AVLYTICS

artificial intelligence for video surveillance

The Most Cost Effective
Artificial Intelligence for Surveillance Solutions

Edge Web User Interface

Version 1.0

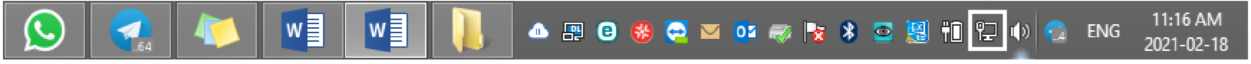
Manual

INDEX

1. How to access the AVLYTICS User Interface

This manual will guide you through each page of the AVLYTICS Edge Device Web User Interface.

Select the internet settings icon on your taskbar

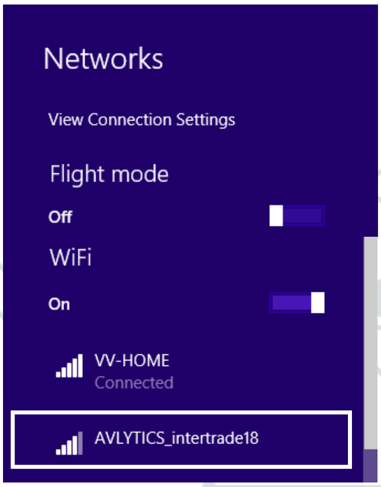


Establish a wireless connection to the device in order to access the Web user interface. The devices are supplied with a preconfigured wireless access point enabled.

There are two methods in which to access the user interface. The first is through the use of a VPN (Virtual Private Network) connected computer, and the second is on site through the Wireless AP (Access Point).

To access the device through wireless, the installer must be on site and within range of the devices wireless signal broadcasting capability.

The device will broadcast its SSID which is *AVLYTICS_intertradeX*, where the X represents the devices unique ID number.



To connect to the wireless AP, click on WIFI icon on your task bar and then select the SSID of the device to connect to. You will be prompted to enter a password. The password for the device is the Client ID that you were supplied with.

If the password is entered correctly you will have successfully joined to the device's wireless, and you will be able to connect to the device's user interface.

The device has a default IP Address of **10.55.55.1** , and also has a built-in DHCP server that will issue your PC with a Network address in the same range which will enable the connection.
Please ensure that your wireless adapter is configured to obtain an IP Address Automatically (set to DHCP).

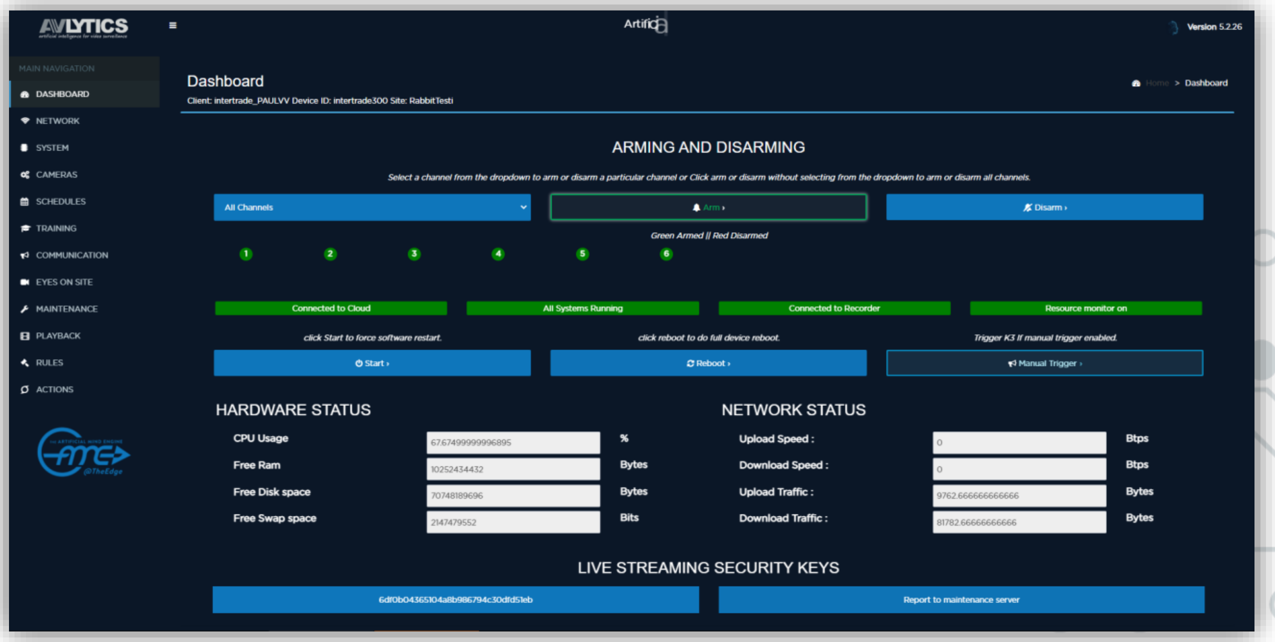
Once your wireless connection has been established, open a Google Chrome webpage and enter the device's IP address followed by port 8000: **http://10.55.55.1:8000**

You will be prompted for a password, please use your Client ID provided as the password.

Well done! You have successfully connected to the device and are now able to perform various tasks and configurations.

2. Dashboard

On successful login the user will be presented with the Dashboard page of the device.
The dashboard page is divided into four sections: *Arming / Disarming*, *Force Start and Reboot*, *System Health Status*, and *Live Streaming Security Keys*.



Dashboard

Client: intertrade_PAULVV Device ID: intertrade300 Site: RabbitTesti

ARMING AND DISARMING

Select a channel from the dropdown to arm or disarm a particular channel or Click arm or disarm without selecting from the dropdown to arm or disarm all channels.

Green Armed || Red Disarmed

click Start to force software restart.

click reboot to do full device reboot.

Trigger K3 If manual trigger enabled.

HARDWARE STATUS

CPU Usage	67.67499999996895	%
Free Ram	10252434432	Bytes
Free Disk space	70748189696	Bytes
Free Swap space	2147479552	Bits

NETWORK STATUS

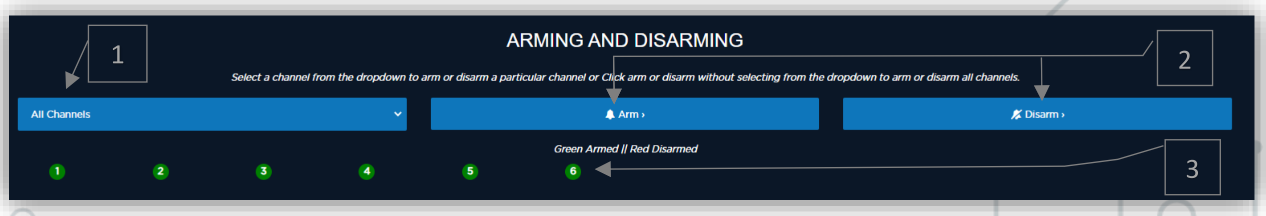
Upload Speed :	0	Btps
Download Speed :	0	Btps
Upload Traffic :	9762.666666666666	Bytes
Download Traffic :	81782.66666666666	Bytes

LIVE STREAMING SECURITY KEYS

6df0b04365104a8b986794c30dfd51eb

2.1 Arming / Disarming

Similar to an alarm system, the device allows the user to Arm and Disarm it, to either enable or disable the sending of notifications. Notifications are sent in the event of any moving object being detected.



ARMING AND DISARMING

Select a channel from the dropdown to arm or disarm a particular channel or Click arm or disarm without selecting from the dropdown to arm or disarm all channels.

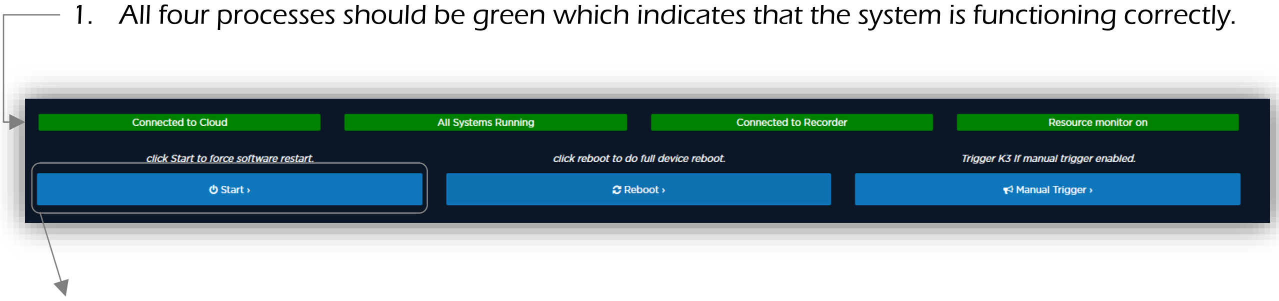
Green Armed || Red Disarmed

1. The first dropdown selector allows the user to address all channels or an individual channel.
2. Following the selector are two buttons, one to Arm and another to Disarm the selected channel/ channels.
3. The Armed Status indicator panel shows the armed status of each channel.
   Green indicates that a channel is armed and ready to send notifications if movement is detected on that particular channel. Red indicates that a channel is disarmed and no alerts or notifications will be sent in the event of movement being detected.

2.2 Force Start and Reboot

This section indicates the current status of each process running on the device.

