Eagle Eye Application Note - AN003

Real-time Video Monitoring and Insight Using Eagle Eye Cloud VMS Analytics

2025-10-16 Revision 3.0

Target Audience

This Application Note is intended for administrators of Eagle Eye Cloud VMS. Anyone who wants to set up or configure Analytics will benefit from this app note. No prior background knowledge is needed.

Introduction

Eagle Eye Cloud VMS Analytics can be used for both real-time monitoring and for mining insights from historical video. Eagle Eye Networks offers five different Analytics: Counting, Line Crossing, Intrusion Detection, Loitering, and Camera Tampering.

Analytics are available for any camera connected to a Bridge/CMVR (except analog cameras on hybrid Bridges/CMVR). All five analytics can be activated simultaneously. It's important to note that the stream used for analytics is MJPEG (secondary stream), and the camera should support a frame rate of 12 fps for best results.

Analytics are available on all Editions of the Eagle Eye Cloud VMS (Standard, Professional, and Enterprise). Read the application note, AN043 Eagle Eye Cloud VMS Editions Explained in Detail, for more information.

Background

Each analytic serves its own purpose and is described below:

- **Counting:** Used to count objects crossing a line in either direction. For the highest accuracy in counting objects, use a dedicated camera mounted with a top-down view at an angle less than 10° from the floor, where objects remain the same size as they travel through the image. For best results, the camera should be ceiling-mounted at 10–12 feet. For the object to be counted, at least 50% of it must cross the line. You can configure only

one line per camera. It is important to note that this analytic is pixel-based, meaning that it will count each group of pixels crossing the line as one object. If multiple objects cross at the same time and are very close together, it may only be counted as a single object.

- **Line Crossing:** When an object crosses a specified line in the selected direction, an alert can be generated. As with 'Counting', 50% of the object must cross the line to be detected, and only one line can be configured per camera.
- **Intrusion Detection:** If an object enters a defined forbidden area, an alert can be generated. There is no limitation on how many areas can be defined in the camera view. The camera's angle should be set such that objects passing through the frame are a consistent size. For best results, the camera should have a view perpendicular to the defined forbidden area.
- **Loitering:** If an object remains in a defined region longer than a specified time (between 1 second and 2 minutes), an alert can be generated. Just as with 'Intrusion Detection', there are no limits on the number of areas that can be defined per camera.
- **Tampering:** Tampering detection generates an alert when someone tries to block the camera's view or when the image is significantly altered.

Functionality

Analytics must be configured on each camera, and the menu is available in **Camera Settings > Analysis**, as shown in Figure 1.

