AI Powered Tailgating Detection

Datasheet v4.3

Revision Date : July, 2021

AllGoVision

see. sense. secure

Website: www.allgovision.com

Email ID : contact@allgovision.com

Contents

COPYRIGHT INFORMATION

INTRODUCTION

Tailgating –The Tailgating feature identifies individuals or vehicles that closely follow the individual or the vehicle preceding them to gain entry to a controlled/restricted access area. It detects and deters unauthorized access through secure gateways and logs potentially unsafe activities through accurate visual verification. This feature is compatible with all leading access control systems and it is extremely simple to configure and deploy. Backed by advanced object classification servers, this feature can reliably detect and distinguish between multiple objects types and enables customizable detection for both humans and vehicles. It also comes with flexible output triggers that effectively initiates the follow-up actions for almost all application requirements. The Tailgating feature is primarily used in offices, shopping malls, and gated communities to deter and prevent unauthorized access.

Deep Learning: A subset of Artificial Intelligence, Deep Learning technology exposes machines to high volumes of tagged data. The machine is then tasked to 'learn', 'analyse', and 'detect' the same information in new datasets which ensures more proficient detection and identification of objects. Since Deep Learning technology is also powered by robust hardware infrastructure, the analytic output is better and faster.

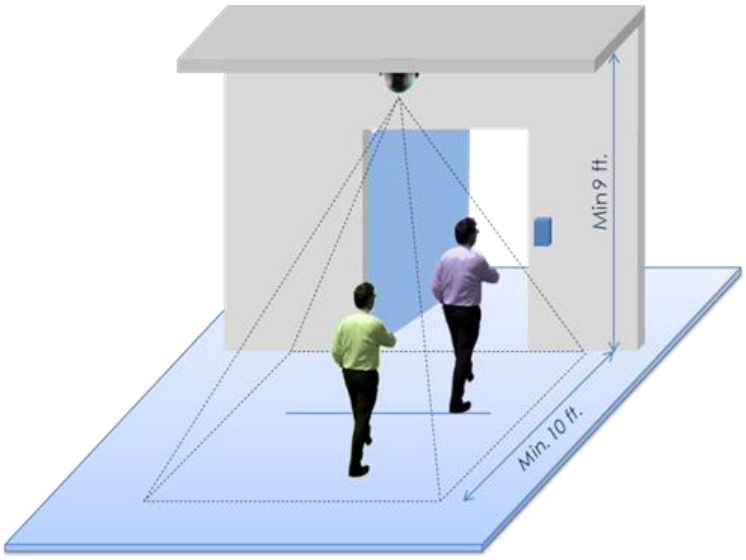
Use of Deep Learning in Tailgating: The use of Deep Learning for Tailgating brings it closer to human perception. Advanced Deep Learning methods can assess large datasets of moving and stationary objects and the layered filters can take the minutest details into account. This increases the degree of accuracy in generating alerts against Tailgating. Thanks to the technology's improved processing performance and superior object classification capabilities, it can efficiently detect and identify multiple object types with low visual biasing and false alarms.

SYSTEM REQUIREMENTS

AllGoVision analytics has the following system hardware and software requirements.

CATEGORY	REQUIREMENT
Operating System	Ubuntu server 18.4, Windows Server 2016, Windows Server 2019
Network	Ethernet, 1GB or higher recommended
Hardware Requirements	x86_64 Platform, AVX 2 Support 6th Gen and above + Nvidia GPU
Frame Rate	Frame Rate > 10 fps
Database	Maria DB (X64) 10.3.13.0
Stand Alone version camera support	Camera Models from Axis, Pelco, Bosch, Hikvision, Honeywell, IQinvision, Sony, Dahua, Panasonic, Brickcom, Indigovision, Cisco, Samsung, Acti, Digital Watchdog, and others (ONVIF Cameras).
VMS Support	Honeywell DVM, Honeywell Maxpro, Milestone, Genetec, IndigoVision, ExacqVision, Cognyte (Verint), Bosch, Network Optix Note: With VMS all cameras supported by VMS will be supported
Reporting & Analysis Software	AllGoVision Alarm Center

INSTALLATION



Overhead Camera Height of Installation = minimum 9-10 feet

Focusing over the area where people are entering / exiting through accessing gate

The distance covered in the camera view along the movement direction = minimum 10 ft.