1. All four processes should be green which indicates that the system is functioning correctly.



click Start to force software restart.

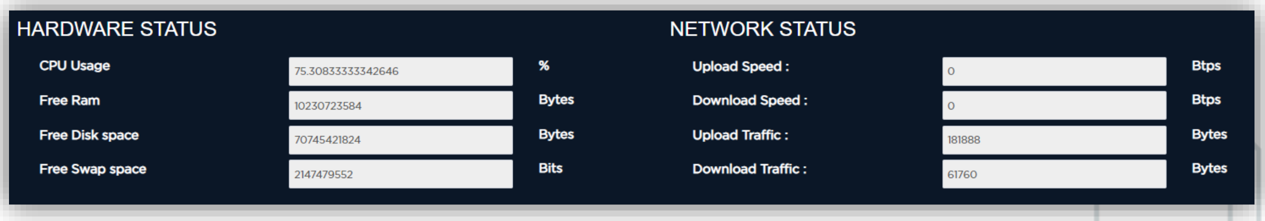
click reboot to do full device reboot.

Trigger K3 If manual trigger enabled.

2. If any of the processes are red, it indicates a possible problem with that process and the system should either be rebooted or forced to start all the processes by clicking on the 'Start' button.
3. The devices has the ability to allow a user to remotely activate the K3 relay output. This is a custom feature and needs to be enabled by a support representative. To make use of this feature, please contact support and request that manual trigger to be enabled.

2.3 System Health Status

The system health status section on the dashboard allows the user to gain basic insight into the device's resource consumption and general hardware health statuses.

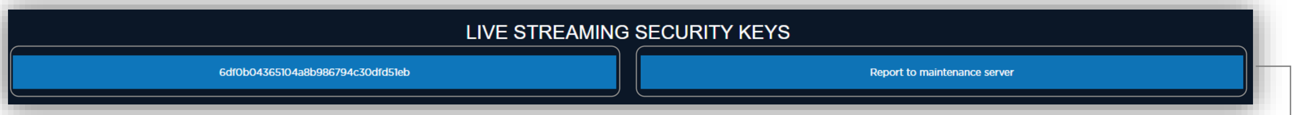


HARDWARE STATUS			NETWORK STATUS		
CPU Usage	75.30833333342646	%	Upload Speed :	0	Btps
Free Ram	10230723584	Bytes	Download Speed :	0	Btps
Free Disk space	70745421824	Bytes	Upload Traffic :	181888	Bytes
Free Swap space	2147479552	Bits	Download Traffic :	61760	Bytes

- CPU Usage – Shows the current consumption of the Central Processing Unit (should be less than 85%).
- Free Ram – Shows the Available Random Access Memory (should be above 100 bytes).
- Free Disk Space – Shows how much disk space is available on the SD card or Hard Drive (should be more than 1000 bytes).
- Free Swap Space – Shows available virtual memory (should be more than 20 bits).
- Upload and Download Speed – The device has the ability to measure the internet speed received from the ISP (Internet Service Provider). The upload and download speed is displayed in BPS (bits per second). These tests are disabled by default as they consume additional bandwidth. These can be enabled by a support representative on request.
- Upload and Download Traffic –shows the amount of data that has been uploaded and downloaded to/ from the VPN since the last reboot.

2.4 Live Streaming Security Keys

To add the device to the AVLYTICS software package, the security keys are required for authentication, by means of username and password. This key may be found in the Live Streaming Security Keys section. Select the keys in the 'keys' section (as indicated below), the copy and paste it in the AVLYTICS software menu when adding the device. If you cannot copy the keys from the web browser, ensure that you are using chrome browser.



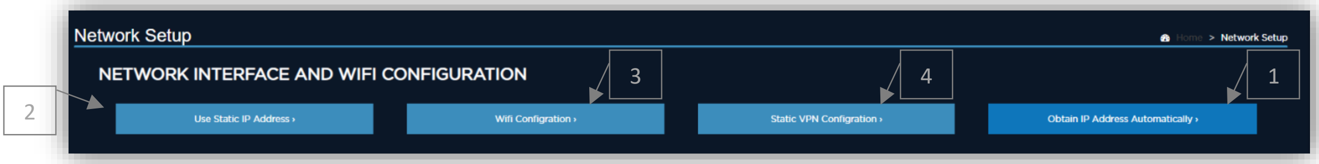
LIVE STREAMING SECURITY KEYS

6df0b04365104a8b986794c30dfd51eb
Report to maintenance server

The Maintenance Server waits for Health Status messages from the Edge Device, and produces a report every 10 minutes. Should the device not be responding, log into the Web User Interface and select the 'Report to maintenance server' option, which will force a report to be sent.
The keys for live streaming can also be received on Telegram by issuing a ***/getkeys*** command on the Telegram info group.

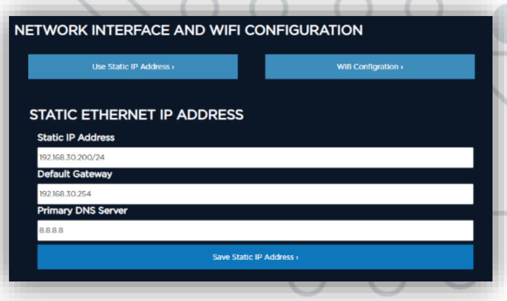
3. Network Setup Menu

The Network setup page allows the installer to configure the Local Network Connection parameters.


Network Setup
Home > Network Setup
NETWORK INTERFACE AND WIFI CONFIGURATION
2
Use Static IP Address ›
3
Wifi Configration ›
4
Static VPN Configration ›
1
Obtain IP Address Automatically ›

1. The AVLYTICS devices are supplied with DHCP enabled, which means the device will obtain an IP address automatically.
2. The installer can choose to either obtain a Local Network IP Address automatically (DHCP), or manually enter an allocated IP address on the network. Caution should be taken when using this facility, if the parameters are incorrectly configured it will not be possible to connect to the client's CCTV system. The local IP address should be configured in the same network range as the CCTV system network, to which this device will be plugged into.

   To set a static Local Lan IP Address, click on Use Static IP Address and complete the Text boxes in the Following format :
   Static IP Address: **x.x.x.x/x**
   Default Gateway: **This is your local network Router's IP Address.**
   Primary DNS Server: **8.8.8.8**

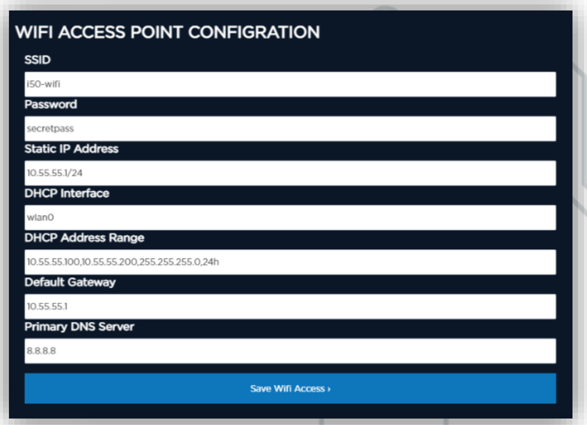


STATIC ETHERNET IP ADDRESS

Static IP Address
192.168.30.200/24
Default Gateway
192.168.30.254
Primary DNS Server
8.8.8.8

3. The AVLYTICS device is supplied with a pre-configured WIFI access point. To change any of the WIFI related configuration, click on the WIFI Configuration Button and make the relevant changes.

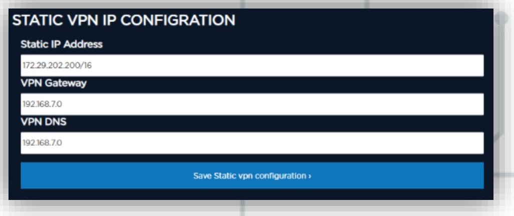
   If you are unsure of which setting to use, please contact your client's network manager and establish whether or not a DHCP server is present and accessible by the device or if a static IP address should be manually configured.



WIFI ACCESS POINT CONFIGRATION

SSID
i50-wifi
Password
secretpass
Static IP Address
10.55.55.1/24
DHCP Interface
wlan0
DHCP Address Range
10.55.55.100,10.55.55.200,255.255.255.0,24h
Default Gateway
10.55.55.1
Primary DNS Server
8.8.8.8

4. The AVLYTICS devices are supplied with a Static VPN IP address configured.
   To make changes or view the static VPN IP address, select the *'Static VPN Configration'*.