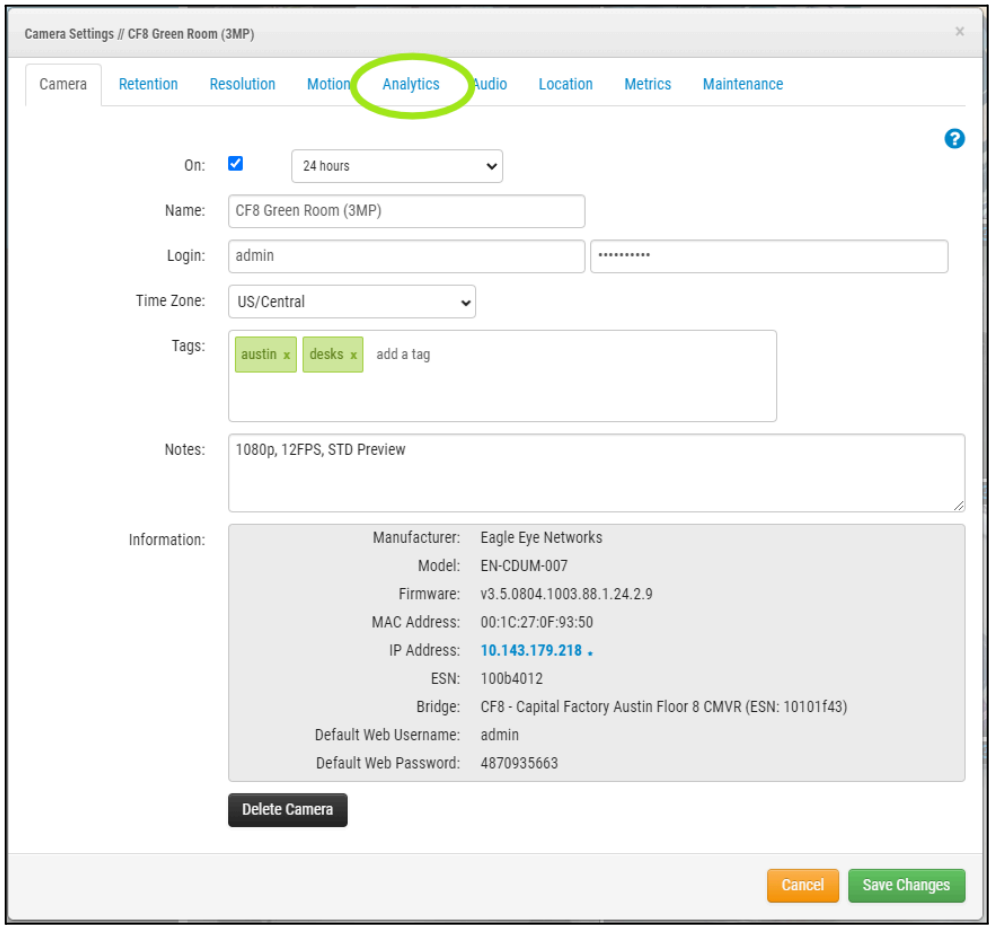

Figure 1: Analytics tab location within the camera settings window

From within this menu, activate any of the five analytics that the Eagle Eye Cloud VMS provides. If required, activate all analytics for each camera. See Figure 2.

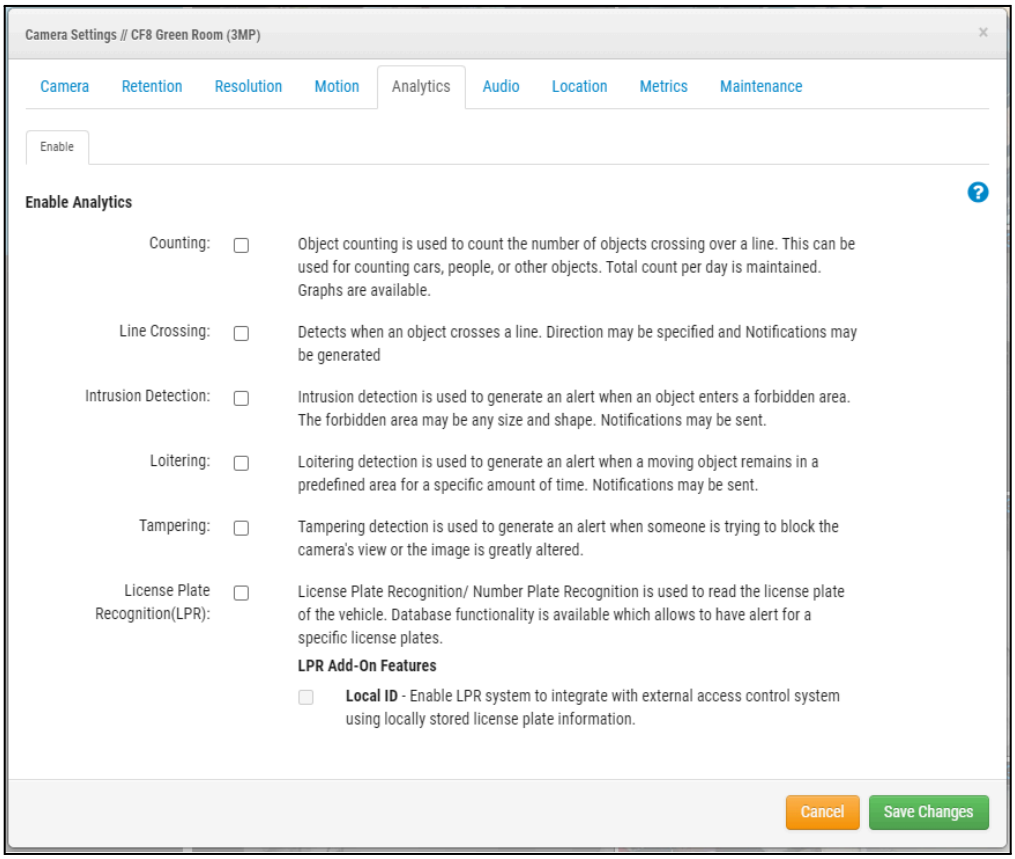

Figure 2: Analytics tab within camera settings

When activating Analytics, it's important to select and check the following:
Resolution menu → Preview Video → Quality → Set to Analytics (this is usually done automatically).

- Ensure Preview Video Quality is set to Analytics under the Resolution tab.
- By clicking an analytic, it becomes enabled, and a new sub-tab appears for each enabled analytic under the Analytics tab. See Figure 3.