No occlusion scenario

TECHNICAL HIGHLIGHTS

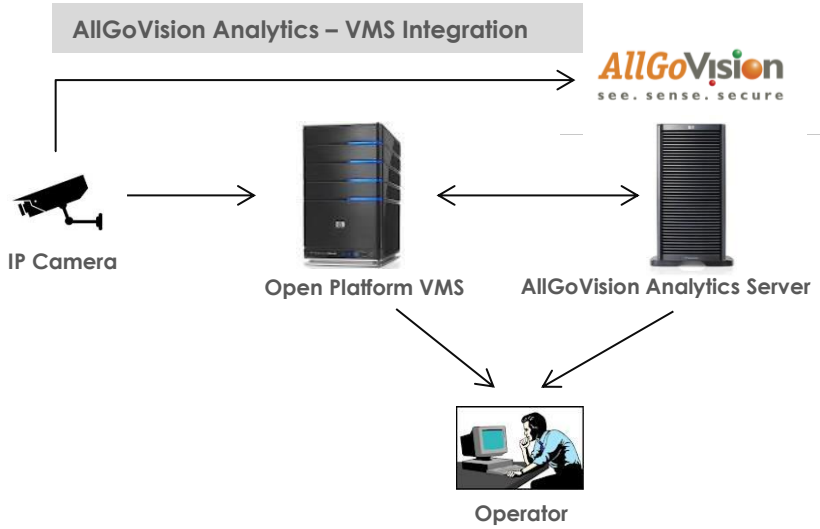
- ✓ High accuracy using propriety AI based algorithms
- ✓ Detection works both day and night, even with partially occluded persons
- ✓ Detection is immune to shadows, lighting changes, other moving objects in scene and animals
- ✓ Low alarm miss-rate
- ✓ Capability to handle occlusions due to various objects
- ✓ Generated alarms may be filtered using metadata attributes of person

INTEGRATION FLEXIBILITY

AllGoVision application is available in 2 flavours:

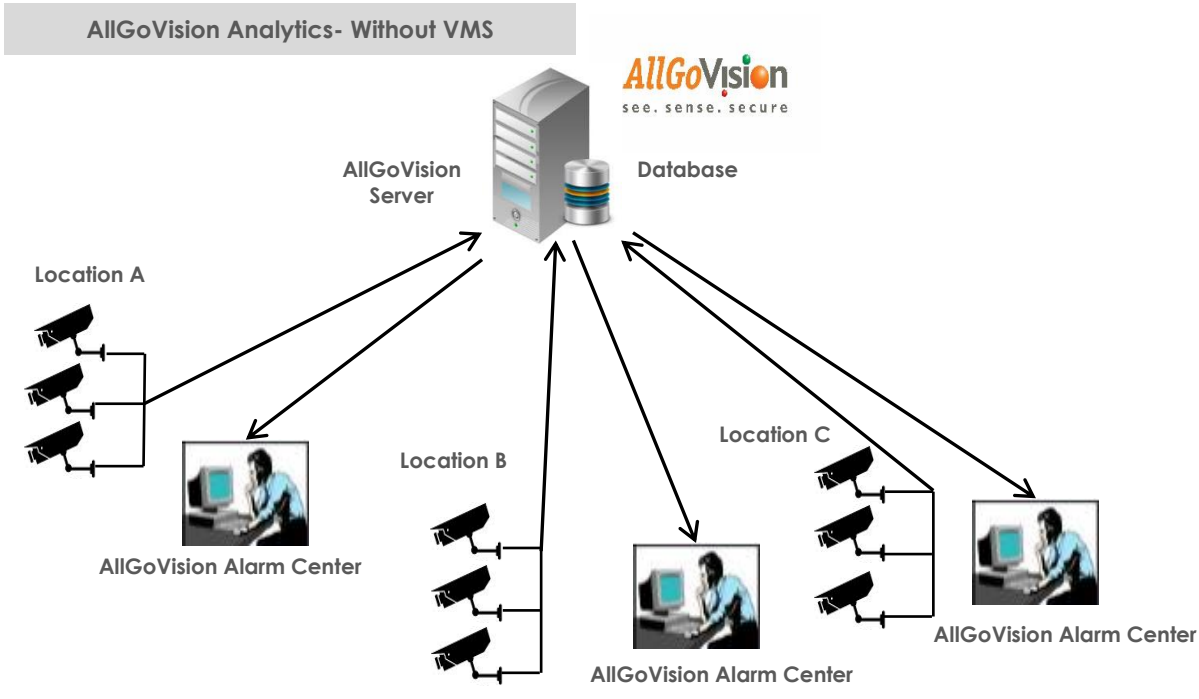
With VMS:

AllGoVision application is based on Open Platform Standards.
It is integrated with many open platform VMS.



