Eagle Eye Application Note - AN096

Eagle Eye Cloud VMS and Sentinel Integration: How to Use Eagle Eye Automations in the Enhanced User Interface

2025-10-23 Revision 1.0

Target Audience

This Application Note is intended for Eagle Eye Cloud VMS account administrators responsible for setting up and configuring the Cloud VMS. It provides guidance on configuring Automations for Alerts via Rules and Actions for Monitor Computer Systems, Sentinel alarm monitoring system, and for alarm center admin users configuring monitored sites.

Introduction

This document details how to configure Automations for events in the Eagle Eye Cloud VMS. By following this guide, users can leverage AI-based analytics, motion detection, or bridge analytics to detect and report Alarms to Sentinel Monitoring software. The following information is covered in this Application Note.

- Configuring cameras with desired alert types for Sentinel Alarms
- Integration between Eagle Eye Networks Cloud VMS and Sentinel overview
- Creating Rules with Automations
- Creating Actions with Automations
- Validation & Troubleshooting

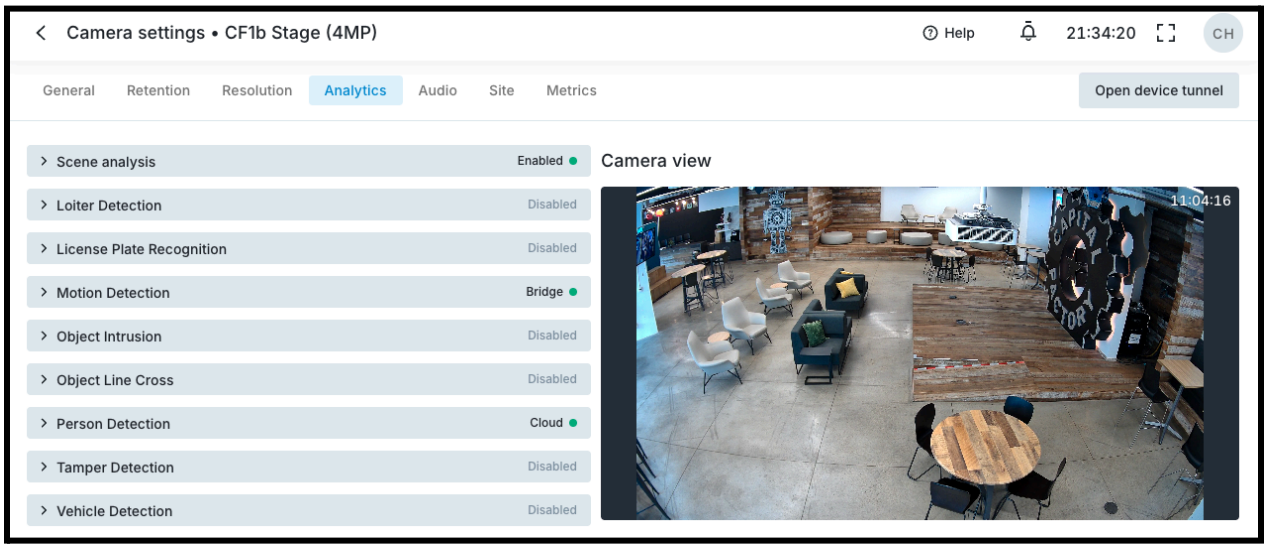
Camera Setup

Use the instructions in this section to correctly set up cameras with regions of interest, bridge analytics, or Eagle Eye Precision Person & Vehicle Detection (Person and Vehicle Alerts require a subscription for Eagle Eye Cloud VMS Camera Analytics).

Camera Settings

- Navigate to Camera **Settings** from the VMS Dashboard (menu to the right of the camera name and status), or from Live View/History Browser (menu in top right of image). Users need access to edit cameras to do this.

- Navigate to the **Analytics** tab:

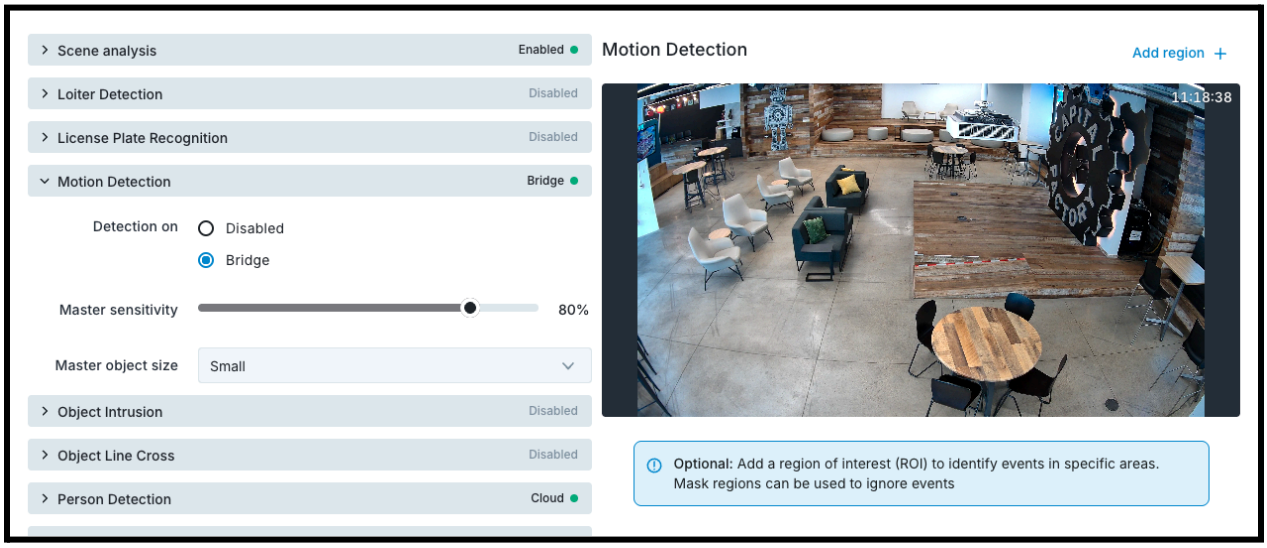


- Based on camera activity or purpose, choose the best alert type for Sentinel monitoring.
  Sentinel Supports the following Analytics:
  - Motion Detection and Motion In Region Detection
  - Loiter Detection
  - Object Intrusion
  - Object Line Cross
  - Tamper Detection
  - Person Detection
  - Vehicle Detection

- Open the configuration using the drop-down menu for Analytic type.

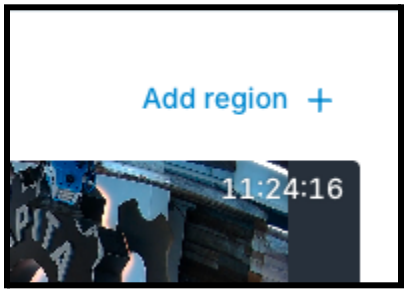
Configure Motion Analytics on the Camera

- The Motion Detection analytic must be ON for the camera for any bridge analytic or cloud AI to function or generate alerts.

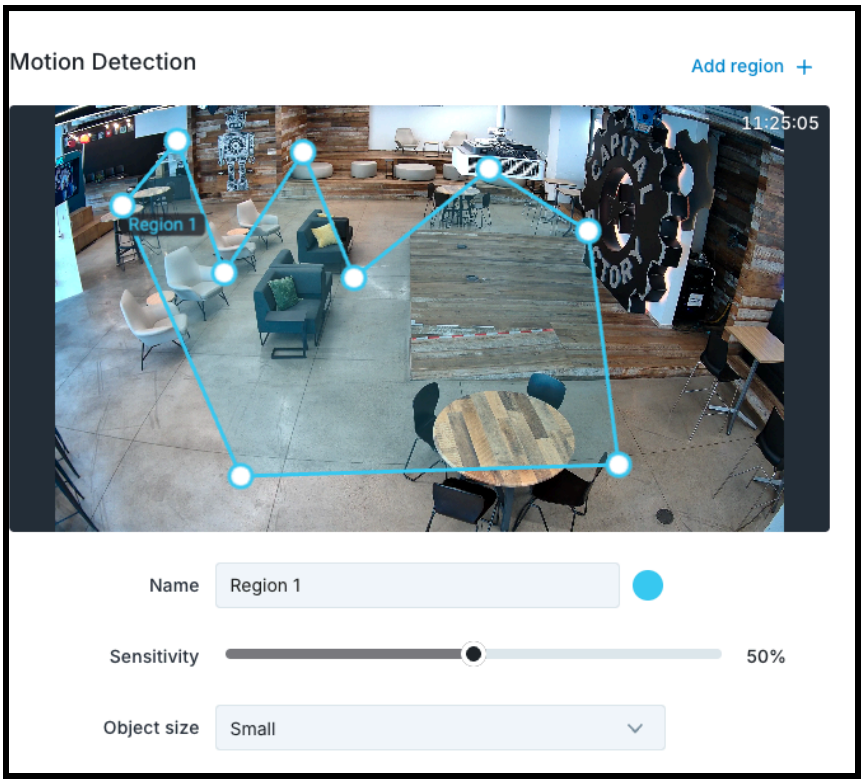


  - By default, cameras are set to a sensitivity of 80% and “small” object size detection.
  - Based on camera placement or other factors, these may need to be adjusted to increase or decrease motion capture within the field of view (FoV).

