GANZ
Security Solutions

AI Box - 4Ch / 8Ch / 16Ch

User Manual v1.0.0

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 acc idents or damage by using this product can result in liability for accidents or damage.

In order to improve the performance of the product a firmware upgrade may be released without prior notice, though require manual installation by way of the FW upgrade function.

AI Box - 4Ch / 8Ch / 16Ch

User Manual v1.0.0

Contents

AI Box - 4Ch / 8Ch / 16Ch

User Manual v1.0.0

1. Overview

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.

2. 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

3. 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

4. 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

CORP HQ +1 (919) 230-8700 | WEST COAST +1 (310) 222-8600

5. During installation

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

- Secure at least 18 centimeters of distance between cooling fan and wall for 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 specification sheet. Using any other adapter could cause fire, electrical shock, or damage to the product
- Incorrectly connecting the power supply or replacing battery may cause explosion, fire, electric shock, or damage to the product

6. While in use

- Do not apply excessive force to or shake it while in use
- Only use attachments/ accessories specified by the manufacturer

7. WARNING

To reduce the risk of fire or electric shock, do not expose this product to ra in 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 th e 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

8. Key features

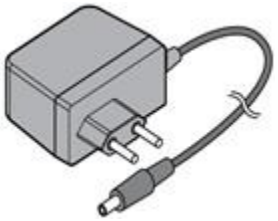
This device is based on the latest deep learning technology of intelligent video analysis which has up to 16 channels network camera video inputs. The features include object identification, object counts and object tracking by AI technology. Also, it allows to configure various trigger rules to ring alarms and can be utilized for various purposes by interworking with external network dev ices 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 480 fps, 4K video up to 120fps

2. Components

1. Components


Cable clamp


Adapter

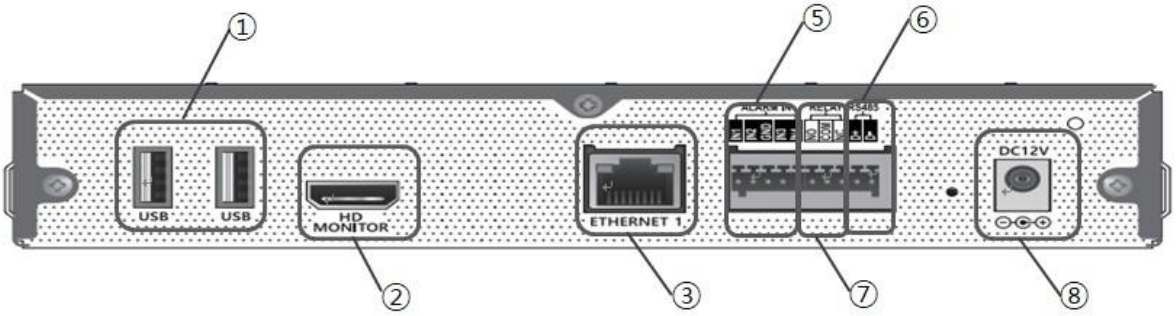

Screw

2. Front panel Names and functions

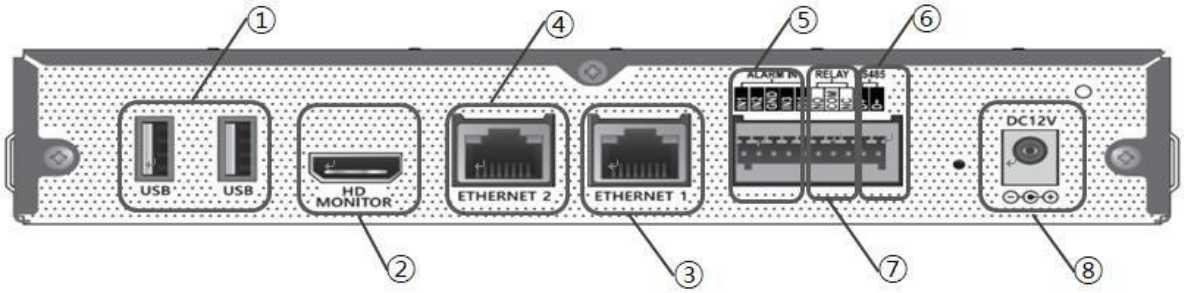
List	Status sign LED	Description
POWER		Red light blinks during the boot phase and green light during operation.
STATUS		Status light blinks when an event occurs after passing the set condition.
ETH1		ETH1 light blinks when communication is taking place via the ETH1 port or turns off when communication is not taking place.
ETH2		Headlight turns on when communication is taking place via the ETH2 port or turns off when communication is not taking place.

3. Rear panel Name and functions

- 4CH



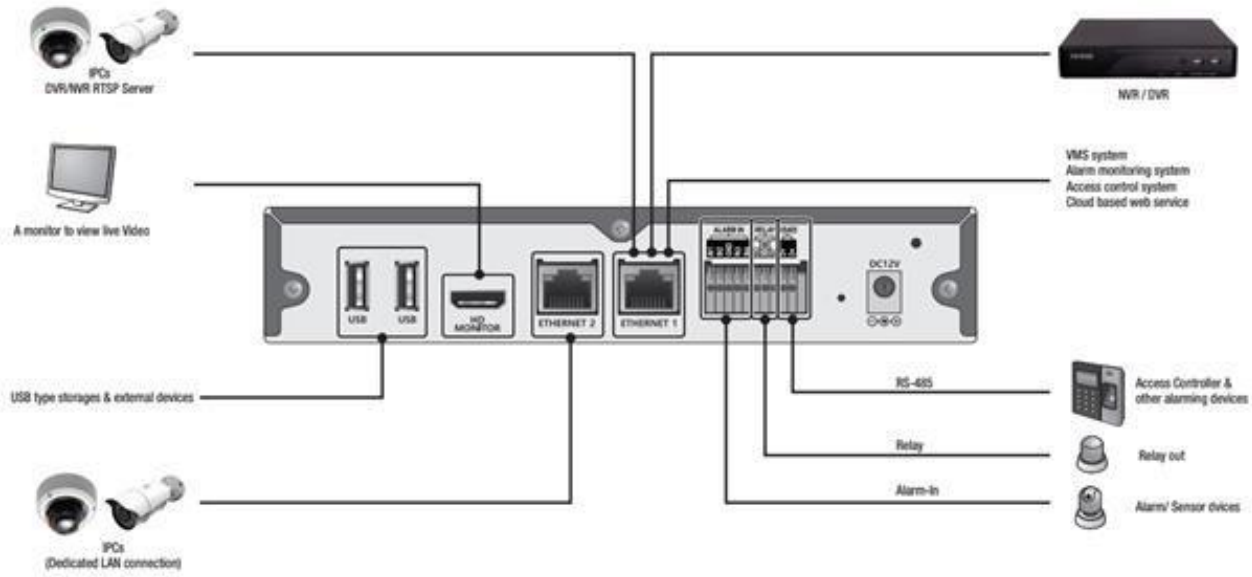
- 8CH / 16CH



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

3. Installation

1. Basic connection configuration



2. Network setting

Basic requirements of Web

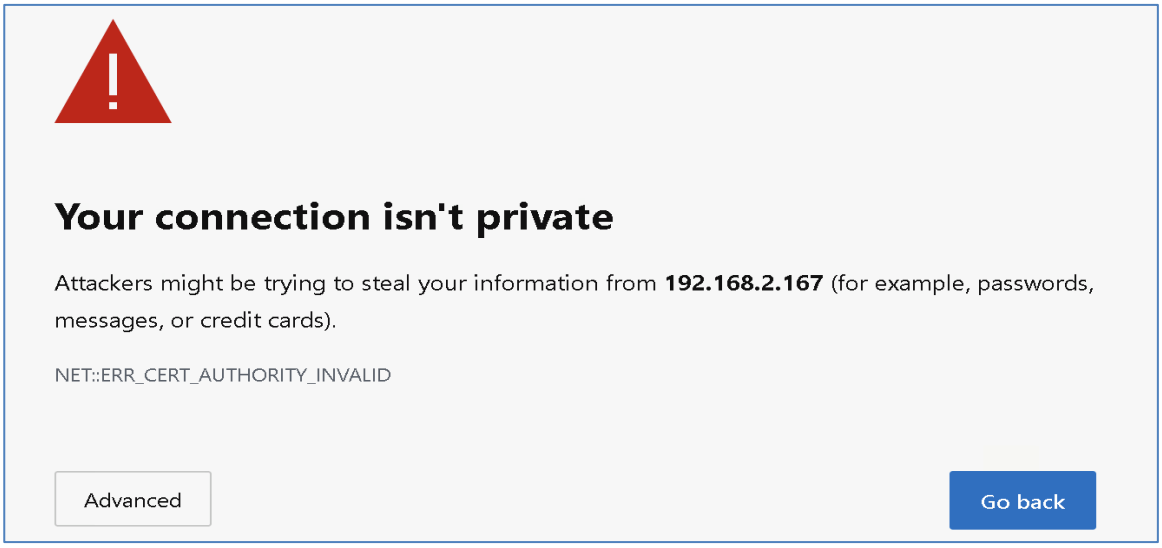
Name	Description
Recommended Browser	Google Chrome, FireFox, MS Edge
OS	Window / Mac / Linux
RAM	≥1GB

CORP HQ +1 (919) 230-8700 | WEST COAST +1 (310) 222-8600
ganzsecurity.com

3. Web access setting page

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).

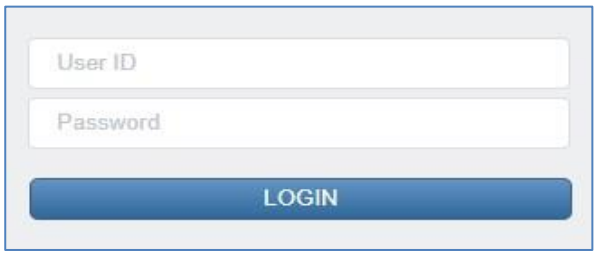
- IP address: https://<AI Box IP>:8443 (e.g.: https://10.10.10.10:8443)
- Note: Default Network security settings are HTTP, which will invoke browser security warnings
- With Chrome as the example, select 'Advanced' to continue past the security warning



- A new security warning, regarding trust of the security certificate will appear
- Below the warning, the message 'Continue to 'AI BOX IP address (unsafe)' will appear
- Click on the warning message to continue onto the AI Box login screen
    - This is a completely safe procedure as the browser is only connecting to the AI Box

- Primary username: ADMIN (Default)
- Password: 1234 (Default)

Note: *It is recommended to change the default password for safety purposes*
A strong password will consist of a combination of upper- and lower-case letters, numbers, and punctuation symbols.

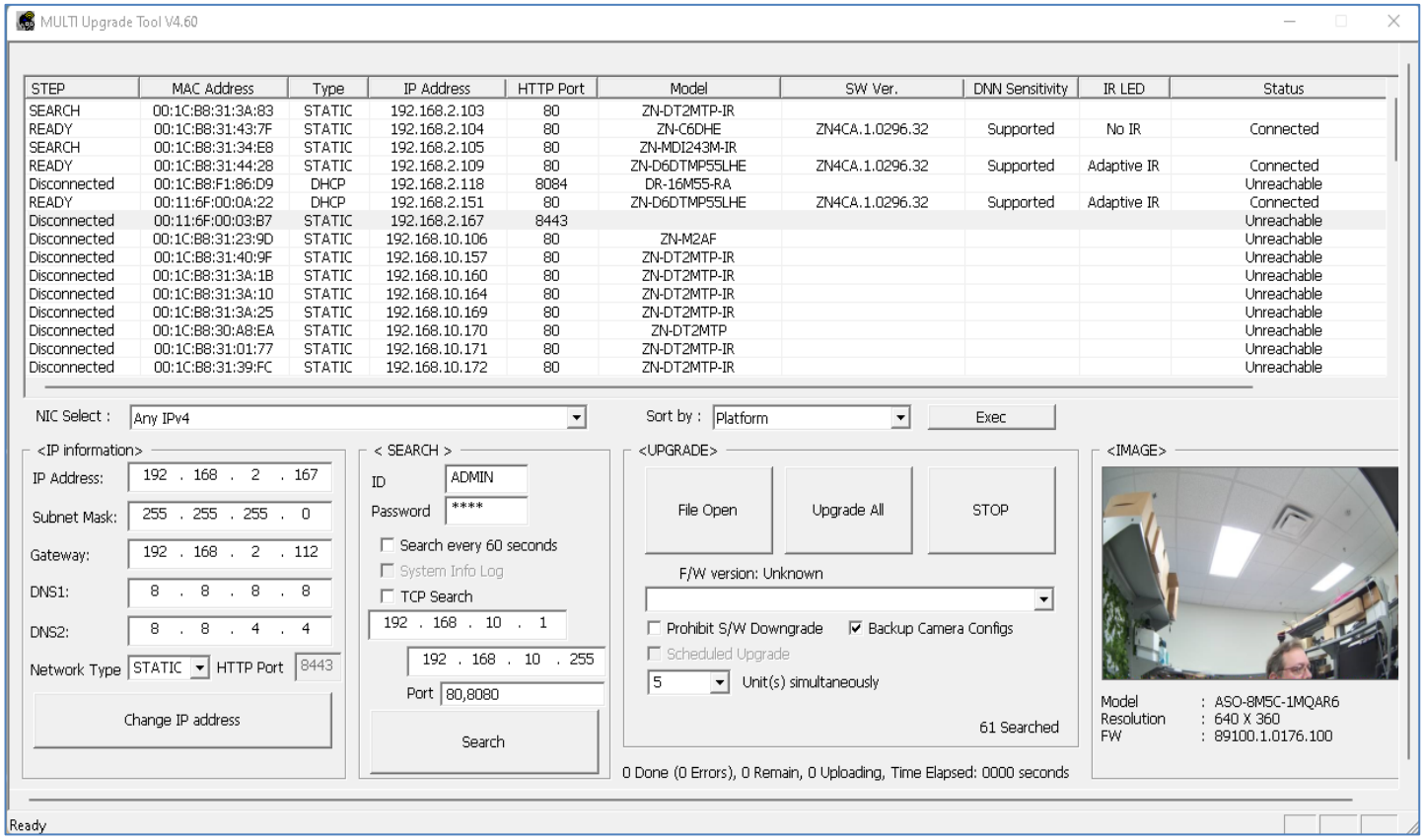


4. Discovery tool

The 'Admin_Tool.exe' allows for the discovery and configuration of the GANZ AI BOX in a network.

The 'Ganz MDload' tool is used for discovery and configuration of Ganz PixelPro IP cameras, the Ganz PixelMaster eNVR, the Ganz Digimaster DVR, and the Ganz AI Box.

- Clicking the 'Search' button will initialize a search and discovery inquiry of the local network
- Devices are discovered by way of their Mac address, not by their IP address
- Search results are displayed on the screen
- The current MDload tool does not list the AI Box model, a revision is in works
    - The AI Box can be recognized by its default HTTP Port of 8443



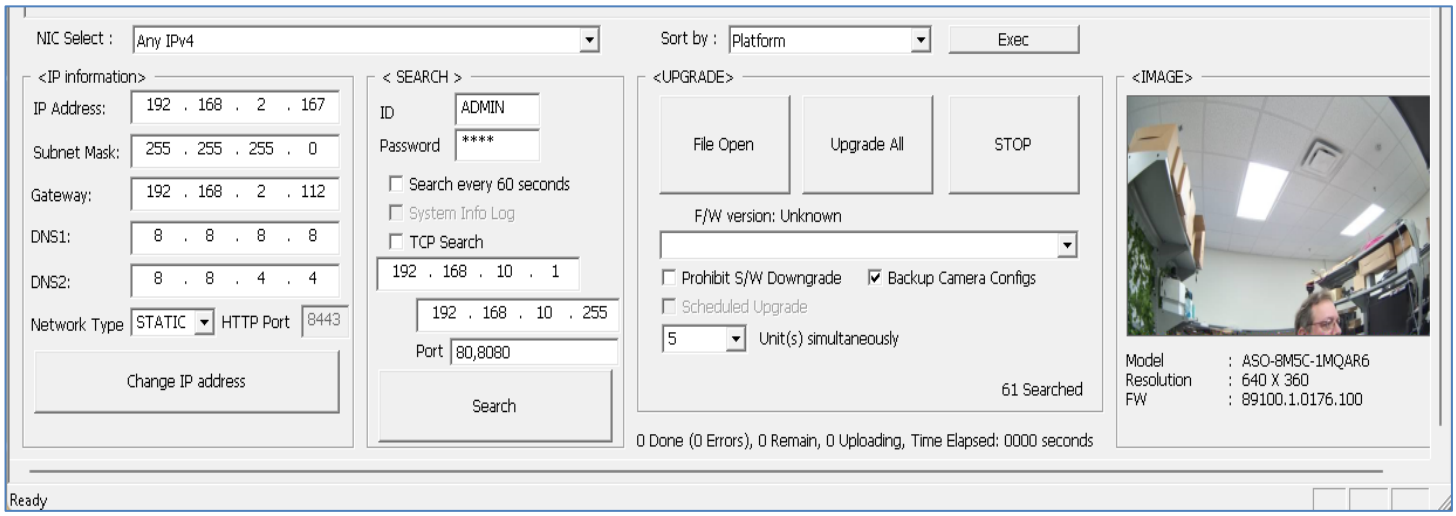
1. Set the Network Type

To set the network type, select the device from the list, highlighting it.

- Network Type: Select either 'DHCP' or STATIC'
  - Selecting 'DHCP' sets the device to query the local DHCP server for IP configuration
  - Selecting 'STATIC' will allow for manual assignment of the device IP configuration
    - Please input the IP Address, Subnet Mask, Gateway, and DNS information

- Change IP address: Click the 'Change IP address' button to commit the changes to the device
  - After a short period, the list will update, and the new network configuration will be listed
  - Please confirm that the new network configuration is correct

- Double click the device information in the list above to open the device setting page



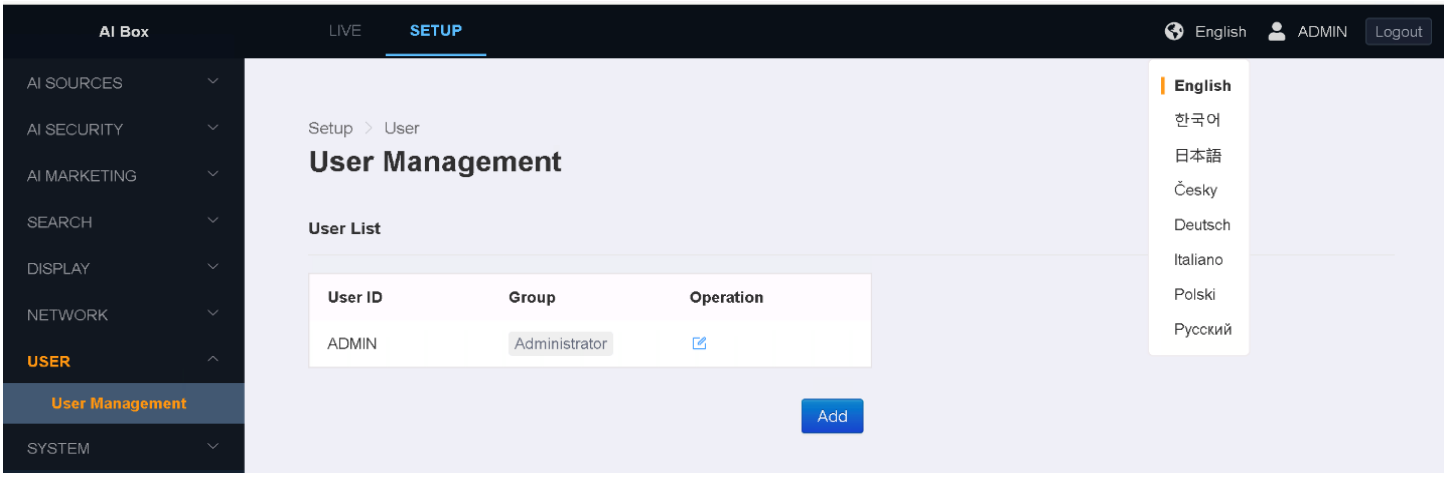
4. System Settings

System settings for the AI Box consist of the Network, User management, Language, Date and Time, and System Management.

1. Language setting

Set the language which will be displayed on the system.
The AI Box language can be changed at any point within the AI Box setup menu.
Select the 'Global' icon in the top right corner and select the language of choice.

- Languages: English, Korean, Japanese, Czech, German, Italian, Polish, and Russian



5. AI Sources

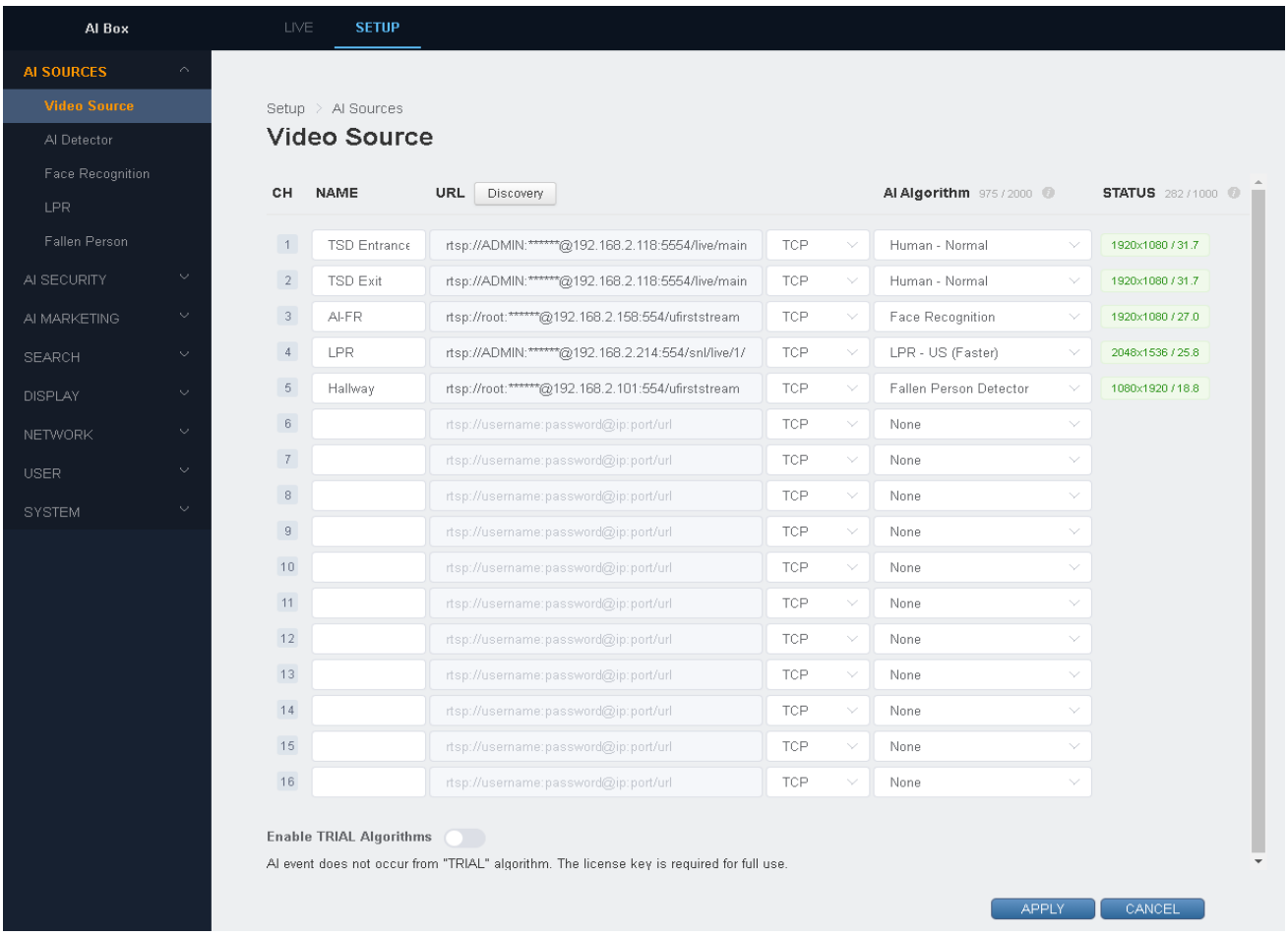
1. Video Source

The AI Box may support up to 16 channels of video from a server or device that supports IP cameras or RTSP streaming. Once configured, a select AI algorithm by be assigned to each video channel.
Select 'Setup/AI Sources/Video Source' to modify or add video sources to the AI Box.

The AI Box offers three options for adding video sources.

- Option one; ONVIF discovery tool
- Option two; Manually applied device RTSP syntax
- Option three; Dedicated DVR / NVR with support for AI Box Plug & Play

[Caution] Video resolution can be connected to a maximum channel resolution of 2 Meg pixels, and 30fps. When connecting a 4K camera, you should connect the channel at a lower 7fps or less to connect all channels.

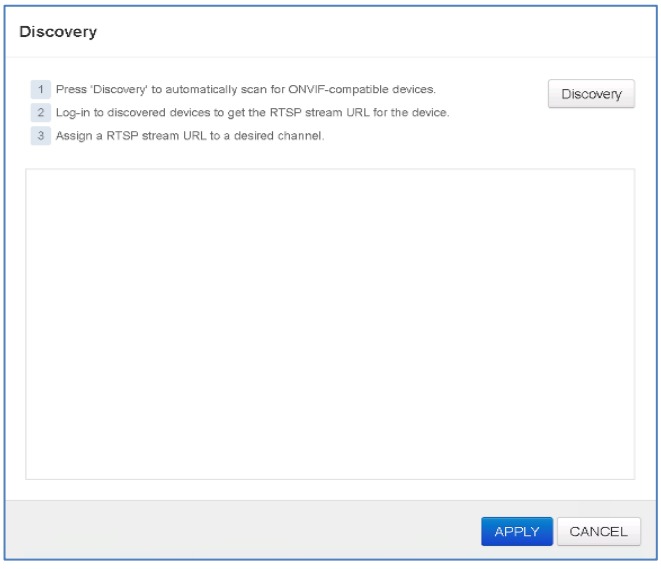


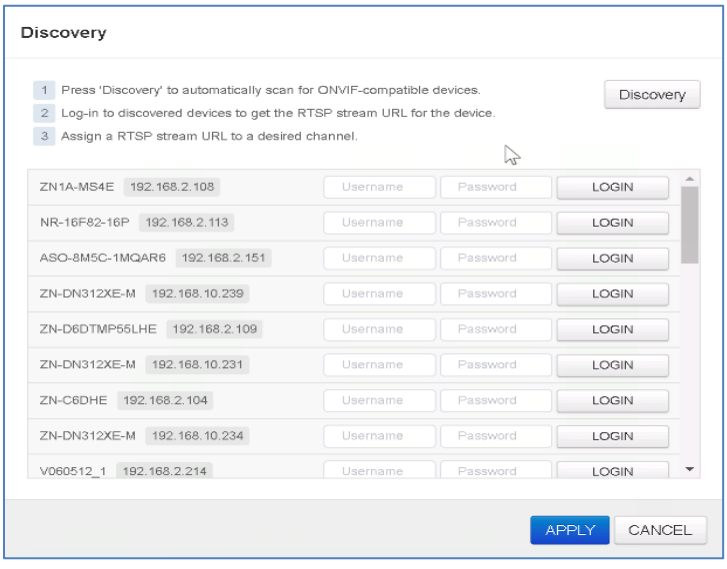
2. ONVIF discovery tool

The ONVIF discovery tool allows discovery of IP cameras, DVRs, and NVR connections using the ONVIF discovery protocol. The video stream address can be configured by searching for the 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, username and password.
- Press the <Login> button to view the video stream address.
- Select 'Apply' to confirm and save the added stream.
- 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.



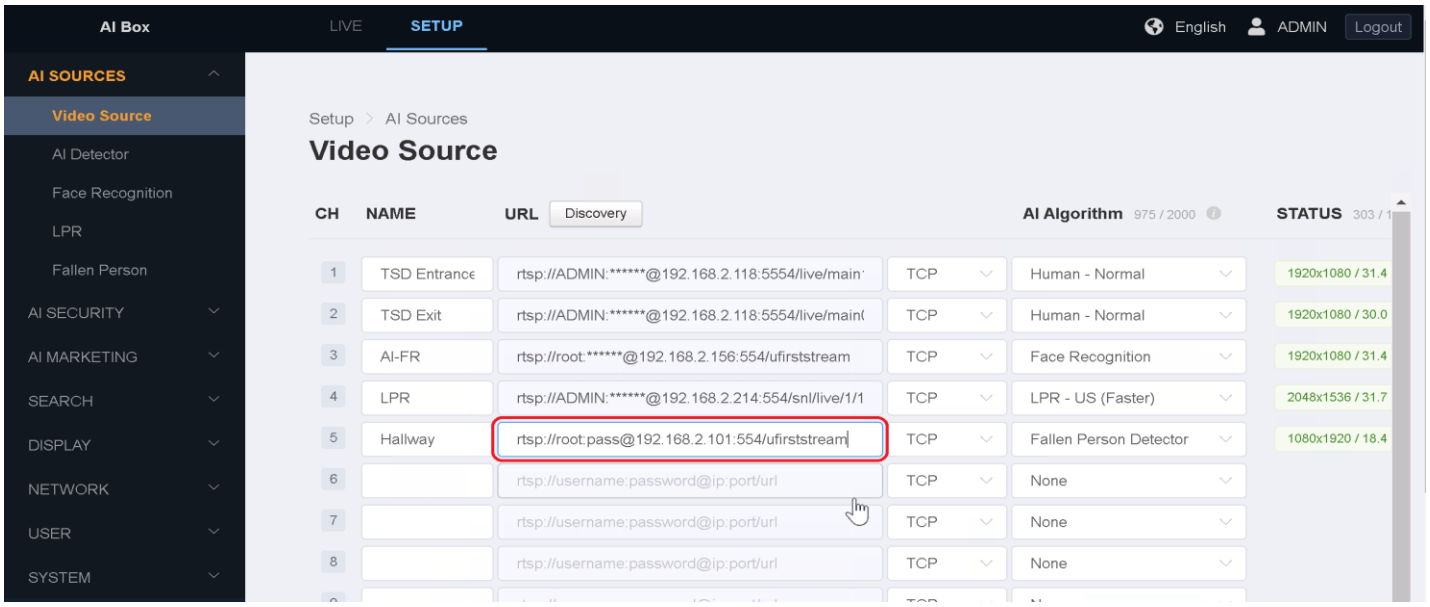


3. Connection via manual entry of RTSP address

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

- Confirm with manufacture of device, the RTSP syntax to use
- URL: enter the RTSP syntax of the device targe
    - example: rtsp://root:pass@192.168.2.101:554/ufirststream

- Select protocol TCP, UDP, or Multicast
- Select the AI Algorithm, example; Human – Normal
- Select 'Apply' to confirm, and save

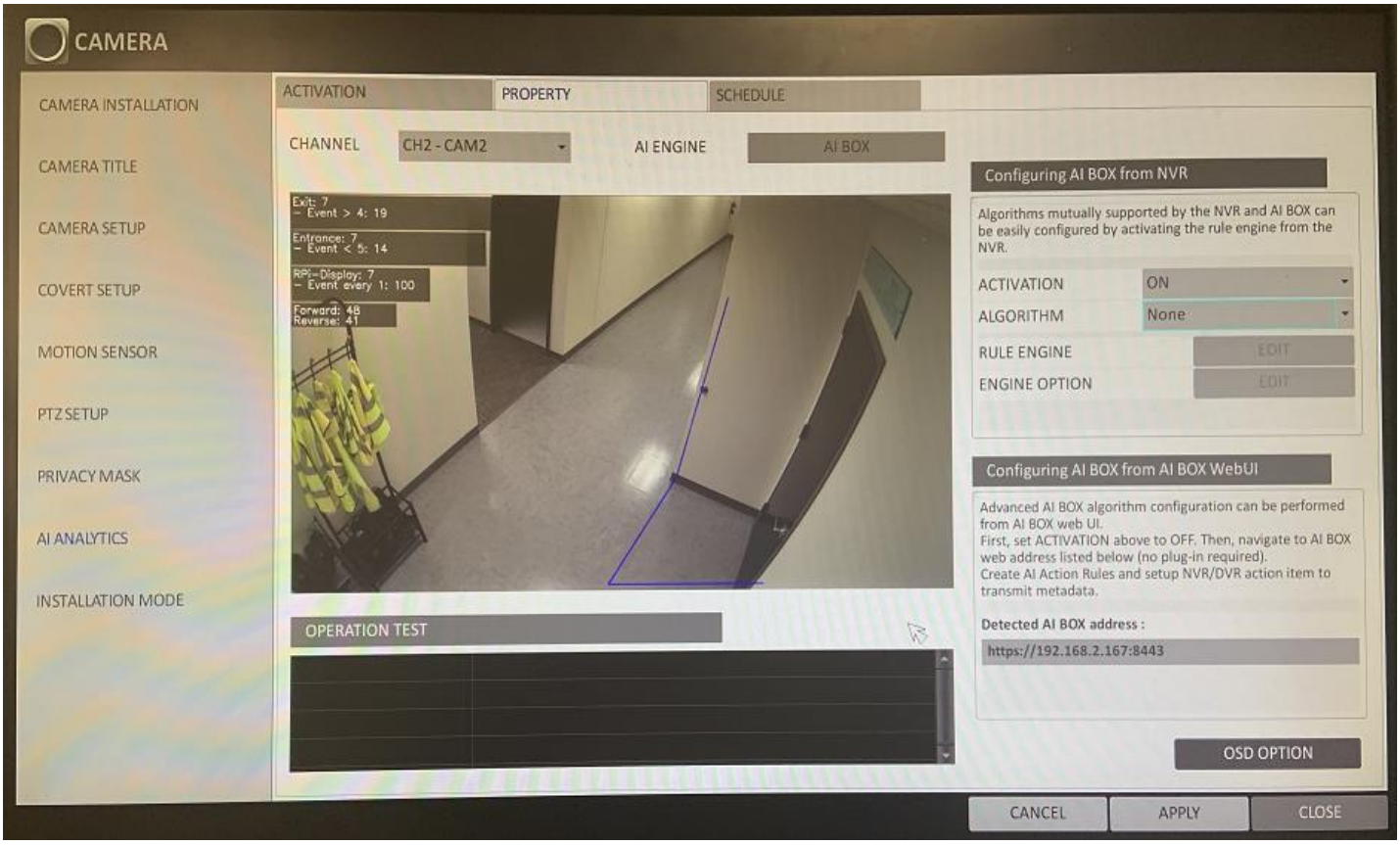


4. DVR / NVR auto connection

The Ganz AI Box supports auto connection to a dedicated DVR (Ganz Digimaster), or dedicated NVR (Ganz PixelMaster) that offer support for the AI Box Plug & Play functionality.

The AI Box can automatically connect through the menu of the DVR (Ganz Digimaster), or NVR (Ganz PixelMaster) without setting the device through the AI Box's Web UI.

Please refer to the DVR (Ganz Digimaster) or NVR (Ganz PixelMaster) user guide for details.



5. AI Algorithm

After configuring a select video source, select either a basic AI algorithm, licensed based AI algorithms, or custom AI algorithms to apply to the channel for analyses by.

Basic AI Algorithm
Basic AI algorithms are algorithms that are standard on the AI Box.

- **Human / Vehicle - Far**
  - This algorithm is optimized to distinguish people and vehicles in the far distance

- **Human / Vehicle - Normal**
  - This algorithm detects medium distance of people and vehicles

- **Human / Vehicle - Normal (Faster Objects)**
  - This algorithm is optimized to track fast moving people and vehicles
  - Higher accuracy can be obtained when using 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
  - Human far: Width – 1.00% / Height – 3.00%
  - Vehicle far: Width – 2.00% / Height – 1.50%
  - Human normal: Width – 1.25% / Height – 4.50%
  - Vehicle normal: Width – 3.00% / Height – 2.25%

- Minimum detectable object size of Loitering, Enter / Exit and Line Crossing
  - Human far: Width – 1.25% / Height – 5.00%
  - Vehicle far: Width – 3.00% / Height – 2.50%
  - Human normal: Width – 2.00% / Height – 6.00%
  - Vehicle normal: Width – 7.00% / Height – 6.00%

Licensed AI Algorithm
Licensed AI algorithms are algorithms that require the purchase of a license to register of the algorithm.

- Some licensed AI Algorithms: Privacy Masking, Face Recognition, LPR, and Fisheye

Custom AI Algorithm
Custom AI algorithms are algorithms trained and tailored toward a specific requirement such as helmet or mask detection.

Note: Choosing a particular AI algorithm will reduce the number of AI algorithm assignable channels, as each AI algorithm has a different resource overhead requirement.

Each AI Box offers a finite number of AI algorithmic units, or resources, usable by a selected AI Algorithm.

- The 4Ch AI Box offers a total capacity of up to 1000 AIu's (250 AIu's per channel)
- The 8Ch AI Box offers a total capacity of up to 2000 AIu's (250 AIu's per channel)
- The 16Ch AI Box offer a total capacity of up to 2000 AIu's (125 AIu's per channel)

* If the required AI unit resource cost is 500AIu's

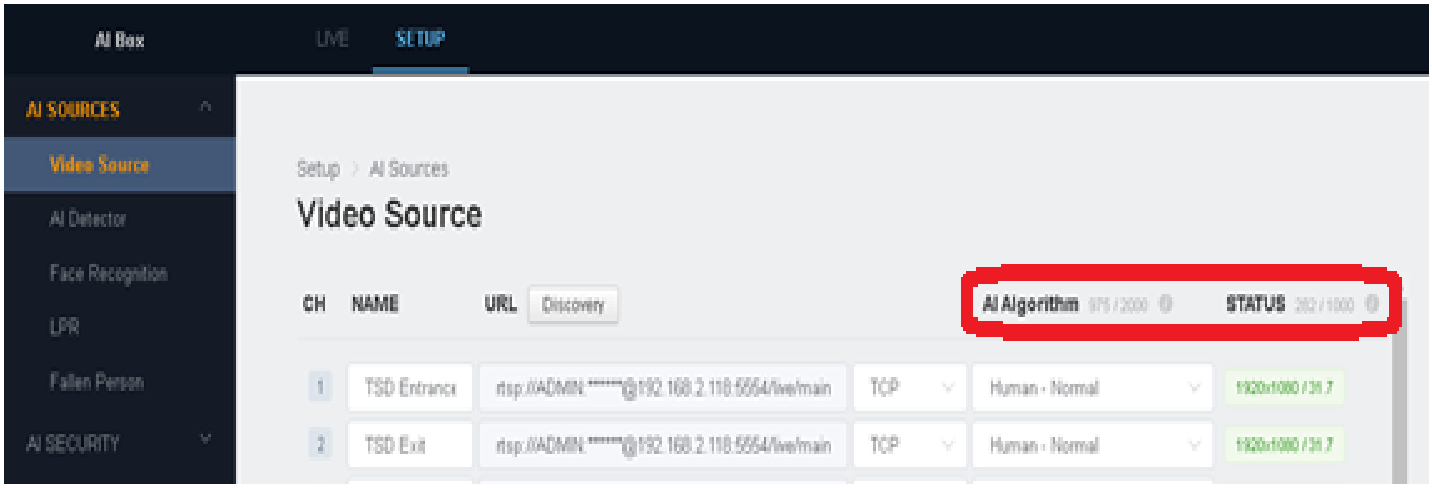
- 4Ch AI Box: maximum allocation is 2 channels (= 250 AIu's x 2 Ch's = 500 AIu's)
- 8Ch AI Box: maximum allocation is 2 channels (= 250 AIu's x 2 Ch's = 500 AIu's)
- 16Ch AI Box: maximum allocation is 4 channels (= 125 AIu's x 4 Ch's = 500 AIu's)

AI Engine resources

- Within the Video Source menu, reference the AI Algorithm indicator
- This is a reference of the current resources used by the applied Analytics

Video Decoding resources

- From the Video Source menu, reference the STATUS indicator
- This is a reference of the current resources used for Video Decoding



2. AI Detector

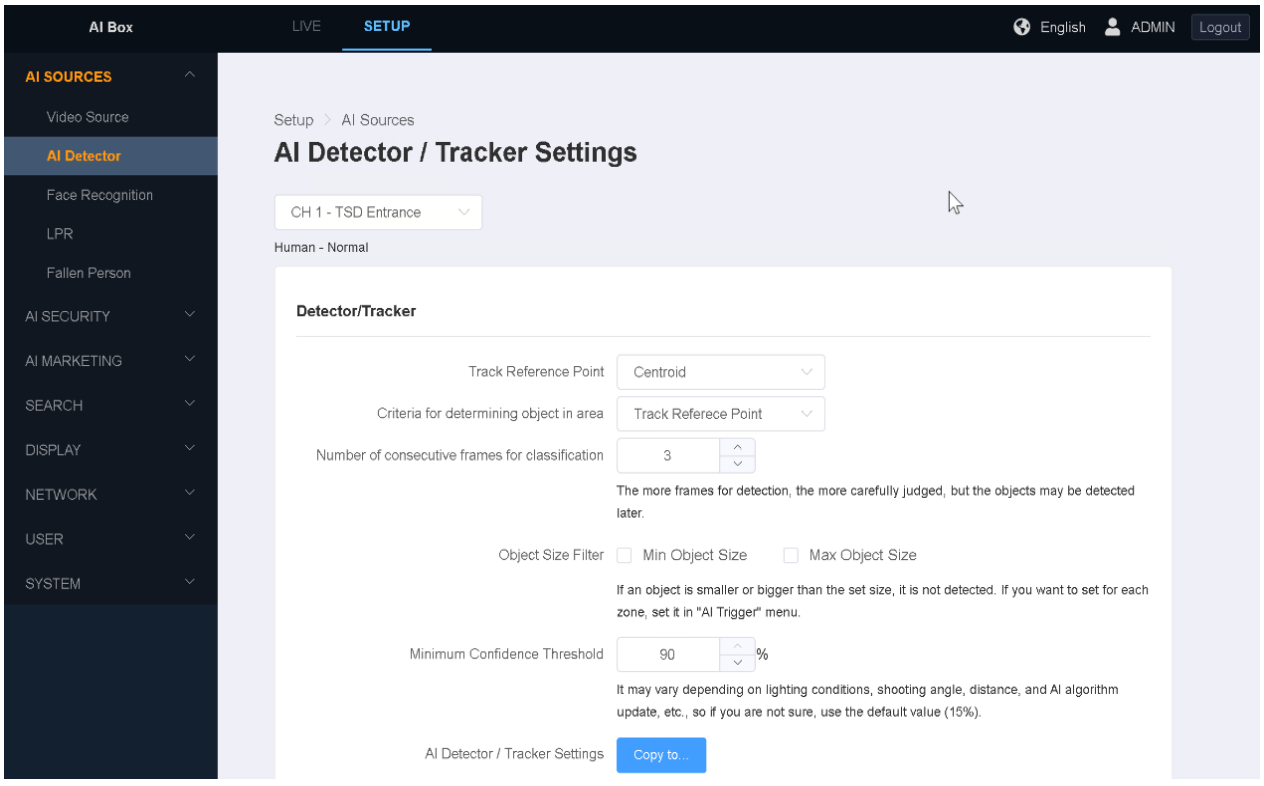
The AI Detector is where the AI Tracking configuration may be found SETUP/AI SOURCES/AI Detector

- Channel selector: Select target channel to configure AI Detector for
- Track Reference Point: select either Centroid, Bottom, Top, Left, or Right
- Criteria for determining object in area: Track Reference Point, or All points of bounding box
- Number of consecutive frames for classification: 1 ~ 50
    - The more frames for detection, the more carefully judged, but objects may be detected later

- Object Size Filter: Min Object Size, and or Max Object Size
    - If an object is smaller or bigger than the set size, it is not detected.
    - If you want to set for each zone, set it in the “AI Trigger” menu.

- Minimum Confidence Threshold: 15% ~ 90%
    - It may vary depending on lighting conditions, shooting angle, distance, and AI algorithm update, etc. If you are not sure, use the default value of 15%

- AI Detector / Tracker Settings: Copy to…
    - Copy settings to selected target channel, or channels

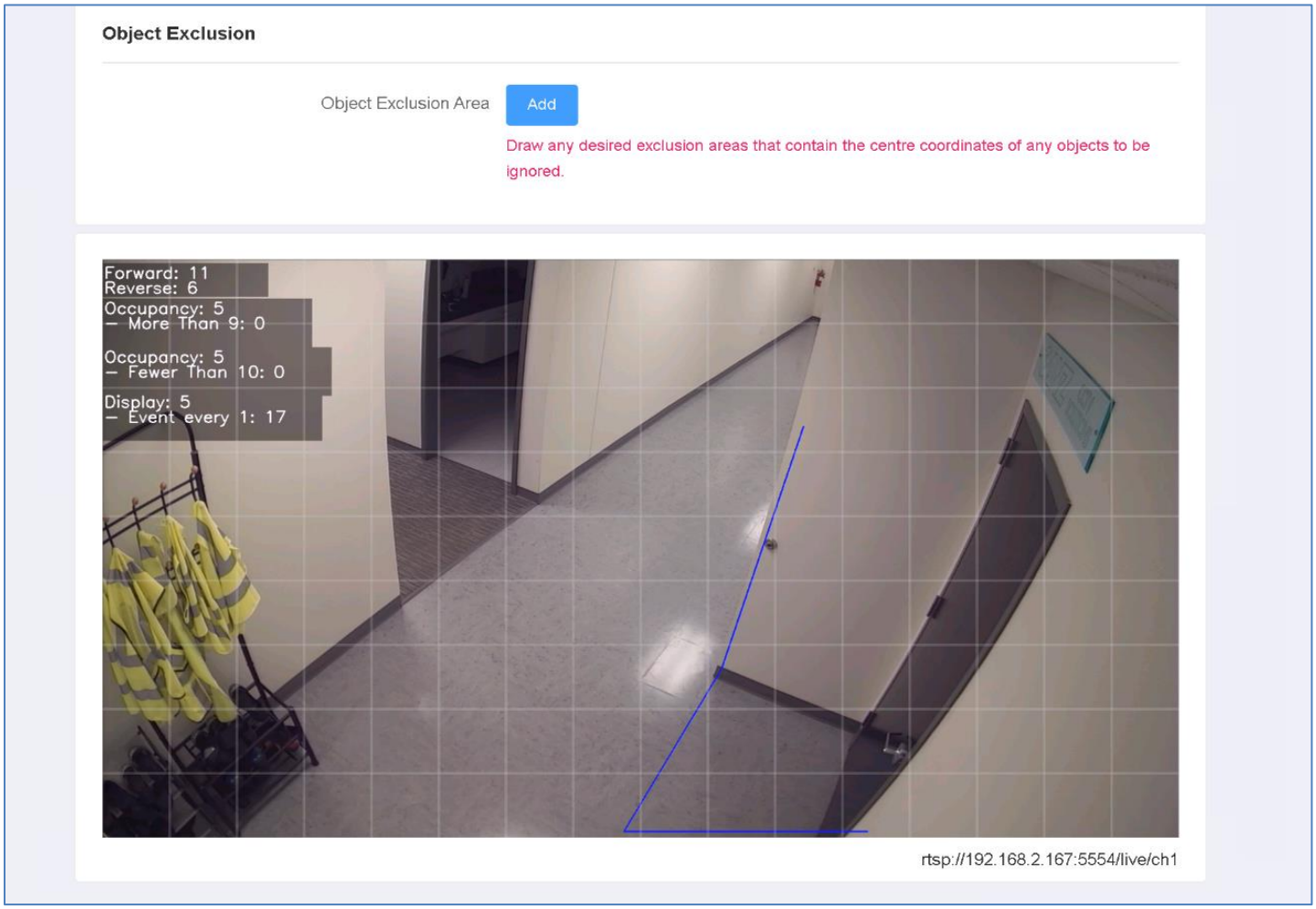


Object Exclusion

The 'Object Exclusion' found at 'Setup/AI Sources/AI Detector, offers configuration of the exclusion mechanism. This allows for the creation of a zone of exclusion, where AI detection is turned off. No objects will be detected or classified.

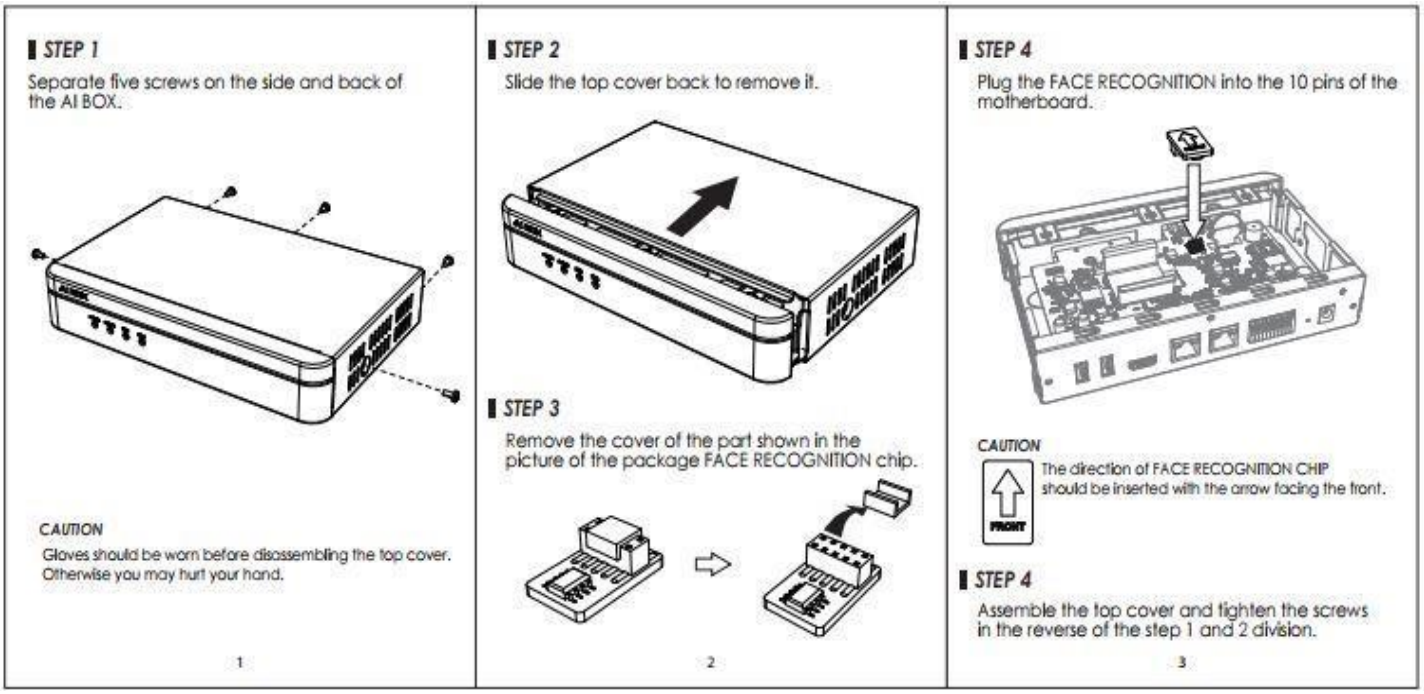
- Object Exclusion Area: select 'Add'
  - A zone will appear, each time 'Add' is selected
  - Pull zone points to stretch, shrink, and expand the exclusion zone
  - Many zones may be created, and overlap

- Select 'Apply' to confirm and save all AI Detector settings.



3. Face Recognition

To use the face recognition function, the AI Box requires the installation of the FR chip.
The AI Box with the FR chip already installed maybe an option at time of purchase. If the AI Box did not come with the FR chip, the chip can be purchased separately and installed.

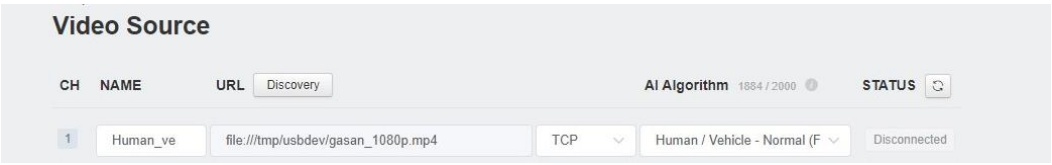


1. FR Algorithm

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

Video Source menu is located at SETUP/AI SOURCES/Video Sources -> Set the target channel AI Algorithm to Face Recognition.

- Select 'Apply' to confirm and save all AI Algorithm settings.

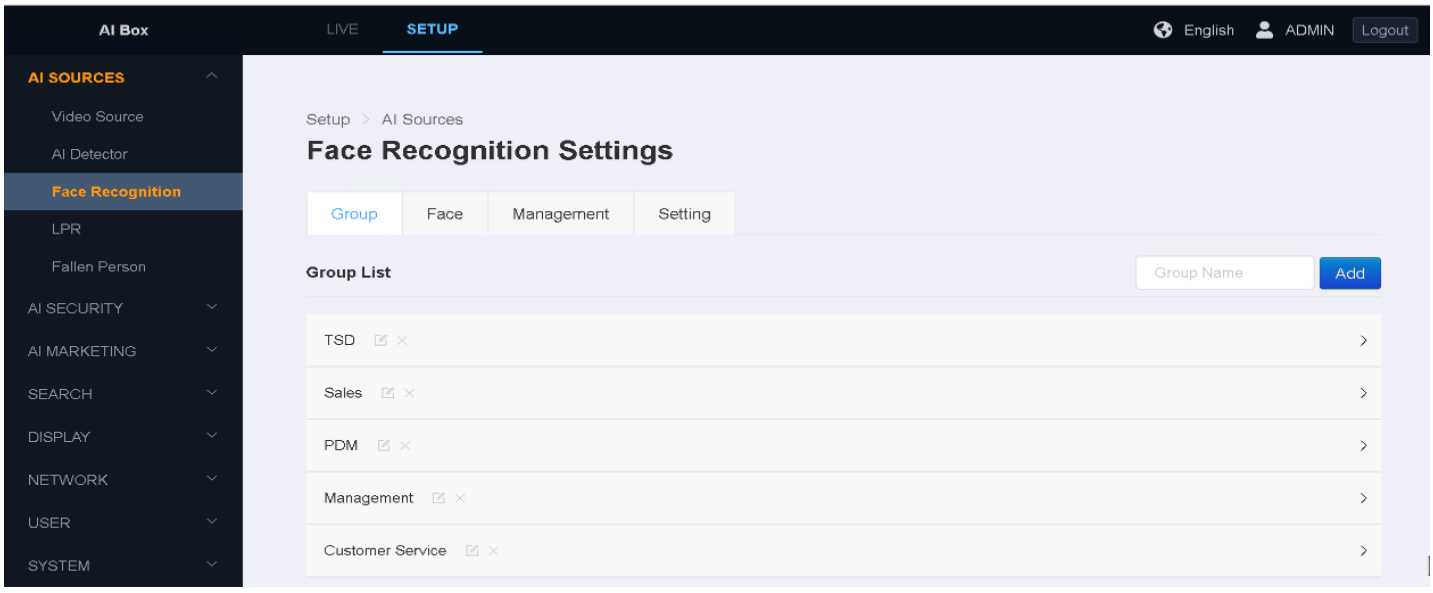


2. FR Group List

You can create a group of face recognition databases in the 'Groups' tab of the 'Face Detection' menu under SETUP/AI SOURCES/Face recognition – Note: A Face Recognition AI License is required for the function.

SETUP/AI SOURCES/Face recognition It is possible to create a group of face recognition databases from the Group menu.

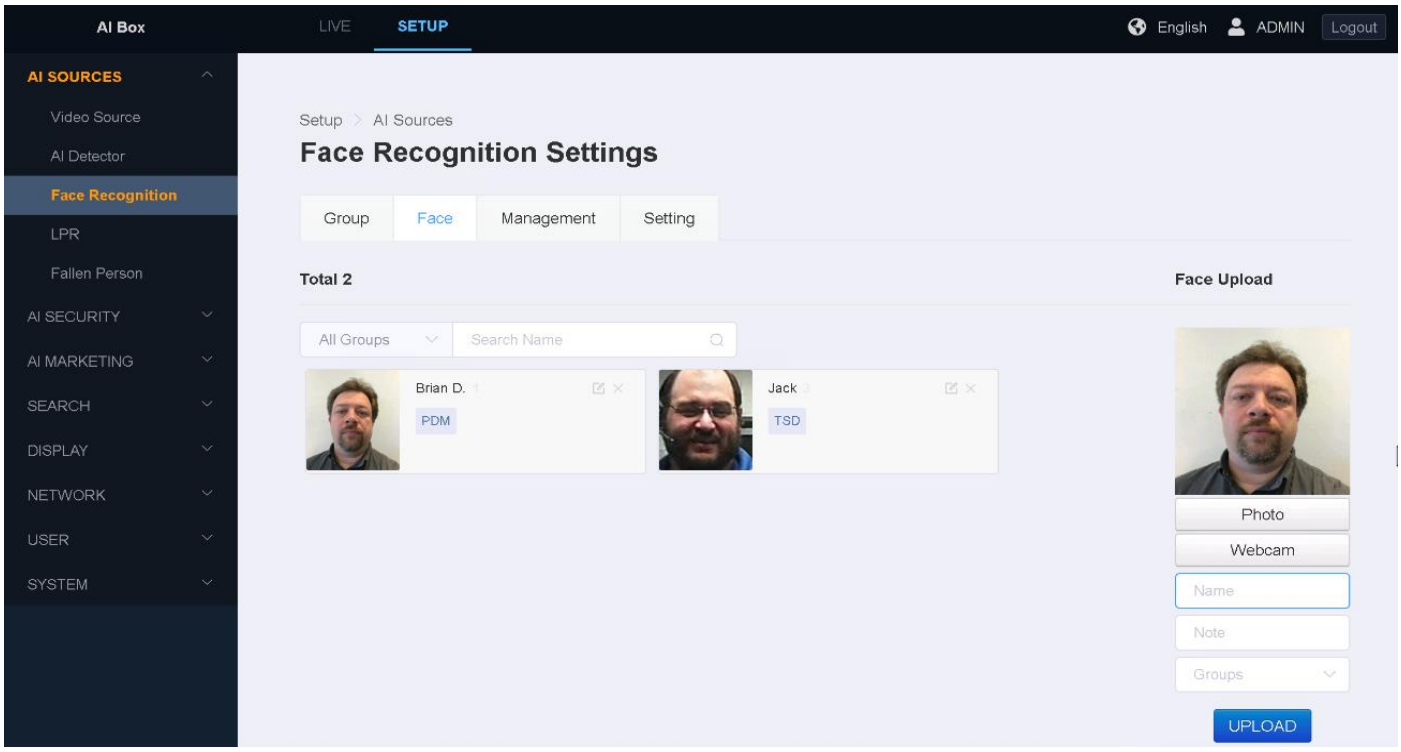
- Group Name: Enter a group name according to intent
- Select 'Add' to create a face recognition group database



Face recognition data can be added individually in the SETUP/AI SOURCES/Face recognition -> ‘Face tab’ of the 'Face Detection' menu.

