu under the 'Action Rules' menu.
- 2) Click the TCP Tab to enter the TCP preset list and click the 'Add' button.

Setup > AI Security

Event Action

Network System VMS

Email HTTP TCP FTP ONVIF

TCP preset

Name

Host

Port

- 3) Input a name for the TCP preset in Name section.
- 4) Input the host IP address or domain name where the TCP receiving server is running.
- 5) Input the Host port number of the TCP receiving server.

Event Action Message

Editable Box

Message Example



- 6) Edit the TCP action message. You can configure the message by using a template or by including an event attribute token.

Message Example

```
1
My AI Trigger
Enter/Exit
3
00115F2A0096
1561961100.123000
2000-07-01T00:00:00.012345+00:00
```

- 7) Check the 'Message Example' for an example of the actual message being sent.
- 8) Click the 'TEST' button to send the example message to the server and check whether it is received.
- 9) Click the 'APPLY' button at the bottom to save.

Setup > AI Security

Event Action

Network System VMS

Email HTTP **TCP** FTP ONVIF

TCP preset

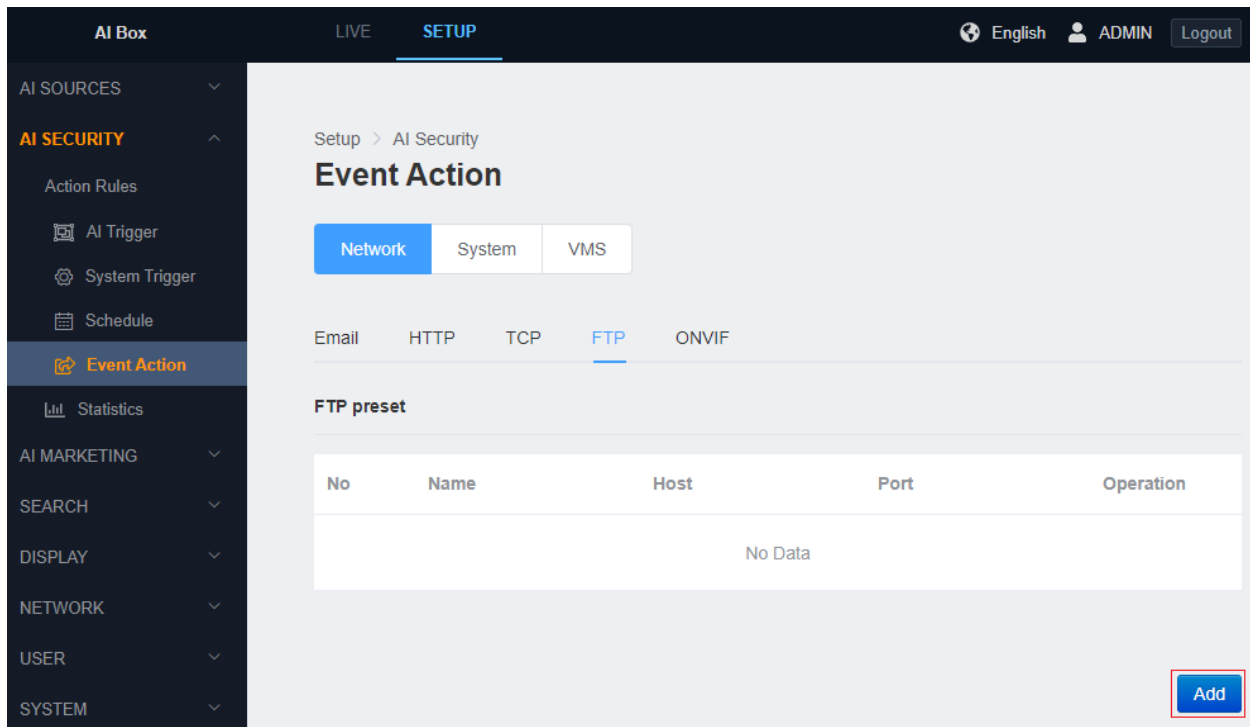
No	Name	Host	Port	Operation
1	test	test	1	Edit Delete

[Add](#)

- 10) Check the TCP preset section that you added in the list.

■ FTP

You can set the FTP callback preset in the FTP section. The FTP preset sets the server address and port information for receiving messages. In addition, the message format to be sent when an event occurs can be set using the event property value token. You can also send a test message to confirm that the settings are correct.



- 1) In the 'SETUP' tab, enter the 'Event Action' menu under the 'Action Rules' menu.

- 2) Click the FTP Tab to enter the FTP preset list and click the 'Add' button.

Setup > AI Security

Event Action

Network System VMS

Email HTTP TCP **FTP** ONVIF

FTP preset

Name

Host

Port
(Default: :21, 1025~65535)

Passive Mode

Username

Password

- 3) Input a name for the FTP preset in Name section.
- 4) Input the host IP address or domain name where the FTP receiving server is running.
- 5) Input the Host port number of the FTP receiving server.

Snapshot Time Range

- 6) Edit the Snapshot Time Range (From secs before, To secs after)

Directory Name Format	<input type="text" value="Use template"/>	Use
	<input type="text" value="Select to add tokens"/>	Add
<input type="text"/>		
File Name Format	<input type="text" value="Use template"/>	Use
	<input type="text" value="Select to add tokens"/>	Add
<input type="text"/>		
Send example message		TEST

- 7) Edit the the Directory Name Format and File Name Format. You can configure the Directory Name Format and File Name Format by using a template or by including an event attribute token.
- 8) Click the ‘TEST’ button to send the example Name to the server and check whether it is received.

Setup > AI Security

Event Action

Network System VMS

Email HTTP TCP **FTP** ONVIF

FTP preset

No	Name	Host	Port	Operation
1	test	test	21	Edit Delete

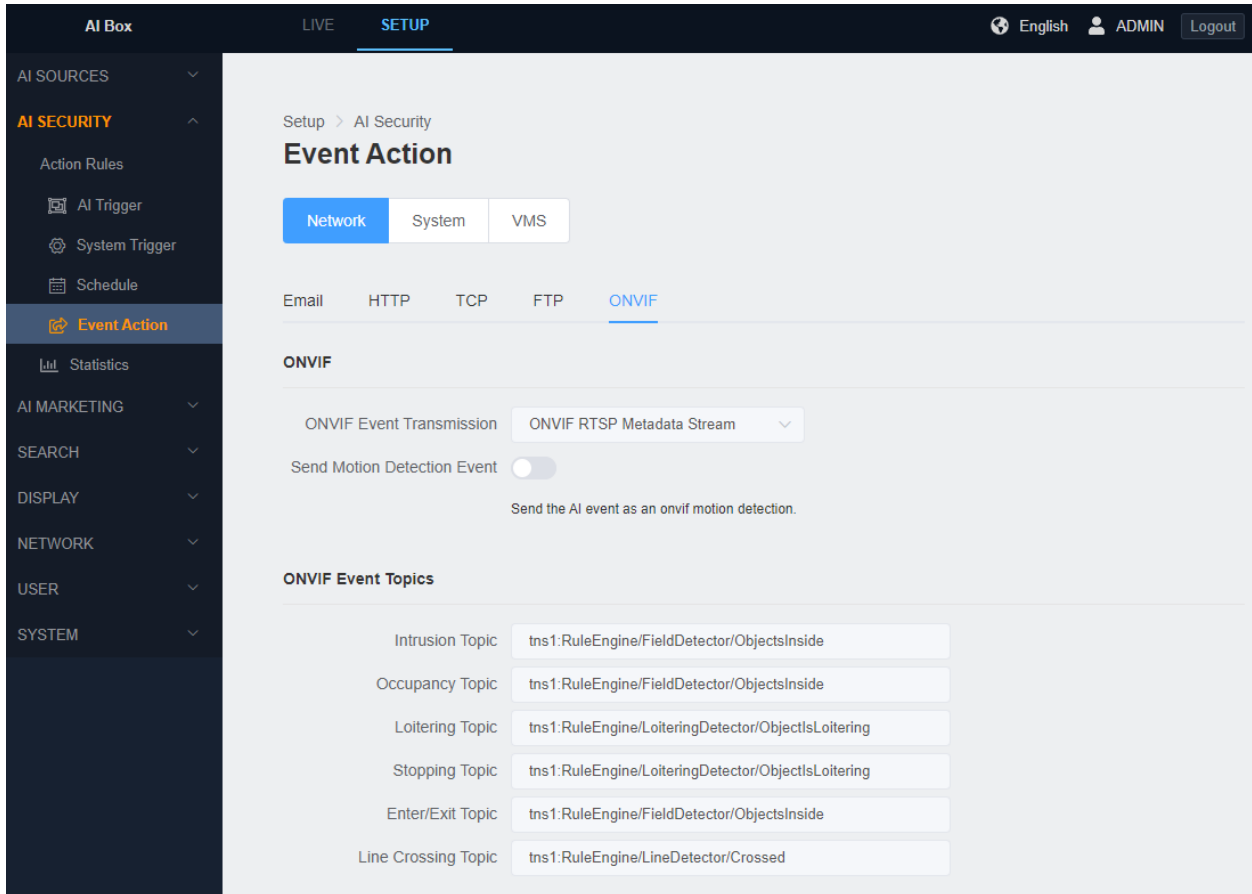
[Add](#)

9) Click the 'APPLY' button at the bottom to save.

