User Manual

FENCE Monitoring System

Advance Communications Sdn. Bhd.

VERSION 2.0

Table of Contents

Overview

FENCE monitoring system is a web application used together with the FENCE hardware provided by Advance Communications Sdn. Bhd. The monitoring system can be viewed via a web browser and function with existing CCTV monitoring applications as well as a standalone application.

This product is currently version 2, inheriting some of the previous version's design. User's familiar with version 1 of the FENCE monitoring system may find the interface slightly similar albeit improved.

The manual is divided into 2 major section, one feature configuration know hows and one feature the operational manual. A final minor section details about the AI-based detector software with a brief showcases of captured images as well as a user guide on camera positioning.

Basic Manual

This is a preface section describing basic operations that one should know in order to use the system.

Login and Navigation

As Administrator

To login as an administrator, first open up a web-browser and navigate to the IP address in which the system is installed on. In our example, the server is installed on the same machine as the web viewer, and we use the loopback IP address (127.0.0.1 or localhost). For installations on DIFFERENT machines, navigate to the following page :

http://<SERVER_IP>:1337/admin/auth/login

where one would replace <SERVER_IP> with the IP address of the machine with the system installed. The administrator port is by default bound to port number 1337. A sample login from the web-browser is shown in figure 1. The URL used in the example is framed in a blue rectangle.

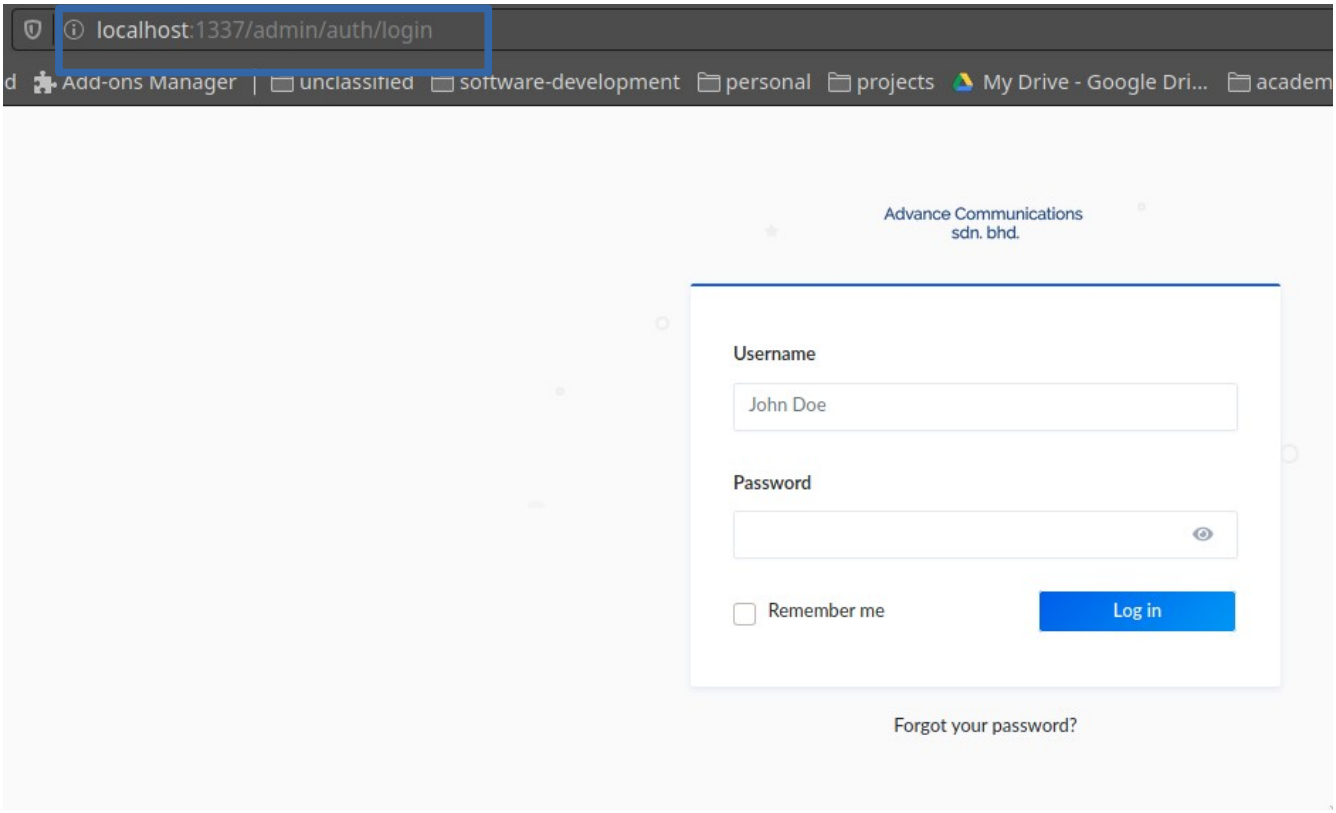


Figure 1

The default login and password is provided by the technician installing the software. Once login, the admin will be greeted by the following page shown in figure 2.

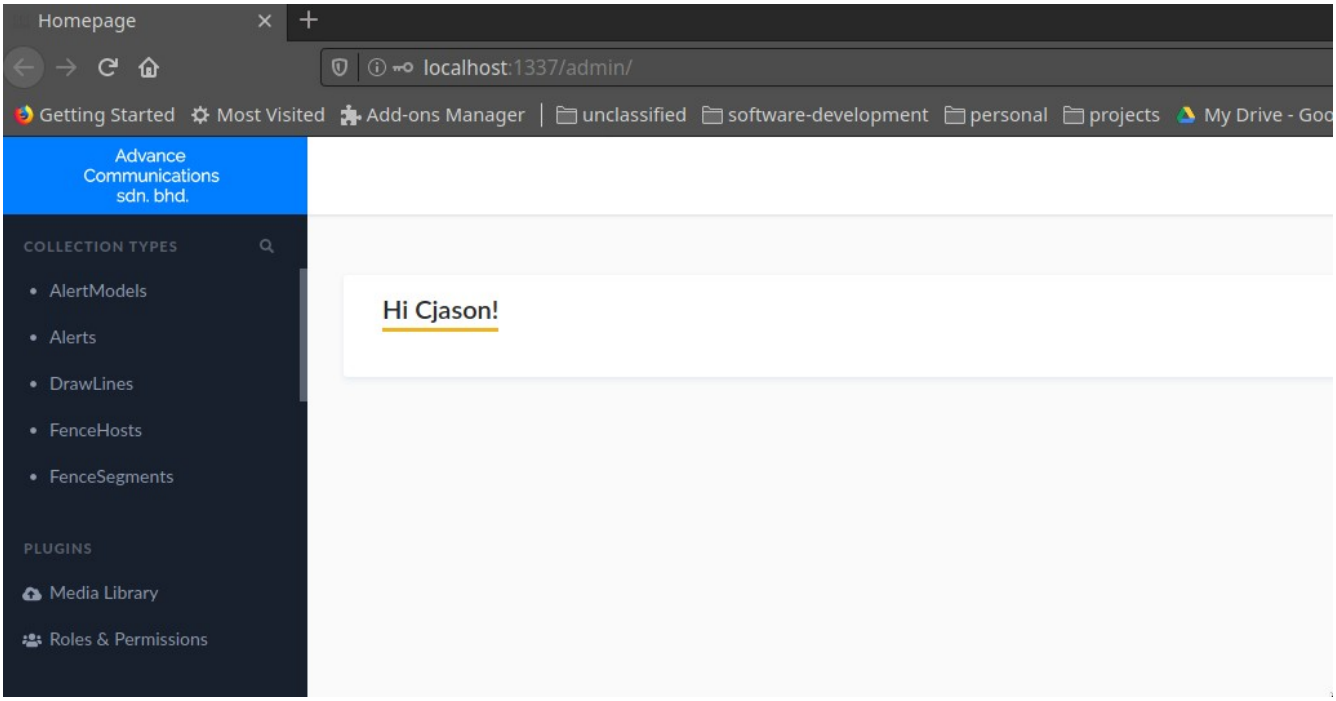


Figure 2

From here, the administrator can perform various actions such as adding new fence segments, IP cameras and view the alerts.

The administrator may click on the menu items on the left (i.e., AlertModels, Alerts etc.) to view them and/or modify them. Additionally, the administrator may also add new users as viewers or admins to the systems through “Collection Types” → “Users”. Different Roles and Permissions may be assigned accordingly from the “Roles & Permissions” menu item.

As Security Operator

The security operator logins on a separate portal. The url to login is as follows :

http://<SERVER_IP>:4000/login

An example of the login page is shown in figure 3. On successful login, the operator will be greeted by a page shown in figure 4.

From figure 4, the operator may choose to navigate into various links (i.e., Profile, Map, Focus, Host Status etc.) Each of this link has its own use and should be viewed by a separate monitor if possible. The uses are described in detail in the “Operator” section found in further sections of this manual.

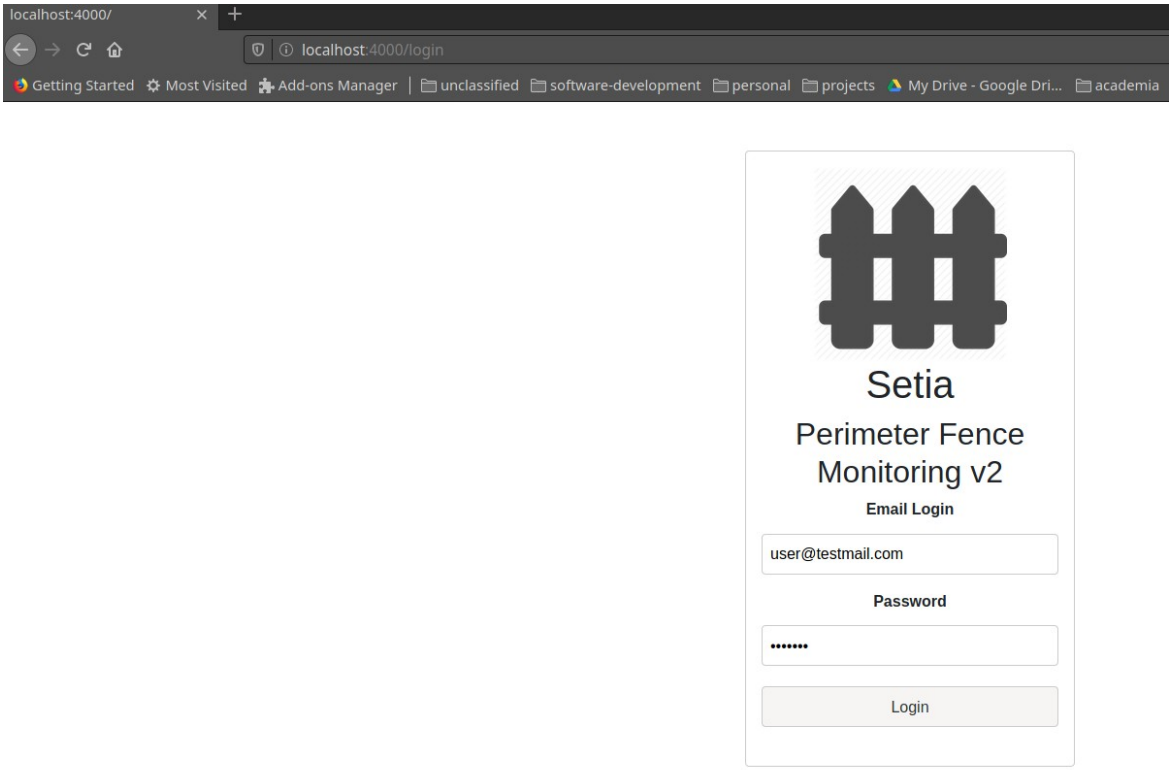


Figure 3.