STATIC VPN IP CONFIGRATION

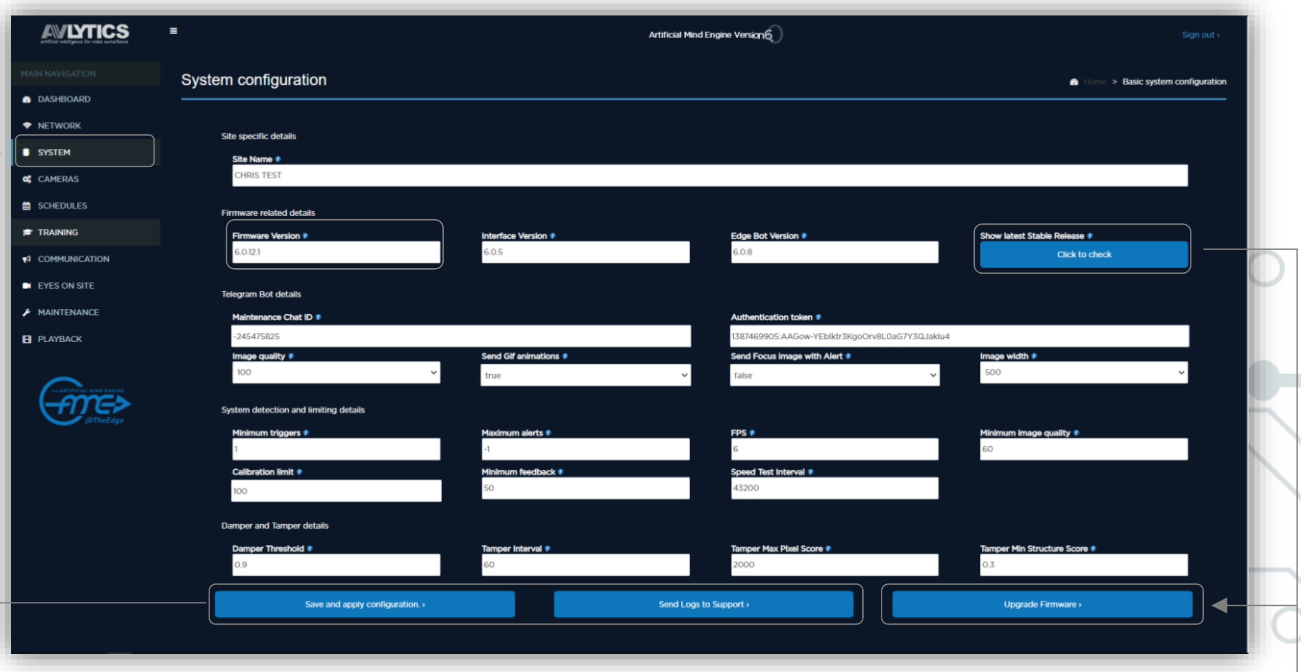
Static IP Address
172.29.202.200/16
VPN Gateway
192.168.7.0
VPN DNS
192.168.7.0

IMPORTANT NOTE

To set the Device back to DHCP, and dynamically assigned the IP Address, click on *'Obtain IP Address Automatically'* and the device will remove the LAN static IP Address and set the device back to DHCP.

4. System Menu

The system page is the main device configuration page.
The table below defines the function of each configurable setting. **These settings should be adjusted with caution and only by a trained and qualified AVLYTICS installer.**



System configuration

Site specific details

Site Name: CHRIS TEST

Firmware related details

Firmware Version: 6.0.12.1
Interface Version: 6.0.5
Edge Bot Version: 6.0.8
Show latest Stable Release

Telegram Bot details

Maintenance Chat ID: -245475825
Authentication token: 1387469905:AAGow-YEblktr3KgoOrv8L0aG7Y3QJaklu4
Image quality: 100
Send Gif animations: true
Send Focus Image with Alert: false
Image width: 500

System detection and limiting details

Minimum triggers: 1
Maximum alerts: -1
FPS: 6
Minimum image quality: 60
Calibration limit: 100
Minimum feedback: 50
Speed Test Interval: 43200

Damper and Tamper details

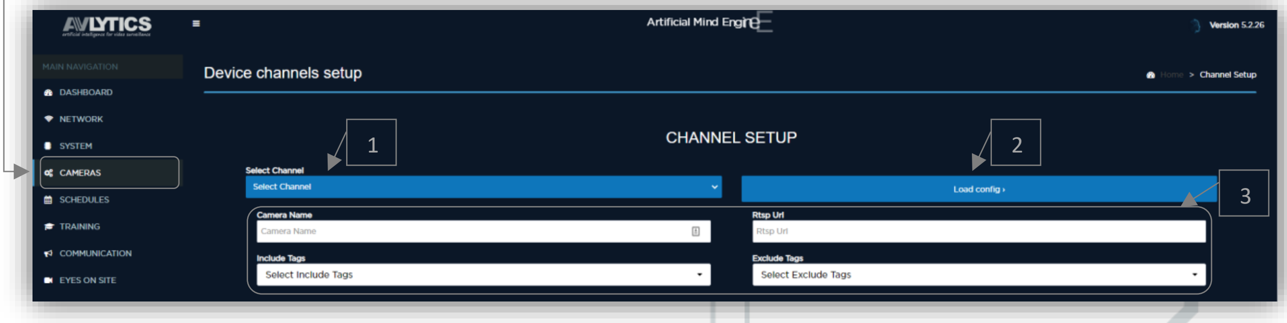
Damper Threshold: 0.9
Tamper Interval: 60
Tamper Max Pixel Score: 2000
Tamper Min Structure Score: 0.3

The AVLYTICS Developers are constantly improving the software features and hardware resource optimisations. To check if the device is on the latest stable release, click on ‘***click to check***’ button to see what the latest available firmware is. If the ‘***Firmware Version***’ on the left, is a lower value than the latest available version, please select the ***‘Upgrade Firmware’*** function to automatically set the device to the latest version, the device will edit the configuration and restart the services if once this option is selected.

After making any changes to the configuration, ensure to ‘***Save and apply configuration***’. The device will reboot with the new settings configured. If you are experiencing any issues with the device, and the device support staff request the logs, please select the ‘***Send logs to Support***’ function. The device will send a brief log to AVLYTICS support ticketing system for debugging.

5. Cameras Menu

The Cameras Menu item will allow the configuration of stream related settings. The device is preconfigured for the number of licensed channels.



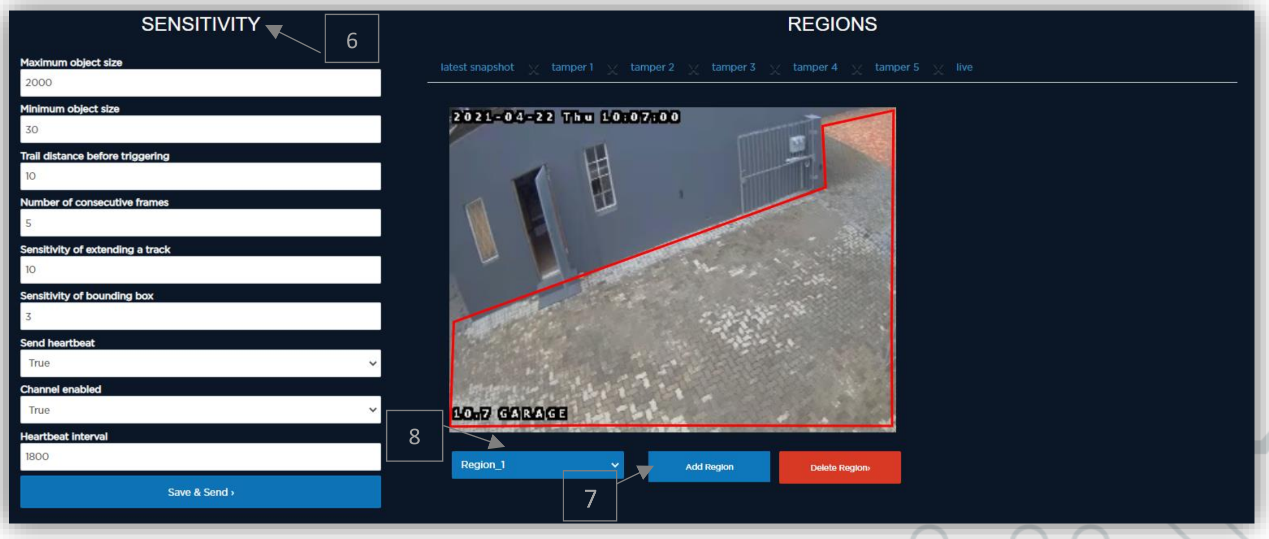
1. To configure the settings for a camera, select the channel number from the '*Select Channel*' dropdown menu.
2. Select the '*Load config*' function to load the current configuration for the selected channel.
3. There are four basic settings that should be configured before any stream analysis will commence.
   - **Camera Name** - This is to reference the camera to a particular area on the property.
   - **RTSP URL** – The RTSP URL is the Real Time Streaming Protocol destination that the device should analyse. Most of the CCTV manufacturers will have an RTSP URL to access their hardware. The most common URLs are:
     - **Hikvision** : rtsp://username:password@ip:port/streaming/channels/x0y
     - **Dahua** : rtsp://uname:pword@IP:port/cam/realmonitor?channel=X&subtype=y
     - **Avtech** : rtsp://username:password@ip:port/live/video/chX/z
     - **Provision** : rtsp://<username>:<password>@<ip address>:<RTSP port>/chID=x&streamType=z&linkType=tcp

       *** In the above URLs, the channel number = x, stream type = y and z.**
       y = stream numbers, either 0,1,2,3, or 4.
       z = stream name, either sub or main
   - **Include Tags** - The Include tags are the Tag types that are available for the device to predict in the event of any movement being detected.
   - **Exclude Tags** - The Exclude tags are the Tag types that should be excluded if predicted. The Tags that are marked with a Tick will be excluded if that are predicted which means they will be detected at the edge device and if the event is predicted to be something that is in the exclude options it will not be sent as a notification.
4. After the stream configuration is applied, adjust the sensitivity settings to suit the environment.
5. On the left of the interface are the settings that can be adjusted and on the right is a display of the region, tamper images and Live stream.