- Photo: Click the photo button to upload a picture.
    - In the case of a photo, it can be resized, if the size is large
    - Photos with only faces taken from the front are more accurate

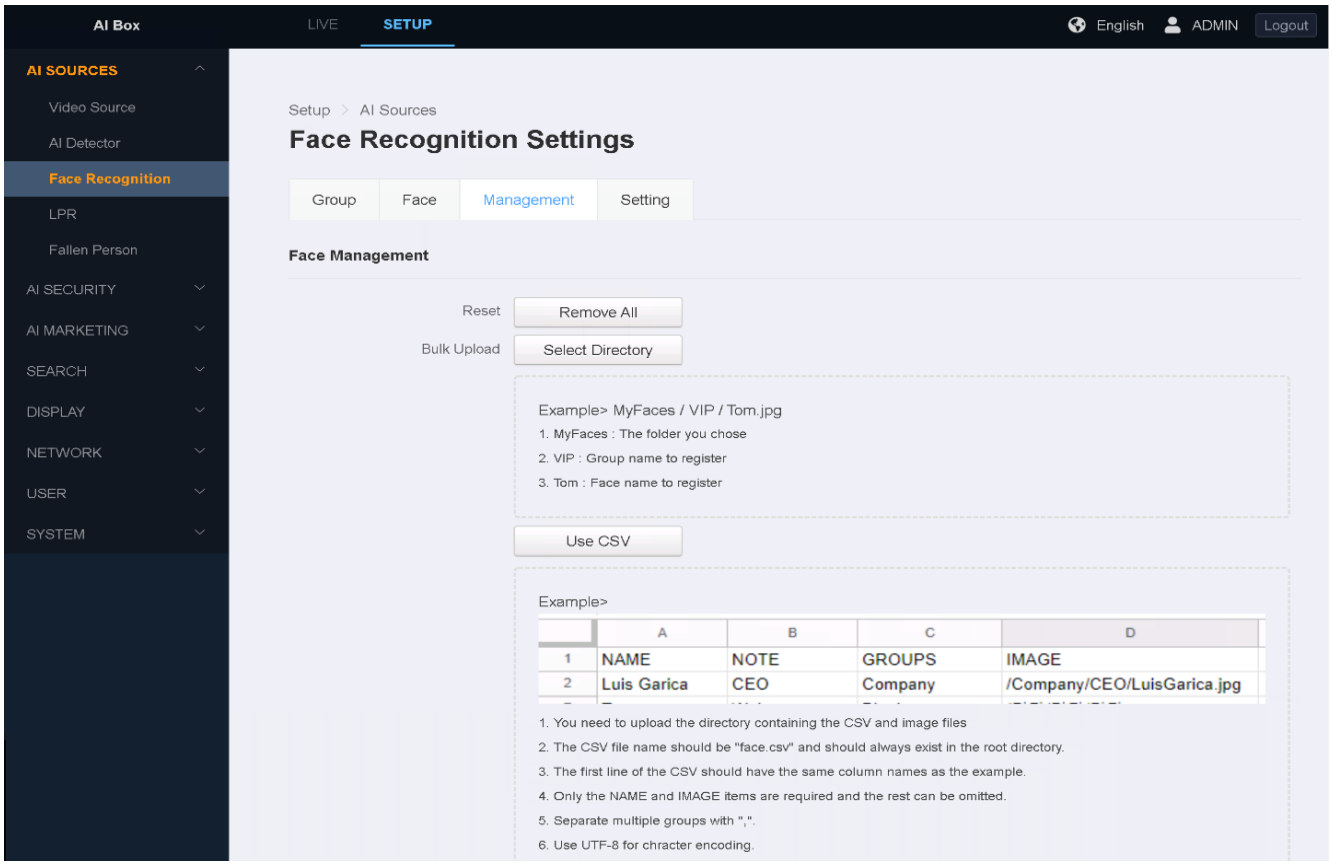
- Webcam: Click the Webcam button to use a photo taken with a PC connected Webcam
- Name: Enter the name of the person whose photo was submitted to the database
- Note: Enter any note related to the person whose photo was submitted to the database
- Group: Select the face recognition group data base to assign the person’s photo to
- Select ‘UPLOAD’, to upload the person’s photo and information to the assigned face recognition data base



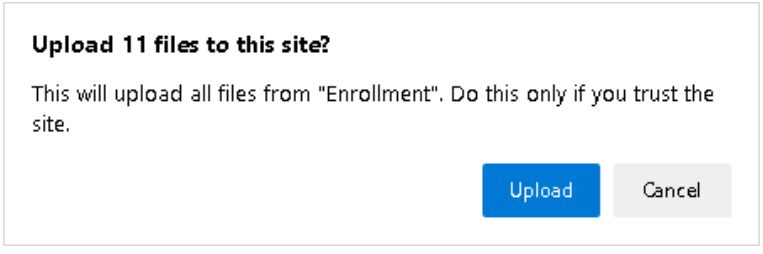
Face Recognition Management

Face Recognition Subjects may be managed in bulk from the 'Management' tab under the SETUP/AI SOURCES/Face recognition -> ‘Face Recognition Settings'.

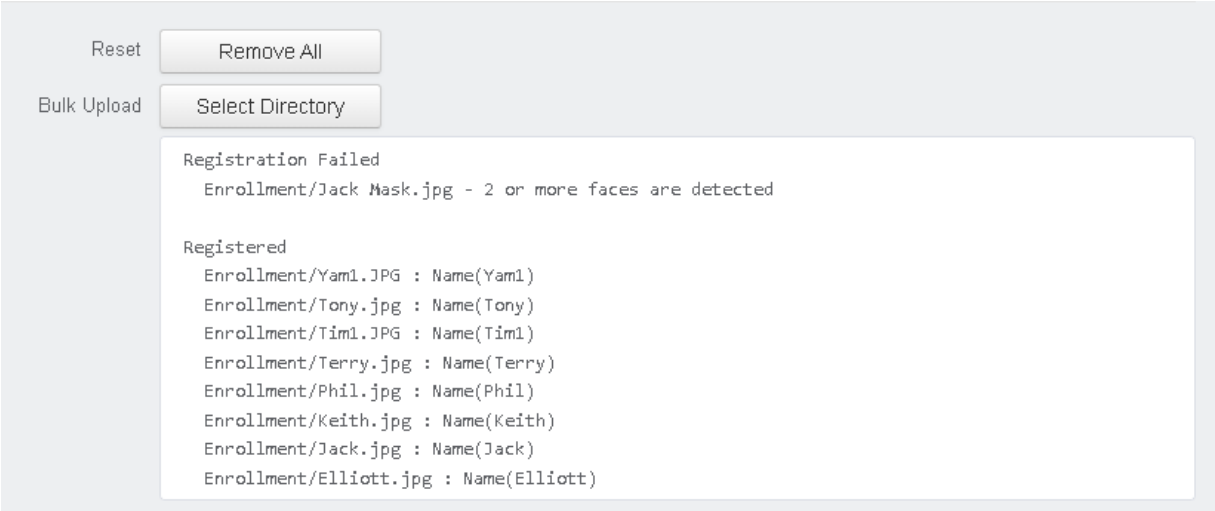
- Reset: Will ‘Remove All’ face recognition data from the AI BOX
- Bulk Upload: ‘Select Directory’ – navigate to the directory folder location of FR images
    - This function will select and upload all the images contained within the target folder



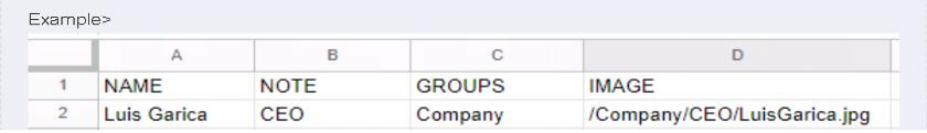
- Bulk Upload: A popup message will alert as to how many images will be updated for ‘Enrollment’
    - Select ‘Upload’ to begin uploading the discovered images



- Bulk Upload: After 'Upload' completes, a registered status message will appear
  - Registration Failed: Listing any failed registrations
  - Registered: Listing all successfully enrolled registrations

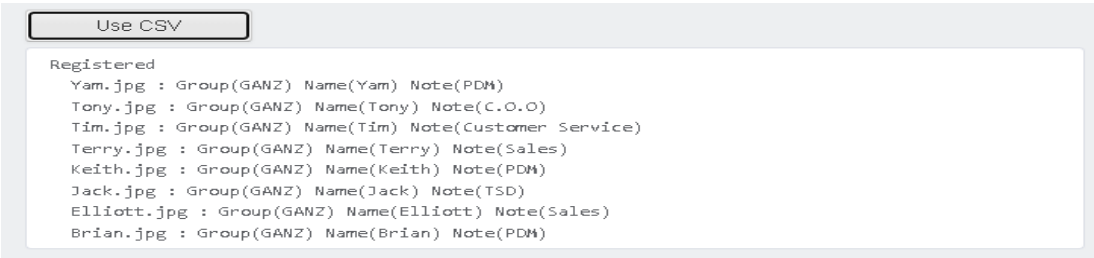


- Use CSV: Select 'Use CSV' to upload a CSV file containing Face Recognition enrollment information
  - CSV file management is support for instances of large FR databases
  - upload the CSV file containing the following information
    - CSV format: Column headers – Name / Note / Groups / Image



	A	B	C	D
1	NAME	NOTE	GROUPS	IMAGE
2	Luis Garica	CEO	Company	/Company/CEO/LuisGarica.jpg

- Use CSV: After 'Upload' completes, a registered status message will appear
  - Registration Failed: Listing any failed registrations
  - Registered: Listing all successfully enrolled registrations



4. LPR: License Plate Recognition

1. LPR AI Algorithm

Set the AI algorithm to LPR in the Video Source menu under AI Source.

Video Source menu is located at SETUP/AI SOURCES/Video Sources -> Set the target channel AI Algorithm to LPR.

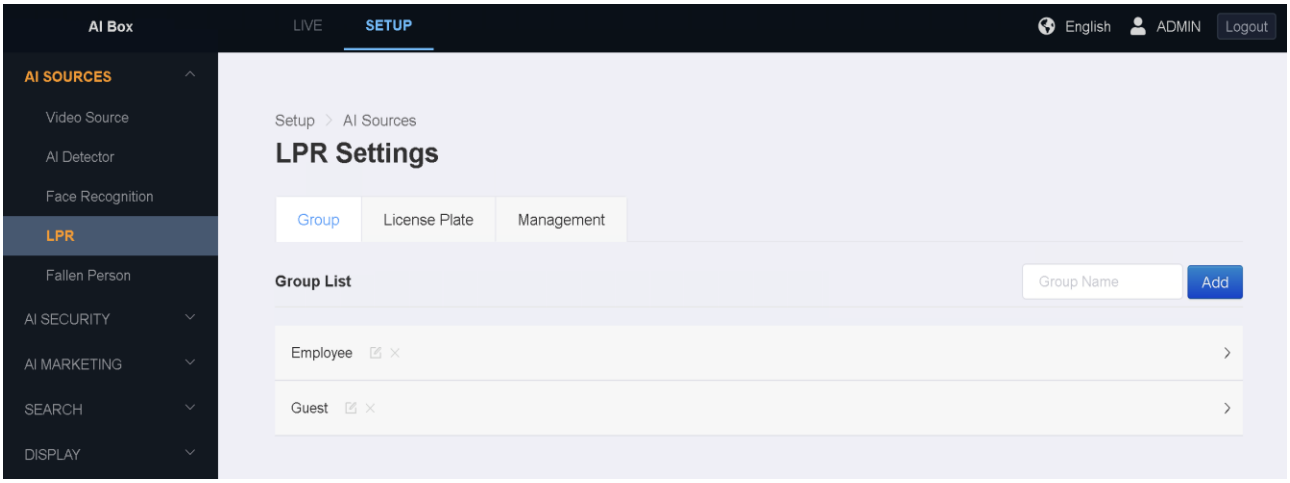
- Select 'Apply' to confirm and save all AI Algorithm settings.

2. LPR Group List

You can create a group of LPR databases in the 'Groups' tab of the 'LPR' menu under SETUP/AI SOURCES/LPR. Note: an LPR AI License is required for the function.

SETUP/AI SOURCES/LPR - It is possible to create a group of LPR databases from the Group menu.

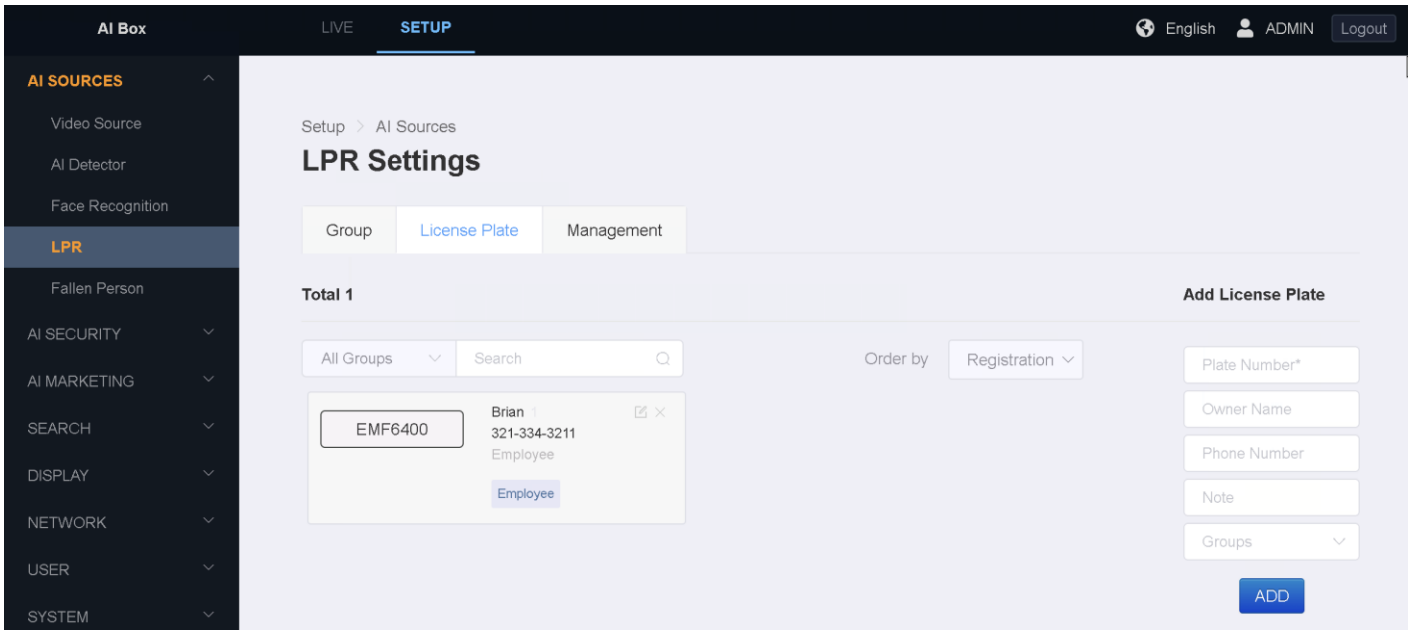
- Group Name: Enter a group name according to intent
- Select 'Add' to create an LPR group database



License place recognition data can be added individually in the SETUP/AI SOURCES/LPR -> ‘License Plate tab’ of the 'LPR Settings' menu.

- Add License Plate: Add an individual license plate
  - Plate Number:
  - Owner Name: Enter the name of the person whose photo was submitted to the database
  - Phone Number:
  - Note: Enter any note related to the person whose photo was submitted to the database
  - Groups: Select the LPR group to assign the license plate information to
  - Select ‘ADD’, to add the license plate information to the LPR database

- Order by: Select either ‘Registration’, ‘Name’, or ‘LPR’

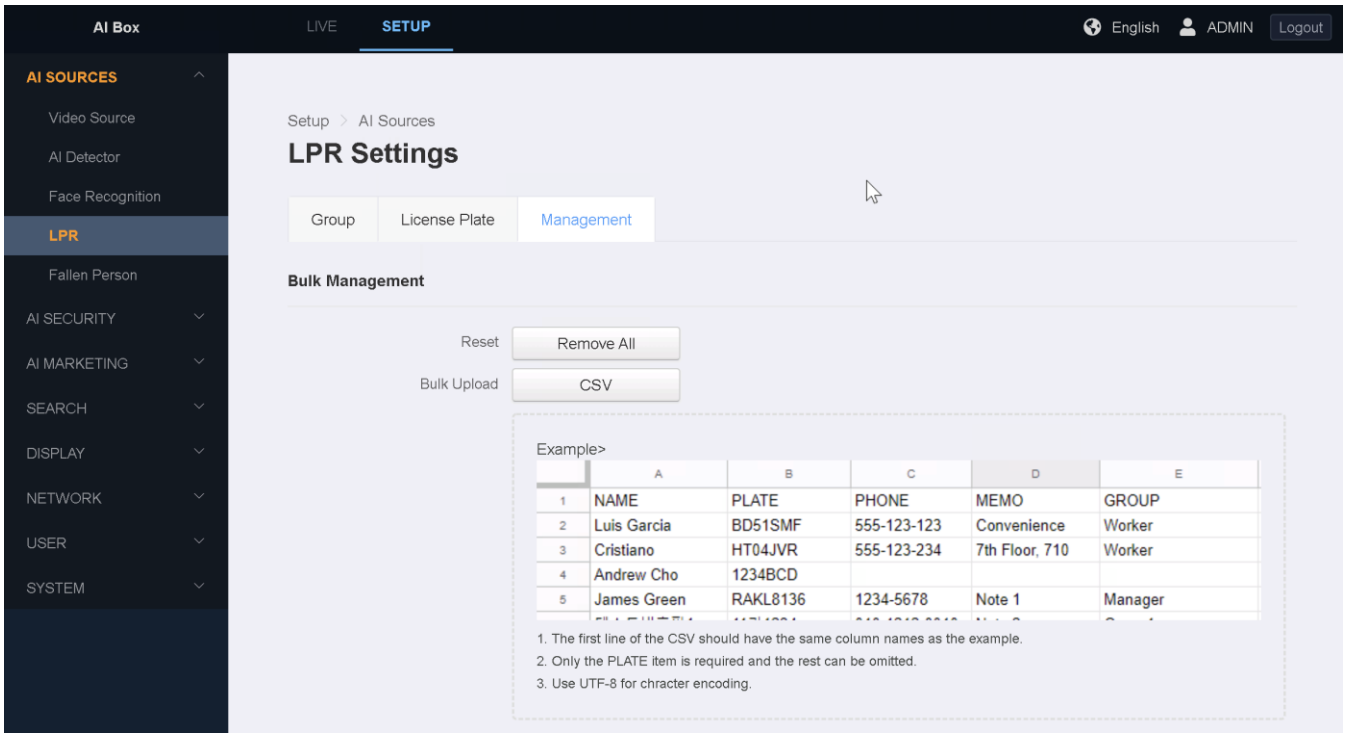


License Plate Management

License plates may be managed in bulk from the 'Management' tab under the SETUP/AI SOURCES/LPR -> 'LPR Settings'.

- Reset: Will 'Remove All' license plate recognition data from the AI BOX
- Bulk Upload: Select 'CSV' to upload a CSV file containing license plate enrollment information
  - CSV file management is support for instances of large LPR databases
  - upload the CSV file containing the following information
    - CSV format: Column headers – Name / PLATE/ PHONE / MEMO / Group

- CSV: After 'Upload' completes, a registered status message will appear
  - Registration Failed: Listing any failed registrations
  - Registered: Listing all successfully enrolled registrations



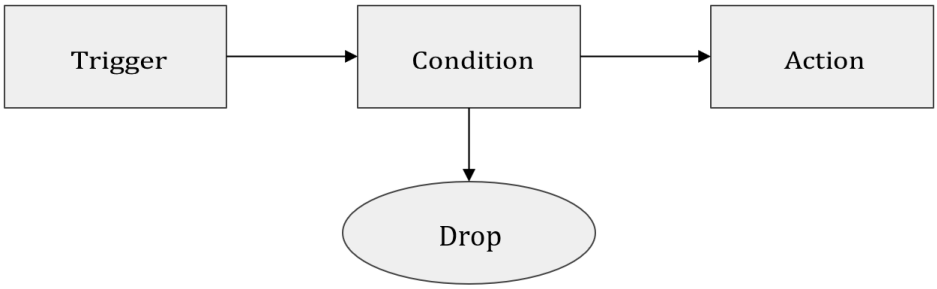
	A	B	C	D	E
1	NAME	PLATE	PHONE	MEMO	GROUP
2	Luis Garcia	BD51SMF	555-123-123	Convenience	Worker
3	Cristiano	HT04JVR	555-123-234	7th Floor, 710	Worker
4	Andrew Cho	1234BCD			
5	James Green	RAKL8136	1234-5678	Note 1	Manager

6. AI Security

1. Action Rule Overview

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

Action Rule composition



There are 2 types of triggers, an AI Trigger, and a System Trigger. Both kinds can trigger an Action Rule.

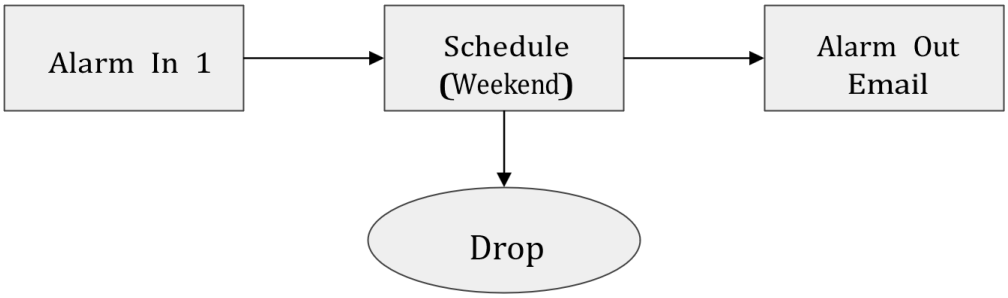
- AI Trigger: is an event discovered by the AI
- System Tigger: Events detected by system sensors, example sensor state changes

The 'Condition' is a filter component for a trigger. Typically, a 'Schedule' condition is to set to filter a condition by a time component.

The Action defines the action to be performed when a trigger event occurs, and a condition is met.

- An Action can define and perform various types of actions, including exporting alarm outputs or sending their events to the ONVIF Metadata Stream.

Action Rule example



CORP HQ +1 (919) 230-8700 | WEST COAST +1 (310) 222-8600
ganzsecurity.com

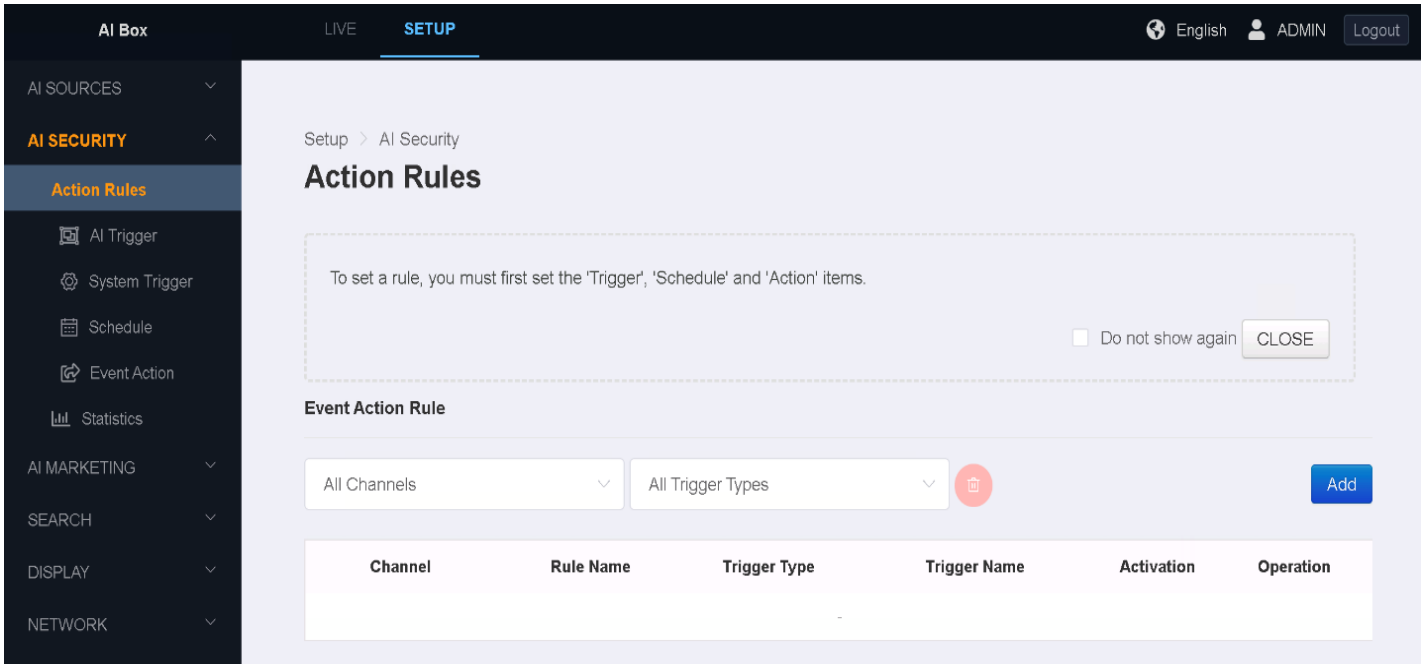
2. Action Rules

Action Rules are a formula by which an 'AI Trigger', or 'System Trigger' a combined with an 'Event Action' to create a rule. When a trigger is acknowledged, initiate a predefined action(s)

To configure an 'Action Rule', go to SETUP/AI Security/Action Rules

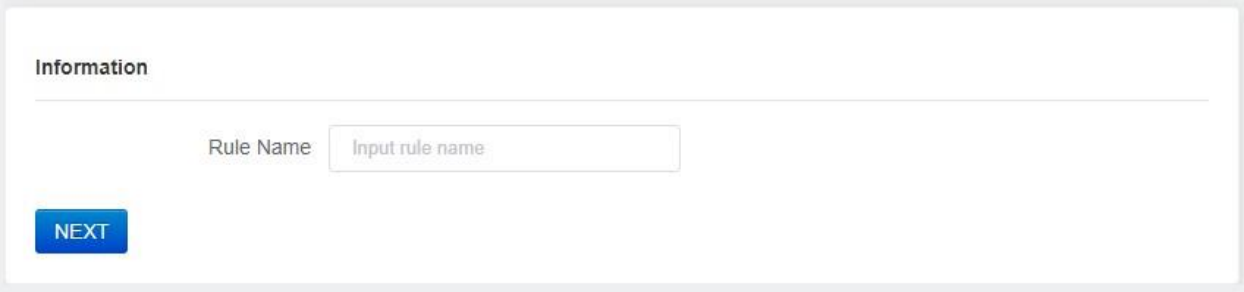
- Note: To set a rule, you must first set the 'Trigger', 'Schedule' and 'Action' items
  - Select 'CLOSE' if you do not wish to show this message again.

- Select 'Add' to create an action rule

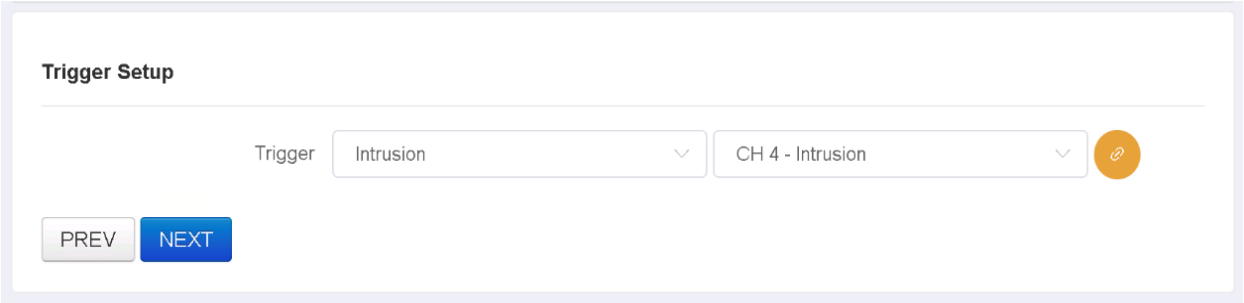


- Event Action Rule: A step indicator is used to track the current rule creation progress

- Rule Name: Title the rule name according to intent
- Select 'NEXT' to continue



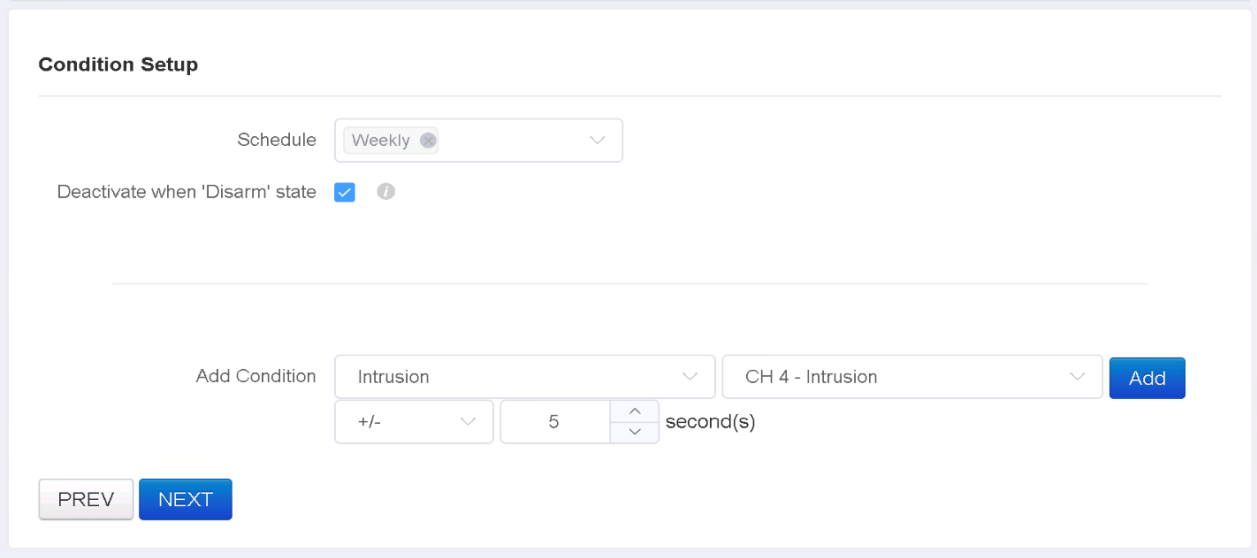
- Trigger: Select an available trigger type from the trigger list menu
  - Select a related trigger preset from the preset list menu
- Select 'NEXT' to continue



Create a condition or multiple conditions: A condition is 'True' if any of the selected items are met when multiple schedules are selected. A condition is 'False' if any of the selected items are not met when multiple schedules are selected.

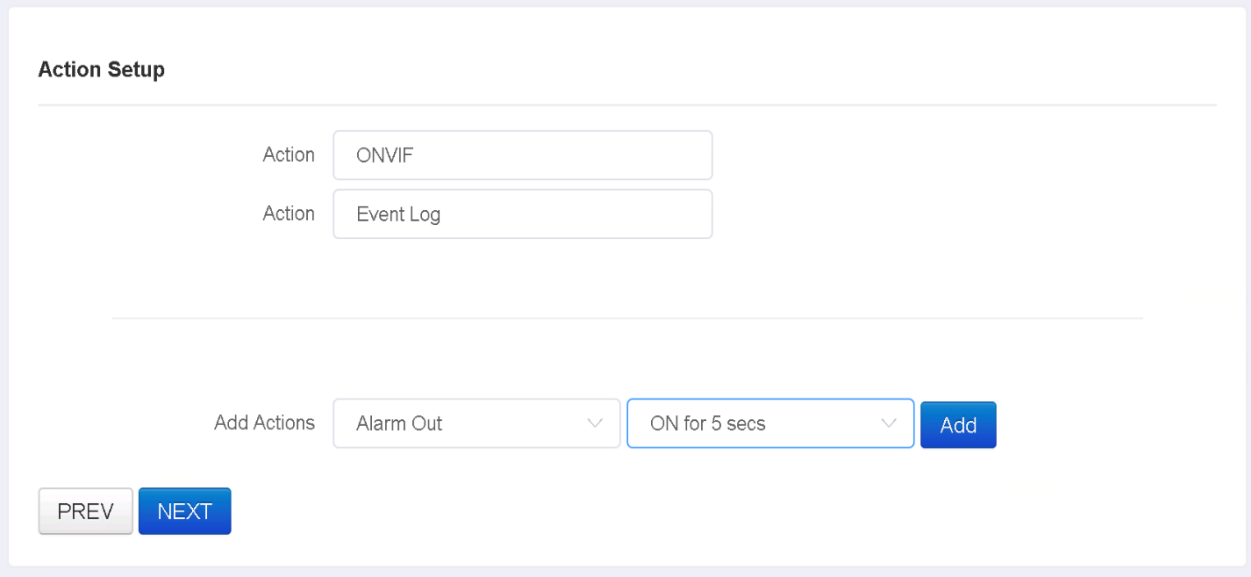
- Schedule: Select the desired schedule from the schedule list menu
  - It is set to 'Always' by default

- Deactivate when 'Disarm' state: Check to enable deactivating the rule upon a disarm
- Condition: Select the '+' icon to add a condition to the schedule
    - Select Type: Select a trigger type from the list menu
        - List: Intrusion, Alarm in, Virtual Trigger, Counter, Face Recognition, LPR
    - Select a related condition preset from the preset list menu
    - Set the Condition Trigger valid time between 1 to 20 seconds
        - Based on the Rule Trigger occurrence time set in the Trigger Set up step
        - + t seconds: true if condition occurs within t seconds of trigger
        - - t seconds: true if condition occurred t seconds before trigger
        - +/- t seconds: true if condition occurs t seconds before/after trigger
- Click 'Add' to add the condition to the schedule
- Repeat steps to add addition conditions to the schedule
- Select 'NEXT' to continue

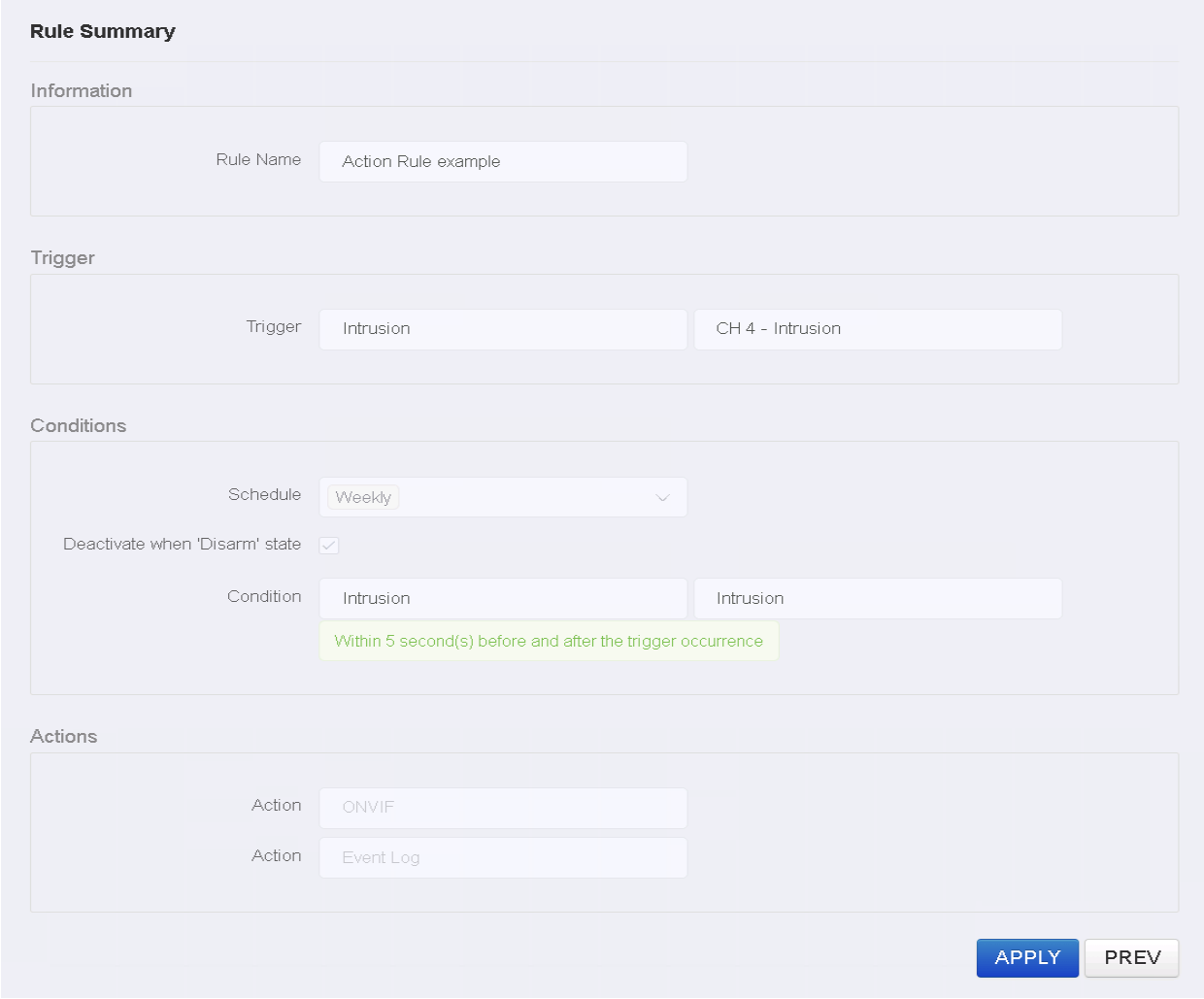


- Action: ONVIF
- Action: Event Log
- Add Actions: Select an action type from the list menu
    - List includes actions from the 'Event Action' menu
    - Select a related action preset from the preset list menu

- Click 'Add' to add the action to the action setup
- Repeat steps to add addition actions to the action setup
- Select 'NEXT' to continue



- Check the settings in Summary.
- Click the 'APPLY' button to create the rule.



3. AI Trigger

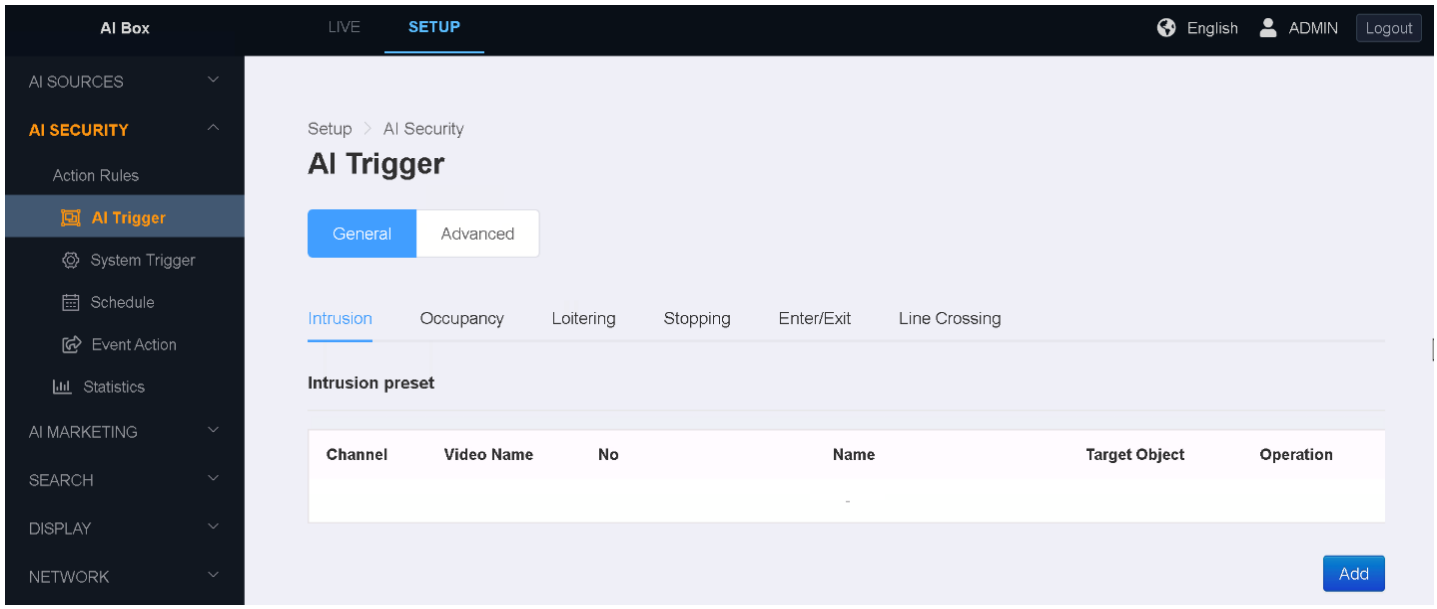
1. General: Intrusion Preset

Intrusion is a function that is triggered when a new target appears in the ROI (regent of interest) set in the prior AI Detector/Tracker menu.

To create an intrusion-based AI trigger, go to SETUP/AI Security/AI Trigger->Intrusion

- Select 'General' if not already selected
- Select 'Intrusion' if not already selected
- Click the 'Add' button at the bottom

[Caution] The determination of whether an object is inside an intrusion zone is based on the track reference point having been set to 'Centroid' for the AI detector in use.



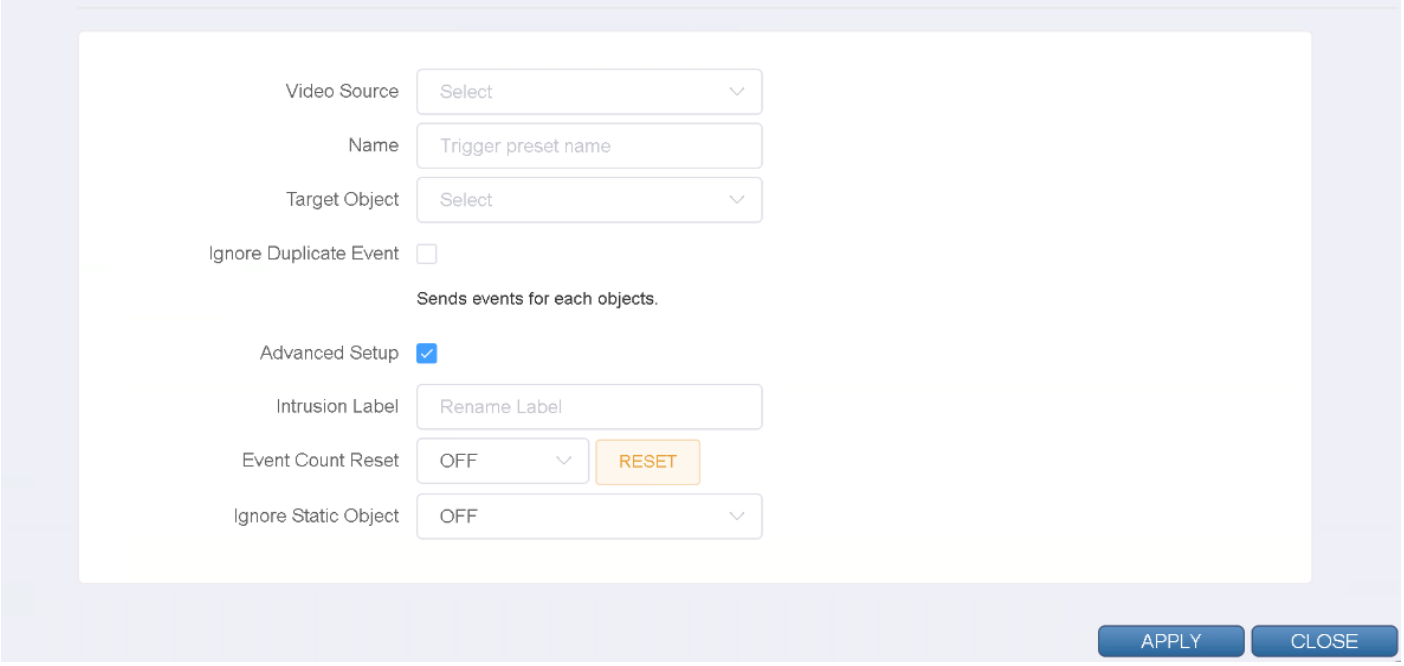
- Video Source: Select the AI Detector (Target 'Video Source')
- Name: Title the Intrusion preset according to intent
- Target Object: Based on the channel assigned analytic. Example: Person, Vehicle…
    - Objects may vary depending on the algorithm of the selected 'Video Source'.
    - It is possible to select multiple objects for detection.

- Ignore Duplicate Event: Selected a 1-, 5-, 15-, 30-, or 60-minute time threshold.
    - When enabled, only the first object that breaks into the zone will raise an event.
    - Before a new event occurs, the current event must clear

- Reminder Duration: Only available when Ignore Duplicate Event is activated
    - The event frequency setting reminds the user if the intrusion continues.

- Advanced Setup: Offers additional configuration options when selected
    - Intrusion Label: Label the Intrusion widget counter according to intent
    - Event Count Reset: Select the hour of time to reset the widget's counter
        - You can also reset manually by pressing the Reset button.

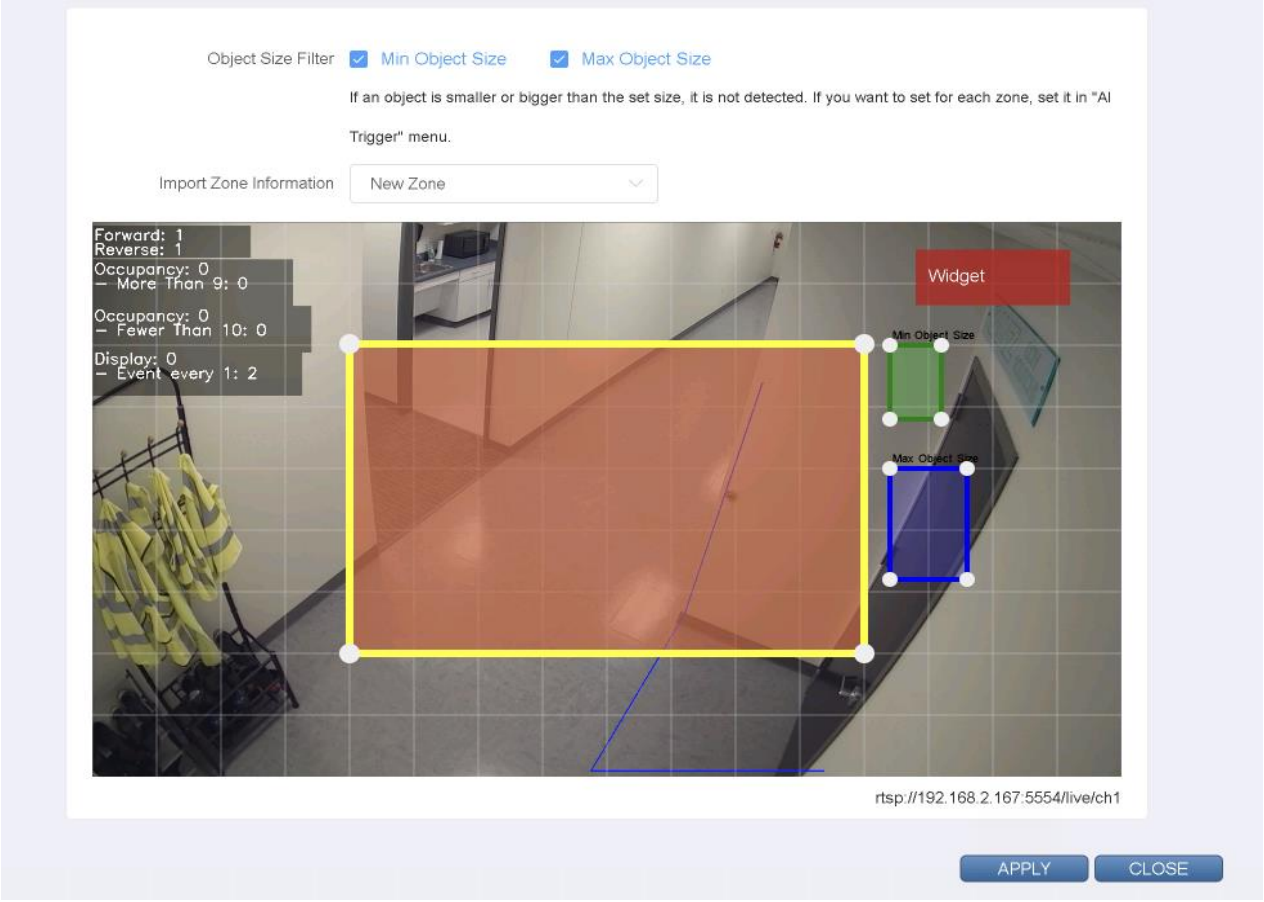
    - Ignore Static Object: Select 'On' or 'Off' based on stationary, or static object
        - Ignore objects that are not moving when enabled.
        - An event may occur if there is no movement and then movement again.



Set ROI (regent of interest) zone

- Object Size Filter: Set the 'Min Object Size', and or 'Max Object Size'
  - Drag object size zone to required dimensions
  - If an object is smaller or bigger than the set size, it is not detected.
  - If you want to set for each zone, set it in the "AI Trigger" menu.

- 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.
- Drag the Widget rectangle in the upper right corner to set where the widget will appear.
- Click the 'APPLY' button at the bottom to save.
- After confirming the settings, click the 'CLOSE' button at the bottom to check the list.



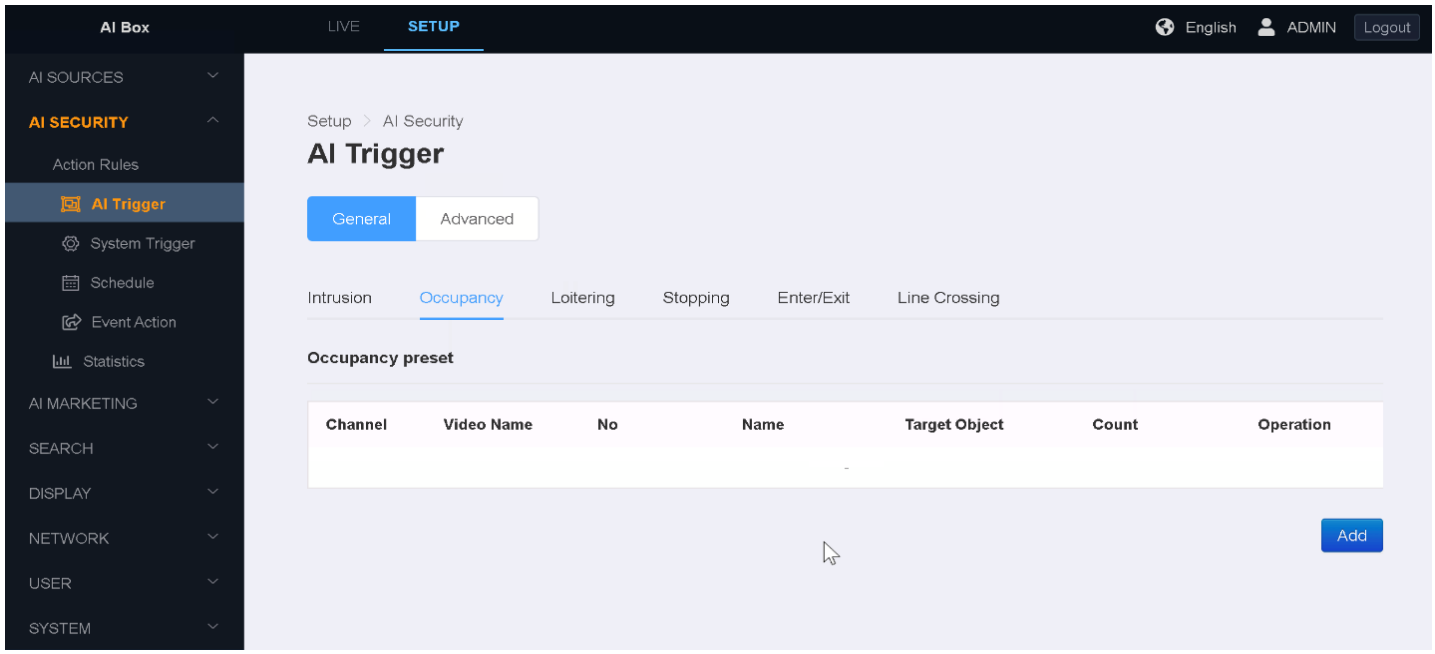
2. General: Occupancy Preset

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.

To create an occupancy-based AI trigger, go to SETUP/AI Security/AI Trigger->Occupancy

- Select 'General' if not already selected
- Select 'Occupancy' if not already selected
- Click the 'Add' button at the bottom

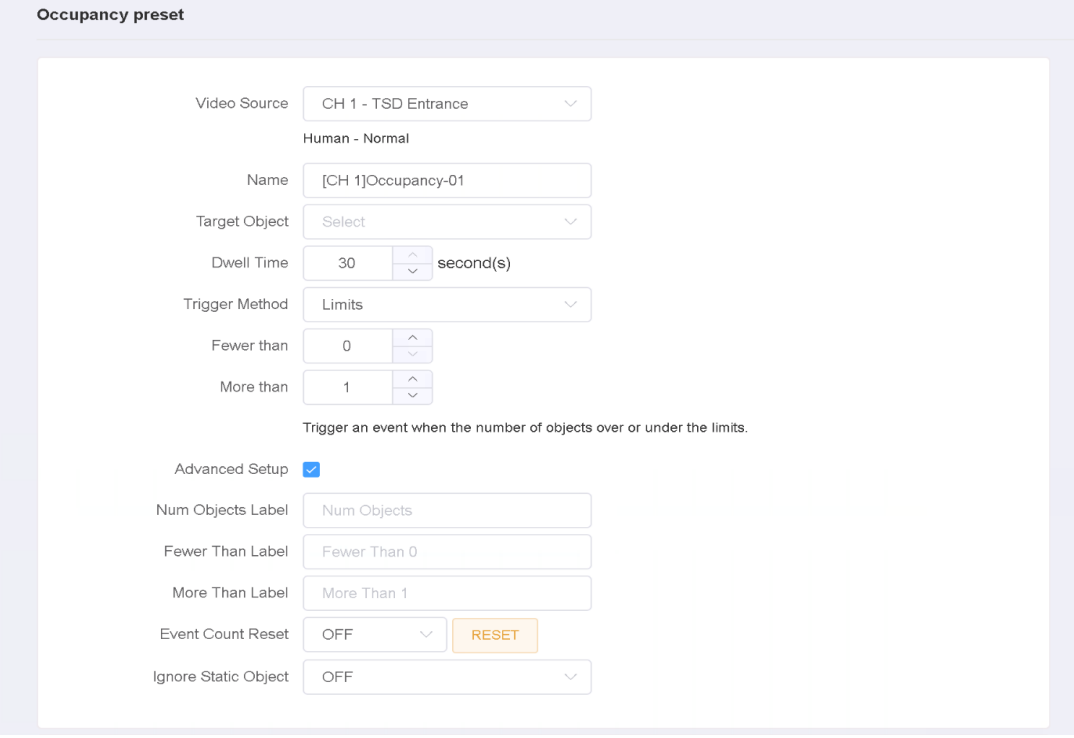
[Caution] The determination of whether an object is inside a section is based on the center coordinates of the object.



- Video Source: Select the AI Detector (Target 'Video Source')
- Name: Title the Intrusion preset according to intent
- Target Object: Based on the channel assigned analytic. Example: Person, Vehicle…
    - Objects may vary depending on the algorithm of the selected 'Video Source'.
    - It is possible to select multiple objects for detection.

- Dwell Time: Select 0 ~ 30 second(s) Triggered when target stays longer than set time.
- Trigger Method: Limits, Every N objects, Report Num Objects
- Fewer than: 0 ~ 99 Triggers if detected number of targets is less than the set number.
- More than: 0 ~ 99 Triggers if detected number of targets is more than the set number.
- Advanced Setup: Offers additional configuration options when selected
    - Num Objects Label: Label the Occupancy widget counter according to intent
    - Few Than Label: Label the Occupancy widget counter according to intent
    - More Than Label: Label the Occupancy widget counter according to intent
    - Event Count Reset: Select the hour of time to reset the widget's counter
        - You can also reset manually by pressing the Reset button.

    - Ignore Static Object: Select 'On' or 'Off' based on stationary, or static object
        - Ignore objects that are not moving when enabled.
        - An event may occur if there is no movement and then movement again.

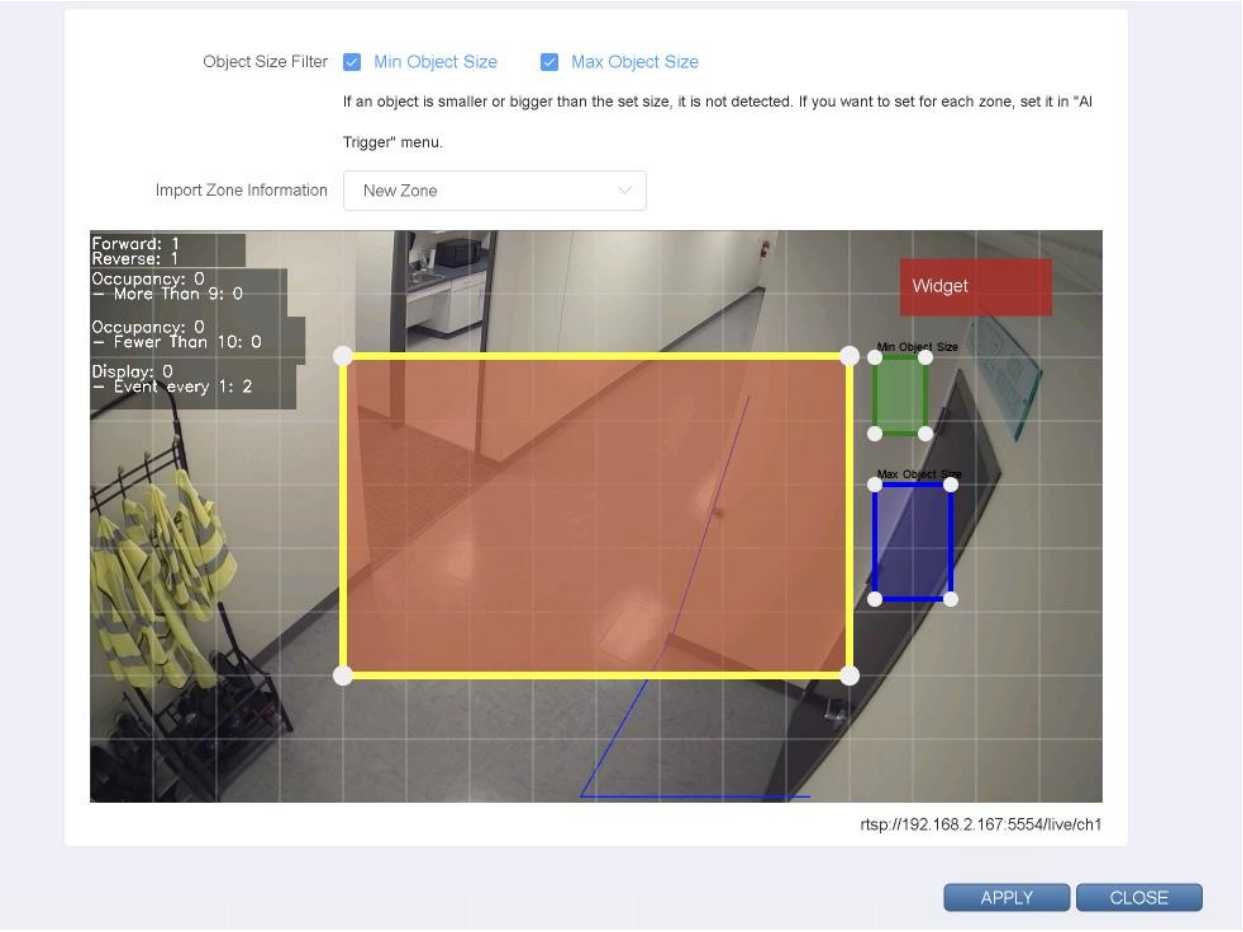


Set ROI (regent of interest) zone

- Object Size Filter: Set the 'Min Object Size', and or 'Max Object Size'
  - Drag object size zone to required dimensions
  - If an object is smaller or bigger than the set size, it is not detected.
  - If you want to set for each zone, set it in the "AI Trigger" menu.