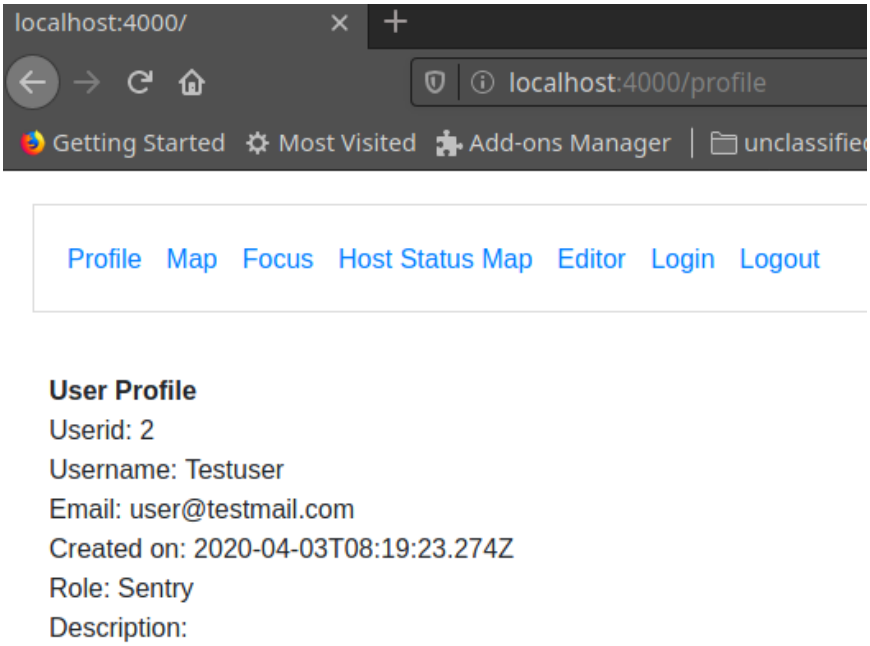


Figure 4.

Admin Section

Users

The password provided by the technician can be changed in the “User” menu under the page shown in figure 2 (Type in “User” in the search bar under “Collection Types”). Users can be added or modified from this page as shown in figure 5.

To add a new user, click on “Add New user” on the top right side of the screen and key in the details accordingly. To modify a user attribute (such as passwords), the admin may click on the user to be modified, which will bring up a page shown in figure 6.

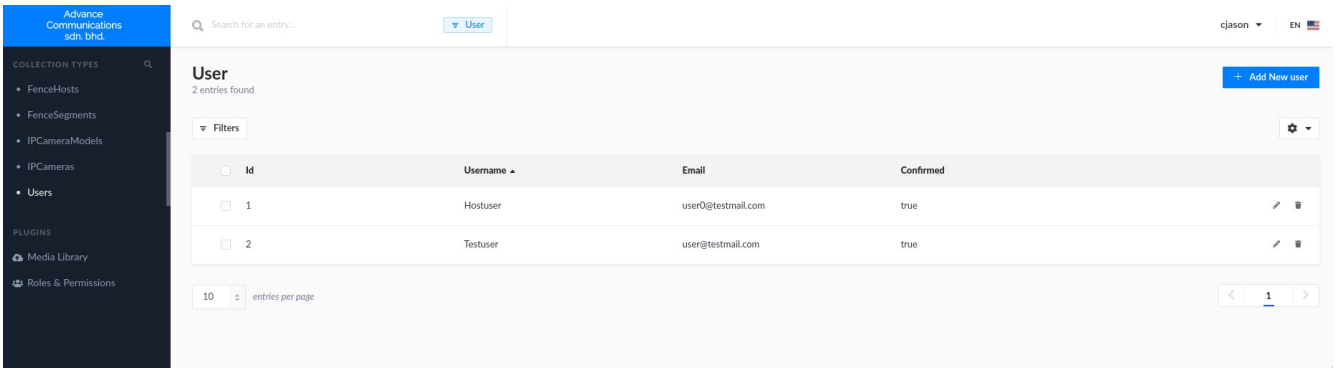


Figure 5.

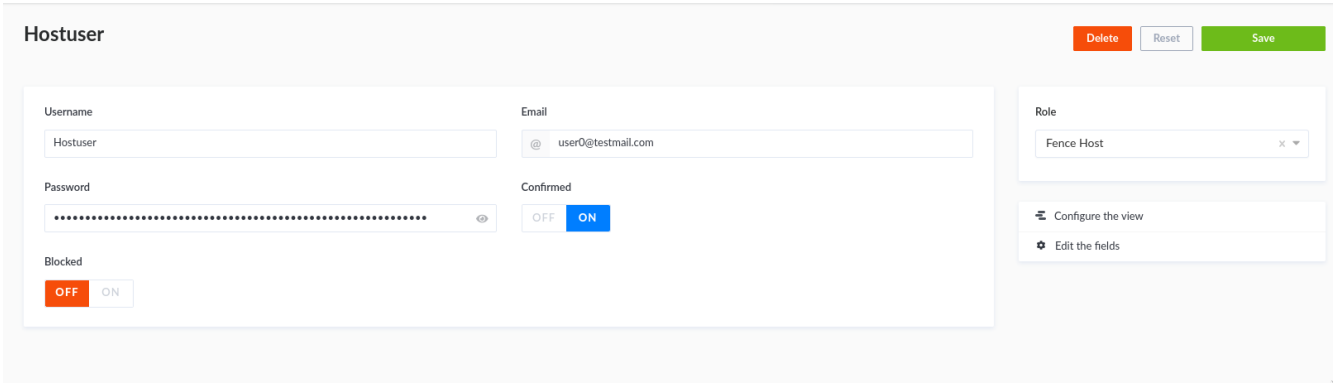


Figure 6.

Users may also be assigned different roles (Selected from the right side) as shown in figure 6. However, the role and its permissions must be first configured (Please refer to the installing technician on whether a permission is safe to be enabled or not).

FENCE Elements

FENCE elements may be added/modified through a few data types. Typically, a FENCE monitoring host controller requires its own record in the database as well as a well defined FENCE segments and AlertModels in order for the system to work. **The end-user is strictly advised against performing this setup themselves and should seek help from a technician during installation.** This manual will detail how to modify FENCE elements should there be a need to do so.

FENCE HOST

A FENCE host is the central controller combining multiple segments together. Figure 7 shows a sample configuration with 1 host. A host serves as a logical unit to join up multiple segment. The host is responsible for pushing any alert from any of its segments to the server. The only attribute that can be configured without risk of breaking the system is the HostName. This is the name that will be displayed when an alert arises, indicating which host is responsible for triggering the alert and thus allowing the operator to identity the corresponding region and segment.

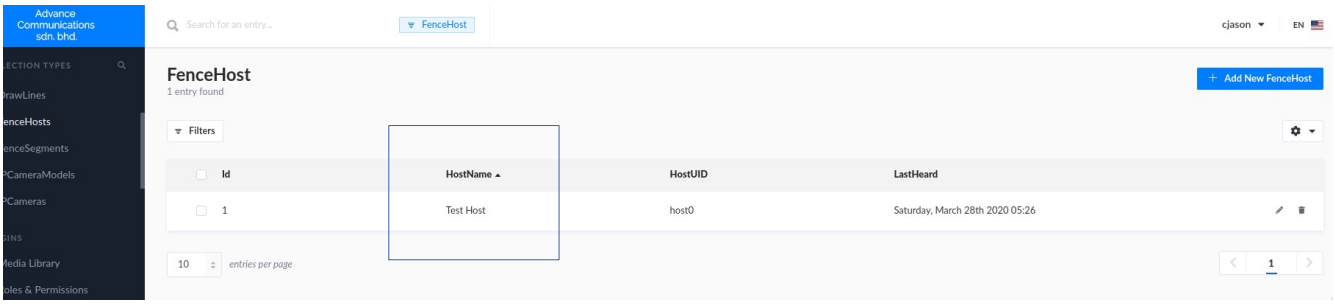


Figure 7.

One may also observed that a “LastHeard” field is present to indicate when does the host last replied to the server’s heartbeat queries. All segment under a host that has failed to reply to the hearbeat will be drawn **BLACK** in the operator’s “Host Status Map” to indicate an unresponsive host, which should then be checked for malfunctions or damage.

FENCE SEGMENT

A FENCE segment is a logical unit combining several sensors together. Every alert triggered by a host will have an “Origin” segment, which means that the host detected a sensor on the “Origin” segment has been disturbed. A segment need not be a straightline and can be multiple line segments which can account for a curved fencing area. Figure 8 shows the table with one sample segments. Similarly to a FENCE host, the only attribute that can be configured without risk of breaking the system is the SegmentName. This name will be displayed when an alert arises, and could be used to indicate which parts of the area that the user is trying to guard is being infiltrated.

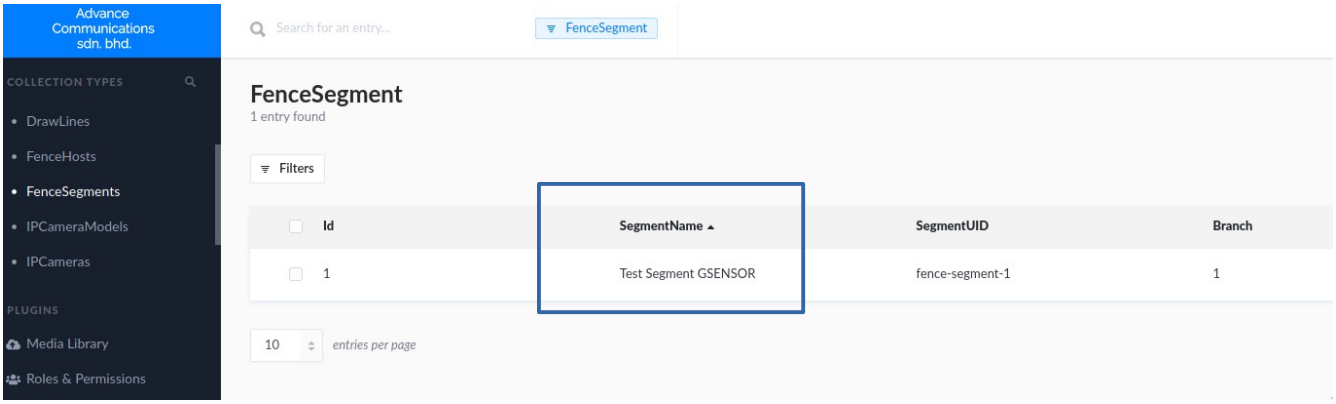


Figure 8.

A Segment must belong to a Host element. An orphaned segment cannot trigger alerts. Please be mindful when editing the configuration as it might cause some segments to not trigger. This manual advise only an experienced admin or technician should modify the configurations for FENCE Host, Segment and IP Cameras.

IPCameras

IPCameras can be configured through the menu “IPCamera” and “IPCameraModels”. An IPCameraModel represents a specific model of IPCameras by a manufacturer. A sample list of models are shown in Figure 9.