10) Check the FTP preset section that you added in the list.

■ ONVIF

ONVIF RTSP Metadata Stream is available in the product, so do not need separate preset settings. In the ONVIF Tab, you can see the ONVIF Topic name for each trigger type.



1) In the ‘SETUP’ application tab, enter the ‘Event Action’ menu below the ‘Action Rules’ menu.

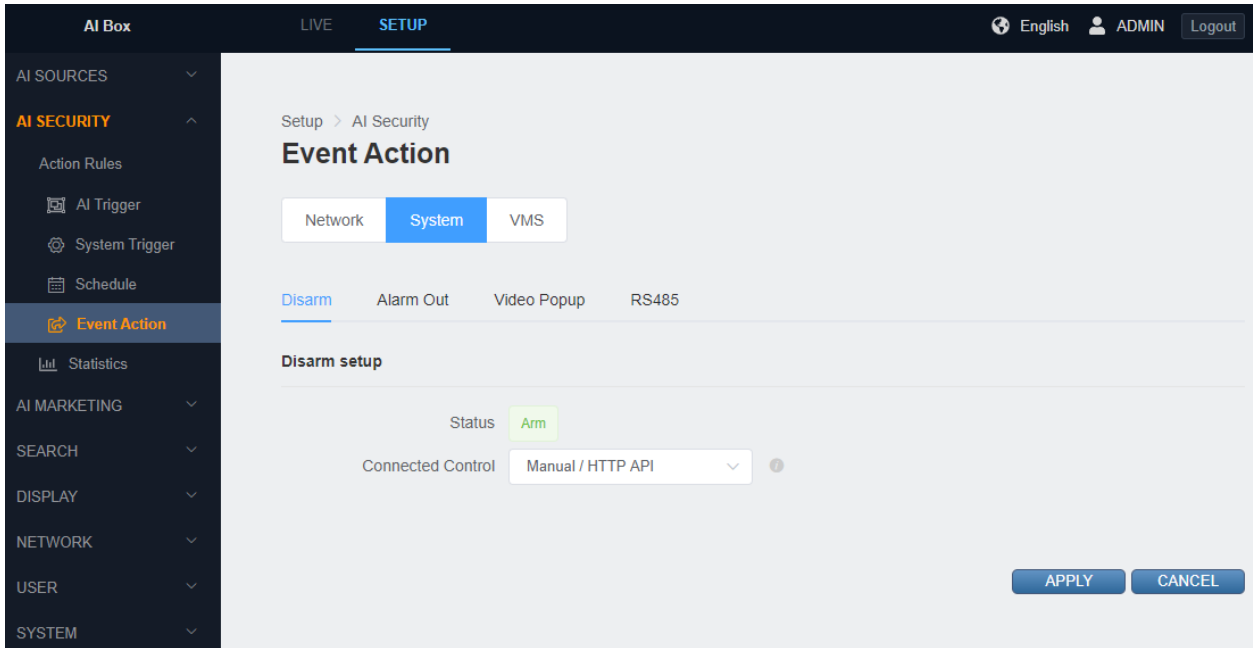
2) Click ‘ONVIF’ Tab.

- **System event action**

- **DISARM**

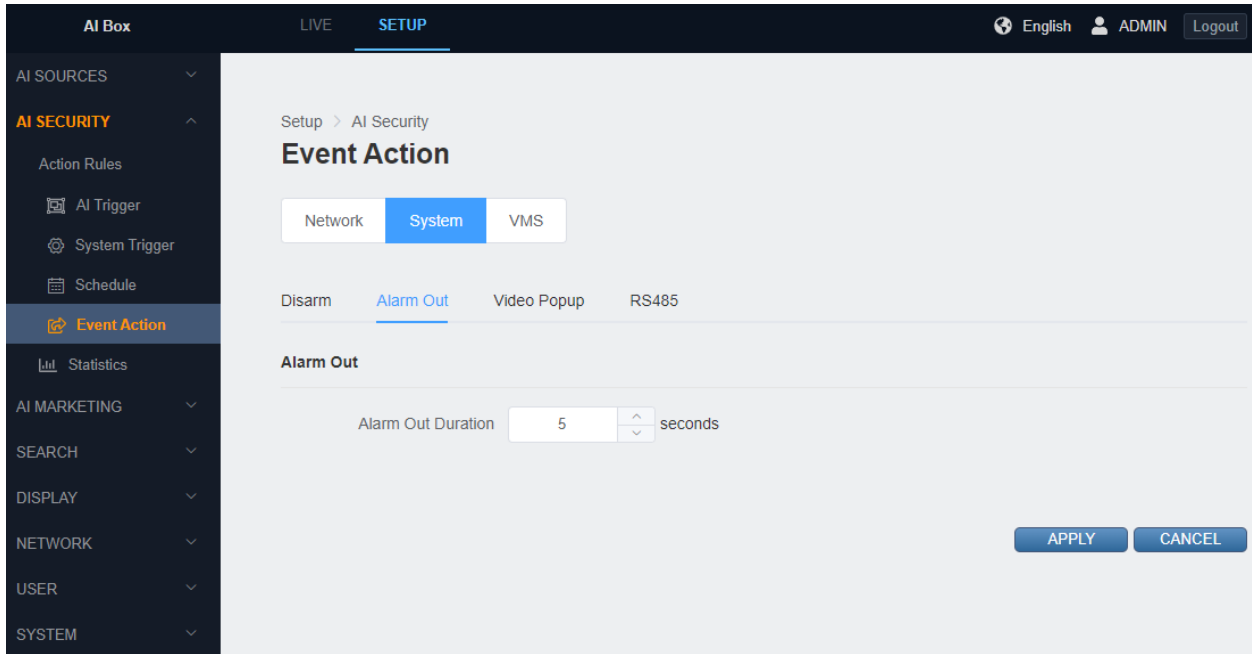
AI BOX is an ARM state that can generate an alarm action event at any time. However, the connected controller can be changed to DISARM state to prevent alarm.

m action event. For example, alarm events are not important during system checks, so you can create and work with the DISARM state as shown above.



■ Alarm Out

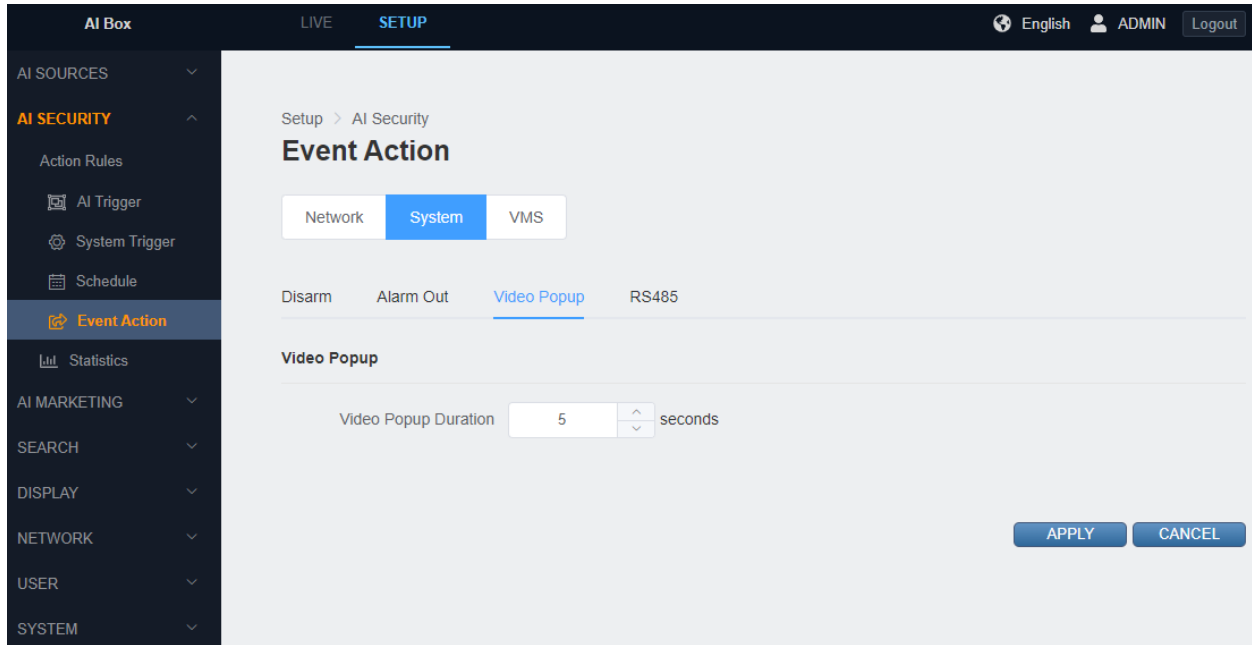
It is possible to set how long it will activate from the Alarm Out Duration when the Alarm Out action is activated. The entry default is 5 seconds.