IMPORTANT NOTE

The channel and configuration loaded earlier in item 1) will be active for the settings that follow below. To change the settings on a different channel, select the channel you would like to configure and then select the "Load Config" function in item 2).

6. The Sensitivity settings will be populated with the default settings, the region section displays the latest snapshot from the selected camera. The live link will change the snapshot to a live display of the camera stream, this is useful for monitoring the detections and whether the sensitivity settings are correct for the environment.
   Any changes of the sensitivity settings will apply immediately after selecting the '***Save & Send***' button, the results of the changes can be witnessed though this live view functionality.



SENSITIVITY

Maximum object size: 2000

Minimum object size: 30

Trail distance before triggering: 10

Number of consecutive frames: 5

Sensitivity of extending a track: 10

Sensitivity of bounding box: 3

Send heartbeat: True

Channel enabled: True

Heartbeat interval: 1800

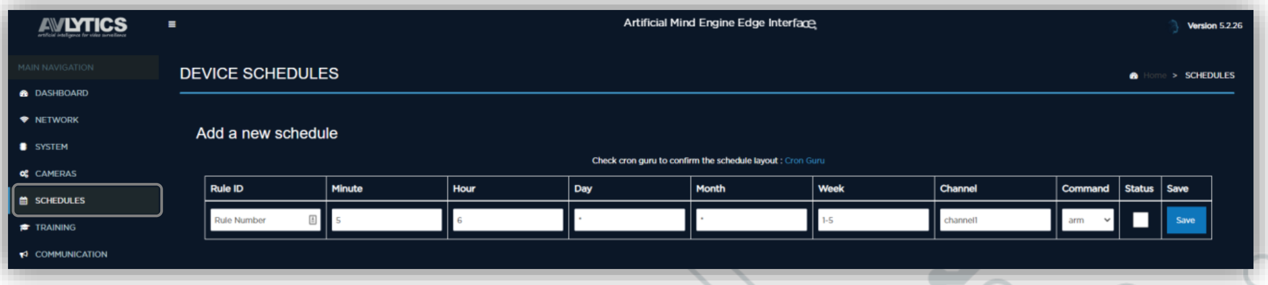
IMPORTANT NOTE

For a detailed explanation of each of the '***Sensitivity***' settings and how they should be adjusted, please refer to the Advanced Configuration Guide.

7. To create a region, or area of interest, select the '***Add Region***' function and use your mouse to draw a bounding block on the CCTV image displayed. Do this by clicking on one place, and then another area to draw a straight line. Draw multiple lines to connect the bounding box. Any activity in this area will result in a positive activation, and an alert will be generated in accordance with your settings. The region can be deleted and redrawn if required, as well as additional regions added.
8. To display or overlay the region, or area of interest, select the region name from the dropdown list located under the snapshot image.
9. **Tamper Images**: In the snapshot images there are up to 5 tamper images which the device will use to monitor whether the scene has changed significantly. The tamper images will be replaced with the latest snapshots every time the configuration is loaded. After camera installation please ensure to '***Load config***' once during the day and also at least once during the evening, do this every time the camera is adjusted or the view is changed. This will ensure that the device is aware of what the scene looks like both during day time and night time. If the scene changes significantly the device will generate a tamper alarm which will be sent to the Telegram group as well as the Armed Response Control Room (if the signal type is selected for monitoring).

6. Schedule Menu

The Schedule page allows the configuration of the automatic Arming and Disarming functionality. An Arming / Disarming schedule can be configured for each channel individually or for all channels, as the device accepts multiple schedules.



DEVICE SCHEDULES

Add a new schedule

Check cron guru to confirm the schedule layout : Cron Guru

Rule ID	Minute	Hour	Day	Month	Week	Channel	Command	Status	Save
Rule Number	5	6	*	*	1-5	channel1	arm	□	Save

To configure a schedule please input the following parameters.

- **Rule ID** - This is a descriptive value to identify the schedule.
- **Minute** - Input the exact minute at which the schedule activates.
- **Hour** - Input the exact Hour at which the schedule activates.
- **Day** - Input the day (this is for 1 particular day in the month)
- **Month** - If the schedule is to be applied to a specific month only.
- **Week** - This is the most common option. The week option accepts the following values which indicate the day of the week, and then sets this as a weekly schedule:
  - Every day of the week: 0,1,2,3,4,5, 6
  - Every week day (Mon – Fri): 1-5
  - Weekends (Saturday as 6 and Sunday as 0): 0,6
- **Channel** – The channel setting accepts values for example ‘***channel1***’ for single channels or ‘ * ’ for all channels.

IMPORTANT NOTE

Only one channel may be specified per schedule rule, if different schedules are required for different channels, for example, please create a schedule for channel1 and a separate schedule for channel2 etc.

- **Command** - The command dropdown selection box allows for either an arm command or a disarm command to be sent at the particular schedule time.
- **Status** - The status checkbox allows the schedule to be set but not activated. Please click on the status checkbox to ensure that the schedule is in fact activated.
- **Save Button** - Select the save button to apply the newly created schedule.

1. Saved Schedules Area

The saved schedules section of the page displays schedules that are already configured on the device. If multiple schedules have been configured, ensure that they are all displayed in this section.

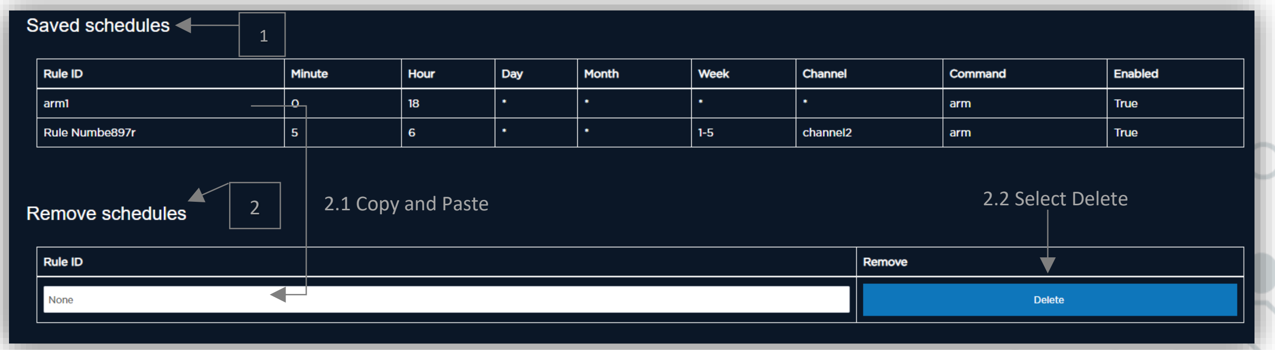
2. Remove Schedule Area

The remove schedule section of the page allows the deleting/removing of configured schedules.

2.1 To delete or remove a schedule, copy the Rule ID from the Saved schedules section of the page and paste that rule id into the Remove Schedule, Rule ID block.

2.2 Click Delete button to remove the schedule rule.

The page will refresh and the saved schedules section will be updated to display the remaining saved schedules.



Saved schedules

Rule ID	Minute	Hour	Day	Month	Week	Channel	Command	Enabled
arm1	0	18	*	*	*	*	arm	True
Rule Numbe897r	5	6	*	*	1-5	channel2	arm	True

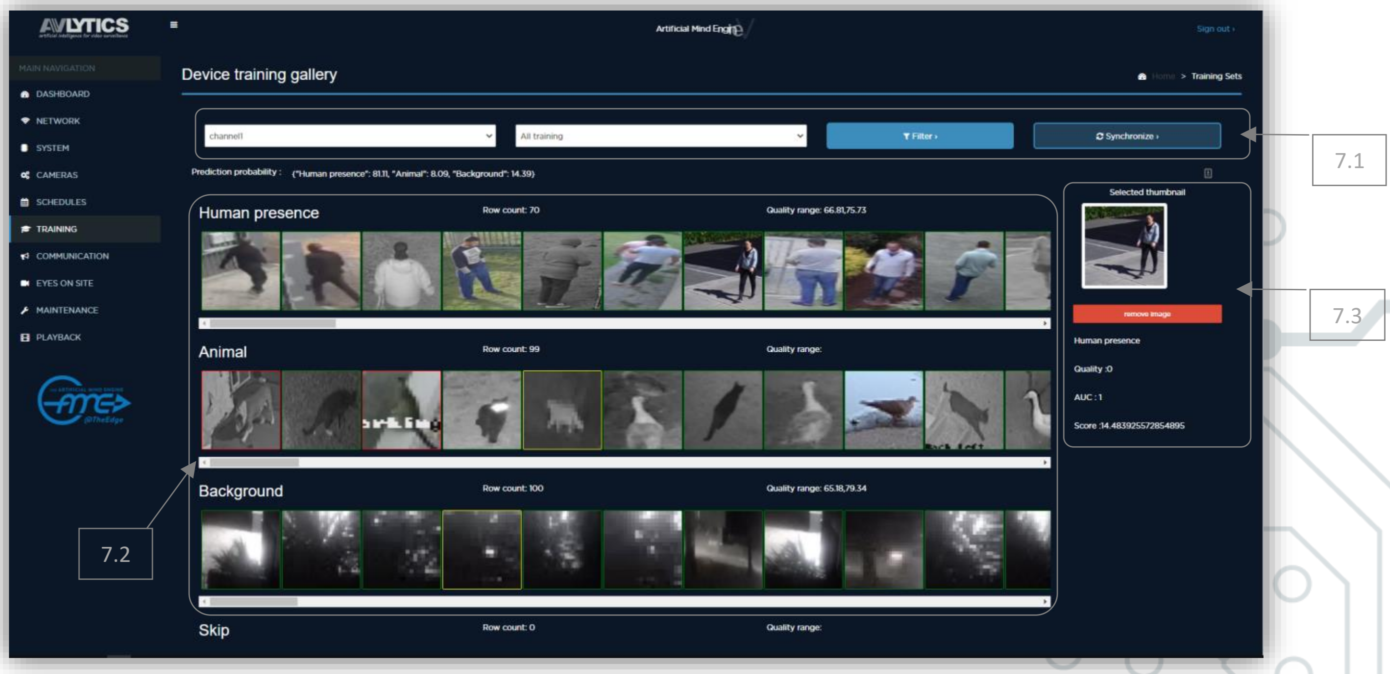
Remove schedules

Rule ID	Remove
None	Delete

7. Training

The Training page is used to assess and visualize the device's training sets per channel. The page is divided into three main sections:

1. Selection boxes, filters and synchronising
2. The visual film strip display
3. Selected thumbnail properties



Device training gallery

channel1 | All training

Prediction probability : {"Human presence": 81.11, "Animal": 8.09, "Background": 14.39}

Human presence — Row count: 70 — Quality range: 66.81,75.73

Animal — Row count: 99 — Quality range:

Background — Row count: 100 — Quality range: 65.18,79.34

Skip — Row count: 0 — Quality range:

Selected thumbnail

Human presence

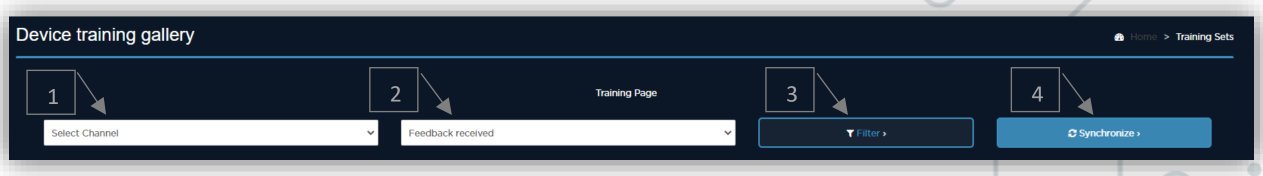
Quality :0

AUC : 1

Score :14.483925572854895

7.1 Selection Boxes, Filter and Synchronise

These are used to filter the filmstrips to a particular channel and show specific types of images.



Device training gallery

Training Page

Select Channel | Feedback received

1. From the first dropdown, select the channel of interest, you will now be working on the channel selected.
2. On the second dropdown select the alert types that should be displayed. The options are - My Training (Feedback received), My Alerts (Recent Alerts), My Defaults (Preloaded Defaults).
   - 2.1. My Defaults are preloaded images from various sites which gives the device a good start in understanding and identifying the various anomalies detected by the device.
   - 2.2. My Training filter will limit the visualization to events that have been sent to the devices as "feedback or Training ".
   - 2.3. My Alerts filters the images to display events that the device has alerted on in the last 1 Hour

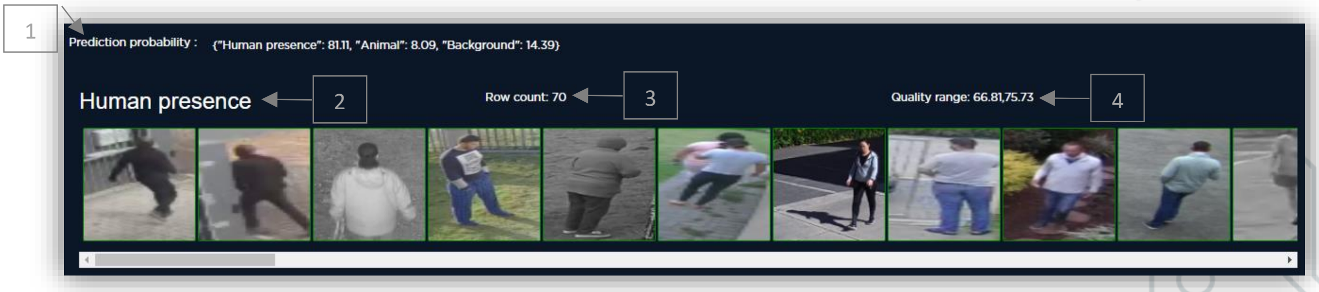
3. Filter Button: The filter button is used to filter the page to the current selection.
4. Synchronize Button: The Synchronize button is used to force the device to recalibrate its training for the particular channel.

7.2 Visual 'Film Strip" Display

After the channel and training type filters have been applied, click on filter to filter the filmstrip images.

The user interface will display a row of images for each Image category in the devices channel configuration include tag options. Each row of information will contain thumbnails of the latest 100 images in that category. Each category has the following headings:

1. Prediction Probability: The interface displays what the current training set for this channel will predict in the event of a similar detection taking place. In the example below we can see that the device's training predicts that the probability of this event being predicted as Human presence has a high probability of 81.11 which is much higher than the other categories that have similar features. In this example Background and Animal both received a score for having features in common with what is being predicted, however Human presence won the competition by over 66 points.
2. Category Name: For example - Human presence
3. Row Count: The number of images trained in this category.
4. Quality range: The range of quality levels throughout the category, for example, 66.81 to 75.73


Prediction probability : {"Human presence": 81.11, "Animal": 8.09, "Background": 14.39}

Human presence

Row count: 70

Quality range: 66.81,75.73

IMPORTANT NOTE

If the quality range is vast or has a difference of more than 10 points, it means the device will not be as accurate as if the quality range were for example 5 points apart. The smaller the quality range the more accurate the predictions will be. The quality range is directly related to the detection resolution.

In the "Human Presence" Film Strip above, you can see that the Quality Range is just below the recommended threshold of 10 points (66.81 - 75.73).

Problem Solving Tools:

Coloured Borders on Images:

The images are colour coded as to the status of each image in the training Set.
The colour coding is representative of the following conditions:

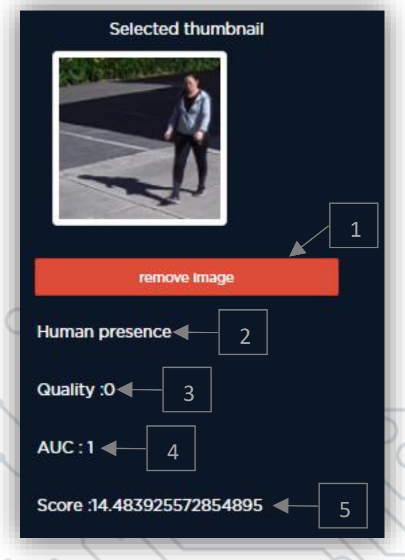
- **Green**: An Image with a green border illustrates that the particular image conforms with the rest of the category and is a **good example** / sample of what the device will categorise as that particular category.
- **Yellow**: An Image with a yellow border illustrates that the particular **image does not conform** with the rest of the images in that category or that the difference between this image and the rest of the images is greater that should be expected and misclassification can be expected when the device makes a prediction on an anomaly.
- **Red:** An Image with a Red border illustrates that the particular **image does not conform** with the rest of the training set for that category or that the device believes that **this image belongs in a completely different category**. In these conditions misclassifications are expected and corrective action should be taken to improve the devices prediction accuracy.

Row Count Less than 50:

- The device has a configuration option called '*min_feedback*', which represents the minimum number of sample images a category should have for the device to use that category when making predictions.
- If this number has not been reached or a ***value less than 50*** is represented in the heading of the row (Row Count), it means the ***device will not use that category when predicting on an anomaly***. In These conditions all of the images will have a red border as this tag has not been calibrated to compete.
- Corrective action is to train more images of that category on the particular channel in question.

7.3 Selected Thumbnail Properties

The properties window will allow the user to view and manipulate the device's training. To view a thumbnail or particular images properties, click on the thumbnail image and the properties will be displayed on the right of the interface.



Selected thumbnail

Human presence

Quality :0

AUC : 1

Score :14.483925572854895

1. The user is able to remove or delete the selected image from the training set by selecting the thumbnail image in the film strip and clicking on the '***remove sample***' button. This will instruct the device to locate this image in the database and remove it from the training set for that channel.
2. The class classification of the image selected in the film strip will indicate whether the image has been predicted as Human, Animal, Vehicle or Background.
3. Quality Score: Shows a pixel per meter equivalent value which represents the quality of the detection. Default images will have a Score of 0 as the quality cannot be measured comparing the image to the current environment as it was a preloaded default sample. As the device receives training it will prioritize which events are used in the training set. The default images will be overwritten as the device learns in its current environment.

4. AUC Value: This represents the Area Under the Curve, which is a scientific measurement to ensure conformity or equality. All samples should have an AUC value of 1. If the AUC is 0 it means the device believes that this sample is in the incorrect category.

5. Error Score: This value is a visual indication as to the deviation from the norm or mean of a particular category. The higher the error score, the higher the probability of the selected sample degrading the devices training on this channel.

