AvidBeam

AvidBeam AvidGuard™ User Guide

Contents

Overview

Introduction

AvidGuard is a product developed by AvidBeam Technologies for security and surveillance applications. AvidGuard is used to monitor areas for intrusion of different types of objects including humans, cars, animals, or any other object of interest. Upon detection of such objects, AvidGuard signals an alarm on user screen or through an email or SMS. The list of alarms as well as the details information about the actions taken upon each alarm is stored for future review and analysis. This document describes on more details AvidGuard features, installation and usage guidelines.
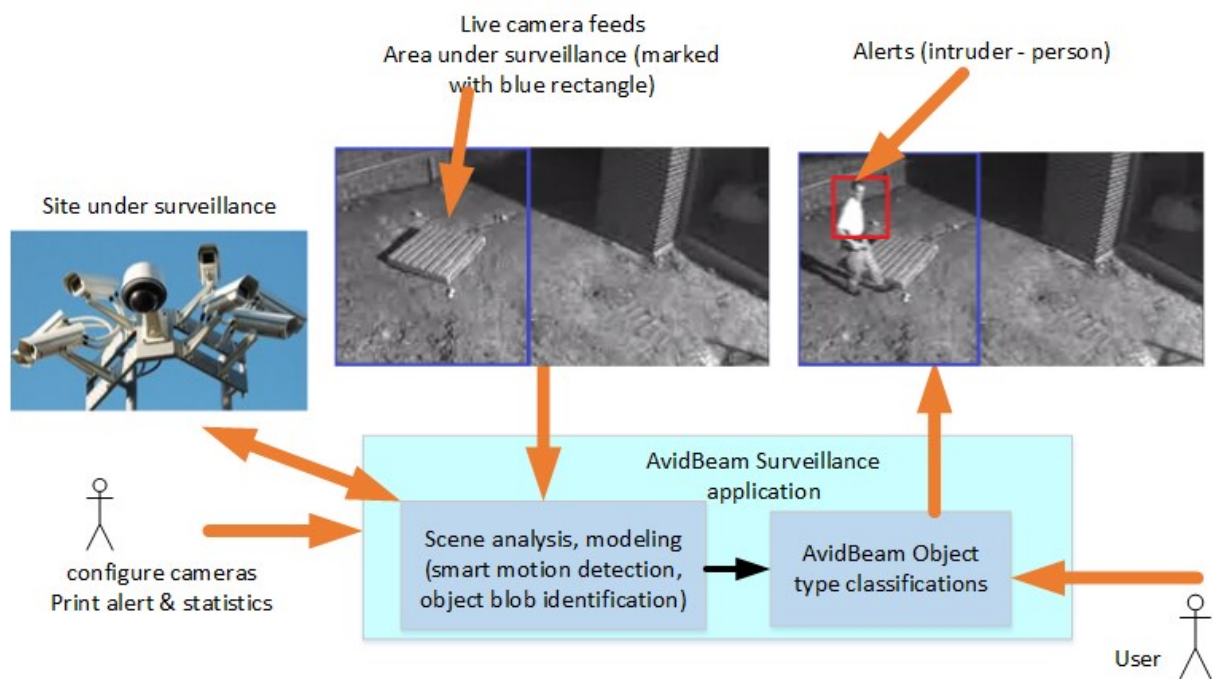

Figure 1 AvidGuard Solution

Definitions and Acronyms

ATUN™	AvidBeam's scalable video processing and computer vision product
RTSP	Real Time Streaming Protocol
ViBE™	Video Information Business Engine
AvidGuard™	AvidBeam ViBE for Security applications

How AvidGuard™ works

AvidGuard is a scalable application, i.e., it can process many or large number of cameras. AvidGuard is powered by AvidBeam ATUN™ platform which handles the scalability of AvidGuard. AvidGuard features are summarized as follows

ATUN™ is intended to process big video data in the form of RTSP streams and/or video files. The platform comprises big data tools, computer vision algorithms, image and video processing features and an easy-to-use web interface to enable computer vision developers to easily scale and extend their algorithms with more features.

ATUN™ enables you to run your plugin, or pre-built AvidBeam® plugins, connect cameras and processing servers, use existing media inputs and launch the platform to process input data and visualize results. ATUN™ replicates your plugin based on allocated processing cores and stores the output in a database to be later viewed and inspected using the dedicated web interface.

Developer can write their computer vision algorithm in a customized ATUN™ plugin using the ViBE™ SDK and API.

AvidGuard™ High Level Features

AvidGuard features can be summarized as follows
1. Supports input from cameras or video files
2. Detect different types of objects such as people, car, masked people, selected weapons, animals
3. Report and alert upon detection via email, SMS, or display
4. Maintain history log of reported alarms, action taken per each alarm, and alarm acknowledge details
5. Ability to train the detection for new objects or update existing object training.

AvidGuard™ Web Views (pages)

In AvidGuard, there are two categories of web views
1. Configuration Web Interfaces: those are the interfaces used for configuring and running a plugin to the prototype. Those views should be used only by AvidGuardystem administrator to add cameras, plugins with new features, and start/stop surveillance jobs.

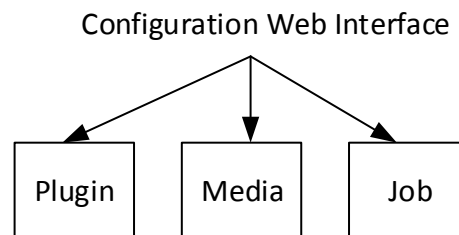Configuration Web Interface

Plugin   Media   Job

Figure 2 ATUN Configuration Views

2. AvidGuard User web views: those are the web views used by AvidGuard users (monitoring agent) as shown in Figure 4 and they are used to display/visualize the video surveillance prototype specific output such as Alert, Alert history, detected and recognized objects, etc.
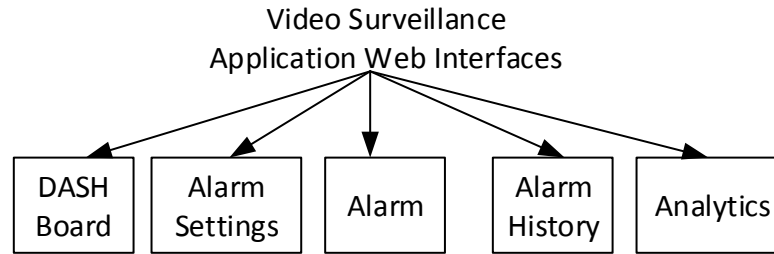
Video Surveillance
Application Web Interfaces

DASH Board | Alarm Settings | Alarm | Alarm History | Analytics

Figure 3 Video Surveillance Solution Views

The details of each web interface will be described in the following sub sections.