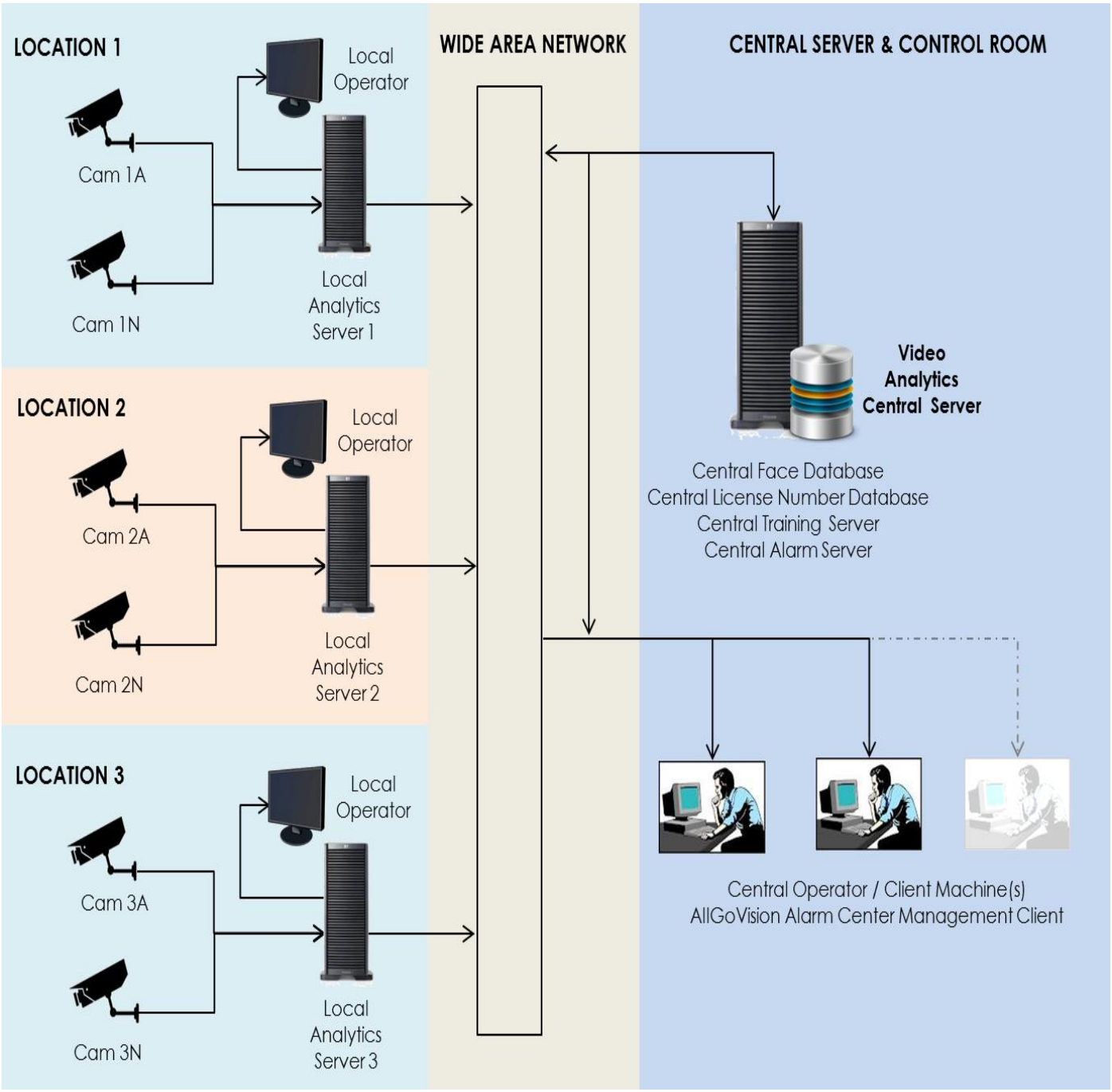
Without VMS:

- It is a standalone application.
- Directly takes the video feed from camera.
- The alarms and reports are seen in AllGoVision Alarm Center.