- 1) In the 'SETUP' application tab, enter the 'Event Action' menu under the 'Action Rules' menu.
- 2) Input the value for the 'Alarm Out Duration'. You can use the UP/DOWN buttons or input a number directly. It is possible to set a value from 1 to 60.
- 3) Click the 'APPLY' button at the bottom to save

■ Video Popup

Set action rule. If you add the video popup in the action setting, the channel where the event occurred on the live screen pops up for the set time.



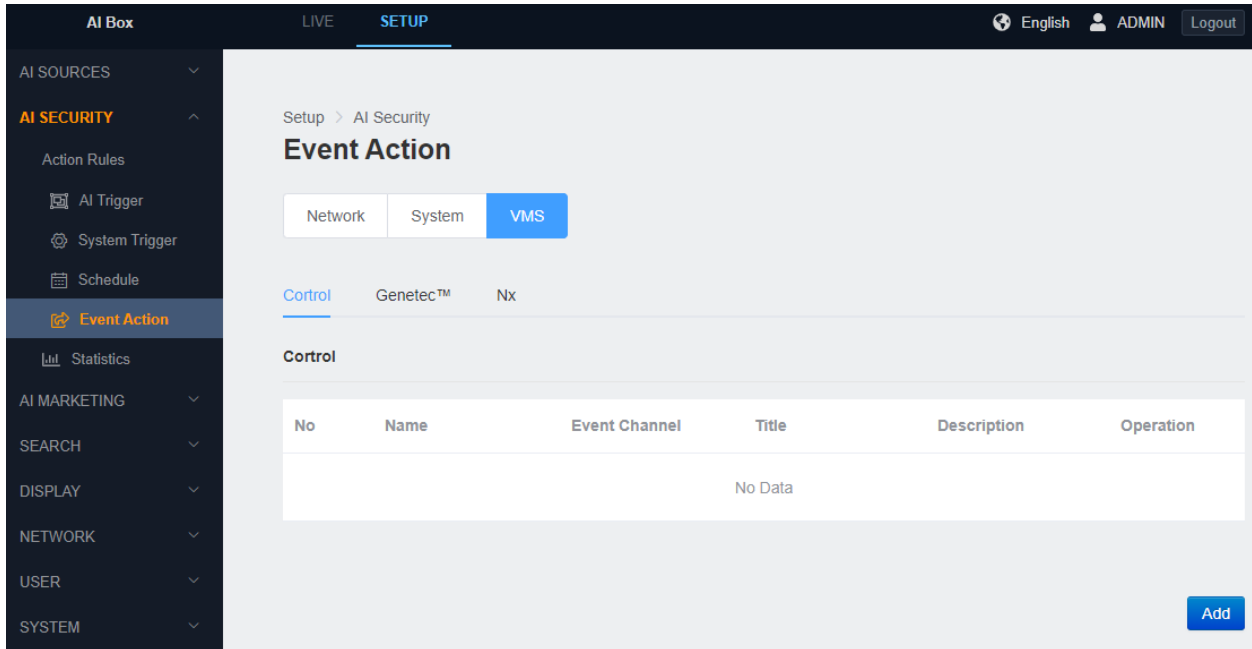
■ RS485

RS485 exports action messages sequentially without using a separate protocol. This can be used by setting the default baud rate and editing the action message.

The screenshot shows the GANZ AI Security configuration interface. The top navigation bar includes 'AI Box', 'LIVE', and 'SETUP'. The user is logged in as 'ADMIN' in 'English'. The left sidebar lists various categories: AI SOURCES, AI SECURITY (expanded), AI MARKETING, SEARCH, DISPLAY, NETWORK, USER, and SYSTEM. Under AI SECURITY, options include Action Rules, AI Trigger, System Trigger, Schedule, Event Action (selected), and Statistics. The main content area is titled 'Event Action' and shows tabs for 'Network', 'System' (selected), and 'VMS'. Below these are tabs for 'Disarm', 'Alarm Out', 'Video Popup', and 'RS485' (selected). The 'RS485' configuration section includes a 'Baud Rate' dropdown set to '115200 bps', an 'Event Action Message' dropdown set to 'Use template' with a 'Use' button, and a 'Select to add tokens' dropdown with an 'Add' button. There is an 'Editable Box' for text input and a 'Message Example' section. A 'Send example message' button with a 'TEST' label is located below the message example. At the bottom right, there are 'APPLY' and 'CANCEL' buttons.

- 1) Select RS485's Baud Rate.
- 2) Edit the Event action message. You can configure the message by using a template or by including an event attribute token.
- 3) Check the Message Example for an example of the actual message being sent.
- 4) Click the 'TEST' button to send the example message to the server and check whether it is received.
- 5) Click the 'APPLY' button at the bottom to save.

- VMS Event Action



- Control

See video tutorial (<https://youtu.be/yDxTFfNnmY>)

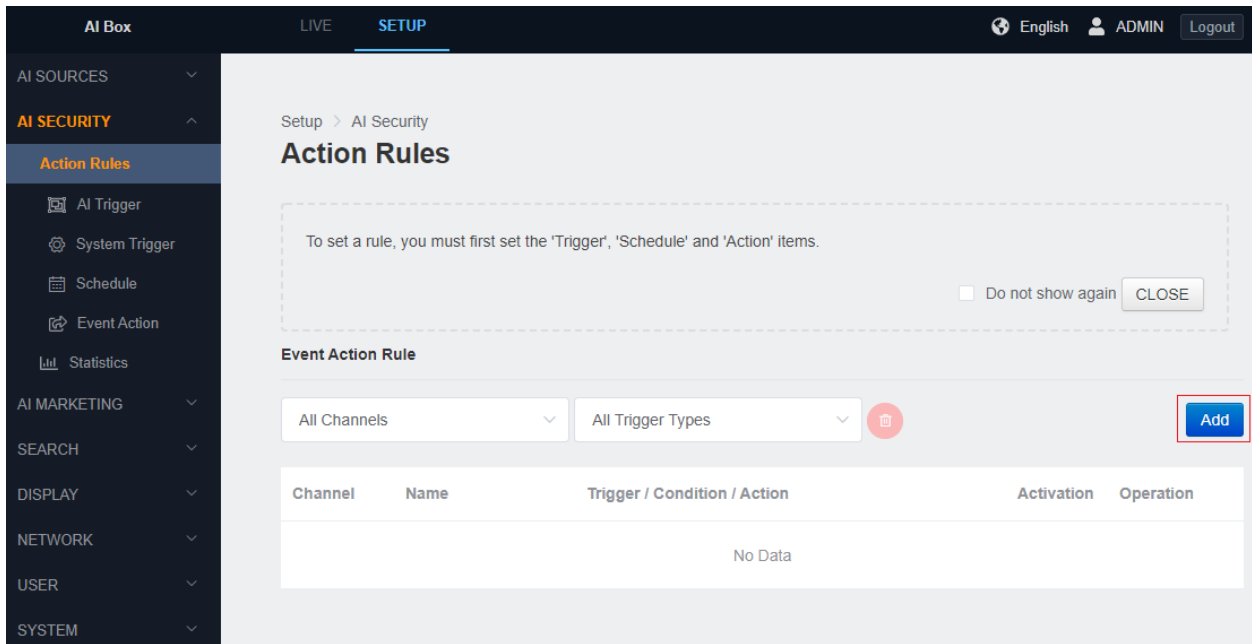
- Genetec™

See video tutorial (<https://youtu.be/ewjL8QHgR-w>)

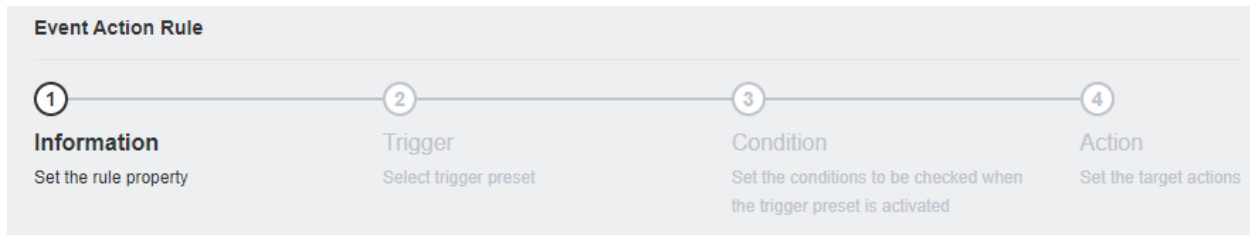
- Nx

See video tutorial (<https://youtu.be/QRpj3BiHfiM>)

● Action Rules Setting



- 1) In the SETUP application tab, enter the Action Rule menu under the 'Action Rules'.
- 2) Click the 'APPLY' button at the bottom to save.



- 3) At the top of the UI, you will see a step indicator indicating the current progress step. Edit the HTTP action message. You can configure the message by
 - 4) using a template or by including an event attribute token.