Configuration Web Interfaces

Configuration includes many parameters such as camera URL or input video file path, how many instants of the plugin will be run and on how many cores, other specific plugin parameters include specific region of interest (ROI) where the plugin will process events that occurs only inside it.

Plugin View

The plugin view or web interface allows clients to upload their plugin into the solution. At the moment, there are different plugins that are loaded into the prototype. However, in the future more plugins can be added or existing plugins can be modified and uploaded.
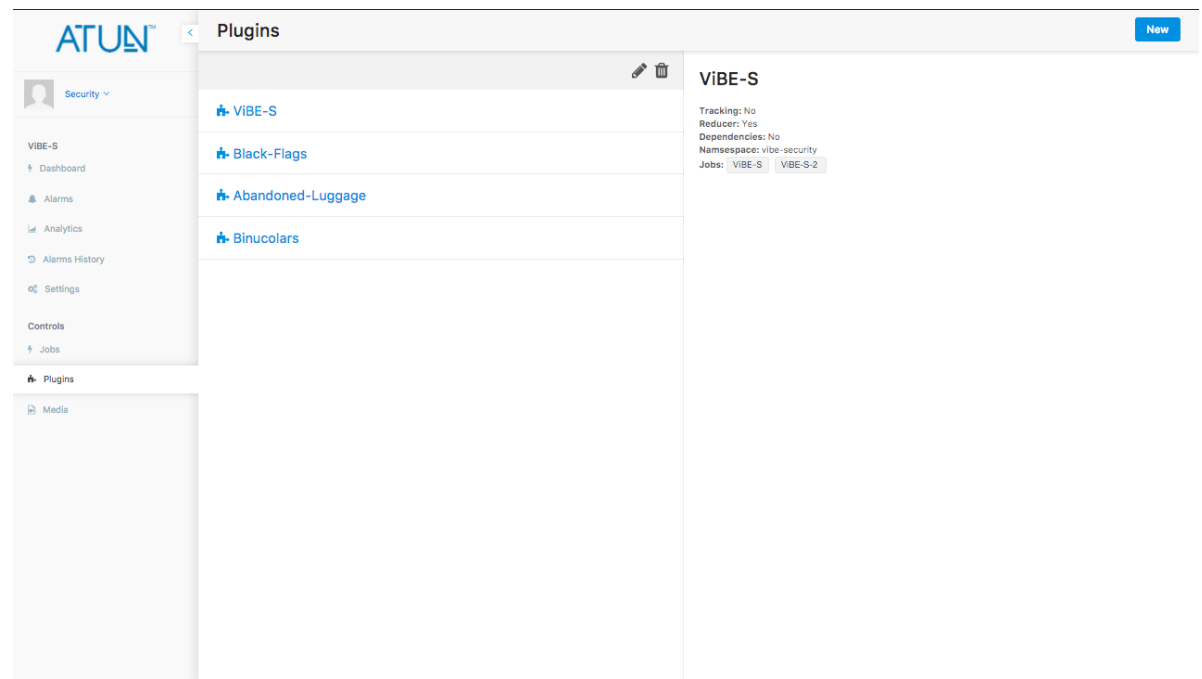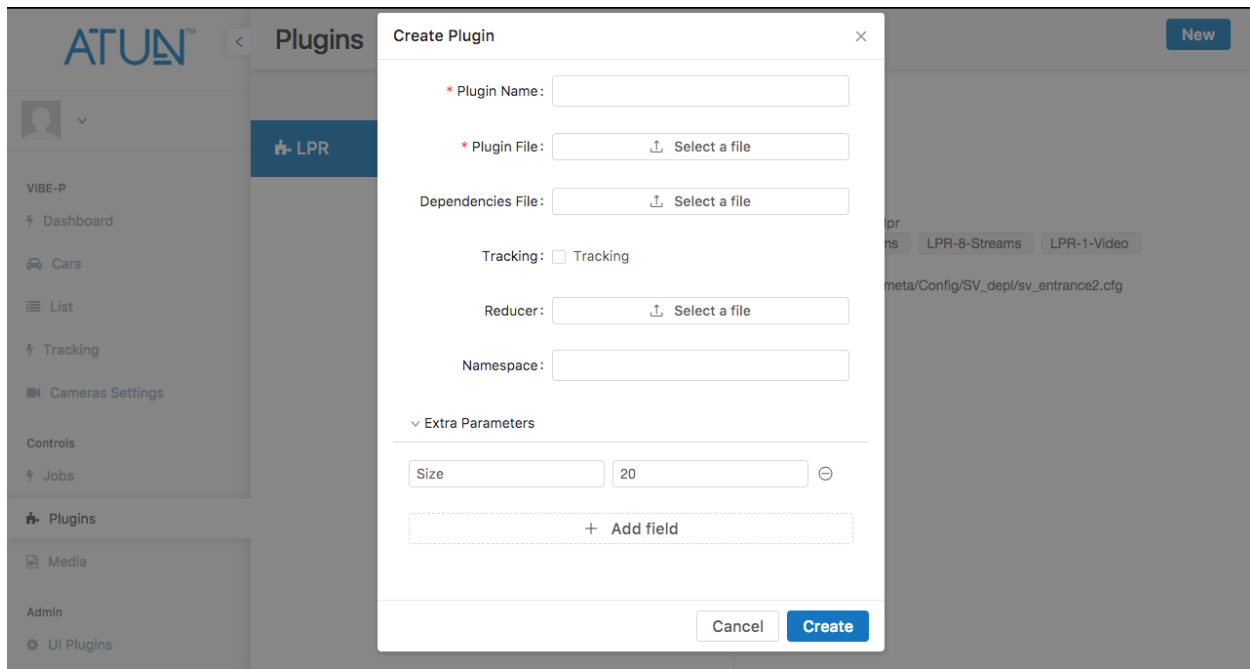
Figure 4 Plugin Configuration