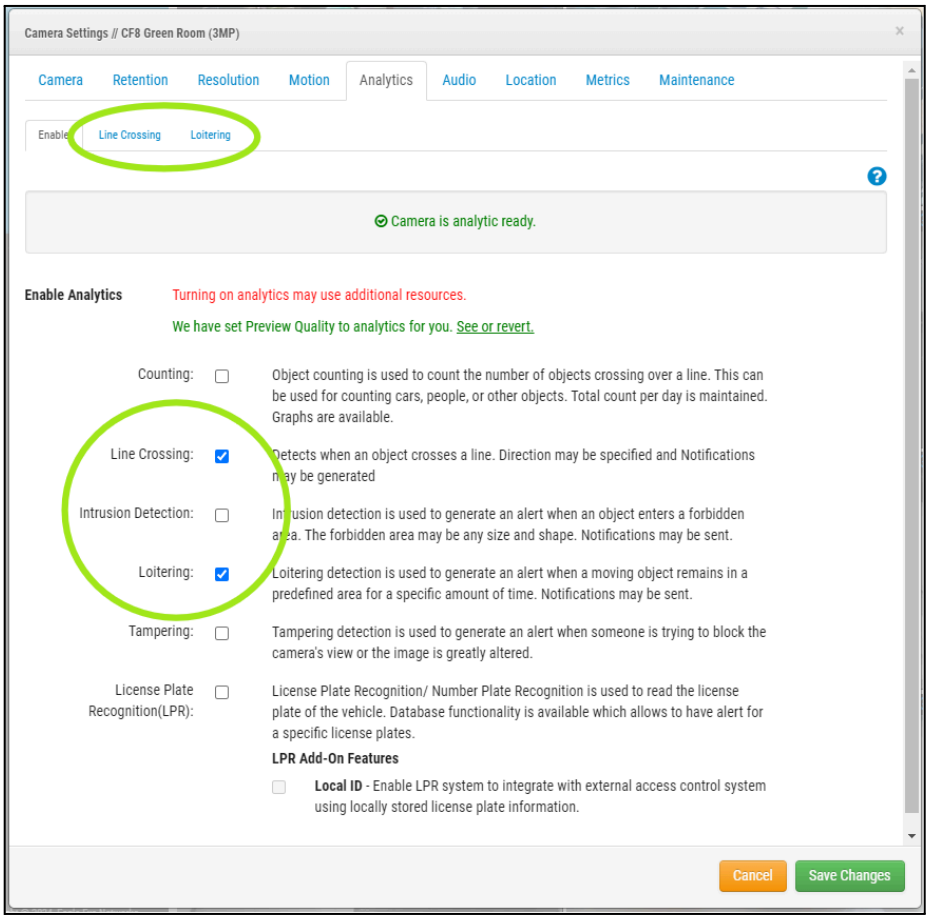

Figure 3: Analytics tab within camera settings

Separate tabs allow the user to configure each Analytic. Each analytic must be enabled before selecting **Save Changes**; otherwise, it will not be applied. For all analytics except "Tampering," it is important to note that the configuration of the "Object Detection Settings" applies to the camera view, meaning the minimum and maximum object detection sizes will be the same for all analytics in use. Select the blue question mark in the top right corner for more information on Object Detection Settings.