Information

Rule Name

NEXT

5) Create a name for the action rule and click the 'NEXT' button to move on to the next step.

Rule Summary

Information

Rule Name


Trigger

Conditions

Actions

6) The settings will be updated each time steps in the Action Rule Summary proceed.

Trigger Setup

Trigger 

PREV **NEXT**

7) Set the trigger type and its type in the Trigger Setup step. Then select Trigger Preset and click the 'NEXT' button to move to the next step

Condition Setup

Schedule

Condition

8) Select the desired item from the schedule preset.

It is set to 'Always' if you do not select a Schedule preset.

The condition is 'True' if any of the selected items are met when you select multiple schedules.

9) Click the + button to add another trigger to the condition.

Condition Setup

Schedule

Add Condition

10) Select the Trigger type and preset.

11) Set the Condition Trigger valid time.



It is based on the Rule Trigger occurrence time set in the Trigger Set up step

- In case of + t seconds, it is true when condition trigger occurs within t seconds after trigger occurrence
- In case of - t seconds, it is true if condition trigger occurred before trigger occurred.
- In case of +/- t seconds, it is true when condition trigger occurs before or after trigger occurs within t seconds.

12) Click the <Add> button to add it to Condition.

Action Setup

Action ONVIF RTSP Metadata Stream

Action Event Log

Action Email TEST

Add Actions Select Action Type Select Preset Add

PREV NEXT

13) To delete the trigger added as a condition, click the trash can icon on the right.

14) When you have finished setting the condition, click the 'NEXT' button to move on to the next step.

Setup > AI Security

Action Rules

To set a rule, you must first set the 'Trigger', 'Schedule' and 'Action' items.

Do not show again

Event Action Rule

All Channels All Trigger Types

Channel	Name	Trigger / Condition / Action	Activation	Operation
CH 4	test	LPR <input type="button" value="LPR"/>	<input checked="" type="checkbox"/>	Edit Delete
		Schedule <input type="button" value="Always"/>		
		ONVIF RTSP Metadata Stream		
		Event Log		
		Email <input type="button" value="TEST"/>		

15) ONVIF RTSP Metadata Stream is the default in Action

All events with rules set are sent to the RTSP Metadata Stream.

16) To add another Action, select the Action type and preset in the Add Actions item and click the <Add> button.

17) To delete the added Action, click the trash can icon on the right

18) When you have completed the Action setup, click the 'NEXT' button to move on to the next step.

Rule Summary

Information

Rule Name

Trigger

Trigger

Conditions

Schedule

Actions

Action

Action

Action

19) Check the settings in Summary.

20) After completing the review, click the 'APPLY' button to create the rule.

1.Counting

This item can be viewed by processing the number of triggers of AI security items.

The screenshot displays the GANZ AI Security interface. The top navigation bar includes 'AI Box', 'LIVE', and 'SETUP' tabs, along with language and user settings. The left sidebar lists various menu items, with 'AI SECURITY' and 'Statistics' highlighted. The main content area shows the 'Statistics' section with 'Counting' and 'Reporting' tabs. Under 'Trigger Counting', there are several configuration options: 'Channel' set to 'All Channels', 'Trigger Type' set to 'Select', and 'Counting Type' set to 'Hourly'. There are also 'From' and 'To' time range input fields, a 'Counting' button, and an 'Export CSV' button.

- 1) In the Settings tab, enter the Statistics menu under the AI Security menu.
- 2) Select the desired channel and trigger type.
- 3) Choose whether to process statistics by day or by time.
- 4) Set the desired time interval for processing and press the Counting button to display the searched content at the bottom.
- 5) If you press the CSV button, you can download the searched contents in CSV file format.

2. Reporting

It is a function to periodically send the statistics data to a specific administrator or automatically upload the data by FTP.

1) Set the report name and select a frequency. Frequency setting guide - You can receive data automatically by selecting the following cycle.

1.1) Hourly: Automatically receive data every hour,

1.2) Daily : If you specify the desired time zone, data is automatically received at the set time zone every day.



1.3) Weekly: If you specify the desired day and time zone, data is automatically received.

1.4) Monthly : If you specify the desired day and time zone, data is automatically received.

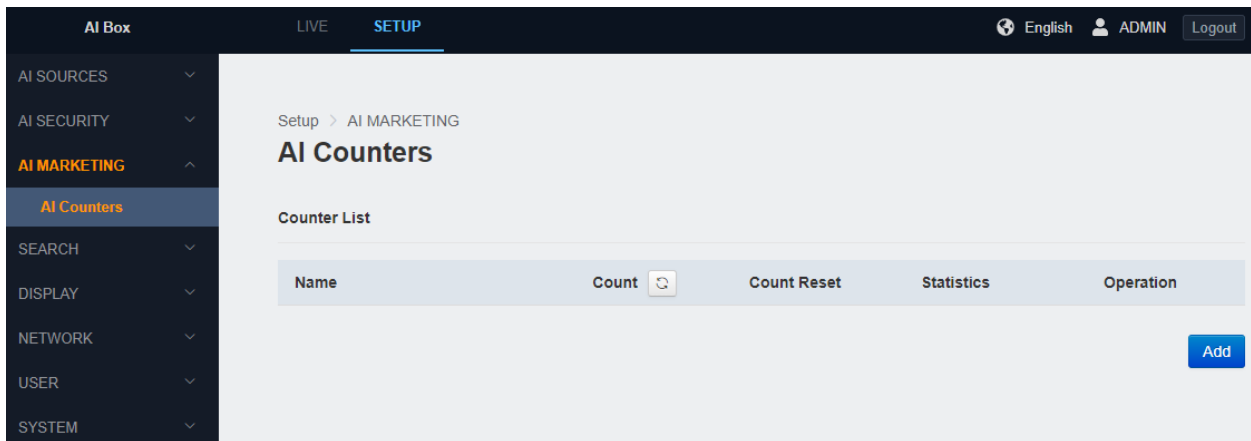
Select the trigger that will receive the report, and click the Add button to add it. Select the recipient by e-mail: Settings-> AI Security-> Network-> Presets of email. After selecting the recipient's email preset, select the registered email recipients and click the Add button to add them.

2) If you set the receiver to FTP, you can set the FTP server for uploading statistics datum.

Select FTP as Recipient, check FTP address, FTP Port, Passive Mode in Host, FTP user, FTP password, FTP directory path to receive, File Prefix information and apply.

This setting corresponds to the Retail solution item of AI BOX.

Usage: In case of CCTV security, the event occurrence count is mainly managed as a cumulative count. However, if you apply an acceleration count instead of a cumulative count, you can find out the status of the customers who visited the store every predetermined time.



- Press the Add button to add an AI counter.

Setup > AI MARKETING

AI Counters

Add Counter

Name

Counting Zones

Video Source	Name	Operation
CH 1 - Human_ve		Edit Delete

Count Reset

Frequency	Day	Time	Operation
Daily	-	09:00	Edit Delete

- 1) Name the counter.
- 2) Add the area where you want to use counter.
- 3) Add a schedule to specify when to reset the counter during the day.
- 4) Press the Apply button to create the counter.

Zone Setup



Video Source	CH 1 - Human_ve	Zone Name	<input type="text"/>
Target Object	Person	Zone Type	Line
		Count Increase	Forward
		Count Decrease	Reverse

CANCEL APPLY



- This is an additional zone setting screen.
 - 1) Select the video source.
 - 2) Select the detection target.
 - 3) Enter the name of the area.

- 4) Select whether to make a counter cross line or line in / out area.
- 5) It sets the increase and decrease of count.
- 6) Click the Apply button to save the above.

Setup > AI MARKETING

AI Counters

Counter List

Name	Count 	Count Reset	Statistics	Operation
test	2	<input type="button" value="Reset"/>		Edit Delete

- The AI counter is created.
- 1) Possible to check the current count by the refresh button next to the Count.
 - 2) Press the counter reset button to reset.
 - 3) Possible to print the counter statistics by pressing the Statistics button.
 - 4) Possible to modify or delete the counter by pressing the Edit and Delete button.

Counter Statistics

Counter

Resolution

Period -

Time Filter

Days of week Filter

Data Format

Request URI

- This is the screen when the counter statistics button is pressed.
- 1) Types of counters to output or respond to statistics. Multiple selection is also possible.
 - 2) Select the unit.
 - 3) Select the period you want to send statistics.
 - 4) Possible to filter only business hours.
 - 5) Possible to filter only 5 days a week.
 - 6) Possible to respond to the request in JSON format and download it in CSV format.