When adding a plugin to ATUN, the user can also specify a set of parameters to be used with this plugin as shown in Figure 6

Figure 5 Specifying ATUN Plugin Parameters

Media View

The Media web interface provides a mechanism for defining the input video source to the prototype. Client can either choose a camera URL or a video file for each media input source. Client can also use this web interface to view the RTSP stream contents coming from the selected media input as shown in Figure 7
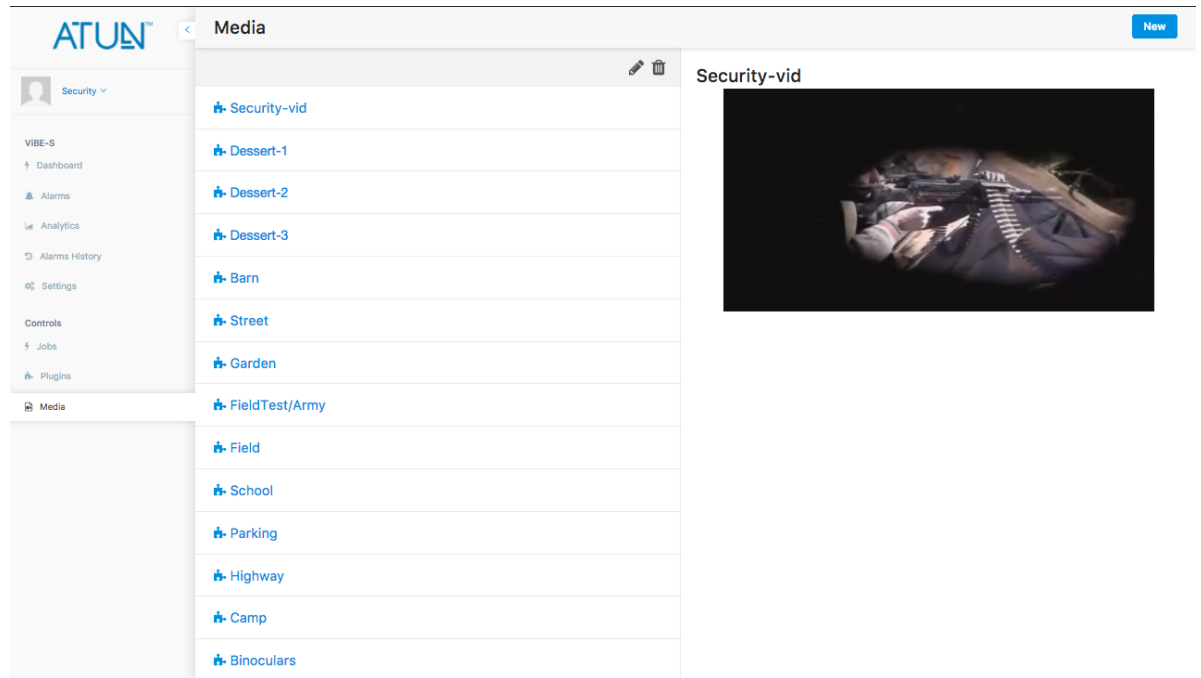
Figure 6 Media Source Configuration

Job View

The job web interface as shown in Figure 8 allows system administrator to attach a specific media source to a specific plugin. Once this is completed, the actual processing job can be then be started by pressing the start button on the view.
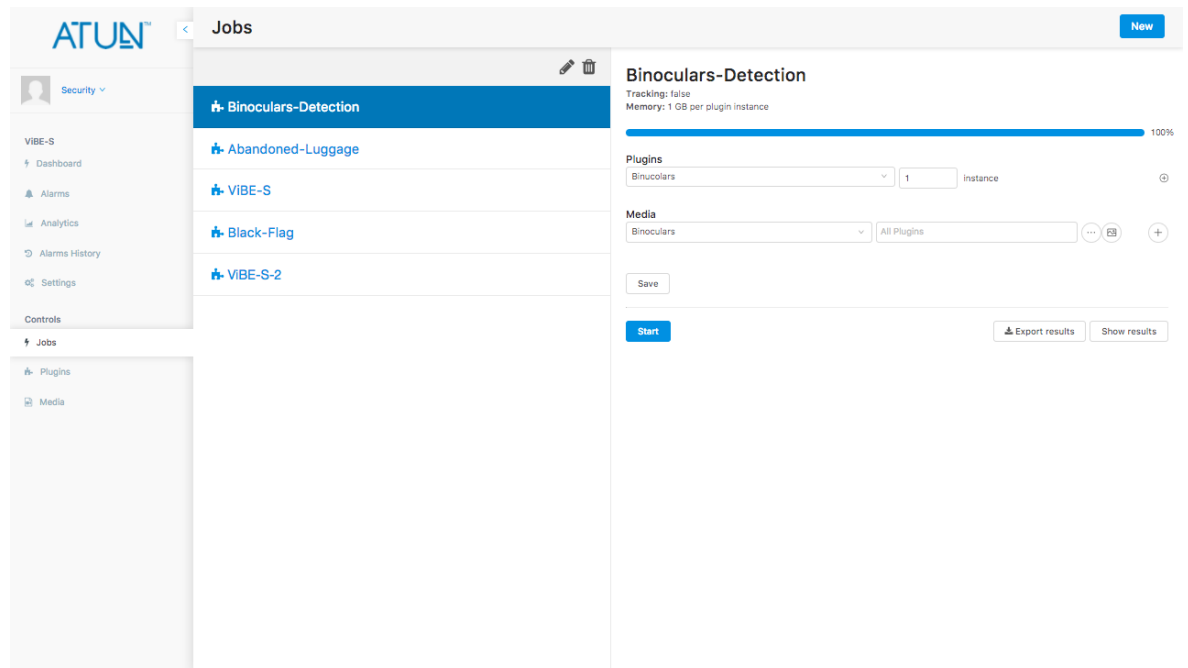
Figure 7 Jobs Configuration

Once a job is started, a progress indicating how much % of input data has been processed (if the input is a video view) and at any moment, the client can stop the processing by pressing the stop button.