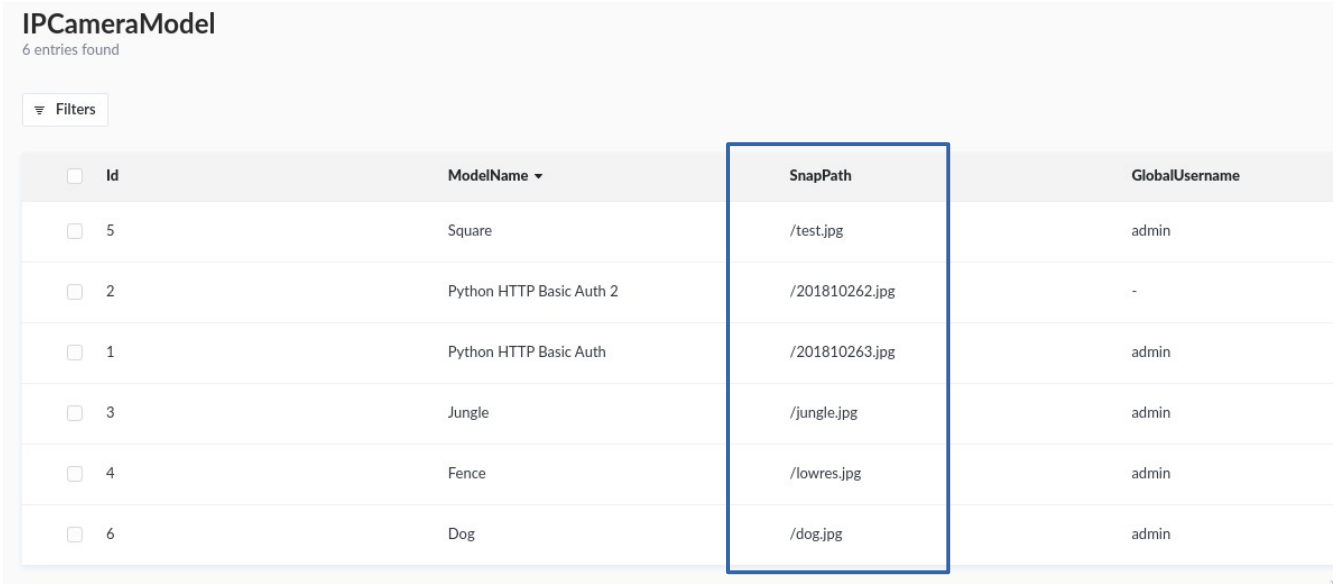


Figure 9

Once a model is configured, New IPCameras can be added and assigned with the same model type. This allows the server to capture still images or obtain the MJPEG / H.264 stream from the camera in the event of an alert being triggered.

It is important to have “SnapPath” be configured correctly. This field represents the URL PATH in which the server will attempt to obtain a still image from the IP Camera. This field should be carefully configured or the server will not be able to obtain the images from the IP Cameras. The URL PATH MUST begin with a forward slash ‘/’ followed with the PATH given by the respective camera models. For example, the sample models in figure 9 “Square” shows that *t*est.jpg is the path to obtain the image from the “Square” camera model. This meant that the server will attempt to access https://<CAMERA_IP>/test.jpg when an alert associated with a camera of type “Square” is triggered.

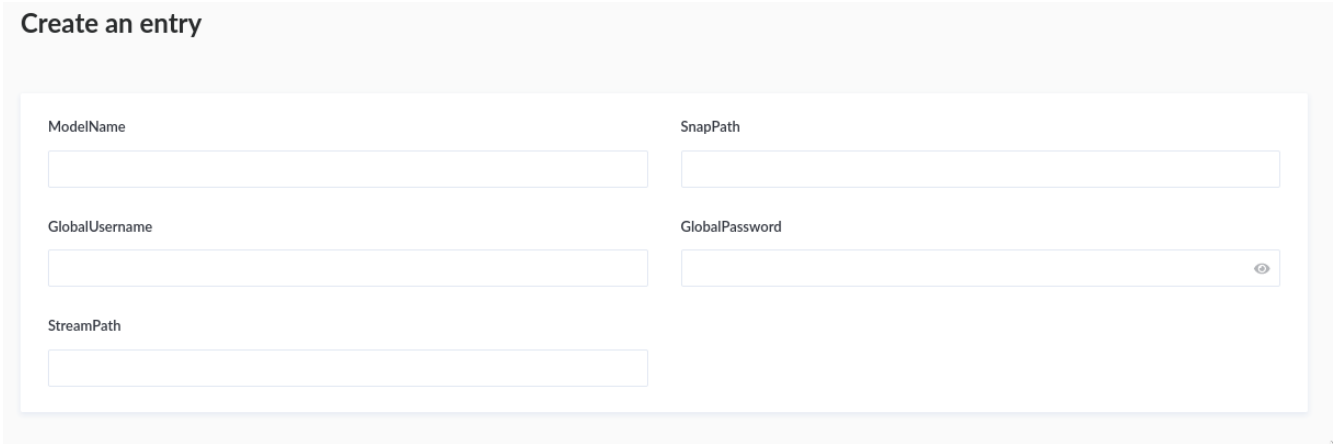


Figure 10

Figure 10 shows a form to create a camera model. The “GlobalUserName” and “GlobalPassword” field are for cameras that the user wants to have **SAME** password for all of its types. If the user wants to configure with unique usernames and passwords for EACH camera, refer to the IPCamera Creation section below. “StreamPath” should be left empty if the user does not want to stream the MJPEG / H.264 feed during alert triggering. The field should ALSO include the streaming port first before the path. (e.g., :554/example_path)

IPCamera Creation and Linkage

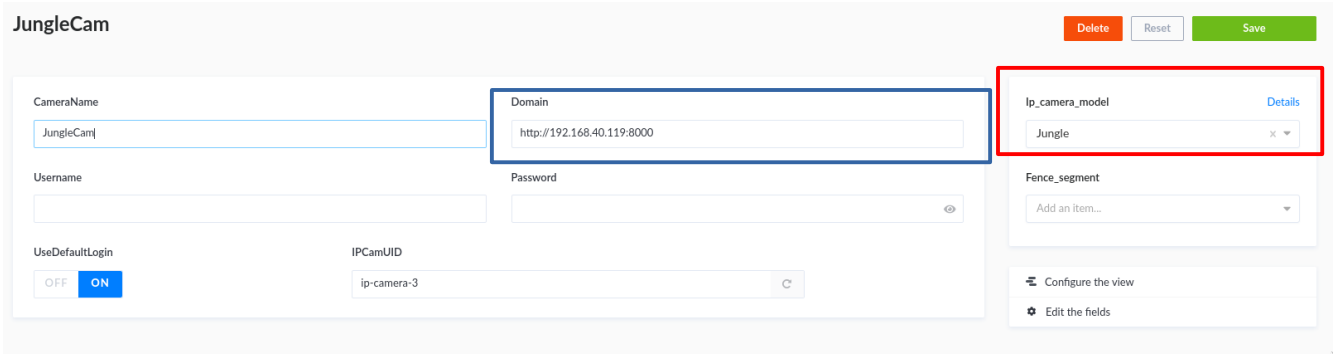


Figure 11

Figure 11 shows a page to modify an existing camera (same form/fields when adding a camera, except there is no option to “delete” when newly adding one). The “Domain” field shown in the blue box is the protocol + ip + port details formatted as follows :

<protocol>://<ip_address>:<port>

Currently, only HTTP is supported. Username and Password indicate the **UNIQUE** username/password used to access the camera’s footage and images. Note that if a user has already set a global username and password from the camera model, the field may be left empty. The “UseDefaultLogin” should also be set to “ON” if the user intends to use the global username/password supplied by the IPCameraModel, and “OFF” otherwise. The red box shown in figure 11 indicate the model associated with the current camera. In this case, the “JungleCam” camera is an IPCamera of type “Jungle”. (Note

that usually, the IPCameraModel follows the model name of an actual IPCamera (e.g., MOBOTIX M16B)

A Camera object may only be linked to ONE fence segment. To have the same physical camera link to multiple segments, a duplicate camera object of the same Domain and Model may be created with different ID. A user may select from the “fence_segment” field to link a camera to a segment. A linked camera will capture images when a segment triggers an alert.

Aside from configuring linkage from the IPCamera’s form. Admins can also configure linkage from the FENCE segment form. Figure 12 shows an example page to modify a FENCE segment.

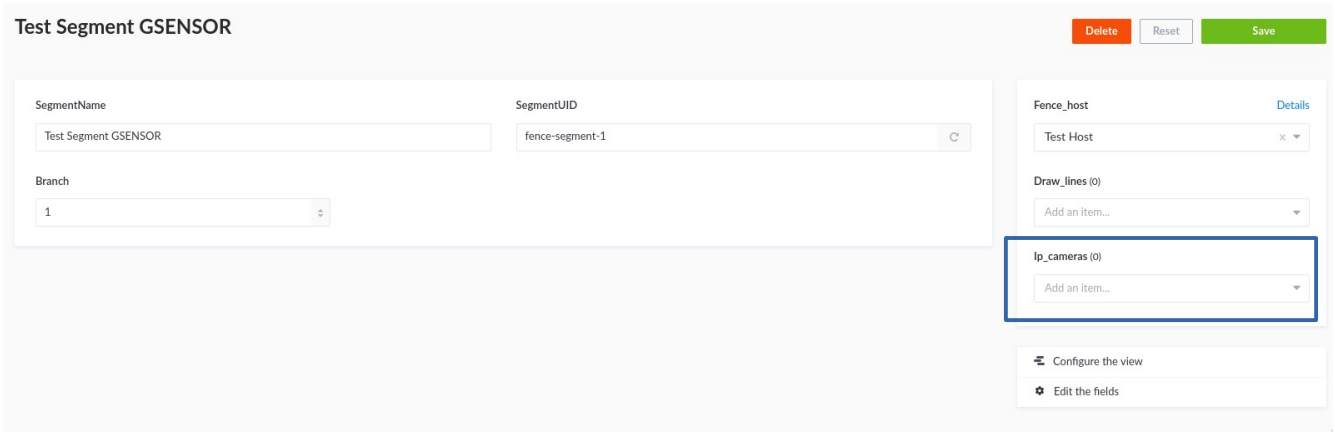


Figure 12

The blue box in figure 12 allows user to select IPCameras to link to the current FENCE segment “Test Segment GSENSOR”. A segment may have **MULTIPLE** cameras linked to it to account for a long physical segment and wider camera coverage. However, a camera may only be linked to **ONE** segment. To link a physical camera to multiple segments, create duplicate of camera objects as described above.

Alerts

Admins can view alerts through the “Alert” collection type. Figure 13.1 shows the alert view table, which can be easily accessed through the left menu.