- For enabling **Motion In Region** Detection, or creating Motion Masks (areas of the FoV that should not be included in recordings or Alerts), select **Add Region +** above the camera image:

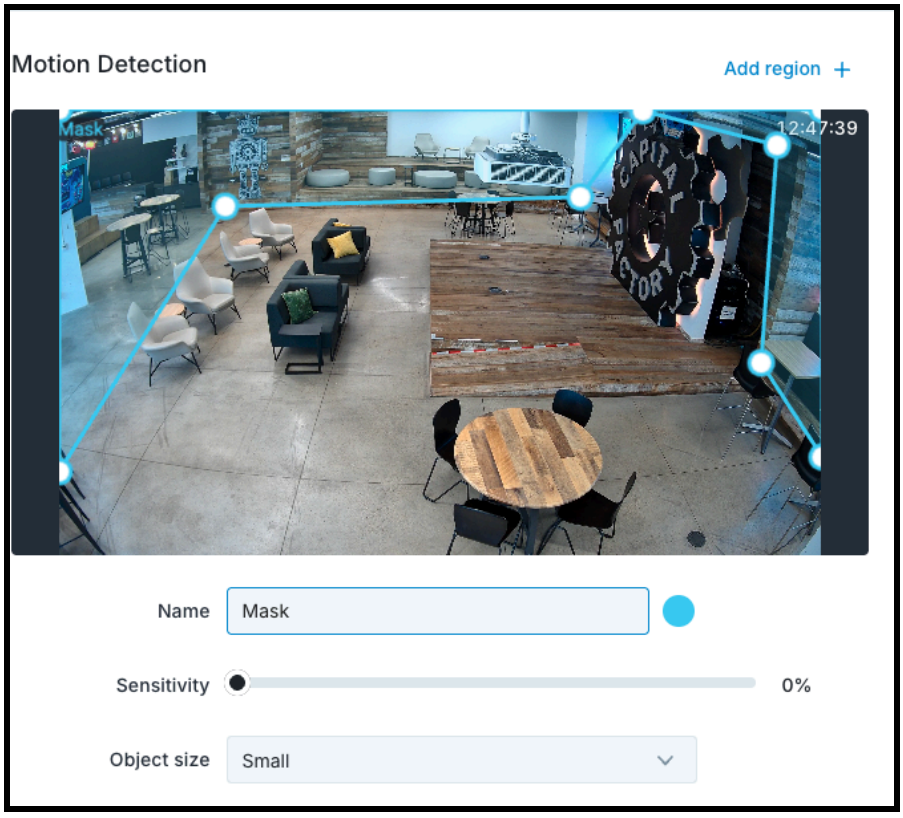


- A dot appears on the screen. Click it to create the first point in a polygon. Add more points to the polygon by clicking to create an area overlay for a region of interest (ROI). Complete the ROI by connecting the last dot to the first.
Once the ROI is saved, the dots can be adjusted to fine-tune the ROI by clicking on the saved region in the camera image. These regions will be where motion is anticipated, which would be an alert-worthy location:



- To set a **Motion Mask**, follow the same steps. In addition, choose 0% in the sensitivity slider to stop activity within the ROI from sending alerts or generating motion recordings.

  Note: Any Motion Mask in the camera settings that overlaps a bridge analytic or Eagle Eye Precision Person & Vehicle Detection **will not generate alerts**.



- Click **Save Changes** to apply the settings.
- Once a Motion ROI is created, the activity within it can be used in Automations to send Motion In Region alerts to Sentinel.
    - If the entire FoV is needed to generate alerts, either do not create an ROI, or in the Automation Rules, choose **Motion Detected** instead of Motion In Region for the Event type in the rule.

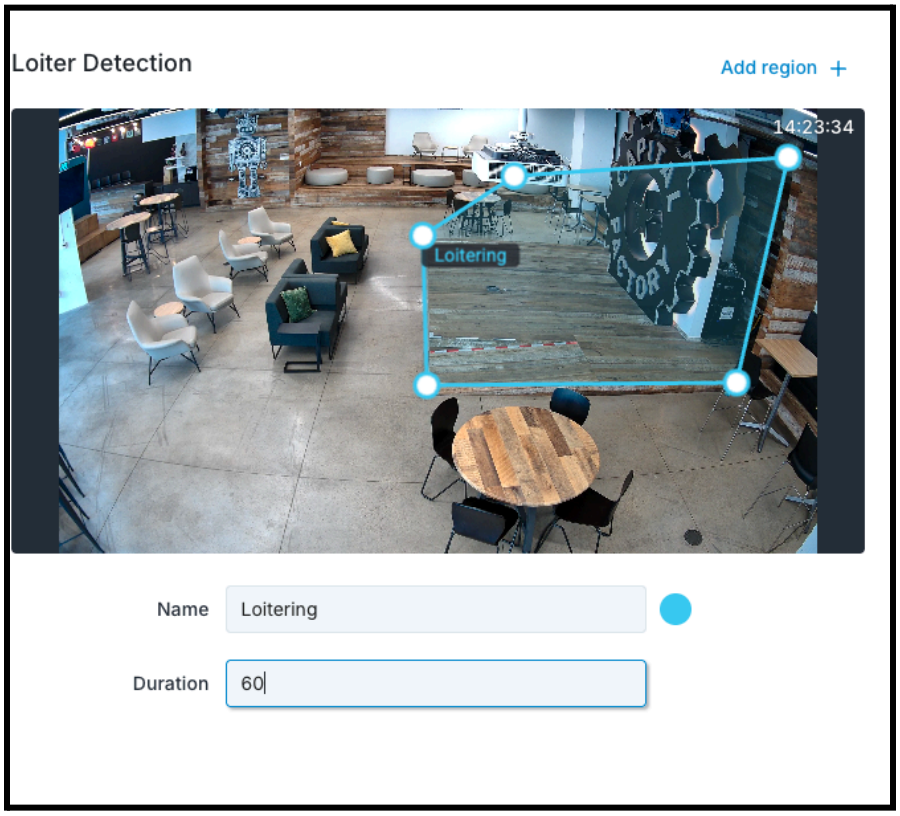
Configuring Bridge Analytics on the Camera

Bridge analytics can be used to generate specific alerts, based on the needs for more refined events over general, non-specific motion activity. Be aware that if a **Motion Mask** in the camera settings overlaps an analytic, that region **will not generate alerts**.

Note: Every Eagle Eye bridge and CMVR has a maximum capacity for bridge analytics to be enabled. Before enabling these features, consult the respective data sheet for your application at een.com/docs/

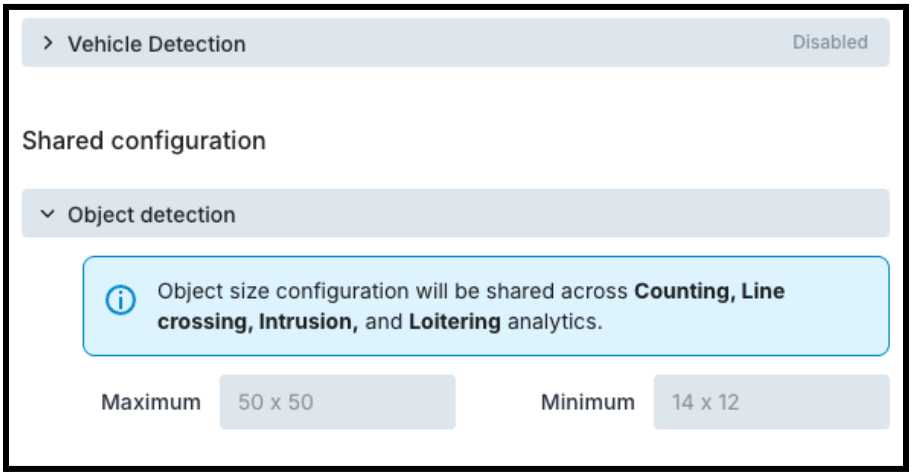
To keep the guide from becoming too specific to Analytics, we will use **Loitering Detection** as the example. The same setup relates to other analytics; a complete guide to the Cloud VMS can be accessed from the **Help** button at the top of the page in the web browser.