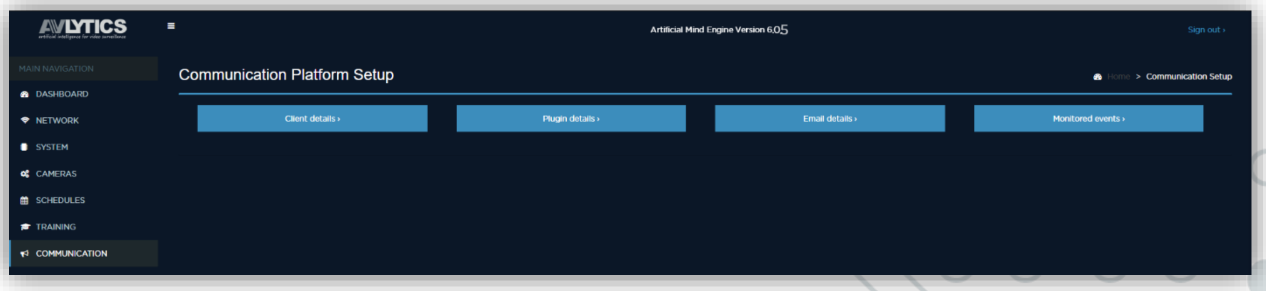
IMPORTANT NOTE

Please note that the device is **not self-learning** and training will need to be applied from either the SeeingAME Hub or AVLYTICS Software to improve the device's accuracy.

8. Communication Platform Setup

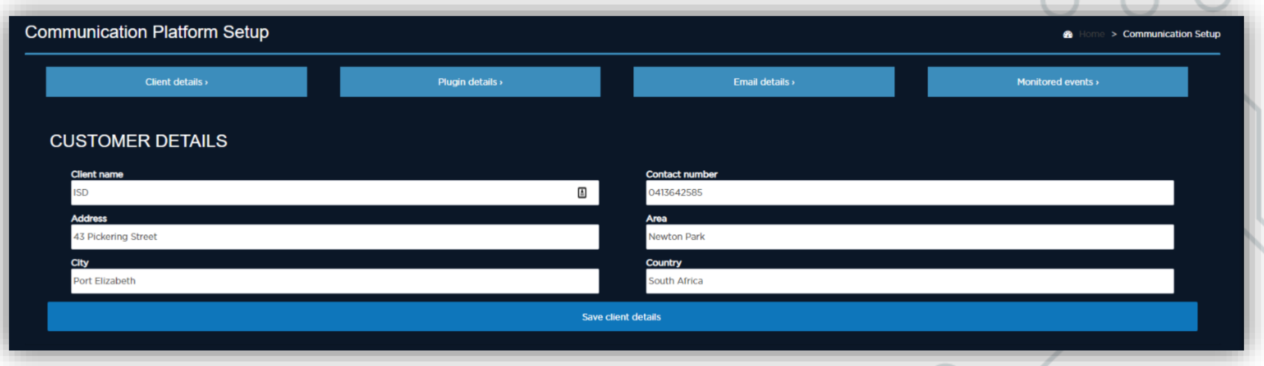
The Communication page is used to configure how, when and to which control room environment the device should send notifications and alerts. The page is divided into four sections:

1. Client details
2. Plugins details
3. Email details
4. Monitored Events



8.1 Customer Details

The customer details section allows the user to configure some site specific details which will be used to identify the device. These values do not have any impact on the operation of the device and are only used as for customer reference.



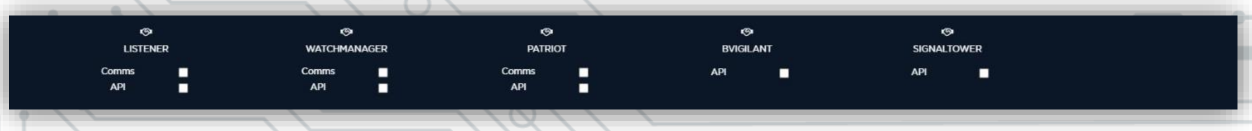
CUSTOMER DETAILS

Client name: ISD
Contact number: 0413642585
Address: 43 Pickering Street
Area: Newton Park
City: Port Elizabeth
Country: South Africa

8.2 Plugins

The Plugins section is of critical importance, **configuration in this area should be carried out with caution** as even small configuration issues can cause the device to stop reporting to a control room. The AVLYTICS devices support third party integration. Below is a list of control room packages that AVLYTICS can integrate with.

8.2.1) Control Room Software: The device is capable of reporting to various software platforms, the device can report to multiple platforms simultaneously.



LISTENER
Comms □
API □

WATCHMANAGER
Comms □
API □

PATRIOT
Comms □
API □

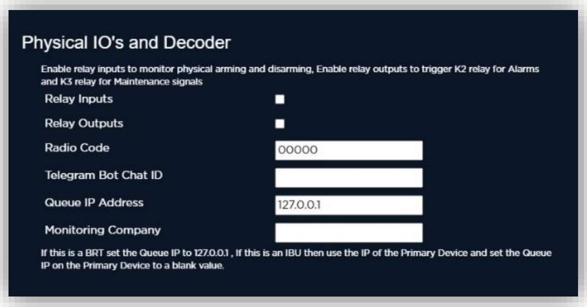
BVIGILANT
API □

SIGNALTOWER
API □

There are two integration mechanisms:

- **Comms** – This is an Integration protocol that requires AVLYTICS Comms third party software to be installed in the control room, on a PC that has network communication to the Control Room Package communication server.
- **API** – The **A**pplication **P**rogramming **I**nterface option allows the device to communicate directly to the control room, via the control room package API's.
  If API is selected and the relevant information configured to enable the integration, no additional software is required in the control room.

8.2.2) Physical IO's and Decoder Setup.



Physical IO's and Decoder

Enable relay inputs to monitor physical arming and disarming, Enable relay outputs to trigger K2 relay for Alarms and K3 relay for Maintenance signals

Relay Inputs	□
Relay Outputs	□
Radio Code	00000
Telegram Bot Chat ID	
Queue IP Address	127.0.0.1
Monitoring Company	

If this is a BRT set the Queue IP to 127.0.0.1 , If this is an IBU then use the IP of the Primary Device and set the Queue IP on the Primary Device to a blank value.

This option allows the user to select whether or not Relays are triggered in the event of a prediction taking place.

Relays Inputs - Tick to enable Physical inputs (Arming / Disarming & Mains Failure).
Relay Outputs - Tick to enable Output triggers on BRT.

IMPORTANT NOTE

Relay Output Functions :

- K1 will activate when the device is Armed.
- K2 will activate on a Valid Video Event (ie. Human presence).
- K3 will activate on any Maintenance Event (ie. Video Loss, Mains failure).
- K4 will activate in the event of a Power failure.

Radio Code - This is the code that is assigned to the site decoder in the control room software configuration. This is also referred to as an Xmitter number or Radio Number. Please request the account code from the monitoring Company and type in the given value.

Telegram Bot Chat ID - This is used to specify which Telegram maintenance group the device uses for two way communication.

Queue IP - The Queue IP allows the device to receive event from a different device. On a **BRT** device ensure that the Queue IP is configured at **127.0.0.1** , this instructs the device to process its own alerts. If the device is an **IBU** then ensure that the Queue IP is the **Local IP Address** of the main AVLYTICS device.

Monitoring Company - This option provides flexibility in the monitoring process, so that the device may be added to Client A's HUB, but actually report its events to Client B's Control Room.

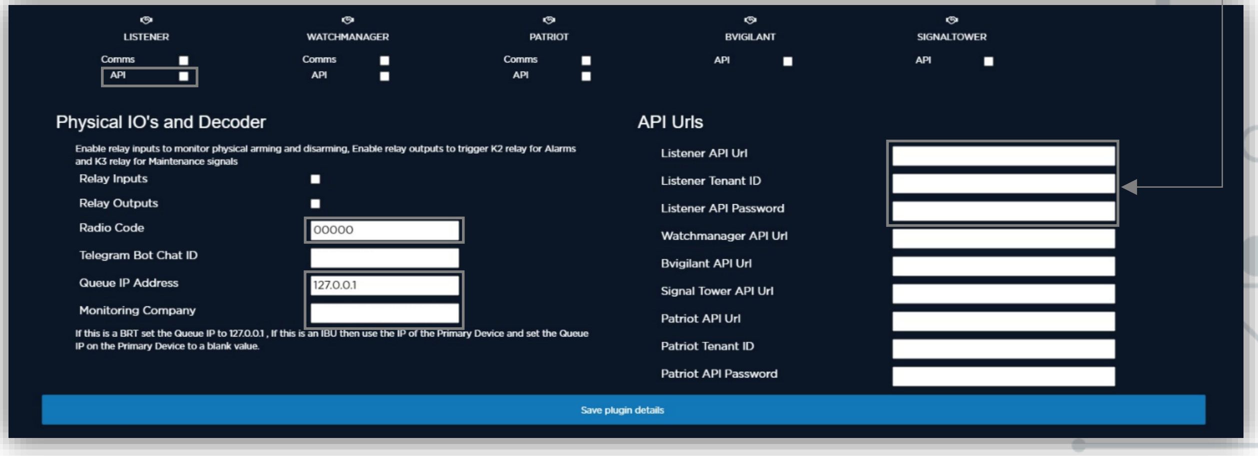
IMPORTANT NOTE

If this option is used contact AVLYTICS tech support to configure the rerouting in the backend of the device. Changing the Value without changing the backend routing will result in messages not getting through to the Control room.