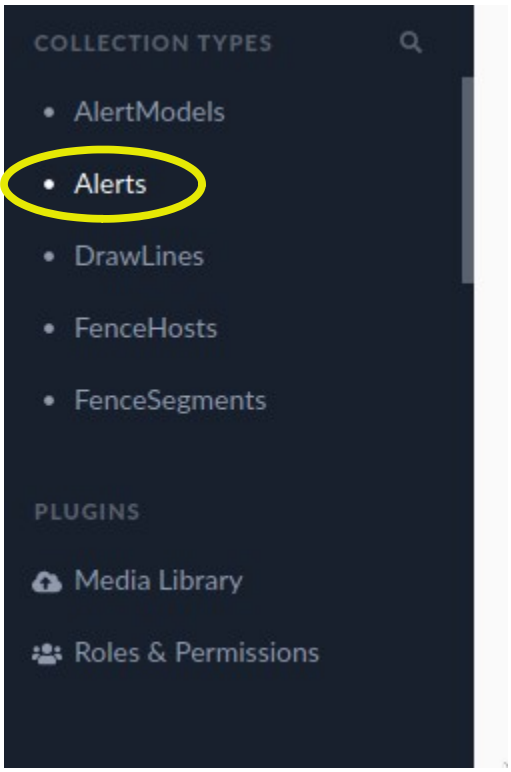


Figure 13

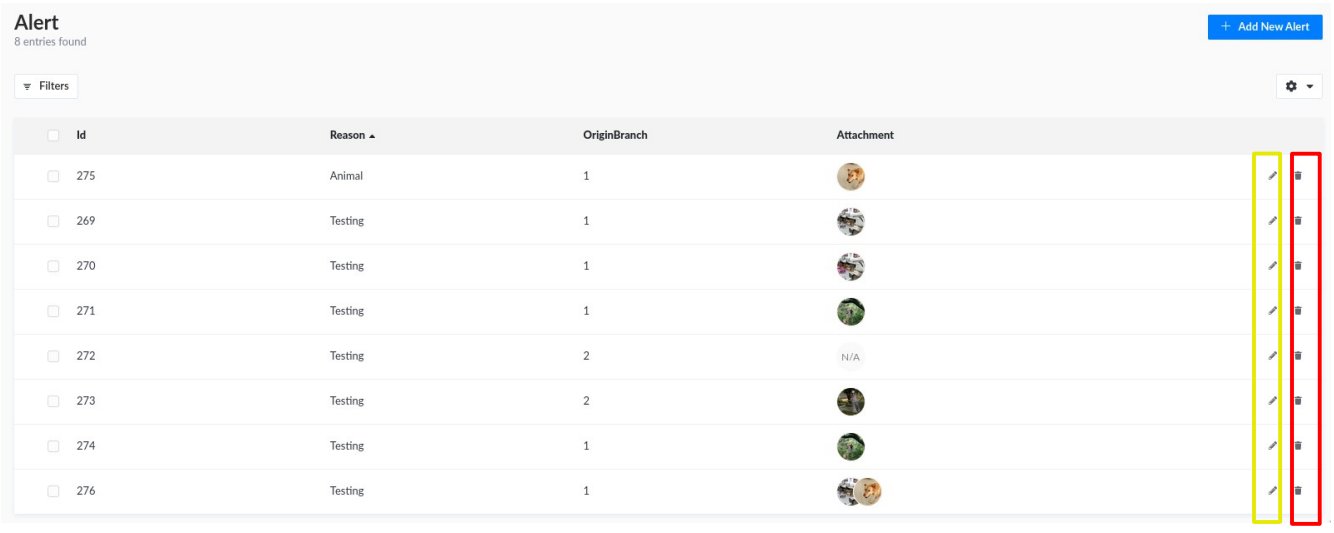


Figure 13.1

Alerts can be viewed in detail from this page by simply clicking on any rows. The “Reason” field is empty because the security operator has yet to decide the cause of the alert. See Security Operator’s Focus UI section for more information. The created_at field indicates the time of creation fo the alert.

To view an alert or modify it, simply click on the “pen” button shown highlighted in a yellow box in figure 13.1. To delete the alert, one may click on the “garbage” button shown highlighted in the red box. Figure 13.2 shows an alert in detail, with a registered reason “Testing”.

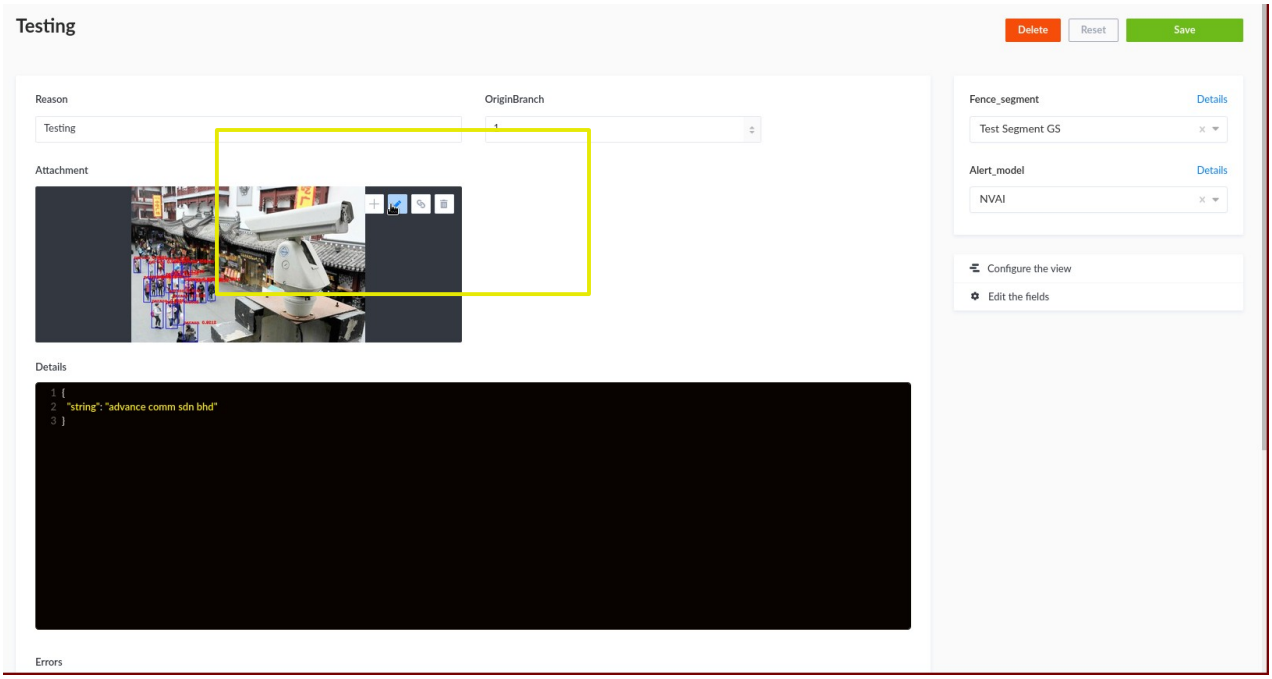


Figure 13.2

To view the alert’s image, click on the edit button as shown highlighted in the yellow box in figure 13.2 by first bringing the cursor near the image and wait for the bar to pop-up. Figure 13.3 shows a sample captured image with its details. The admin may download the image by clicking on the download button shown highlighted by the yellow box in figure 13.3.

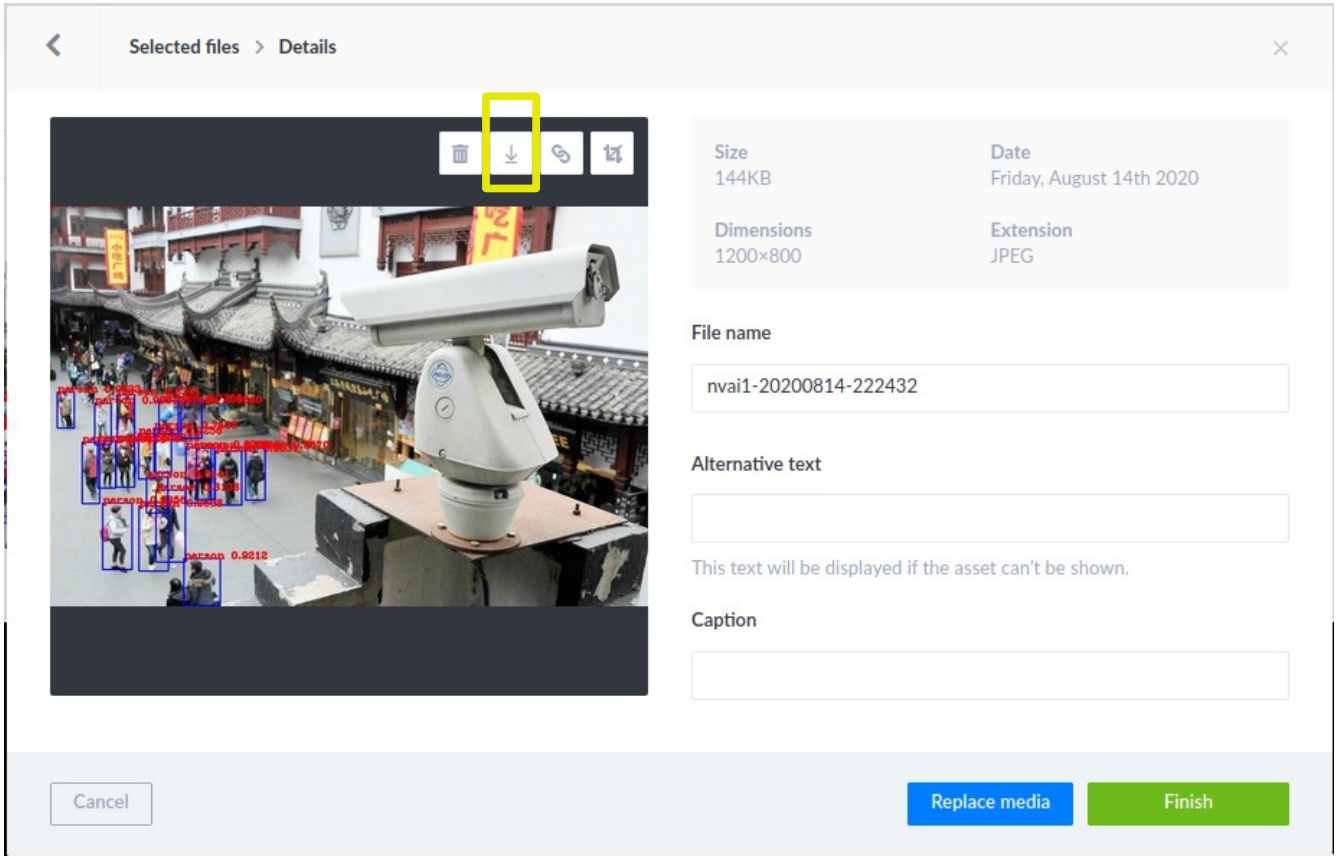

Selected files > Details
Size
144KB
Date
Friday, August 14th 2020
Dimensions
1200×800
Extension
JPEG
File name
nvai1-20200814-222432
Alternative text
This text will be displayed if the asset can't be shown.
Caption
Cancel
Replace media
Finish