- Select the drop-down for Loitering, and create an ROI where loitering should be detected (same function as Motion ROI).

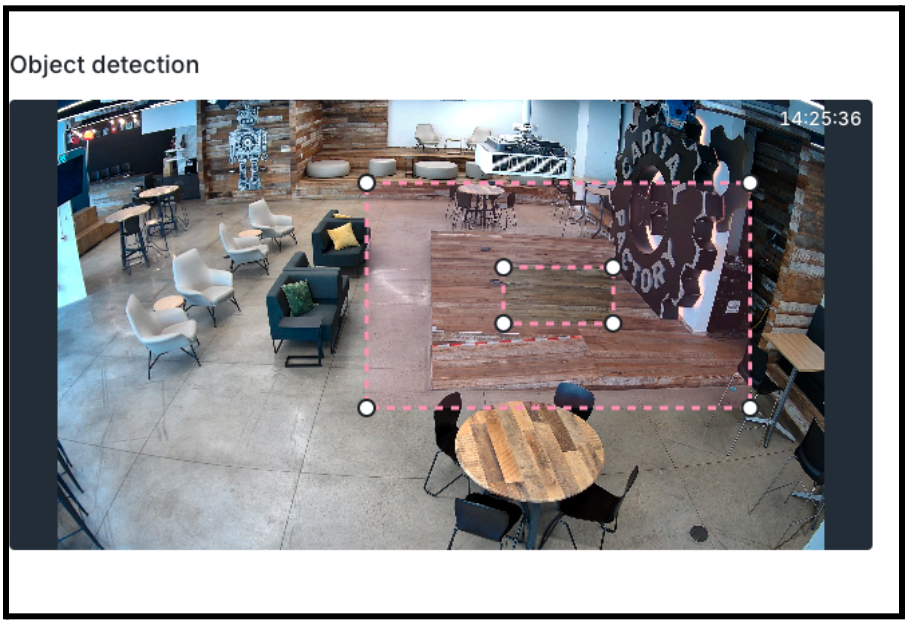


- Choose the desired amount of dwell time before Loitering is detected (1-120 seconds).

- Locate the **Object detection "Shared configuration"** drop-down from the area below Analytics.



- The shared configuration applies to all bridge analytics. Adjust the boxes so that the internal box is smaller than the anticipated objects in the ROI, and the outer box is bigger than the anticipated objects. The location of the box in the FoV is irrelevant; it can be dragged into a place in the region that is being monitored, so that alerts are generated for objects that are bigger than the internal box and smaller than the outer box. For a consistent setup, if applicable, have another person or object placed in the FoV that meets the parameters for detection, to make sure the object is contained within the highlighted area between the two boxes.

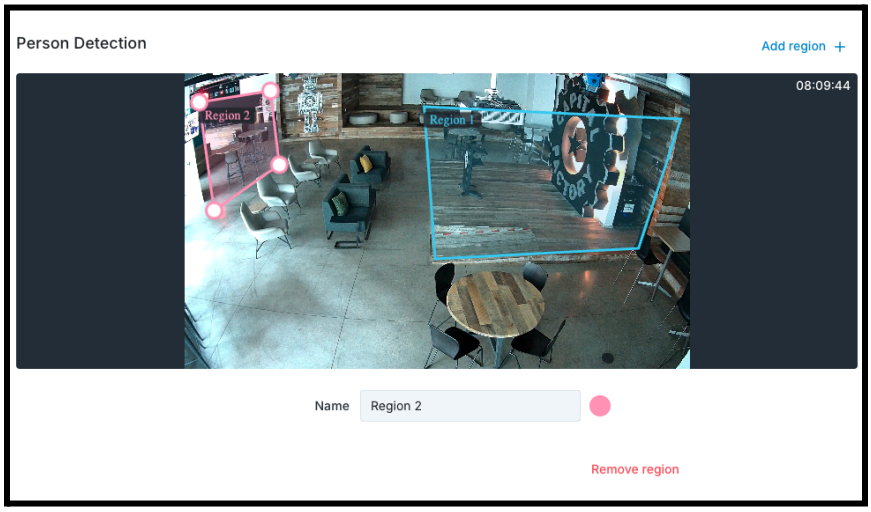


Configuring Eagle Eye Precision Person & Vehicle Detection on the Camera

The setup for Eagle Eye Precision Person & Vehicle Detection is the same as for setting Motion Regions or Analytic Regions. Create an area in the camera view where persons or vehicles need to generate alerts. If the entire FoV needs to be aware of these objects, no ROI is necessary; however, be mindful that if a Motion Mask is enabled in the camera settings, this region will not generate alerts.
A key distinction between bridge analytics and Eagle Eye Precision Person & Vehicle Detection is the absence of restrictions on the number of cameras on the bridge that enable this feature, as event processing is handled in the cloud.
Person and vehicle alerts significantly reduce false positive events, as these objects are almost always associated with real alerts.

- Bridge analytics and Eagle Eye Precision Person & Vehicle Detection alerts cannot currently be combined into a single event; each should be used independently. For example, if an alert should be generated by a person crossing a line in a specific direction, an Object Line Cross Analytic should be configured for the area. Additionally, a Person ROI can increase detection for people in the same location.

- You can also set up multiple ROIs to capture people or vehicles in different locations in the camera's FoV.



Sentinel Integration and Site Setup (For Sentinel Account Admin)

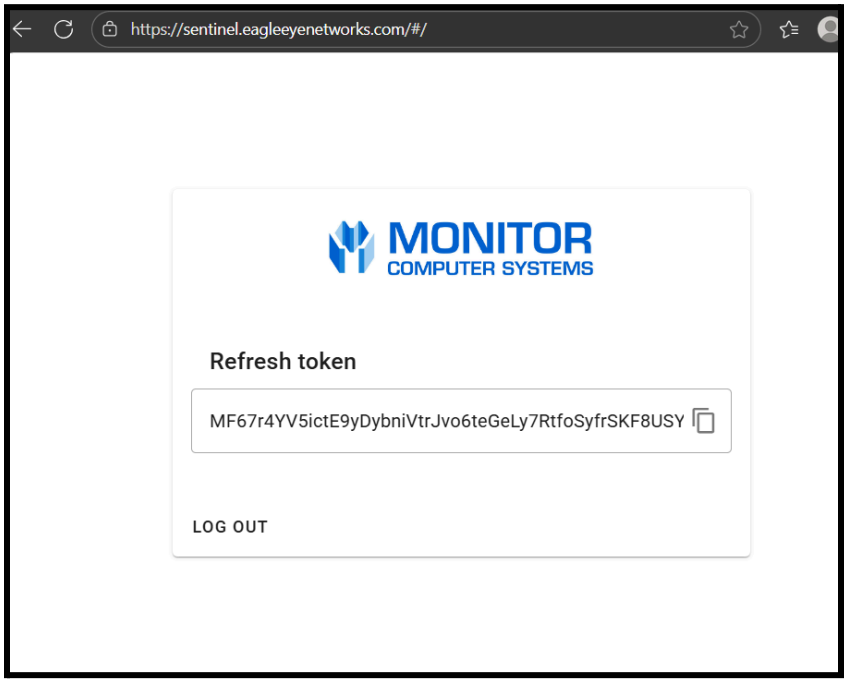
Monitor Computer Systems is an industry leader in remote security monitoring. Typically, Sentinel service providers, Eagle Eye Cloud VMS resellers, and installation technicians are separate entities that need to work together to deploy a site for the end customer properly. If your company handles both integrations for your customers, you will have more say in how sites are deployed in Sentinel; however, if your company uses another vendor for remote services, it is important to discuss the deployment with your counterpart so the sites work together across both platforms.

Getting Started

After the Cloud VMS account is created in Eagle Eye Networks Cloud VMS, and all needed devices are online, the first step is to use an existing user from the account, or create a specific user in the account specifically for the integration to Sentinel (a specific user is recommended for long-term support of the integration). The user must belong to

the sub (end-user) account to be monitored (it cannot be a Reseller-level user; this is not supported). The user should have access to all necessary devices to be monitored, with at least the ability to view and download video. The user, if new, should first make sure they can log in to the Cloud VMS account and that they have created a password for their email address in Cloud VMS. The next step is to obtain an Authorization Token (Refresh token) for Sentinel. This token can be generated by anyone with access to the user's email address and Cloud VMS password.