- 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.

- Drag the Widget rectangle in the upper right corner to set where the widget will appear.
- Click the 'APPLY' button at the bottom to save.
- After confirming the settings, click the 'CLOSE' button at the bottom to check the list.



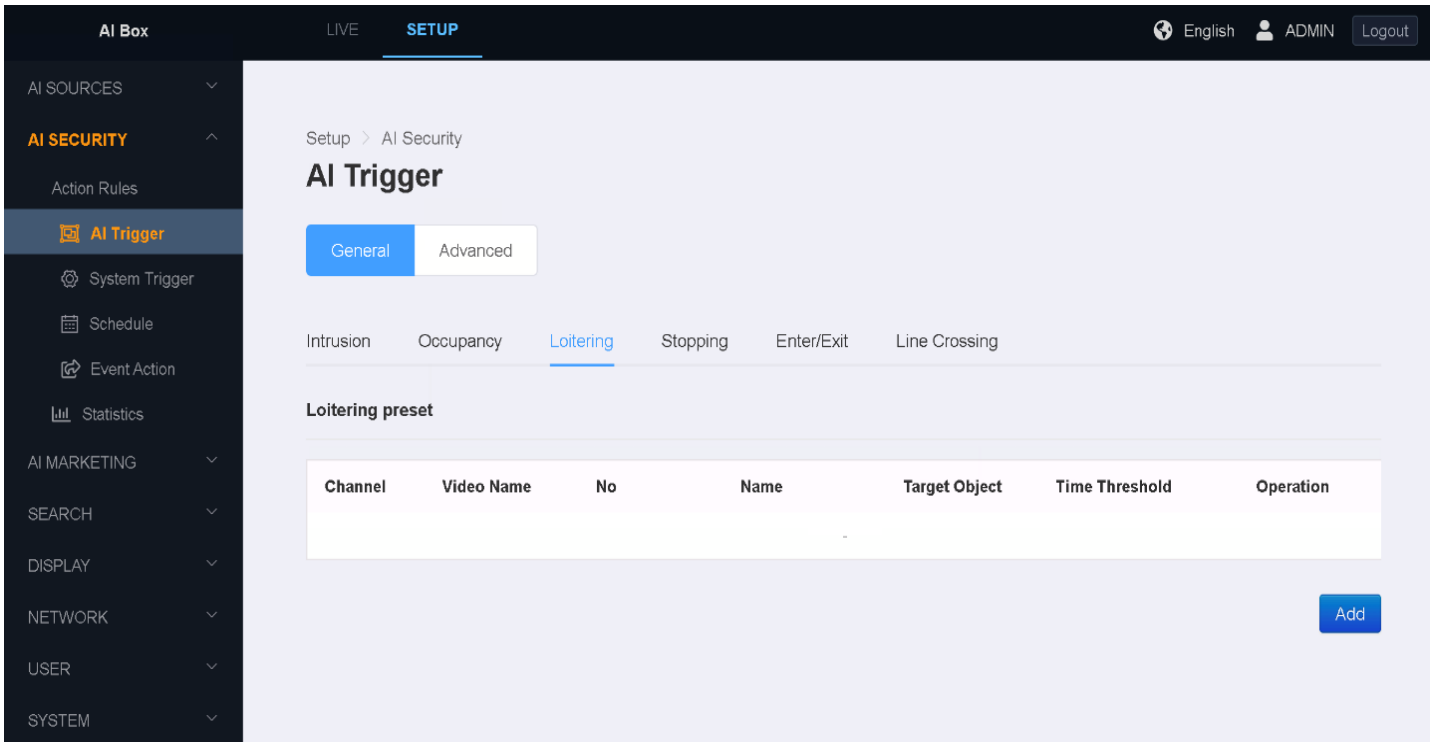
3. General: Loitering Preset

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.

To create a loitering-based AI trigger, go to SETUP/AI Security/AI Trigger->Loitering

- Select 'General' if not already selected
- Select 'Loitering' if not already selected
- Click the 'Add' button at the bottom

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



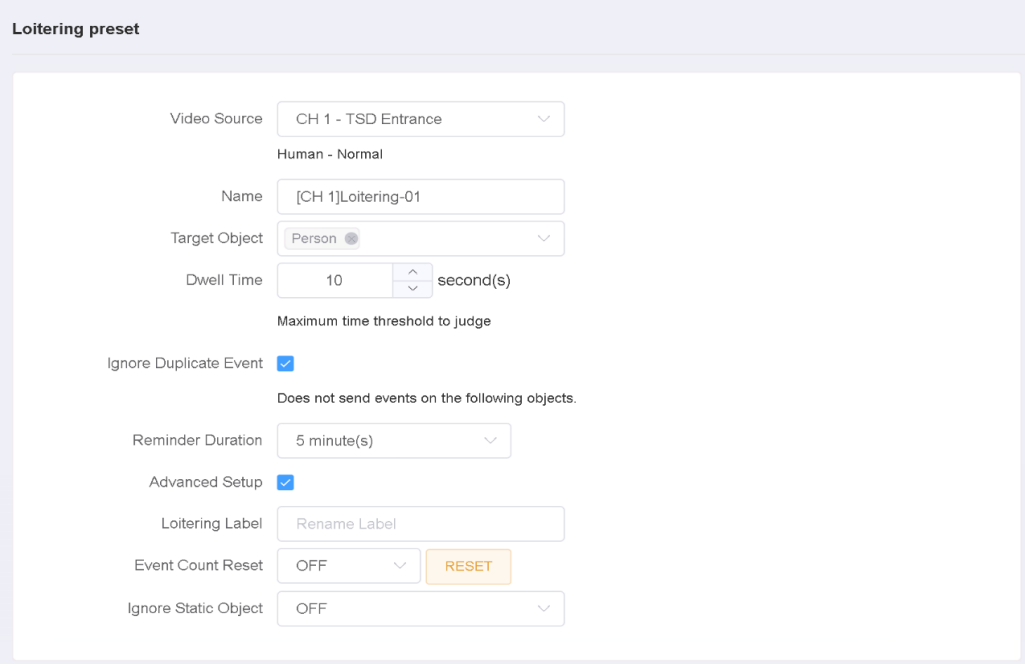
- Video Source: Select the AI Detector (Target 'Video Source')
- Name: Title the Intrusion preset according to intent
- Target Object: Based on the channel assigned analytic. Example: Person, Vehicle…
    - Objects may vary depending on the algorithm of the selected 'Video Source'.
    - It is possible to select multiple objects for detection.

- Dwell Time: Select 0 ~ 30 second(s) Triggered when target stays longer than set time.
- Ignore Duplicate Event: Selected a 1-, 5-, 15-, 30-, or 60-minute time threshold.
    - When enabled, only the first object that breaks into the zone will raise an event.
    - Before a new event occurs, the current event must clear

- Reminder Duration: Only available when Ignore Duplicate Event is activated
    - The event frequency setting reminds the user if the intrusion continues.

- Advanced Setup: Offers additional configuration options when selected
    - Loitering Label: Label the loitering widget counter according to intent
    - Event Count Reset: Select the hour of time to reset the widget's counter
        - You can also reset manually by pressing the Reset button.

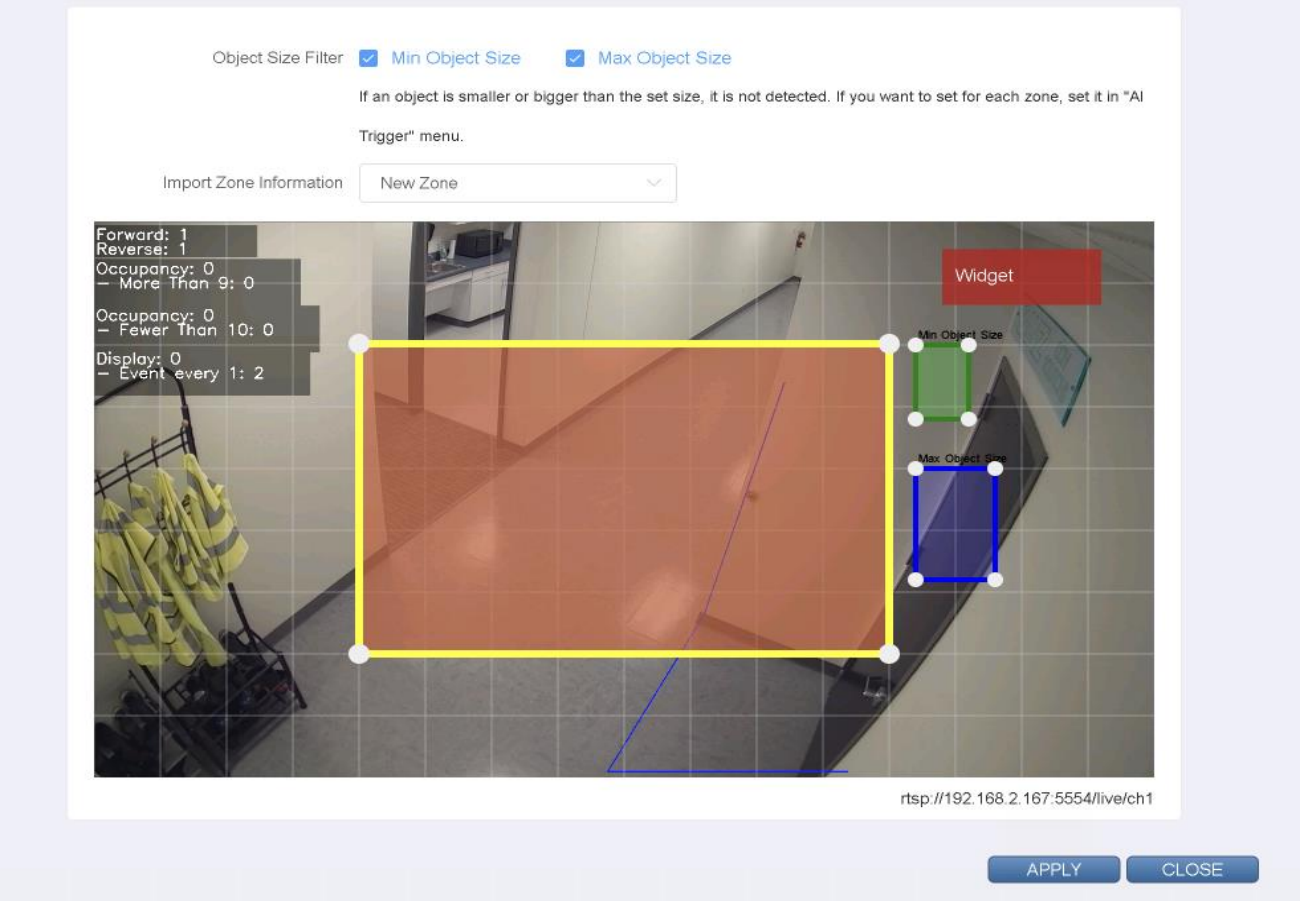
    - Ignore Static Object: Select 'On' or 'Off' based on stationary, or static object
        - Ignore objects that are not moving when enabled.
        - An event may occur if there is no movement and then movement again.



Set ROI (regent of interest) zone

- Object Size Filter: Set the 'Min Object Size', and or 'Max Object Size'
  - Drag object size zone to required dimensions
  - If an object is smaller or bigger than the set size, it is not detected.
  - If you want to set for each zone, set it in the "AI Trigger" menu.

- 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.
- Drag the Widget rectangle in the upper right corner to set where the widget will appear.
- Click the 'APPLY' button at the bottom to save.
- After confirming the settings, click the 'CLOSE' button at the bottom to check the list.



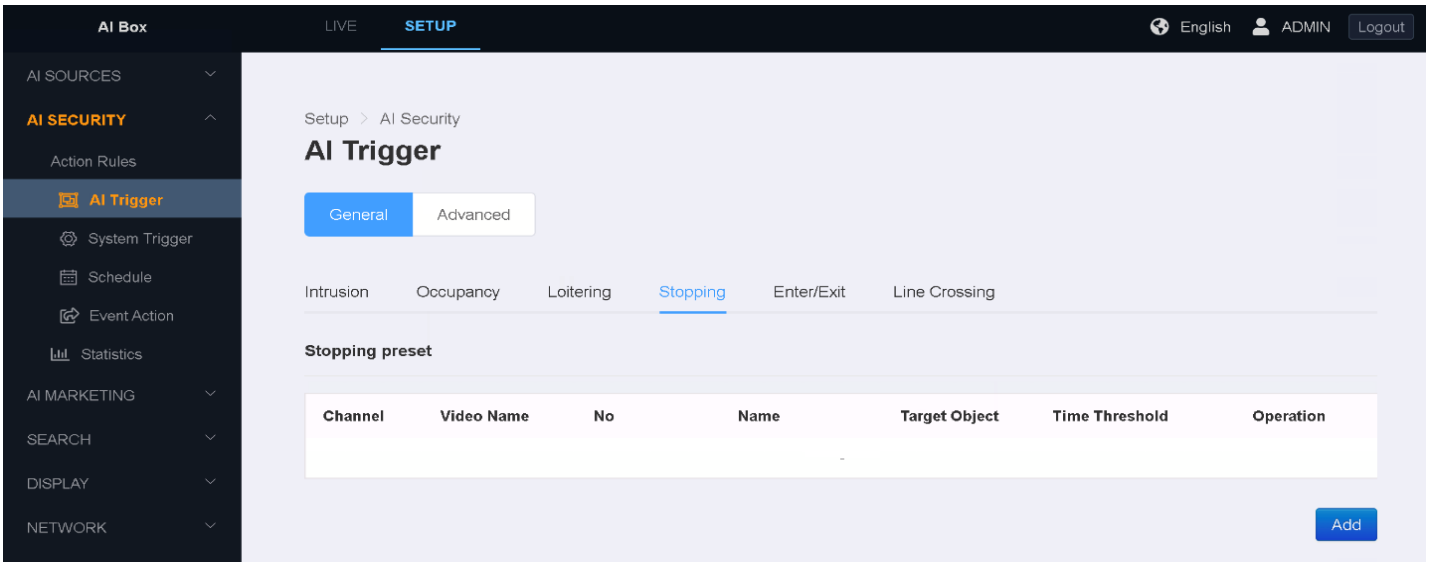
4. General: Stopping Preset

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.

To create a stopping-based AI trigger, go to SETUP/AI Security/AI Trigger->Stopping

- Select 'General' if not already selected
- Select 'Stopping' if not already selected
- Click the 'Add' button at the bottom

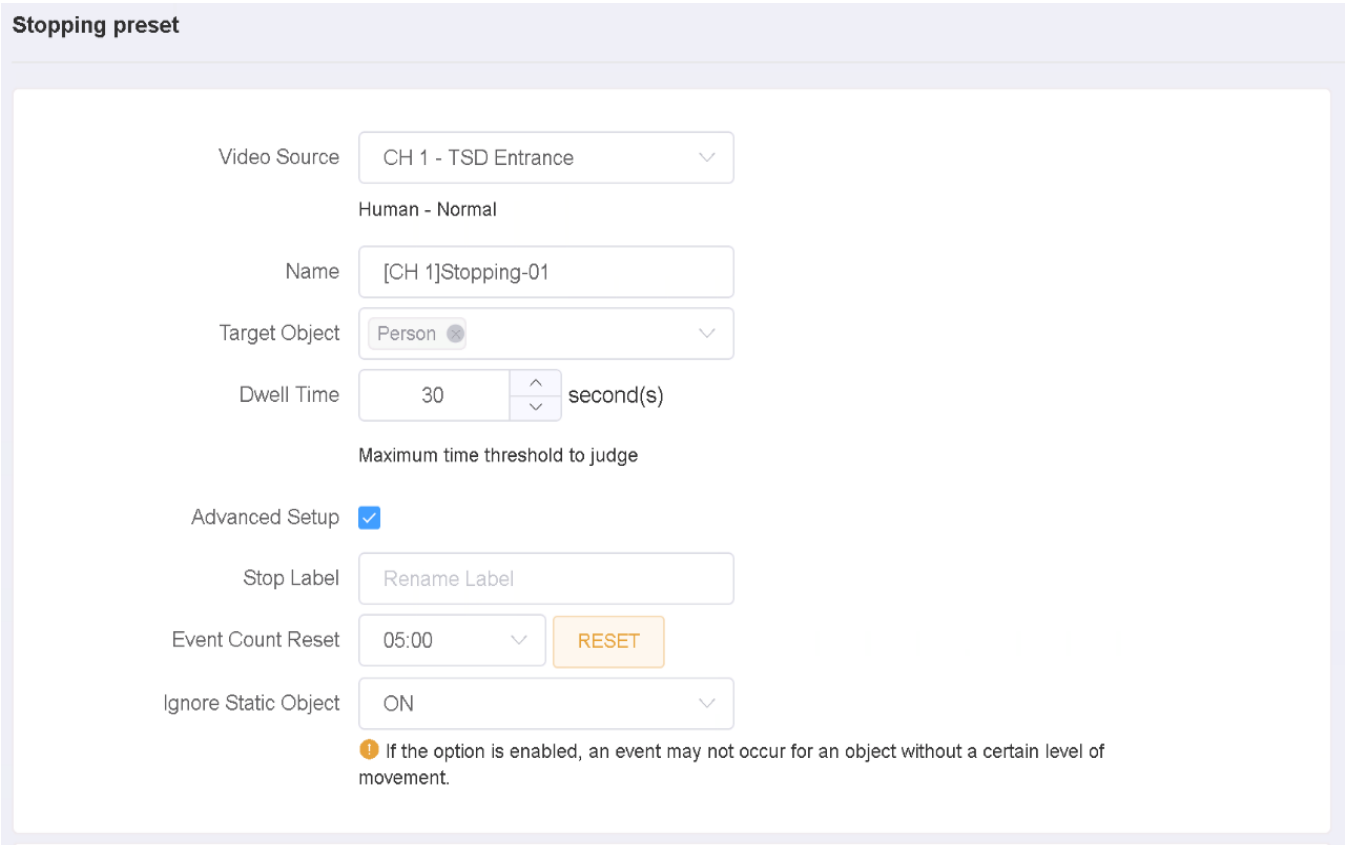
[Caution] The determination of whether an object is inside a section is based on the center coordinates of the object.



- Video Source: Select the AI Detector (Target 'Video Source')
- Name: Title the Intrusion preset according to intent
- Target Object: Based on the channel assigned analytic. Example: Person, Vehicle…
    - Objects may vary depending on the algorithm of the selected 'Video Source'.
    - It is possible to select multiple objects for detection.

- Dwell Time: Select 0 ~ 30 second(s) Triggered when target stays longer than set time.
- Advanced Setup: Offers additional configuration options when selected
    - Stop Label: Label the Stop widget counter according to intent
    - Event Count Reset: Select the hour of time to reset the widget's counter
        - You can also reset manually by pressing the Reset button.

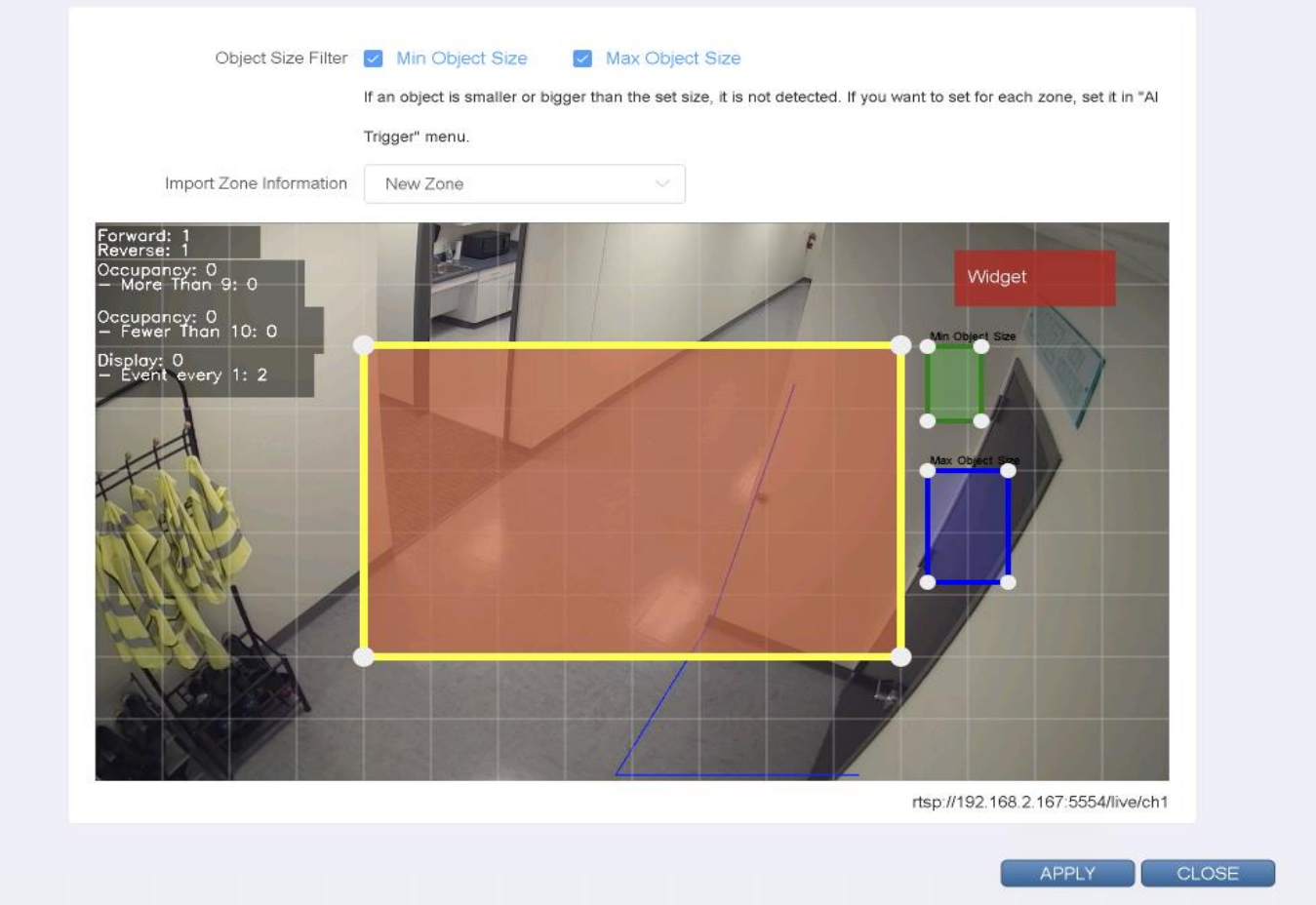
    - Ignore Static Object: Select 'On' or 'Off' based on stationary, or static object
        - Ignore objects that are not moving when enabled.
        - An event may occur if there is no movement and then movement again



Set ROI (regent of interest) zone

- Object Size Filter: Set the 'Min Object Size', and or 'Max Object Size'
  - Drag object size zone to required dimensions
  - If an object is smaller or bigger than the set size, it is not detected.
  - If you want to set for each zone, set it in the "AI Trigger" menu.

- 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.
- Drag the Widget rectangle in the upper right corner to set where the widget will appear.
- Click the 'APPLY' button at the bottom to save.
- After confirming the settings, click the 'CLOSE' button at the bottom to check the list.



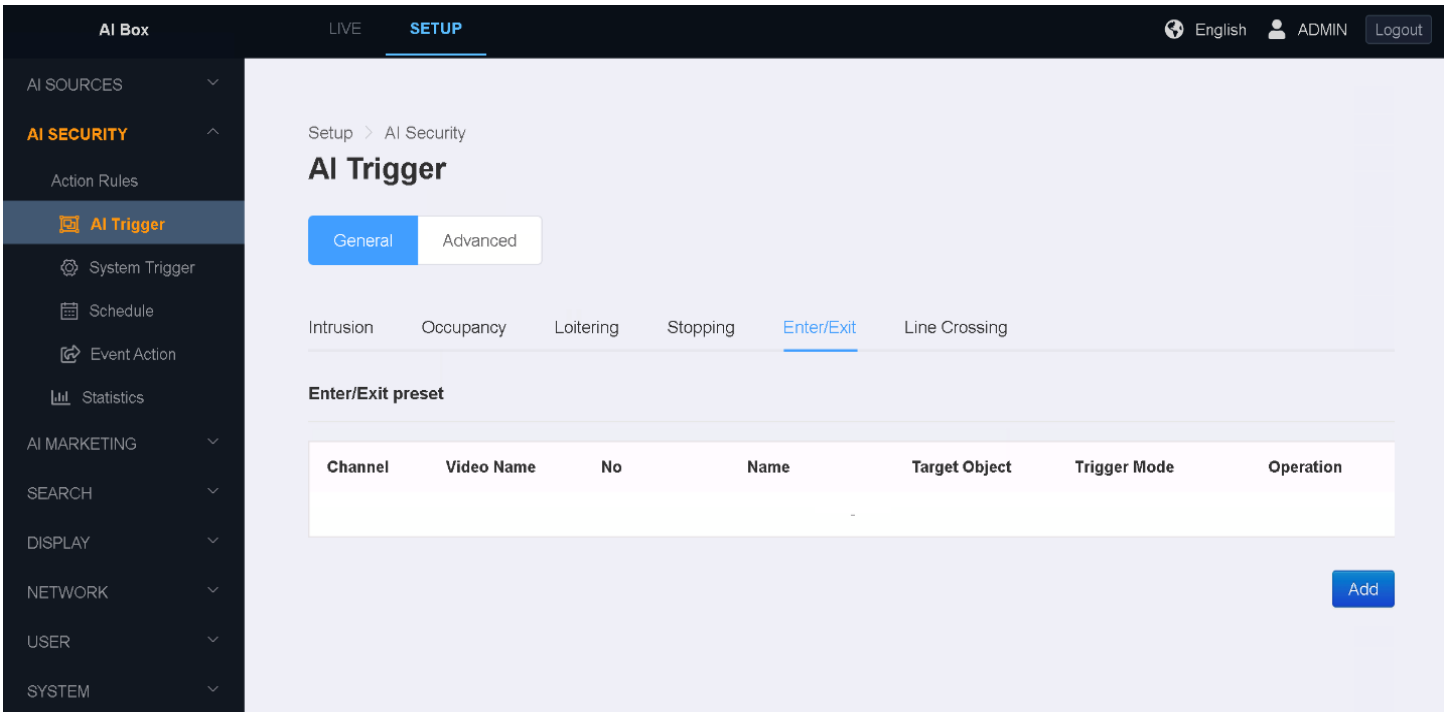
5. General: Enter/Exit Preset

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.

To create an enter/exit-based AI trigger, go to SETUP/AI Security/AI Trigger->Enter/Exit

- Select 'General' if not already selected
- Select 'Enter/Exit' if not already selected
- Click the 'Add' button at the bottom

[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.

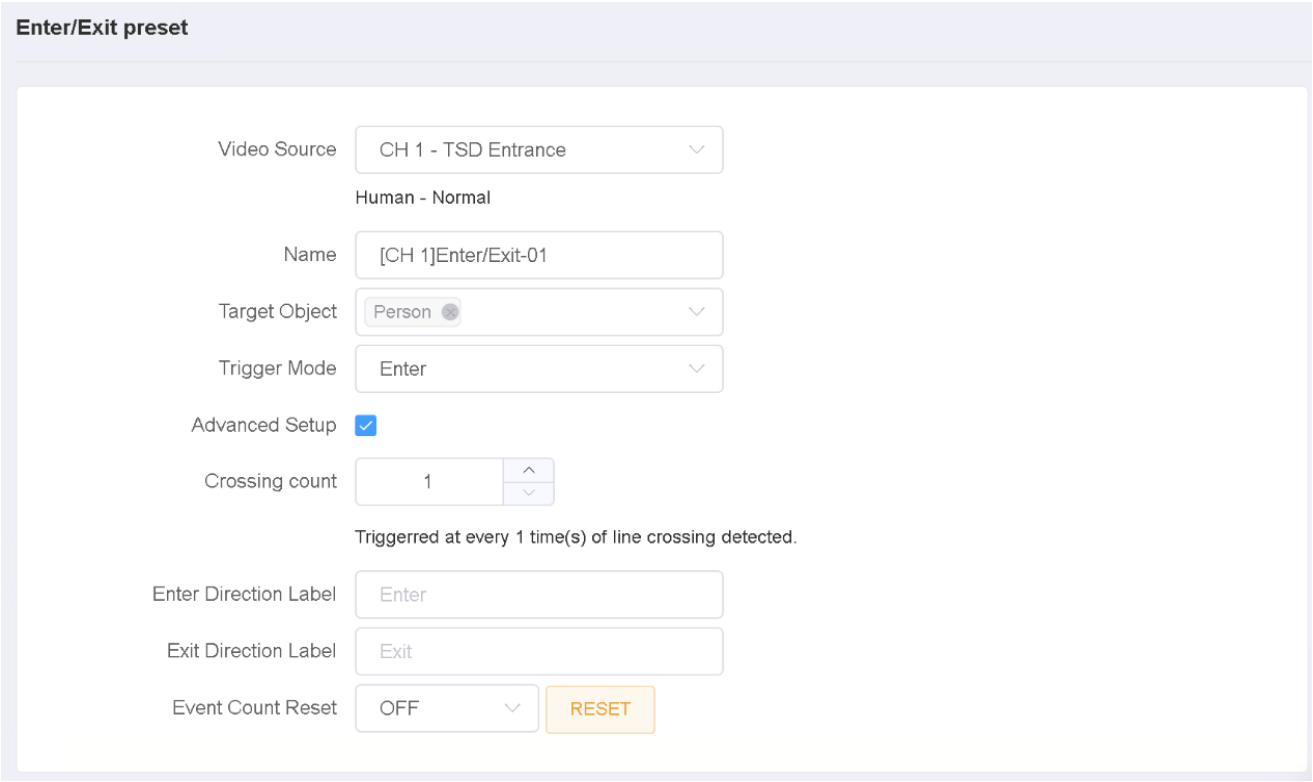


- Video Source: Select the AI Detector (Target 'Video Source')
- Name: Title the Intrusion preset according to intent
- Target Object: Based on the channel assigned analytic. Example: Person, Vehicle…
    - Objects may vary depending on the algorithm of the selected 'Video Source'.
    - It is possible to select multiple objects for detection.

- Trigger Mode: Enter, Exit, Enter or Exit, Stay & Go
    - Detect the target enters the zone.
    - Detect the target exits the zone.
    - Detects the target entering or leaving the zone.

- Advanced Setup: Offers additional configuration options when selected
    - Crossing count: Sets how many times an event will occur when an object crossing the area boundary is detected.

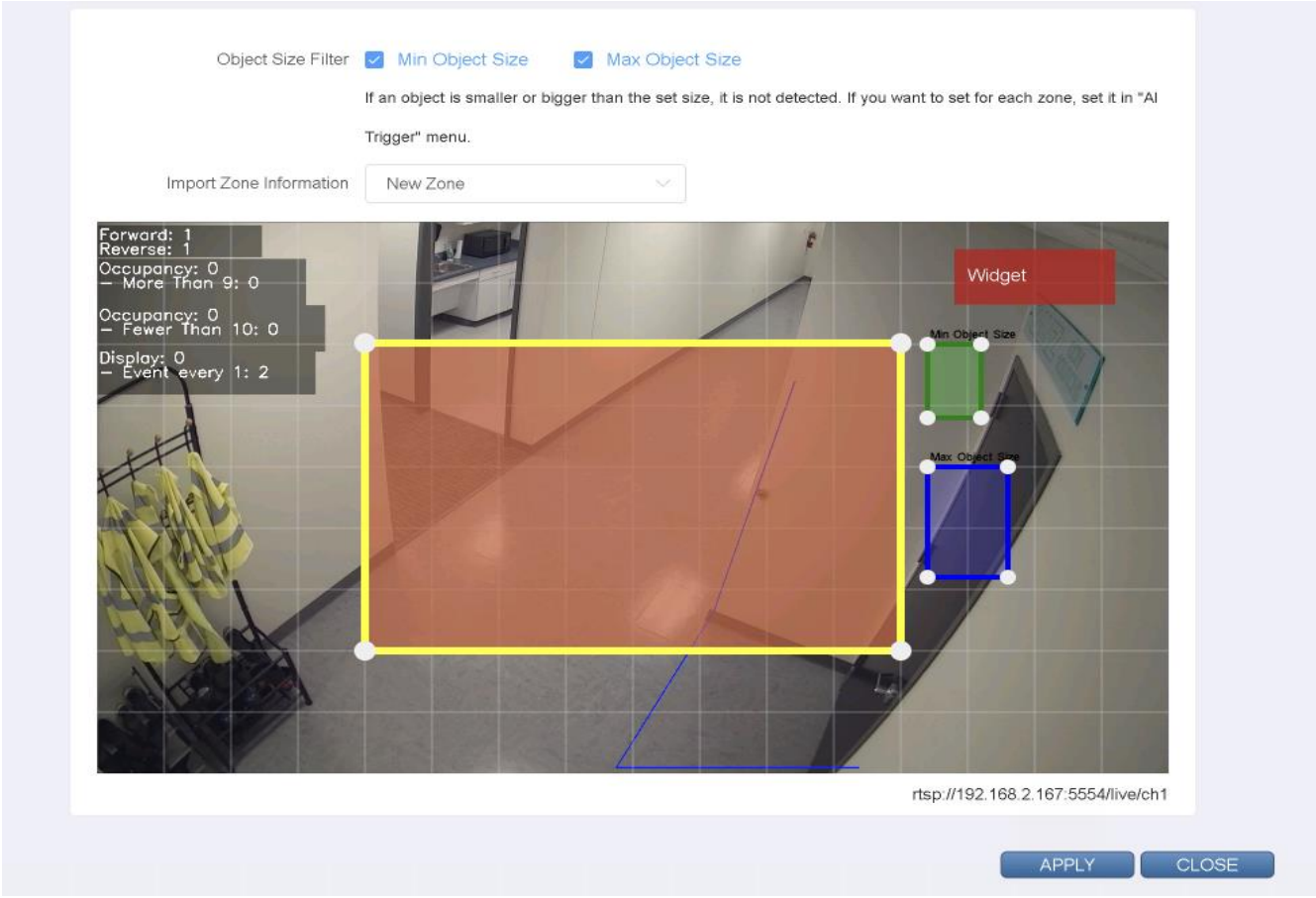
    - Enter Direction Label: Label the Enter widget counter according to intent
    - Exit Direction Label: Label the Exit widget counter according to intent
    - Event Count Reset: Select the hour of time to reset the widget's counter
        - You can also reset manually by pressing the Reset button.



Set ROI (regent of interest) zone

- Object Size Filter: Set the 'Min Object Size', and or 'Max Object Size'
  - Drag object size zone to required dimensions
  - If an object is smaller or bigger than the set size, it is not detected.
  - If you want to set for each zone, set it in the "AI Trigger" menu.

- 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.
- Drag the Widget rectangle in the upper right corner to set where the widget will appear.
- Click the 'APPLY' button at the bottom to save.
- After confirming the settings, click the 'CLOSE' button at the bottom to check the list.



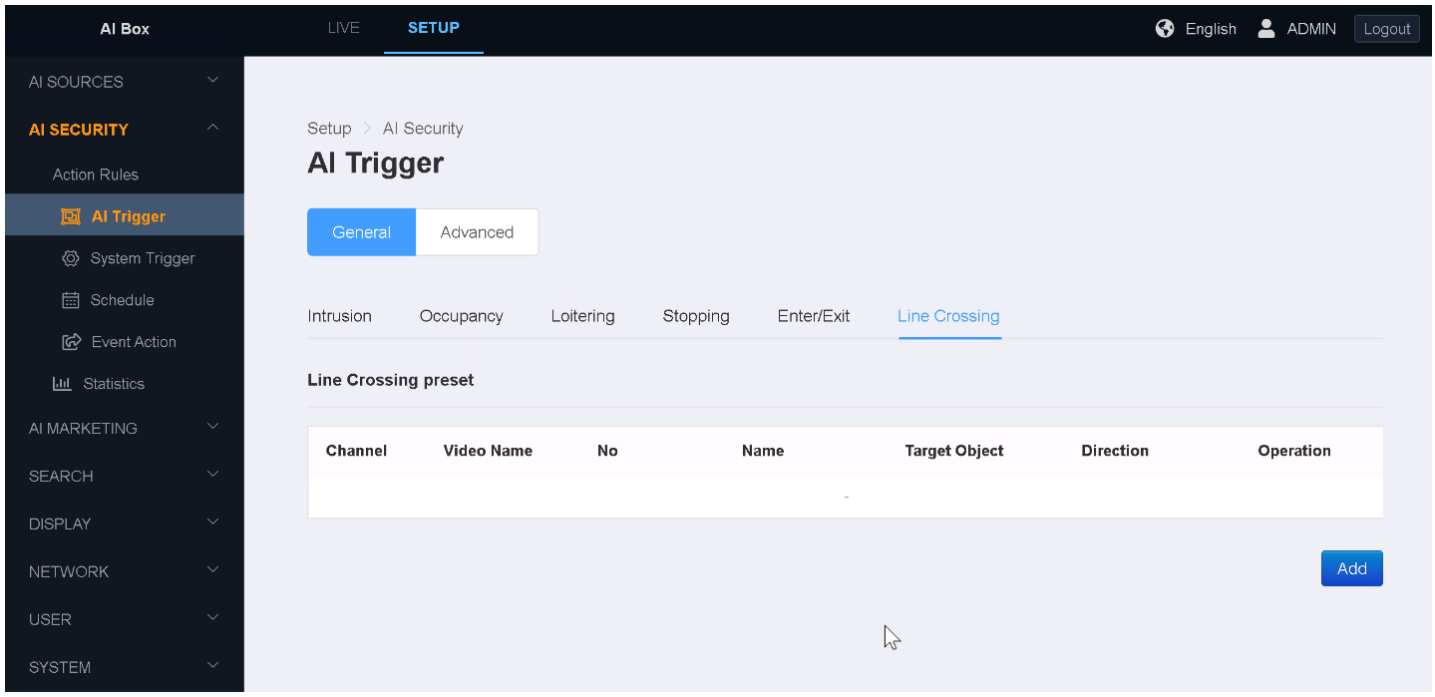
6. General: Line Crossing Preset

Line Crossing is a function set polyline on the screen, and it triggered when the detected object crosses the line.

To create a line crossing-based AI trigger, go to SETUP/AI Security/AI Trigger->Line Crossing

- Select 'General' if not already selected
- Select 'Line Crossing' if not already selected
- Click the 'Add' button at the bottom

[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 SETUP/DISPLAY-> OSD item.

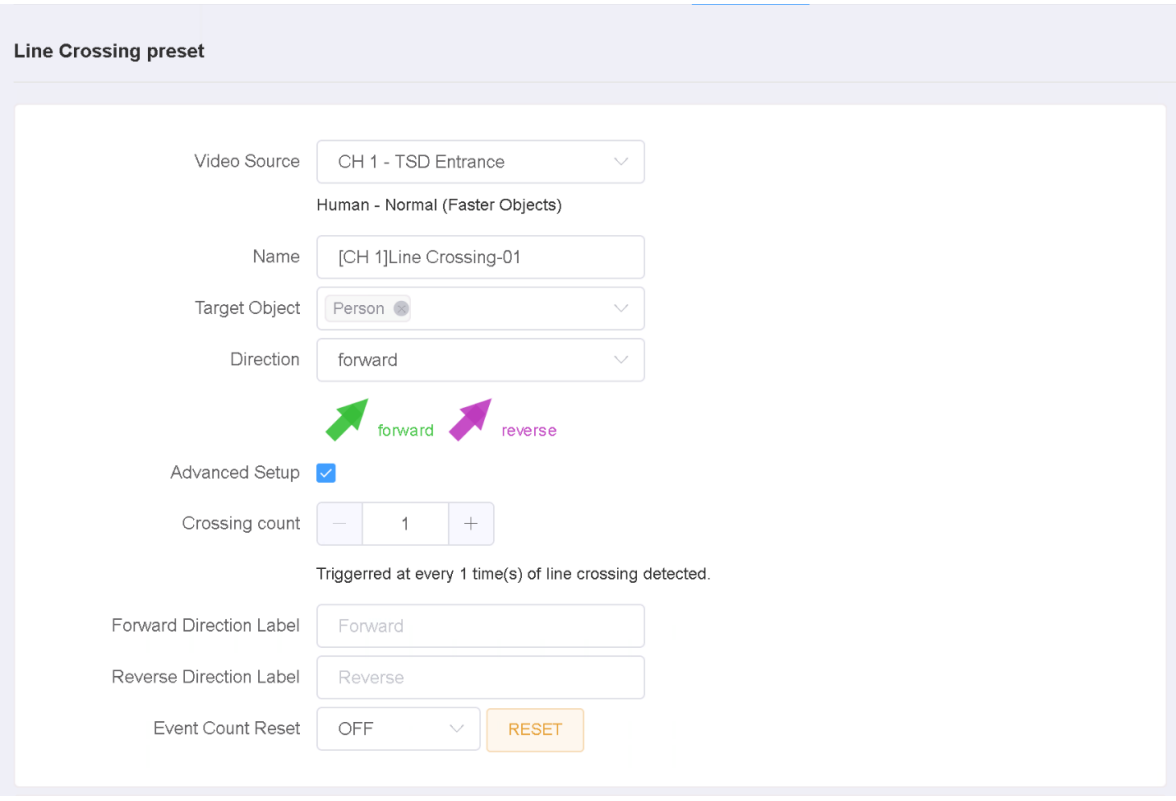


- Video Source: Select the AI Detector (Target 'Video Source')
- Name: Title the Intrusion preset according to intent
- Target Object: Based on the channel assigned analytic. Example: Person, Vehicle…
    - Objects may vary depending on the algorithm of the selected 'Video Source'
    - It is possible to select multiple objects for detection

- Direction: Forward, Reverse, or Both
    - Forward: Determined by the direction of the green arrow
    - Reverse: Determined by the direction of the purple arrow
    - Both: Determined by the direction of both arrows

- Advanced Setup: Offers additional configuration options when selected
    - Crossing count: Sets how many times an event will occur when an object crossing the area boundary is detected

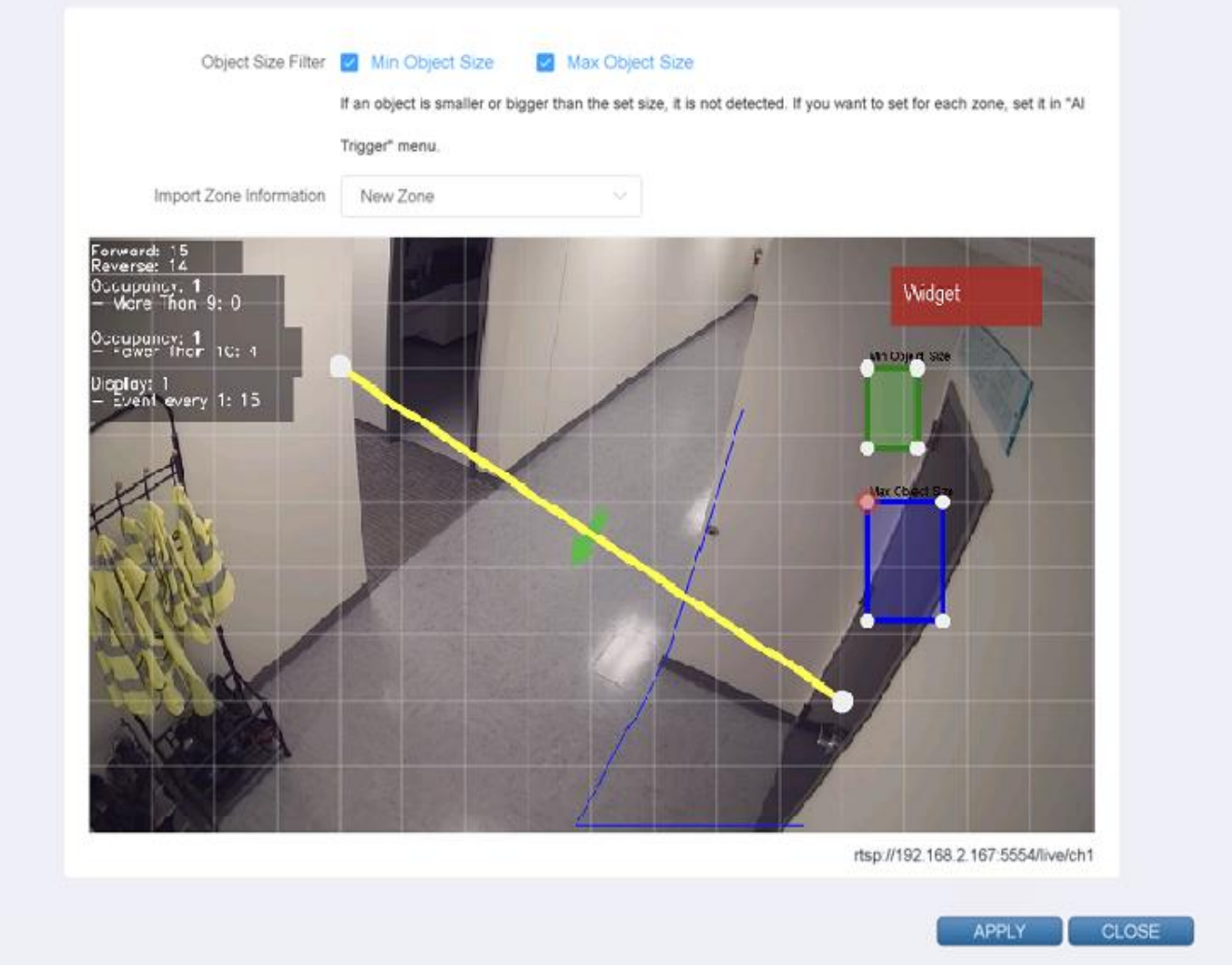
    - Forward Direction Label: Label the Forward widget counter according to intent
    - Reverse Direction Label: Label the Reverse widget counter according to intent
    - Event Count Reset: Select the hour of time to reset the widget's counter
        - You can also reset manually by pressing the Reset button



Set the 'Polyline'

- Object Size Filter: Set the 'Min Object Size', and or 'Max Object Size'
  - Drag object size zone to required dimensions
  - If an object is smaller or bigger than the set size, it is not detected.
  - If you want to set for each zone, set it in the "AI Trigger" menu.

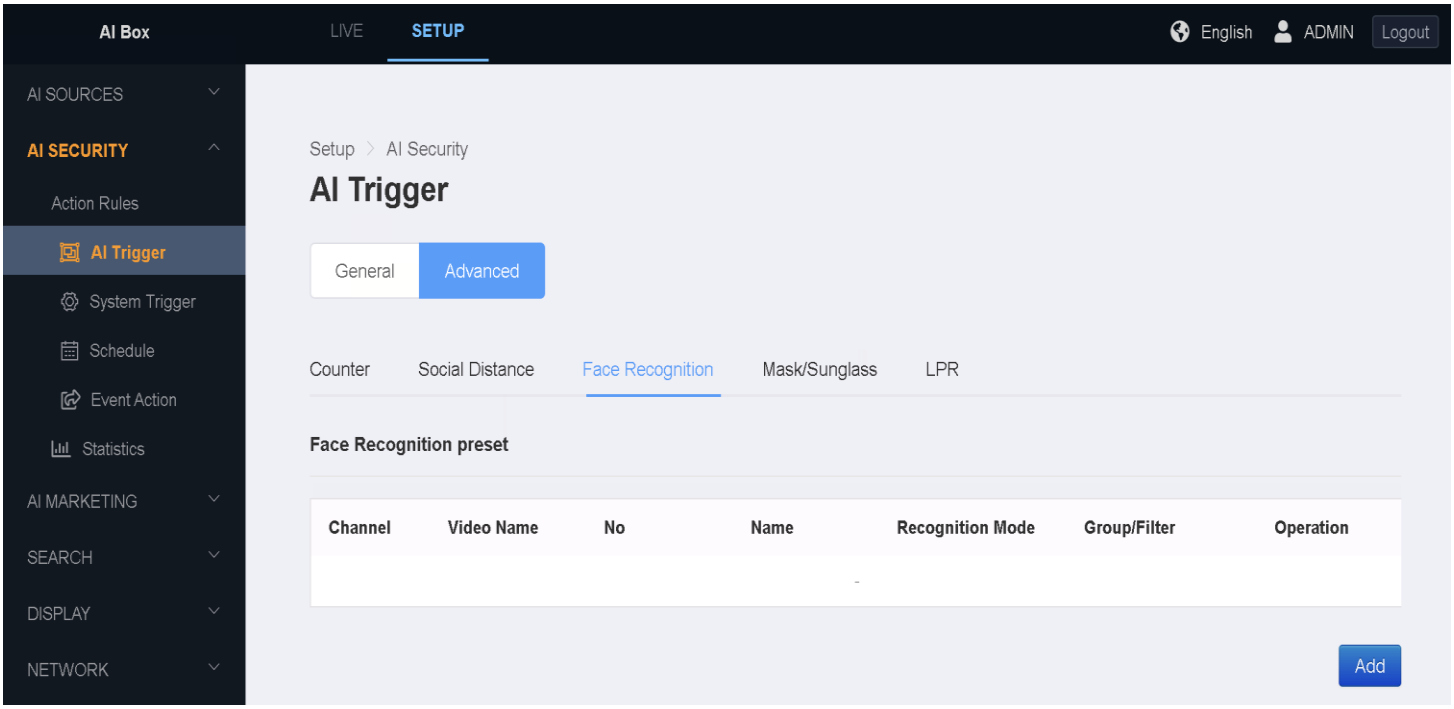
- Move the edge by dragging the edge of the 'Polyline'.
- Click on the line of the 'Polyline' to create a new edge.
- Right click the edge of 'Polyline' to delete the edge.
- Drag the Widget rectangle in the upper right corner to set where the widget will appear.
- Click the 'APPLY' button at the bottom to save.
- After confirming the settings, click the 'CLOSE' button at the bottom to check the list.



7. Advanced: Face Recognition

Face Recognition is an AI source function set under SETUP/AI SOURCES/Face Recognition and is triggered when a face is detected within a target video source.

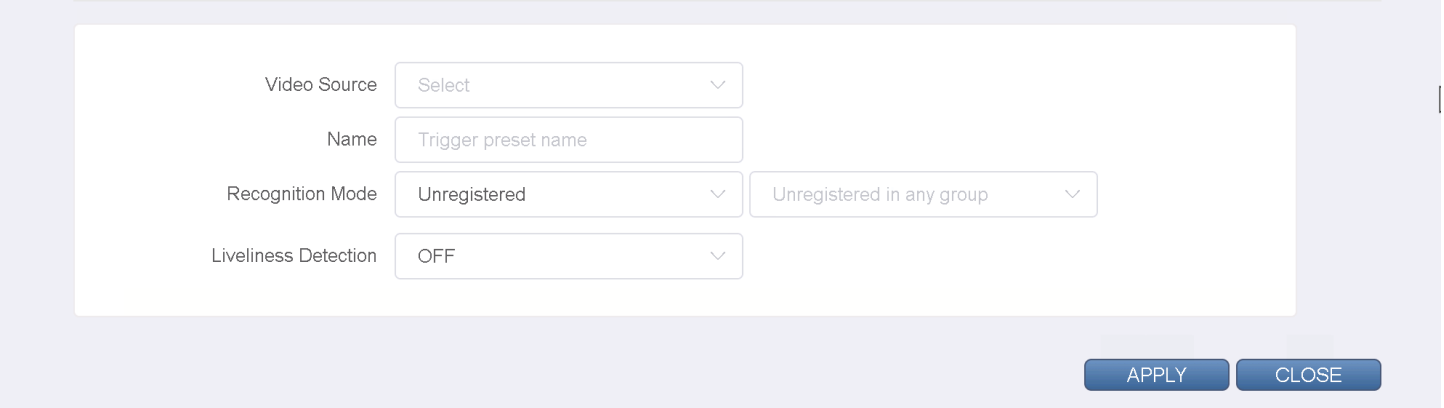
- Click the 'Add' button at the bottom to create a face recognition trigger



- Video Source: Select the Video source from the available listed video channels
- Name: Title the trigger name according to intent
- Recognition mode: Select 'Unregistered', 'Comparison', or 'Facial Attribute Filtering'
    - Unregistered: triggers people who do not belong to any group
        - Liveliness Detection: Determines if live or image, set to 'Off' or 'On'
            - If 'On': set 'Liveliness Threshold' 1 ~ 99
    - Comparison: Compare people registered in the selected group
        - Min Similarity: Set minimum similarity between person and image, 1 ~ 99
        - Liveliness Detection: Determines if live or image, set to 'Off' or 'On'
            - If 'On': set 'Liveliness Threshold' 1 ~ 99

- Face Attribute Filtering: Filter by age and gender
  - Age: 0 ~ 100
  - Gender: All, Male, or Female

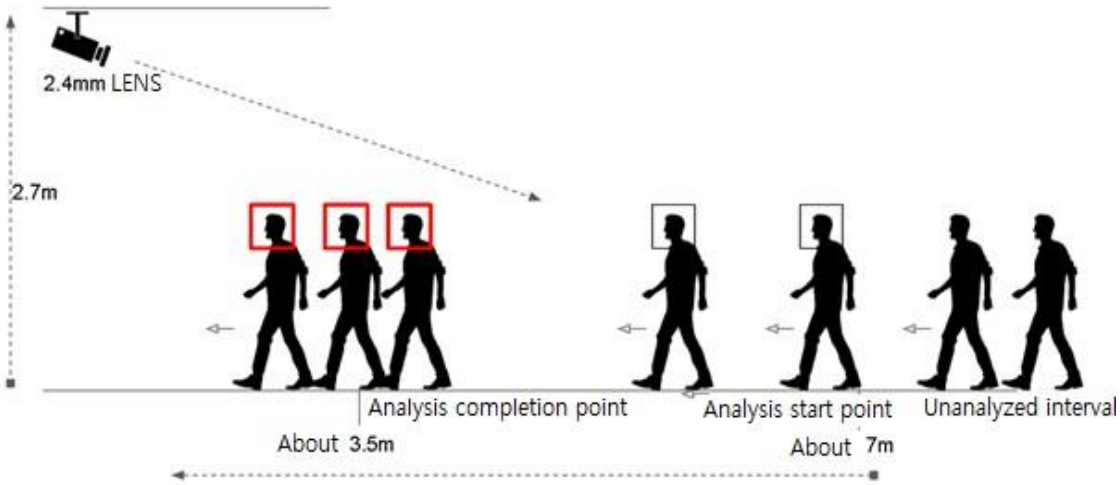
- Click the 'Apply' button at the bottom to save and continue



Face Recognition: Installing a camera

- Install: Install to a location in front of the person's travelling direction
- Angles - Left and Right: The angles at which a camera faces are around 30 degrees
- Horizontal: Install the camera at an angle of 15 degrees to the human face

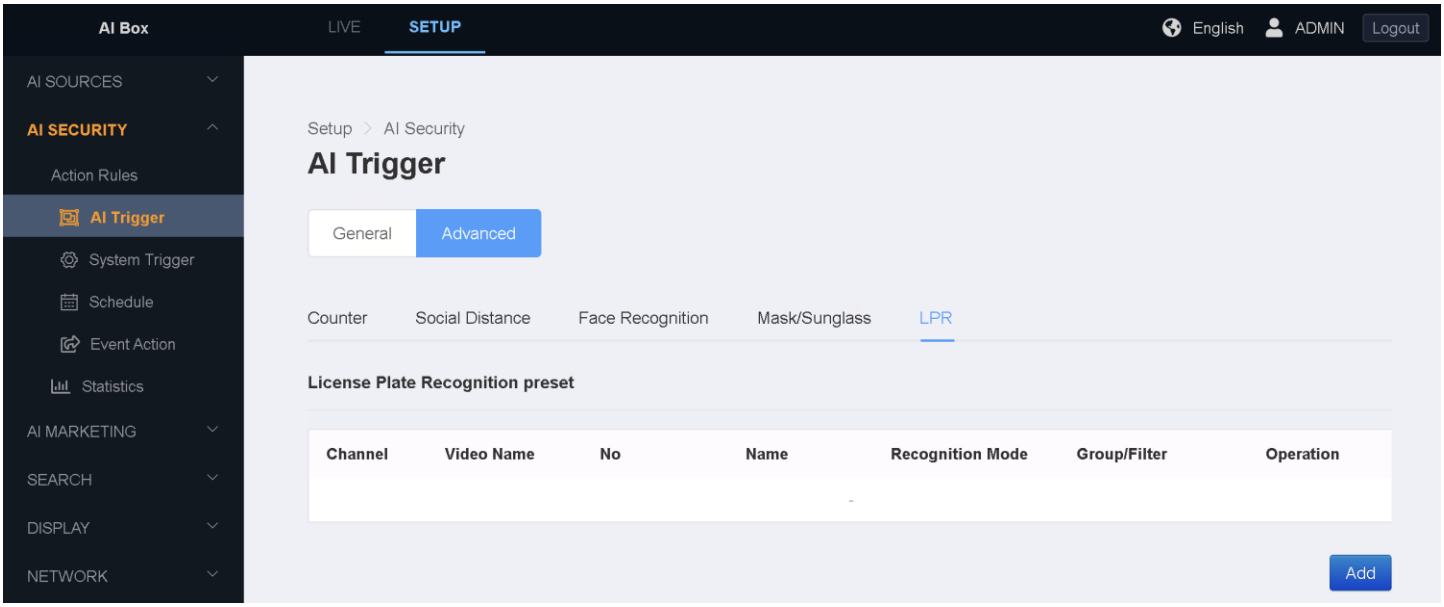
Example: Camera installation to increase accuracy
Increase the accuracy by adding, or confirming about 4 seconds from the start, and end of the analysis
The lower the camera height, being closer to the height of the person, the higher the accuracy



8. Advanced: LPR

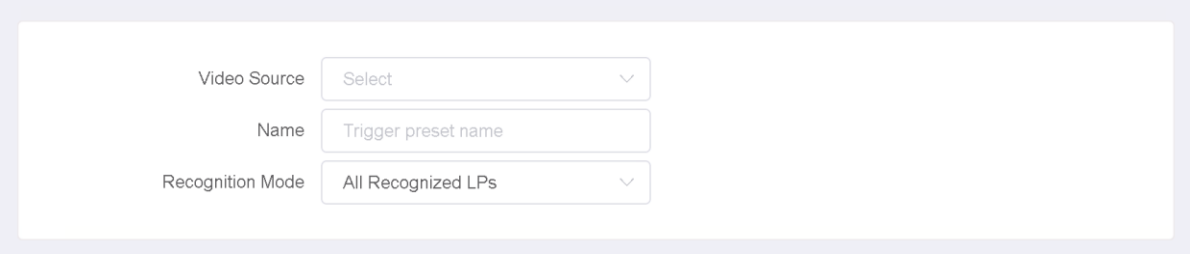
License plate recognition is an AI source function set under SETUP/AI SOURCES/LPR and is triggered when a license plate is detected within a target video source.