Figure 13.3

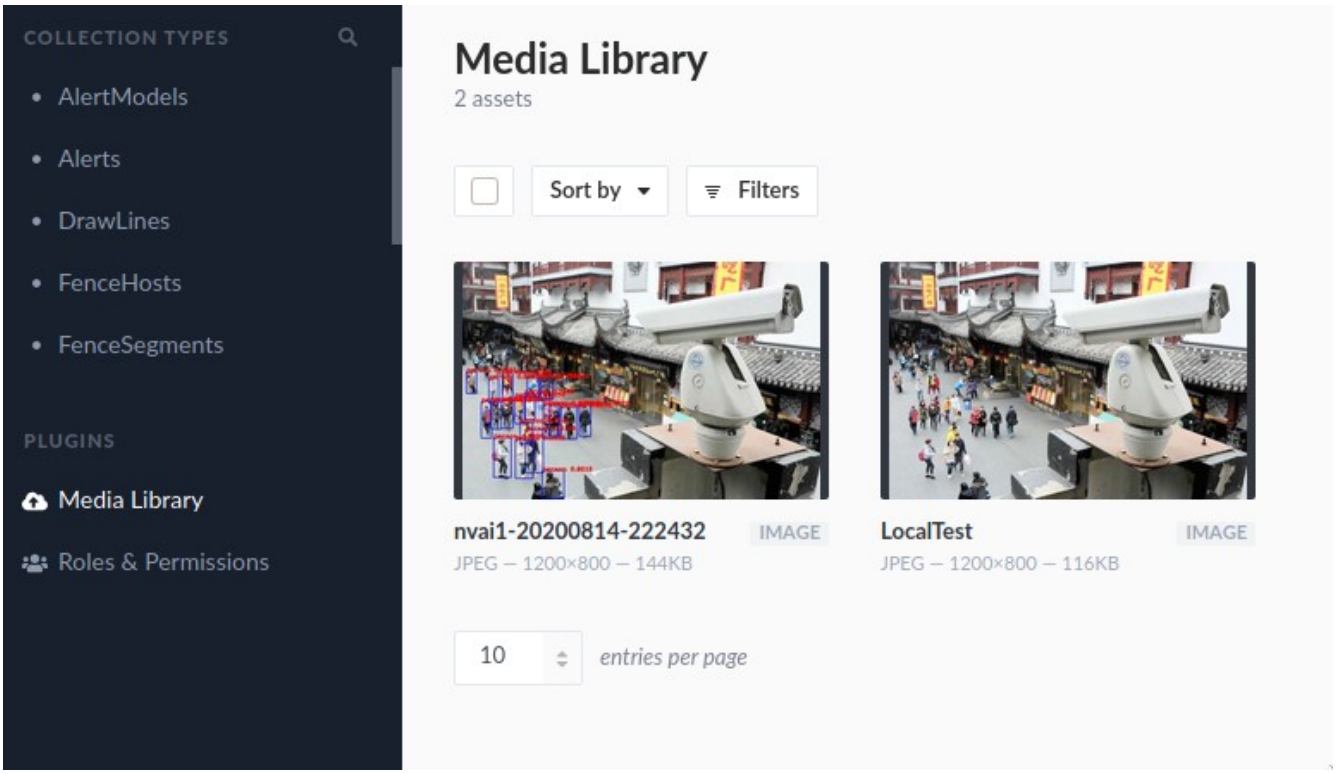


Figure 14

Images captured during alerts may also be seen at the “Media library” menu on the left shown in Figure 14. Notice the image on figure 14 with “nvai” tagged has bounding boxes drawn around detected persons. This is a main distinction between AI-based detections on Advance Communication’s AI software and it’s sensor based hardware, where the AI-based software actually post images themselves to the server instead of grabbing images from the CCTV camera.

Operator Section

MAP EDITOR

The map editor may be accessed by clicking on “Editor” from the landing page as shown by a orange box in figure 15.

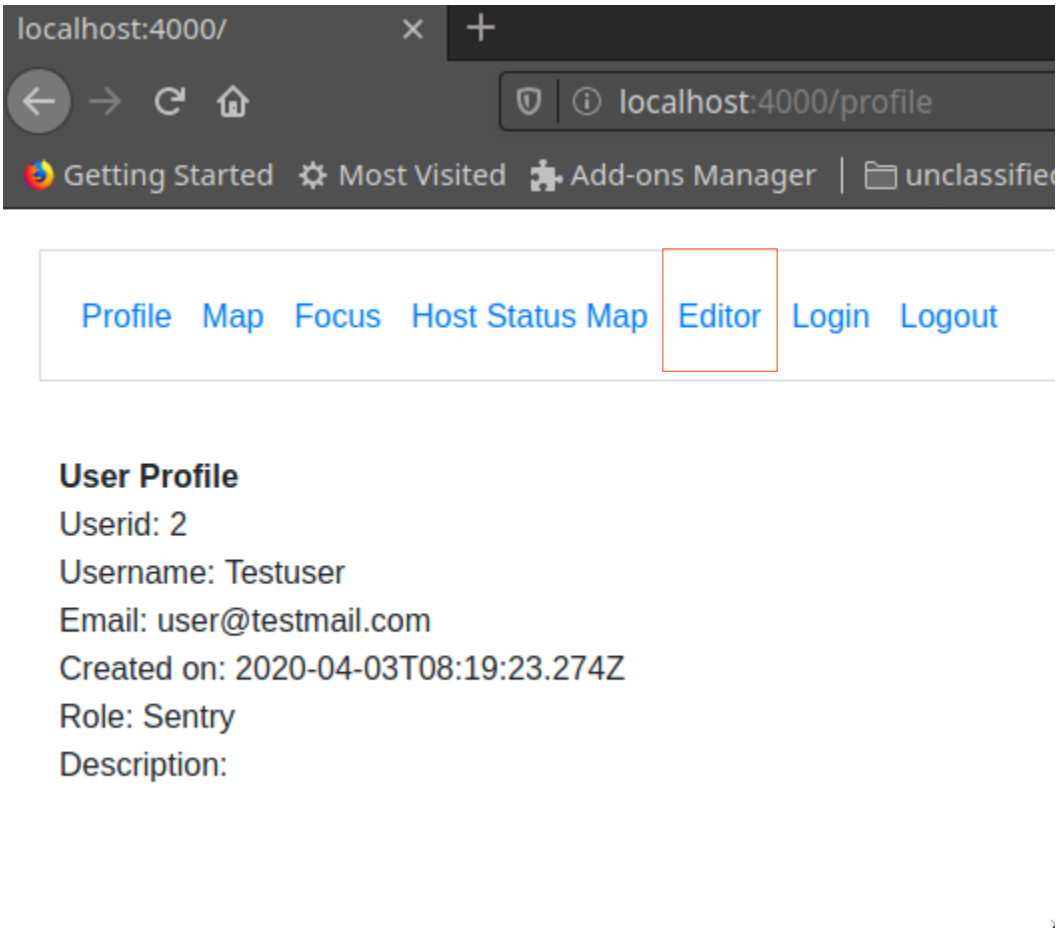


Figure 15

Figure 16 shows the editor web-UI. The operator should see “Segment list received, Select a segment to draw lines” on the top left. If the operator does not see this, the configuration is not done correctly and the system should be reconfigured. Ideally, the segments should be added and configured before finally drawing out the indicator lines on the map.

To draw a single line for a segment, the operator first have to find which segment is being drawn. This can be done by using the Host Filter to filter out the right Host (Host names will be displayed) and subsequently the Segment Filter to filter out the right Segment (Segment names will be displayed). A Segment may have **MULTIPLE** representative lines, allowing a segment to be a approximated curve is necessary. Once the segment is selected, the operator may optionally select a desired color from the color selection pallette. This color will be the blinking color during when an alert is triggered on the map UI. The operator starts drawing by clicking on the starting point and then the ending point on the map. If the operator is happy with the line, they may hit “SPACEBAR” to register the line, or click again on the map to redraw.

Figure 16.

Figure 17 shows a prompt for the operator on the top left to either register the line drawn (as seen on the lower right of the figure) by hitting spacebar or clicking on the map again to redraw.

Figure 17

The prompt displays “Line registered” as shown in figure 18 upon hitting spacebar.

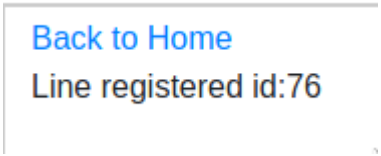


Figure 18

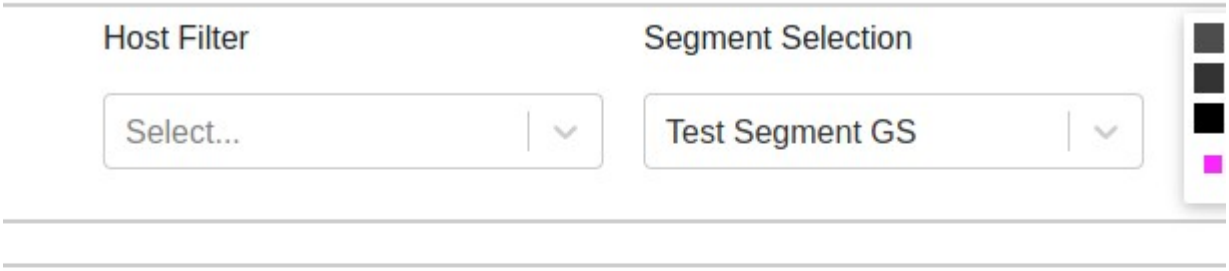


Figure 19 – An example curved line comprising of diferent color on the SAME segment.

Note that ALL line representations of a segment will BLINK when their corresponding segment is triggered. As shown in figure 20, when another segment is selected, all OTHER segment and their line representations will be colored BLACK.

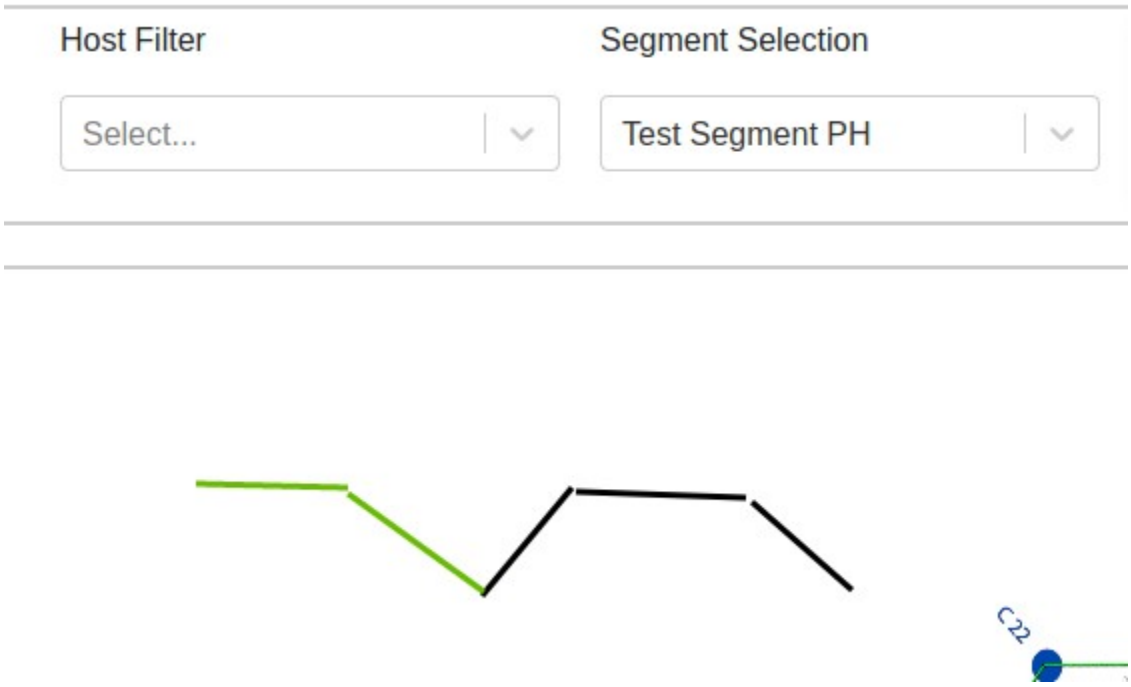


Figure 20 – Only line representations under “Test Segment PH” is colored, where the line representations of “Test Segment GS” is colored black to allow the operator to see the current line representations of the selected segment. (Note that this DOES NOT change their blinking color and only serve to help identify which segment is being drawn currently).