Federated Architecture

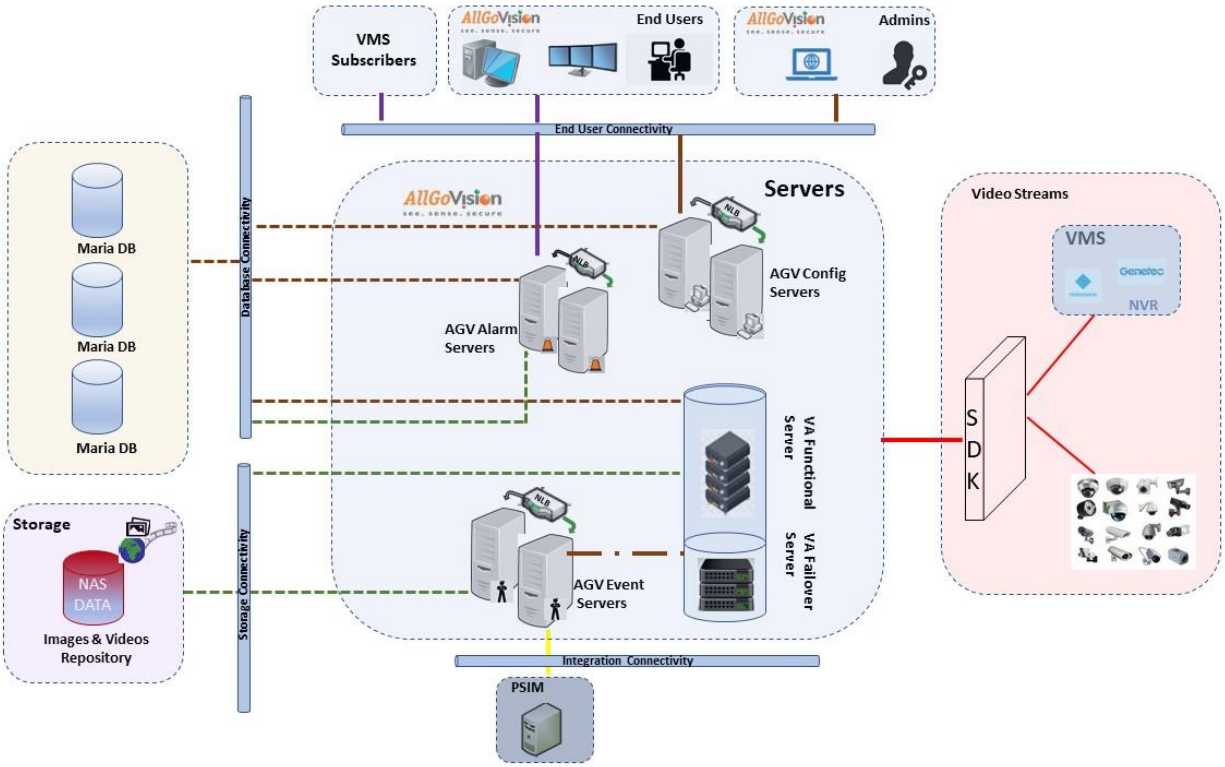
- With Federated Architecture, analytics can be done at local servers and viewed by local operators.
- A central server with a central operator can view all the alarms in the system generated by all the local servers.
- Alarms from different clients can be seen at the central Alarm Center and alarms are differentiated through Client IDs.