- Click the 'Add' button at the bottom to create a license plate recognition trigger

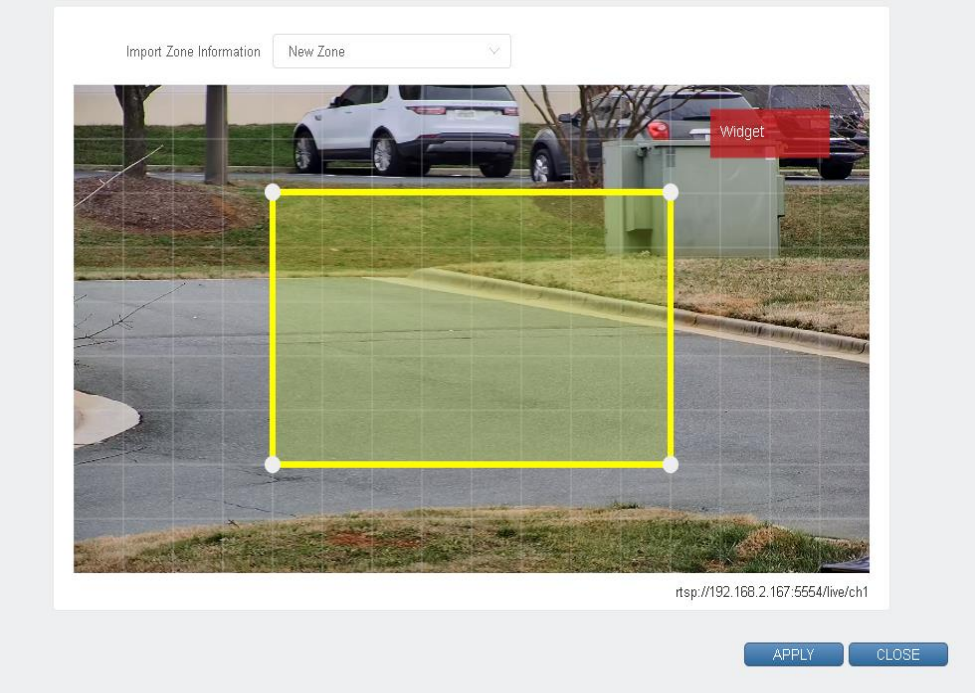


- Video Source: Select the Video source from the available listed video channels
- Name: Title the trigger name according to intent
- Recognition mode: Select ‘All Recognized LPs’, ‘LPs in Groups’, or ‘Unregistered LP’
    - All Recognized LPs: Triggers on recognized LPs only
    - LPs in Groups: Triggers on recognized LPs in LP groups only
        - Group: Select from available ‘Group’, or ‘Groups’
        - Matching Policy: Select from ‘Very High’, ‘High’, or ‘Normal’
            - LP characters match threshold setting

    - Unregistered LP: Triggers on unregistered LPs, not found in any LP group
        - Group: Select from available ‘Group’, or ‘Groups’



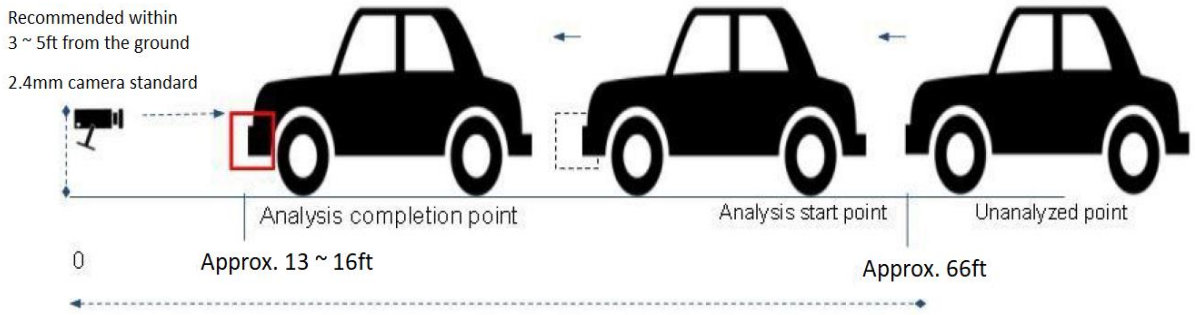
- Area Box: Drag the points of the box to where the license plate is the largest
- Click the 'Apply' button at the bottom to save and continue



LPR: Installing a camera

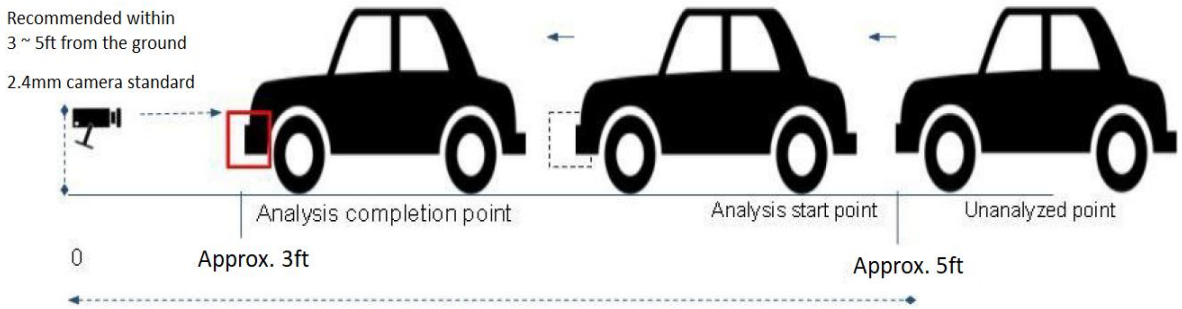
Example: Improving accuracy when installing a license plate recognition camera

- Install: Accuracy high if installed at location in front of vehicle, roughly level with license plate, based on a 10.3mm lens
- Fast Vehicle Speed: Camera and lens selected according to expected vehicle speeds, less than 37mph
- Analysis of LPR process
    - Analysis completions point: About 13~16ft
    - Analysis start point: About 13~16ft ~ about 66ft
    - Unanalyzed interval: Beyond 66ft



Example: Improving accuracy when installing a license plate recognition camera

- Install: Accuracy high if install at location in front of the vehicle, roughly level with license plate, based on a 2.4mm lens
- Slow Vehicle Speed: Camera and lens selected according to expected vehicle speeds, less than 6mph
- Analysis of LPR process
    - Analysis completions point: About 3~16ft
    - Analysis start point: About 3~16ft ~ about 16ft
    - Unanalyzed interval: Beyond 16ft



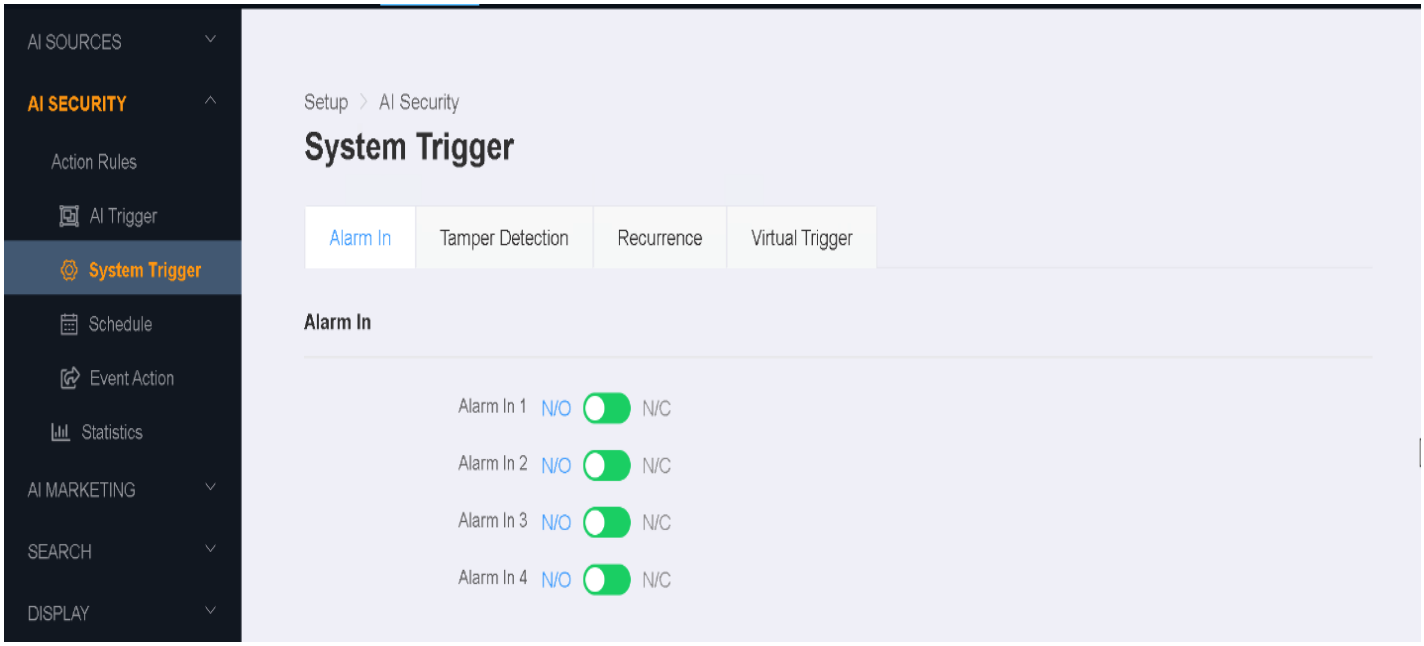
4. System Trigger

1. Alarm in

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

To create the Alarm in based System trigger, go to SETUP/AI Security/System Trigger->Alarm in

- Select 'Alarm in' if not already selected
- Select 'Alarm in 1' to toggle between 'N/O' normally open, and 'N/C' normally closed
- Select 'Alarm in 2' to toggle between 'N/O' normally open, and 'N/C' normally closed
- Select 'Alarm in 3' to toggle between 'N/O' normally open, and 'N/C' normally closed
- Select 'Alarm in 4' to toggle between 'N/O' normally open, and 'N/C' normally closed



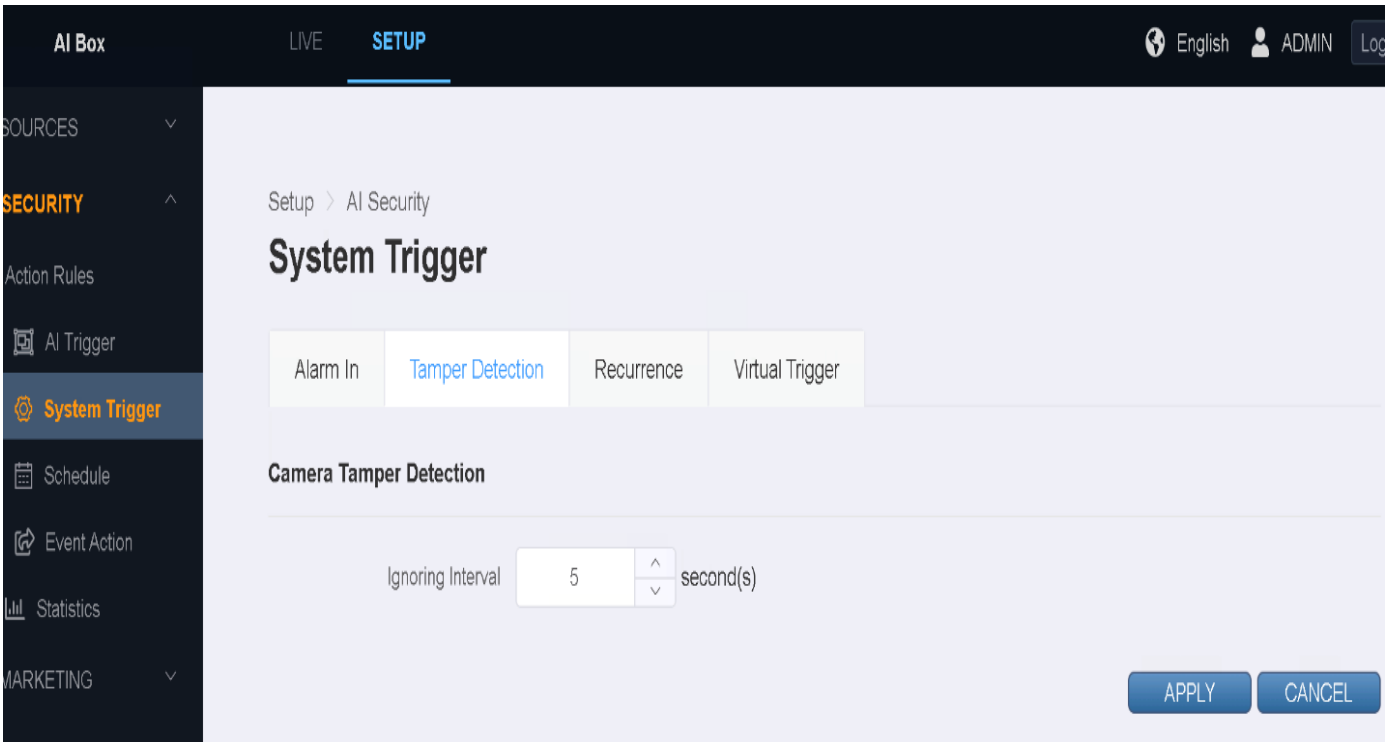
2. Camera Tamper Detection

Camera tamper detection does not require a separate preset setting. Camera tamper detection can be added directly in Action Rule setting.

To enable the Camera Tamper Detection based System trigger, go to SETUP/AI Security/System Trigger->Tamper Detection

- Select 'Tamper Detection' if not already selected
- Set the 'Ignoring interval':
  - The ignoring interval may be set for 1 second, up to 300 seconds
  - Additional temper detection event will be ignored based on the interval setting

- Click the 'APPLY' button at the bottom to save.

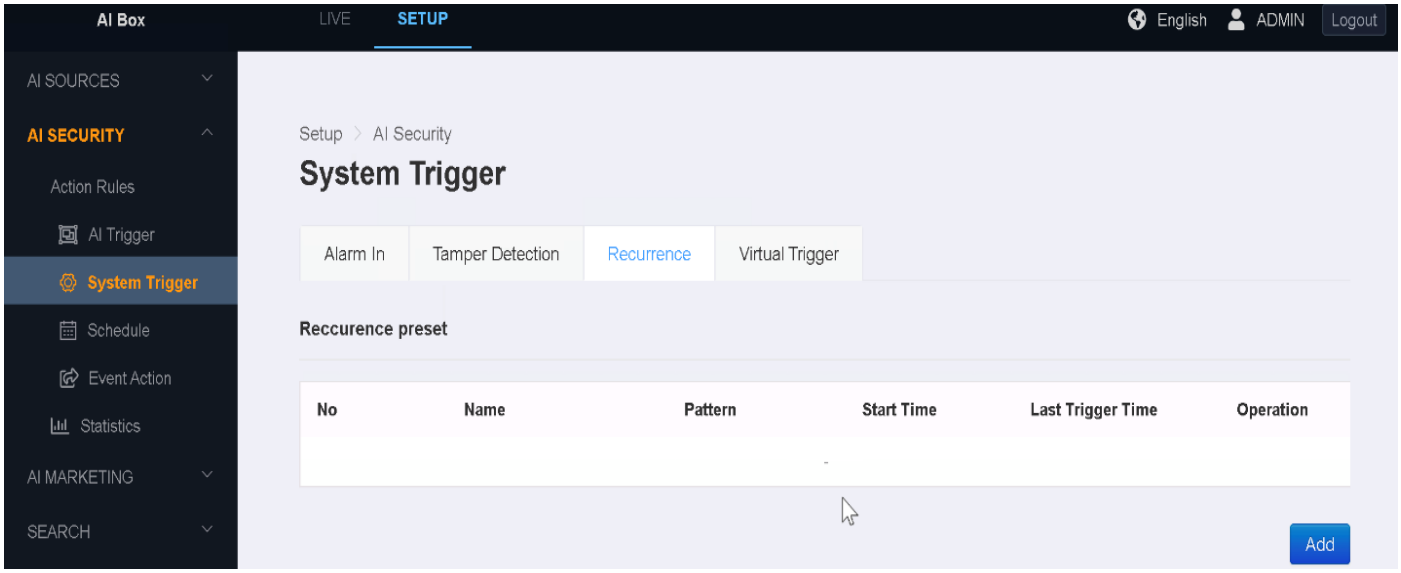


3. Recurrence Preset

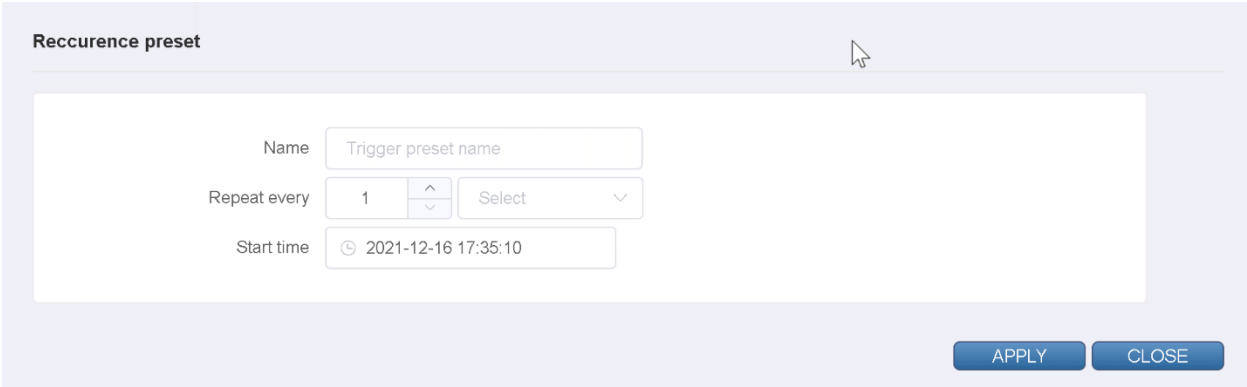
Recurrent does not require a separate preset setting. Recurrence can be added directly in Action Rule setting.

To set the recurrence preset based System trigger, go to SETUP/AI Security/System Trigger->Recurrence

- Select 'Recurrence preset' if not already selected
- Click the 'Add' button at the bottom



- Name: Title the recurrence preset according to intent
- Repeat every: 1 to 100 Seconds, Minutes, Hours, or Days
- Start Time: Set year, month, day, hour, minute, second
- Click the 'APPLY' button at the bottom to save.

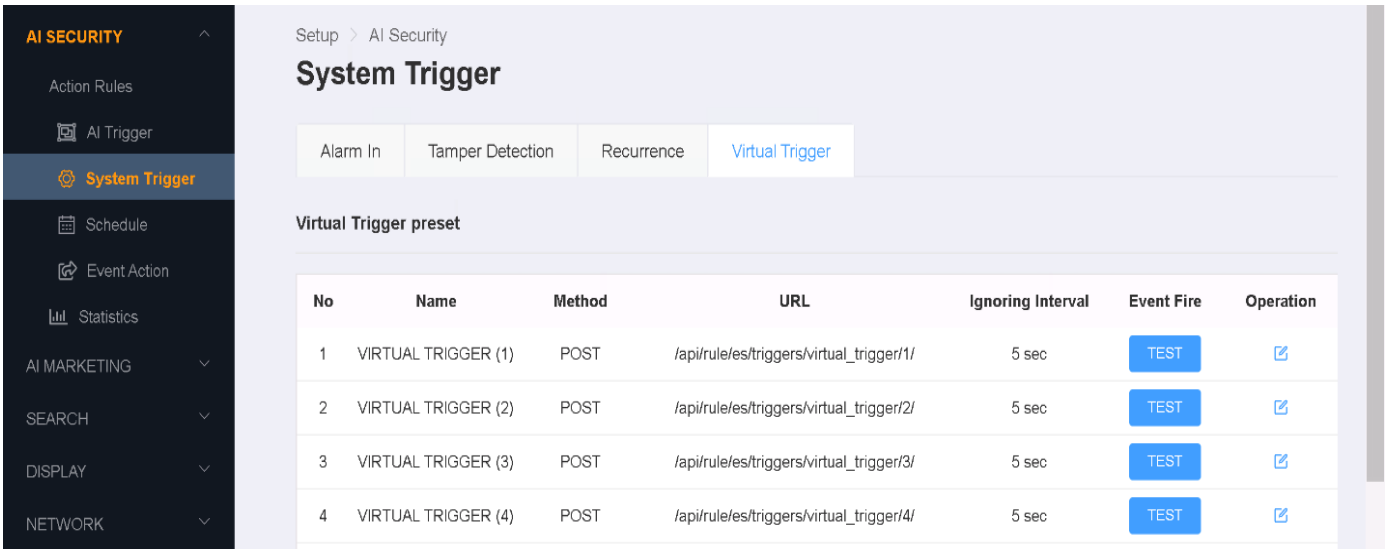


4. Virtual Trigger Preset

Virtual trigger preset does not require a separate preset setting. Virtual trigger preset can be added directly in Action Rule setting.

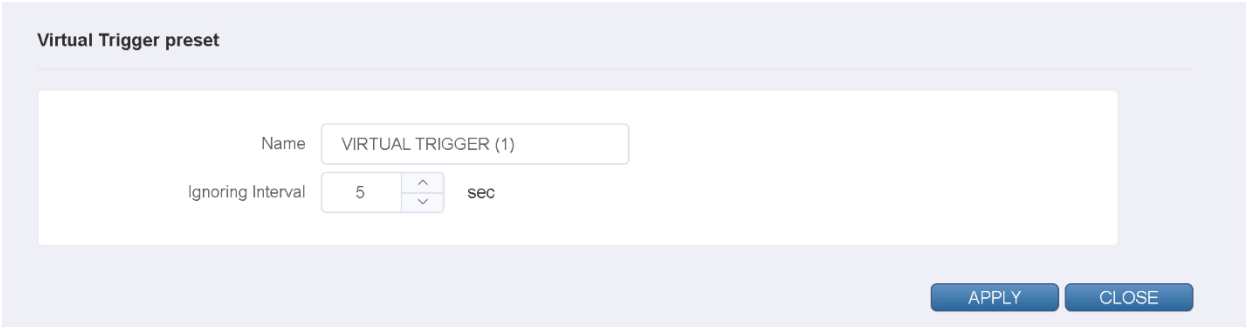
To test the virtual trigger-based System trigger, go to SETUP/AI Security/System Trigger->Virtual Trigger

- Select 'Virtual Trigger' if not already selected
- To edit a 'Virtual Trigger', select the 'edit' icon in the 'Operation' column



- Name: Modify the VIRTUAL TRIGGER title if need, to match intent of trigger
- Set the 'Ignoring interval':
  - The ignoring interval may be set for 1 second, up to 300 seconds

- Click the 'APPLY' button at the bottom to save.

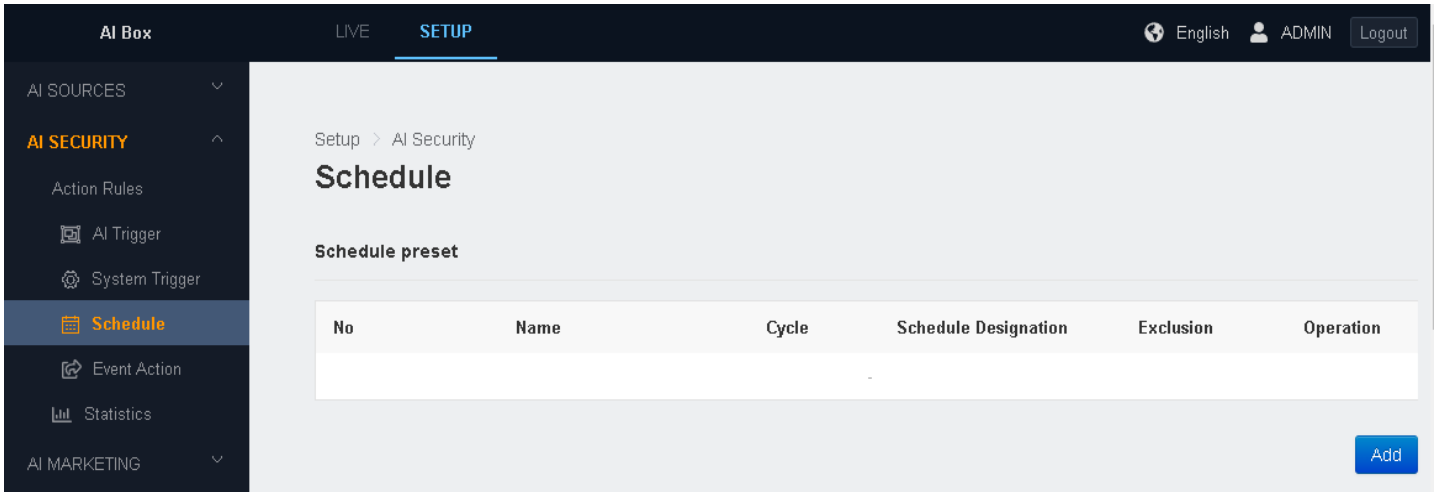


5. Schedule

The schedule preset does not require a separate preset setting. Schedule preset can be added directly in Action Rule setting.

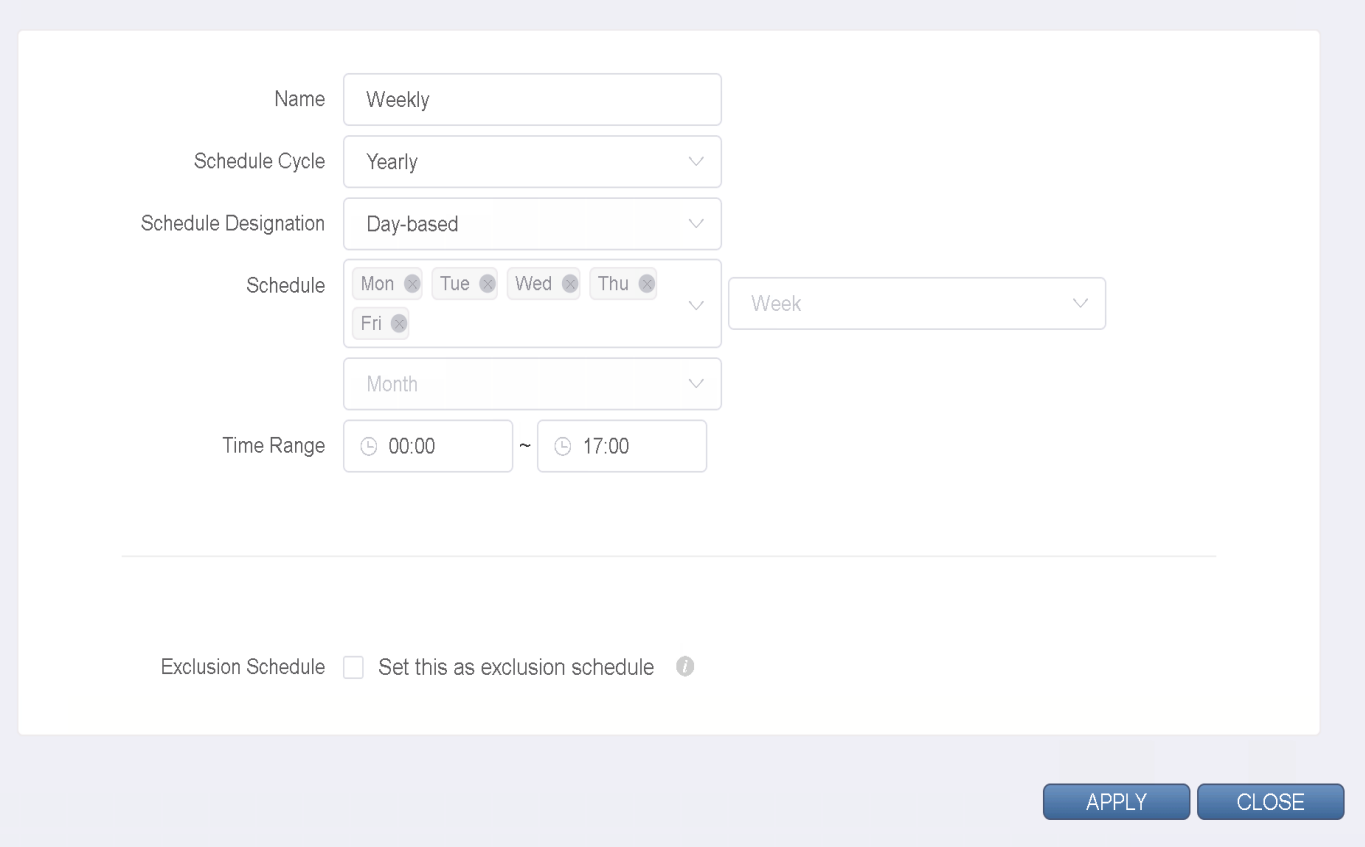
To create the schedule preset based System trigger, go to SETUP/AI Security/Schedule->Schedule preset

- Select 'Add' to create a schedule preset



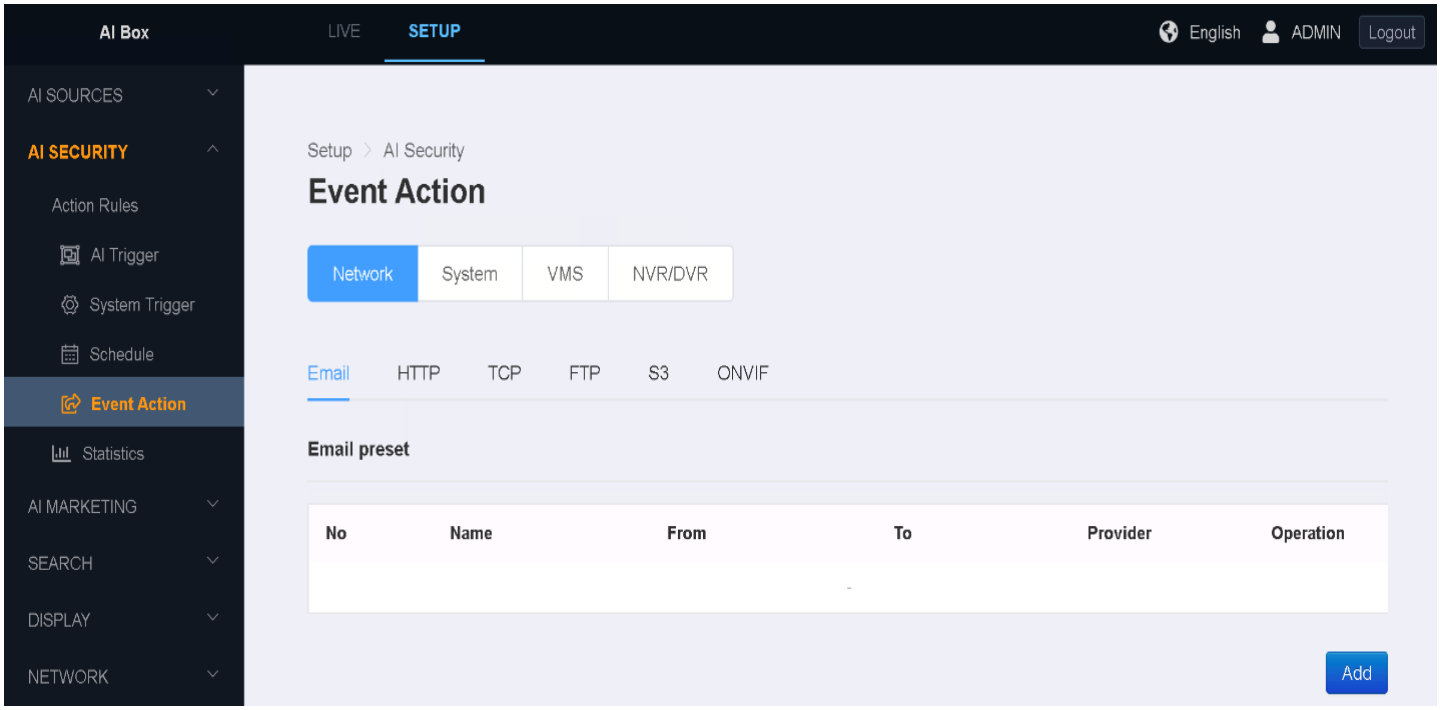
- Name: Title the schedule preset according to intent
- Schedule Cycle: Set for Weekly, Monthly, or Yearly
- Schedule Designation: Set for one of the following.
    - Day-based: Offers selection of a specific day or days, Week number, and Month
    - Date-based: Offers selection of a specific day number or range, and Month

- Time Range: Set a specific time range from 00:00 to 00:00
- Exclusion Schedule: Set this if schedule is meant as exclusion to normal schedule
- Click the 'APPLY' button at the bottom to save



6. Event Action

Event actions define how an event will respond to a trigger.

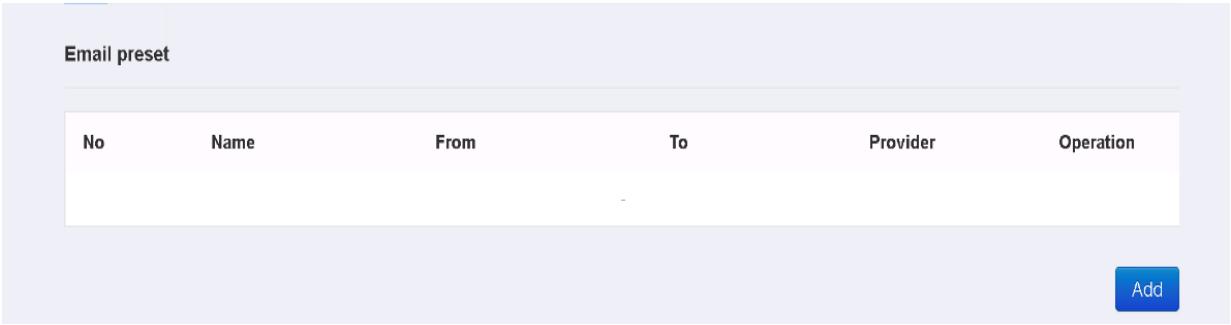


1. Network: Email Preset

Email preset does not require a separate setting. The email preset can be added directly in Action Rules.

To create the Email preset-based event action, go to SETUP/AI Security/Event Action/Network->Email

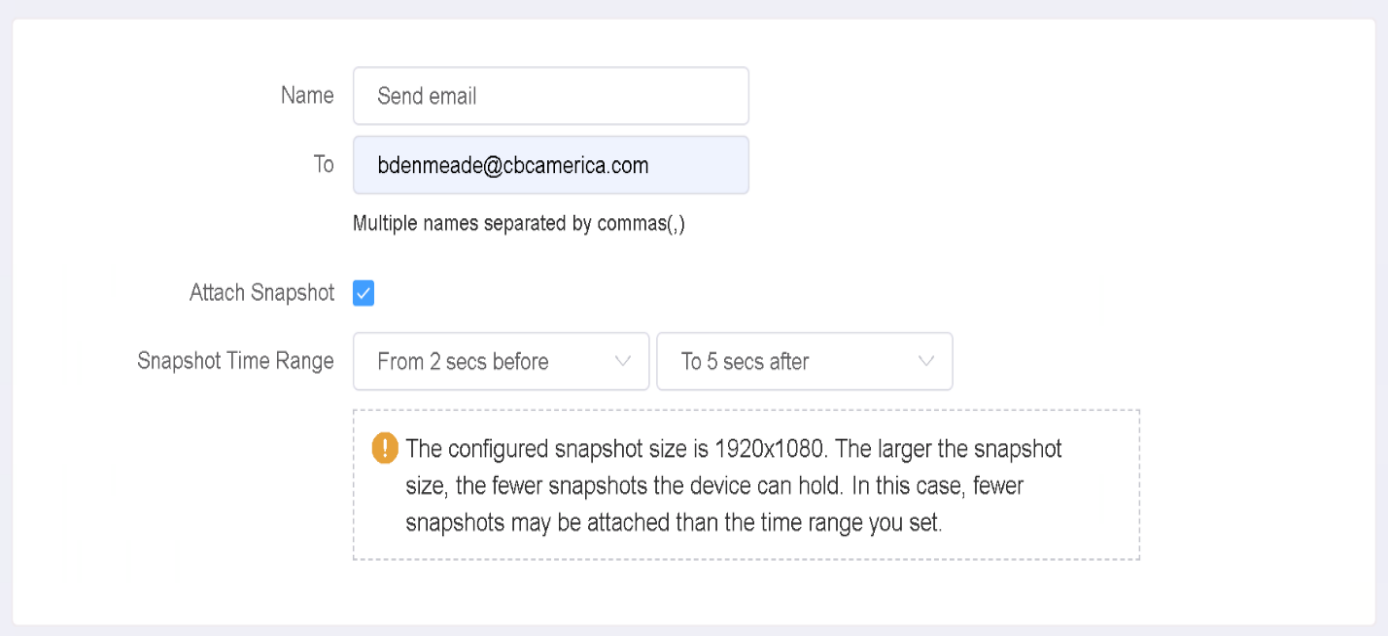
- Select 'Add' to create an email preset



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.

- Name: Title the email preset according to intent
- To: Enter an email recipient (Separate by comma if multiple recipients)
- Attach Snapshot: Check if snapshot is required
    - Snapshot Time Range: The time a snapshot is taken prior to and after trigger
        - From 0 to 10 seconds before
        - To 0 to 10 seconds after

- Note: The larger the snapshot size, the fewer snapshots the AI Box can hold.
    - Fewer snapshots may be attached then the time range that is set.
    - The snapshot size can be adjusted at SETUP/DISPLAY/Snapshot->Snapshot Size
        - Options: 640x360, 1280x720, 1920x1080



- Provider: Select the email service provider
  - Options include 'Gmail', 'Hotmail', 'Yahoo', 'Sureview', 'Sentinel'
  - Select 'Custom' if the service provider you want to use is not listed

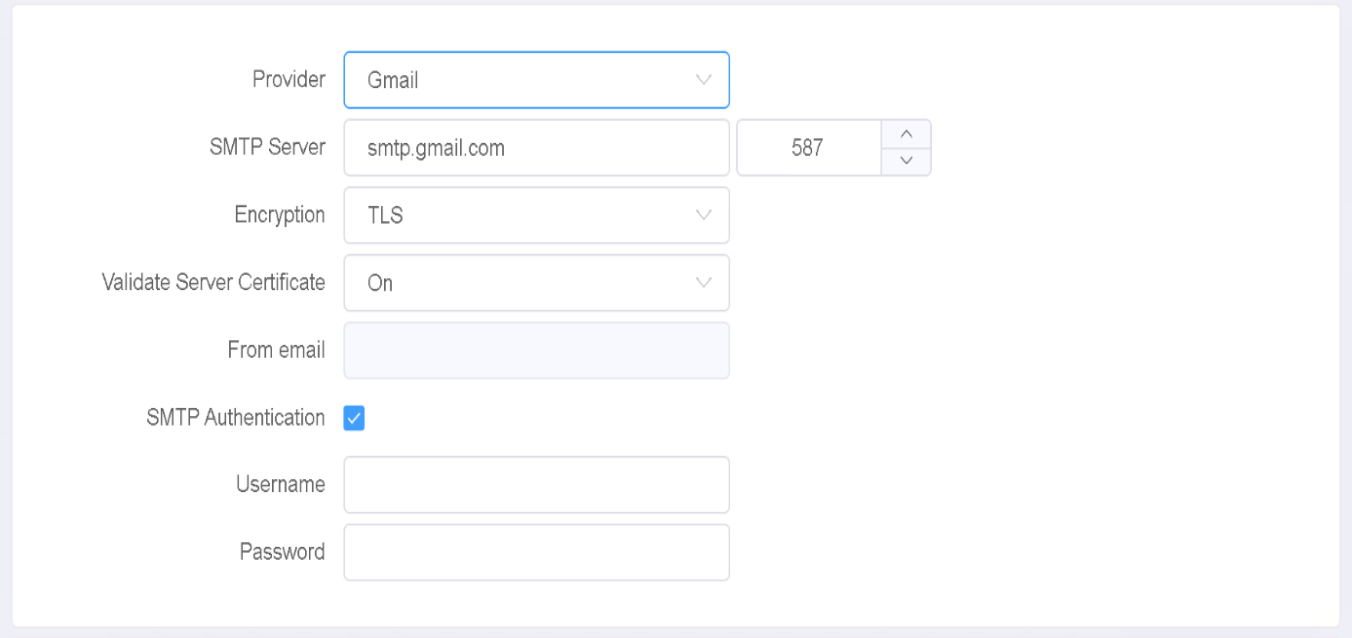
- SMTP Server: Input the SMTP server address, and communication port
  - Example: smtp.gmail.com
    - SMTP port (Default): 25
    - SMTP port (TLS): 587
    - SMTP port (SSL): 465

- Encryption: The encryption is predetermined by the SMTP port requirement
  - The sending email may by encrypted as 'None', 'TLS', or 'SSL'

- Validate Server Certificate: select 'On' or 'Off'
  - Performs a validation on 'TLS', and 'SSL' SMTP server certificates

- From email: email address used to indicate who is sending the email
  - Does not have to be the SMTP email address
  - Email sender should denote person of authority behind AI Box administration

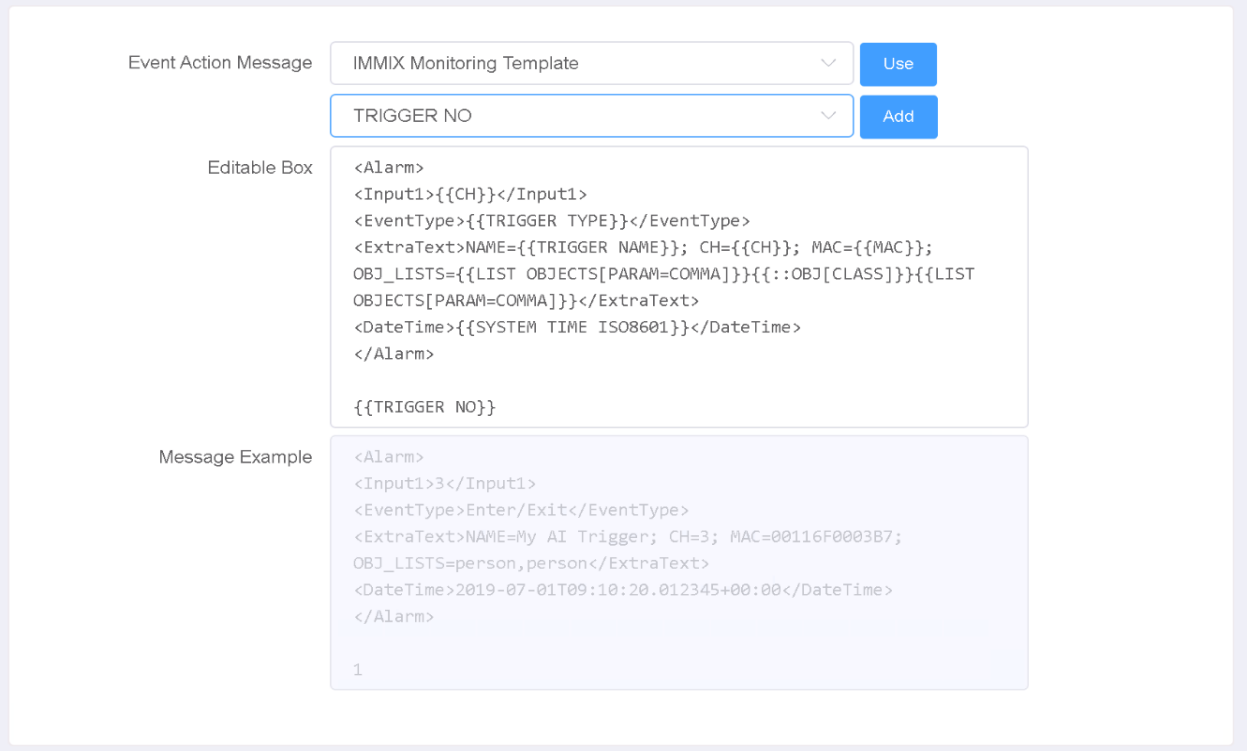
- SMTP Authentication: Check box if SMTP email account user credentials are required
  - When box is checked; SMTP account Username, and Password are required



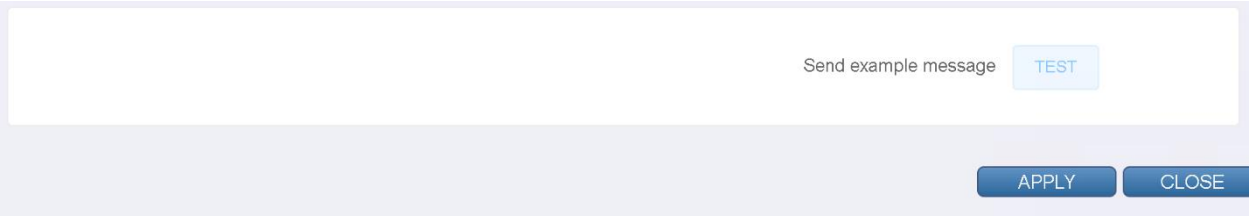
- Event Action Message: Edit the event action message
  - Use template: Configure the message by using a template
    - IMMIX, Sentinel, Sureview, JSON, Simple & Basic msg, Object list
    - Select 'Use' to add template to 'Editable Box'

  - Add attribute token: See Email Attribute Tokens list at end of section
  - Select 'Add' to add attribute token to 'Editable Box'

- Editable Box: Editable preview of the message to be sent



- Send example message: Click 'TEST' to confirm the Email's settings are correct
- Click the 'APPLY' button at the bottom to save.

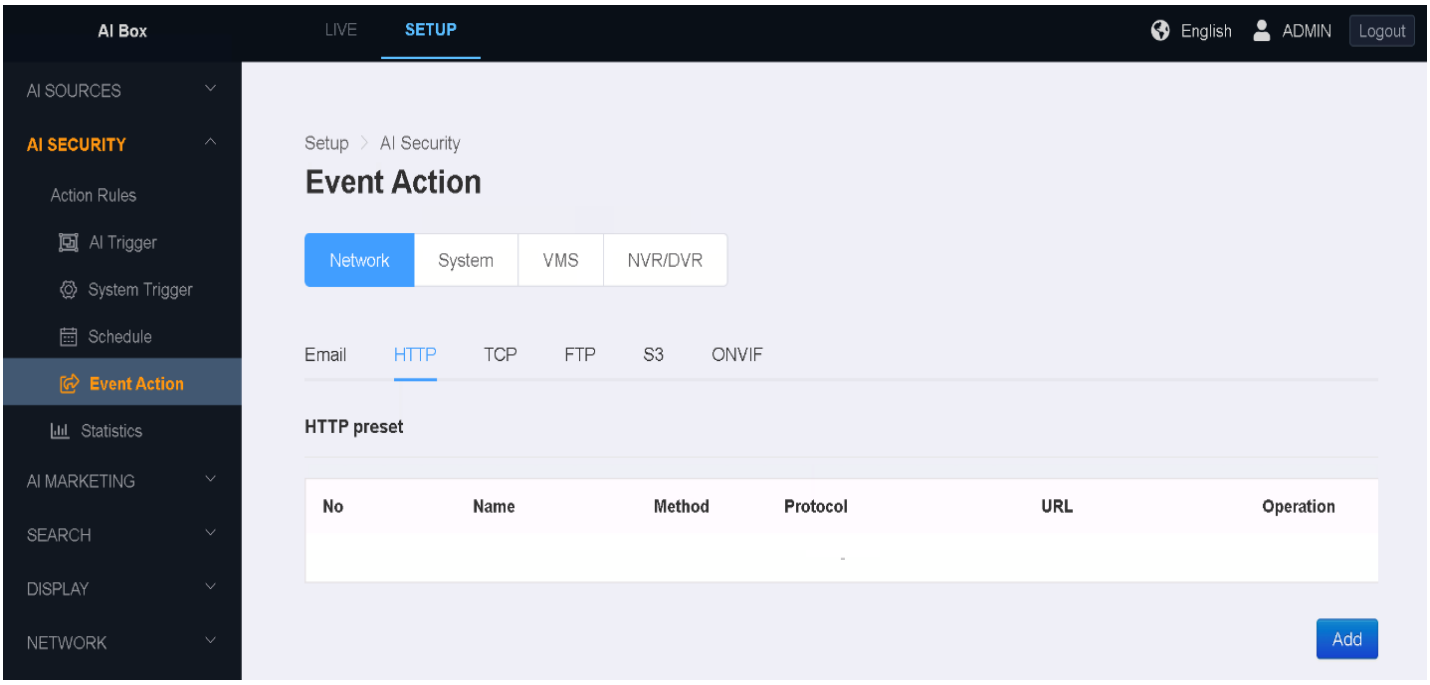


2. Network: HTTP Preset

The HTTP preset does not require a separate setting. HTTP preset can be added directly in Action Rule setting.

To create the HTTP preset-based event action, go to SETUP/AI Security/Event Action/Network->HTTP

- Select 'Add' to create an HTTP preset



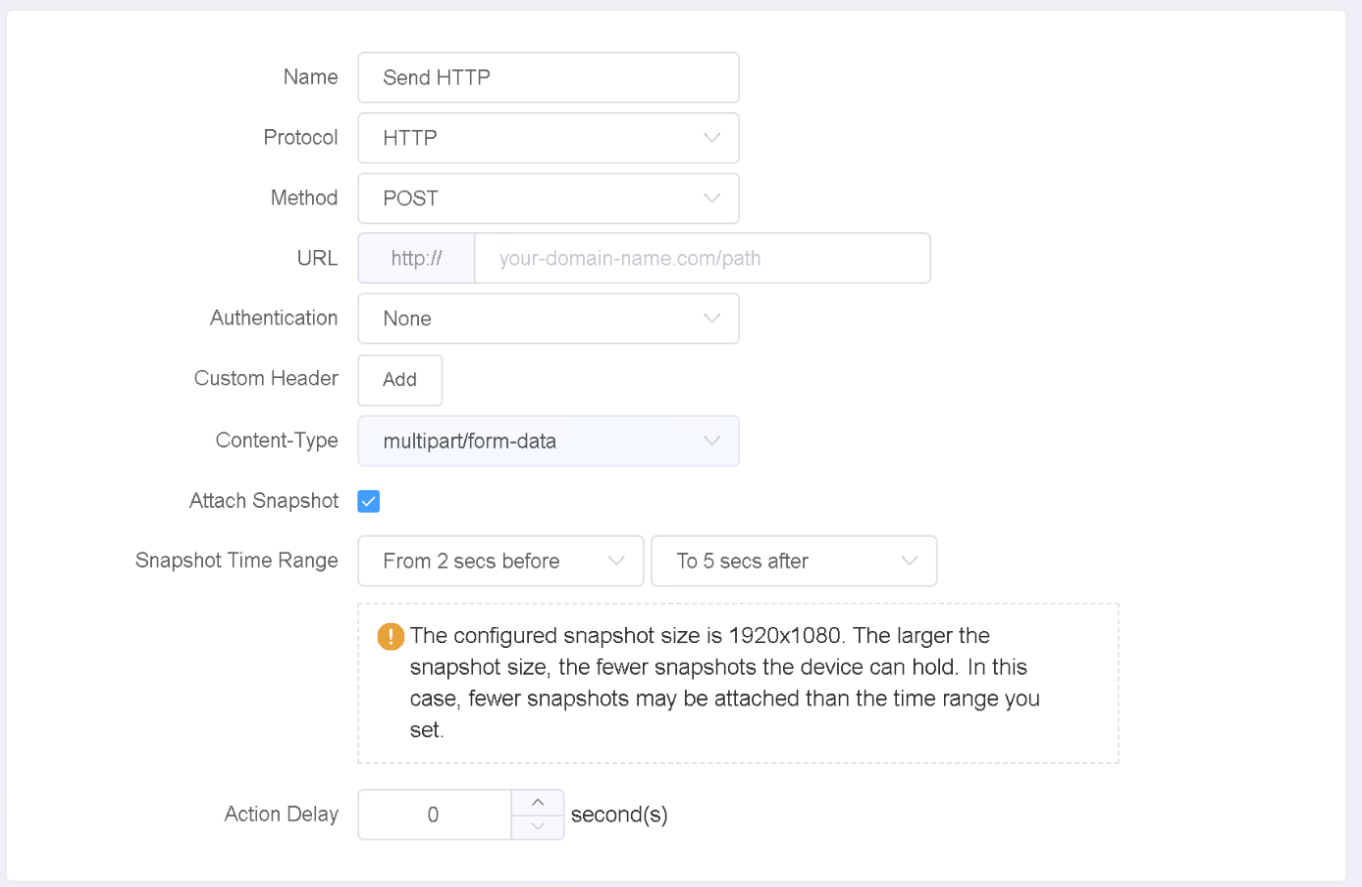
- Name: Title the HTTP preset according to intent
- Protocol: Select either 'HTTP' or 'HTTPS'
- Method: Select either 'GET', 'POST' or 'PUT'
- URL: Enter the target IP address, or URL of the HTTP receiving device
- Authentication: Select 'None', 'Basic', or 'Digest'
    - Note: Basic and Digest require user credentials for HTTP receiving device account

- Customer Header: Allows for the creation and use of a customer HTTP(s) header
    - Note: Alphanumeric characters and hyphen (-) can be used
        - Other characters are removed
        - Space characters are replaced by hyphen (-)

- Content-Type: Default – multipart/form-data (Currently not modifiable)
- Attach Snapshot: Check if snapshot is required
    - Snapshot Time Range: The time a snapshot is taken prior to and after trigger
        - From 0 to 10 seconds before
        - To 0 to 10 seconds after

- Note: The larger the snapshot size, the fewer snapshots the AI Box can hold.
    - Fewer snapshots may be attached then the time range that is set.
    - The snapshot size can be adjusted at SETUP/DISPLAY/Snapshot->Snapshot Size
        - Options: 640x360, 1280x720, 1920x1080

- Action Delay: Adds a delay time from 0 to 10 seconds
    - Note: 'Attach Snapshot' disabled when 'Action Delay' is enabled

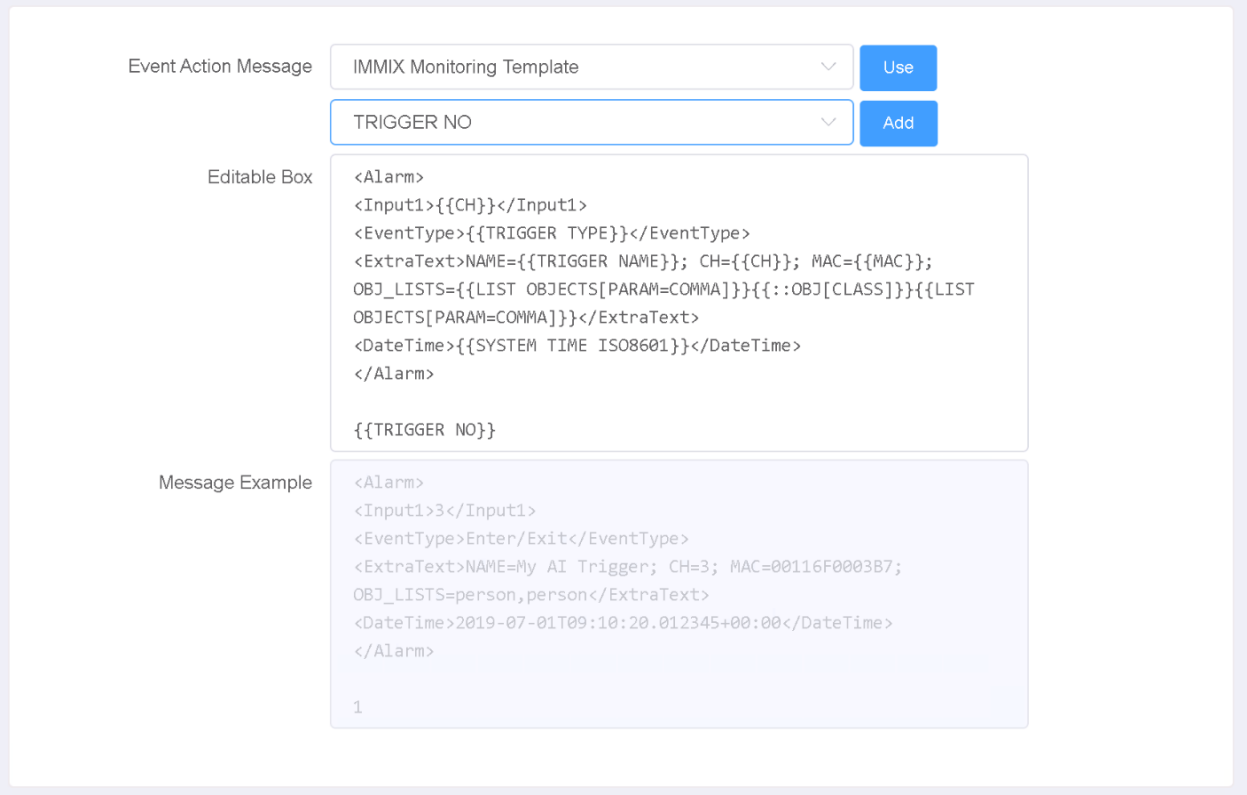


CORP HQ +1 (919) 230-8700 | WEST COAST +1 (310) 222-8600
ganzsecurity.com

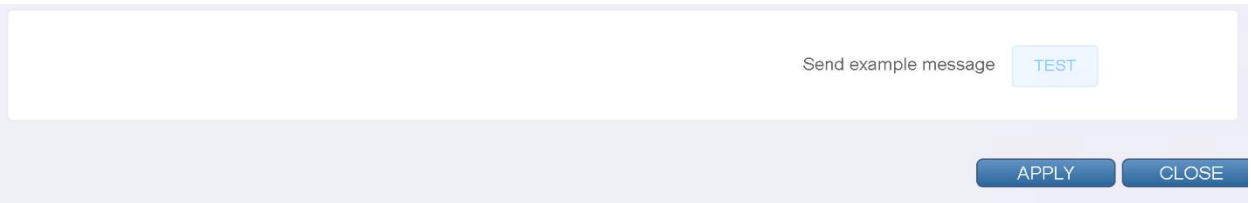
- Event Action Message: Edit the event action message
  - Use template: Configure the message by using a template
    - IMMIX, Sentinel, Sureview, JSON, Simple & Basic msg, Object list
    - Select 'Use' to add template to 'Editable Box'

  - Add attribute token: See Attribute Tokens list at end of section
  - Select 'Add' to add attribute token to 'Editable Box'

- Editable Box: Editable preview of the message to be sent



- Send example message: Click 'TEST' to confirm the Email's settings are correct
- Click the 'APPLY' button at the bottom to save.