To redraw all line representations on a segment (wrongly registered lines or security area expansion), select on a segment and click on “Delete Segment Lines” as shown in blue box in figure 21.

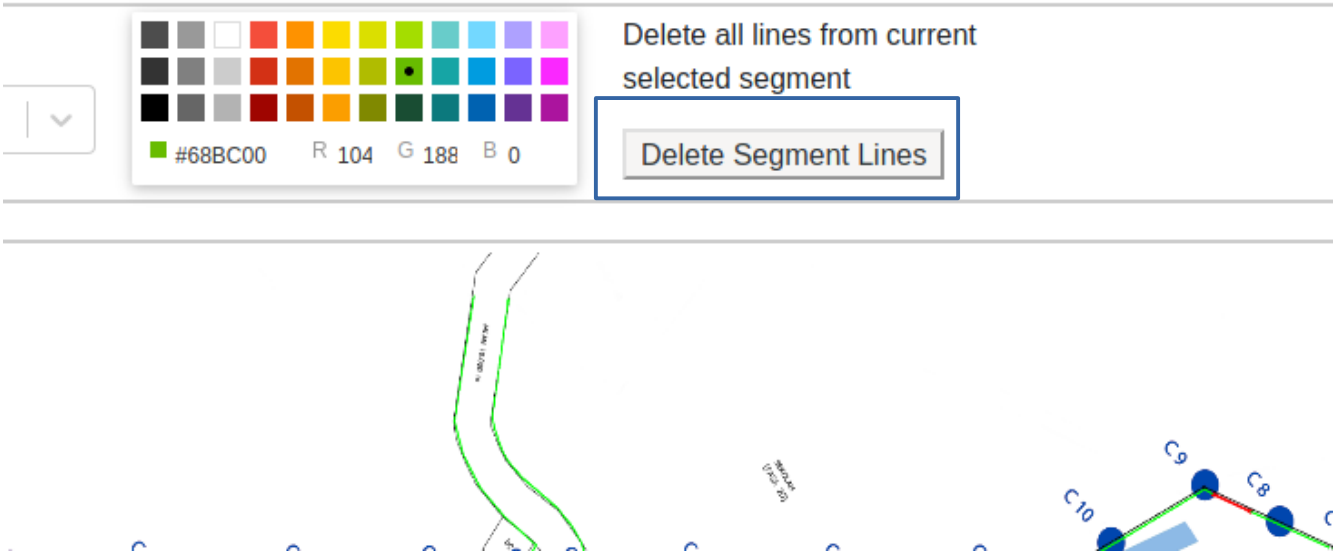


Figure 21

MAP VIEW

The map view indicates triggered alerts by blinking their origin segment's line representations on the map. Figure 22 shows an example of a segment's line representation (circled in yellow) for an alert. Only segments with alerts currently registered in the system will have their line representation blink on the map UI view. Line representations are by default transparent if there are no alerts associated with its segment.

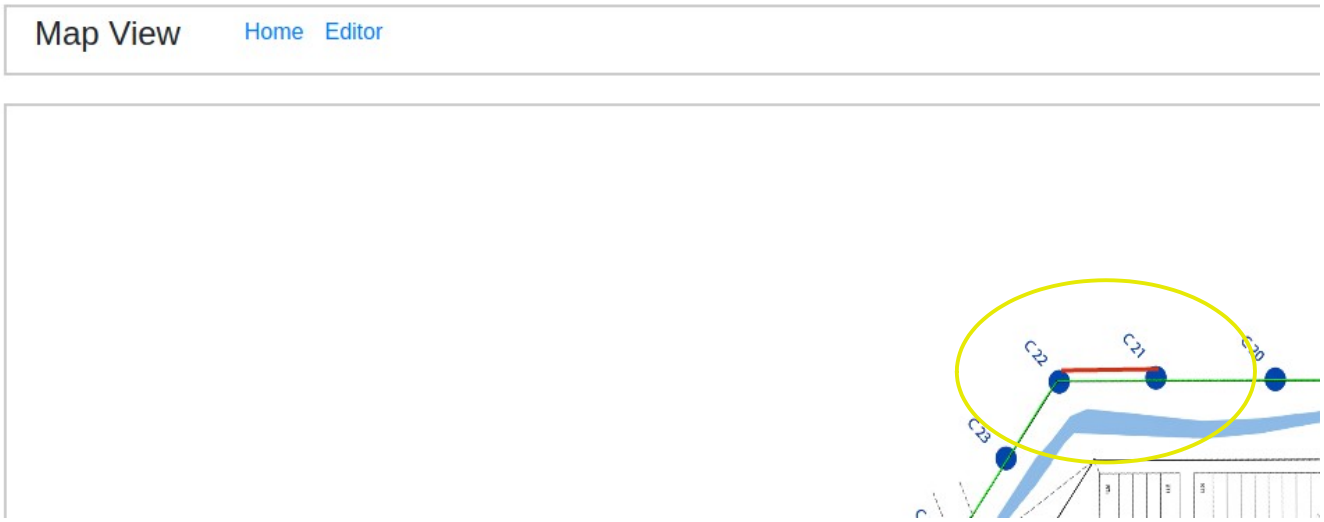


Figure 22

FOCUS VIEW

The focus view allows focused views on the first 4 unattended alerts in triggered in the monitoring system as shown in figure 23. To access the page, simply click on “Focus” from the navigation bar on the operator’s home page.

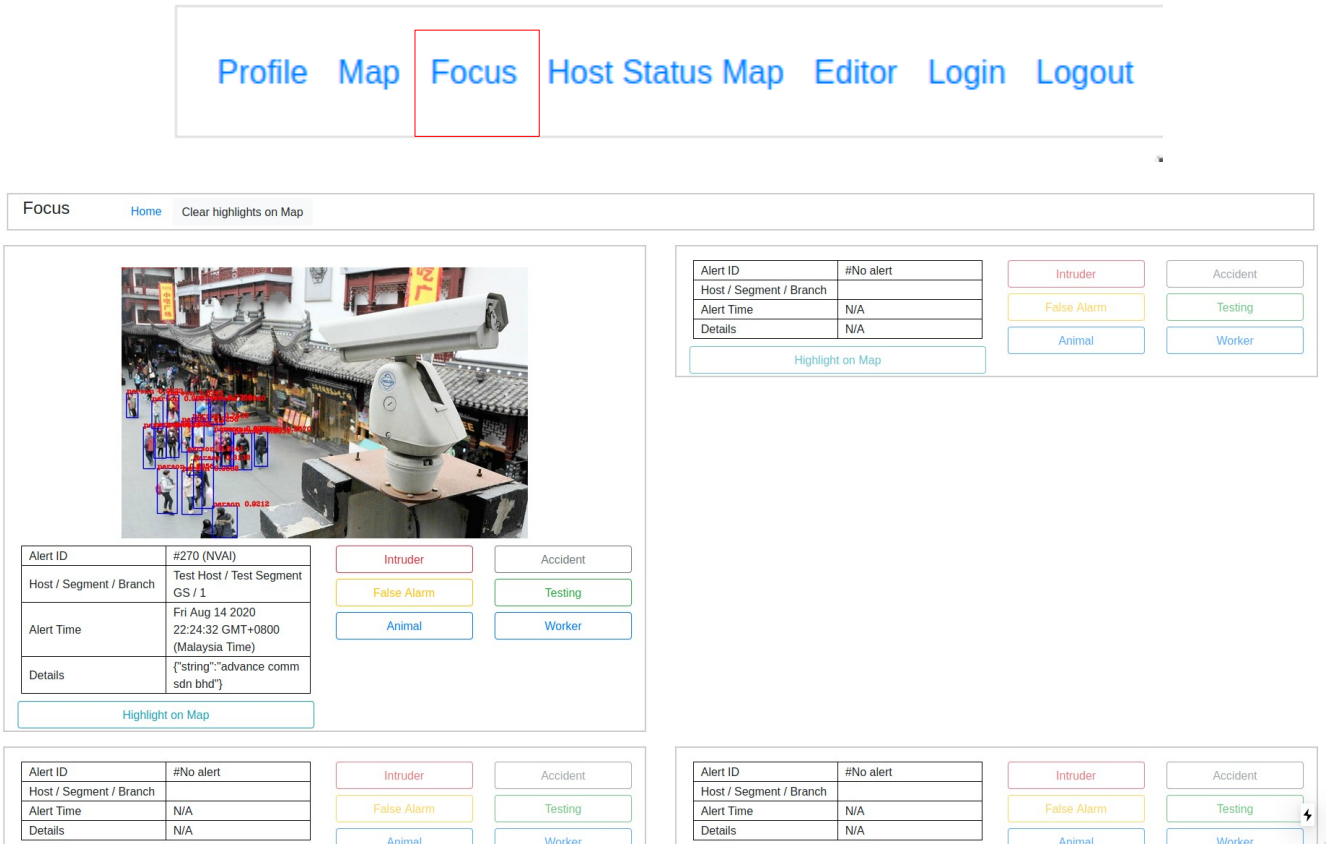


Figure 23

The layout of alerts are arranged based on the following grid pattern :