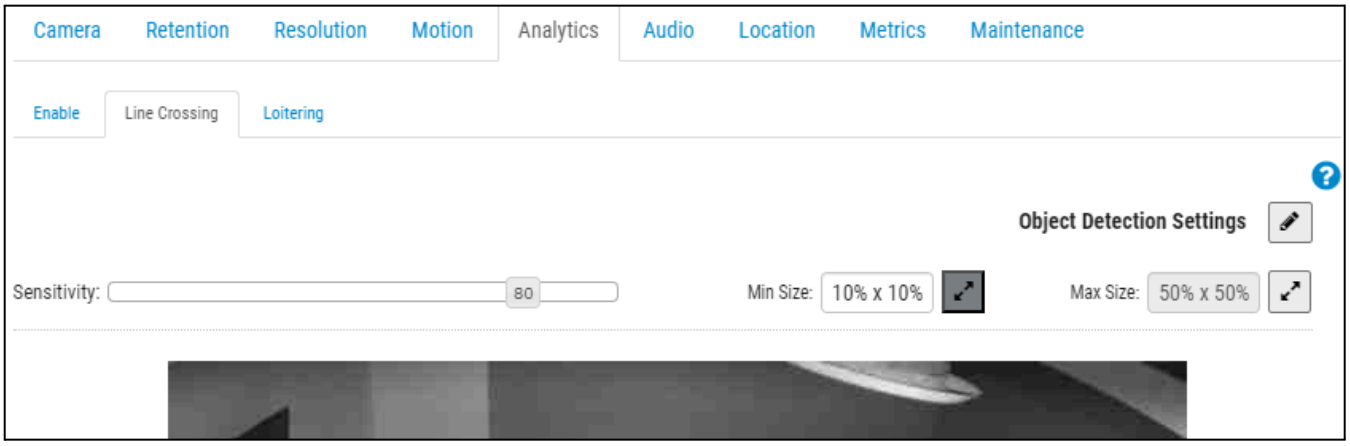

Figure 4: Object detection settings will apply for the camera view

1. Counting

Draw a line in the camera view and set the direction the object will enter. Only draw one line per camera. A top-down view with the camera at an angle less than 10° from the floor is also necessary to ensure the best results, as shown in the picture below.

Note: For best results, place the line in the center of the field of view and allow as much space as possible to either side. Proper configuration should allow the analytic to identify an object fully in view and track its motion clearly over the line. Avoid placing analytic regions or lines near the edge of the view. See Figure 5.

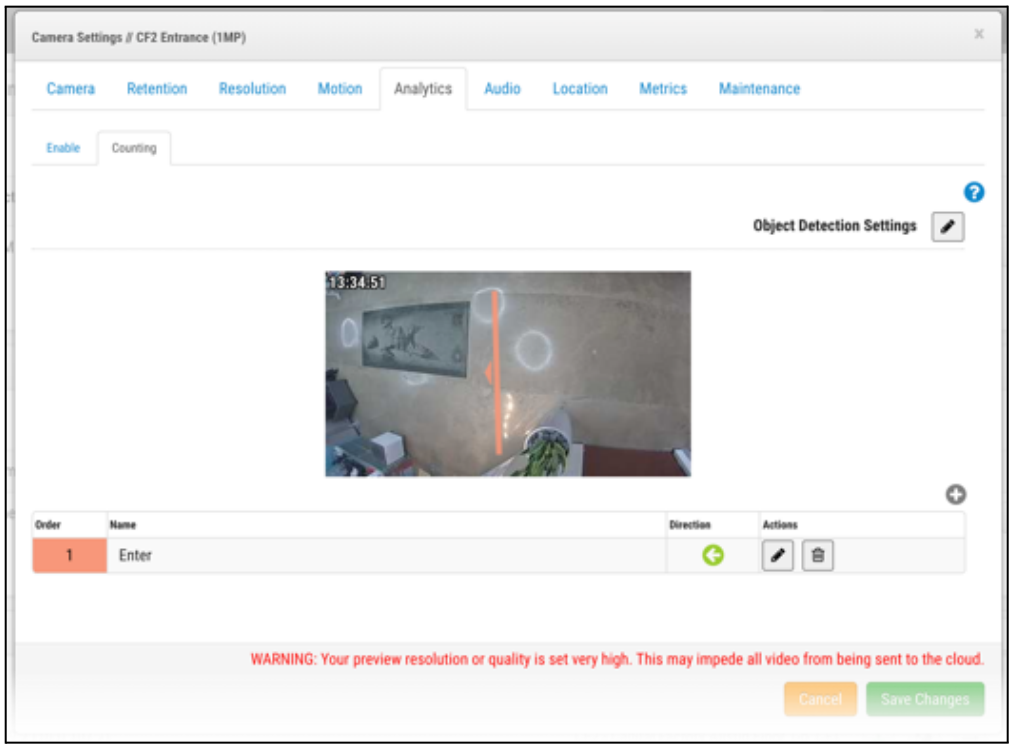

Figure 5: Example of a line placed in the center of the field with plenty of space on either side

The system automatically counts +1 for the chosen direction and -1 for the opposite direction, and counts them in real time, as shown in Figure 6.