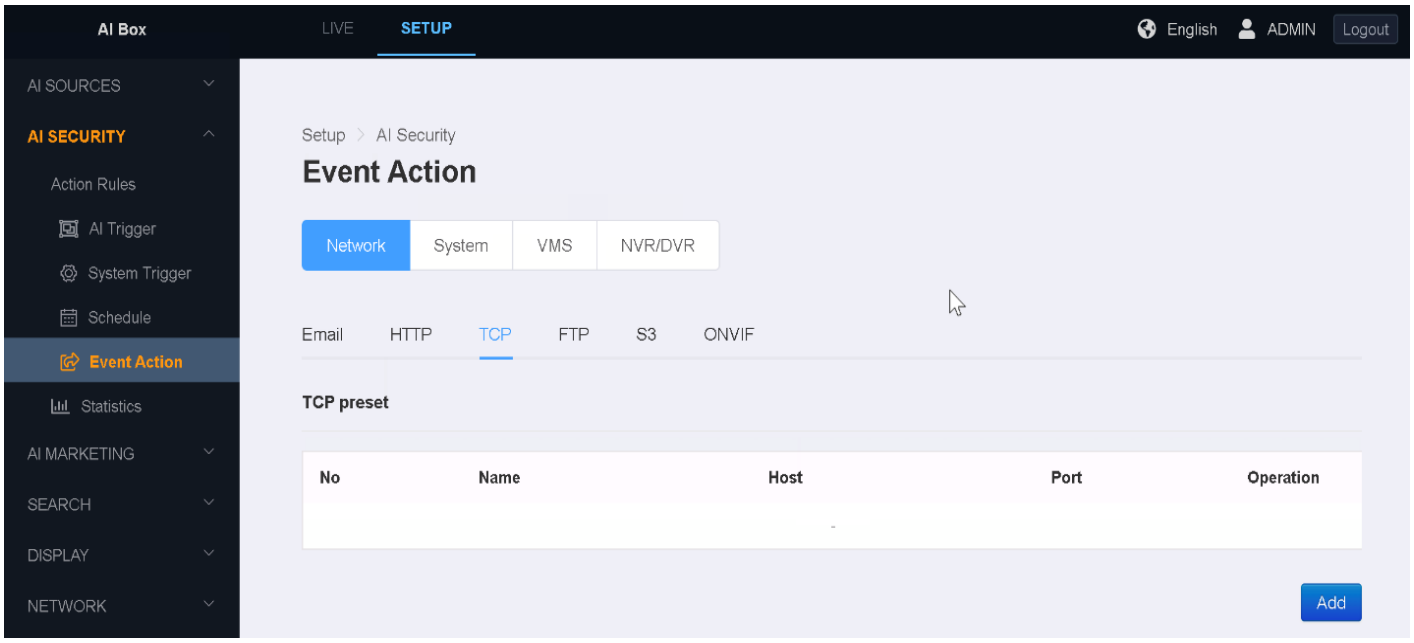


3. Network: TCP Preset

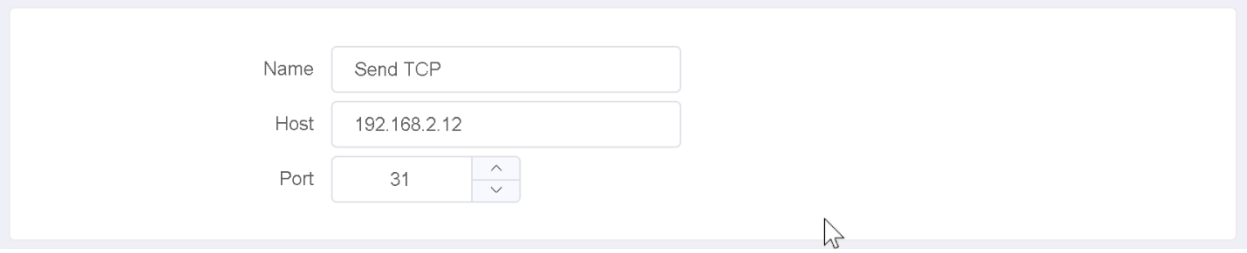
The TCP preset does not require a separate setting. TCP preset can be added directly in Action Rule setting.

To create the TCP preset-based event action, go to SETUP/AI Security/Event Action/Network->TCP

- Select 'Add' to create an TCP preset



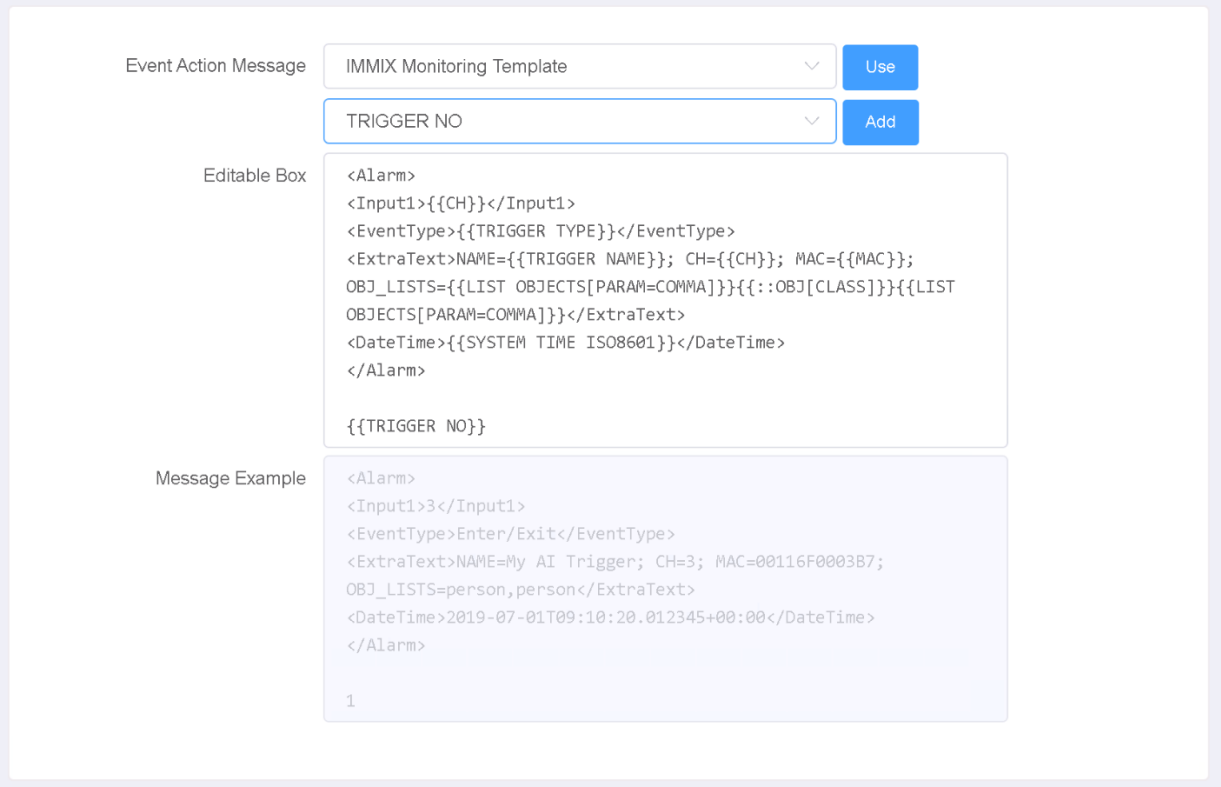
- Name: Title the TCP preset according to intent
- Host: Enter the target TCP receiving device or server IP address
- Port: Enter the target communications port receiving device or server require



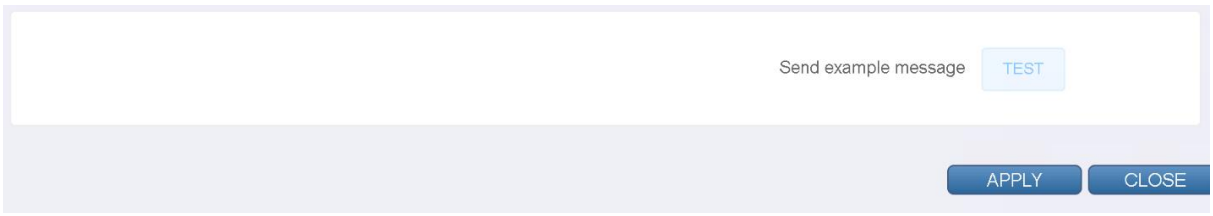
- Event Action Message: Edit the event action message
  - Use template: Configure the message by using a template
    - IMMIX, Sentinel, Sureview, JSON, Simple & Basic msg, Object list
    - Select 'Use' to add template to 'Editable Box'

  - Add attribute token: See Attribute Tokens list at end of section
  - Select 'Add' to add attribute token to 'Editable Box'

- Editable Box: Editable preview of the message to be sent



- Send example message: Click 'TEST' to confirm the TCP settings are correct
- Click the 'APPLY' button at the bottom to save.

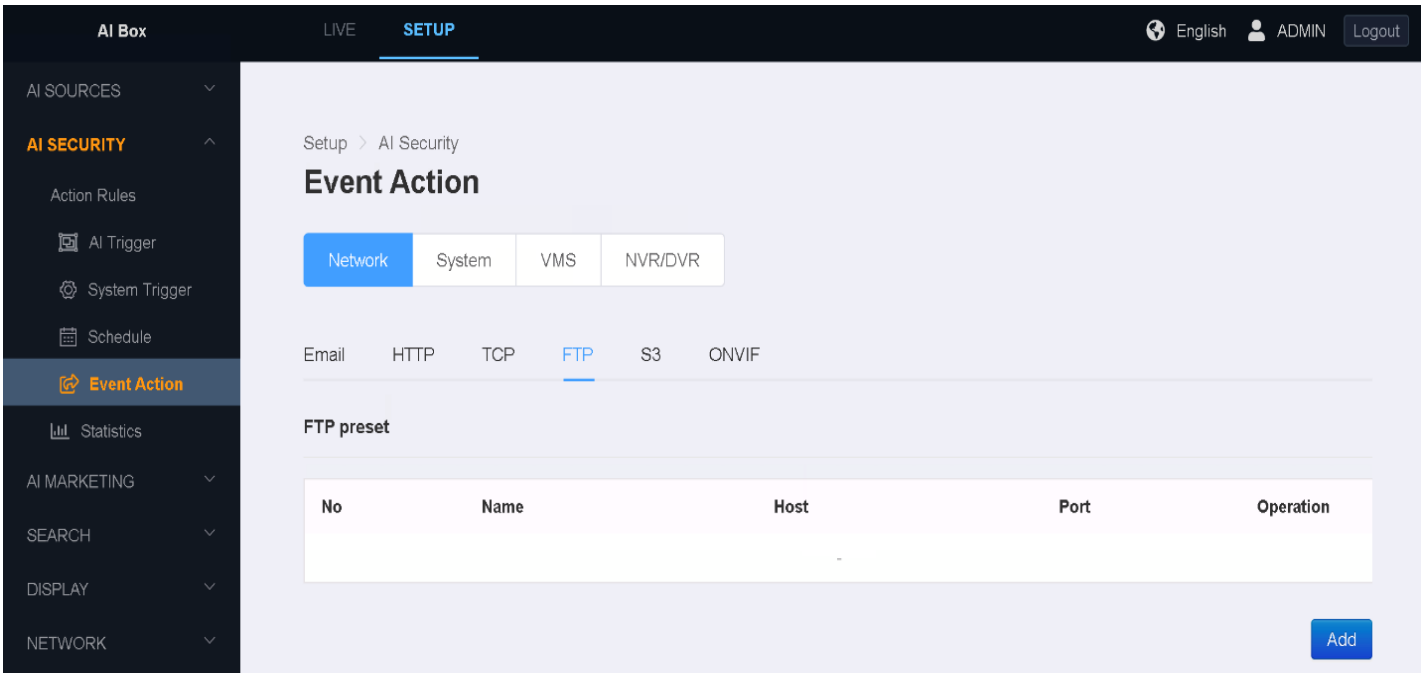


4. Network: FTP Preset

The FTP preset does not require a separate setting. FTP preset can be added directly in Action Rule setting.

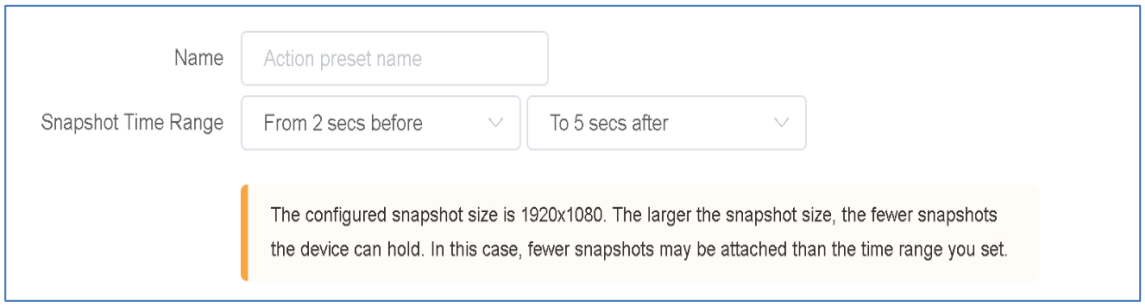
To create the FTP preset-based event action, go to SETUP/AI Security/Event Action/Network->FTP

- Select 'Add' to create an FTP preset

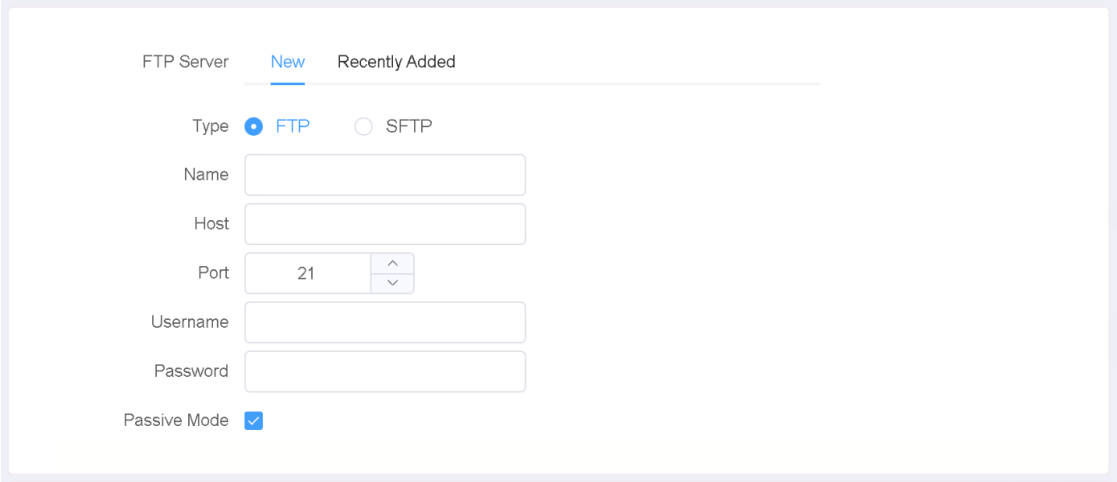


- Name: Title the FTP preset according to intent
- Snapshot Time Range: The time a snapshot is taken prior to and after trigger
    - From 0 to 10 seconds before
    - To 0 to 10 seconds after

- Note: The larger the snapshot size, the fewer snapshots the AI Box can hold.
    - Fewer snapshots may be attached then the time range that is set.
    - The snapshot size can be adjusted at SETUP/DISPLAY/Snapshot->Snapshot Size
        - Options: 640x360, 1280x720, 1920x1080

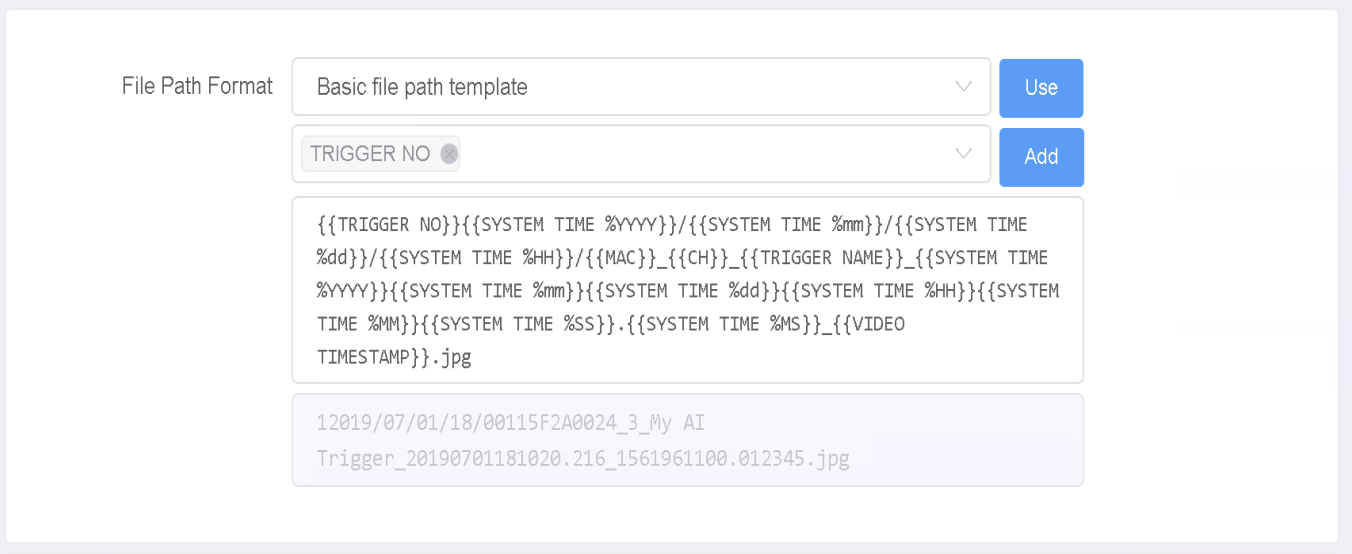


- Type: Select 'FTP' or 'SFTP'
- Name: Title of FTP connection
- Host: IP address of target FTP server
- Port: Communications port of target FTP server
- Username: User credentials with account access right to FTP server
- Password: User credentials with account access right to FTP server
- Passive Mode: Check box if passive mode is preferred for FTP connection

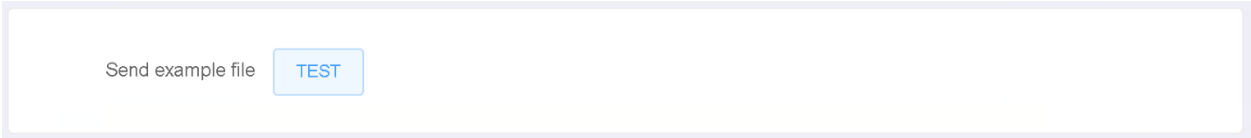


- File Path Format: Enter the FTP file path format, or use a template
  - Use template: Configure the FTP file path by using a template
    - Template: Currently only 'Basic file path template' is available
    - Select 'Use' to add
  - Add attribute token: See Attribute Tokens list at end of section
  - Select 'Add' to add attribute token to 'Editable Box'

- Editable preview of the file path format to be sent



- Send example file: Click 'TEST' to confirm the FTP settings are correct
- Click the 'APPLY' button at the bottom to save.

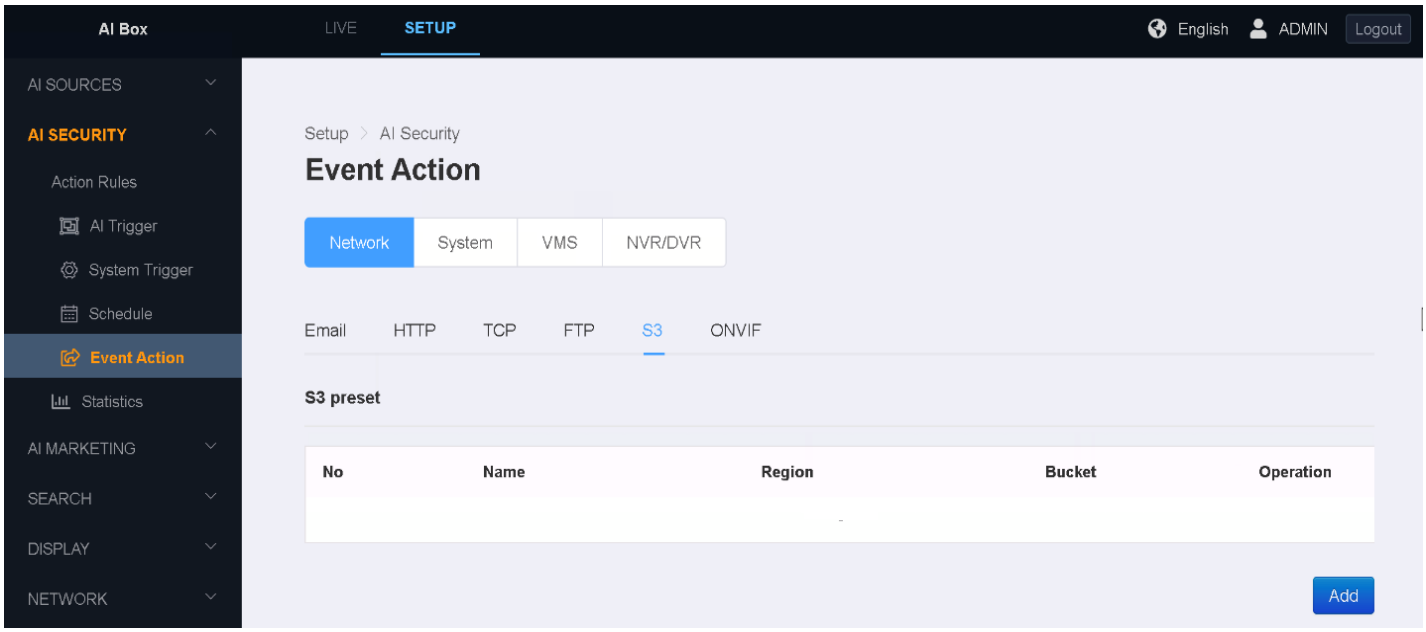


5. Network: S3 Preset

The S3 preset does not require a separate setting. The S3 preset can be added directly to Action Rules.

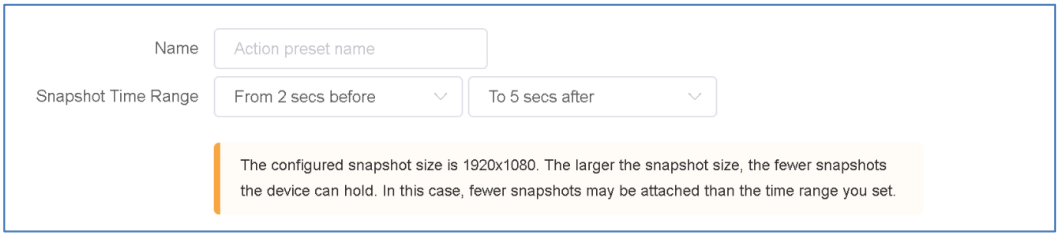
To create the ONVIF preset-based event action, go to SETUP/AI Security/Event Action/Network->S3

- Select 'Add' to create an S3 preset

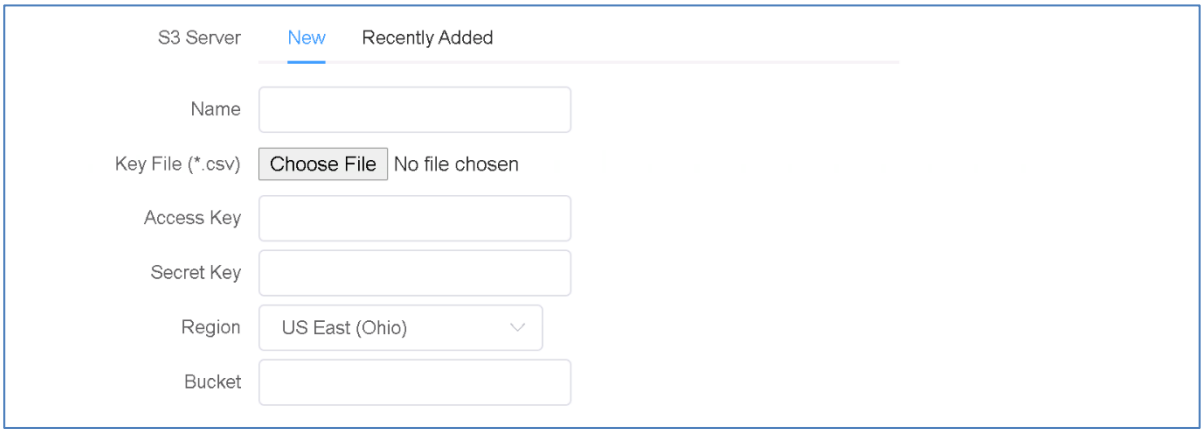


- Name: Title the FTP preset according to intent
- Snapshot Time Range: The time a snapshot is taken prior to and after trigger
    - From 0 to 10 seconds before / To 0 to 10 seconds after

- Note: The larger the snapshot size, the fewer snapshots the AI Box can hold.
    - Fewer snapshots may be attached then the time range that is set.
    - The snapshot size can be adjusted at SETUP/DISPLAY/Snapshot->Snapshot Size
        - Options: 640x360, 1280x720, 1920x1080

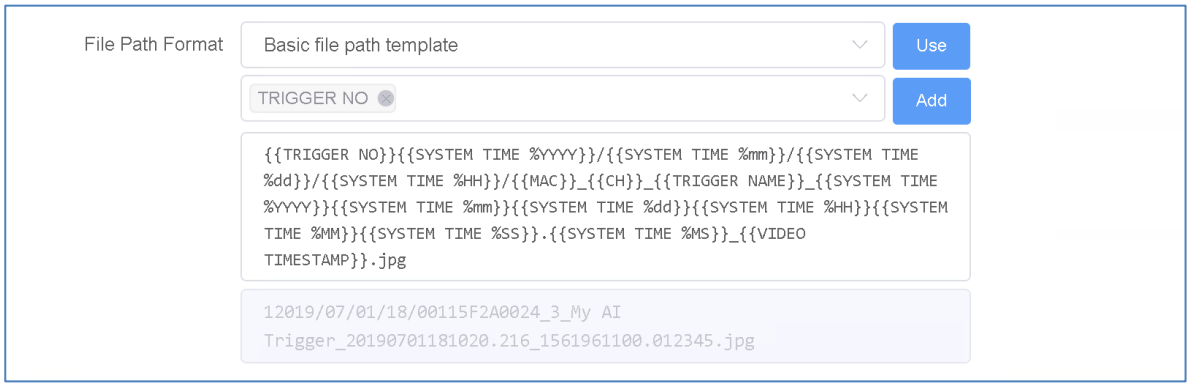


- Name: Title of S3 connection
- Key File (*.csv): Select 'Choose file' and navigate to the S3 key file
- Access Key: Enter the S3 access key
- Secret Key: Enter the S3 secret key
- Region: Select the S3 server regional location
- Bucket: Enter the bucket information

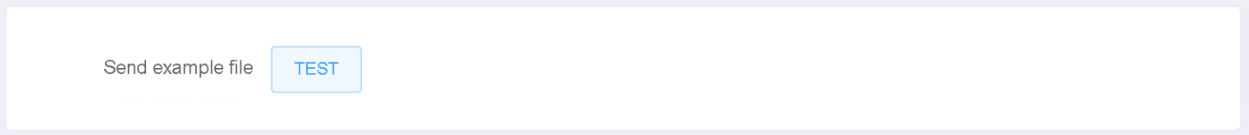


- File Path Format: Enter the S3 file path format, or use a template
  - Use template: Configure the S3 file path by using a template
    - Template: Currently only 'Basic file path template' is available
    - Select 'Use' to add
  - Add attribute token: See Attribute Tokens list at end of section
  - Select 'Add' to add attribute token to 'Editable Box'

- Editable preview of the file path format to be sent



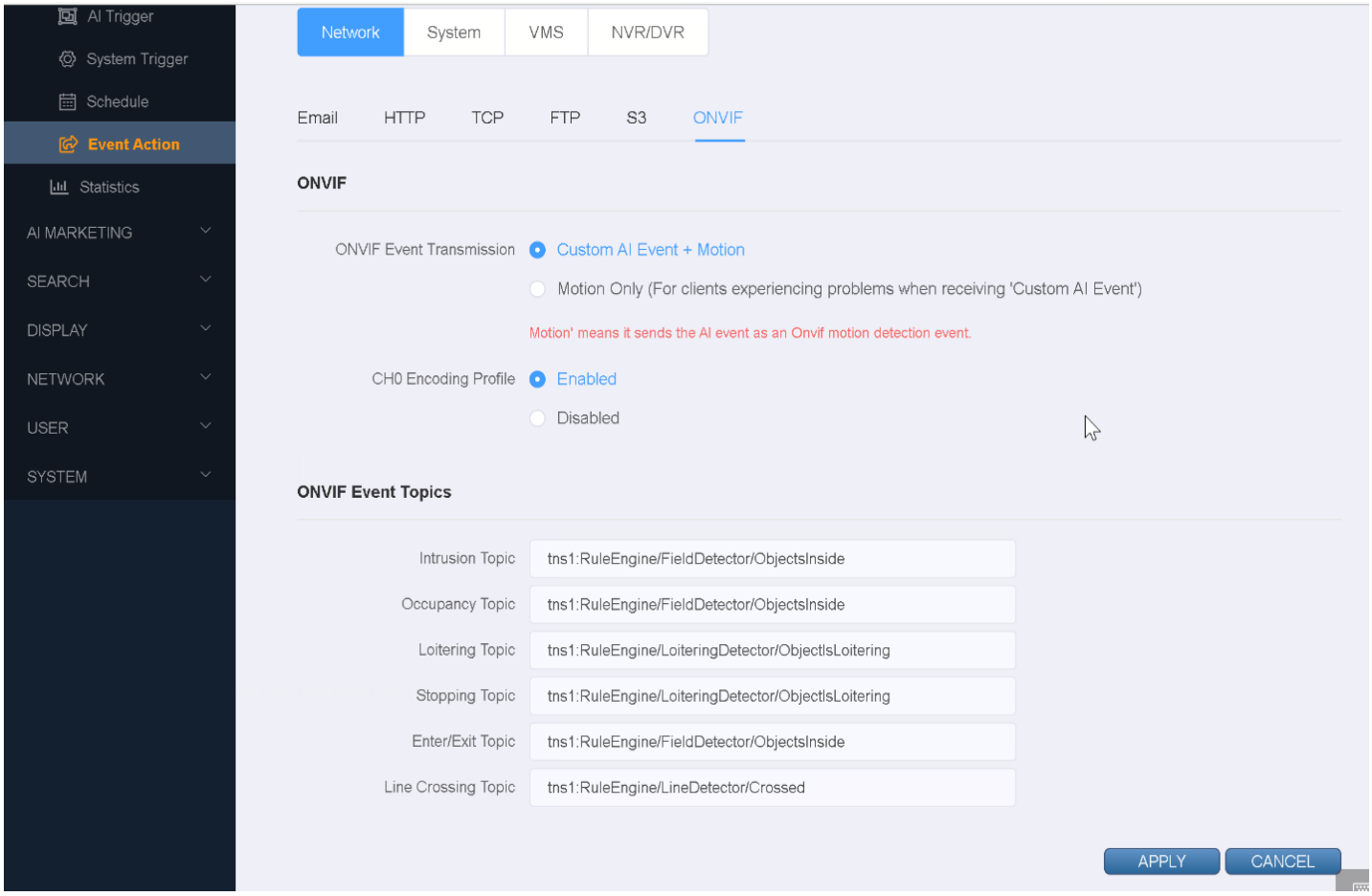
- Send example file: Click ‘TEST’ to confirm the S3 settings are correct
- Click the ‘APPLY’ button at the bottom to save.



6. Network: ONVIF Preset

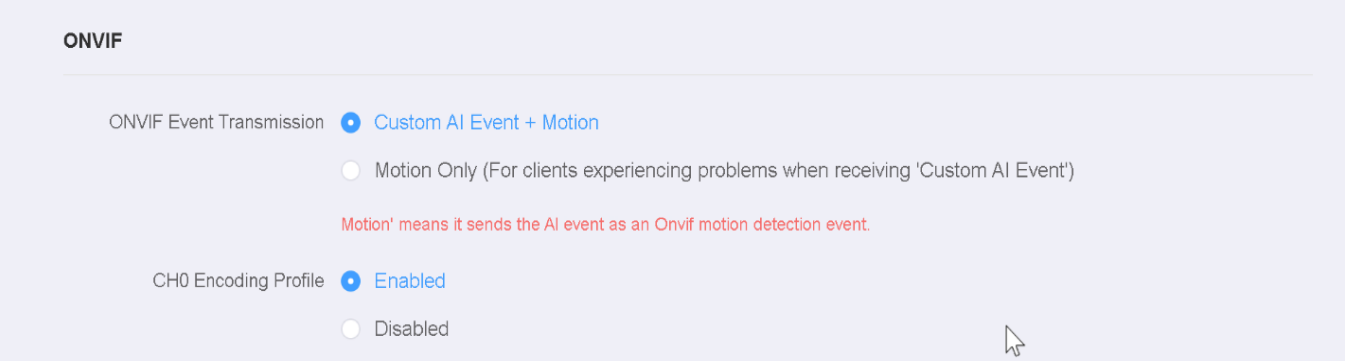
The ONVIF preset does not require a separate setting. ONVIF preset can be added directly to Action Rules.

To create the ONVIF preset-based event action, go to SETUP/AI Security/Event Action/Network->ONVIF



- ONVIF Event Transmission:
  - Customer AI Event + Motion
  - Motion Only (clients experiencing problems when receiving a 'Custom AI Event')
    - Note: 'Motion' - sends the AI event as an Onvif motion detection event

- CH0 Encoding Profile: 'Enabled' or 'Disabled'
  - CH0 displays multi layout video stream



- ONVIF Event Topics:
  - Intrusion Topic tns1:RuleEngine/FieldDetector/Objectsinside
  - Occupancy Topic tns1:RuleEngine/FieldDetector/Objectsinside
  - Loitering Topic tns1:RuleEngine/LoiteringDetector/ObjectisLoitering
  - Stopping Topic tns1:RuleEngine/ LoiteringDetector/ObjectisLoitering
  - Enter/Exit Topic tns1:RuleEngine/FieldDetector/Objectsinside
  - Line Crossing Topic: tns1:RuleEngine/ LineDetector/Crossed

CORP HQ +1 (919) 230-8700 | WEST COAST +1 (310) 222-8600
ganzsecurity.com

7. System: Disarm

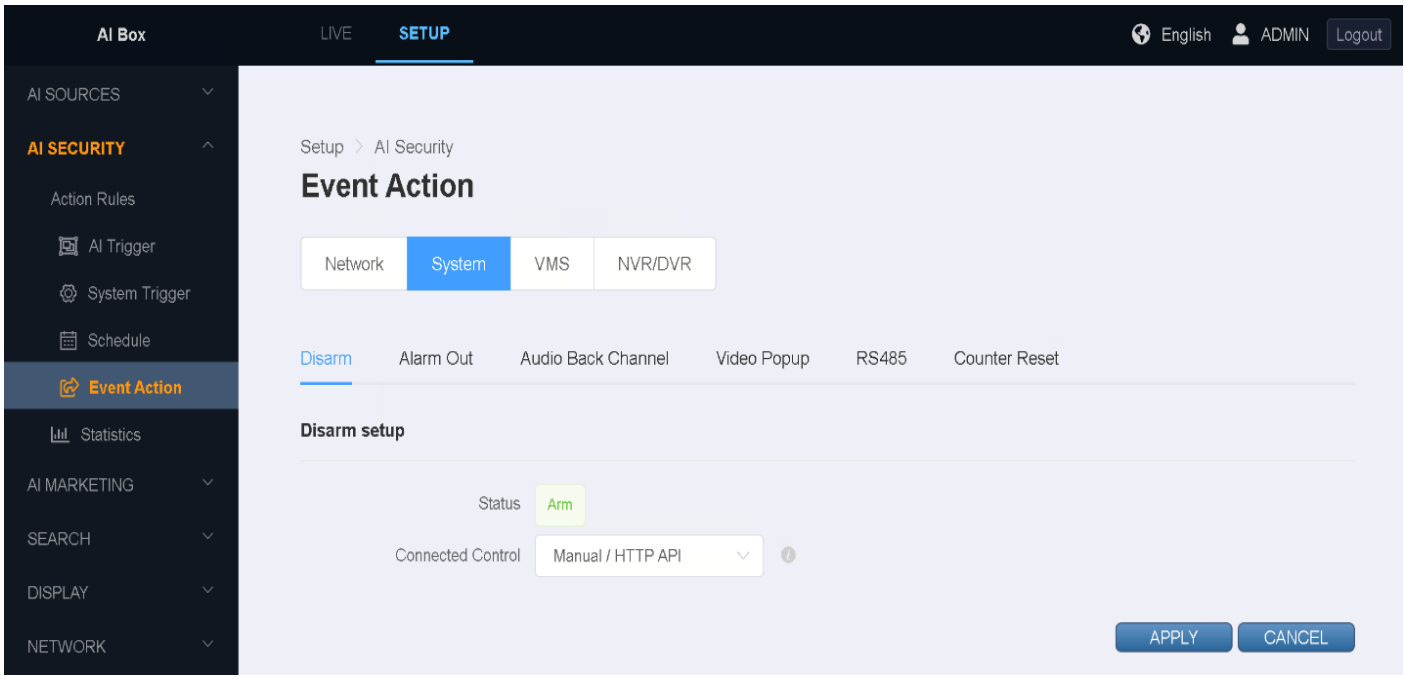
AI BOX is an ARM state that can generate an alarm action event at any time. However, the connected controller can be changed to DISARM state to prevent alarm action event.

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

To configure the 'Disarm setup' event action, go to SETUP/AI Security/Event Action/System->Disarm setup

- Status: Will display 'Arm' or 'Disarm' based on status
- Connected Control: Options include the following
  - Manual / HTTP API
  - Alarm in 1
  - Alarm in 2
  - Alarm in 3
  - Alarm in 4

- Click the 'APPLY' button at the bottom to save

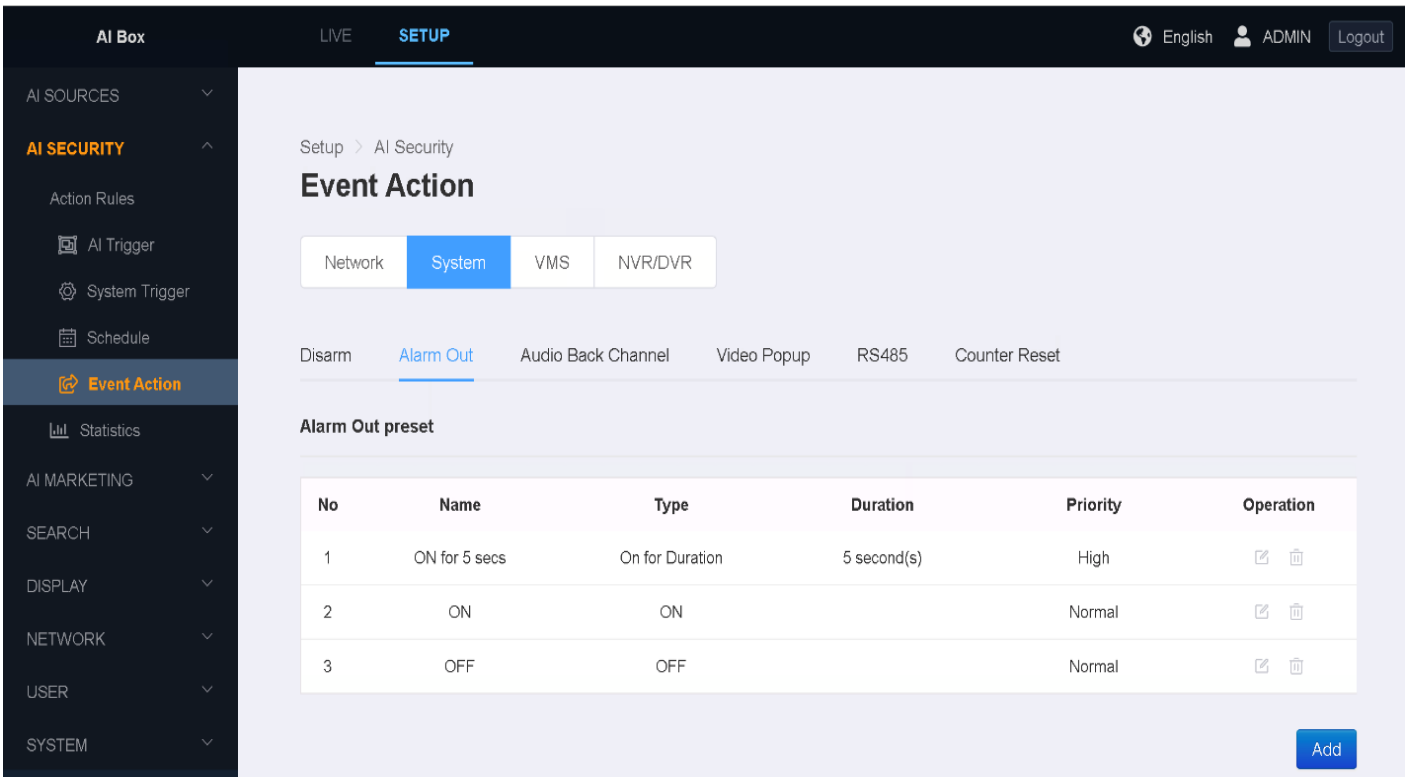


8. System: Alarm Out

It is possible to set how long it will activate from the Alarm Out Duration when the Alarm Out action is activated.

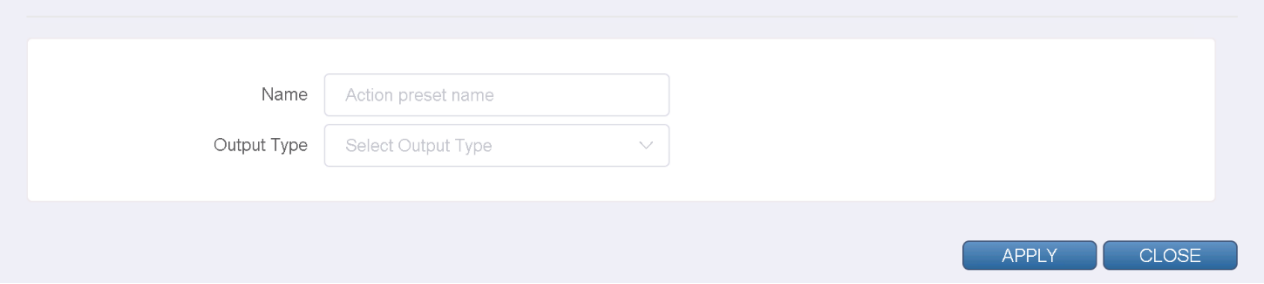
To configure the 'Alarm out' event action, go to SETUP/AI Security/Event Action/System->Alarm Out preset

- Select 'Add' to create an Alarm out preset



- Name: Title the alarm out preset according to intent
- Output Type: Options include the following
    - On for Duration – High Priority (0 to 300 seconds duration)
    - Off for Duration – High Priority (0 to 300 seconds duration)
    - On – Normal Priority
    - Off – Normal Priority

- Click the 'APPLY' button at the bottom to save

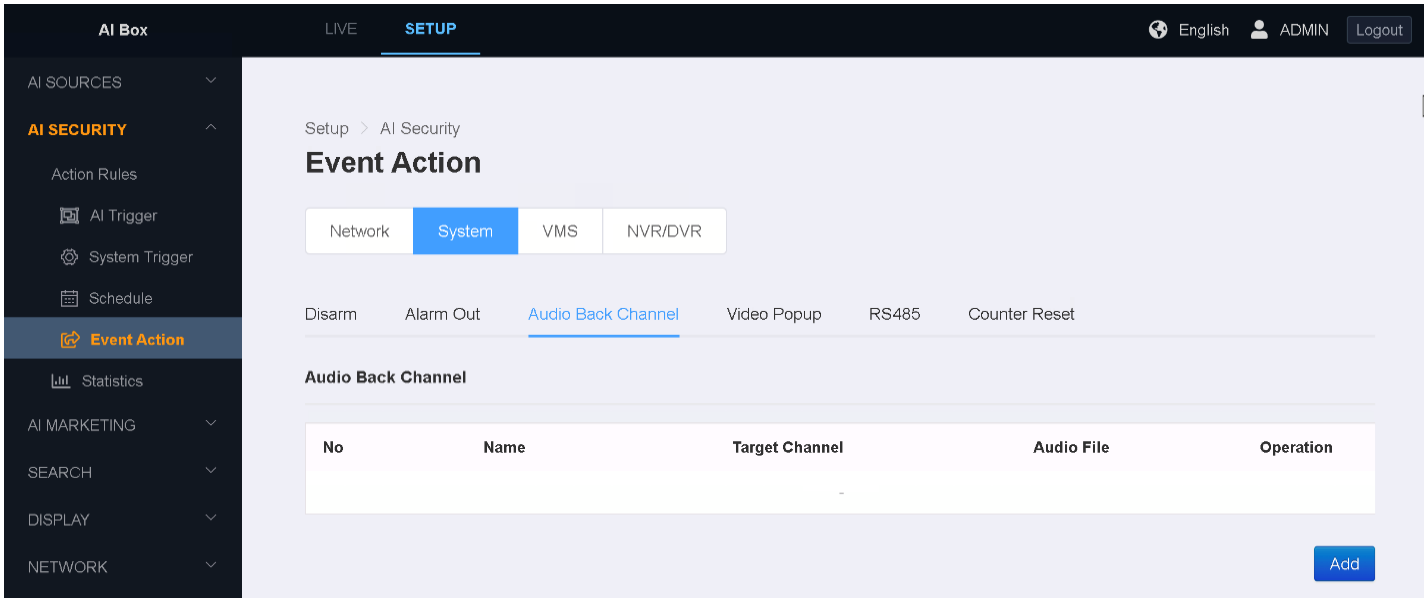


9. System: Audio Back Channel

It is possible to set an audio file to play through a video sources audio channel out channel.

To configure the 'Audio Back Channel' event action, go to SETUP/AI Security/Event Action/System->Audio Back Channel

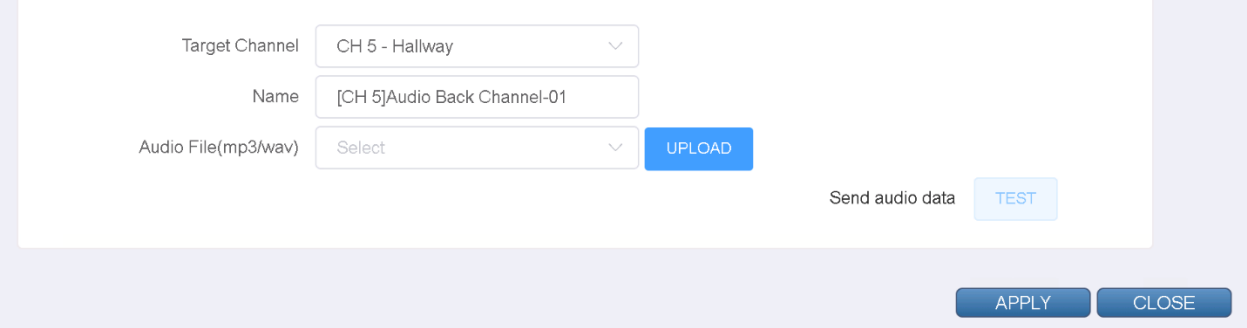
- Select 'Add' to create an audio back channel



- Target Channel: Select the video source from the drop-down list
  - Video source should support audio back channel
  - Video source device should have a speaker attached

- Name: Title the audio back channel according to intent
- Audio File(mp3/wav): Select 'Upload' and navigate to the target audio file
  - Both mp3 and wav audio formats supported

- Click the 'APPLY' button at the bottom to save



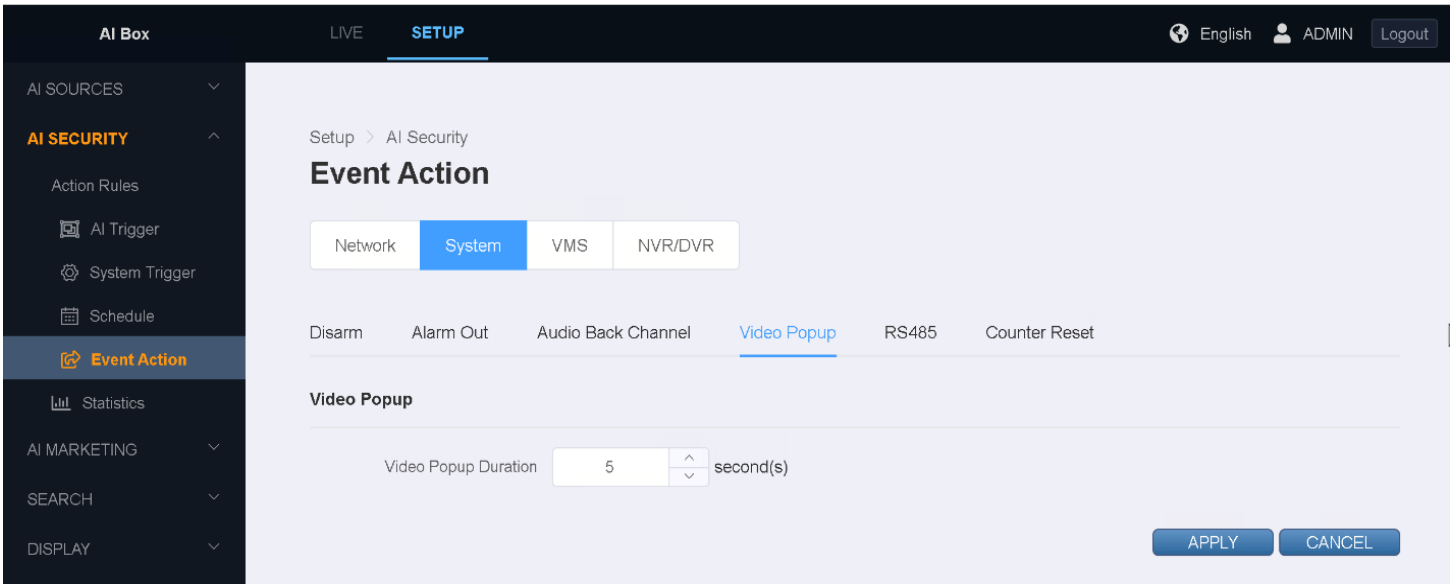
10. System: Video Popup

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.

To configure the 'Video Popup' event action, go to SETUP/AI Security/Event Action/System->Video Popup

- Video Popup Duration: This is the duration of time the popup will be presented
  - Duration time is between 0 and 300 seconds

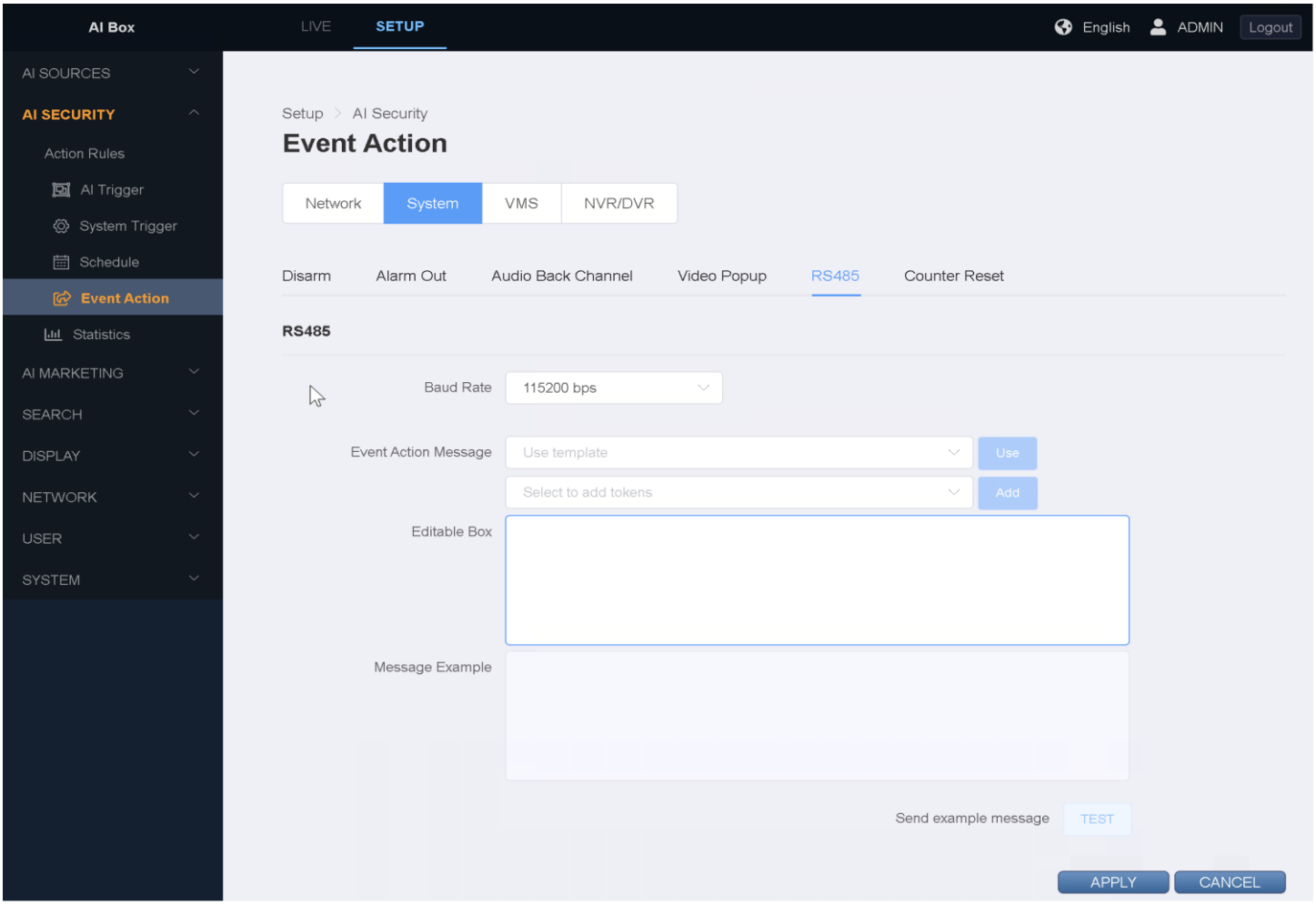
- Click the 'APPLY' button at the bottom to save



11. System: 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.

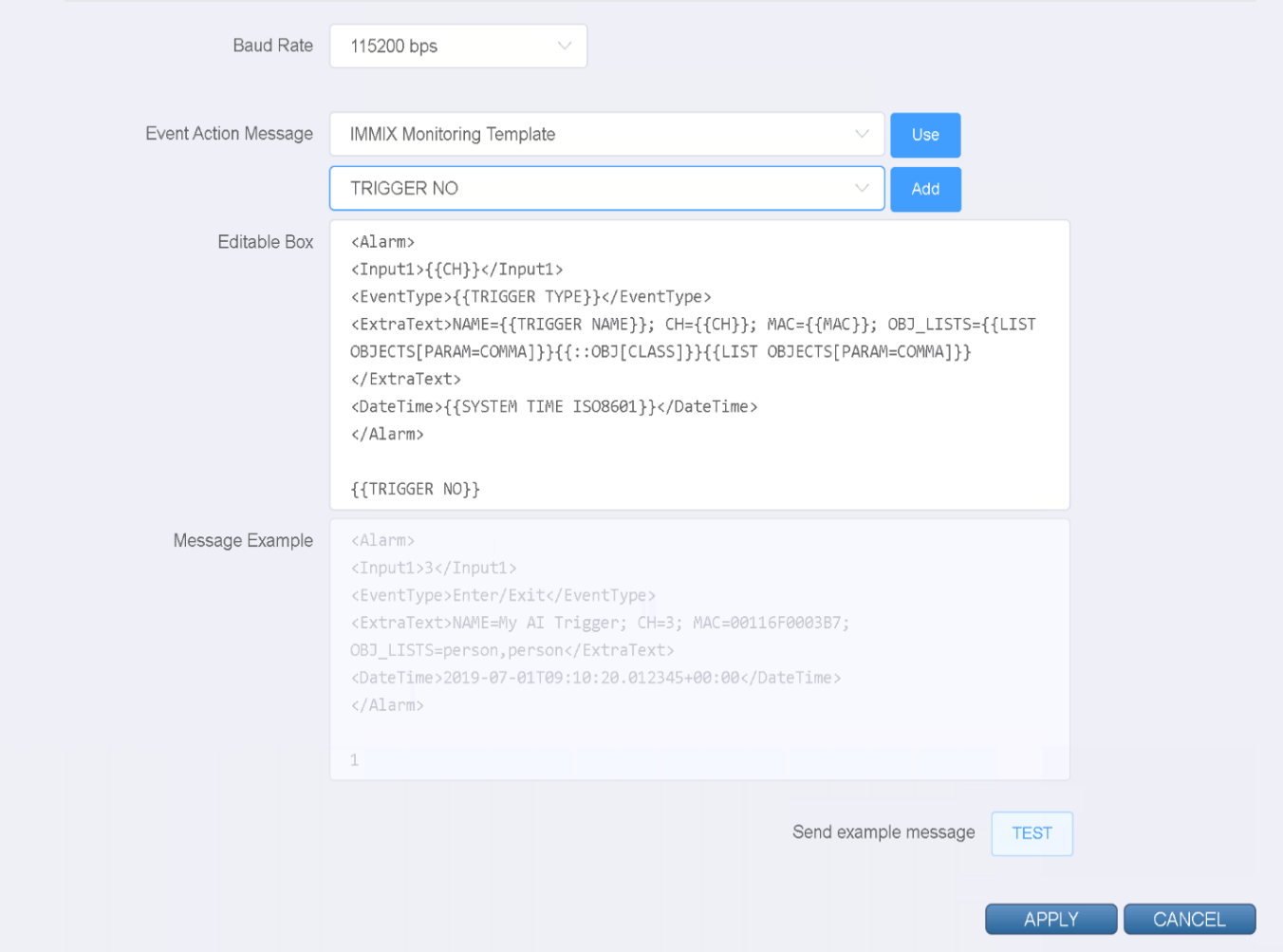
To configure the 'RS485' event action, go to SETUP/AI Security/Event Action/System->RS485



- Baud Rate: This is the rate of communications to take place on the RS485 port
  - Baud rates range between 2400 bps, and 115200 bps

- Event Action Message: Enter a custom, or use a template
  - Use template: Configure the message by using a template
    - IMMIX, Sentinel, Sureview, JSON, Simple & Basic msg, Object list
    - Select 'Use' to add template to 'Editable Box'
  - Add attribute token: See Attribute Tokens list at end of section
  - Select 'Add' to add attribute token to 'Editable Box'

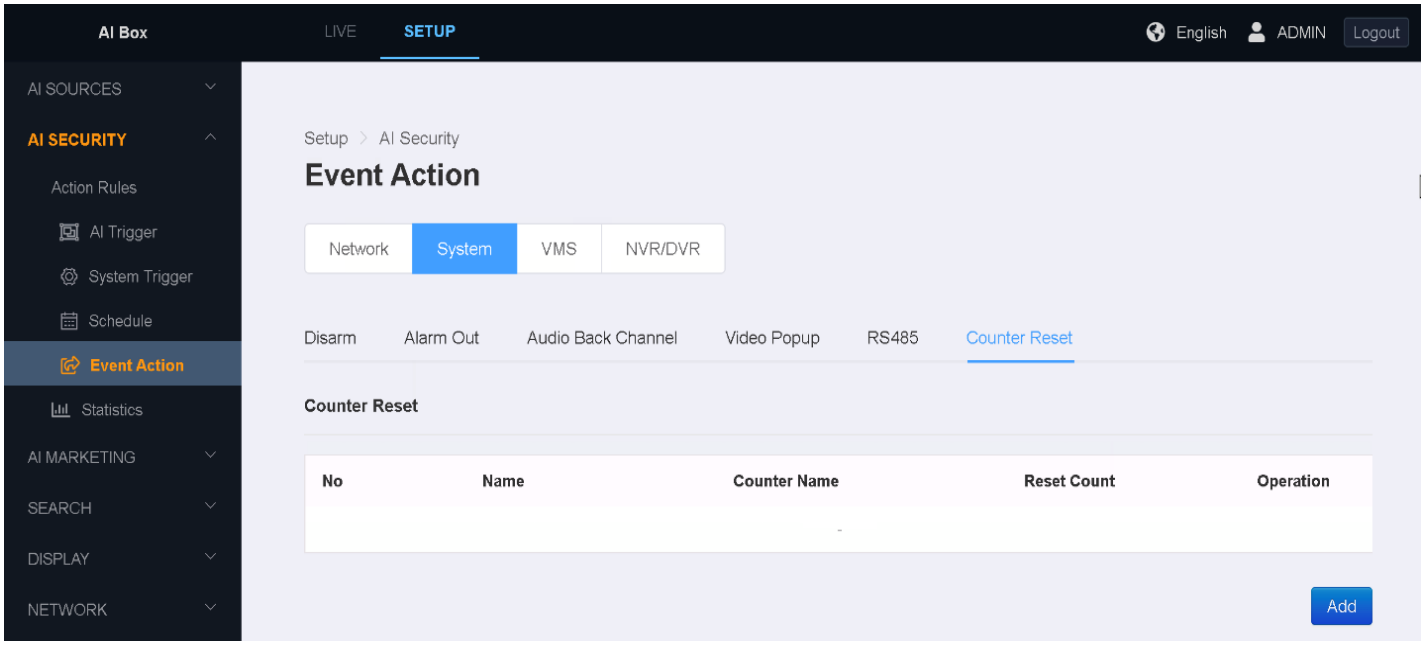
- Editable Box: Editable preview of the message to be sent
- Send example message: Click 'TEST'
- Click the 'APPLY' button at the bottom to save.