8.2.3) API URLs

When using an API to report events into the control room, ensure to complete the following configuration options.

- If using an API, request the API details from your Control Room Software Package representative.
- An example of API Configuration for Listener Control Room Software.
  Request the details from your Listener representative.
  1) Listener API URL.
  2) Listener Tenant ID.
  3) Listener API Password.



LISTENER	WATCHMANAGER	PATRIOT	BVIGILANT	SIGNALTOWER
Comms □	Comms □	Comms □	API □	API □
API □	API □	API □		

Physical IO's and Decoder

Enable relay inputs to monitor physical arming and disarming, Enable relay outputs to trigger K2 relay for Alarms and K3 relay for Maintenance signals

Relay Inputs □

Relay Outputs □

Radio Code: 00000

Telegram Bot Chat ID:

Queue IP Address: 127.0.0.1

Monitoring Company:

If this is a BRT set the Queue IP to 127.0.0.1 , If this is an IBU then use the IP of the Primary Device and set the Queue IP on the Primary Device to a blank value.

API Urls

Listener API Url:

Listener Tenant ID:

Listener API Password:

Watchmanager API Url:

Bvigilant API Url:

Signal Tower API Url:

Patriot API Url:

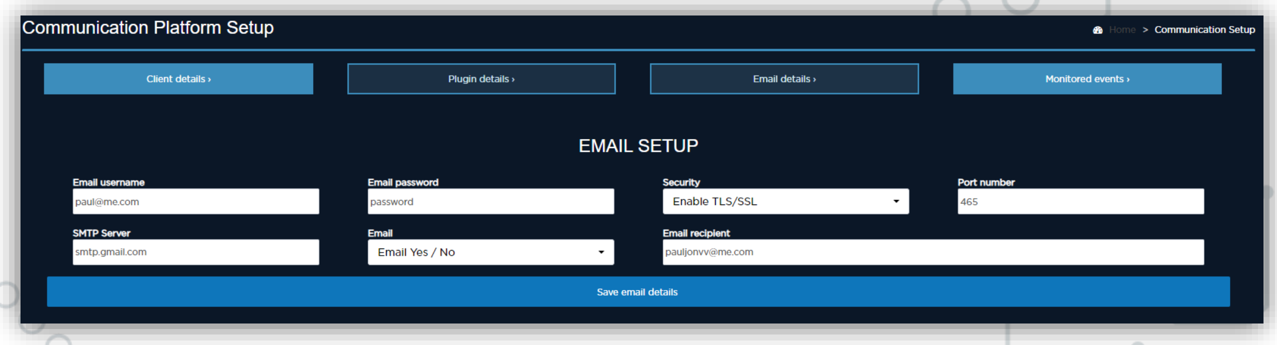
Patriot Tenant ID:

Patriot API Password:

- Ensure to '*Save plugin details*' on completion of the setup.

8.3 Email Setup

The Email setup facility is provided to allow for notifications to be sent via Email opposed to Telegram. The device is capable of reporting to multiple platforms simultaneously, if Email notifications are not required, these configuration options can be ignored.



EMAIL SETUP

Email username: paul@me.com

Email password: password

Security: Enable TLS/SSL

Port number: 465

SMTP Server: smtp.gmail.com

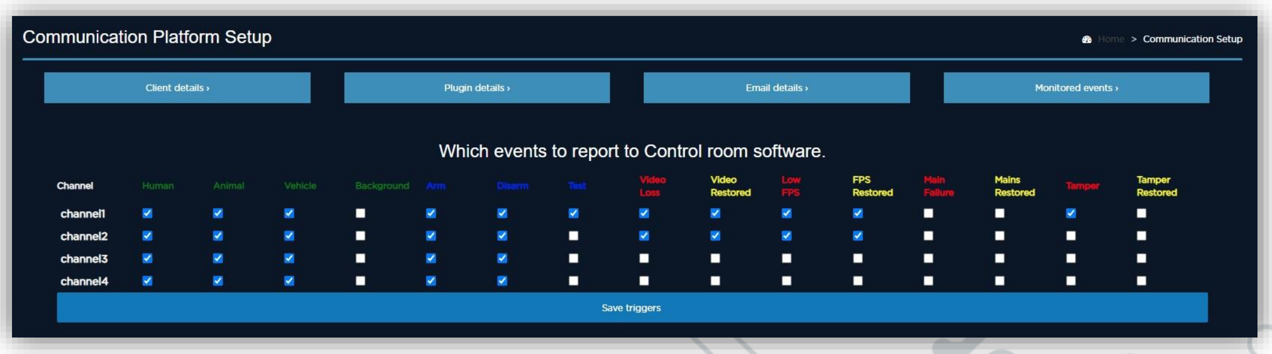
Email: Email Yes / No

Email recipient: pauljonvv@me.com

The email setup section requires the user to input the sender's account information (the same sender account information can be used on multiple devices).
The email message destination will be the email address configured in the Email Recipient input box.
The device sends emails to one recipient of your choosing, do not input more than one address.

8.4 Monitored Events

The monitored events section outlines the current control room reporting criteria. Here you are able to specify which event types should be sent to the control room package, if the control room package integration is enabled.



Communication Platform Setup

Which events to report to Control room software.

Channel	Human	Animal	Vehicle	Background	Arm	Disarm	Test	Video Loss	Video Restored	Low FPS	FPS Restored	Main Failure	Mains Restored	Tamper	Tamper Restored
channel1	☑	☑	☑	□	☑	☑	☑	☑	☑	☑	☑	□	□	☑	□
channel2	☑	☑	☑	□	☑	☑	□	☑	☑	☑	☑	□	□	□	□
channel3	☑	☑	☑	□	☑	☑	□	□	□	□	□	□	□	□	□
channel4	☑	☑	☑	□	☑	☑	□	□	□	□	□	□	□	□	□

The Event types are colour coded for your convenience and indicate which notifications will be received in your control room software.

- Green event types are selected per channel, and you can choose to have Human, Animal, Vehicle or Background video related events sent to the control room.
- Blue event types are informational messages that are sent to the control room, such as when the device is Armed, Disarmed or Test signals are received.
- Red event types are failure alerts and include:
  - Video loss signal - received if a video stream becomes unavailable.
  - Low FPS signal - received when the stream coming from the cameras or DVR is less than the minimum frames per second.
  - Mains failure - received in the event of a power failure.
  - Tamper alert- received if a camera is tampered with.
- Yellow event types are the Restoral Signal/ Notification that is received if the device corrects the failure automatically.

For each Red event type there is a corresponding Yellow event.

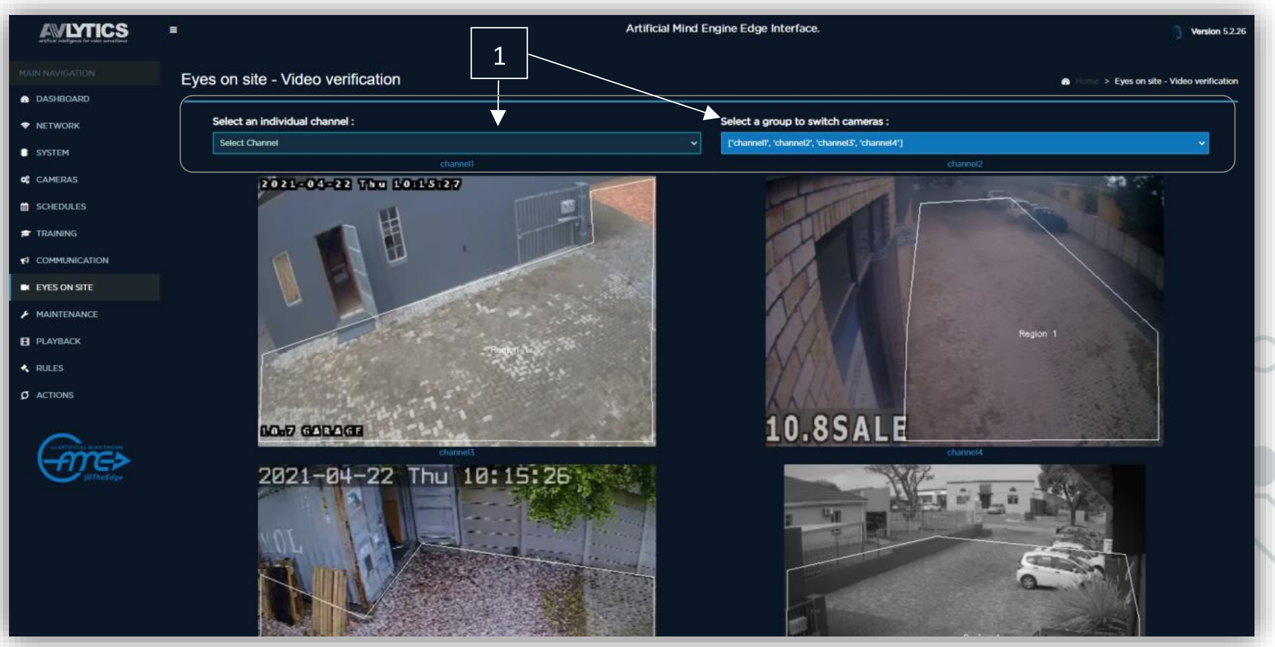
To ensure that you receive these signals, Tick the related check boxes to instruct the device to send these event type to the control room software.