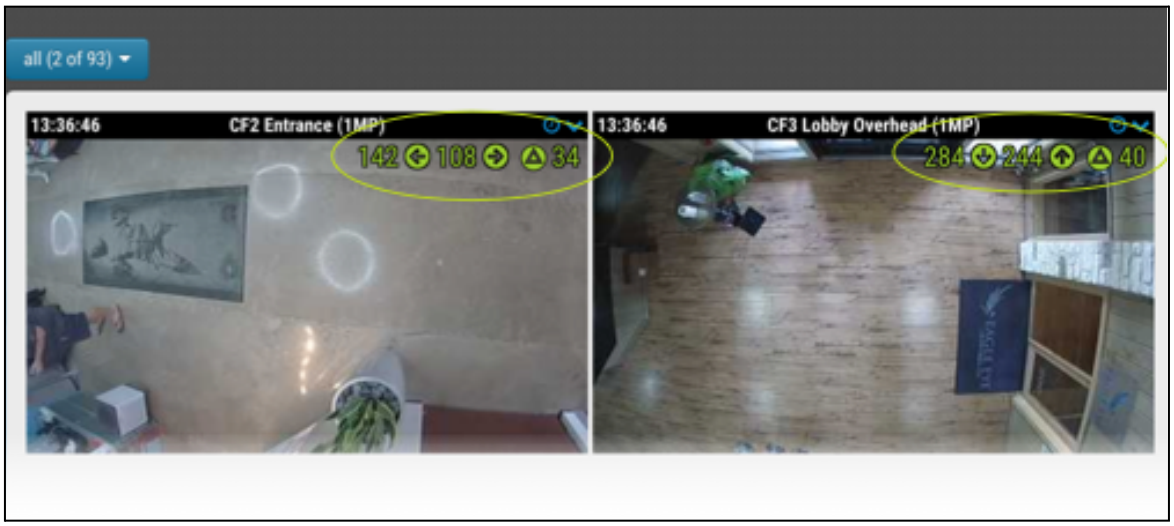

Figure 6: Real-time tracking/counting of objects crossing a line in both directions, including a total

Full statistics are available from analytic graphing, which can be found on the Dashboard next to the camera icons and as shown in Figure 7.

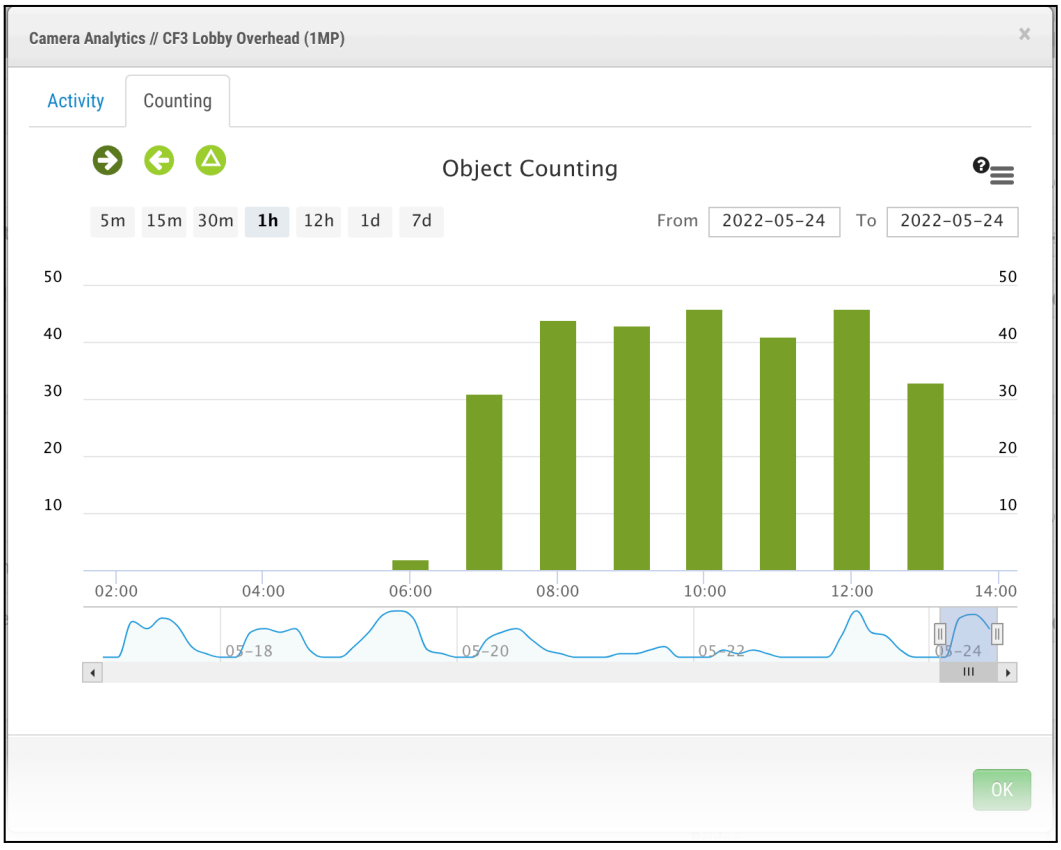

Figure 7: Analytic statistics and graphs can be found on the Dashboard next to the camera icon

The data can be exported in several formats (XLS, CSV, PDF, JPEG, etc.), which are available via the Eagle Eye Networks API, and can be extracted to be analyzed at a later date or injected into third-party systems to be combined with additional data for better management of business KPIs, for example.