1. Search

- Event Log

The screenshot shows the GANZ AI Box interface. The top navigation bar includes 'AI Box', 'LIVE', and 'SETUP' (which is active). On the right, there are options for 'English', 'ADMIN', and 'Logout'. The left sidebar contains a menu with categories like AI SOURCES, AI SECURITY, AI MARKETING, SEARCH (highlighted), Event Log (highlighted), System Log, DISPLAY, NETWORK, USER, and SYSTEM. The main content area is titled 'Event Log' and includes a search and export section. The search criteria are: Channel: All Channels, Time Range: 2019-12-24 12:00:00 To 2019-12-24 18:00:00, and Export: CSV. Below this, it shows 'Total 637' results. A table displays the following data:

Channel	Trigger Type	Rule Name	Actions	Video Timestamp	System Time
4	LPR	test	Email	30337	12/24/2019 16:46:39
4	LPR	test	Email	30340	12/24/2019 16:46:43
4	LPR	test	Email	30340	12/24/2019 16:46:43
4	LPR	test	Email	30343	12/24/2019 16:46:46

You can search or download the action events that occurred in 'Action Rules' of the 'AI Security' menu in CSV format.

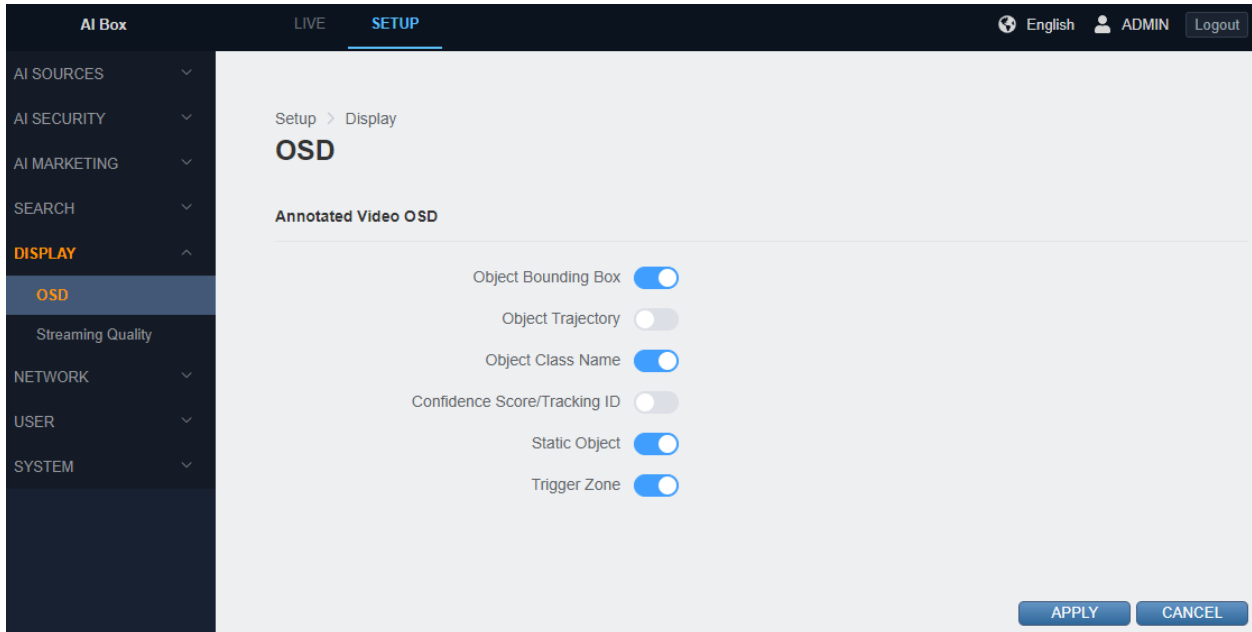
- System Log

Event Type	Description	System Time
User Information	User Login (192.168.200.81)	12/24/2019 14:38:28
User Information	User Login (192.168.200.81)	12/24/2019 14:54:58

You can search and download the necessary system logs such as user login or system startup etc. in CSV format.

2. Display

- OSD



This is the setup for OSD information displayed in Annotated Video's video of AI BOX.

- 1) Object bounding box: Determining whether or not the box is displayed on the object border.
- 2) Object Trajectory: Determines whether or not the screen is displayed on the moving object.
- 3) Object Class Name: Determining whether to display people or cars on the screen.
- 4) Confidence Score/Tracking ID: used for AI debugging.
- 5) Trigger Zone: Determining whether the trigger rule display line or figure is displayed on the screen.



- Streaming Quality

The screenshot shows the 'Streaming Quality' configuration page in the GANZ AI Box setup interface. The page is titled 'Streaming Quality' and is part of the 'Display' setup section. It features a table for 'Annotated Video Streaming Quality' with columns for View, Quality, Channel, and Bitrate. The 'Multiview' section has a 'Quality' dropdown set to 'Highest' and lists channels CH 0 through CH 8 with their respective bitrates. The 'Singleview' section also has a 'Quality' dropdown set to 'Highest' and lists channels CH 4 through CH 8 with their respective bitrates. The interface includes a sidebar with navigation options like 'AI SOURCES', 'AI SECURITY', 'AI MARKETING', 'SEARCH', 'DISPLAY', 'OSD', 'NETWORK', 'USER', and 'SYSTEM'. The top navigation bar shows 'AI Box', 'LIVE', 'SETUP', 'English', 'ADMIN', and 'Logout'.

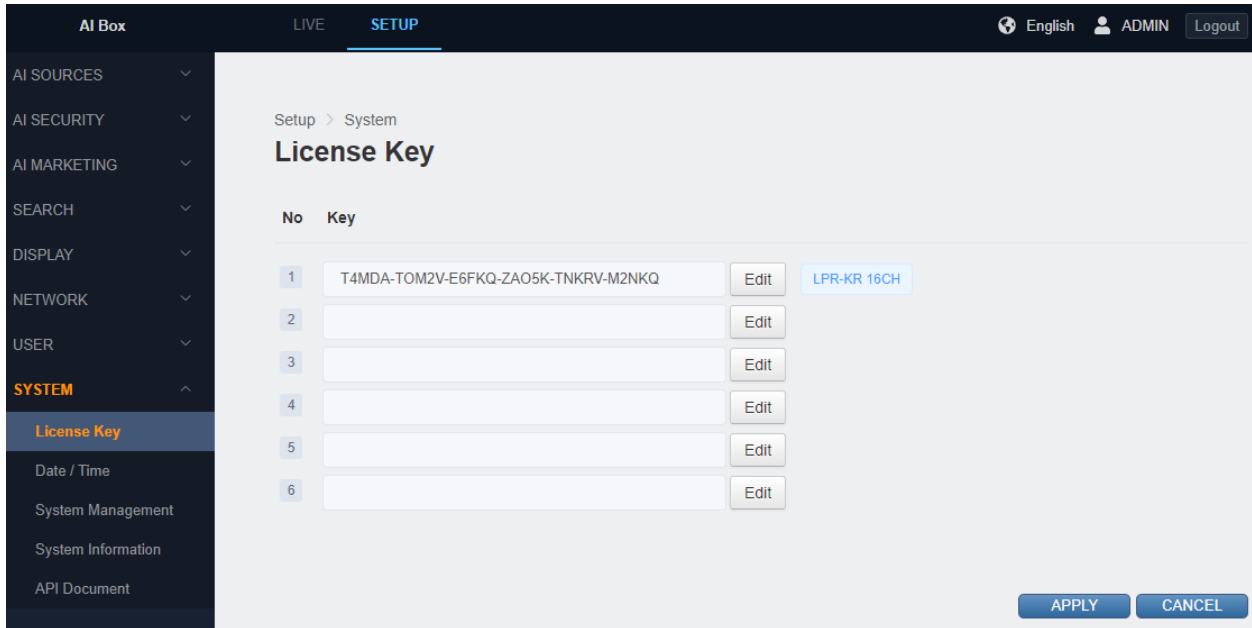
View	Quality	Channel	Bitrate
Multiview	Highest	CH 0	8000 kbps
		CH 1	5600 kbps
		CH 2	4400 kbps
		CH 3	4400 kbps
		CH 4	5600 kbps
		CH 5	4400 kbps
		CH 6	4400 kbps
		CH 7	4400 kbps
		CH 8	4400 kbps
Singleview	Highest	CH 4	5600 kbps
		CH 5	4400 kbps
		CH 6	4400 kbps
		CH 7	4400 kbps
		CH 8	4400 kbps

AI BOX supports not only video streaming for each RTSP channel but also mult i-view streaming showing all channels as one channel.

It is possible to make settings for that streaming quality.

3. System

- License key



Enter a license key to activate additional features that require a license.

If the license is successfully registered, the corresponding item is displayed on the right.

- System information

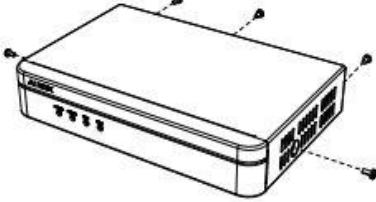
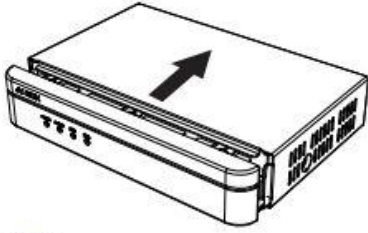
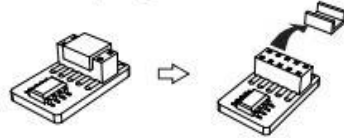
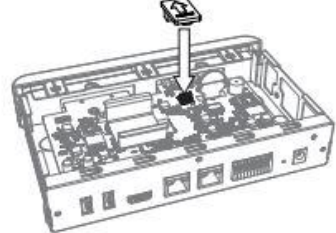

You can find the model name, firmware version, MAC address and etc.