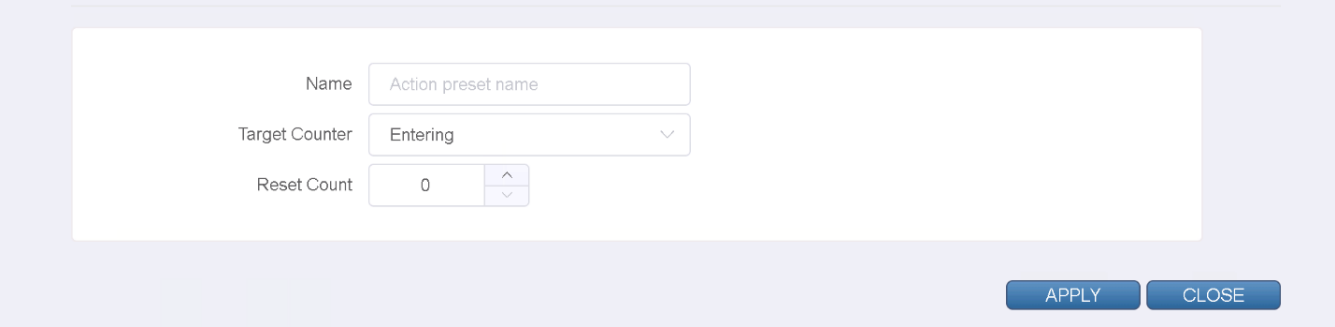
12. System: Counter Reset

The 'Counter Reset' action defines a event action to reset an existing counter action.
To configure the 'Counter Reset' event action, go to SETUP/AI Security/Event Action/System->Counter Reset

- Select 'Add' to create a Counter Reset action



- Name: Title the Counter reset according to intent
- Target Counter: Select the count trigger from the drop-down list of available
- Reset Count: select from 0 up to 9999999
- Click the 'APPLY' button at the bottom to save.

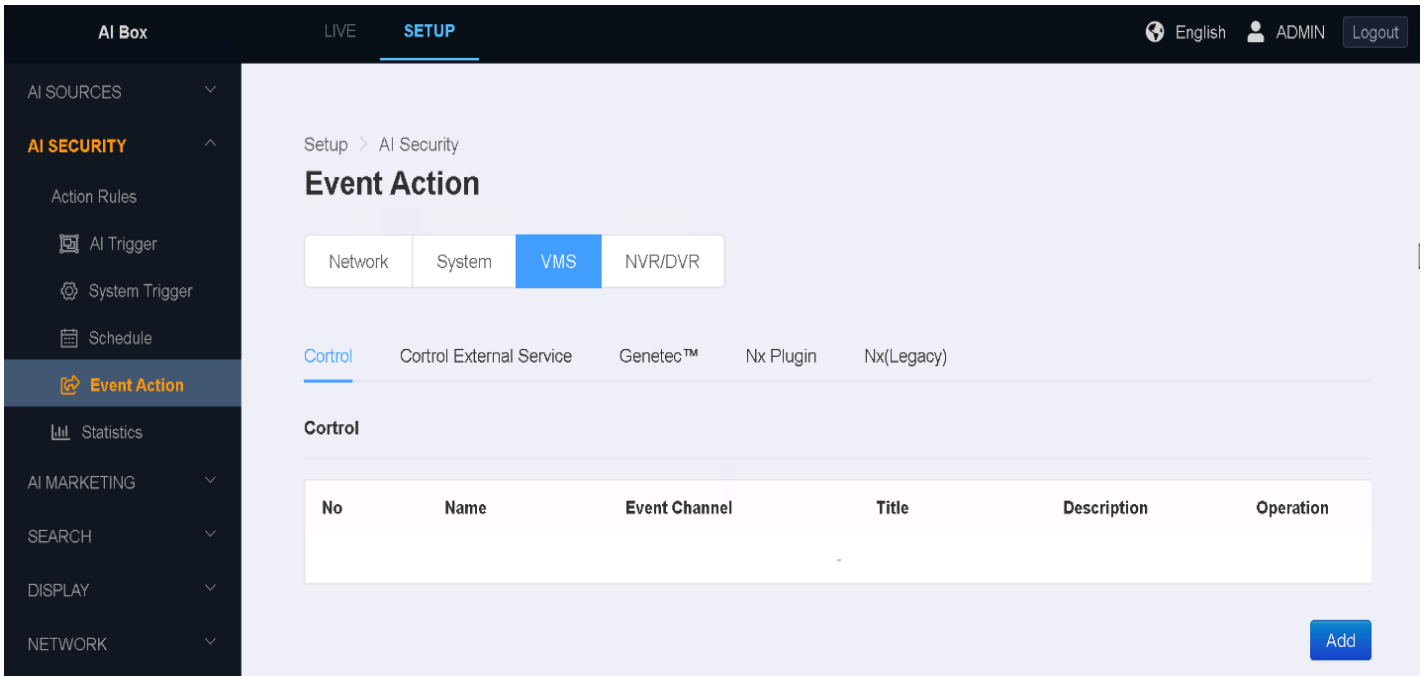


13. VMS: CORTROL

The ‘CORTROL’ action defines an event action to handshake with CORTROL.

To configure the ‘CORTROL’ event action, go to SETUP/AI Security/Event Action/VMS->CORTROL

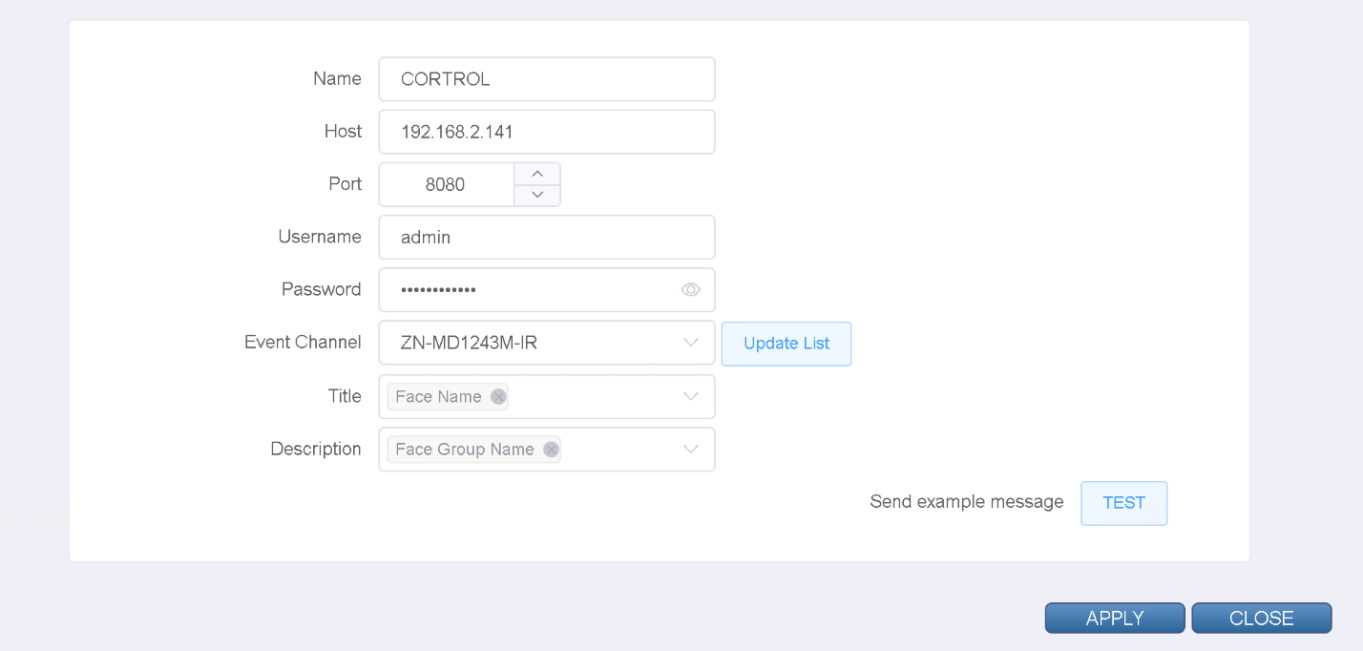
- Select ‘Add’ to create a CORTROL event action



- Name: Title the CORTROL event action according to intent
- Host: Enter the IP address of the target CORTROL server
- Port: Enter the communications port of the target CORTROL server
- Username: Enter the user credentials with CORTROL authentication
- Password: Enter the user credentials with CORTROL authentication
- Event Chanel: Select 'Update List'
    - Event channel will update to present a list of available CORTROL channels

- Title: Select from the drop-down list, example Rule Name, CH, Face Name…
- Description: Select from the drop-down list, example Rule Name, CH, Face Name…

- Click 'TEST' to confirm CORTROL/AI Box communications
- Click the 'APPLY' button at the bottom to save.

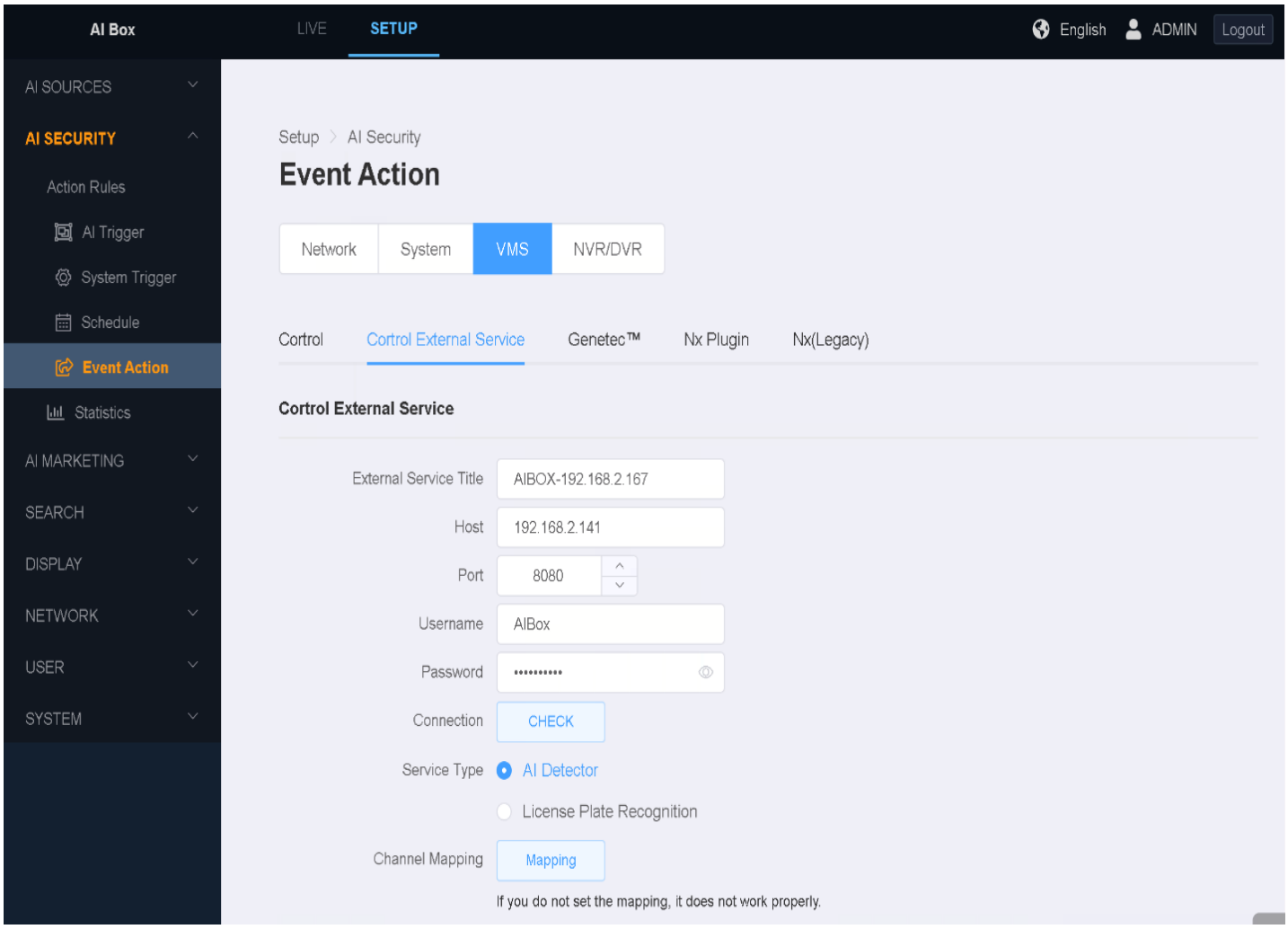


14. VMS: CORTROL External Service

The 'CORTROL External Service' action defines an event action to handshake with CORTROL.

To configure the 'CORTROL External Service' event action, go to SETUP/AI Security/Event Action/VMS->CORTROL External Service

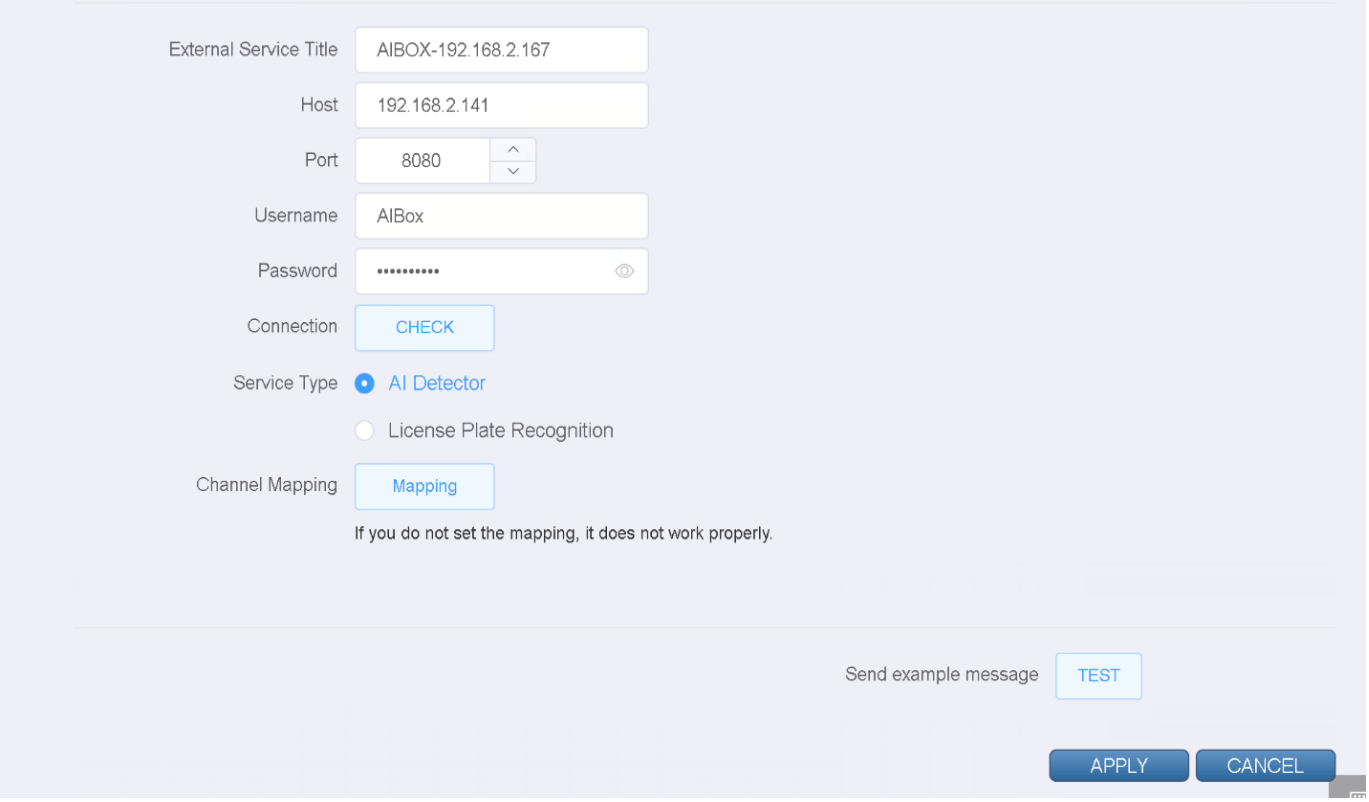
- Select 'Add' to create a CORTROL External Service event action



- External Service Title: Title the CORTROL External Service according to intent
- Host: Enter the IP address of the target CORTROL server
- Port: Enter the communications port of the target CORTROL server
- Username: Enter the user credentials with CORTROL authentication
- Password: Enter the user credentials with CORTROL authentication
- Connection: Select 'CHECK'
    - 'CHECK' will confirm communications between CORTROL and AI Box

- Service Type: Select either AI Detector, or License Plate Recognition
    - Currently only one service type per instance is supported
        - Only one instance is currently support for CORTROL External Service

- Channel Mapping: Select 'Mapping' for a listing of available video sources
- Click 'TEST' to confirm CORTROL/AI Box communications
- Click the 'APPLY' button at the bottom to save.

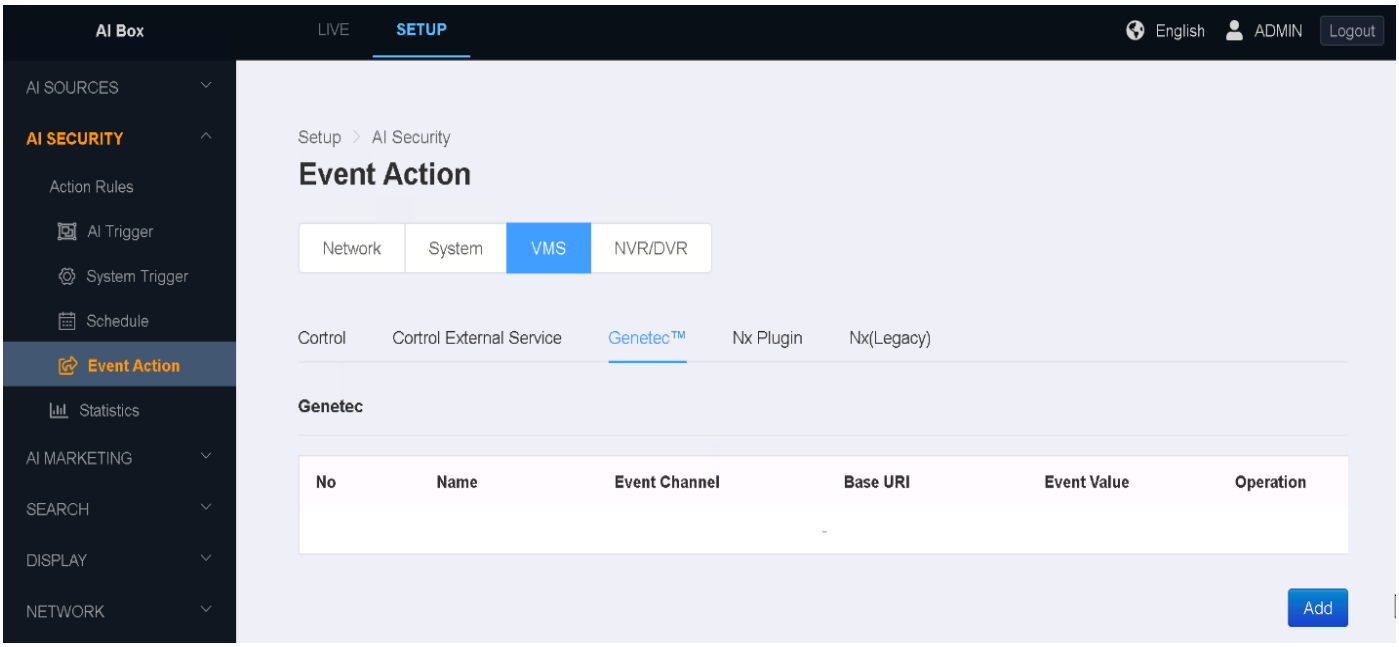


15. VMS: Genetec

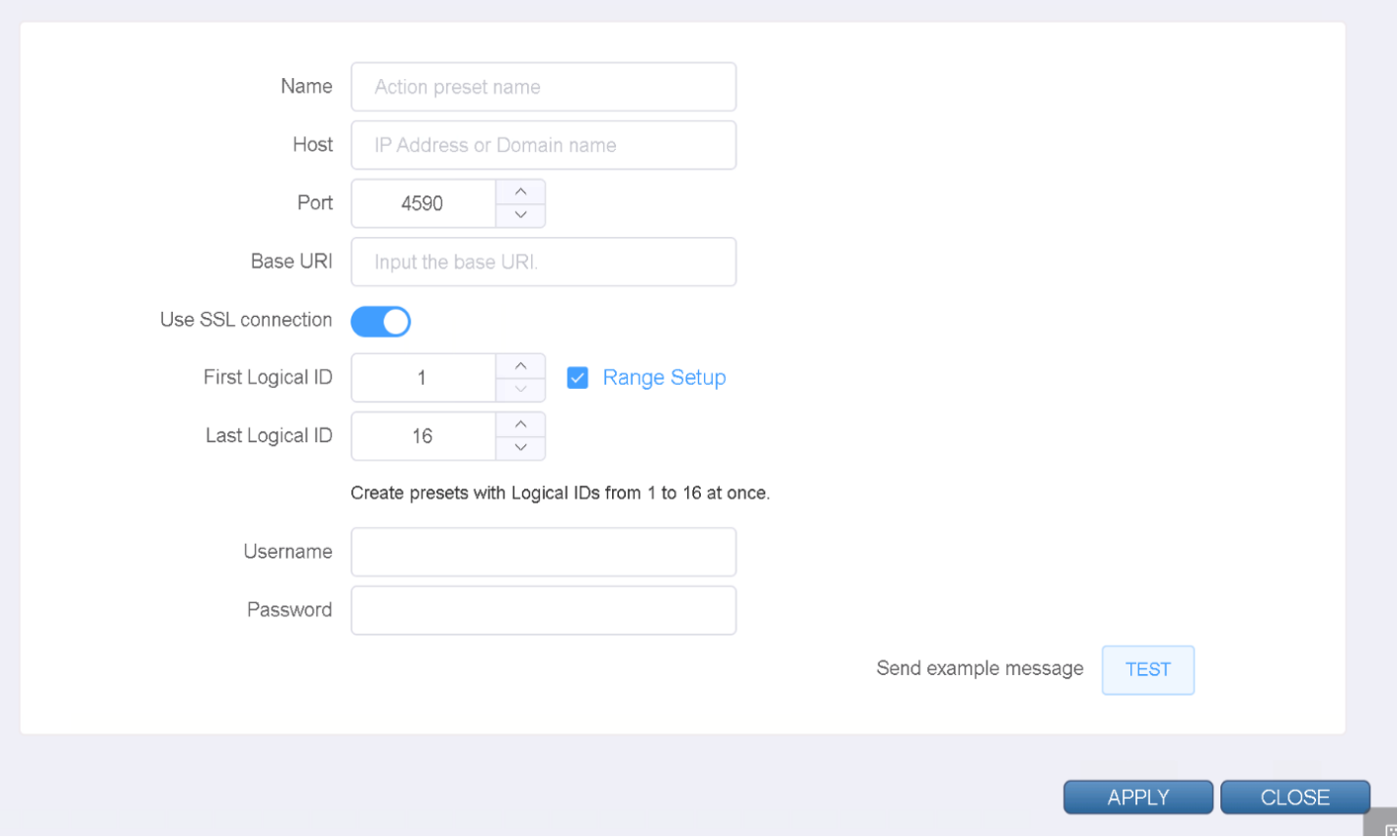
The ‘Genetec’ action defines an event action to handshake with Genetec.

To configure the ‘Genetec’ event action, go to SETUP/AI Security/Event Action/VMS->Genetec

- Select ‘Add’ to create an Genetec event action



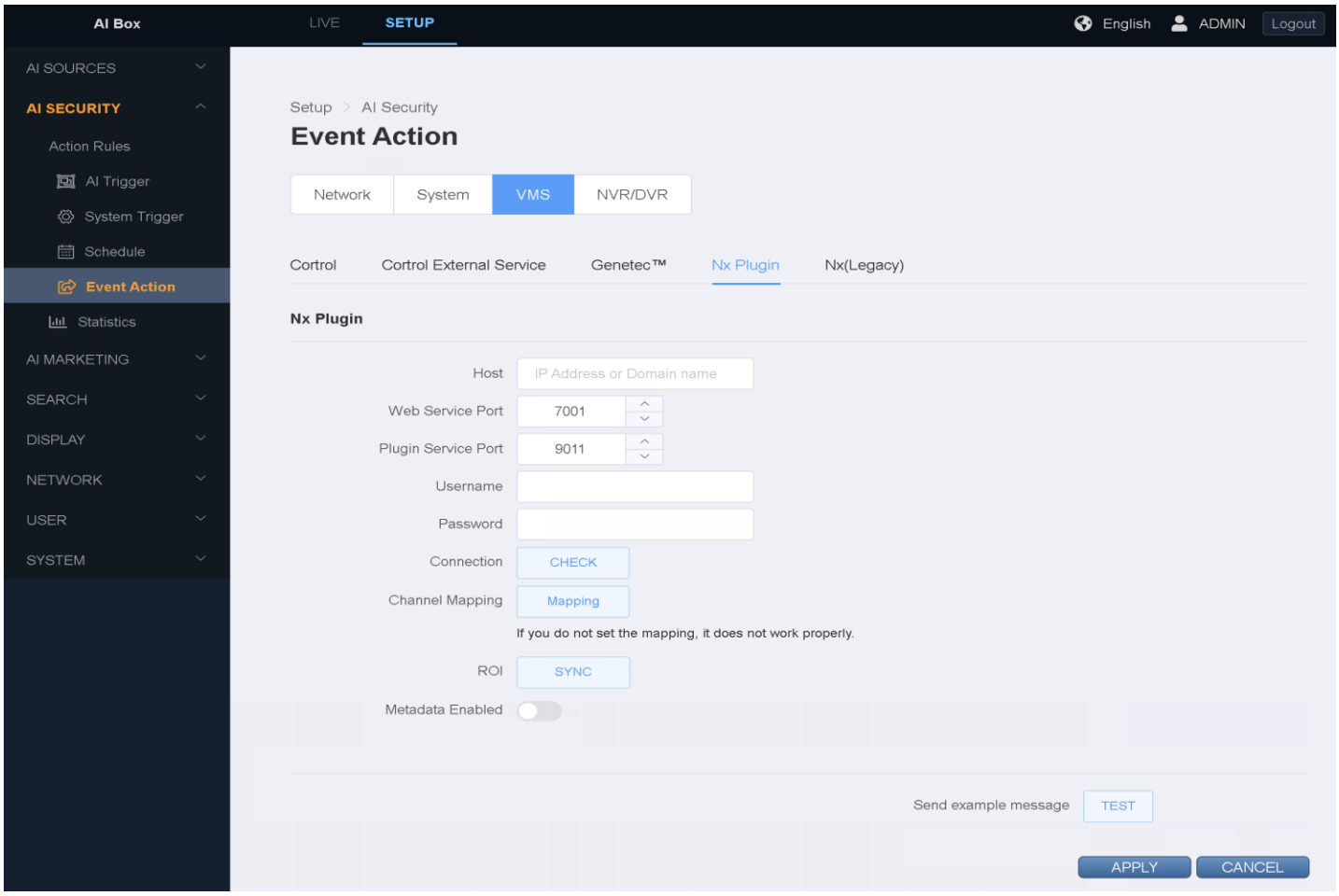
- Name: Title the Genetec event action according to intent
- Host: Enter the IP address of the target Genetec server
- Port: Enter the communications port of the target Genetec server
- Base URI: Input the Genetec base URI
- Use SSL connection: Select if the target Genetec server is using SSL
- First Logical ID: Input the first logical ID for Genetec server
- Last Logical ID: Input the last logical ID for Genetec server
- Username: Enter the user credentials with Genetec authentication
- Password: Enter the user credentials with Genetec authentication
- Click 'TEST' to confirm Genetec/AI Box communications
- Click the 'APPLY' button at the bottom to save.



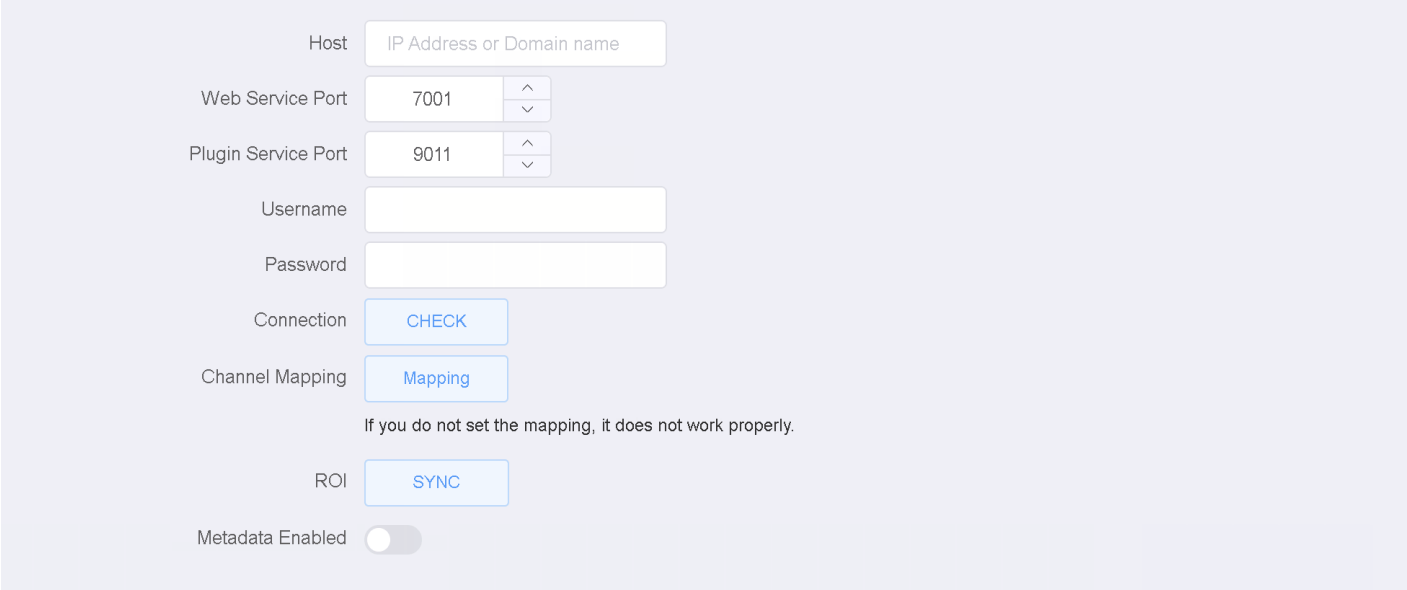
16. VMS: Nx Plugin

The 'Nx Plugin' action defines an event action to handshake via the Nx Plugin.

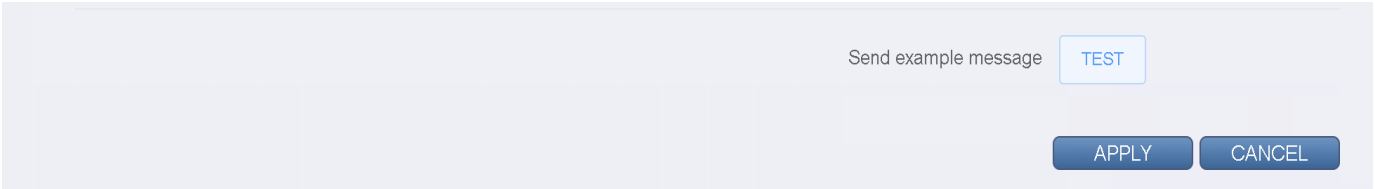
To configure the 'Nx Plugin' event action, go to SETUP/AI Security/Event Action/VMS->Nx Plugin



- Host: Enter the IP address or domain name of the target Nx server
- Web Service Port: Enter the web communications port of the target Nx server
- Plugin Service Port: Enter the plugin communications port of the target Nx server
- Username: Enter the user credentials with Nx authentication
- Password: Enter the user credentials with Nx authentication
- Connection: Select 'CHECK' to confirm communications with the Nx server
- Channel Mapping: Select 'Mapping' for a listing of available video sources
- ROI: Select 'SYNC' to set synchronize the region of interest
- Metadata Enabled: Toggle either 'On' or 'Off' to allow metadata transmission



- Click 'TEST' to confirm Nx plugin/AI Box communications
- Click the 'APPLY' button at the bottom to save



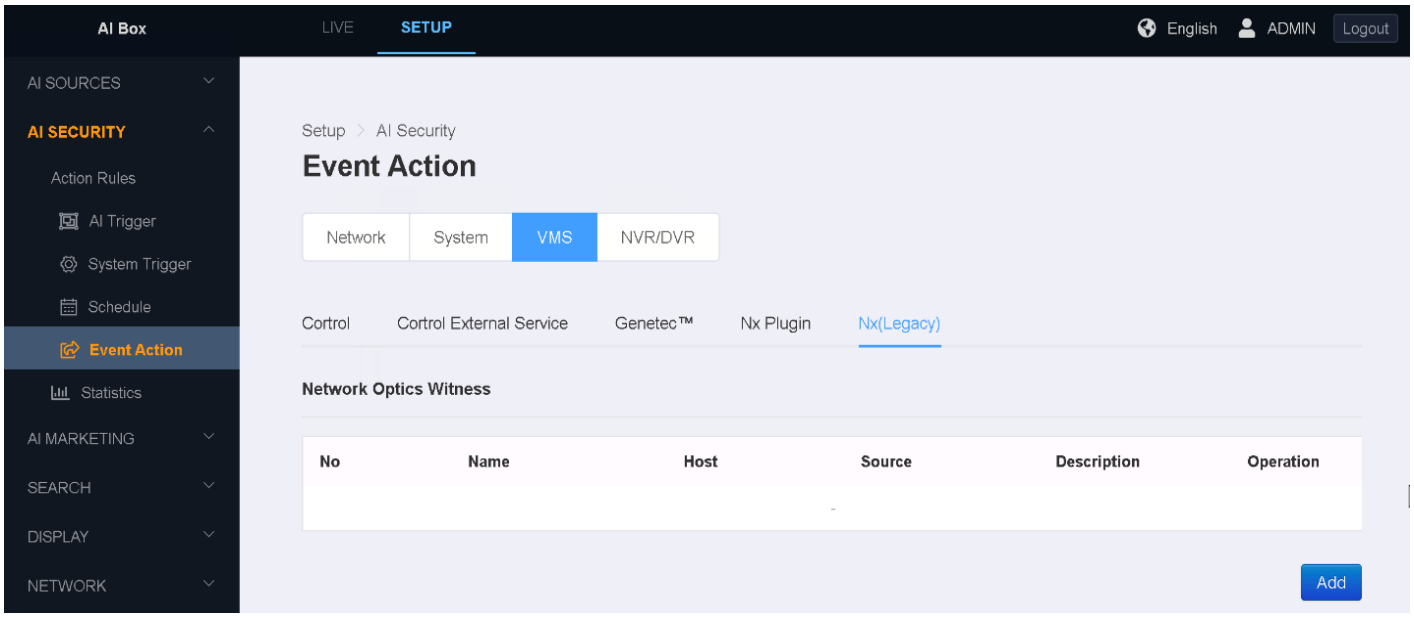
CORP HQ +1 (919) 230-8700 | WEST COAST +1 (310) 222-8600
ganzsecurity.com

17. VMS: Nx (Legacy)

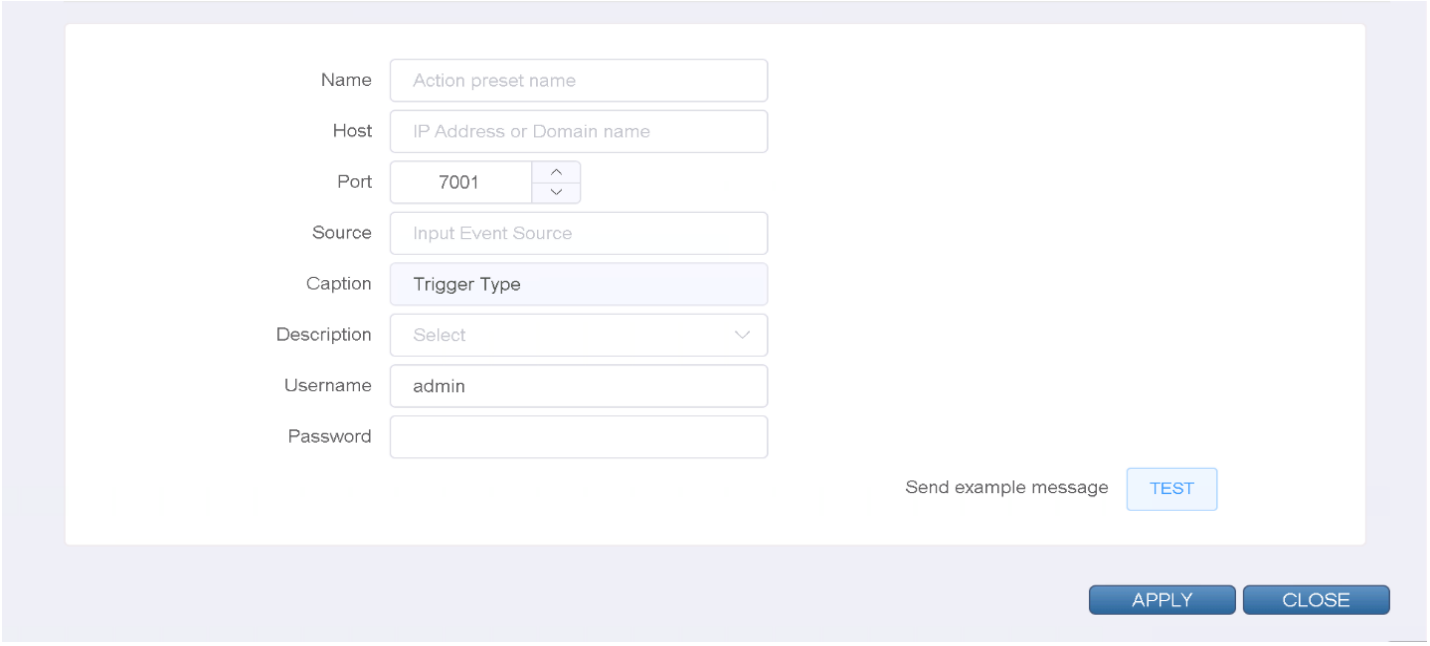
The 'Nx Legacy' action defines an event action to handshake by way of the Nx Legacy option.

To configure the 'Nx Legacy' event action, go to SETUP/AI Security/Event Action/VMS->Nx Legacy

- Select 'Add' to create an Nx Legacy event action



- Name: Title the Nx Legacy event action according to intent
- Host: Enter the IP address or domain name of the target Nx server
- Port: Enter the communications port of the target Nx server
- Source: Enter the Nx event source
- Caption: Currently only lists Trigger Type
- Description: Select from the drop-down list, example Rule Name, CH, Face Name…
- Username: Enter the user credentials with Nx authentication
- Password: Enter the user credentials with Nx authentication
- Click 'TEST' to confirm Nx Legacy/AI Box communications
- Click the 'APPLY' button at the bottom to save



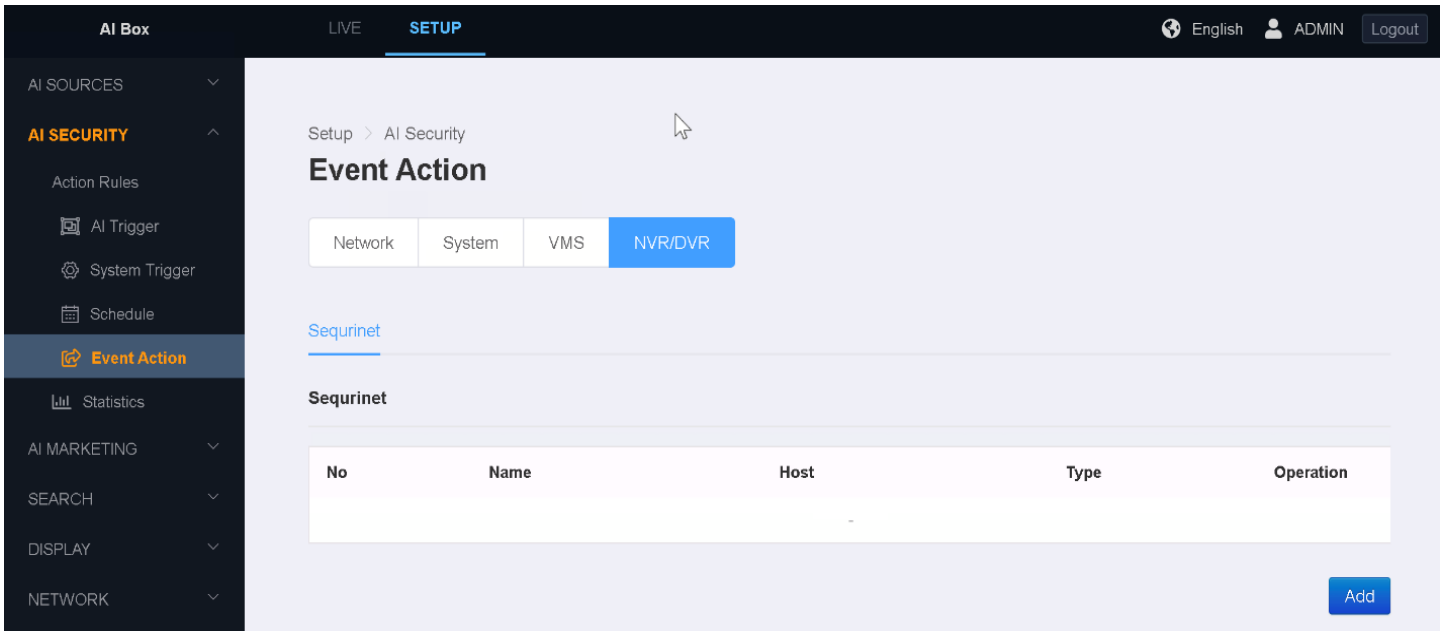
CORP HQ +1 (919) 230-8700 | WEST COAST +1 (310) 222-8600
ganzsecurity.com

18. NVR/DVR: Sequrinet

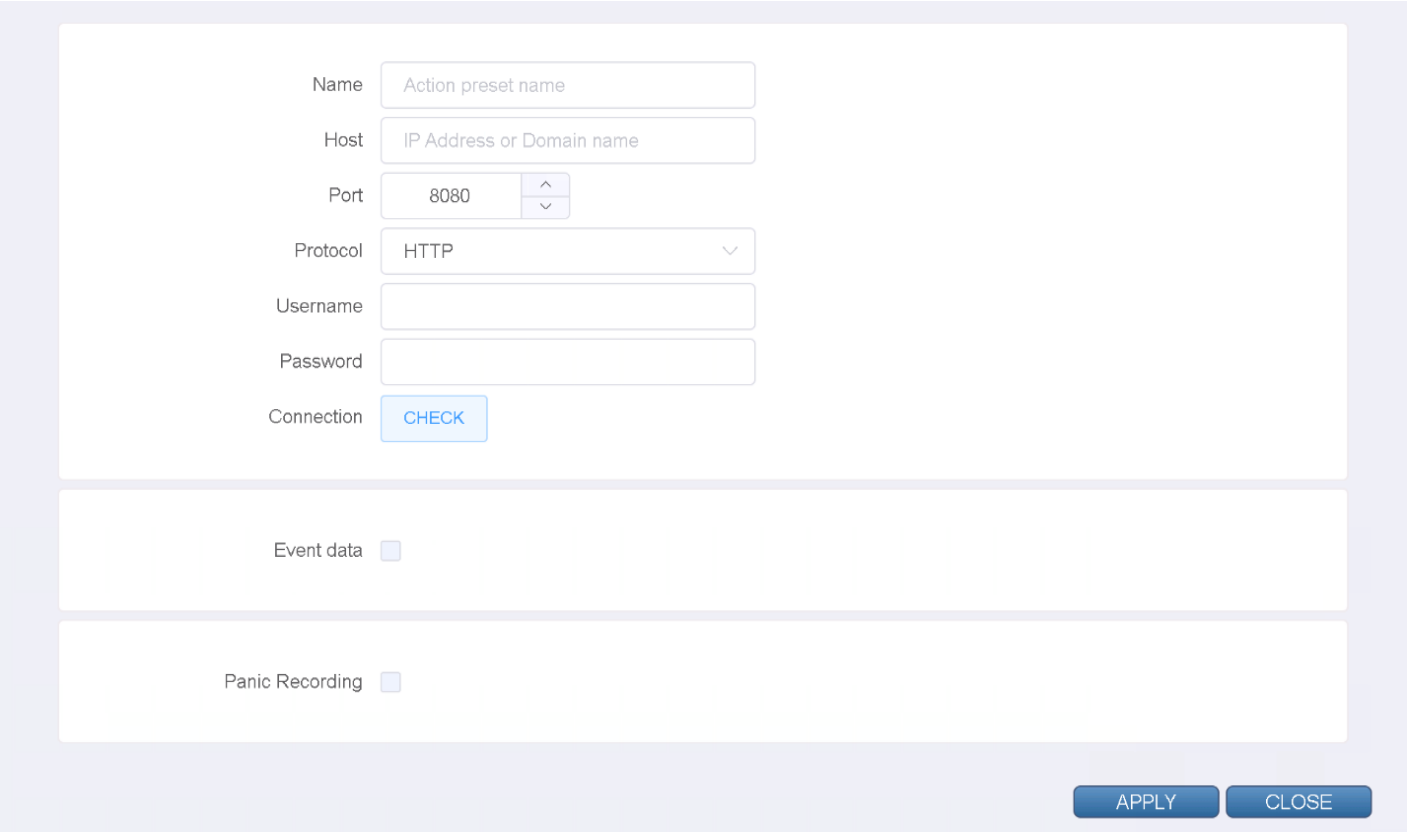
The 'Sequrinet' action defines an event action to handshake by way of the Ganz NVR/DVR Sequrinet option.

To configure the 'Sequrinet' event action, go to SETUP/AI Security/Event Action/NVR/DVR->Sequrinet

- Select 'Add' to create an Sequrinet event action



- Name: Title the Sequrinet event action according to intent
- Host: Enter the IP address or domain name of the target NVR/DVR
- Port: Enter the communications port of the target NVR/DVR
- Protocol: Enter the communications protocol, HTTP, HTTPS
- Username: Enter the user credentials with NVR/DVR authentication
- Password: Enter the user credentials with NVR/DVR authentication
- Click ‘CHECK’ to confirm NVR/DVR/AI Box communications
- Event Data: Select to enable ‘Event Data’ transmission
- Panic Recording: Select to enable ‘Panic Recording’ event data transmission
- Click the ‘APPLY’ button at the bottom to save



19. Network: Attribute Tokens

Attribute tokens and description

TRIGGER NO	Trigger Index
TRIGGER NAME	Trigger name
TRIGGER TYPE	Trigger type
CH	Channel
CH NAME	Channel Name
MAC	MAC Address
SYSTEM TIMESTAMP	System timestamp (UTC)
SYSTEM TIME ISO8601	System time (UTC)
SYSTEM TIME	System time
SYSTEM TIME %YYYY	4-digit year of the system time
SYSTEM TIME %YY	2-digit year of the system time
SYSTEM TIME %mm	Month of system time
SYSTEM TIME %dd	Date of system time
SYSTEM TIME %HH	Hour of system time
SYSTEM TIME %MM	Minute of system time
SYSTEM TIME %SS	Second of system time
SYSTEM TIME %MS	Millisecond of system time
VIDEO TIMESTAMP	Camera timestamp (UTC)
VIDEO TIME ISO8601	Camera time (UTC)
VIDEO TIME STRING	Camera time
VIDEO TIME %YYYY	4-digit year of the system time
VIDEO TIME %YY	2-digit year of the system time
VIDEO TIME %mm	Month of system time
VIDEO TIME %dd	Date of system time
VIDEO TIME %HH	Hour of system time
VIDEO TIME %MM	Minute of system time
VIDEO TIME %SS	Second of system time
VIDEO TIME %MS	Millisecond of system time
RULE NO	Rule index
RULE NAME	Rule name
OCCUPANCY COUNT	Detected occupancy object counts
MORE THAN	More than setting value
FEWER THAN	Fewer than setting value
COUNT N	Count N setting value
LOITERING DURACTION	Detected loitering direction secs
COMBINED COUNT	Combined count of AI Counter
RECOGNITION MODE	Recognition Mode
FORWARD COUNT	Forward count
REVERSE COUNT	Reverse count

# OF OBJECTS	Objects count
LIST OBJECTS	Objects enumeration
LIST OBJECTS [PARAM=COMMA]	Comma separated objects enumeration
::OBJ[INDEX]	Object iteration index
::OBJ[TRACK ID]	Object track id
::OBJ[CLASS]	Object class name
::OBJ[SCORE]	Object confidence score
::OBJ[DIRECTION]	Object direction
::OBJ[DIR_LB]	Object direction label
::OBJ[BBOX_X1]	Object bbox top-left x position
::OBJ[BBOX_Y1]	Object bbox top-left y position
::OBJ[BBOX_X2]	Object bbox top-right x position
::OBJ[BBOX_Y2]	Object bbox top-right y position
::OBJ[FACE_ID]	Face id
::OBJ[FACE_NAME]	Face name
::OBJ[FACE_NOTE]	Face note
::OBJ[FACE_GROUP_NAME]	Face group name
::OBJ[FACE_AGE]	Age guessed by face
::OBJ[FACE_GENDER]	Gender guessed by face
::OBJ[FACE_MASK]	Mask
::OBJ[FACE_GLASSES]	Glasses
::OBJ[LICENSE_PLATE_TEXT]	LP number
::OBJ[LP_NUMBER_ONLY]	LP number only
::OBJ[LP_COUNTRY_CODE]	LP country code
::OBJ[LP_GROUP_NAME]	LP group name
::OBJ[LP_ID]	LP id
::OBJ[LP_DB_NUMBER]	Matching LP number
::OBJ[LP_NAME]	LP owner name
::OBJ[LP_PHONE]	LP phone number
::OBJ[LP_NOTE]	LP note
MORE THAN OF Do not Enter	More than setting value
FEWER THAN OF Do not Enter	Fewer than setting value
MORE THAN OF Please Enter	More than setting value
FEWER THAN OF Please Enter	Fewer than setting value
MORE THAN OF Display	More than setting value
FEWER THEAN OF Display	Fewer than setting value

7. Statistics

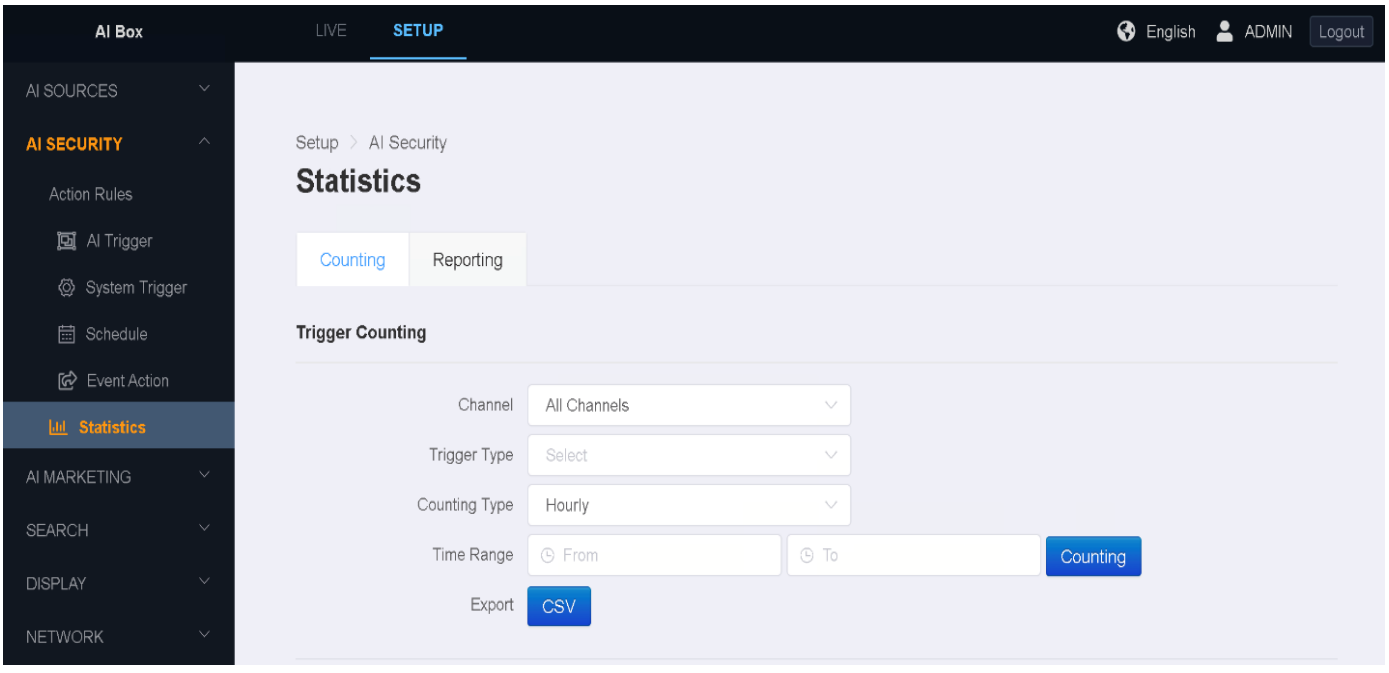
This item can be viewed by processing the number of triggers of AI security items.

1. Statistics: Counting

To configure a 'Statistical Counting', go to SETUP/AI Security/Statistics->Counting

- Channel: Select the desired channel from the list of available channels
- Trigger Type: Select the desired trigger type from the list of available triggers
- Counting Type: Select to process statistics 'Hourly' or 'Daily'
- Time Range: Set the time interval for processing
    - From: Select and set either by hour or by date for the start time
    - To: Select and set either by hour or by date for the end time
    - Counting: Press to display the searched content at the bottom

- Export: Select 'CSV'
    - Download the searched contents in CSV file format.