AvidGuard Web Interfaces

DASH Board View

As shown in Figure 9, The Dashboard view gives an overall summary for the ongoing daily activity throughout the whole solution, through two main panels. The first which is the Alarm Panel which gives an indication about the alerts encountered and how many alerts happened up to the active time. The Second Panel is the Cameras View (elaborated in more details in Figure 10) which gives a summary for the media source found if an alert was found. The Dashboard also includes the most recent detected and recognized object for each defined input media source (IP camera or video file)
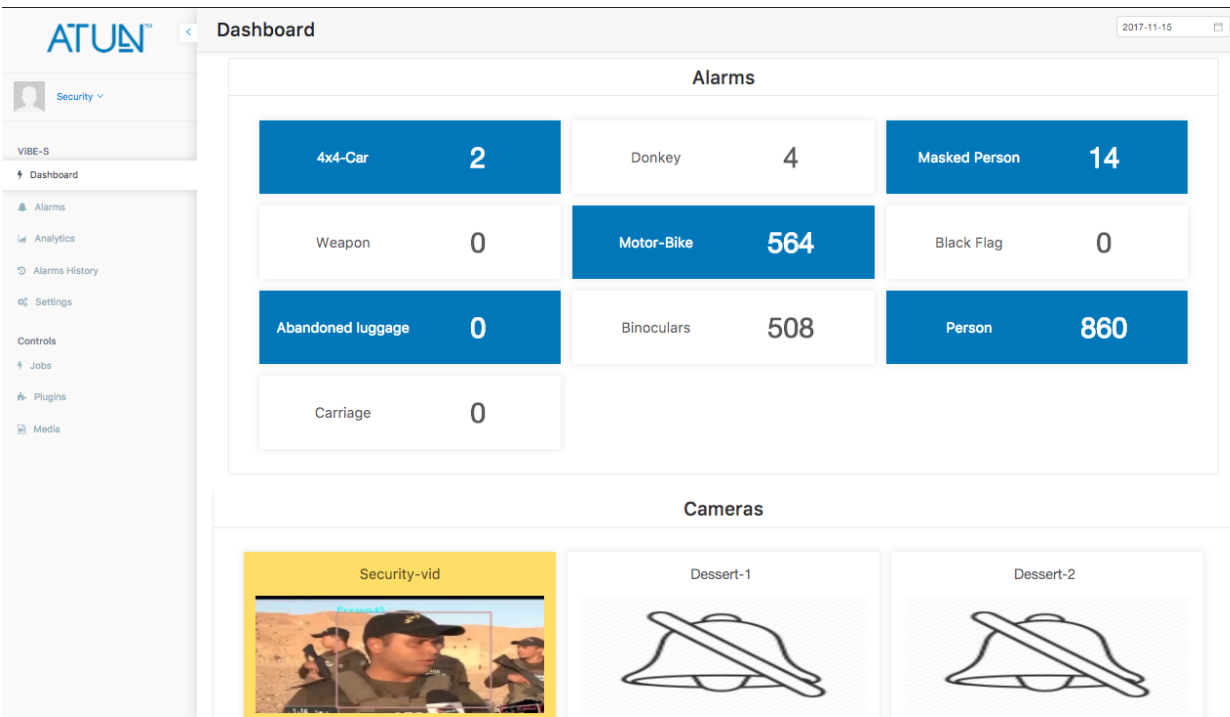
Figure 8 Administrator DASH Board
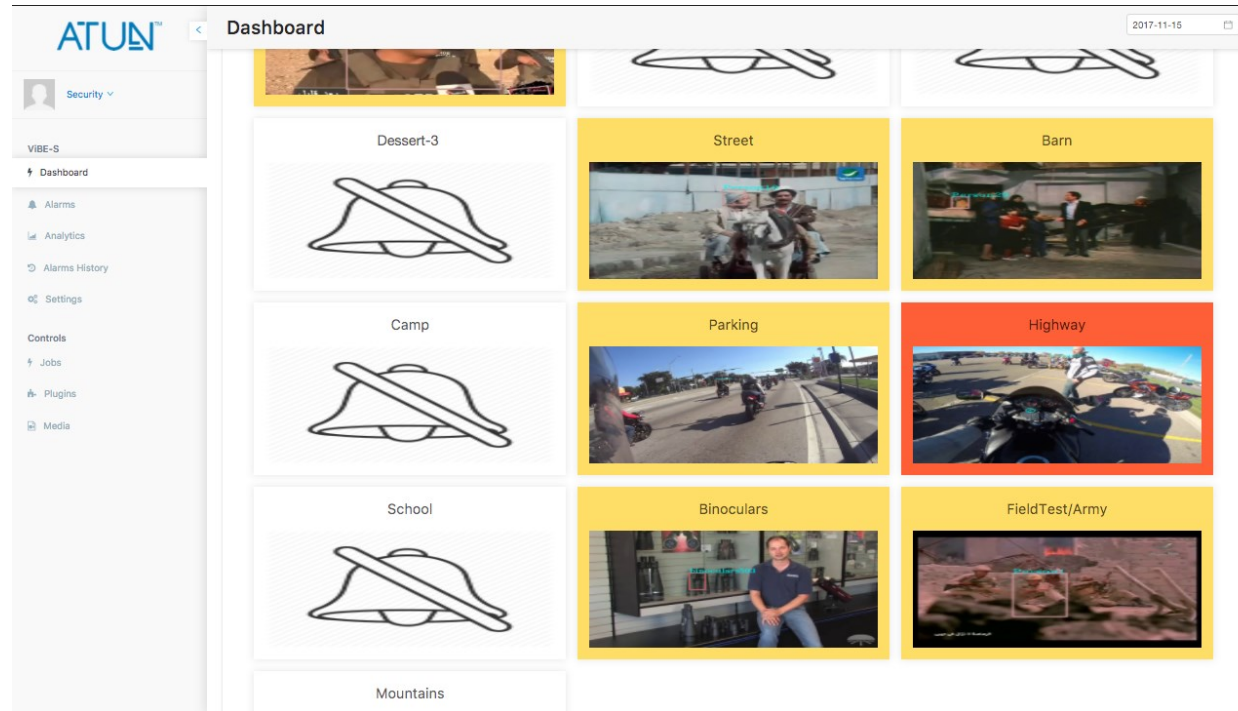
Figure 9 Administrator DASH Board