Redundancy / Failover

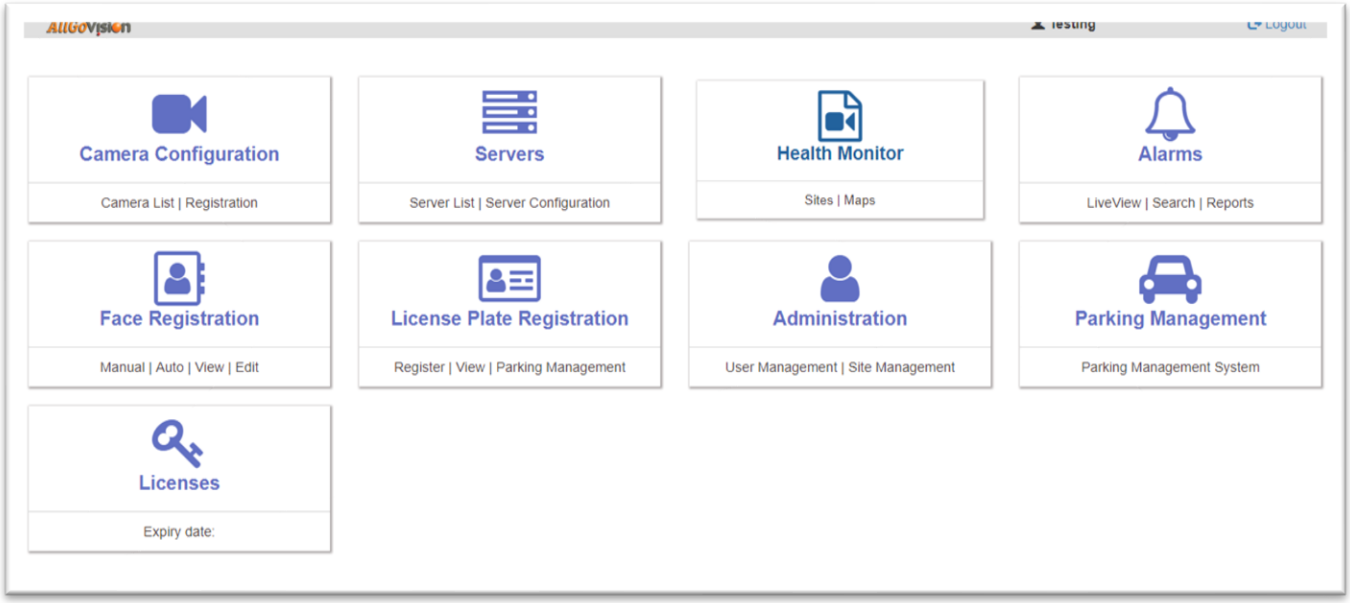
- Config Server can be setup for active/passive redundancy. NLB is used to manage the Active/Passive redundancy. When the active Config Server is up, all requests will be serviced by it. Only when it is down, requests are serviced by the passive Config Server.

- For video analytics, redundancy is achieved by having redundant server capacity for N:1 or 1:1 redundancy. When one or more VA Servers fail, the analytics pertaining to the cameras running in that server are re-assigned to a pre-designated set of servers.