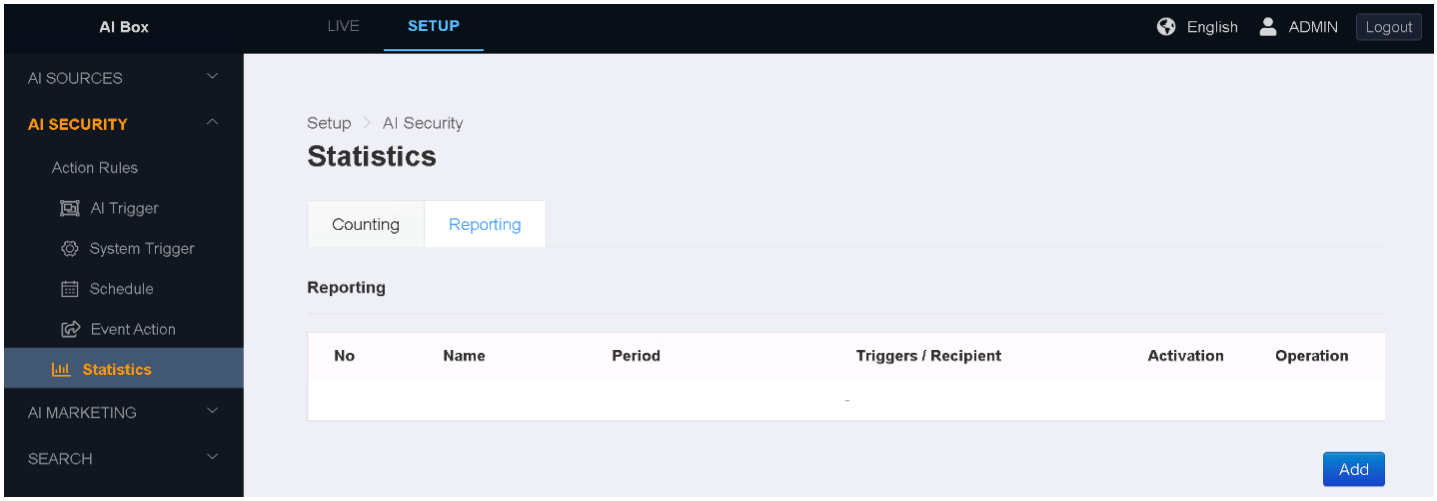


2. Statistics: Reporting

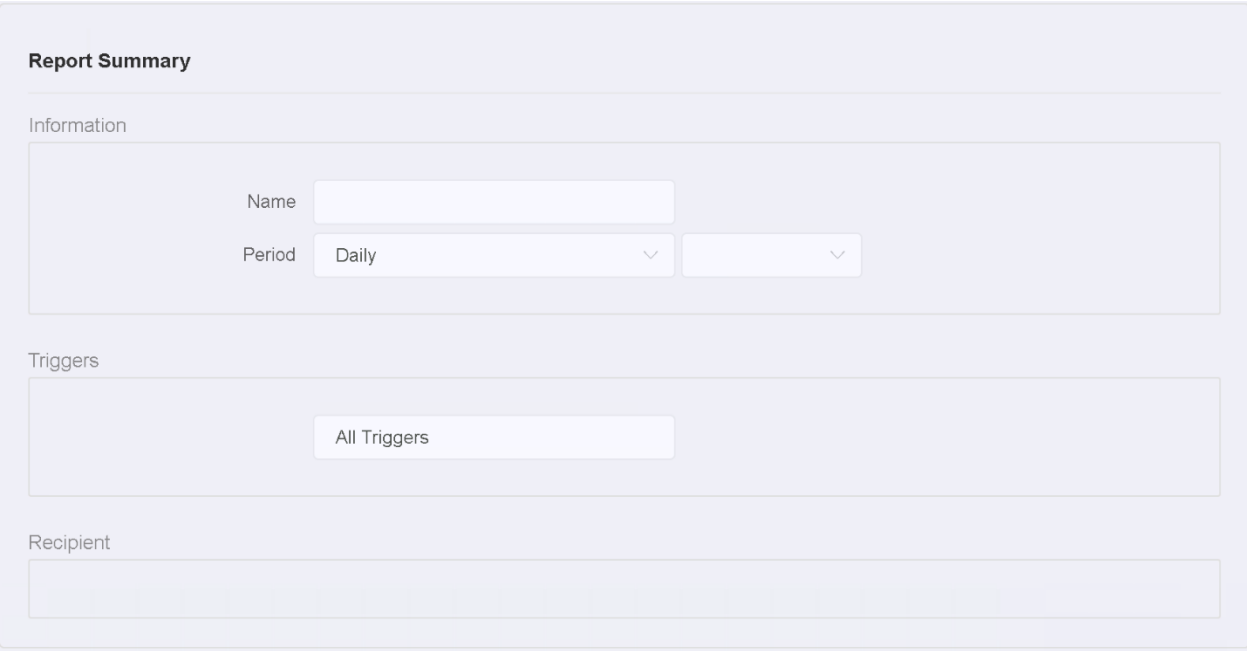
A function to periodically send statistics data to a specified recipient or automatically upload the data to FTP.

To configure a 'Statistical Reporting', go to SETUP/AI Security/Statistics->Reporting

- Select 'Add' to create a statistical report



- Report Summary: This section will be populated upon completion of the report setup

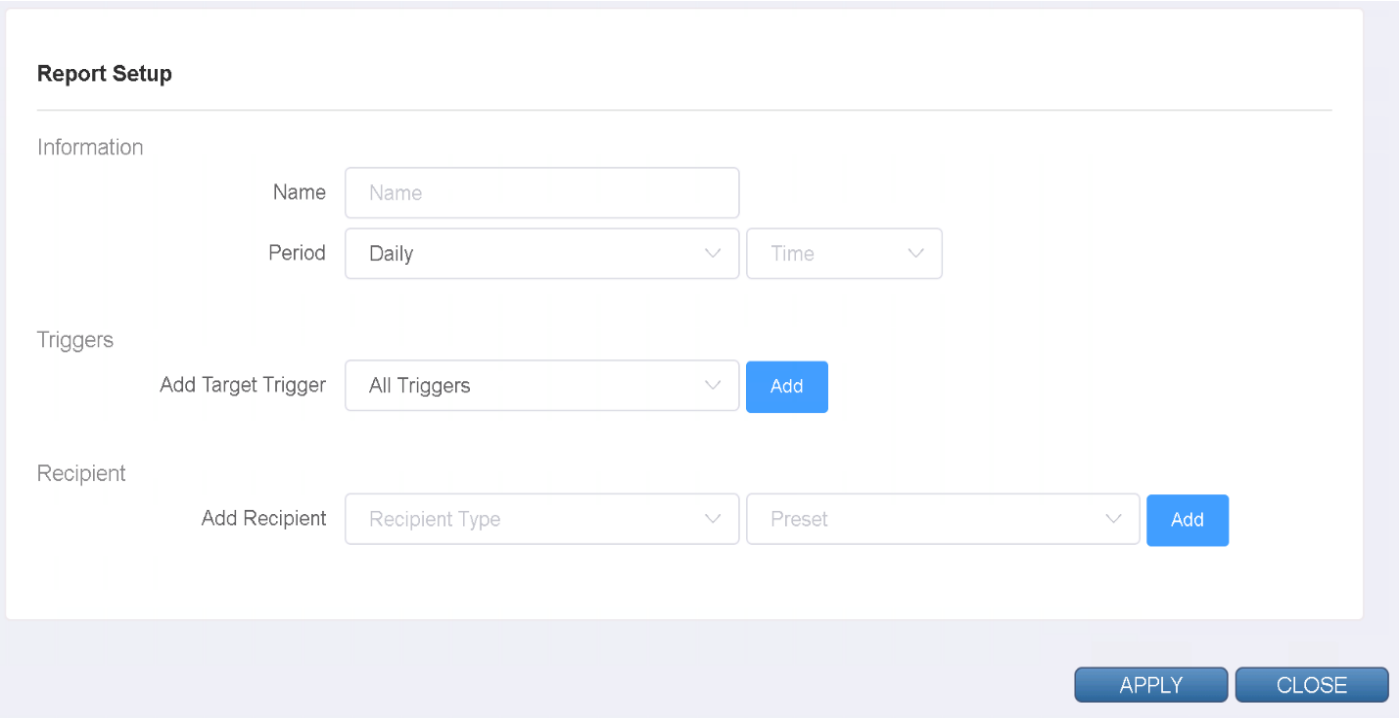


- Name: Title the report name according to intent
- Period: Set to Hourly, Daily, Weekly, Monthly
    - Time: Set the time per the hourly, daily, weekly, or monthly selection
    - This is the time at which the report will be emailed to a recipient

- Add Target Trigger: Select from the list of available triggers
    - Note: some triggers may involve selecting an associated preset
    - Select 'Add' to add the selected trigger to the report
    - Repeat the above sets if additional triggers are to be included

- Add Recipient: Select from Email, FTP, or S3
    - Note: a selected recipient may involve selecting an associated preset
        - Example: Selecting email will require selecting an email recipient
        - Select 'Add' to add the recipient to the report

- Select 'Apply' to complete the report setup



CORP HQ +1 (919) 230-8700 | WEST COAST +1 (310) 222-8600

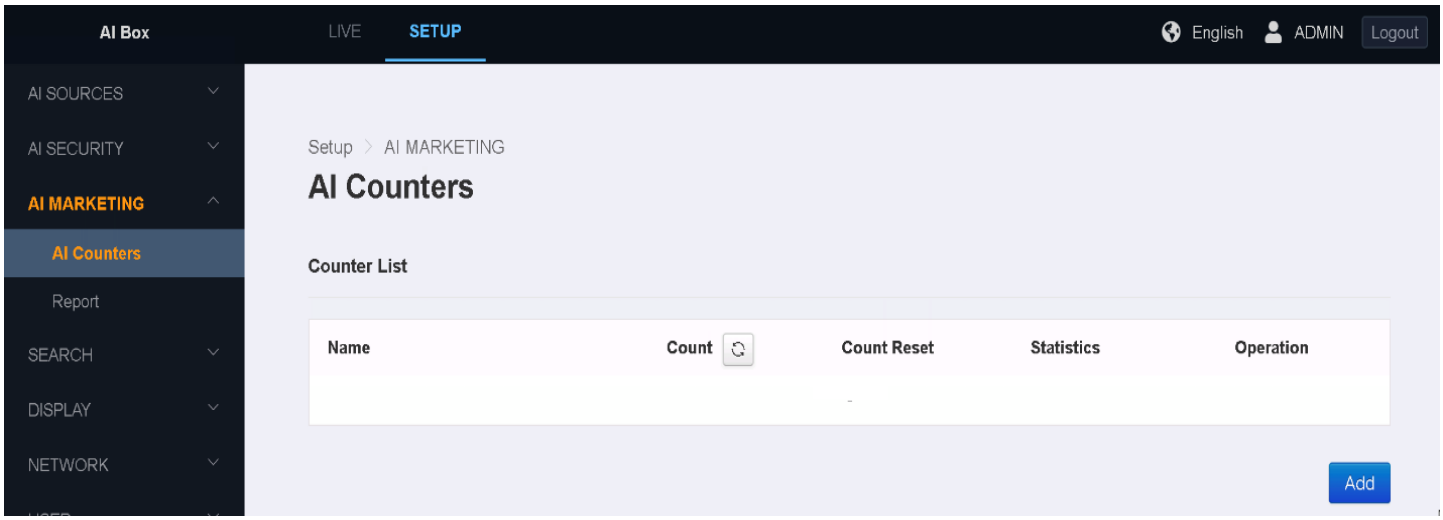
7. AI Marketing

1. AI Marketing: AI Counters

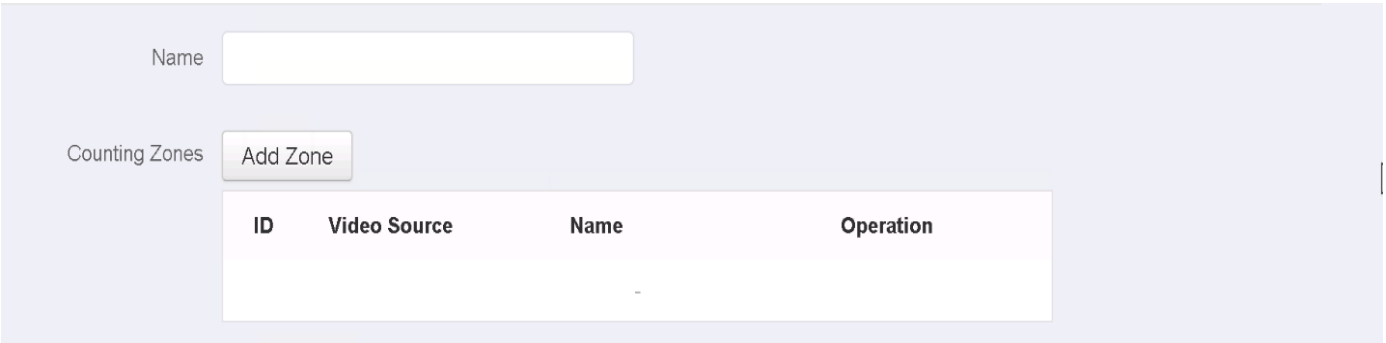
This item can be viewed by processing the number of triggers from AI security items.

To configure 'AI Counters', go to SETUP/AI Marketing/AI Counters

- Select 'Add' to create an AI Counter



- Name: Title the AI Counter name according to intent
- Counting Zone: Click on 'Add Zone'
    - A secondary screen with video source selection will popup



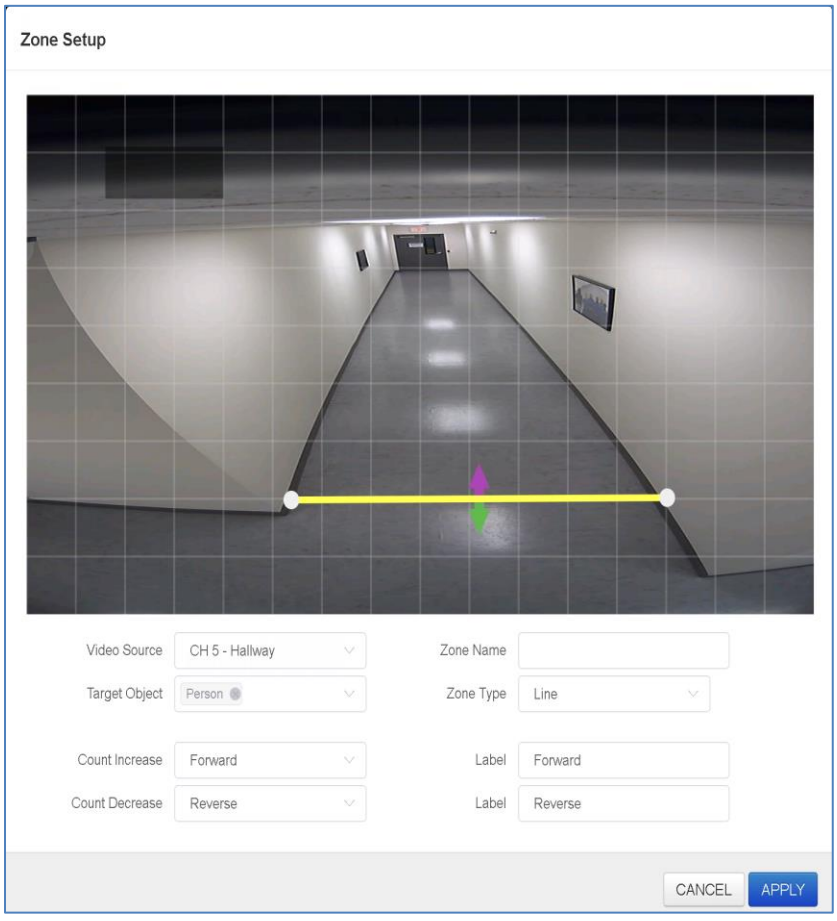
- Video Source: Select from the list of available video sources
- Zone Name: Title the zone name according to intent

- Target Object: Select from the list of available target analytics
    - Note: available analytics are associated with the selected video source

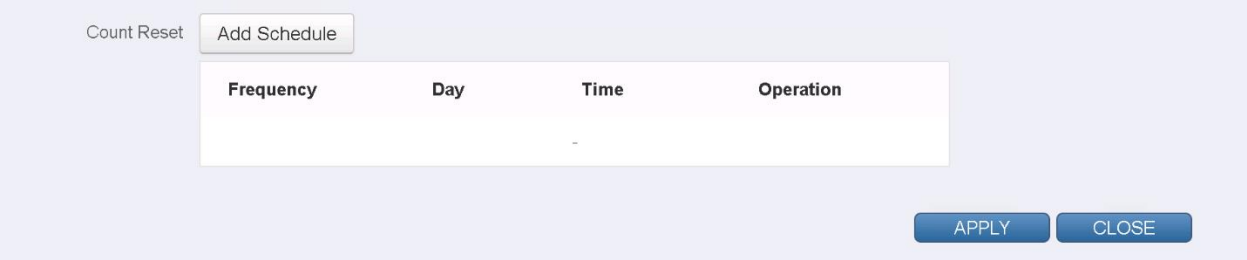
- Zone Type: Select either 'Line' or 'Area' according to intent
    - Note: if 'Line' is selected, the directional arrows are 'Green' and 'Purple'
        - 'Green' for forward and 'Purple' for reverse

- Count Increase: Based on selected direction, /None', 'Both', 'Forward', 'Reverse'
- Label Forward: Label the count name according to intent

- Count Decrease: Based on selected direction, /None', 'Both', 'Forward', 'Reverse'
- Label Reverse: Label the count name according to intent
- Select 'Apply' to save the AI counter and return to the prior AI Counter window

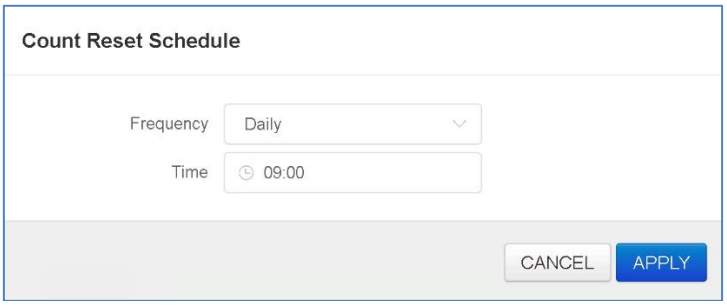


- When it is needed, an option of implementing a 'Count Reset' is possible
- Count Reset: Click on 'Add Schedule'
    - A secondary screen for creating a Count Reset Schedule will popup



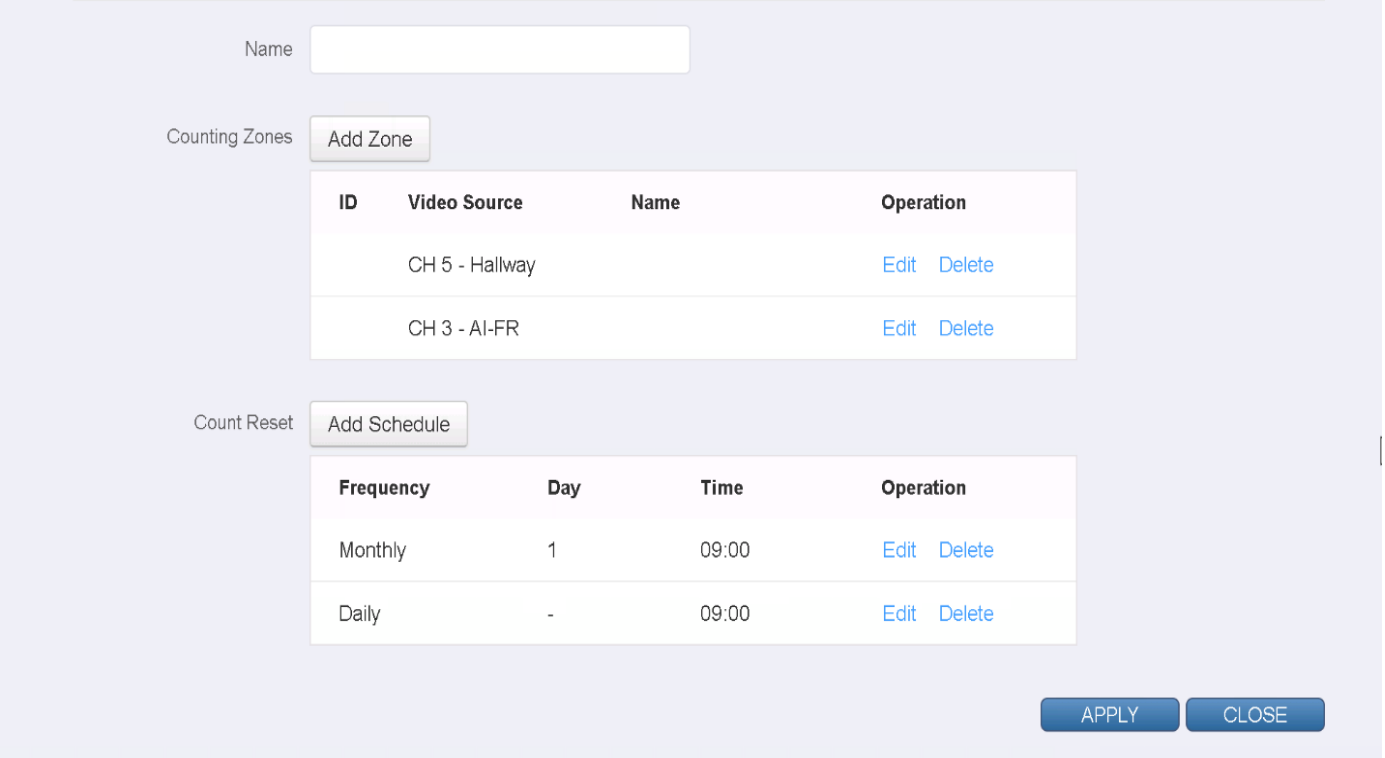
- Frequency: Select 'Daily', 'Weekly', or 'Monthly'
    - Daily selected: Enter a target 'Time' in hour, and or minutes
    - Weekly selected: Enter a target 'Day(s) of the week' + 'Time'
    - Monthly selected: Enter a target 'Day' of the week + 'Time'

- Select 'Apply' to save the Count Reset Schedule



- Note: Multiple Zones, and Schedules may be created, be mindful of intent
  - Selecting 'Edit' will allow editing of listed zones, and or schedules

- Select 'Apply' to save the AI Count

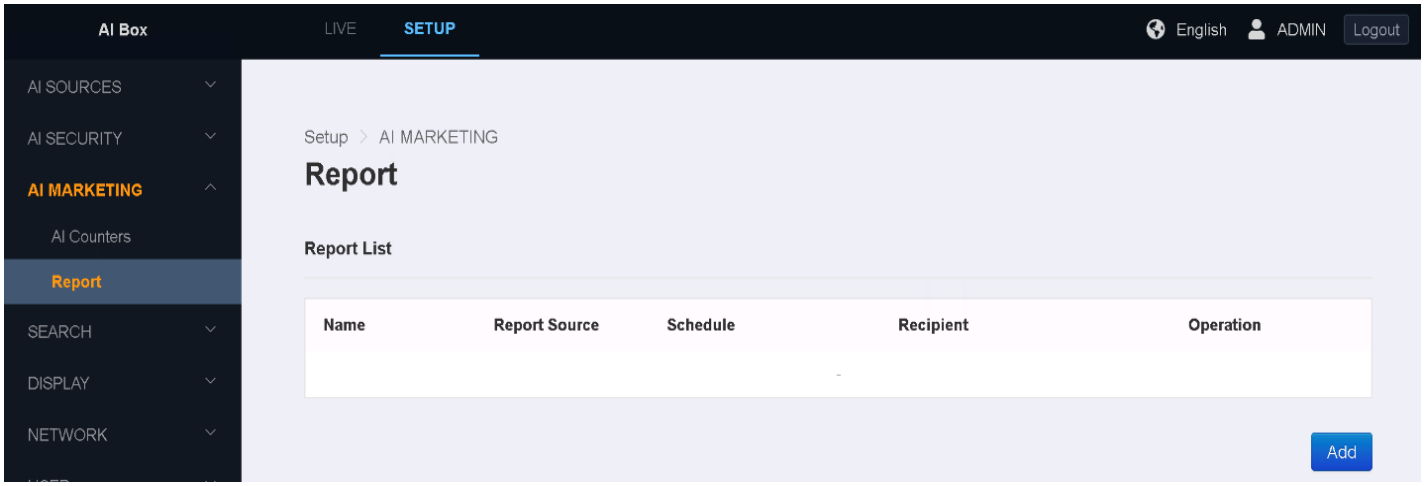


8. AI Marketing: Report

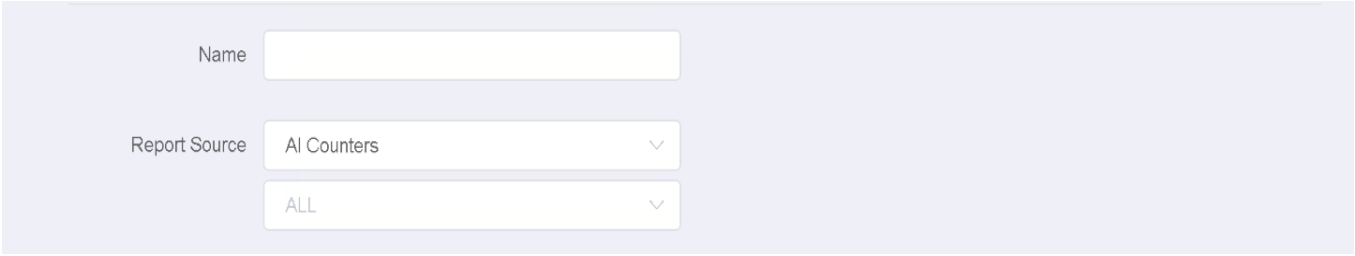
This item can be viewed by processing the number of triggers from AI security items.

To configure a 'Report', go to SETUP/AI Marketing/Report

- Select 'Add' to create a Report



- Name: Name the 'Report' according to intent
- Report Source: Default is AI Counters
    - Optionally select 'All' or from available list of AI Counters



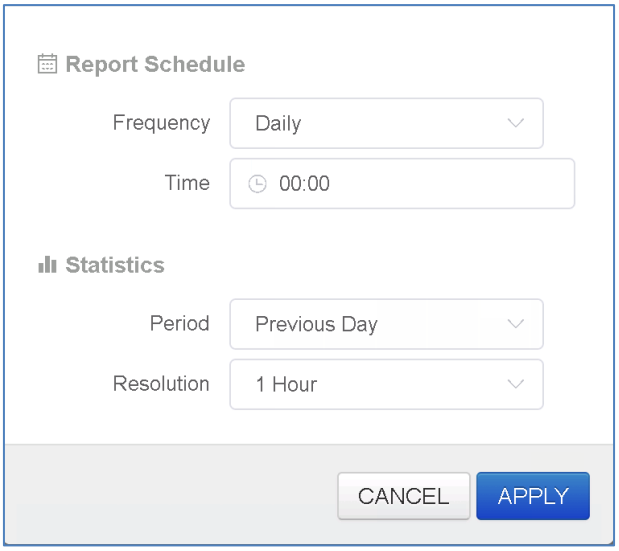
- Schedule: Select ‘Add Schedule’
    - A secondary screen for creating a Report Schedule will popup

- Frequency: Select ‘Every 5 minutes’, ‘Hourly’, ‘Daily’, ‘Weekly’, or ‘Monthly’
- Time: Will default per selection of ‘frequency’
    - Every 5 minutes selected: No modification currently possible
    - Hourly selected: Select from ‘:05’ through ‘:55’ minutes in 5-minute intervals
    - Daily selected: Select within a 24-hour format ‘00:00’
    - Weekly selected: Select the ‘Day of the week’
    - Monthly selected: Select from 1 through 31 for the ‘Day’ of the month

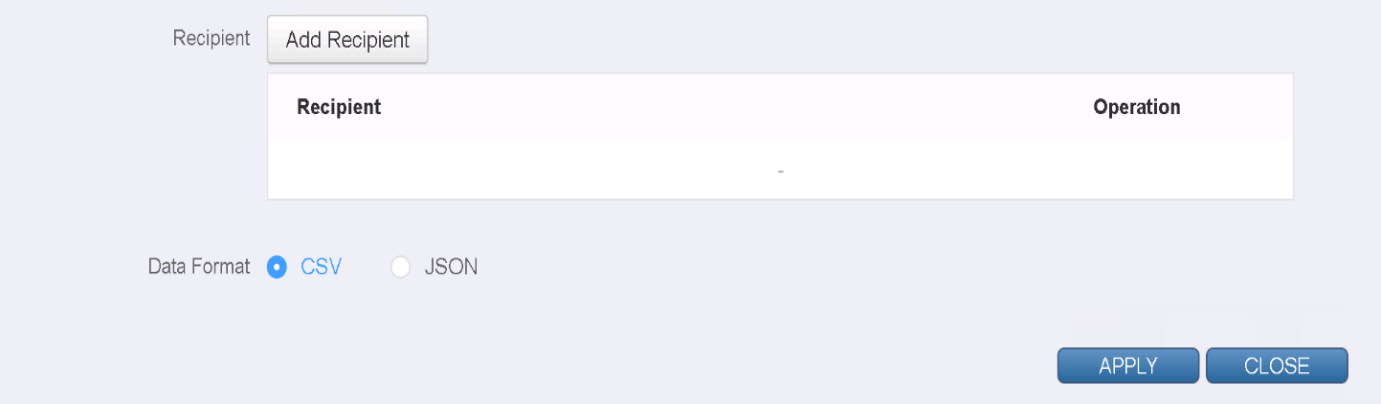
- Period: Will default per selection of ‘Frequency’
    - Previous 5 Minute
    - Previous Hour
    - Previous Day
    - Previous Week
    - Previous Month

- Resolution: Will default per selection of ‘Frequency’
    - 5 Minute
    - 15 Minute
    - 30 Minute
    - 1 Hour
    - 1 Day

- Select ‘Apply’ to save the Report Schedule



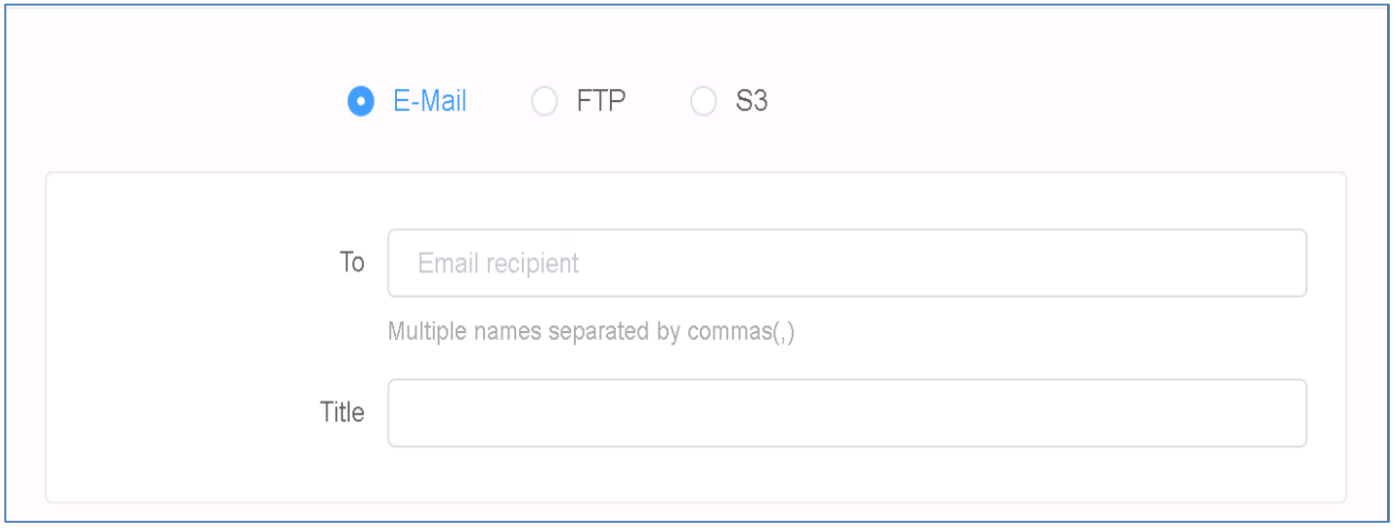
- Recipient: Select 'Add Recipient'
  - A secondary screen for creating a recipient(s) will popup



There are three possible recipients for a 'Report' to be sent to. Recipients include 'E-Mail', 'FTP', and 'S3'. Each recipient has its own required configuration needs.

1. Recipient: E-Mail

- To: Enter an email recipient (Separate by comma if multiple recipients)
- Title: Title the E-Mail according to intent



- Name: Title the SMTP server according to intent
- Provider: Select the email service provider
  - Options include 'Gmail', 'Hotmail', 'Yahoo', 'Sureview', 'Sentinel'
  - Select 'Custom' if the service provider you want to use is not listed

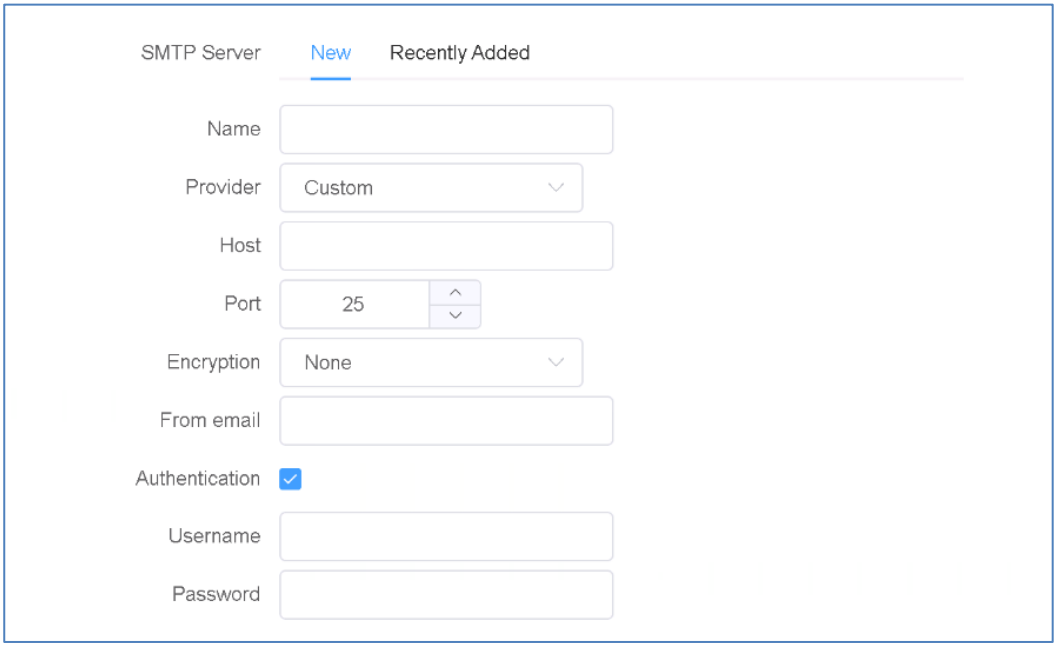
- Host: Input the SMTP server address
  - Example: smtp.gmail.com

- Port: Input the communication port for the SMTP server
    - SMTP port (Default): 25
    - SMTP port (TLS): 587
    - SMTP port (SSL): 465

- Encryption: The encryption is predetermined by the SMTP port requirement
  - The sending email may by encrypted as 'None', 'TLS', or 'SSL'

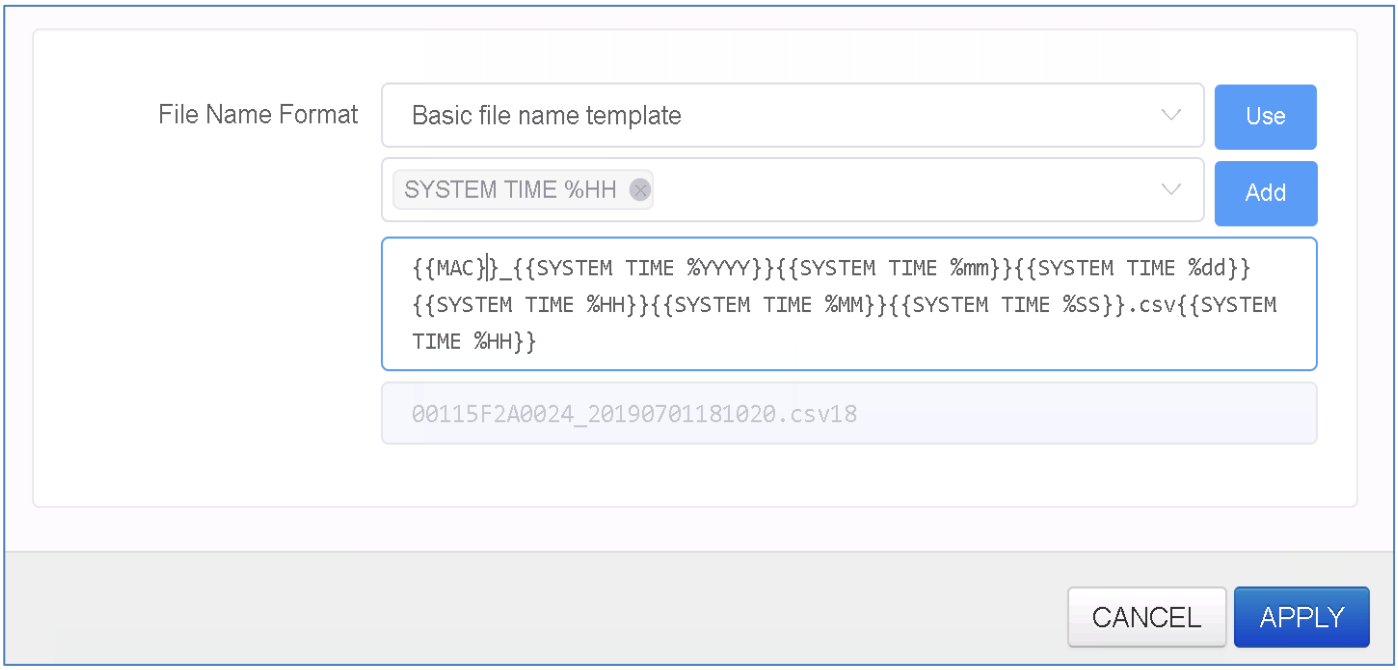
- From email: email address used to indicate who is sending the email
  - Does not have to be the SMTP email address
  - Email sender should denote person of authority behind AI Box administration

- Authentication: Check box if SMTP email account user credentials are required
  - When box is checked; SMTP account Username, and Password are required



- File Name: Edit the emailable file name format
  - Use template: Configure the message by using a template
    - ‘Custom’ and ‘Basic file name template’ available
    - Select ‘Use’ to add the template to the editable preview message box
  - Add an attribute token; Tokens list at end of ‘Events Actions’ section
  - Select ‘Add’ to add an attribute token to the email message

- Confirm email message contents within the editable preview option
- Click the ‘APPLY’ button at the bottom to save.

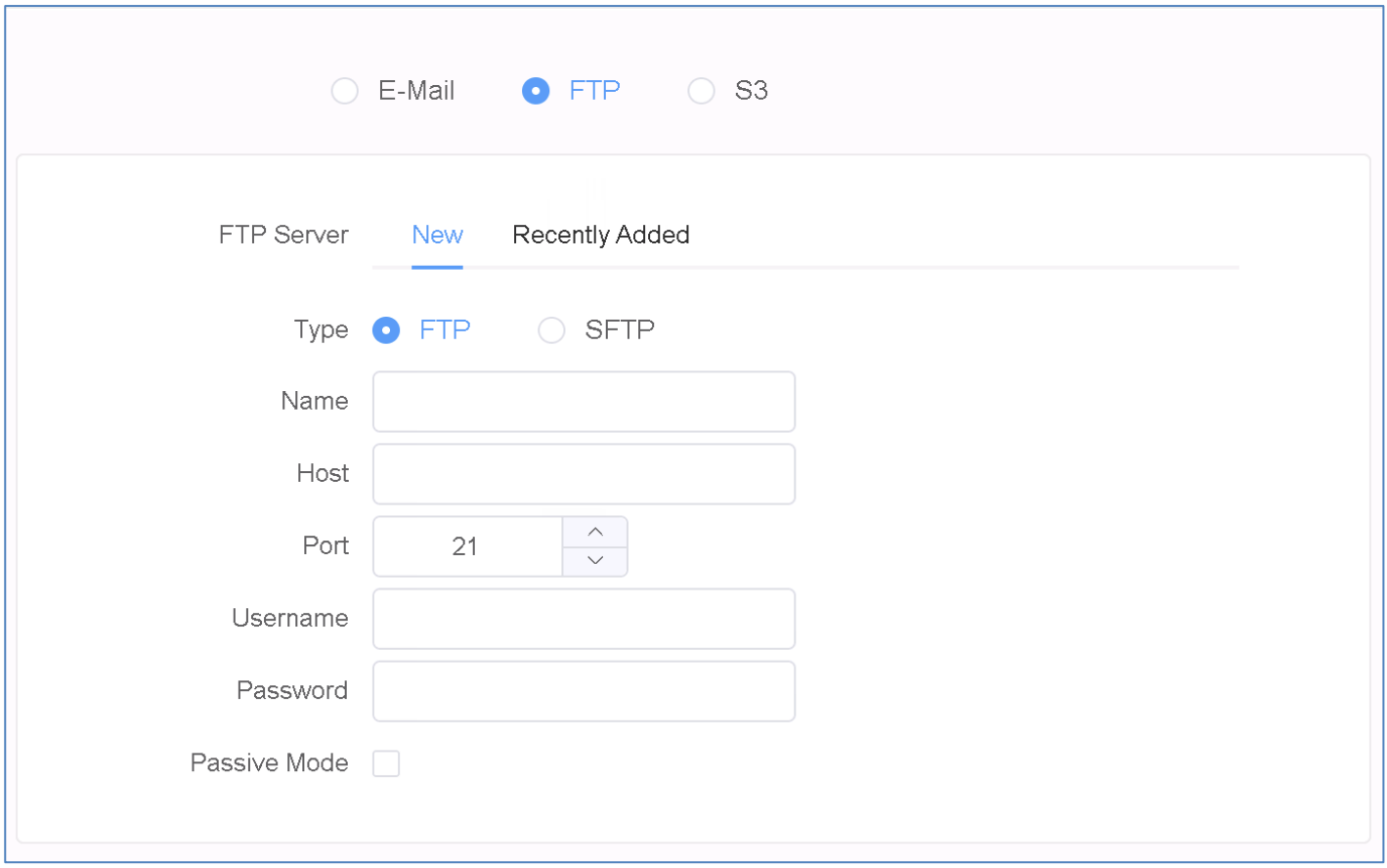


2. Recipient: FTP

- Type: Select 'FTP' or 'SFTP' based on nature of server connection
- Name: Title the FTP server according to intent
- Host: Input the SMTP server address
    - Example: smtp.gmail.com

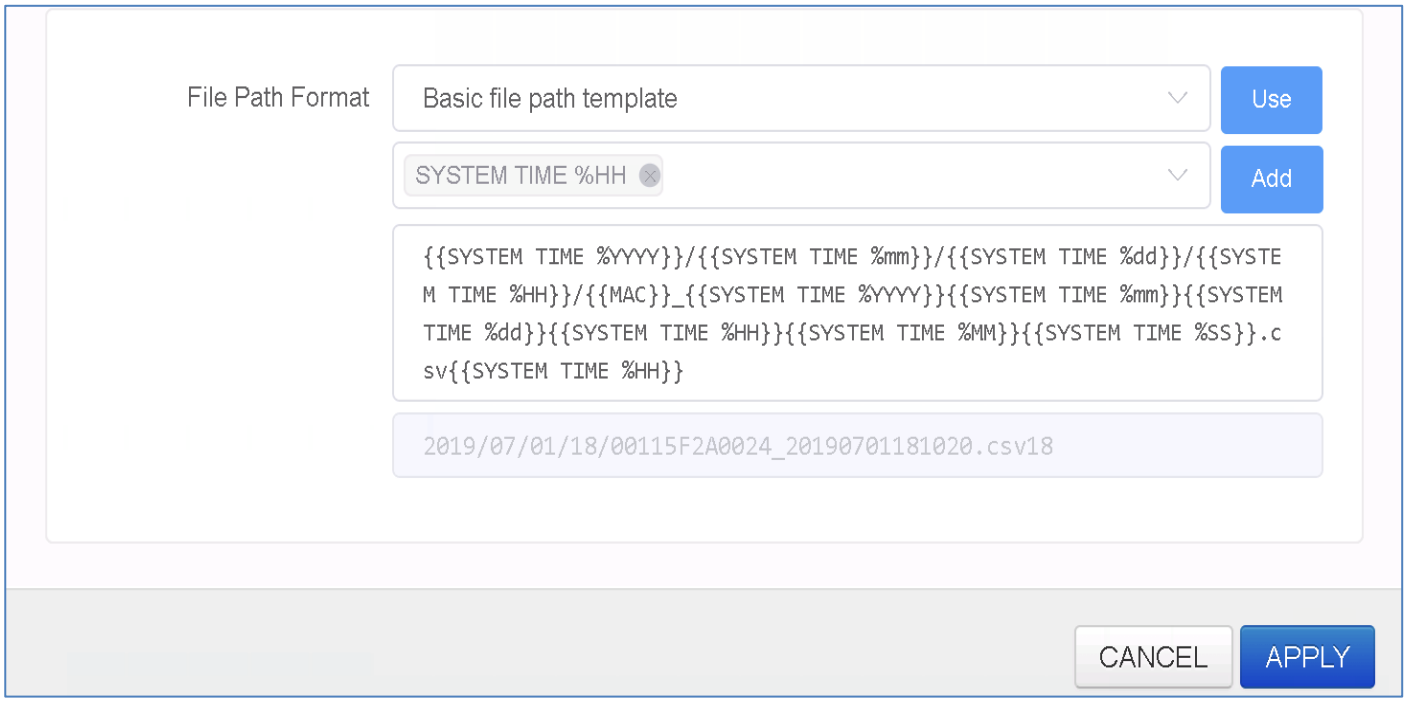
- Port: Input the communication port for the FTP server
    - FTP port (Default): 25

- Username: Enter the FTP username credentials
- Password: Enter the FTP account password
- Passive Mode: Check the box to enable, Uncheck the box to disable



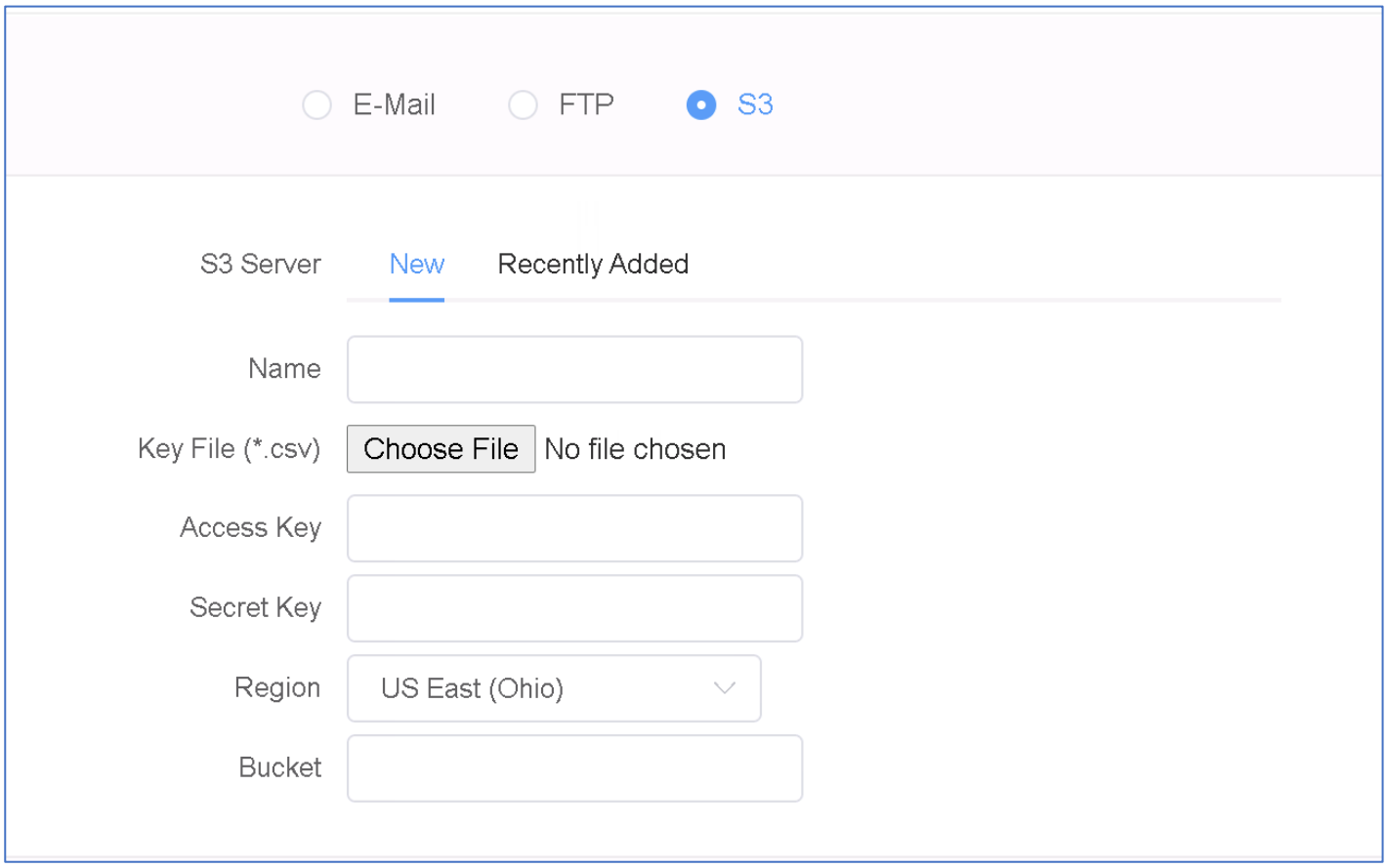
- File Path Format: Enter a file path format
  - Use template: Configure the file path format by using a template
    - 'Custom' and 'Basic file path template' available
    - Select 'Use' to add the template to the editable preview message box
  - Add an attribute token; Tokens list at end of 'Events Actions' section
  - Select 'Add' to add an attribute token to the file path format

- Confirm FTP message contents within the editable preview option
- Click the 'APPLY' button at the bottom to save.



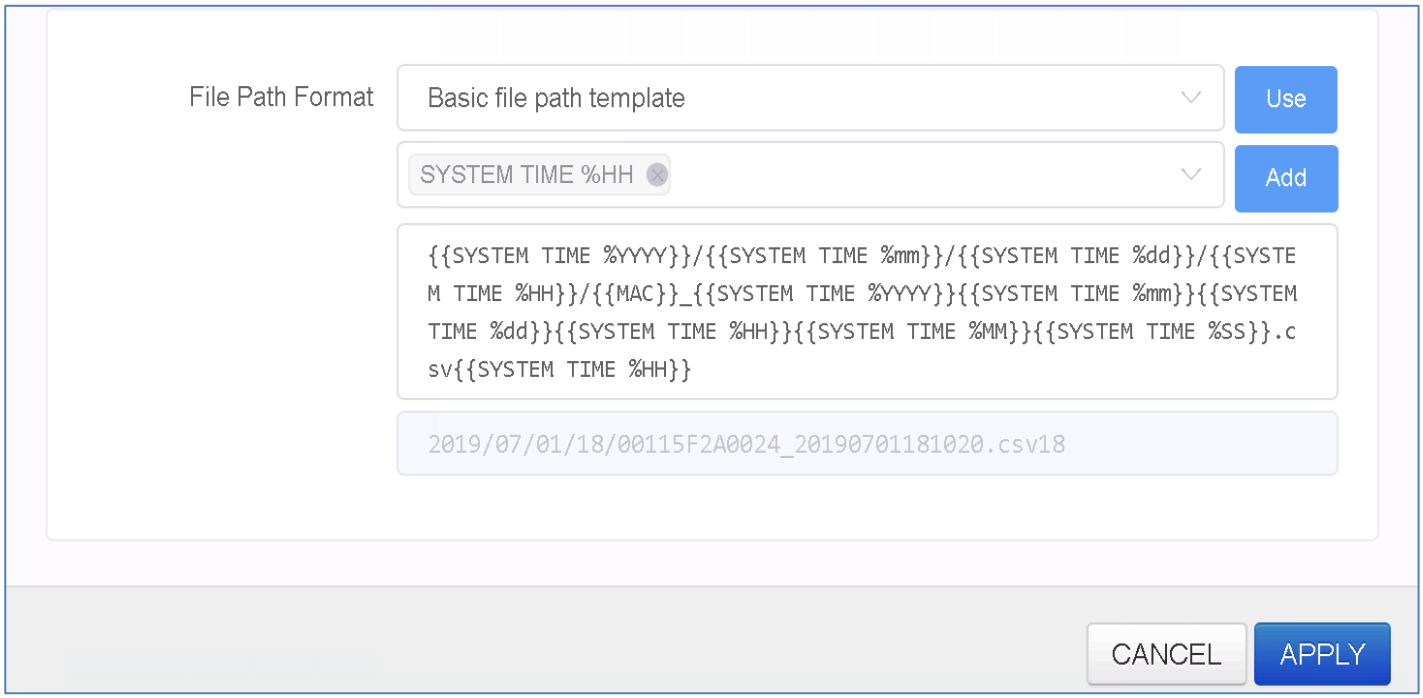
3. Recipient: S3

- Name: Title of S3 connection
- Key File (*.csv): Select 'Choose file' and navigate to the S3 key file
- Access Key: Enter the S3 access key
- Secret Key: Enter the S3 secret key
- Region: Select the S3 server regional location
- Bucket: Enter the bucket information



- File Path Format: Enter a file path format
  - Use template: Configure the file path format by using a template
    - 'Custom' and 'Basic file path template' available
    - Select 'Use' to add the template to the editable preview message box
  - Add an attribute token; Tokens list at end of 'Events Actions' section
  - Select 'Add' to add an attribute token to the file path format

- Confirm S3 message contents within the editable preview option
- Click the 'APPLY' button at the bottom to save



8. Search

1. Search: Event Log

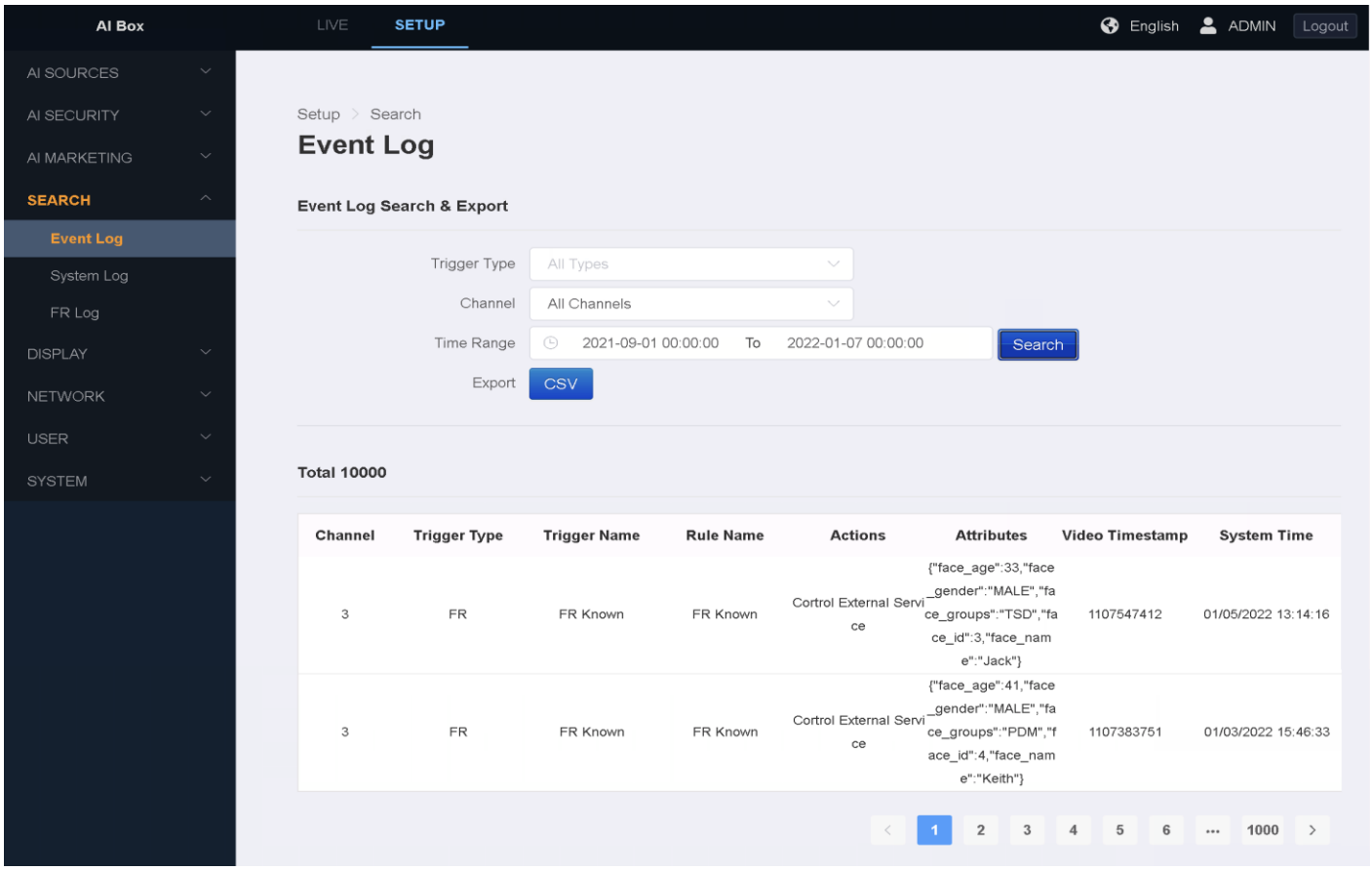
Search and or download to CSV file an ‘Event Log’ based on action events that occurred in the 'Action Rules' under the 'AI Security' menu.

To run an ‘Event Log’ query, go to SETUP/Search/Event Log

- Trigger Type: Select the desired trigger type from the list of available triggers
- Channel: Select the desired channel from the list of available channels
    - Options include ‘All Channels’, and ‘System’

- Time Range: Set a specific time range from 00:00 to 00:00
    - Select ‘Search’ to see results in the below review area

- Export: Select ‘CSV’ to export the search results to a csv formatted file



2. Search: System Log

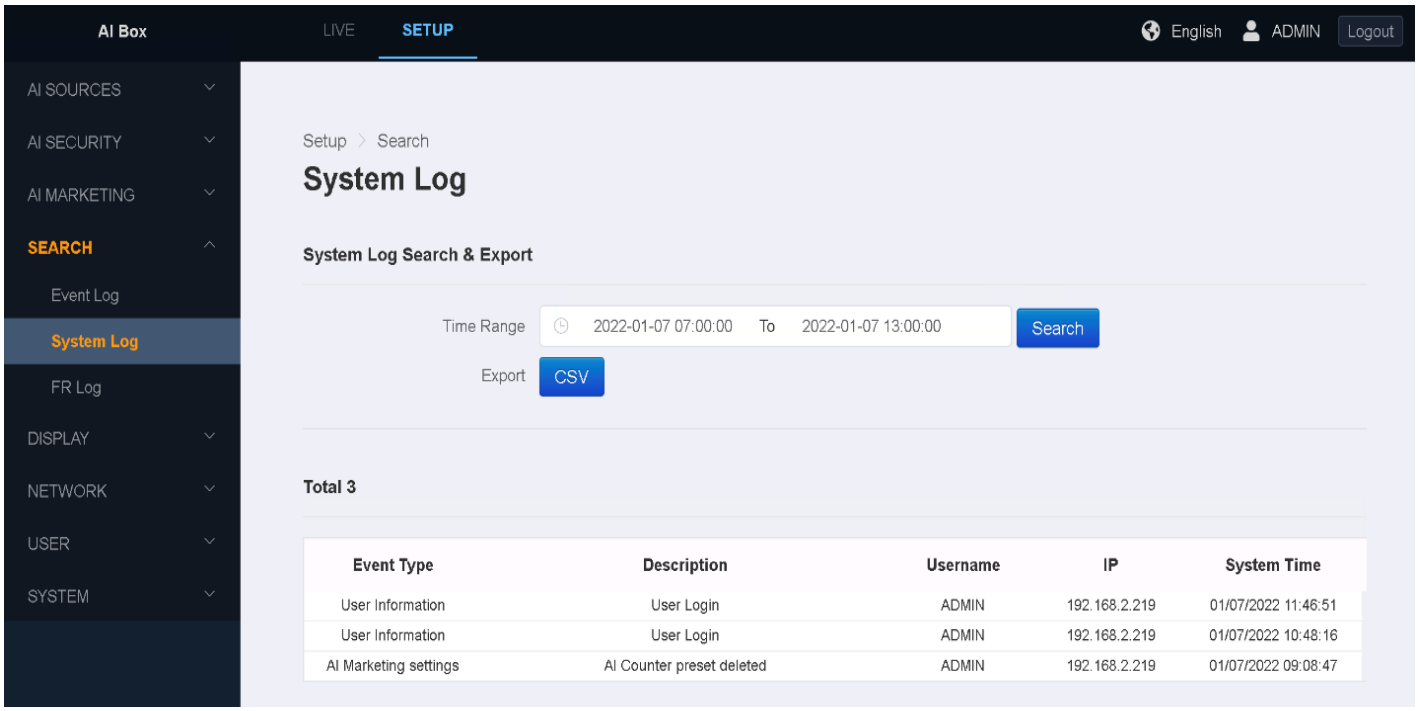
You can search and download the necessary system logs such as user login or system startup etc. in CSV format.