1	2
3	4

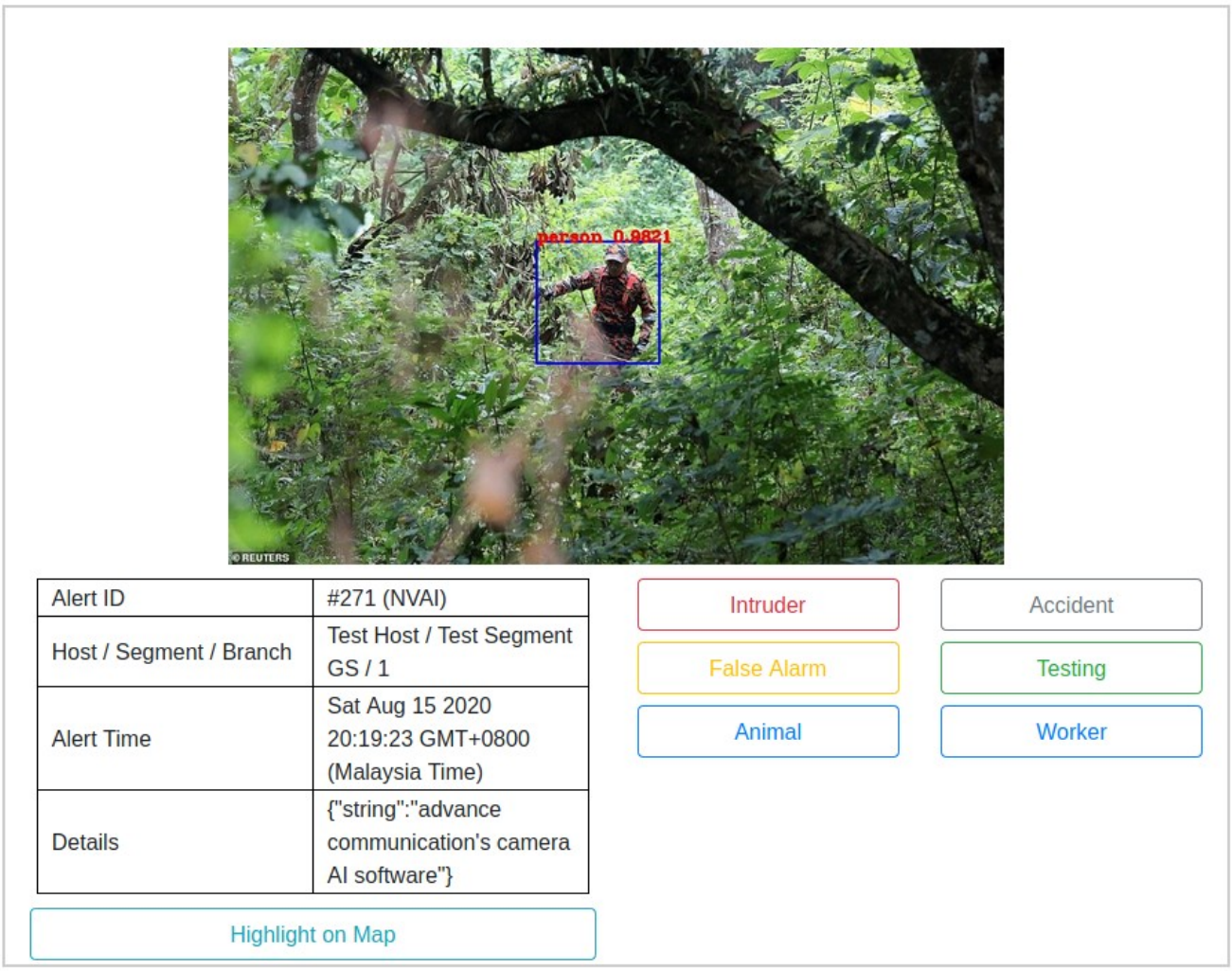


Figure 24

Figure 24 shows one of the 4 alert panes with a captured image. For SENSOR based alerts (GSENSOR, PHOTONBEAMS), the image is captured by the linked IPCamera configured by the system admin. For VISION-AI based alerts, the image is uploaded directly by the image classifier along with its annotations (shown as a bounding box of the detected object, in figure 24, a person with confidence is detected with 98.2% confidence).

The security operator may view the details of the alert on the left table located below the image. The first row describes the ID of the alert recorded in the database, along with the details of the origin of the alert (The FENCE HOST and SEGMENT in which the alert originates from). Alert Time is also displayed along with the details of the alert. The operator may click on “Highlight on Map” button to highlight the alert on the map by ONLY coloring the line representations of the segment corresponding to the alert.

Once the operator has ascertained the cause of the alert, he/she may click on 1 of the 6 buttons found on the lower right of the panel “Intruder, False Alarm, Animal, Accident, Testing and Worker” to register a reason for the alert. This reason is stored in the databse for further reporting. Once an alert is registered with a reason, it no longer is an active alert and is removed from the Focus and Map UI page.

Figure 25 – A focus page on maximum capacity with 4 alerts. Notice the last alert #4 has 2 captured images. This is because multiple cameras may point to the same FENCE segment.

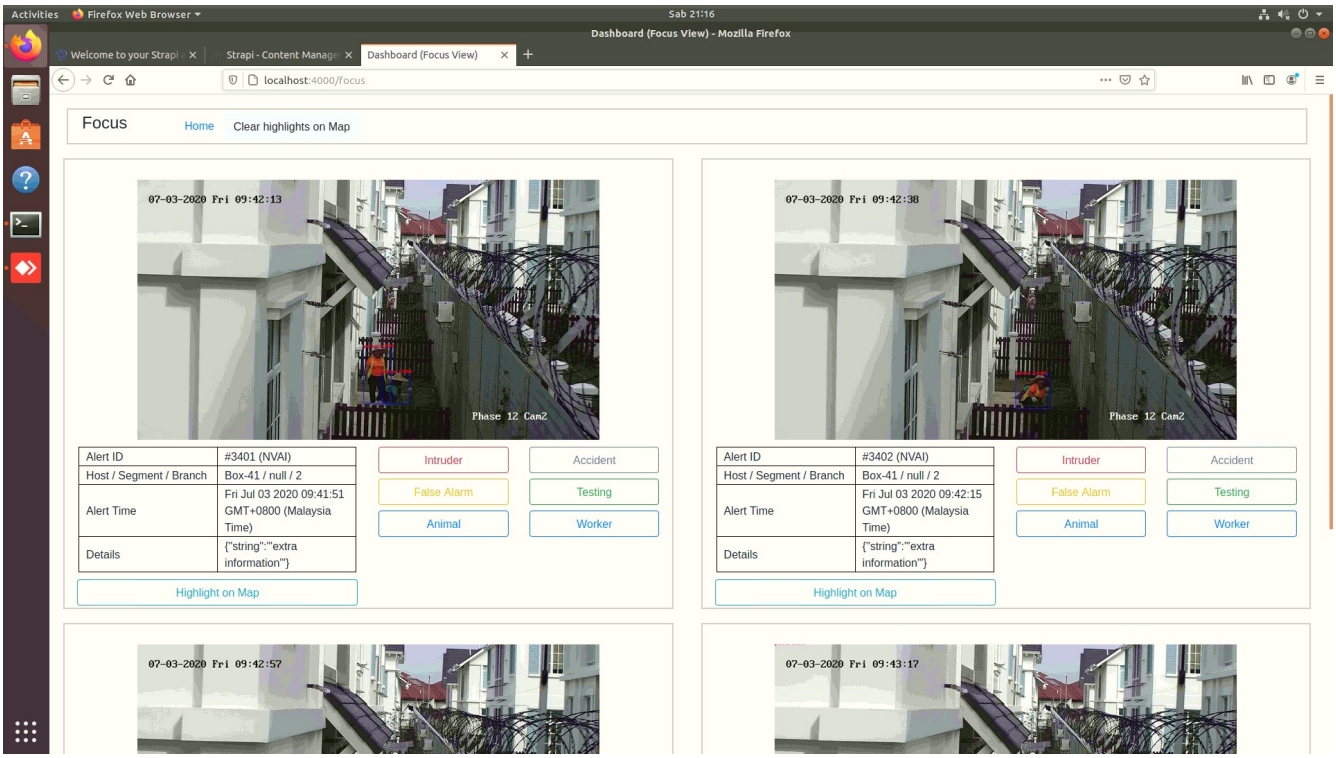


Figure 25.1 – A focus page with alerts from the AI-based detection software.

HOST STATUS MAP

The host status map shows the current downed host (unresponsive hosts) on the system. Controller boxes that are malfunction and their corresponding segments with its lines are colored **BLACK** in this UI page. Figure 26 shows an example of a test system with some of the FENCE hosts downed, the sensors and the segment they cover are thereby colored black to indicate that the area is vulnerable to intruders. The yellow circle in figure 26 highlights the area only and is not part of the UI.

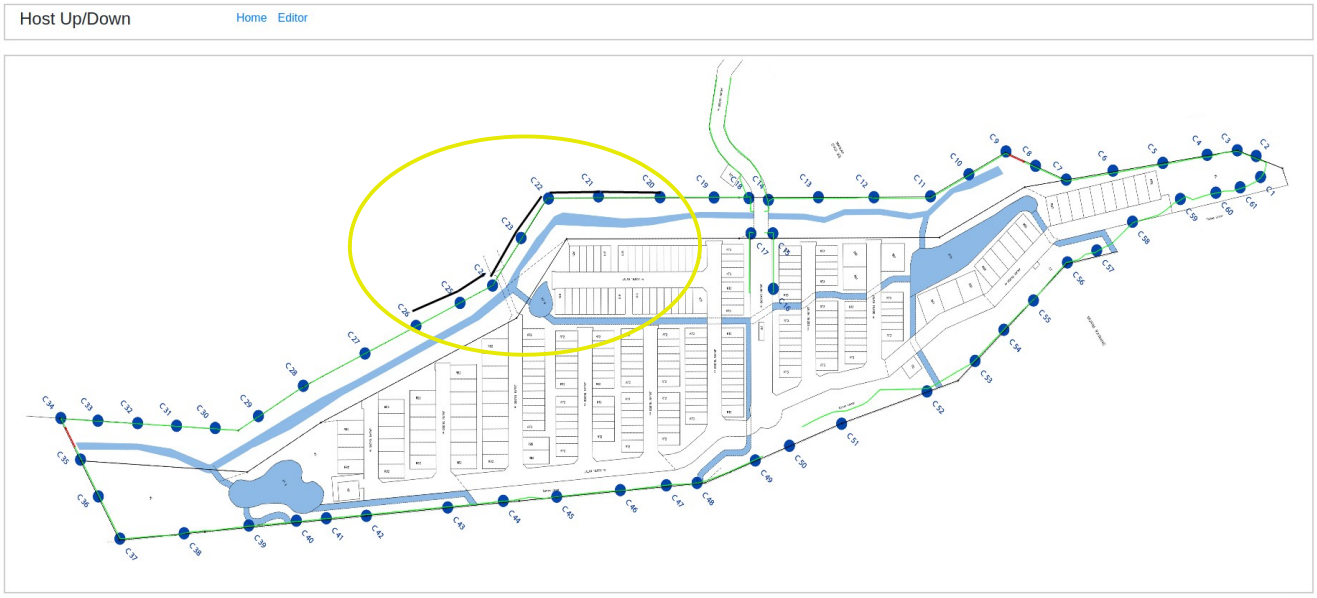
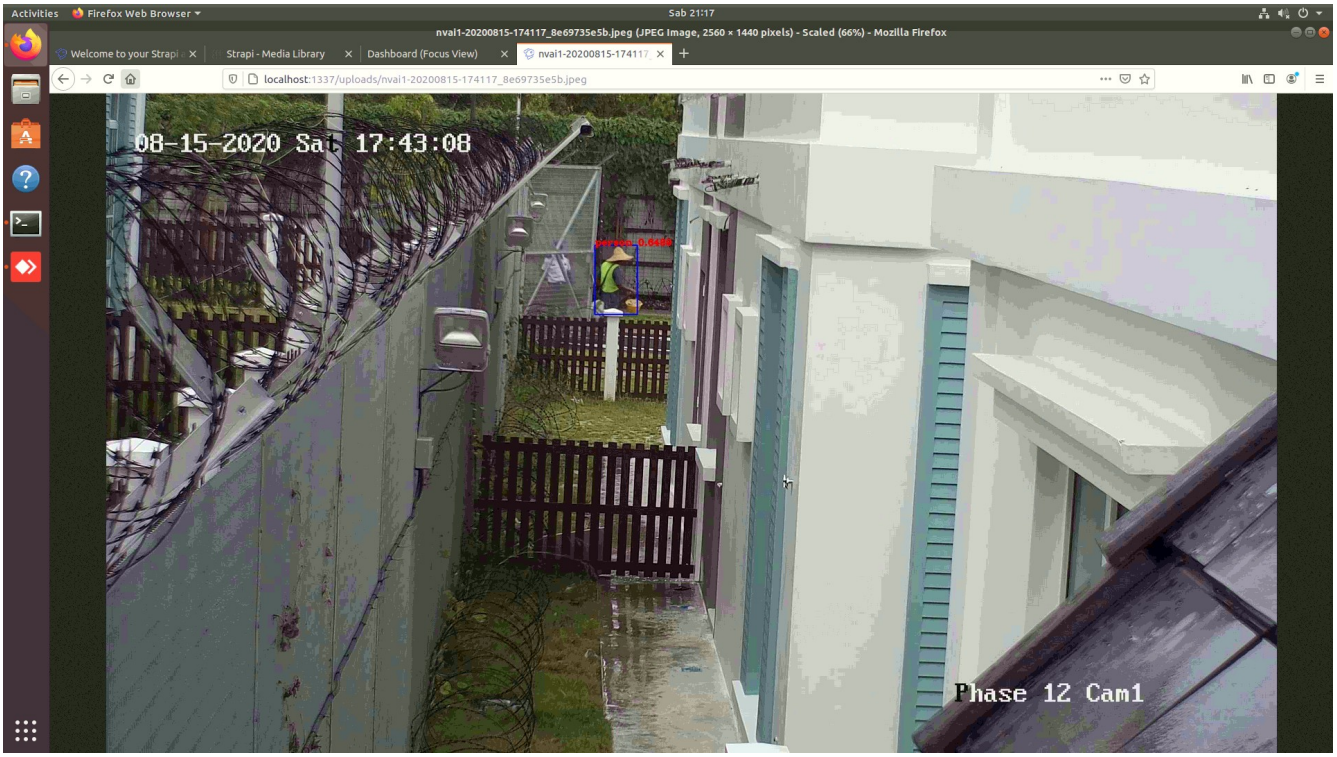
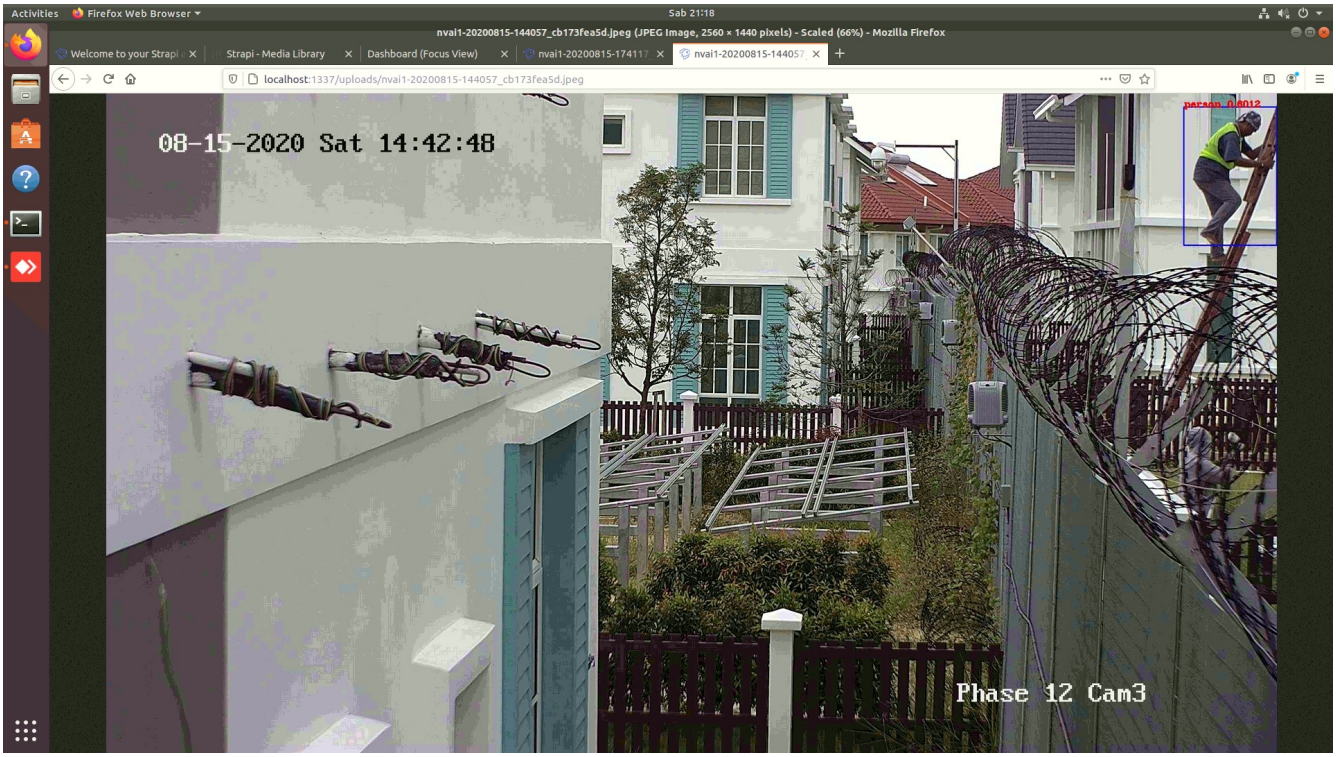