- Go to: https://sentinel.eagleeyenetworks.com/
- Log in with the specific sub (end-user) account user's email and password to receive a refresh token:

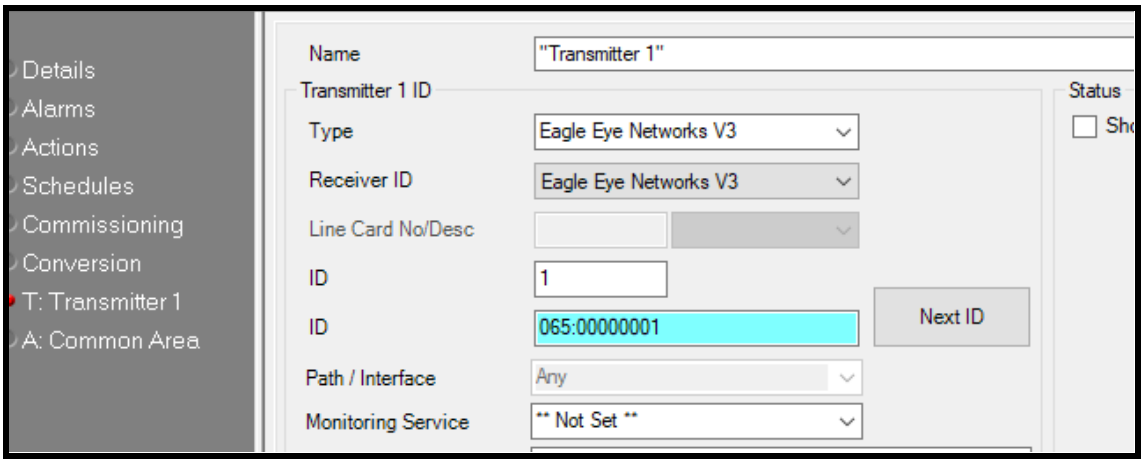


- Copy the token for use in Sentinel (this process can be repeated; the token will not be the same each time, but it will provide the same user access to integrate the needed devices).

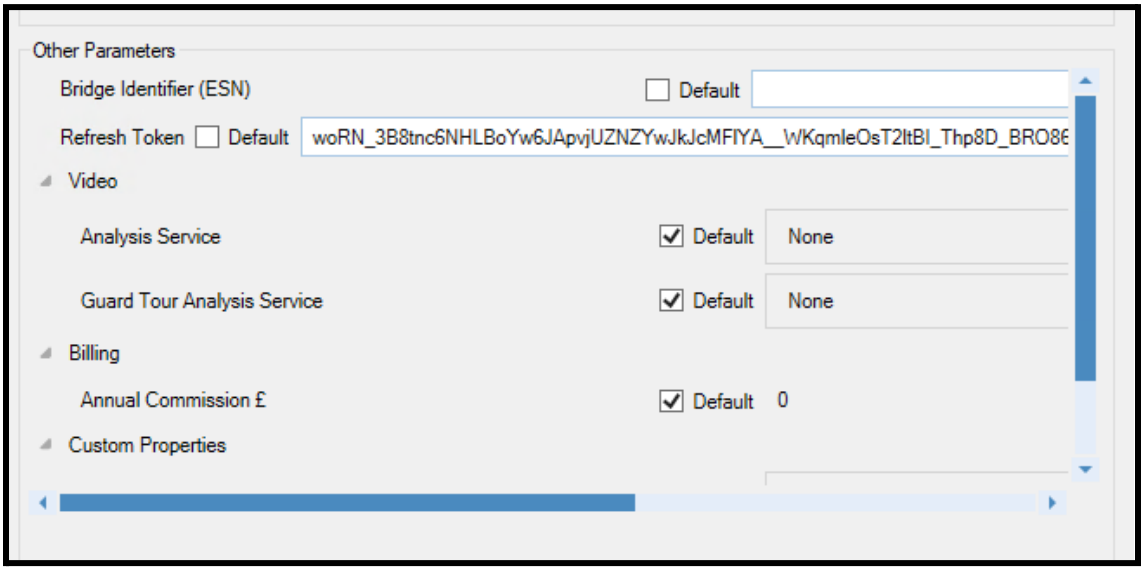
Configuration in Sentinel

This section is intended for persons responsible for account creation and management on the Sentinel platform. This is a truncated version, from the perspective of an Eagle Eye Networks employee, and may not include the full end-to-end steps for Sentinel software, which should be consulted for any real support with the integration of Eagle Eye Networks Cloud VMS into their platform.

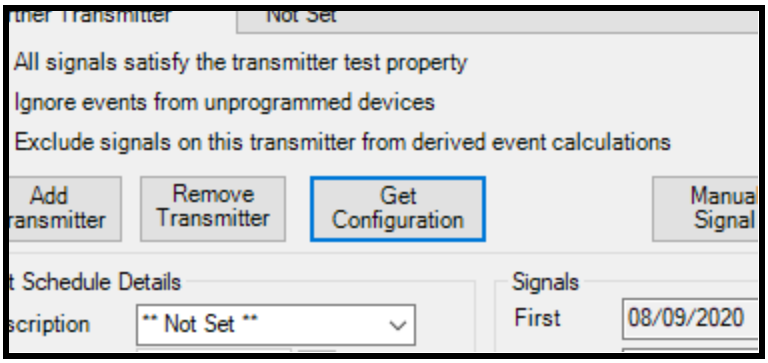
- **Step 1**. In **Sentinel > Customer > Transmitter**, create a **Transmitter** with a name specific to the end user account, and select Eagle Eye Networks V3 as the "Type":



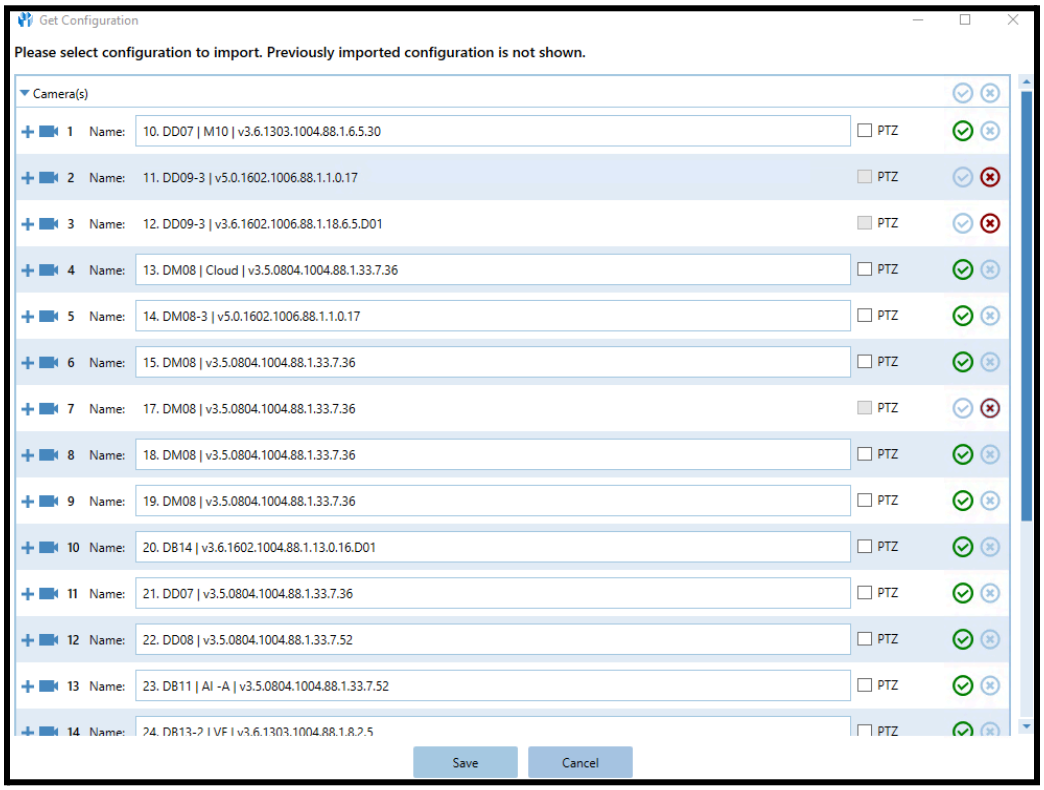
- **Step 2**: In **Other Parameters**, paste the Token that was received at sentinel.eagleeyenetworks.com into the **Refresh Token** field. If there is one or more specific bridges from the VMS account that are needed (to reduce the number of devices imported into Sentinel), enter their ESNs (found in **Cloud VMS > Bridge Settings**) into the **Bridge Identifier** section. Bridges in this case refer to any Eagle Eye Networks Bridge or CMVR device:



- **Step 3**: Click **Get Configuration** to request access to the Eagle Eye Cameras that the user has access to:



- **Step 4**: Once the configuration is fetched, you will receive a popup with the available devices to import, either all from the account or specific bridges that the user has filtered with Bridge Identifiers. Use the selection checks or deselection marks to confirm adding or removing from the import of devices, then select **Save** to continue:



  - **Important Notes About Get Configuration:**
    - The operation performed for Get Configuration in Sentinel is an API call to Eagle Eye Networks for a camera list for the user. It automatically sorts the Camera Inputs in the order of the camera list from the Eagle Eye API.
    - In the example above, I gave my user access to all cameras, which I

purposefully named to call out our API's Lexicographical (alphanumeric) ordering in the Cloud VMS. You can see that, because of this ordering, the device I called "10" in my camera settings is the Highest and appears as camera Name 1 in the Sentinel camera list.
    - Suppose the Cloud VMS account undergoes name changes or cameras are added that affect the alphanumeric value. In that case, Sentinel will not "know" to automatically adjust to these changes for cameras that have already been integrated. It may be possible that, next time a Transmitter is updated for the same Cloud VMS account, duplicated cameras can be imported during the Get Configuration call.
    - Best practice is to inform the Central Station if a camera name has been altered in the Cloud VMS and to manually change the existing camera and alarm Input Names in Sentinel to avoid confusion.

- **Step 5**: Acquire the Sentinel Webhook URL for the Customer Account, needed to finish the integration using Automations in the Cloud VMS Enhanced user interface.
    - The webhook should typically be formatted like: **"http://{sentinelaccountweburl}:{portnumber}/EagleEyeNetworksV3"**

Single Site vs. Multi Site Integration

One Location Monitoring:
With a single site from the Eagle Eye Cloud VMS, where the end customer only needs one physical location enabled for Alarm Monitoring, the site deployment can be done fairly simply by creating a user in the Cloud VMS End User account, which will be used in Sentinel to integrate with the devices that need to generate alerts. This user will need permissions to all the devices, which will generate alerts that need to be monitored.
For simplicity, in either case, the user can have Admin access to the account, and there is no risk of missing permissions. If this does not work for the account for any reason, the user needs, at the very least, the ability to view live video for the specific cameras in the integration.

Multi-Site Monitoring:
If the sub (end-user) account spans multiple sites, the integration might be more complicated to deploy, depending on the Monitoring Center's Alarm Handling requirements. Additionally, the system may need to address time zone dependencies and manage site monitoring schedules when Armed times vary across locations.
Since these requirements can differ between organizations, we can only guide the

process by recommending some configuration options within Sentinel, but the Sentinel onboarding process should follow the Monitoring Center's guidance.

- Users in the Eagle Eye Cloud VMS:
    - Some Monitoring Centers and Cloud VMS Admins have relied in the past on creating specific users in the VMS account who have access only to the segments needed for each site. This can help guarantee that each site will only request specific devices with Get Configuration, and prevent duplicate entries in Sentinel.
    - In our opinion, this option increases deployment difficulty by requiring management of multiple users in Cloud VMS, each of whom must be accounted for and protected, and by requiring understanding of each user's purpose and which sites they are responsible for in Sentinel.

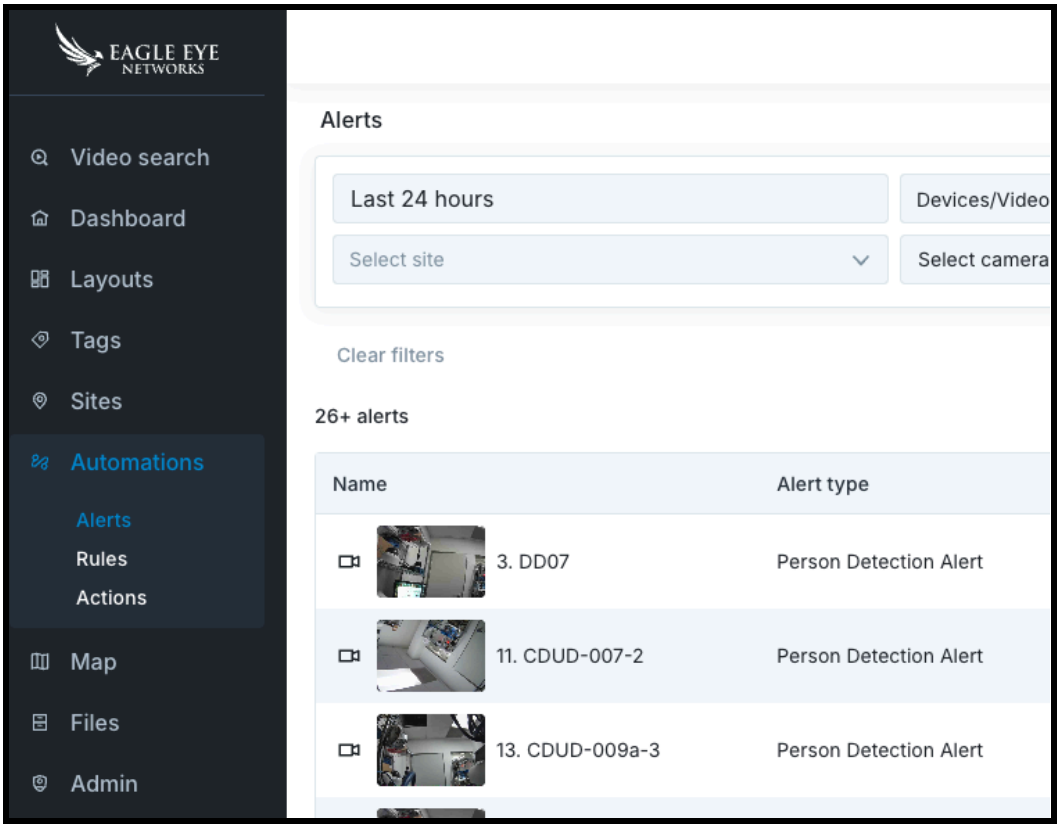
- Bridge Identifiers:
    - This feature is designed to address the need for multiple users in the Cloud VMS account.
    - When adding a Transmitter to the Customer account in Sentinel using the Get Configuration, the Transmitter can target a specific bridge or bridges belonging to the monitored site, and retrieve the necessary cameras from those bridges.
    - Using Bridge IDs is preferred to having multiple users in the account.

Automations - Rules and Actions

The Eagle Eye Networks Cloud VMS Automations feature is specific to the Enhanced Web Interface and enables account users to enable Alert Rules for their devices and control who the alerts go to: Email Notification, Sentinel, other Monitoring software, Webhooks, and more. This feature uses conditional logic and is designed around "if this then that" style enablement. In our case, the "if" statement is called a **Rule**, and the "then" statement is called an **Action**.

The user designated for Sentinel Integration use does not need to be able to create Rules and Actions; these steps can be completed by any user in the account with this access.

Automations Menu
The Automations feature can be accessed in the left-hand menu of the Enhanced Web interface of the Cloud VMS, located at webapp.eagleeyenetworks.com. The user will need Admin permissions to see and create Automations:



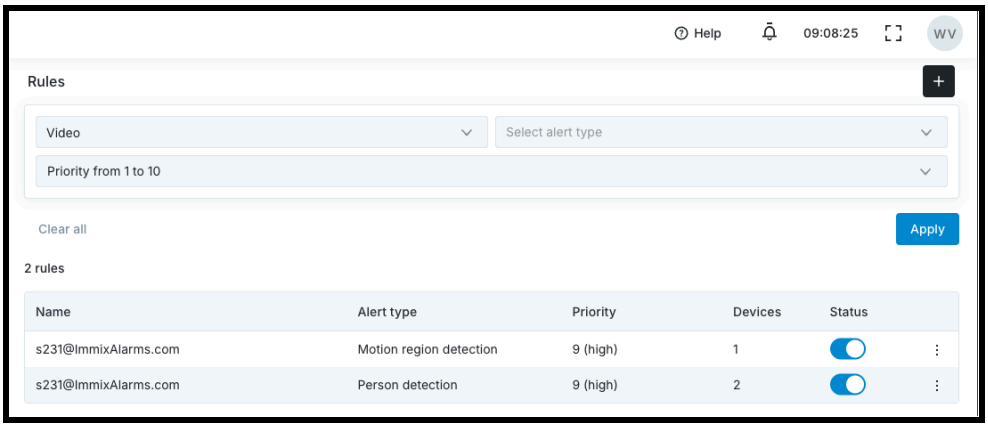
When you first click **Automations**, the **Alerts** page loads, showing alerts generated by created Rules, which can be filtered and sorted by Time, Device, Alert Type, Eagle Eye Site, Camera, and designated Priority.