2. Line Crossing

The configuration is similar to the “Counting” analytic. Draw a line in the view to detect objects crossing it. Remember, only one line per camera and 50% of the object must cross it to be detected. The camera should be installed no more than 45° from the floor.

Note: It is best to draw the line in the middle of the view so the system can detect the object more easily. Avoid putting the line near the edge of the camera view. Fisheye cameras should be avoided. See Figure 8.

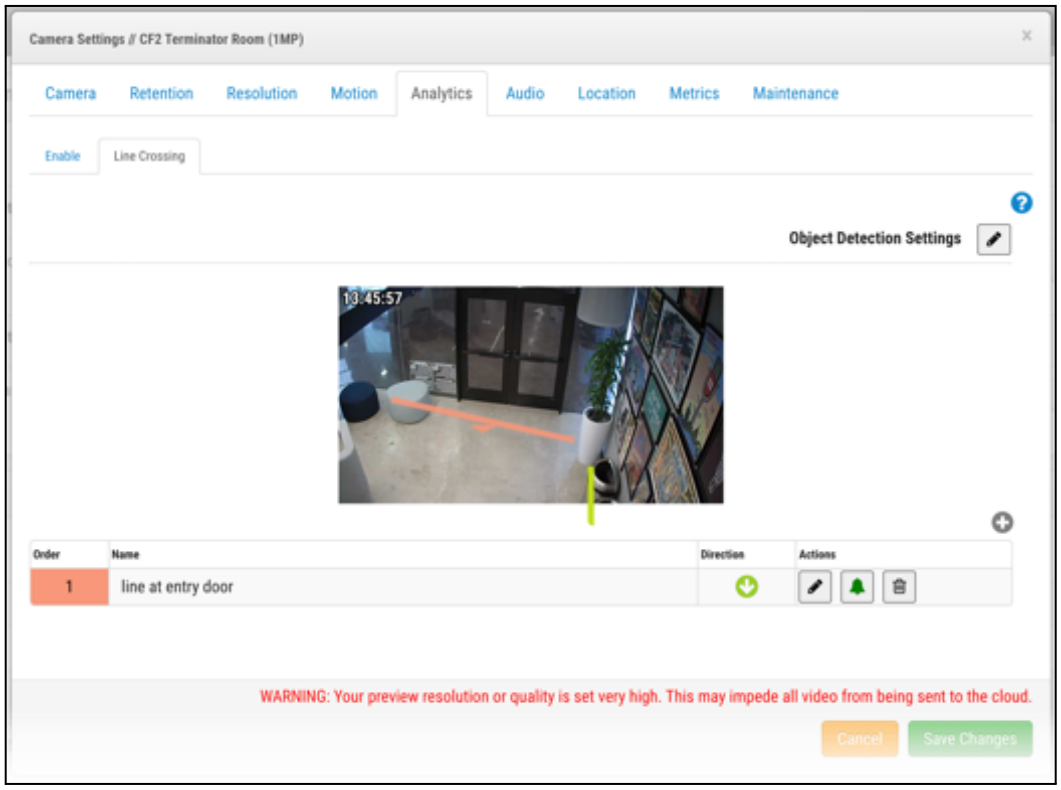

Figure 8: Example setup of the Line Crossing Analytic with the line in the center of the camera view

3. Intrusion Detection

Configuration is done by creating areas in the camera view. There is no limit to the number of areas that can be created, but careful consideration should be given when implementing. The camera’s angle should be set such that objects passing through the frame are a consistent size. For best results, the defined forbidden area should be perpendicular to the camera’s angle of view (e.g., a camera with a bird’s-eye view should have the forbidden area designated on the ground).

Note: Try to avoid creating areas at the edge of the camera view, and, if possible, extend the area so the object can be captured before it goes out of the area and view. The Object Detection settings should be configured to detect the smallest and largest objects that intrude into the defined forbidden area. See Figure 9.