Search and or download to CSV file a 'System Log' based on system events, user login, user actions, system startup, and other system type events.

To run a 'System Log' query, go to SETUP/Search/System Log

- Time Range: Set a specific time range from 00:00 to 00:00
  - Select 'Search' to see results in the below review area

- Export: Select 'CSV' to export the search results to a csv formatted file



3. Search: FR Log (Face Recognition)

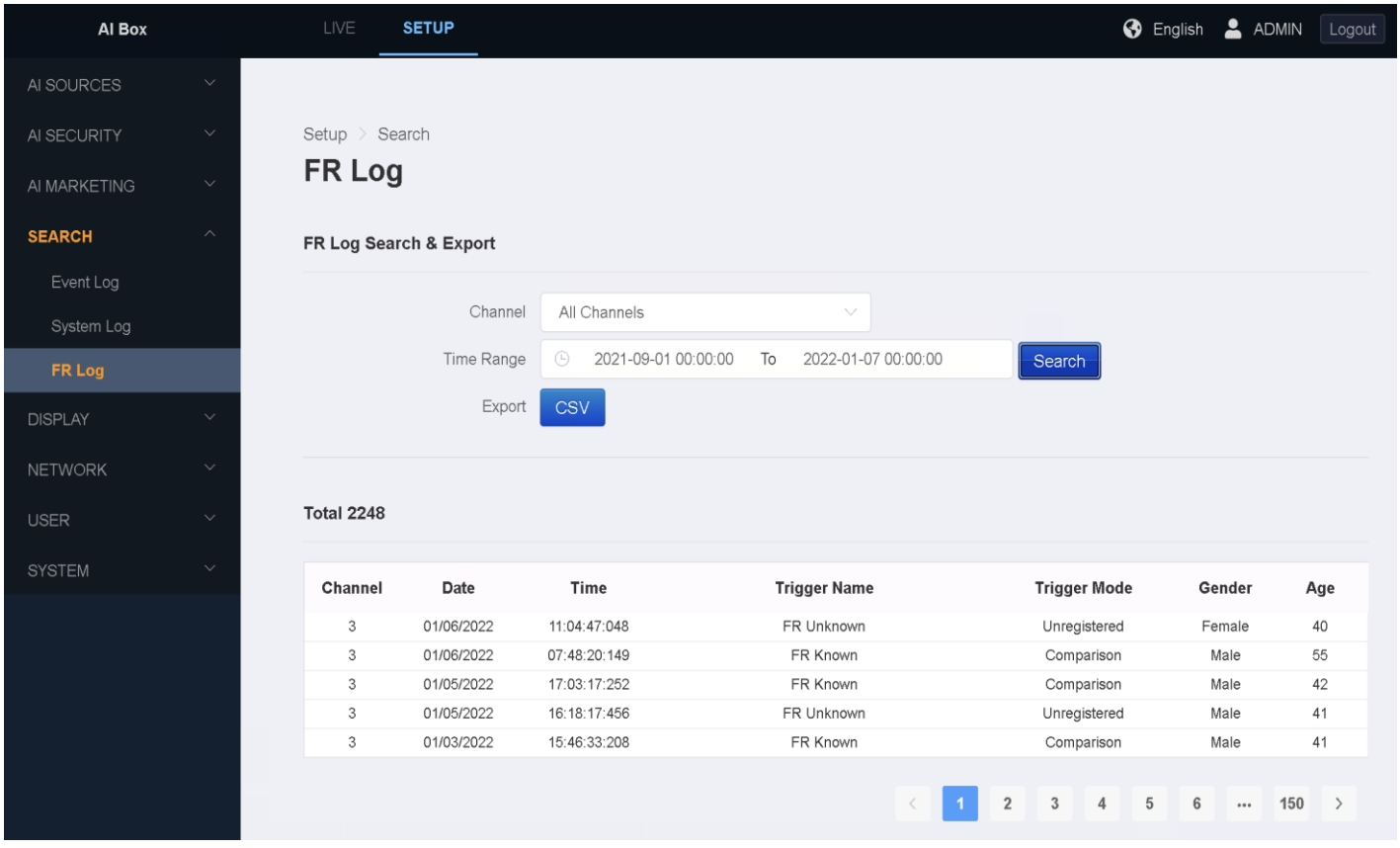
Search and or download to CSV file a ‘FR Log’ based on Face Recognition events that occurred in the 'Action Rules' under the 'AI Security' menu.

To run a ‘FR Log’ query, go to SETUP/Search/FR Log

- Channel: Select the desired channel from the list of available channels
  - Options include ‘All Channels’, and ‘System’

- Time Range: Set a specific time range from 00:00 to 00:00
  - Select ‘Search’ to see results in the below review area

- Export: Select ‘CSV’ to export the search results to a csv formatted file



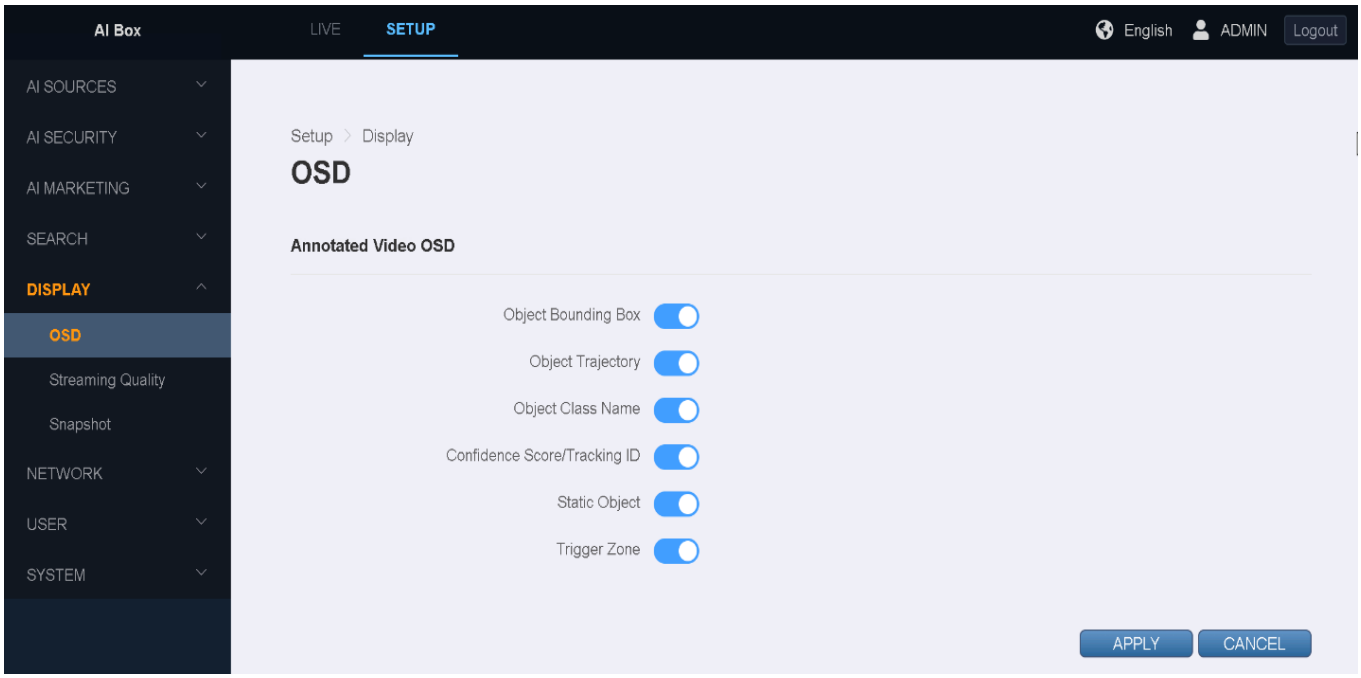
9. Display

1. Display: OSD

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

To make changes to the OSD, go to SETUP/Display/OSD

- Object bounding Box: Determining if the Box is displayed on the object border
- Object Trajectory: Determines if the screen is displayed on the moving object
- Object Class Name: Determining if the screen is displayed on people or cars
- Confidence Score/Tracking ID: used for AI debugging
- Static Object: Determining if the screen is displayed on a static object
- Trigger Zone: Determining if a trigger rule display line or figure is displayed on screen
- Click the 'APPLY' button at the bottom to save



2. Display: Streaming Quality

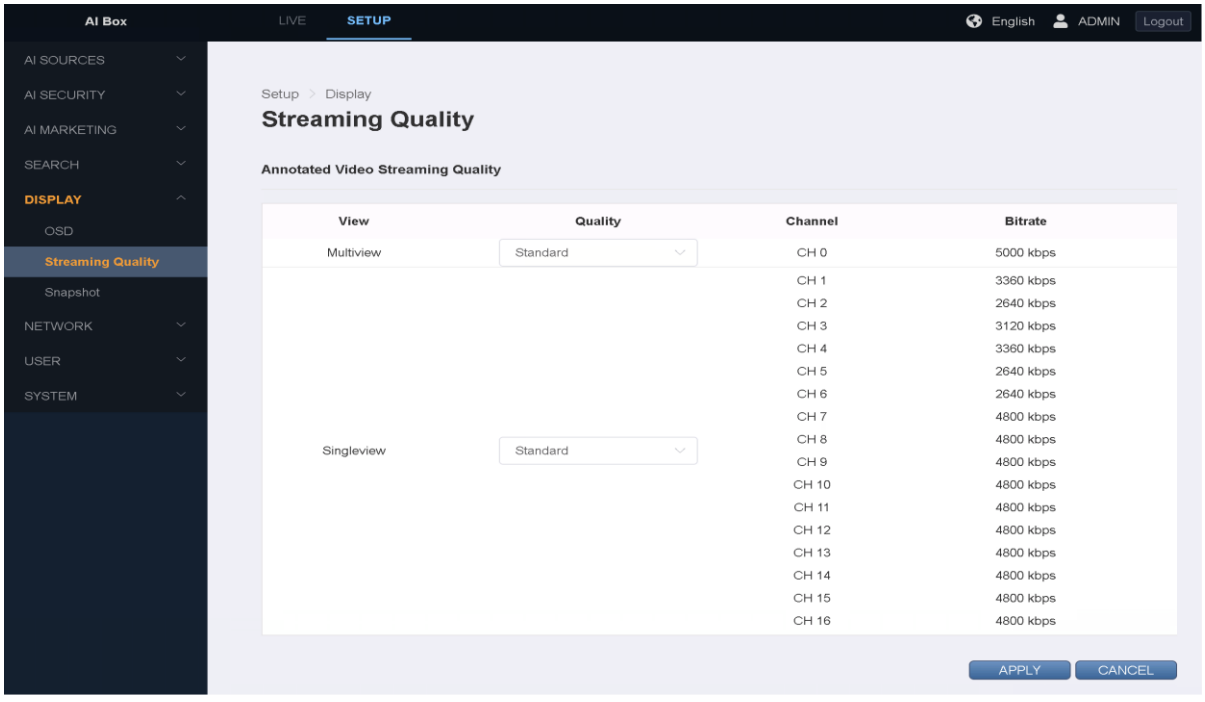
AI BOX supports not only video streaming for each RTSP channel but also multi-view streaming showing all channels as one channel.

To make changes to the 'Streaming Quality' of the AI Box, go to SETUP/Display/Stream Quality

- Multiview: Selectable options include.
  - Highest – Up to 8000Kbps
  - High – Up to 6500Kbps
  - Standard – Up to 5000Kbps
  - Low – Up to 3500Kbps
  - Lowest – Up to 2000Kbps

- Singleview: Selectable options include.
  - Highest – Up to 8000Kbps
  - High – Up to 6400Kbps
  - Standard – Up to 4800Kbps
  - Low – Up to 3200Kbps
  - Lowest – Up to 1600Kbps

- Click the 'APPLY' button at the bottom to save

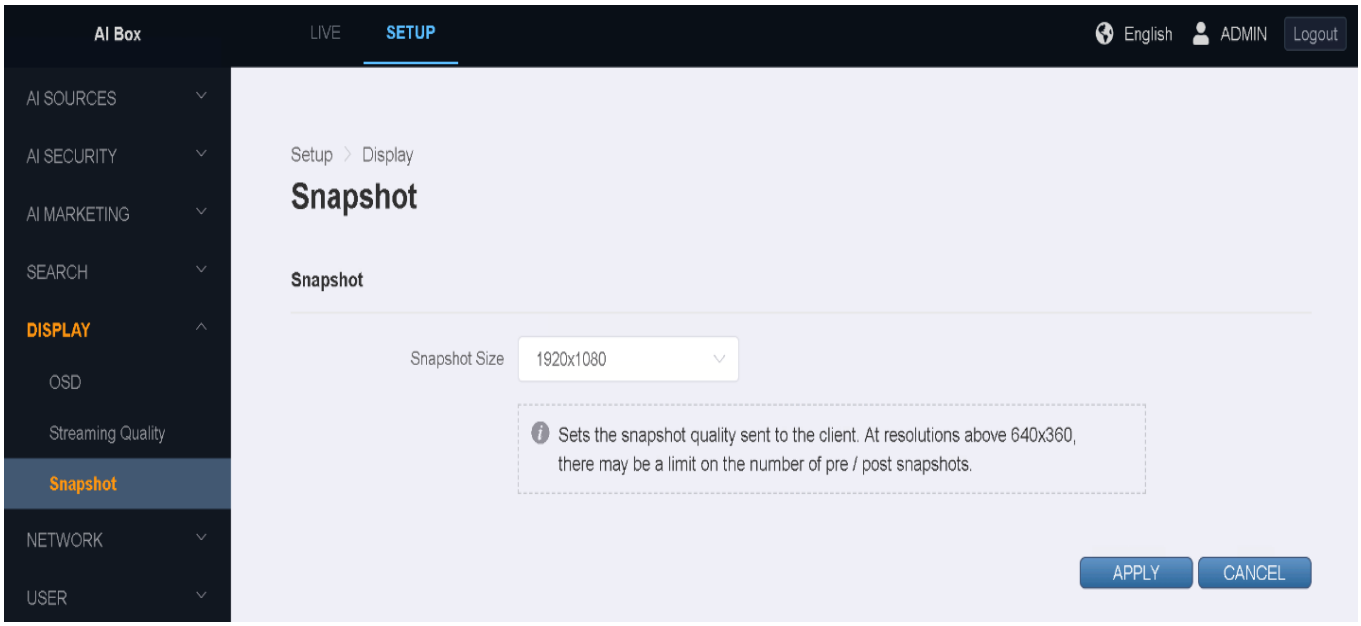


3. Display: Snapshot

AI BOX supports 'Snapshot' actions, as related to 'Event Actions'.

To make changes to the 'Snapshot' resolution size, go to SETUP/Display/Snapshot

- The snapshot size can be adjusted to 640x360, 1280x720, 1920x1080
- Note: The larger the snapshot size, the fewer snapshots the AI Box can hold



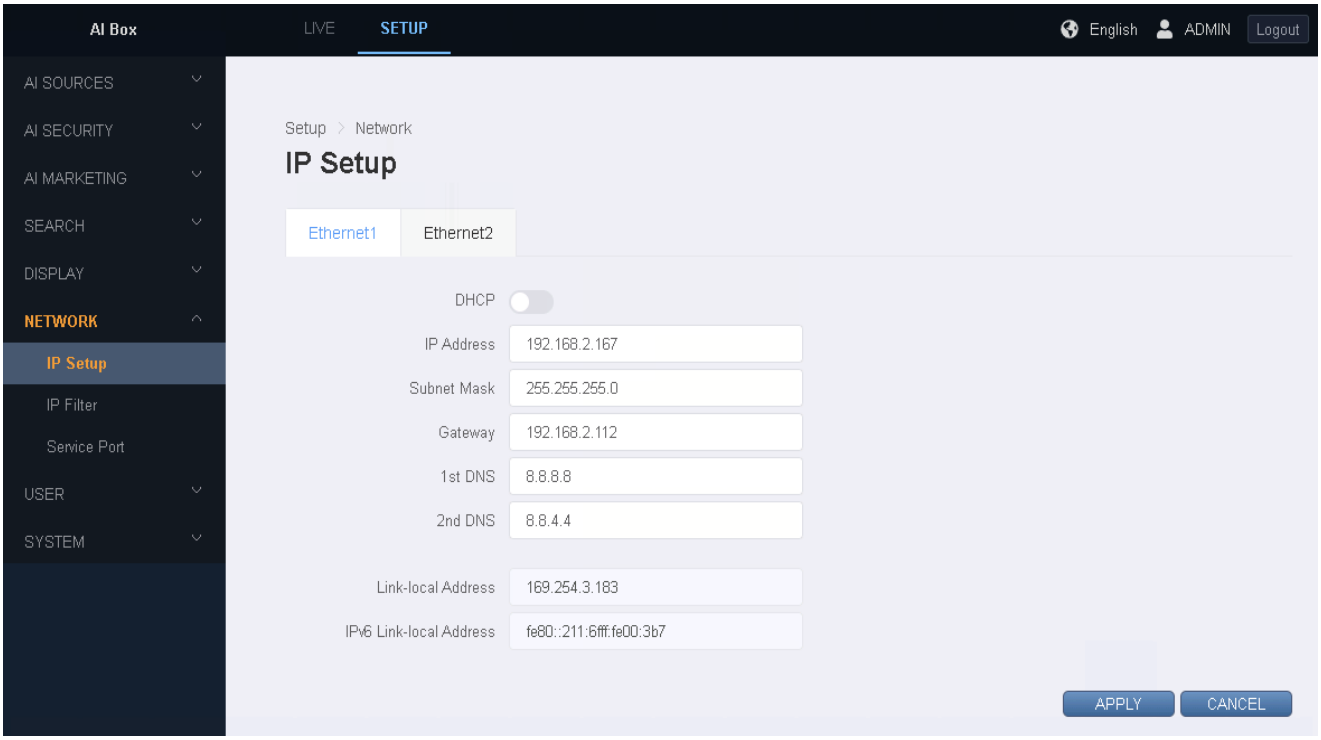
10. Network

1. Network: IP Setup

To change the network-related settings of the AI Box, go to go to SETUP/NETWORK/IP Setup
Select 'Setup/Network/IP Setup' to modify the network type for Eithernet1 and Ethernet2

- Select 'DHCP' to enable or disable the autoconfiguration networking service
- Disabling 'DHCP' allows for manually configuring the device's network settings.
- 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 for the network
    - 1st DNS: Input the 1st DNS value of the device.
    - 2nd DNS: Input the 2nd DNS value of the device.
- Note: DHCP enabled requires a local network DHSP server, or service
- Ethernet1/2 reference ports on back of device to which a network cable is connected
- Select 'Apply' to commit any changes

Note: A Link Local Address is a network address that is valid only for communications within the network segment or the broadcast domain that the AI Box is connected to.

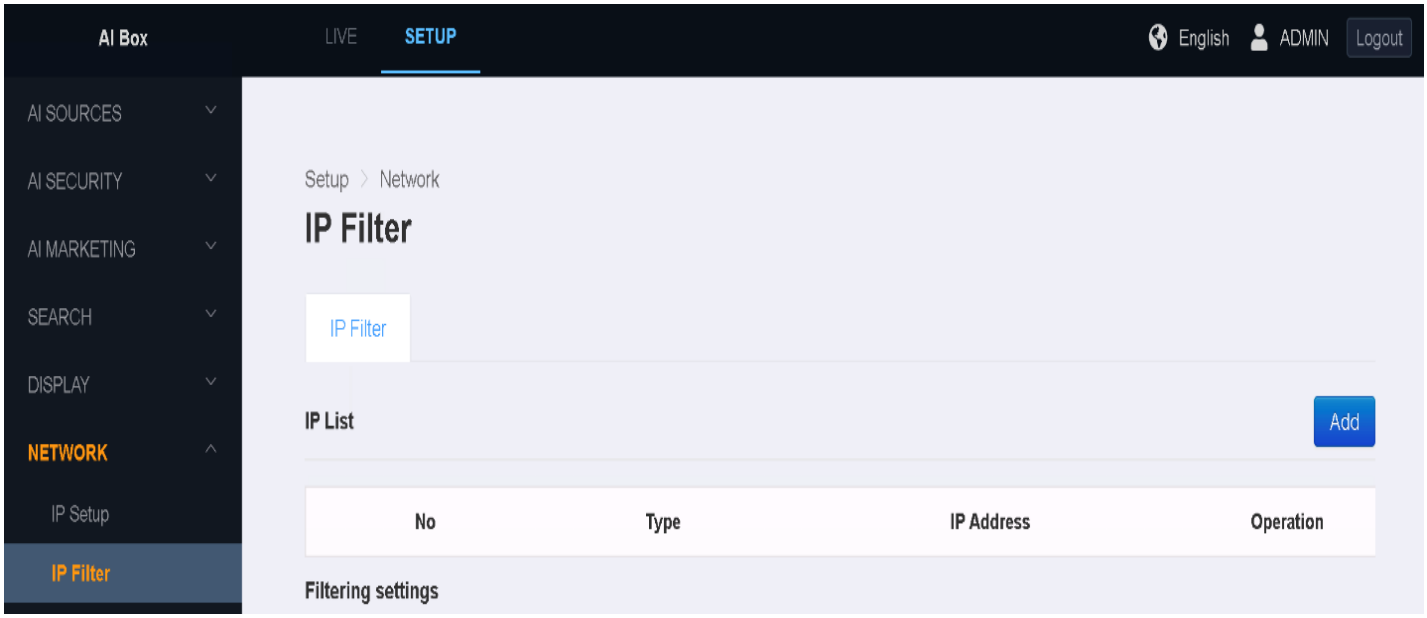


2. Network: IP Filter

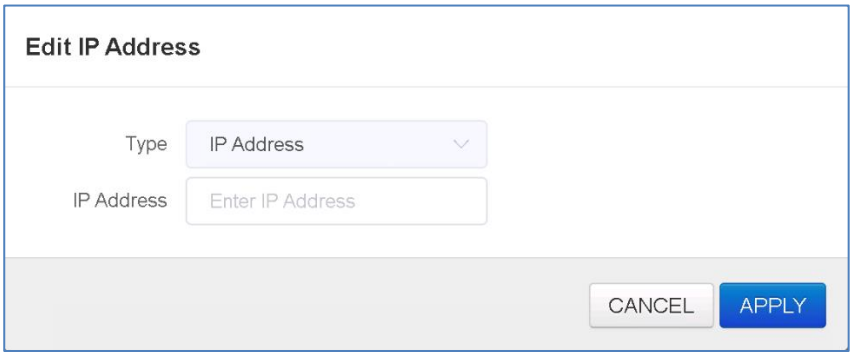
AI BOX supports not only video streaming for each RTSP channel but also multi-view streaming showing all channels as one channel.

To make configure the 'IP Filter' network option, go to SETUP/NETWORK/IP Filter

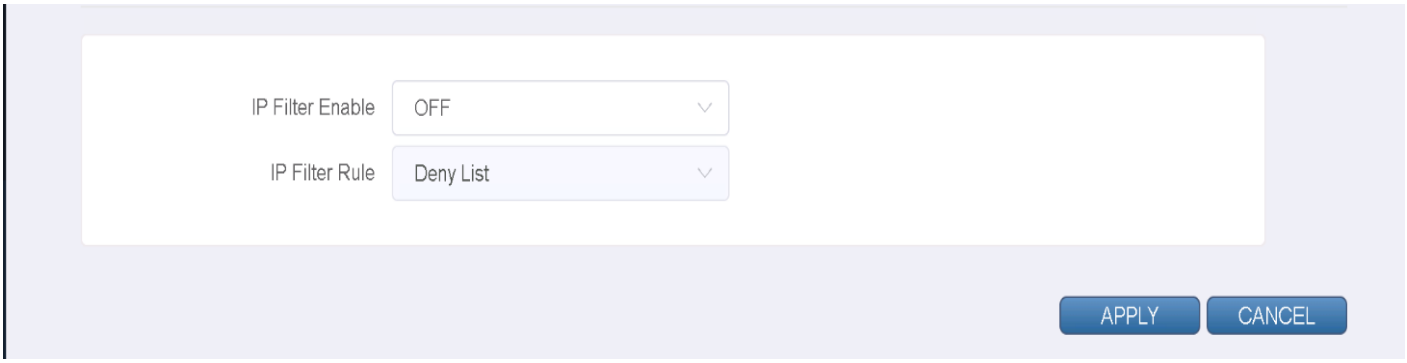
- Select 'Add' to enter an IP address into the IP List



- Type: Default IP Address – currently no modifiable
- IP Address: Enter the IP address that will be filtered
- Select 'Apply' to commit the IP address to the IP list



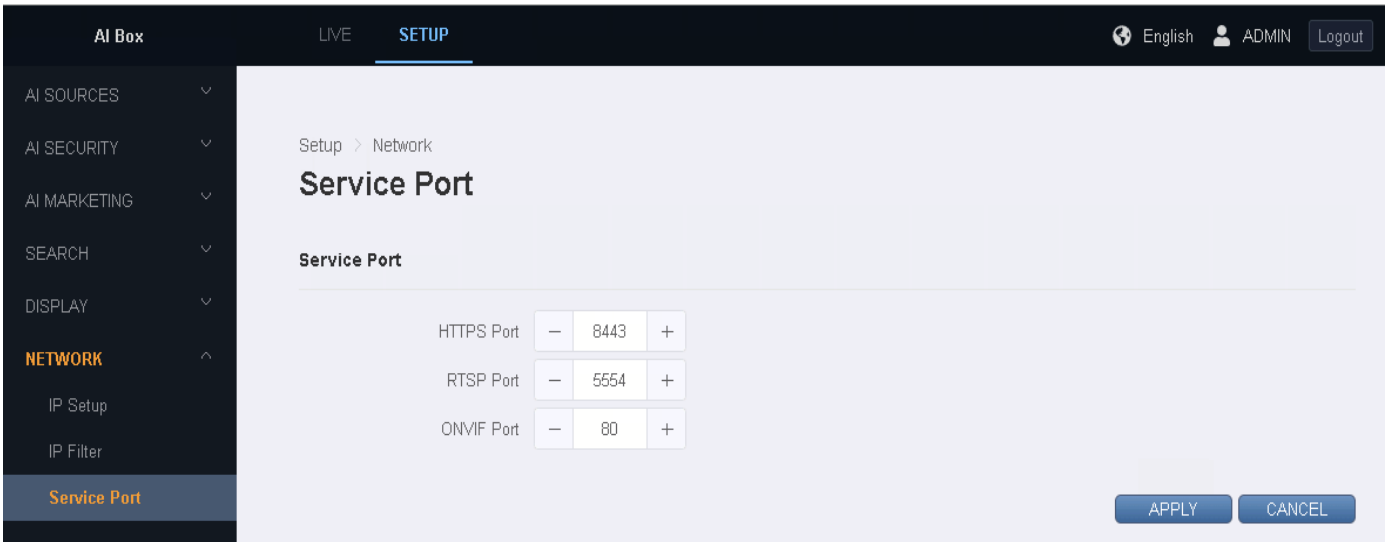
- IP Filter Enabled: Default OFF – Select 'Off' or 'On'
- IP Filter Rule: Default Deny List – Select 'Allow List' or 'Deny List'
- Select 'Apply' to commit any changes



3. Network: Service Port

Select 'Setup/Network/Service Port' to modify the network service ports of the AI Box.

- HTTPS: Default 8443 – Select plus or minus to modify
- RTSP: Default 5554 – Select plus or minus to modify
- ONVIF: Default 80 – Select plus or minus to modify
- Select 'Apply' to commit any changes

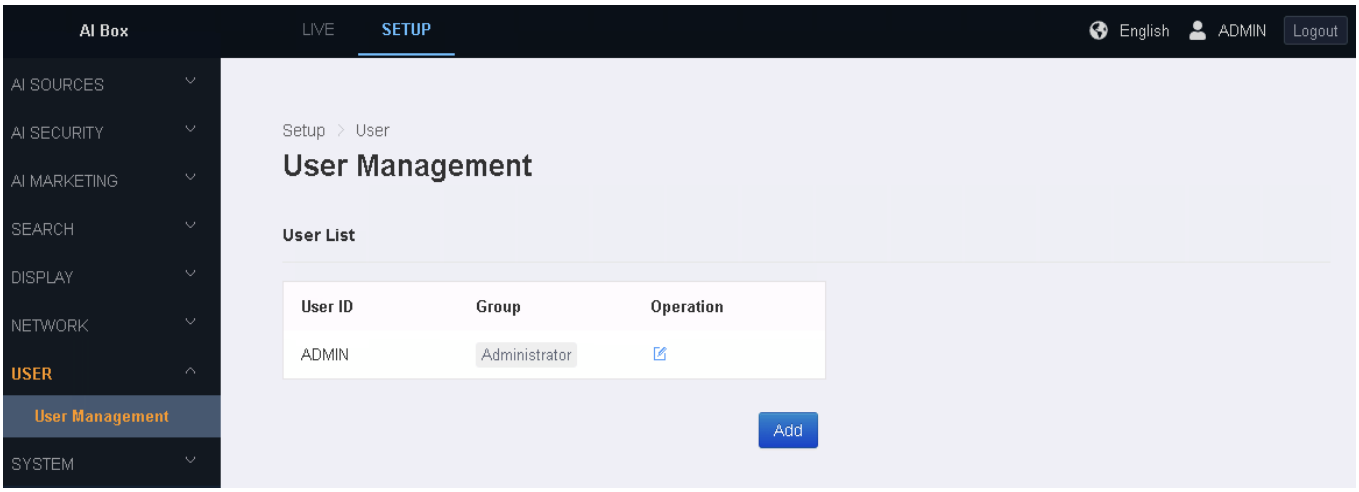


11. User

User accounts are created to limit the permissions of individuals who are logged onto the AI Box. Permissions include two predefined access levels Administrators, and Viewer's.

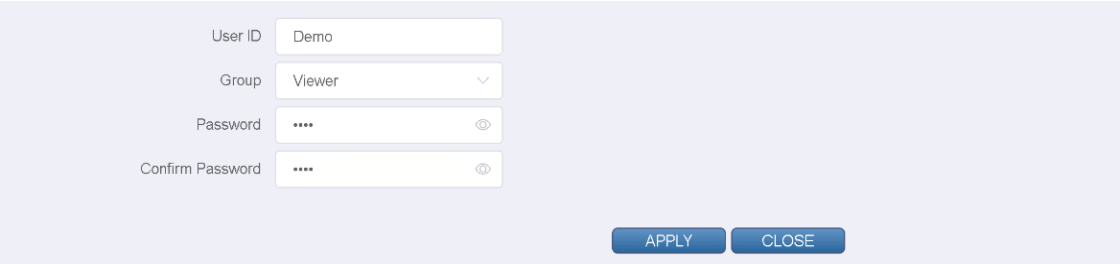
Select 'Setup/USER/User Management' to modify the user accounts of the AI Box.

- Select the operation modify icon , to change or modify an existing user.
- Select 'Add' to create a new user



- Select 'Add' to create a new user
- User ID: Enter the username
- Group: Select 'Administrator' or 'Viewer'
- Password: Enter a password
    - Select from 8~16 uppercase, lowercase, number, and special characters

- Confirm Password: Re-enter password to confirm matched characters
- Select 'Apply' to commit any changes



12. System

1. System: Date/Time

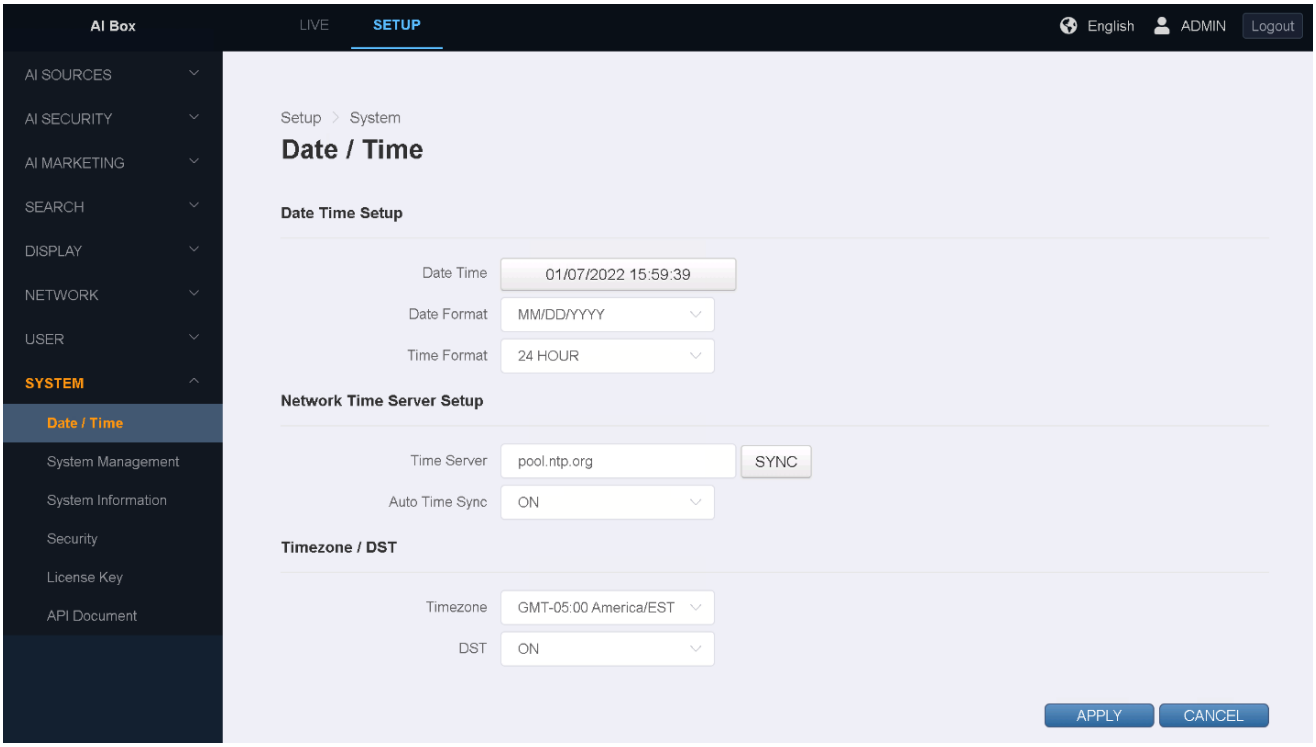
Date/Time maintains the AI Box system wide date and time format, and time sync.

To change the Date/Time setting of the AI Box, go to SETUP/SYSTEM/Date/Time select 'Date/Time' to modify the following time related functions of the AI Box

- Select 'Date Time' to manually enter the year, month, day, and time
- Select 'Date Format' to select YYYY/MM/DD, MM/DD/YYYY, or DD/MM/YYYY
- Select 'Time Format' to select 24 hour or AM/PM formatting
- Select 'Time Server' to manually enter the address of an NTP server
    - Press the 'SYNC' button to automatically synchronize the system date and time.

- Select 'Auto Sync' to synchronize the time periodically through the NTP server.
- Select 'Time zone' to set the local time zone of the AI Box
- Select 'DST' to enable or disable the Daylight Savings Time

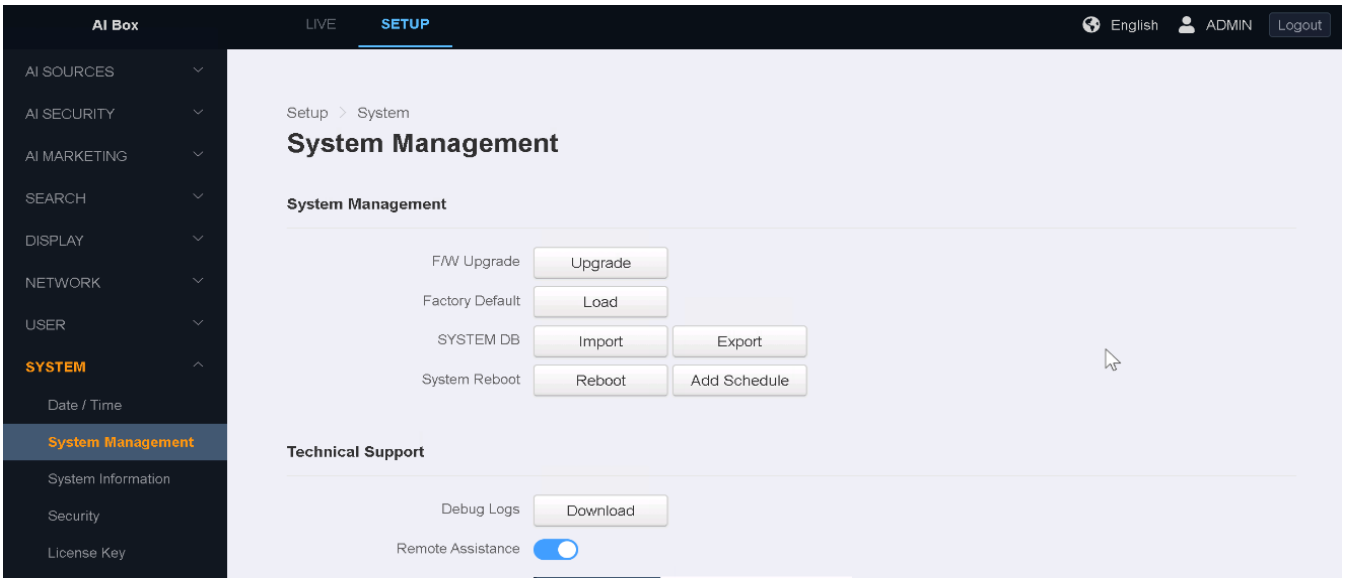
※ The DNS address of the device must be set correctly if the address of NPT server is a domain.



2. System: System Management

System Management is designed for the maintenance, performance, and trouble shoot of the AI Box.

To modify the system settings of the AI Box, go to go to SETUP/SYSTEM/System Management

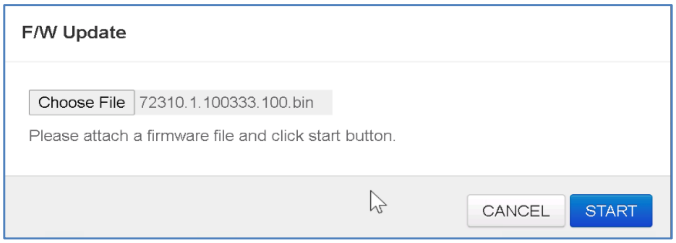


Firmware: The firmware upgrade process is intended for adding new features, and or bug fixes.
All functions shut down during the firmware upgrade. Never disconnect power or LAN during firmware upgrade process. Power cannot be lost when upgrading as it will cause a failure and require maintenance.

It takes approximately 3-10 minutes for the unit to reboot after the firmware upgrade process.

- Select 'F/W Upgrade' to initialize the upgrade process
- Select 'Choose File' to navigate to the storage location of the new firmware.
- Select 'Start' once the firmware file has been selected.
- The AI Box will reboot when the firmware upgrade is complete

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

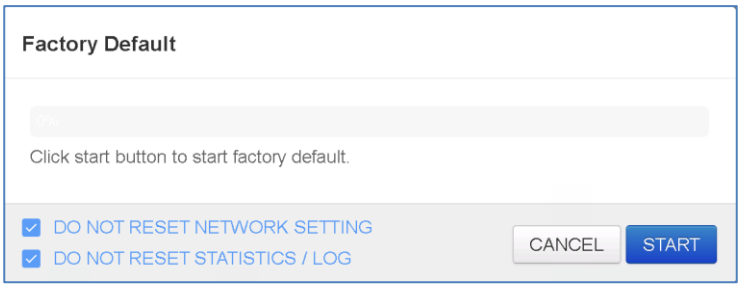


Factory Default: When the AI Box is not responding per standard expectations, or system functions are not clearing per need, a factory defaulting of the AI Box may be recommended.

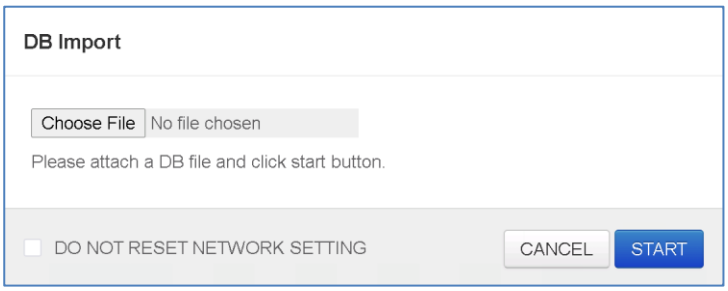
Reset the AI Box device to factory default settings.

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

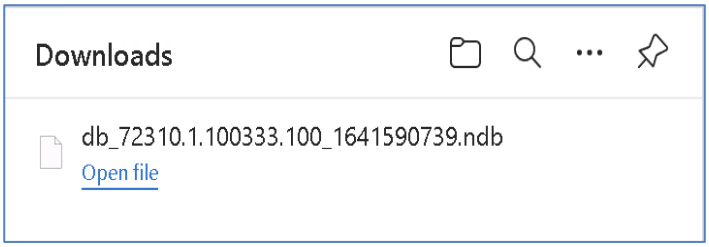
[Caution] If the AI BOX is not connected to a Dynamic Host Configuration Protocol (DHCP) network, the IP address settings for the AI BOX will be lost and the server will not recognize the camera. DHCP On is the default setting for the AI BOX IP address



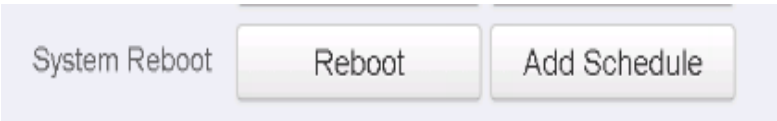
System DB: The AI Box supports importing an existing configuration of settings, and functions.



The AI Box supports exporting of the existing settings, and functions via the web browsers download function.

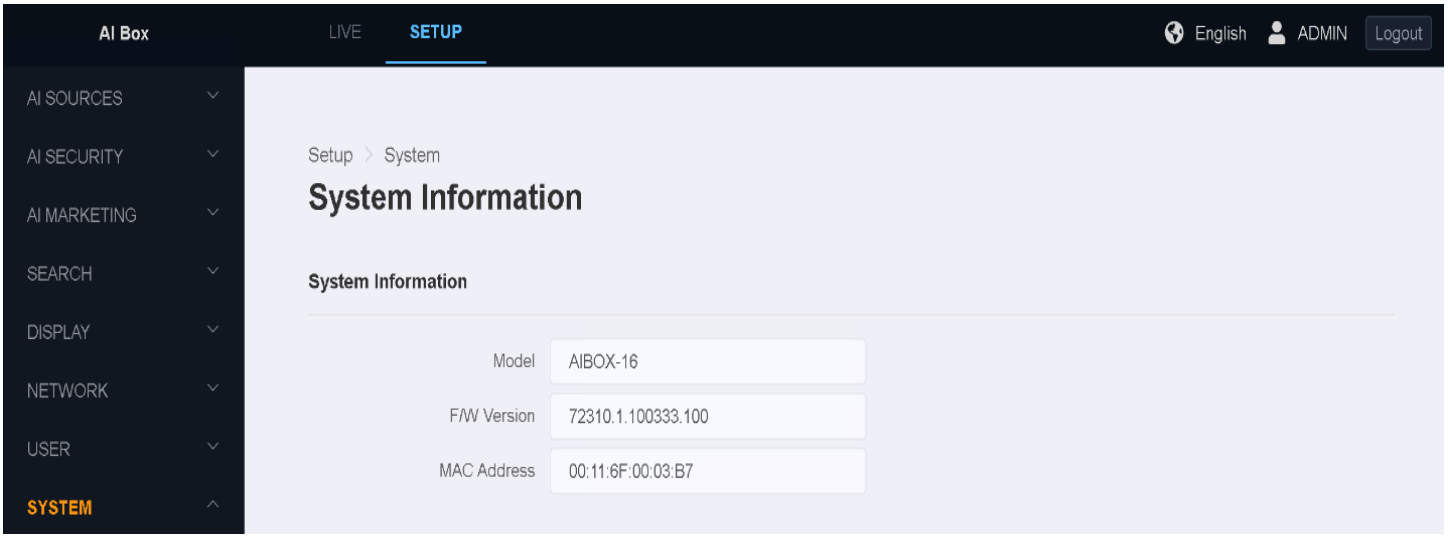


The AI Box supports both a manual, and schedule-based system reboot.
Schedule requires the selection of ‘Daily’, ‘Weekly’ or ‘Month’, with associated time, ‘Hour’, ‘Weekday’, or ‘Day of Month’



3. System: System information

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



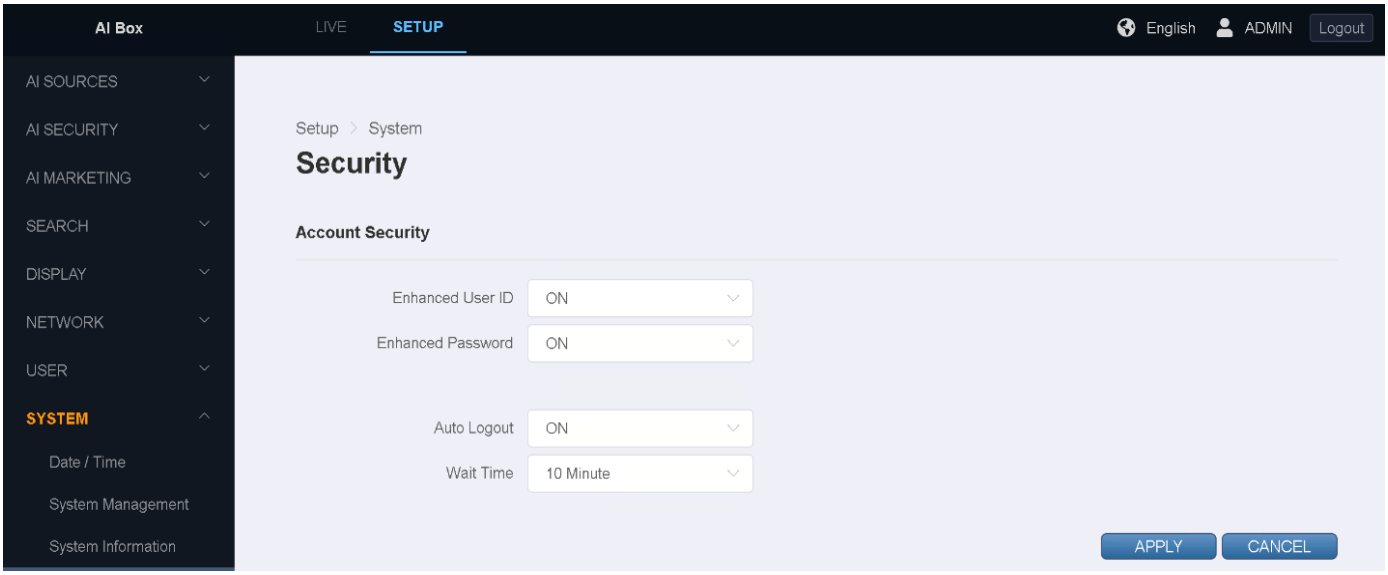
4. System: Security

- Enhanced User ID: Select ‘On’ or ‘Off’
  - Enhanced ID enables

- Enhanced Password: Select ‘On’ or ‘Off’
  - Enhanced Password enables

- Auto Logout: Select ‘On’ or ‘Off’
- Wait Time: Select 1-minute, 2-minute, 3-minute, 5-minute, or 10-minute before auto logout is initiated

- Select ‘Apply’ to save changes

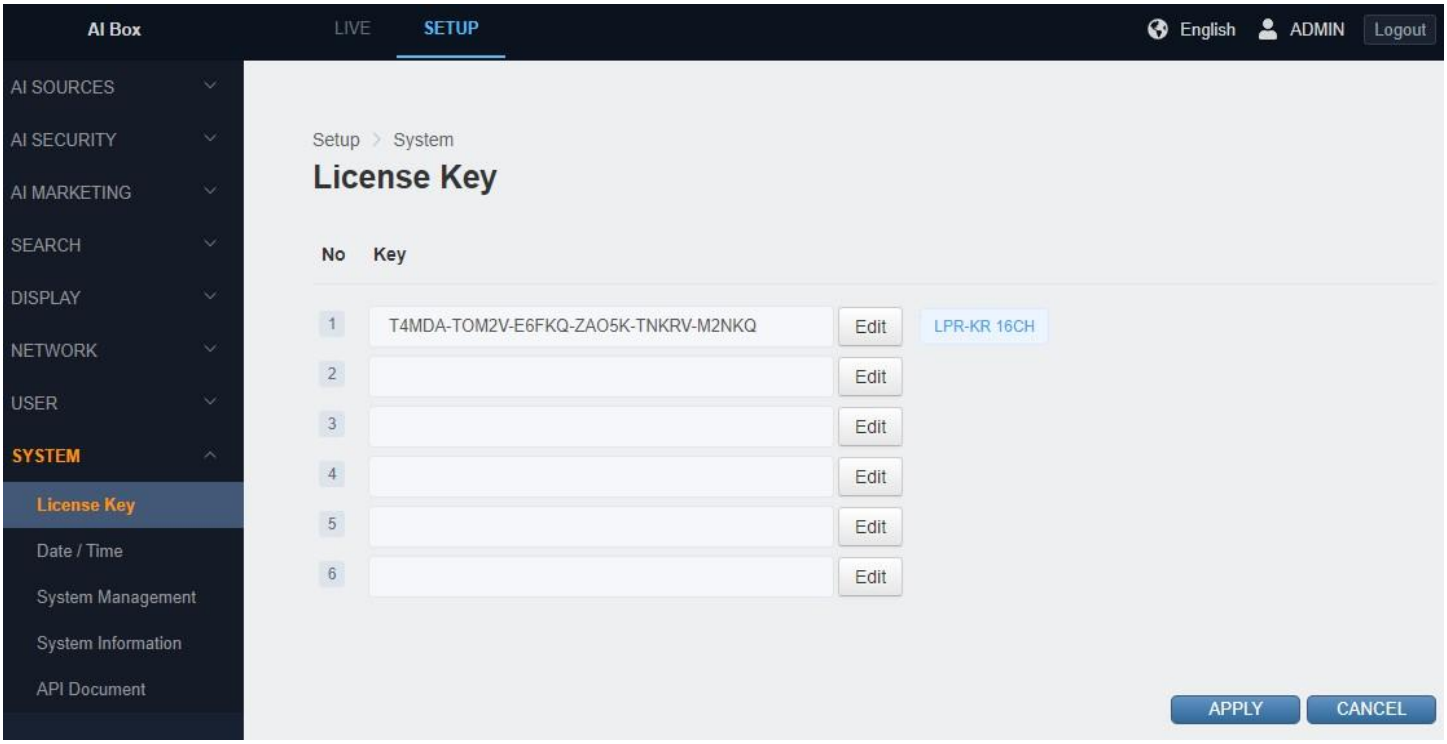


5. License key

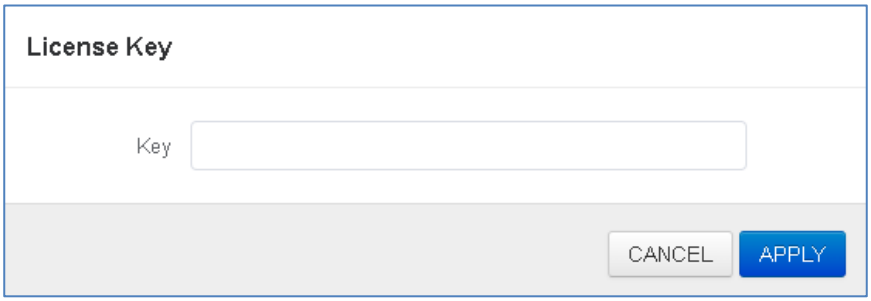
Enter a license key to activate additional features that require a license.
If the license is successfully registered, the corresponding item is display ed on the right.

To add a license key to the AI Box, go to go to SETUP/SYSTEM/License Key

- Select 'Edit' to enter the license key

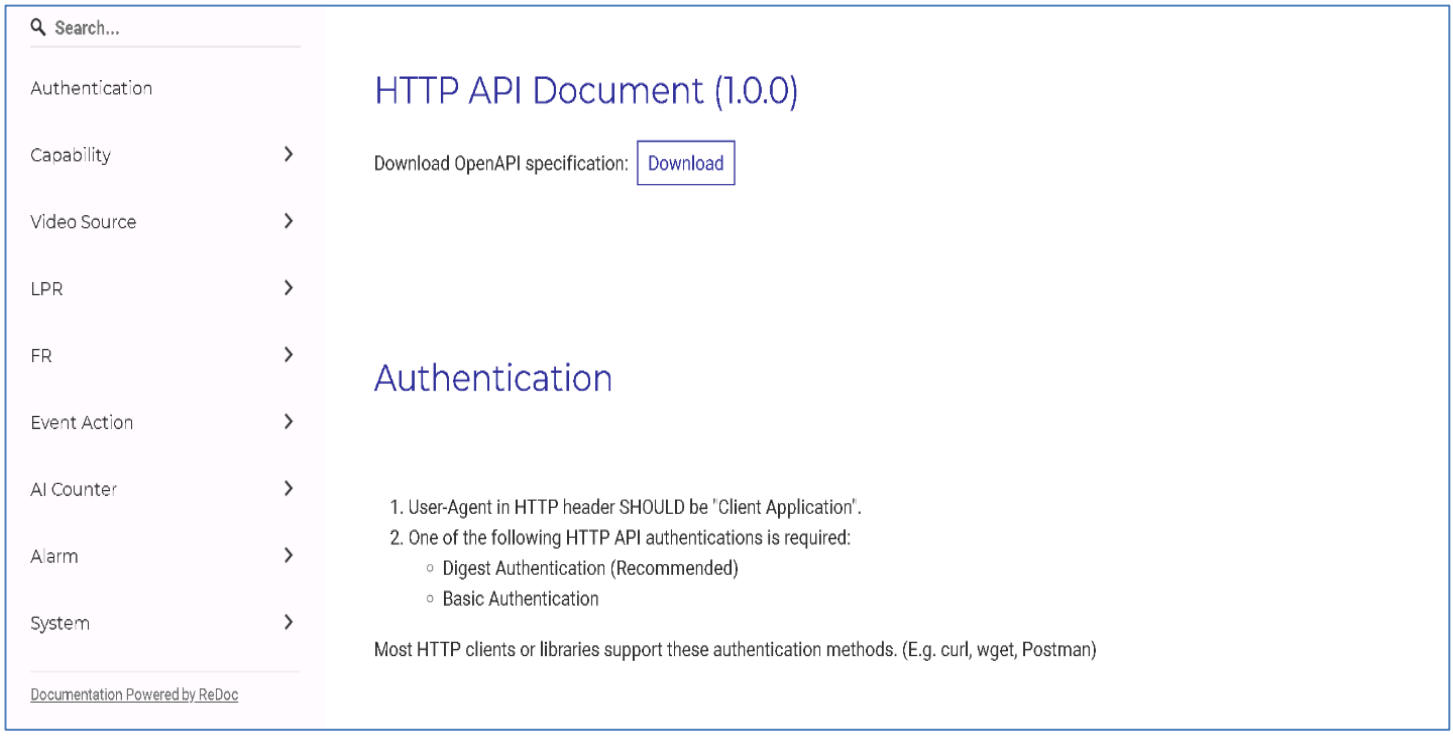


- Key: Copy or paste the license key into the 'Key' area
- Select 'APPLY' to save and continue
- After confirming the new key is listed, select 'APPLY' to save and continue



6. API documentation

API document is embedded to work with AI BOX.



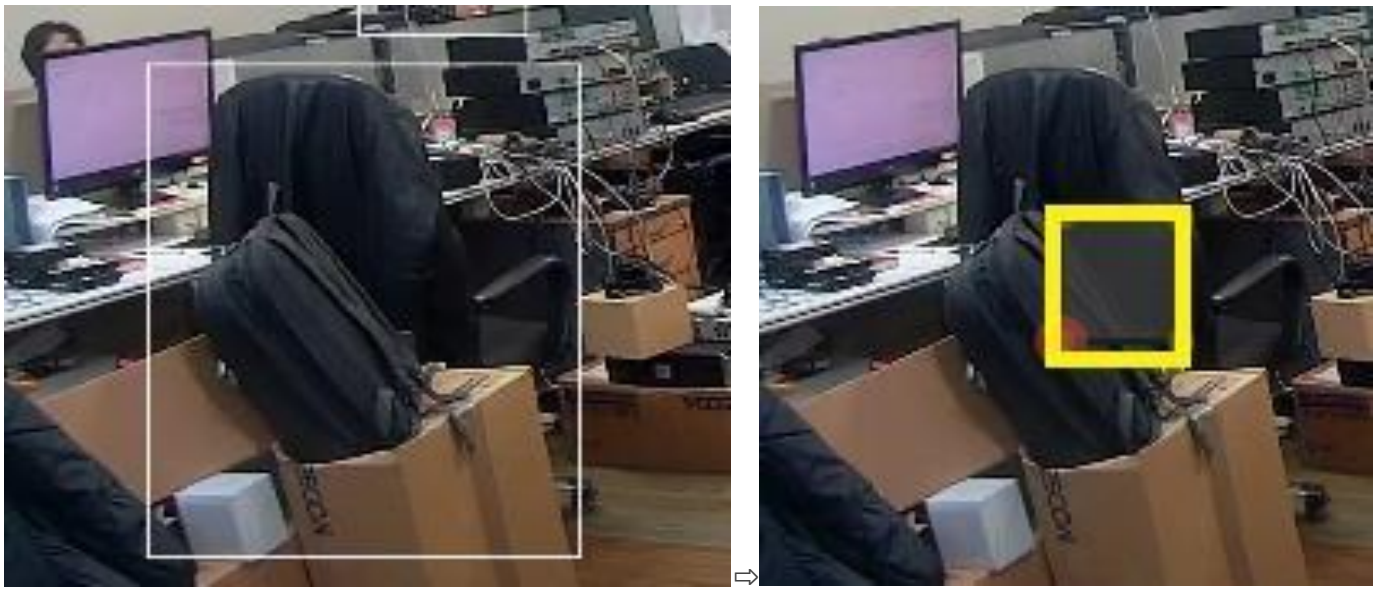
13. False detection filter setting

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.)



14. 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 HDMI 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)

THE END -

CORP HQ +1 (919) 230-8700 | WEST COAST +1 (310) 222-8600
ganzsecurity.com