The Alerts page gives instant insight into confirmation that the camera is generating events, which are being evaluated by the Rules engine, and generating an Alert. It can be used to ensure that the necessary elements in the camera view for sending a notification are functioning, which can help during the setup of the Sentinel site.

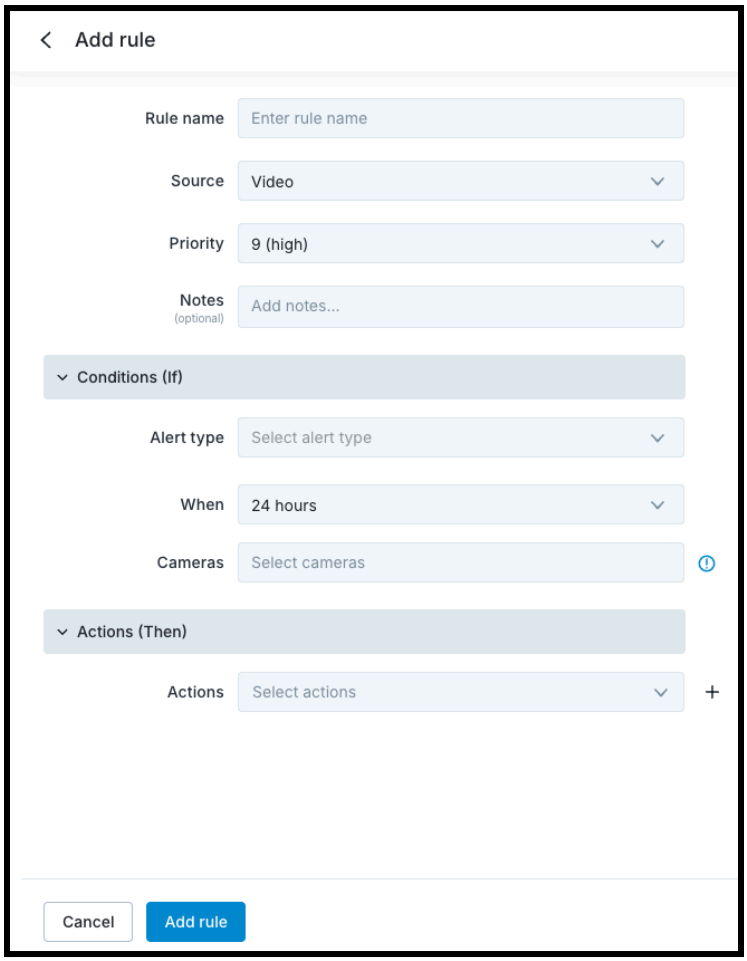
Configuration of Rules

Now that all the cameras are configured for their respective Analytic, they can be placed in a Rule for Alert generation.

- Step 1: Select the **Rules** submenu from **Automations**, then select the “+” icon from the top right of the page:

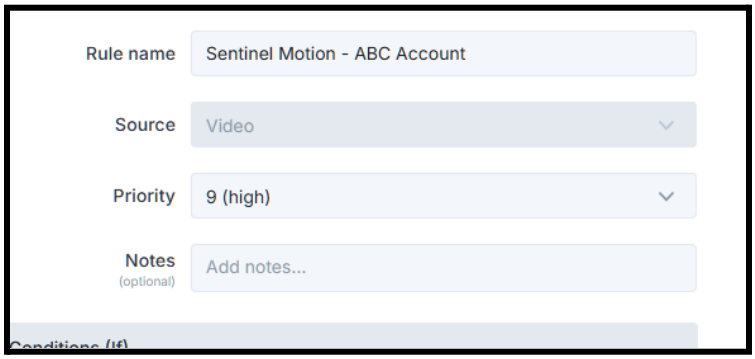


- This opens the **Add Rule** menu:

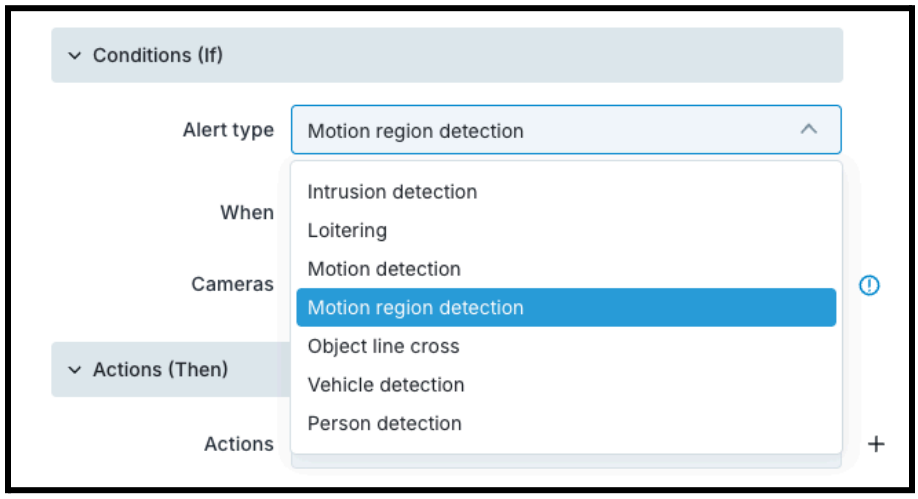


- **Name** the Rule in such a way that it is instantly recognizable as associated with Sentinel, aligns with the Transmitter the rule is being created for, and, for even more specificity, include details of the Alarm Type you will be including for the Action.
- The **Source** for Video alarms is the default option, and what you will use.

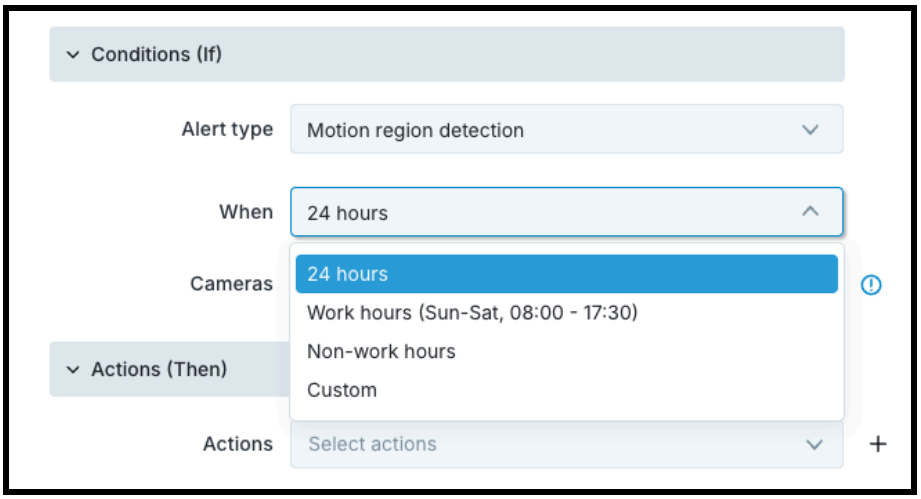
- The **Priority** is self-assigned. This can be a way to track in the account the perceived "value" of the alert. Think of it as a way to filter alert types, where a low-priority alert is something that happens that does not need immediate action. A high-priority alert is something that would involve a response from Sentinel. There is no difference in alert delivery; this is a sorting feature only.
- **Notes** are also self-assigned for Account needs or to provide additional context on why the rule exists.