- API documentation

API document is embedded to work with AI BOX.

1. Face recognition license required

To use the face recognition function, you need to purchase FR chip separately.

<p>STEP 1 Separate five screws on the side and back of the AI BOX.</p>  <p>CAUTION Gloves should be worn before disassembling the top cover. Otherwise you may hurt your hand.</p> <p>1</p>	<p>STEP 2 Slide the top cover back to remove it.</p>  <p>STEP 3 Remove the cover of the part shown in the picture of the package FACE RECOGNITION chip.</p>  <p>2</p>	<p>STEP 4 Plug the FACE RECOGNITION into the 10 pins of the motherboard.</p>  <p>CAUTION The direction of FACE RECOGNITION CHIP should be inserted with the arrow facing the front.</p>  <p>STEP 4 Assemble the top cover and tighten the screws in the reverse of the step 1 and 2 division.</p> <p>3</p>
--	--	--

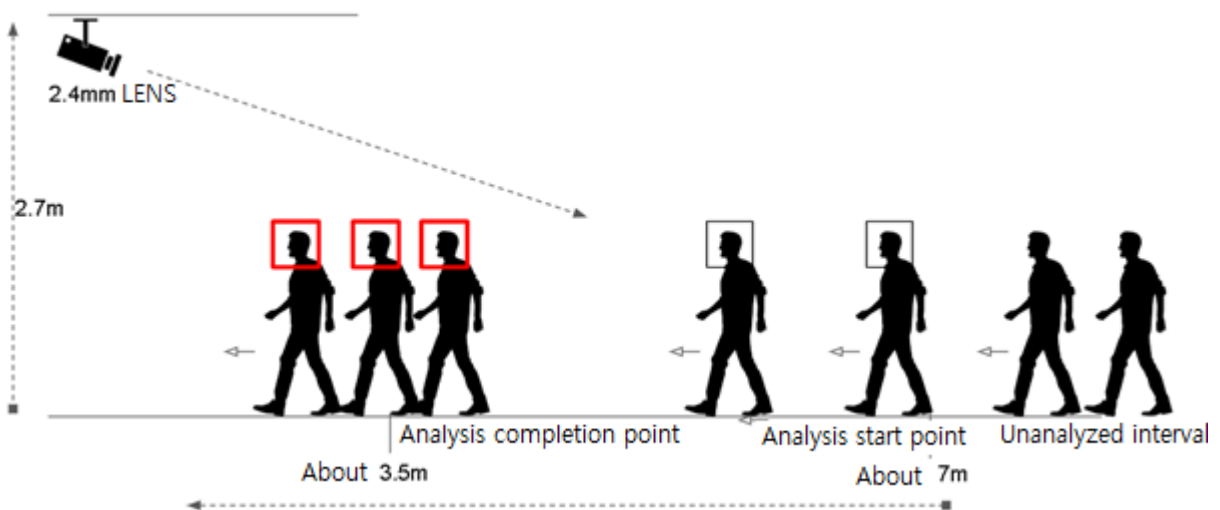
<p>Warranty of the product</p> <ol style="list-style-type: none"> The warranty is 2 years. Face Recognition is shipped from AI BOX or purchased separately from the Face Recognition licenses key protector. AI BOX products that support Face Recognition are equipped with Face Recognition licenses key protector by default. <p>4</p>	<p>Rev00 MX41AUD4</p>	 <p>Install Guide</p> <p>WARNING If static electricity occurs during installation, the product may not work. Be sure to wear gloves and avoid static electricity.</p>
---	---------------------------	--

2. Note of installing the camera for Face Recognition

1) It should be installed in front of the person's direction.

(The left and right angles at which the camera faces the face is around 30 degrees)

2) Horizontal, Install the camera at an angle of 15 degrees to the human face.



<Camera installation example to increase accuracy>

3) You can increase the accuracy if you have about 4 seconds from the start of the analysis to the end of the analysis.

4) The lower the camera height, the higher the accuracy (closer to the height of the object).

3. Face recognition engine applied

Setup > AI Sources

Video Source

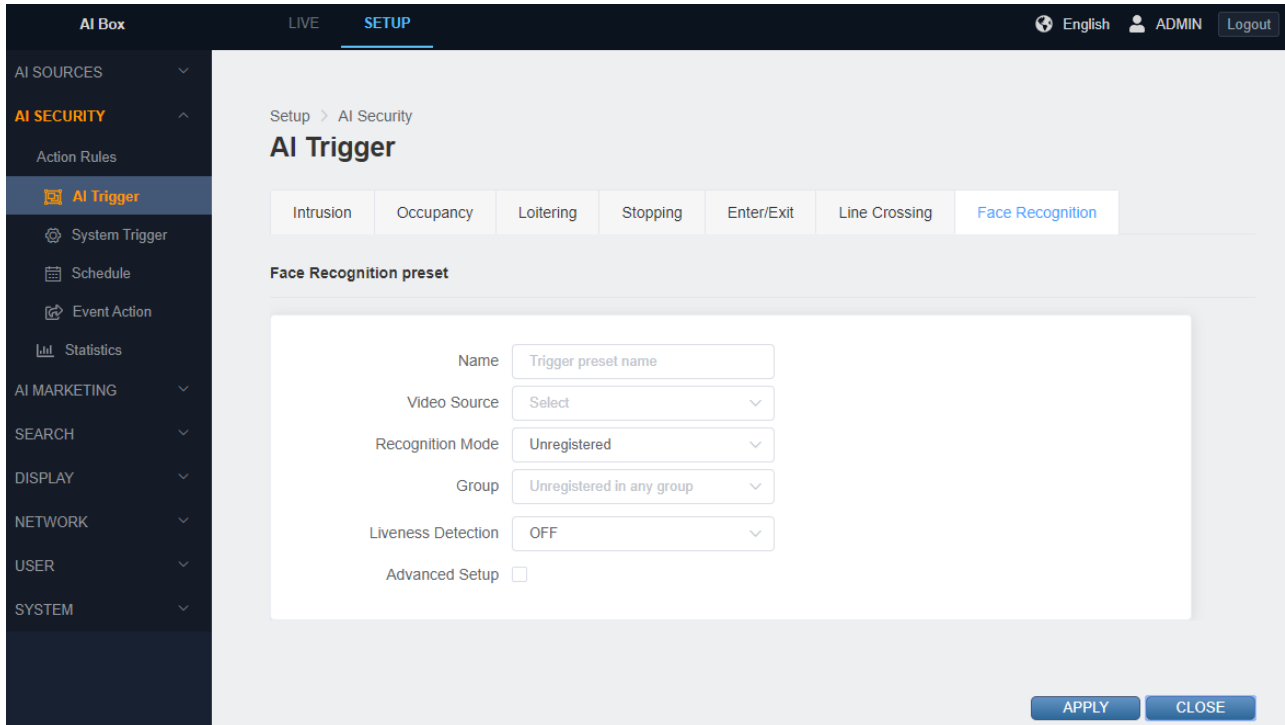
CH	NAME	URL	Discovery	AI Algorithm	1884 / 2000	STATUS
1	Human_ve	file:///tmp/usbdev/gasan_1080p.mp4	TCP	Human / Vehicle - Normal (F)		Disconnected
2	Gender	file:///tmp/usbdev/face.mp4	TCP	Human - Normal		Disconnected
3	Privacy	file:///tmp/usbdev/person_02.mp4	TCP	Human - Far		Disconnected
4	LPR	file:///tmp/usbdev/lpr_front_1.mp4	TCP	LPR - KOR (Faster Objects)		Disconnected
5	Snow	file:///tmp/usbdev/snow_06.mp4	TCP	Human - Normal		Disconnected
6	Fisheye	file:///tmp/usbdev/fisheye_6.mp4	TCP	Human - Normal		Disconnected
7	Office	rtsp://ADMIN:*****@192.168.200.229:554/live/ma	TCP	Human - Normal		Disconnected
8		rtsp://username:password@ip:port/url	TCP	None		Disconnected

APPLY CANCEL

Set the AI algorithm to Face Recognition in the Video Source menu under AI Source.

AI source -> Set AI Algorithm to Face Recognition in the Video source menu.

4. AI Trigger setting



Set up the trigger in the Face Detection tab of the AI Trigger menu under AI Security.

AI security -> AI trigger -> Set the trigger in the face detection menu.

- 1) Set the Preset name.
- 2) Select the Video source.
- 3) Select the Recognition mode.

- Unregistered: triggers people who do not belong to any group.
- Group comparison: Compare people registered in the selected group to trigger the appropriate person.
- Face Attribute Filtering: It triggers by filtering the age or gender by the result of face analysis.