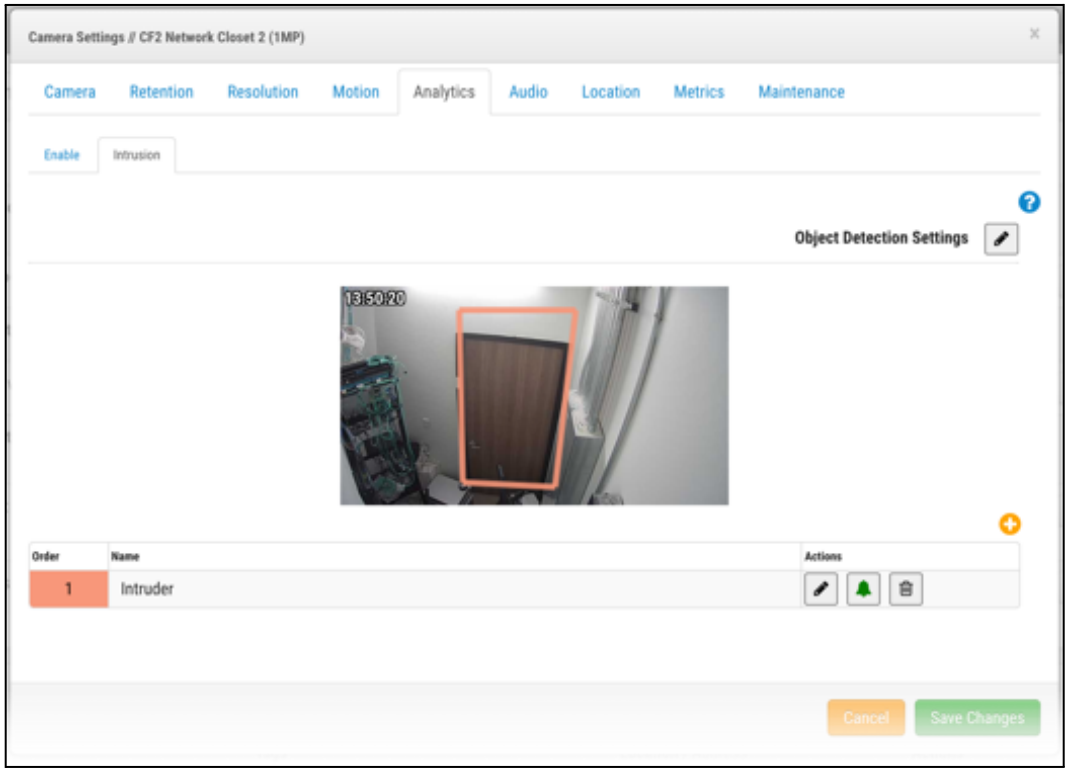

Figure 9: Example setup of the Intrusion Detection Analytic that avoids creating areas at the edge of the camera view

In this configuration, any person who enters the room will trigger an alert. As shown in Figure 9, options for where to place the area within the camera view may be limited.

4. Loitering

Configuration is similar to “Intrusion Detection” where areas are drawn within the camera view. However, in this case, the alert will trigger only when an object remains in the area for longer than the specified time. As shown in Figure 10, there is a parameter called “Dwell time,” and any dwell time can be selected (from 1 second to 2 minutes). For best results, the area defined should be perpendicular to the camera’s angle. Standard fixed-lens cameras should be used. Fisheye, PTZ, and motorized lens cameras should be avoided to prevent unexpected issues.
Note: Try to create an area that covers more than what is required to get the best results, especially with objects, as there tends to be a lot of movement. See Figure 10.