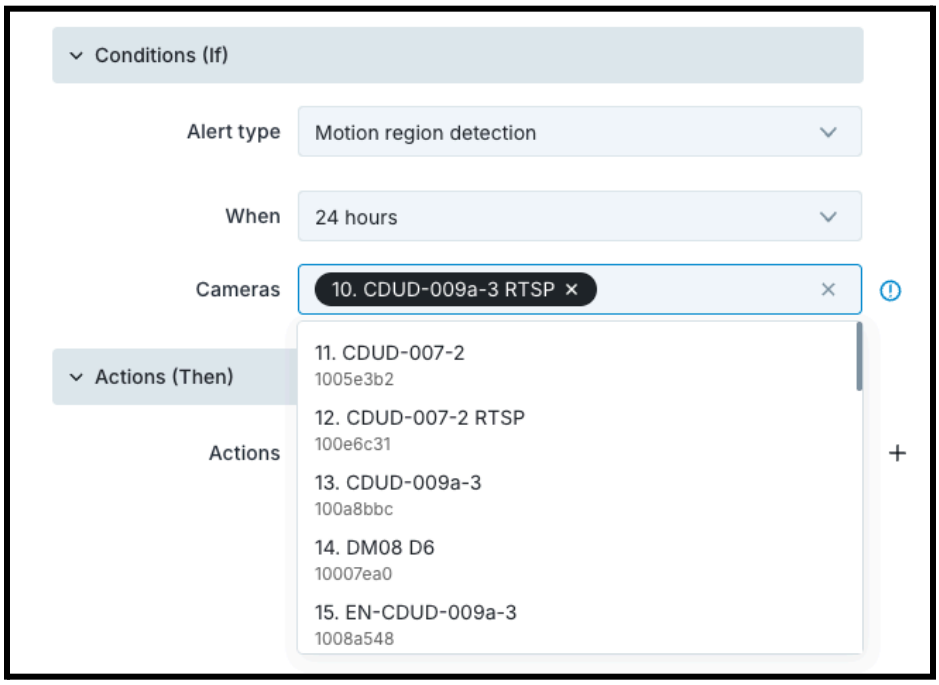
- The **Conditions (If)** are the essential part of the Rule, starting with **Alert Type**. Currently, only **One Alert Type** can be configured at a time. This means that if your Monitored Site needs to receive a mix of Motion Alarms, bridge analytics, and Person or Vehicle Alarms, you must create separate rules for each.



- **When** allows for a schedule of Alert Times to be followed. Times can be always, during, or after work hours for the account, or have a custom schedule. Many monitoring centers will charge per Alarm received, so it is important in these cases to make sure your Alert Times are only set for when the Monitoring Center is expecting them to occur:



- **Cameras** allow for searching for and adding a camera or cameras that contain the configured settings to follow the specific Alert Type, for this Rule, and the preceding Action:



Configuration of Alerts

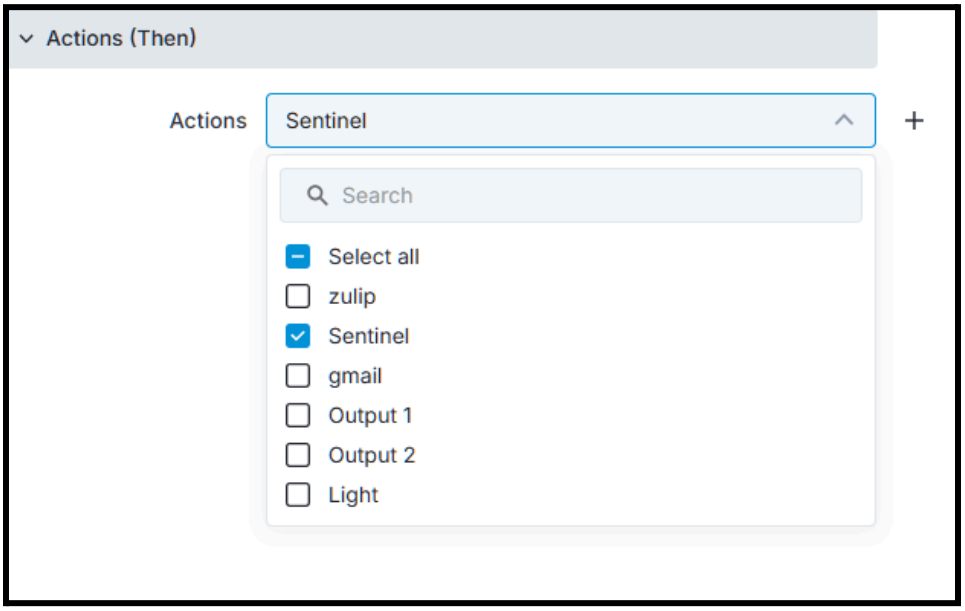
Once the Site is deployed to Sentinel, and ready to receive alarms, take the webhook URL for the account (provided by Sentinel and typically "**http://{sentinelaccountweburl}:{portnumber}/EagleEyeNetworksV3**"), and use it in the creation of the Action. At the time of this Application note, "https" is not supported in Cloud VMS.

Actions can be created before the Rule or at the same time as making the Rule.

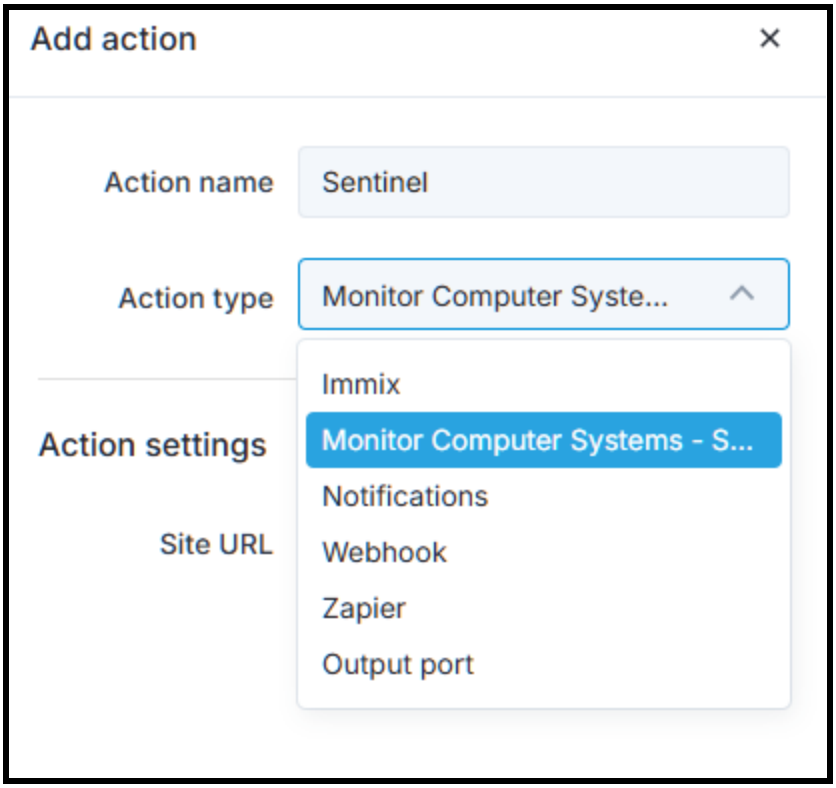
Rules can contain multiple Actions. For example, an end user of the account would also like to receive the same alerts that Sentinel processes. In that case, there can be an Action for Sentinel and an action for Email Notifications for the user, both applied to the same Rule.

Note: A single Action can be attached to multiple Rules, so it may be easier to create the Actions before the Rules, and apply them to the Rules during the setup.

- From the Rule, under Actions (Then), use the drop-down to select the Action or Actions to apply to the Rule:



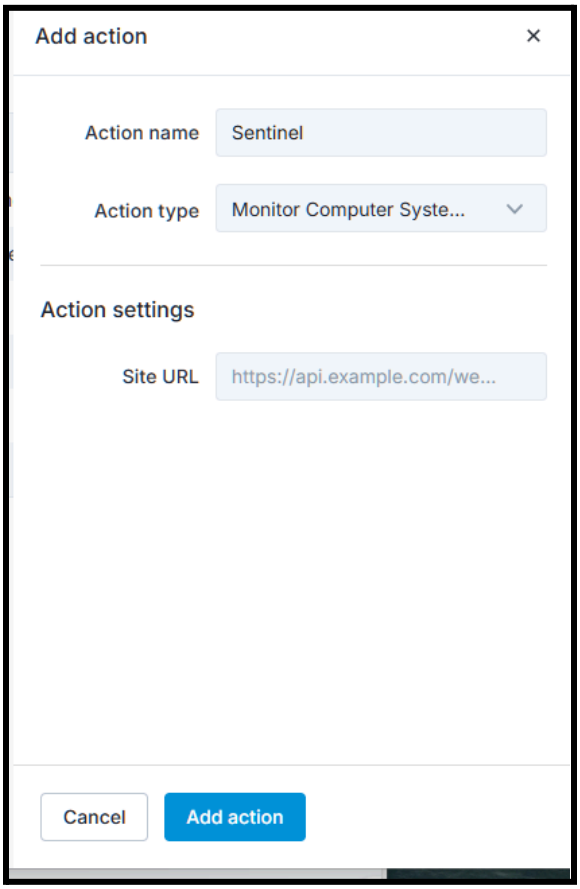
- If no Action is created yet for this Rule, then select the "+" icon to the right of the Action drop-down to create the Action:



- Alternatively, before Rule creation, go to the Actions submenu from Automations, and create Actions to be available for Rules by clicking the “+” button on the top right:

- Creating an Action is the same no matter where you begin. For Action Type, select “Monitor Computer Systems - Sentinel” from the options. Input the webhook into

the Site URL box, and click **Add Action** to save.