Settings View

The Settings view is divided into two main tabs which user can navigate through

1. Alarms Settings: The Alarms Setting tab is shown in Figure 11 provides a mechanism for user to create a custom Alarm. User can add a new alarm with the specified inputs as shown in Figure 12.
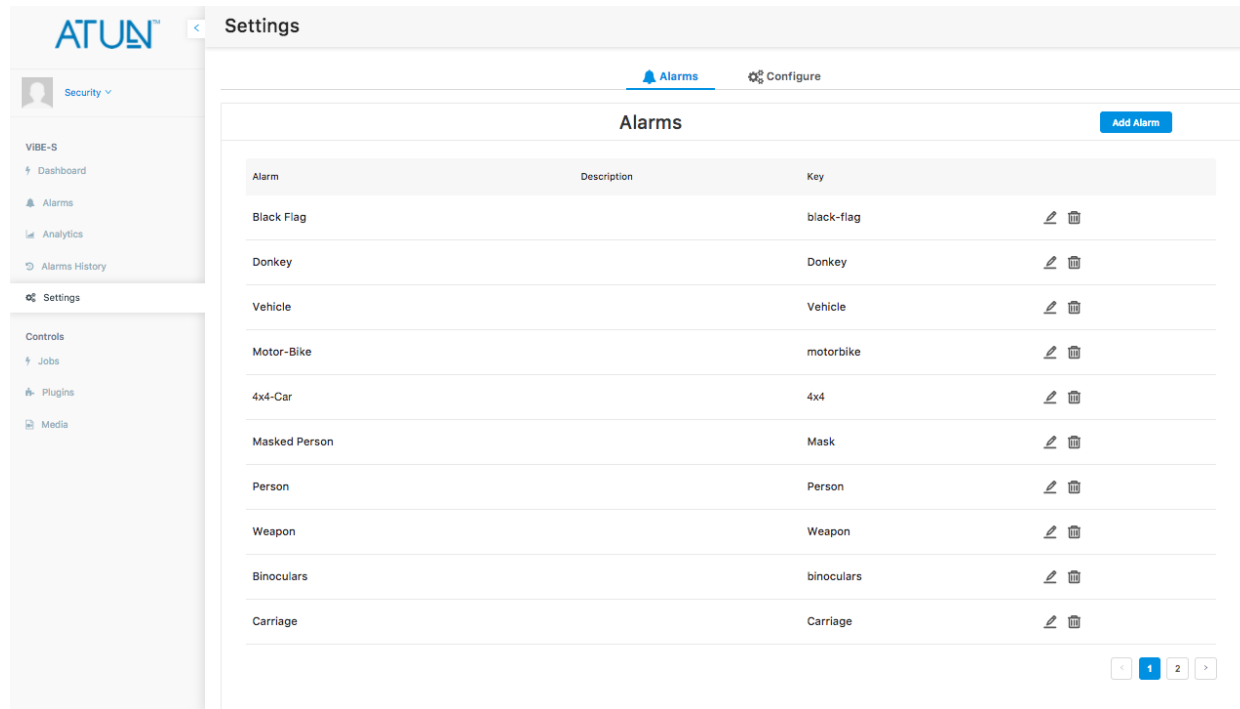
Figure 10 Alarm Settings View
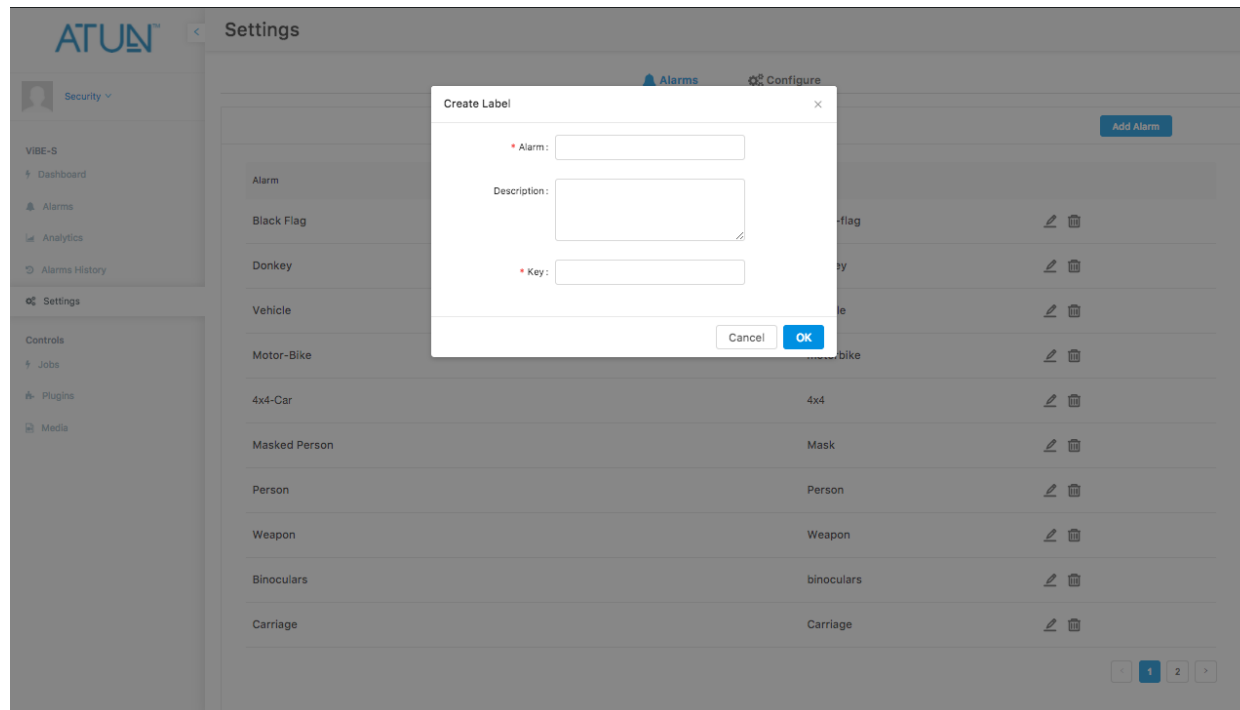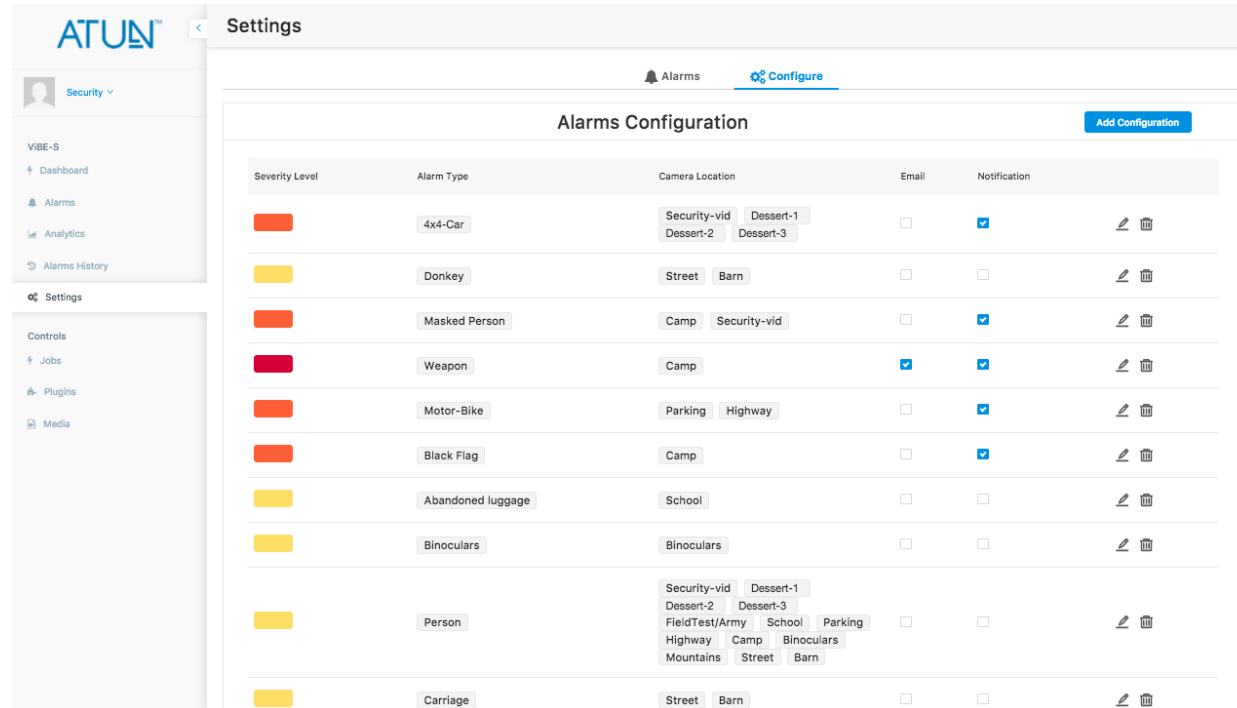
Figure 11 Create New Alarm