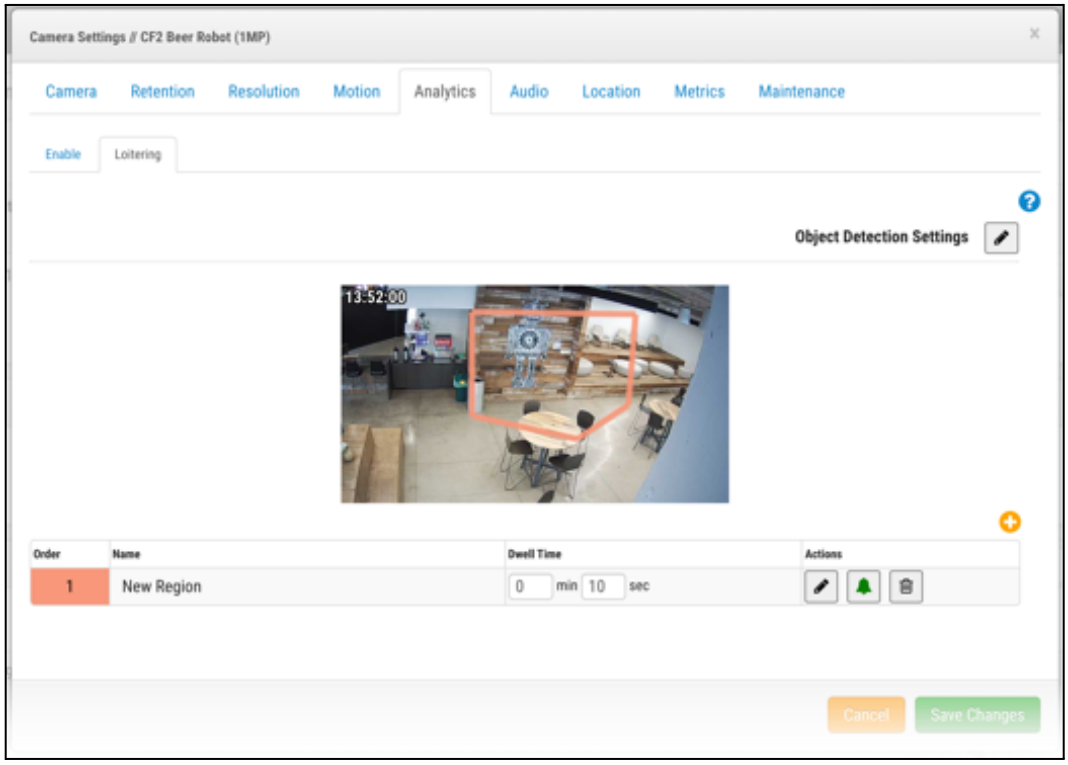

Figure 10: Example setup of the Loitering Analytic with a larger area than is required

5. Camera Tampering

For camera tampering analytics, sensitivity is the only parameter to adjust, depending on how you want alerts sent when the initial view changes.

Note: Leave the parameter as is for initial testing and adjust it as necessary based on the alert level you require. See Figure 11.

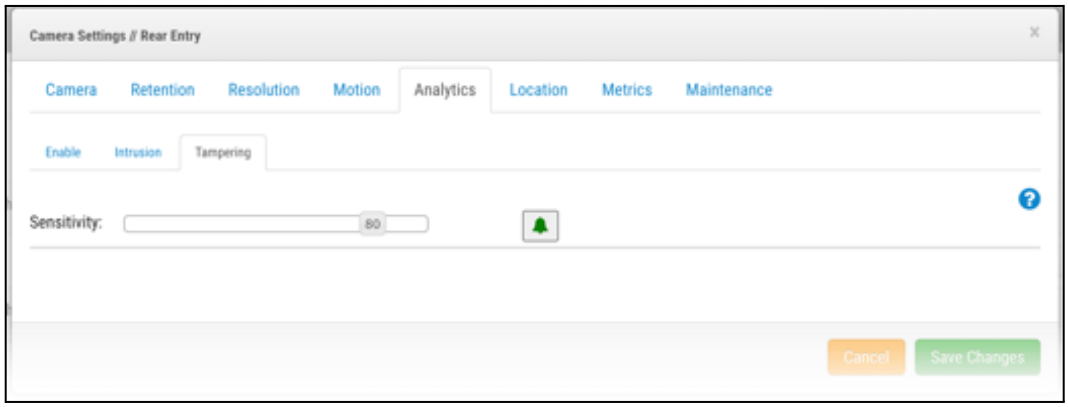

Figure 11: Example view of the sensitivity setting. Leave as is for initial testing and adjust as necessary

Usage

There are a variety of uses for Eagle Eye Networks Cloud VMS analytics. Knowing that existing IP cameras already installed at a customer site can be used, there is no need for a large up-front capital expenditure on cameras to optimize operations through the use of business analytics.

Object Counting

- Count objects crossing a specific threshold through the view of a camera.

Line Crossing

- Line Crossing can be used to track vehicles as they enter and exit designated areas, or for situational awareness when monitoring crowds or temporarily restricted areas.
- Line Crossing tracks an object's movement over a specified line and results in an alert and event recording so that notifications always occur when a person or object crosses a line.
- More focused on security, Line Crossing analytics will help detect in real time when an object crosses a restricted threshold and can provide alerts for this activity if desired.

Intrusion Detection

Using Areas, Intrusion Detection allows for the monitoring of certain locations within a camera's view and for various purposes, such as the following:

- Protecting an asset in a specific location
- Parking spaces
- Restricted area bypassing a door (an example of an area more useful than a line)
- Detection of people near a fence or going over a fence
- Set up alert levels for different areas. For example:
    - Configure an area at 15 m - Warning event
    - Configure an area at 7 m - Alert event

Loitering

As with Intrusion Detection, we can use several areas in camera views to monitor different places. Loitering can be used to:

- Help detect suspicious behavior near an office. For example, people hanging out or standing in certain areas
- Identify cars that have been parked longer than expected in a particular space or location
- Identify people lingering in a certain area when they shouldn't be
- Help detect long wait lines/queues as they grow, so actions can be taken to improve the situation (cashier, bank, lobby, etc.).

Camera Tampering

Camera Tampering allows monitoring a camera view to determine whether it is blocked or the view changes. This is important on specific, high-profile cameras when monitoring important assets or areas, and for ensuring that the cameras have the correct view as installed.

For integrating Bosch camera analytics, read application note AN075.