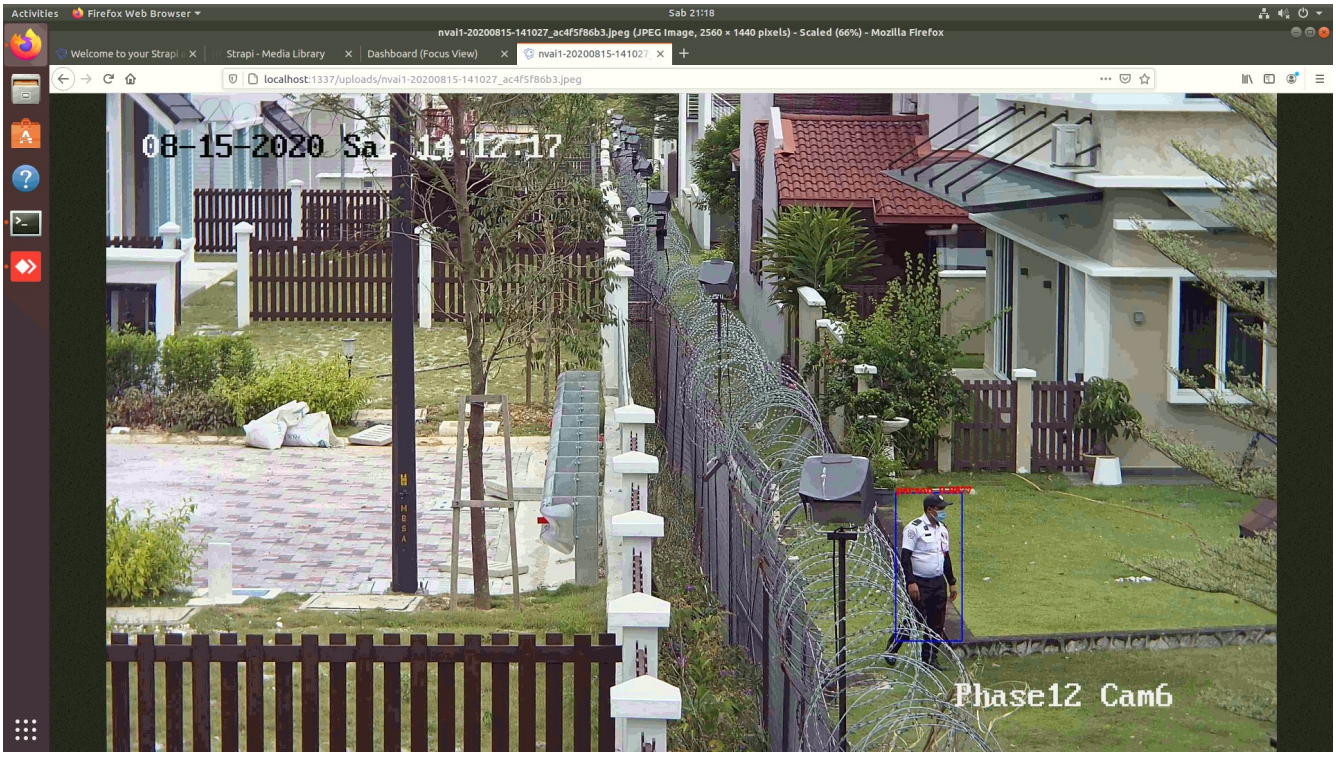
Figure 26

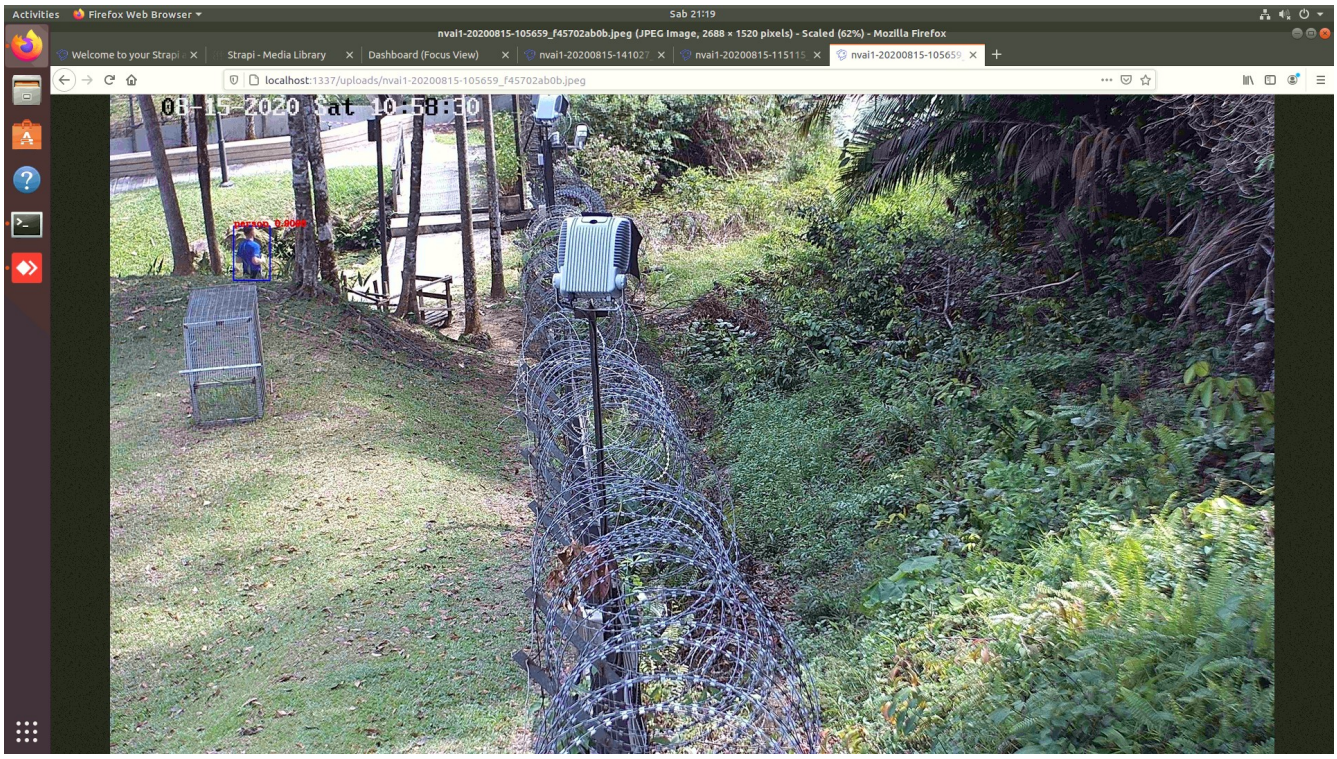
AI-based software detection

The AI-based software detection automatically annotates identified objects (such as persons) in the uploaded image on the server. The following images are example captures from a test installation.









The cameras capturing images to feed the AI-based detector should be in high spots capturing a wide angle in a well-lit environment. The best cameras to feed the AI detector are places with least amount of pedestrians or resident activity because the detector cannot distinguish between legitimate residents or intruders, and will trigger an alert upon detection of ANY person. Adequate lighting and good camera footage is also desireable as it improves the accuracy of the detector.