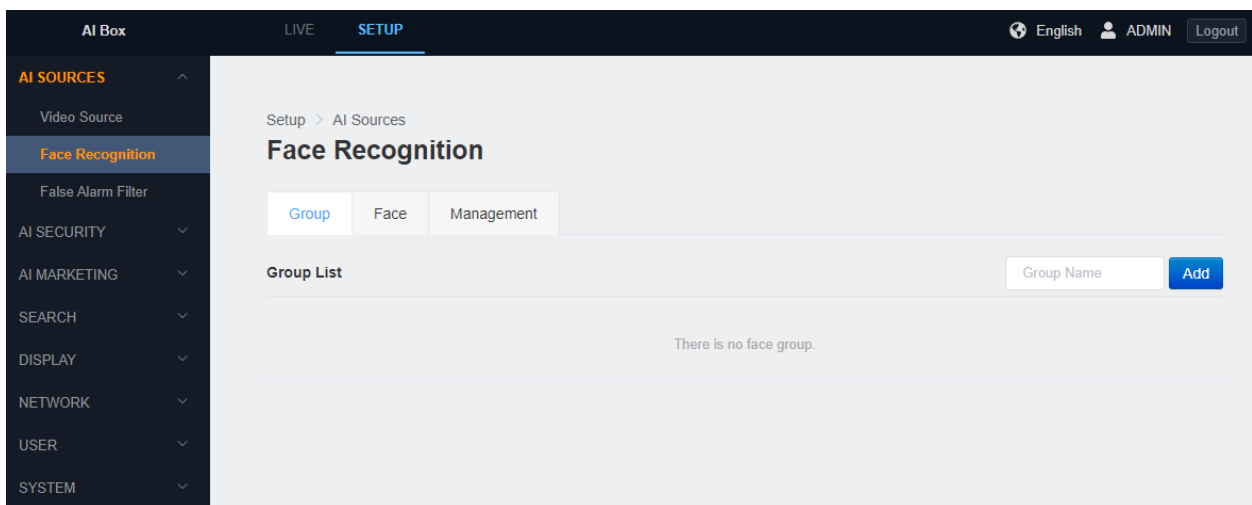
4) Aliveness detection

You can turn the Aliveness detection ON or OFF.

5) Advanced Settings / Counter Reset

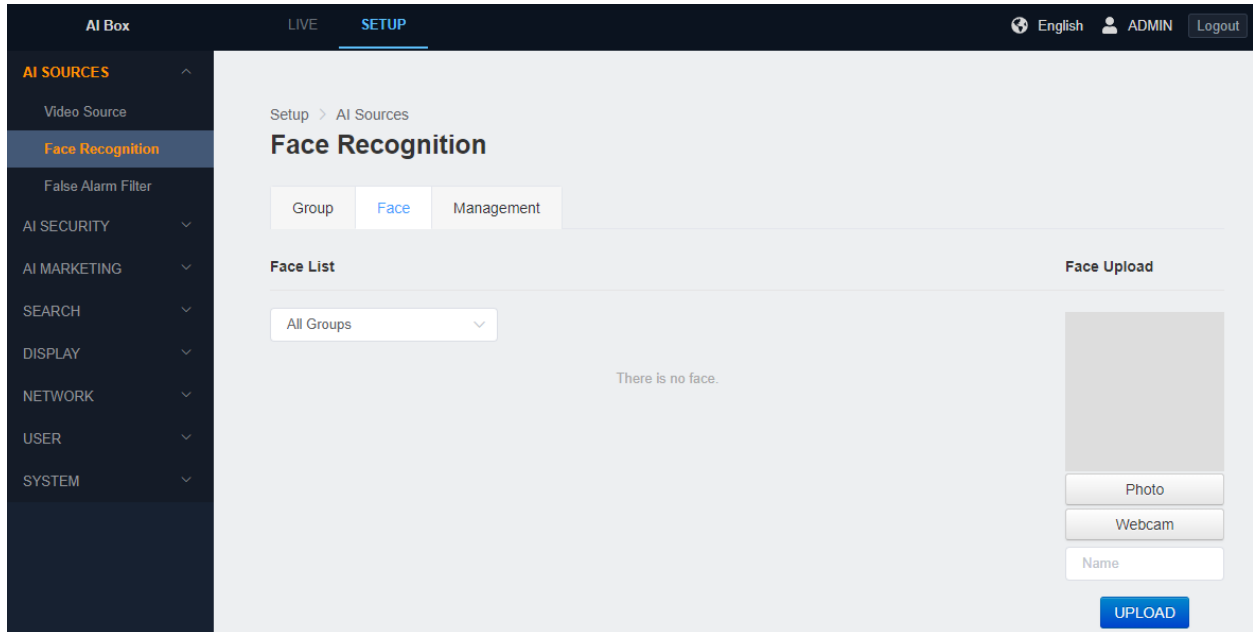
It is possible to reset every day at the designated time. Click the Reset button to reset the current counter.

5. Create a face recognition database



You can create a group of face recognition databases in the 'Groups' tab of the 'Face Detection' menu under 'AI Sources'.

AI source -> Face recognition -> It is possible to create a group of face recognition databases from the Group menu.

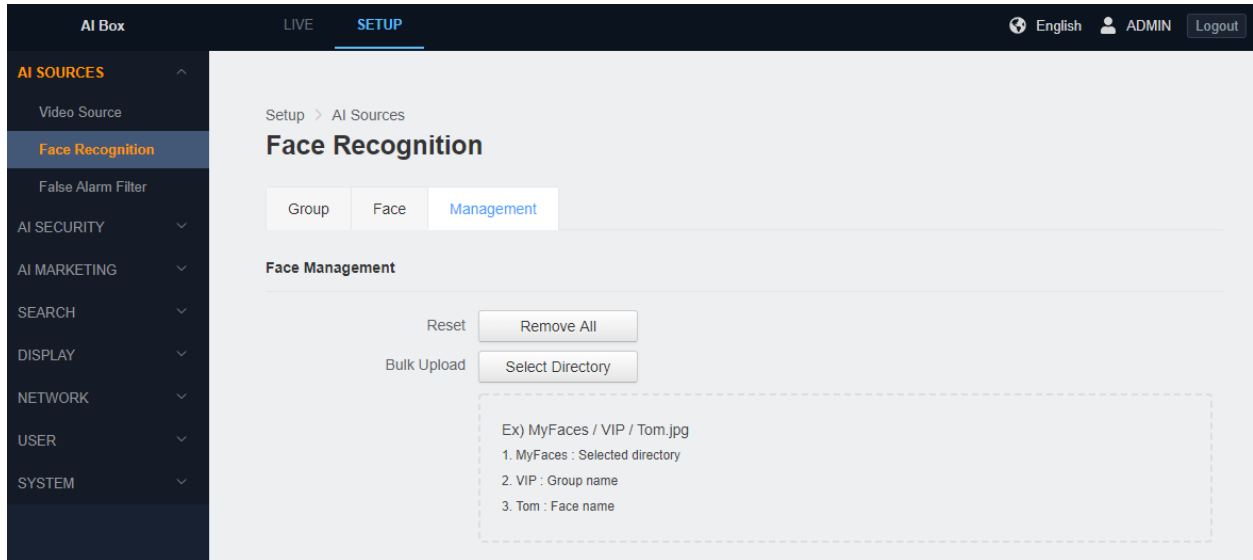


Face data can be added individually in the 'Face' tab of the 'Face Detection' menu under 'AI Source'.

AI source -> Face recognition -> It is possible to create a group of face recognition databases from the Group menu.

Click the photo button to upload a picture. In the case of a photo, it can resize by itself even if the size is large. Photos with only faces taken from the front are more accurate.

Click the Webcam button to allow you to directly register photos taken with the Webcam connected to your computer to AI BOX.



You can manage them in bulk from the 'Admin' tab under the 'Face Detection' menu under 'AI Source'.

AI source -> Face recognition -> It is possible to manage them in bulk from the Management menu

Remove All: Delete all face data in AI BOX.