2. Alarms Configuration Settings: The Alarms Configuration Settings tab as shown in Figure 13 provides mechanism for user to configure the predefined alarms with the required cameras through a series of inputs as shown in Figure 14:

- Select the object upon which the alarm will be activated
- Choose the alarm severity which are divided in Critical with red color code, Major with orange color code and Minor with yellow color code
- Choose the required cameras upon which the alarm will be activated
- Action to Be Taken either send an email or show a notification with a required message predefined by the user.

Figure 12 Alarm Configuration Settings
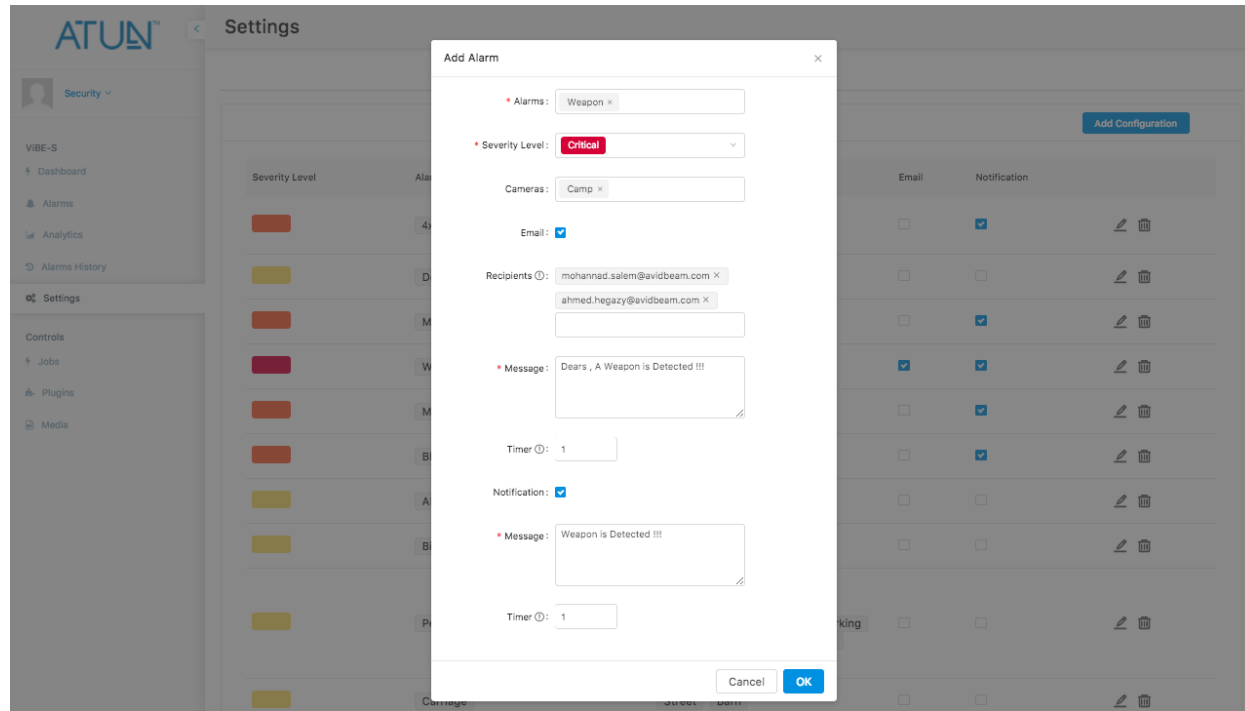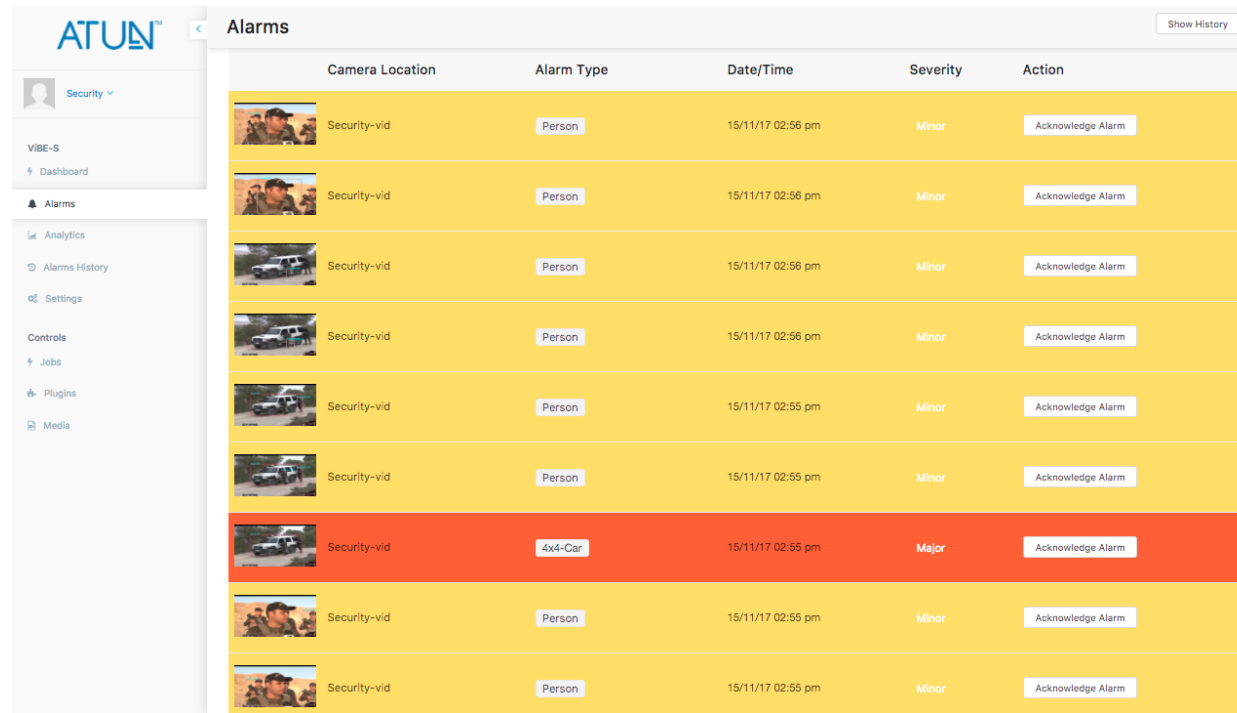
Figure 13 Configure Alarm

Alarm View

The Alarm view (Figure 15) lists all alarms that occurred with the latest alarm on top of the view. Different color codes are used based on alarm severity level.

- Red: Critical
- Orange: Major
- Yellow: Minor

Figure 14 Administration Alarm View

In order to make sure that the alarm has been acknowledged, the solution user should press the acknowledge button for each individual alarm. Once the acknowledge button is pressed, the alarm will be delisted from the alarm view and added to the alarm history view.

Alarm History

The Alarm history view (Figure 16) lists all previously detected alarms whether it was acknowledged or not acknowledged. Briefly it is a history for all the alarms detected by ATUN.

Figure 15 Administrator Alarm History

Analytics View

Analytics view (Figures 17 & 18) provides data analysis to the data extracted from the input camera feeds and stored in the database. The data analysis provides a good summary for each camera with severities and alarms found.

Analytics view supports 4 different Graphs:

1. Basic Column: (Figure 17) Number of Alarms Per Cameras: Cameras Graph showing the number of Alarms for Each Camera per hour
2. Pie Chart: Alarms Distribution per Camera location: Showing the distribution of All Cameras with each camera's Alarms.
3. Pie Chart Alarms Distribution per Type: Showing the distribution of all alarms and when clicked on any alarm, the cameras that detected this alarm will be displayed.
4. Pie Chart - Alarms Distribution per Severity: Showing the distribution of all severities and when clicked on severities it shows the distribution of this severity among all cameras.
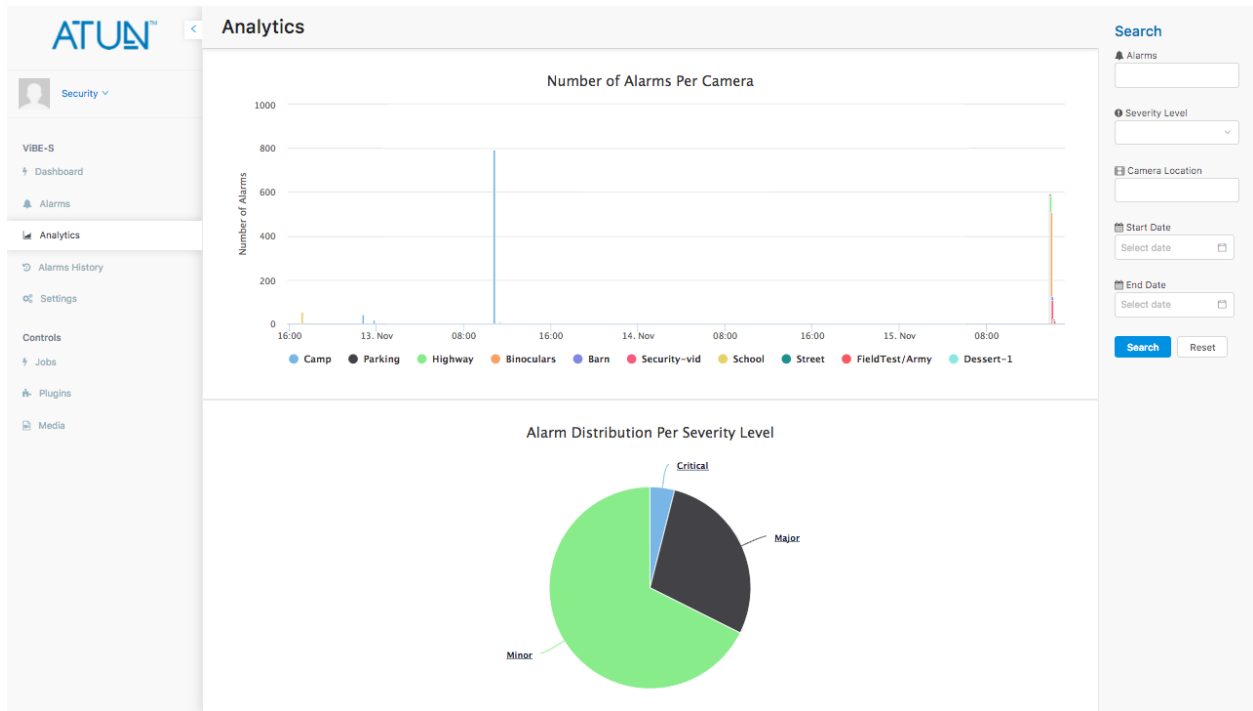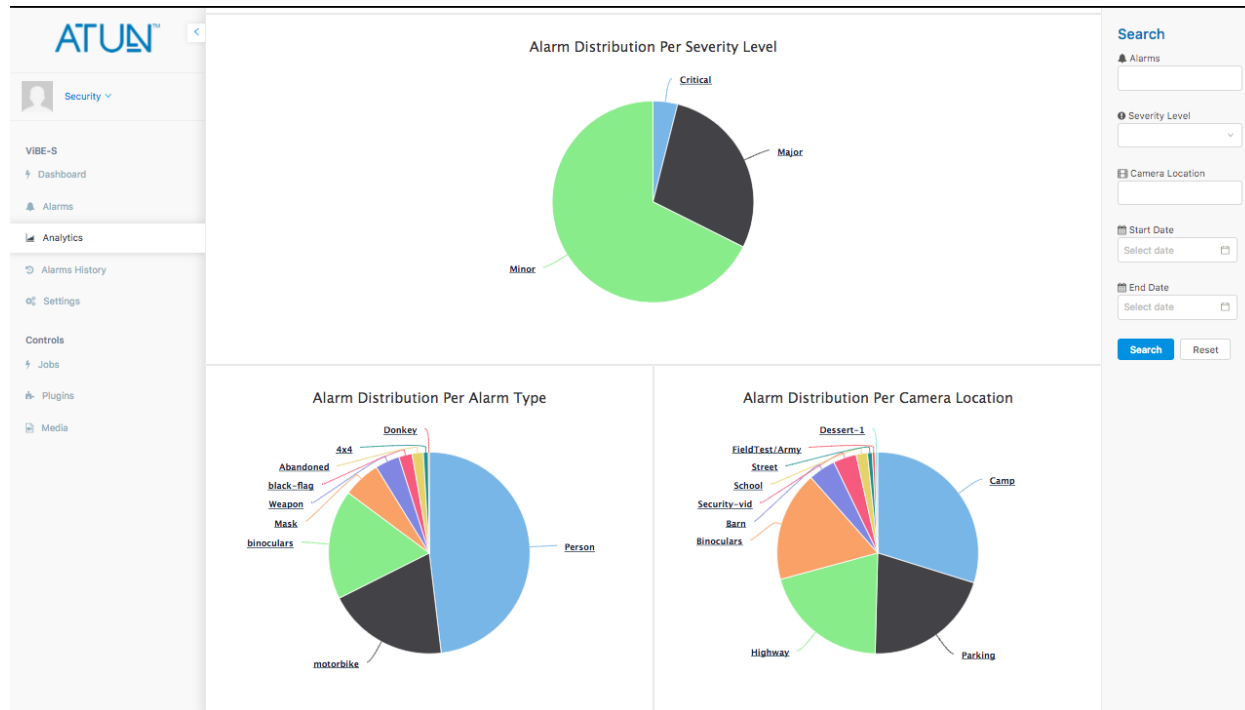
Figure 16 Analytics View

Figure 17 Alarm Distribution

AvidGuard Hardware Requirements

AvidGuard has a minimum requirements as follows
1. Minimum of 4 cores for a single camera, then an additional core for each additional camera
2. NVidia GPU hardware with minimum of 1000 cores (NVidia ??)
3. Ubuntu 16.04

AvidGuard Installation

AvidGuard is installed in few simple steps
1. Download and extract AvidGuard tar file from AvidBeam website
2. Run AvidGuard installation script (./install). The installation script is an interactive script and will require some information such as
    a. Machine specifications (master/slave, memory, etc.)
    b. Plugin name/location
3. Once AvidGuard is installed and launched, admin user should use AvidGuard web configuration to
    a. Add cameras using their RTSP stream IP
    b. Add plugin to be used for video frame processing such as object detection. Those plugins are provided with AvidGuard installation package
    c. Create processing jobs and start them
4. Once the job is started, AvidGuard will start accessing cameras, processing their video feeds, then output the results in the alert, and DASH views