IMPORTANT NOTE

After performing all the configuration changes, select the ' ***Save triggers*** ' option for the device to restart, using the newly configured changes.

9. Eyes on Site

The eyes on site page is used for visual verification of configured parameters.



Eyes on site - Video verification

Select an individual channel : Select Channel

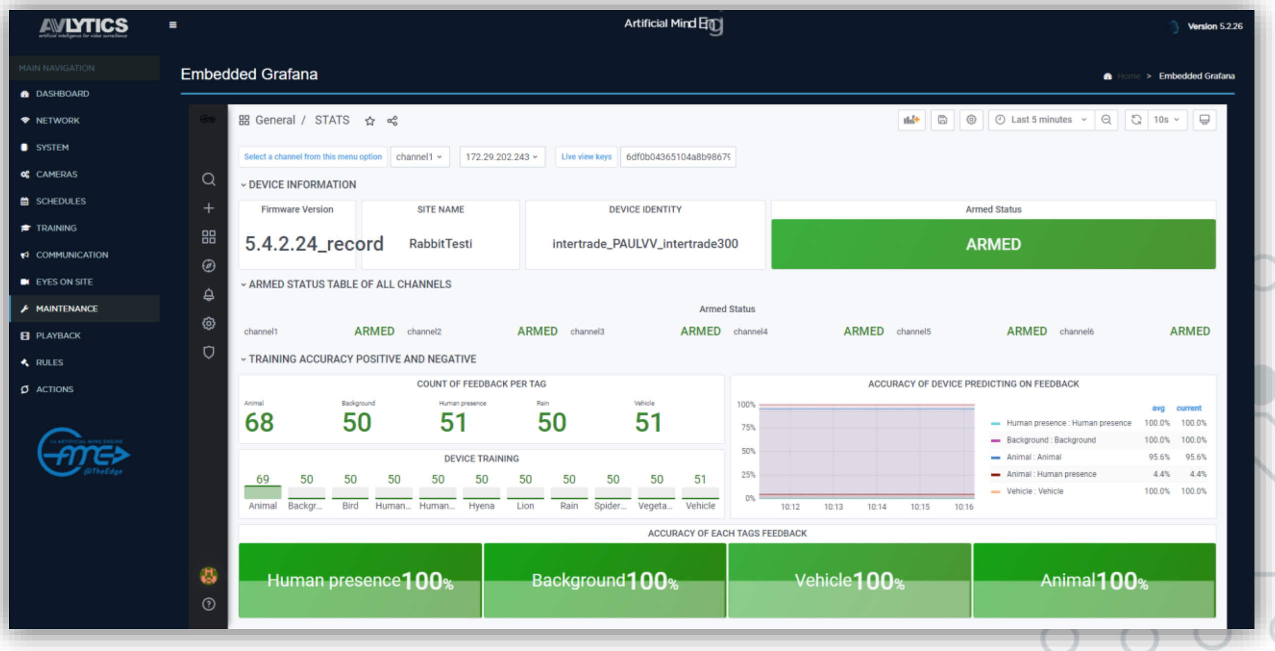
Select a group to switch cameras : ['channel1', 'channel2', 'channel3', 'channel4']

1. There are two options to view the live streams, either a single channel view mode or a multi-channel view mode.

- Select a channel from either single or multichannel drop downs and the device will present a live stream of the selected channel.
- In the live stream the user can observe three key aspects:
    - **The region of interest** - will be overlaid on the live stream as a thin, white line. **Ensure that a region is present or no predictions will take place.**
    - **Detected objects -** will be framed with a green box and followed with a green "tail". As an object moves in the field of view the parameters relating to the detection are displayed as **Meta Data** and overlaid on the live stream image. These parameters include, **Blob size** (the size of the object being tracked), **Displacement** (the distance an object has moved since tracking started), **Quality** (the quality of the features being extracted from the object detected).
    - **Predictions -** objects framed in a Green bounding box, which enter the region will immediately change from a **Green** bounding box to **Red** bounding box. This indicates that the device has made a prediction on the object and will send an alert (only if the device has been configured to send alerts on that particular event type, for example: no animal predications will come through if it was not selected as an ' ***Event Type*** ' alert).

10. Maintenance

The Maintenance Page is an embedded graphing and diagnostic utility that allows the user to inspect the devices performance and configuration. Please refer to the **Grafana user manual** for an in-depth guide on how to use the Grafana tool.



Embedded Grafana

Select a channel from this menu option: channel1 · 172.29.202.243 · Live view keys: 6df0b04365104a8b9867

DEVICE INFORMATION

Firmware Version	SITE NAME	DEVICE IDENTITY	Armed Status
5.4.2.24_record	RabbitTesti	intertrade_PAULVV_intertrade300	ARMED

ARMED STATUS TABLE OF ALL CHANNELS

Armed Status

channel1	ARMED	channel2	ARMED	channel3	ARMED	channel4	ARMED	channel5	ARMED	channel6	ARMED

TRAINING ACCURACY POSITIVE AND NEGATIVE

COUNT OF FEEDBACK PER TAG

Animal	Background	Human presence	Rain	Vehicle
68	50	51	50	51

DEVICE TRAINING

Animal	Backgr...	Bird	Human...	Human...	Hyena	Lion	Rain	Spider...	Vegeta...	Vehicle
69	50	50	50	50	50	50	50	50	50	51

ACCURACY OF DEVICE PREDICTING ON FEEDBACK

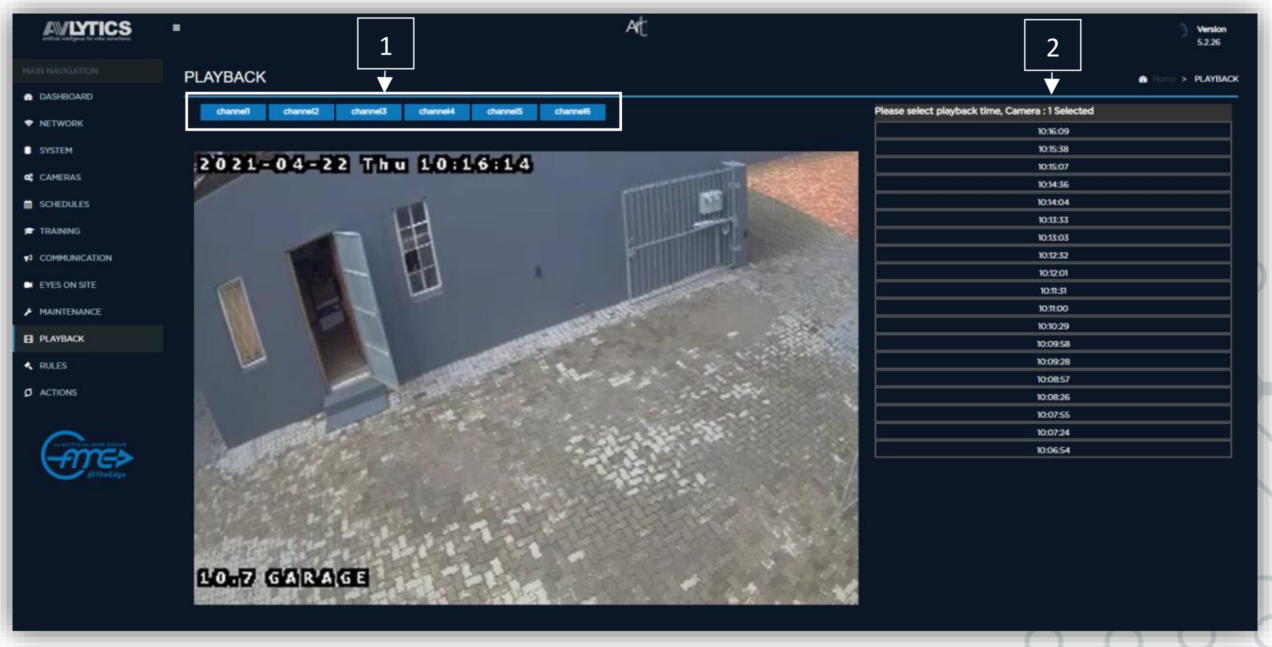
	avg	current
Human presence : Human presence	100.0%	100.0%
Background : Background	100.0%	100.0%
Animal : Animal	95.6%	95.6%
Animal : Human presence	4.4%	4.4%
Vehicle : Vehicle	100.0%	100.0%

ACCURACY OF EACH TAGS FEEDBACK

Human presence	Background	Vehicle	Animal
100%	100%	100%	100%

11.Playback

The playback menu option allows the using to view the last 10 minutes of recording per channel, which the recorder displays in 10 second video clips.



Please select playback time, Camera : 1 Selected

10:16:09
10:15:38
10:15:07
10:14:36
10:14:04
10:13:33
10:13:03
10:12:32
10:12:01
10:11:31
10:11:00
10:10:29
10:09:58
10:09:28
10:08:57
10:08:26
10:07:55
10:07:24
10:06:54

1. To access the playback, click on the channel button.
2. The list of recorded files will be displayed on the right of the screen, click on the time to play the recorded footage for that particular time.

End of Document

Thank you