Validation and Troubleshooting

Validation

Now that Rules and Actions have been created to send Alarm messages to Sentinel, and the Sentinel Sites have been created and configured to receive them, the deployment should be functioning as needed. The next step is to coordinate a site walk for validation.

Note: Validation should be conducted by both the installer and Alarm Monitoring administrator/operators.

As with any professionally monitored surveillance solution, it is important to test that alarms and videos are being received properly before arming a site for monitoring. The installer, after ensuring the site is placed on test within the Sentinel platform, should intentionally trigger all configured motion and analytic alerts and confirm receipt by the monitoring center.

It may be necessary to temporarily adjust the schedules for motion and analytics Rules if these tests are conducted outside the configured schedules. Another option could be to temporarily create a Test Rule armed for 24 hours, which can have the Actions for the site set. This Rule should be deleted or disabled after confirmation.
The Sentinel administrator or operator should place the site in test mode, open the test, and ensure all alarms are received with attached pre-alarm clips, post-alarm clips, and a working live view. Once confirmed, the integrated site is ready to be armed for ongoing monitoring within Sentinel.

Troubleshooting

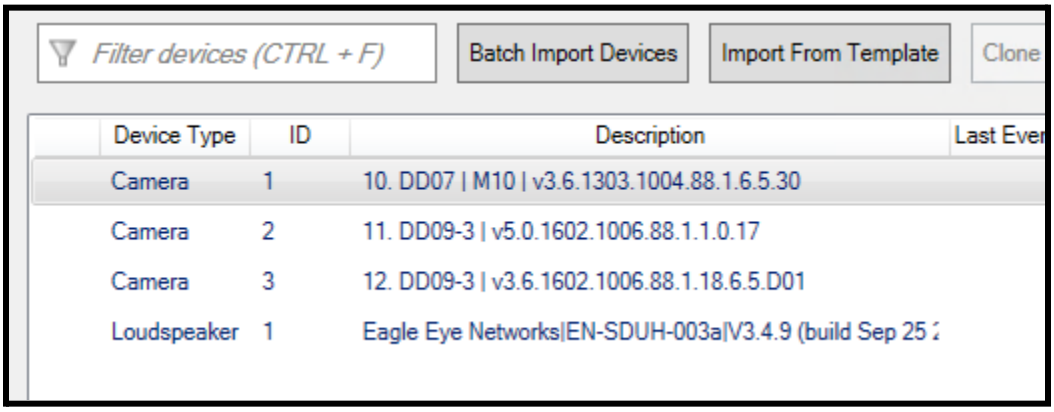
Common Issues:

- **No detection events for the Rule**: Verify that the needed Analytics for the Rule are enabled on the camera, and verify that the Rule's schedule is currently enabled to send alerts
- **False positives**: Adjust sensitivity settings and refine detection zones to reduce unwanted triggers
- **Poor detection accuracy**: Check lighting conditions, camera positioning, and contrast levels
- **Sentinel is not receiving Alarms, even though the Eagle Eye Automations page shows that Alerts are being generated.** This may need assistance from Sentinel to verify settings, but Eagle Eye installers can verify a few things.
    - **Confirm Saved Action:** Verify that the **WebUrl** and **Port** are saved correctly.
    - **Test Port listening:** Use Telnet to confirm the port that Sentinel provided is actively listening. If the Telnet connection fails, Sentinel will need to verify that the server listening port is correct/ active.
    - Confirm with Sentinel that the cameras saved to the Rule are the same as those saved to the Sentinel Site.

Uncommon Issues:

- **Sentinel Duplicate Entries:**
  As mentioned earlier in this document, the Sentinel Integration to Eagle Eye Networks is driven at the API level (which significantly eases deployment compared to on-premises devices requiring manual import); however, it is not always foolproof.
  In the example below, I will show how changing camera names in the Cloud VMS can reorder the device inputs retrieved by the Sentinel Get Configuration, and how this may affect an account reconfiguring devices in Sentinel.

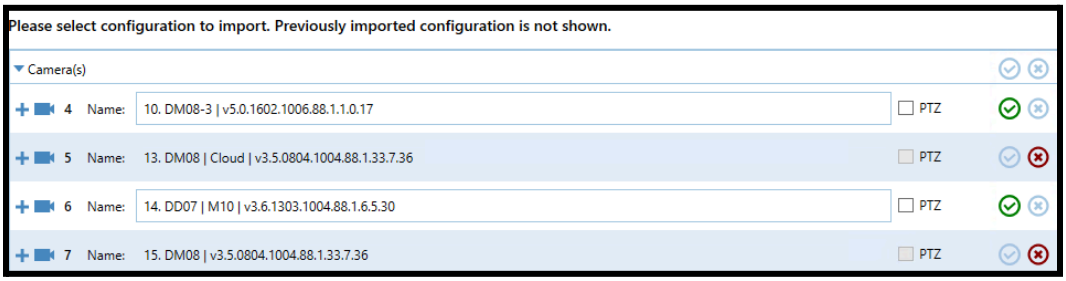
- In Sentinel, I Get Configuration for my account, and import the first 3 cameras in the alphanumeric order from the API:



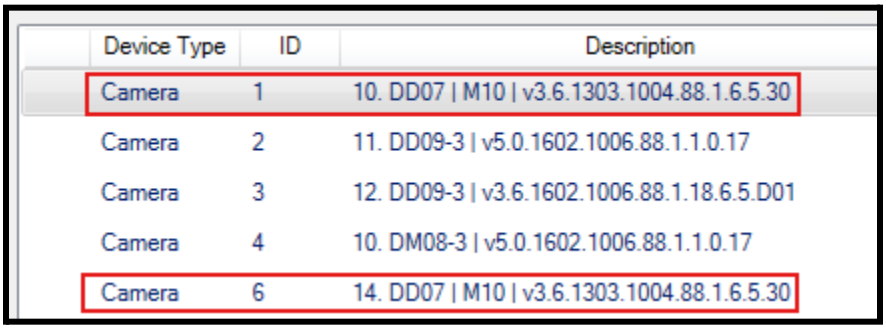
- Now I go into the Cloud VMS and purposefully change my 1st camera name “10” in the account to be the same alphanumeric value as a previously lower value camera “14”, and change my “13” camera to be “10” value:

- Suppose I perform the Get Configuration again for the Transmitter, in an example of an end-user account growing in size and needing additional cameras from the site being monitored. In that case, Sentinel will return the next available Camera Name (4); however, since my camera that was Input value 1, now has an alphanumeric value of the previous 6th camera, and it becomes available again to attach to the transmitter:

New Configuration:



- Now I have a Duplicated Camera in my Sentinel Transmitter settings, and you can see that the Sentinel service does not change the Name value of previously added devices:



Device Type	ID	Description
Camera	1	10. DD07 | M10 | v3.6.1303.1004.88.1.6.5.30
Camera	2	11. DD09-3 | v5.0.1602.1006.88.1.1.0.17
Camera	3	12. DD09-3 | v3.6.1602.1006.88.1.18.6.5.D01
Camera	4	10. DM08-3 | v5.0.1602.1006.88.1.1.0.17
Camera	6	14. DD07 | M10 | v3.6.1303.1004.88.1.6.5.30

- Alarms for duplicated Cameras may confuse the Alarm Handler, and updated Camera Names for the Client vs. what the Monitoring Center knows the camera name to be can lead to further confusion if an Active alarm needs to be escalated to the Site Staff. To limit these issues, it is important to work together with the Monitoring Center team on updates, and additions to a monitored VMS account.

Further Support

Eagle Eye Support is available 24×7 at support@een.com or support.een.com for global phone numbers

Sentinel Support https://www.monitor.uk/contact.html

https://docs.monitor.uk/sentinel/administrator-guide/signalling/cctv-and-audio-systems/eagle-eye-networks-v3#supported-alarms-events