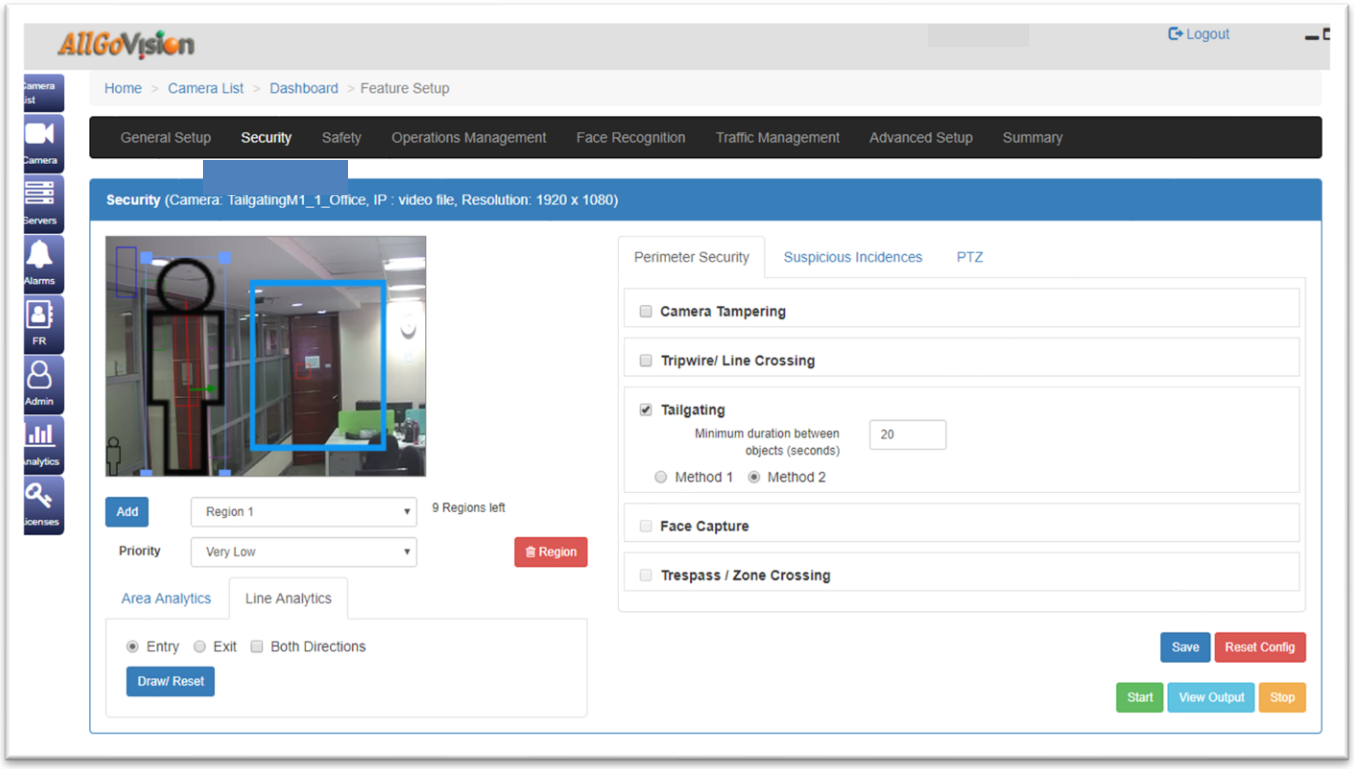


ALLGOVISION GUI

AllGoVision product offers a graphical user interface with the choice of native windows-oriented, tab based, point and pick interface along with the Web UI. The options are provided to add cameras directly or from VMS, provide configuration and view alarms whenever an event occurs.



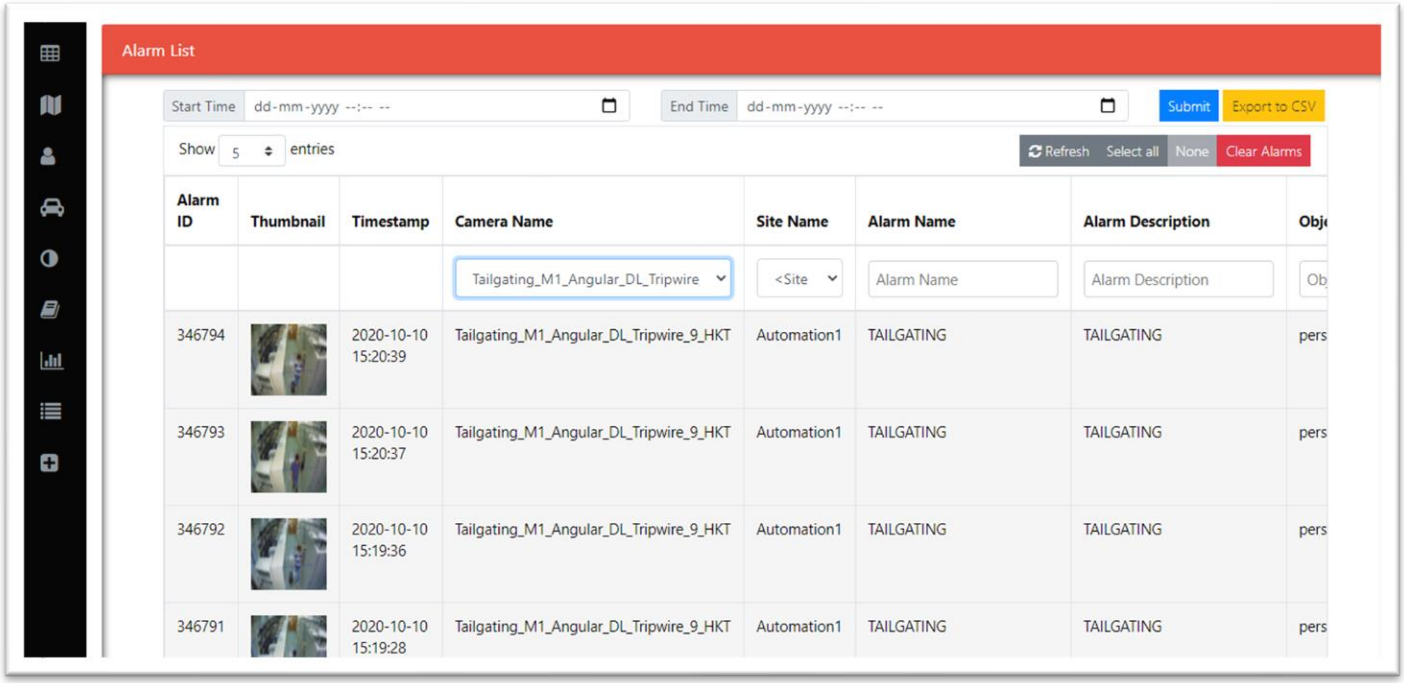
AllGoVision Dashboard



Tailgating Configuration

ALLGOVISION ALARM CENTER

AllGoVision Alarm Center is a Client to view all the alarms generated by AllGoVision analytics running on the same machine or running on different systems in the same network. It also supports report generation.



Tailgating Alarm in Alarm Center