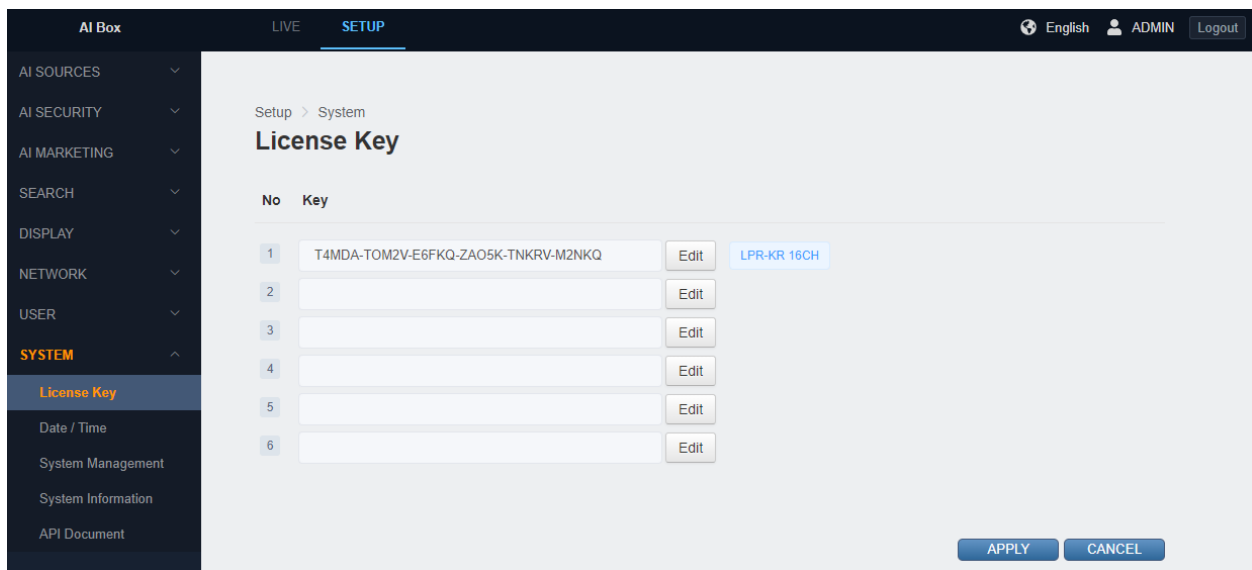
Bulk Upload: This function is to register all the pictures in a folder. The rules in the folder are:

e. g. : MyFaces / VIP / Tom. jpg

The folder in the selected folder is the group name and the file name is the user name of the face.

1. License plate recognition license required

License plate recognition requires a separate license. The license plate recognition algorithm is activated when you purchase the license.



You can find the license key in the 'License Keys' menu under 'System'.

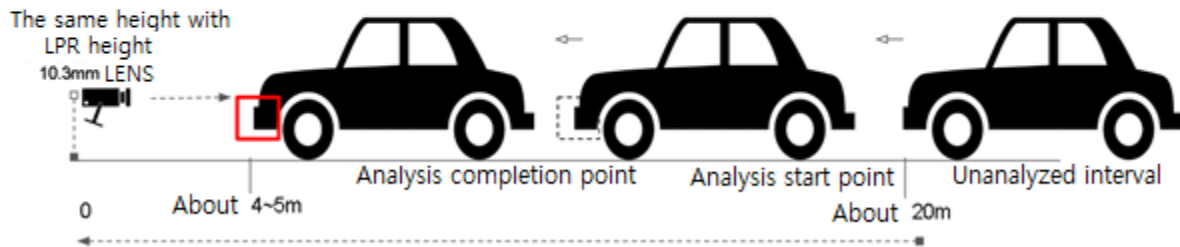
Setting - System menu -> License Key menu -> Check the license key.

2. Note of installing the camera for License Plate Recognition

License plate recognition requires a separate license. The license plate recognition algorithm is activated when you purchase the license.

- 1) The recognition accuracy is high when installed similar to the height of the license plate of the vehicle.
- 2) Camera installation and camera lens should be selected properly according to vehicle speed.

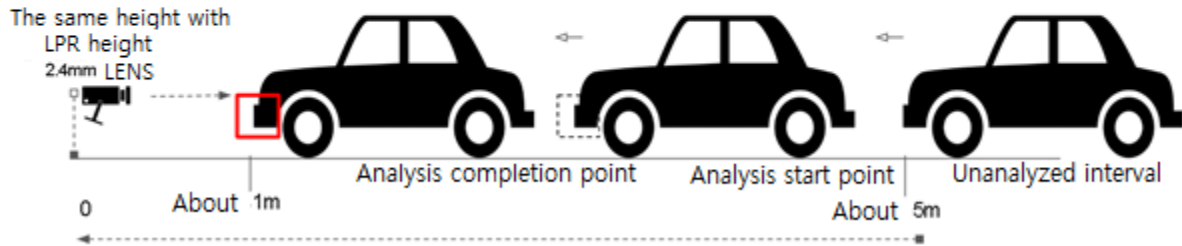
Example of improving accuracy when installing a license plate recognition camera Fast vehicle speed (less than 60 km/sec)



Example 1: Example of improving accuracy when installing a license plate recognition camera

- a. Fast vehicle speed (less than 60 km/sec)
- b. Same as license plate height / 10.3mm lens
- c. Analysis completion point / Analysis start point / Unanalyzed interval
- d. About 4~5m / About 20m

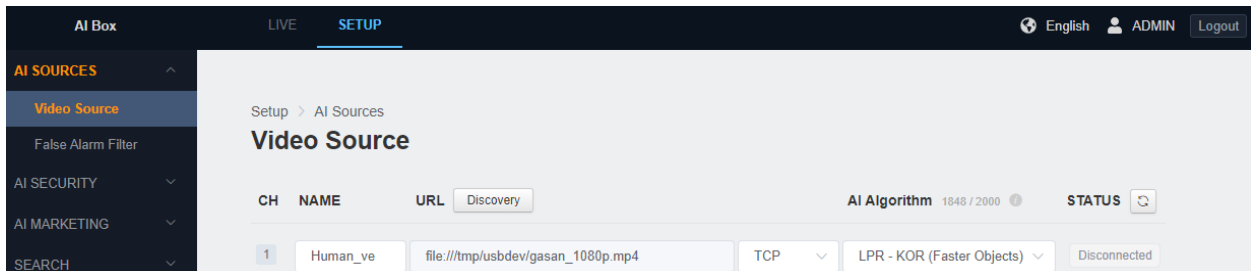
Example of improving accuracy when installing a license plate recognition camera
Slow vehicle speed (less than 10 km/sec)



Example 2: Example of improving accuracy when installing a license plate recognition camera

- a. Slow vehicle speed (less than 10 km/sec)
- b. Same as license plate height / 2.4mm lens
- c. Analysis completion point / Analysis start point / Unanalyzed interval
- d. About 1m / About 5m

3. License plate recognition algorithm





Apply the license plate recognition algorithm from the 'Image Source' menu under 'AI Source'.

AI source -> Video source -> Set AI Algorithm to LPR in the Video source menu.

4. Create License Plate Recognition Trigger

Setup > AI Security

AI Trigger

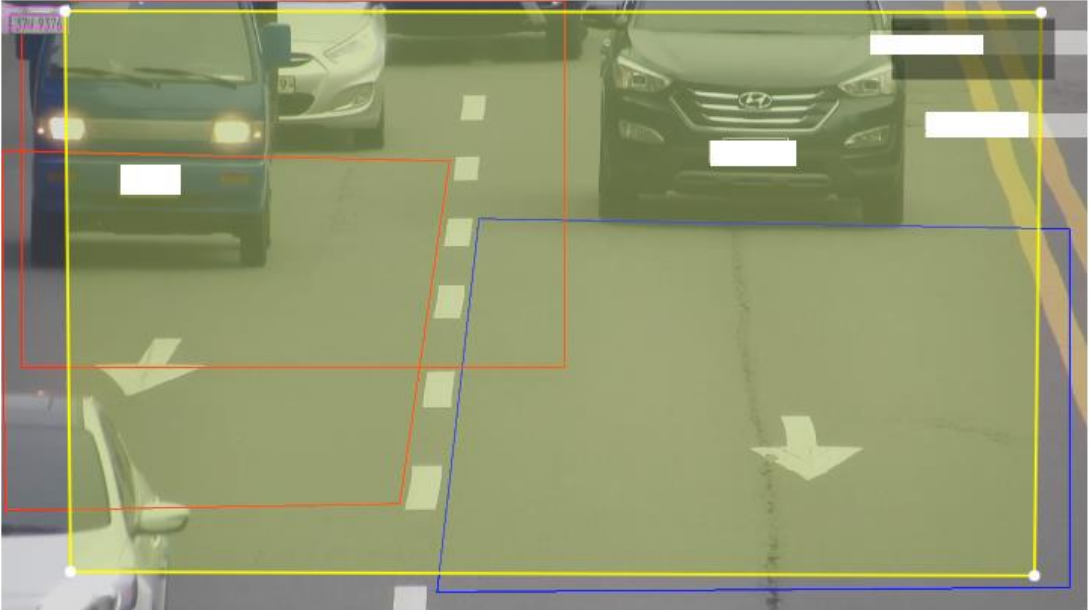
Intrusion Occupancy Loitering Stopping Enter/Exit Line Crossing **LPR**

License Plate Recognition preset

Name

Video Source

LPR - KOR (Faster Objects)



rtsp://ADMIN:****@192.168.200.223:5554/live/ch4

APPLY **CLOSE**

Create a license plate recognition trigger from the ‘AI Triggers’ menu under ‘AI Security’ .



Setting - AI SECURITY -> AI Trigger -> Create a license plate recognition trigger.

- 1) Name the preset
- 2) Select the Video source
- 3) Draw the AREA BOX where the license plate is the largest (the closer the camera is, the larger the license plate).



- THE END -