

Eagle Eye Application Note - AN042

Configuring The Eagle Eye VMS and Immix Integration for Alarm Monitoring

2024-12-27 Revision 3.0

Target Audience

This document is intended for both installers and administrators of Eagle Eye Networks Cloud VMS that are interested in doing professional monitoring of Eagle Eye Networks generated video events through an Immix-supported central station.

Introduction

The Immix platform consists of a suite of central station monitoring software that integrates with a wide variety of video systems and provides monitoring center operators a convenient way to conduct their event-based workflow.

As a cloud-based VMS platform, Eagle Eye Cloud VMS provides convenient and secure remote access to cameras and alerts, making it well suited to surveillance deployments that require professional monitoring, especially when paired with a monitoring station running the Immix suite of software.

At present, the Eagle Eye Networks Immix integration supports the following features:

- **Get config** - A simple process within Immix allows operators to update all available devices from the Eagle Eye Cloud VMS.
- **Live Video** - Live video streams from cameras attached to the Eagle Eye Cloud VMS can be viewed within the Immix platform.
- **Playback** - Recorded video from cameras attached to the Eagle Eye Cloud VMS can be viewed within the Immix platform.
- **PTZ** - Control pan, tilt, and zoom for attached PTZ-capable cameras.
- **Presets** - Apply any pre-configured pan, tilt, zoom setting.
- **Multiview** - Multiple cameras attached to the Eagle Eye Cloud VMS can be viewed simultaneously within the Immix platform.
- **Alarms** - Triggers based on motion, or the Eagle Eye Cloud VMS analytics including line-crossing, intrusion, and loitering can be presented in the Immix platform.

- **Attached clips** - Video clips (images) of an alarm-triggering event will be attached to the alarm and stored within the Immix platform.
- **Post-Alarm Recording** - The Immix platform will record the live view from a camera triggering an alarm for review within the Immix platform.
- **Pre-Alarm recording** - Pre-recorded (buffered) video will be available to the monitoring center, highlighting activity recorded immediately prior to the event.
- **Audio Receive** - Receive audio from any microphone-equipped camera on site.

Suggested Configuration Process

Given that the administration of Eagle Eye Cloud VMS and Immix often fall under the purview of two distinct parties—the installer, and the monitoring center administrator—this document delineates actions for each system. If such a division exists, there will be instances during the process where specific information must be exchanged between the parties for a seamless workflow. These critical junctures are highlighted at each step.

We would suggest the configuration actions are conducted in the following order:

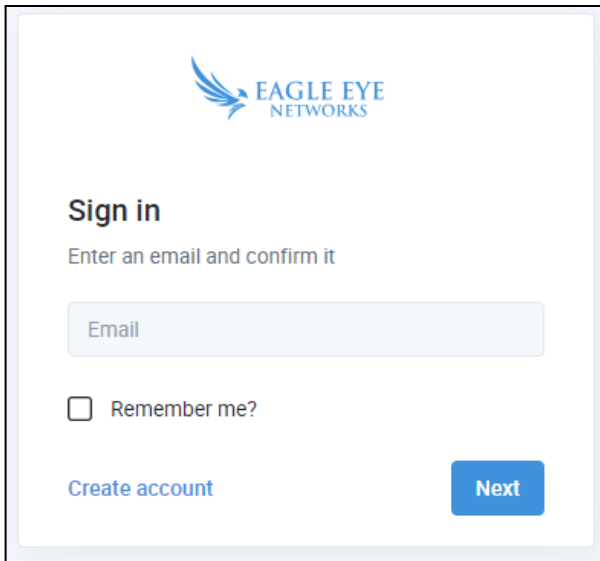
1. Preparation of the Eagle Eye Cloud VMS for addition to Immix by the installer
2. Addition of the Cloud VMS to the Immix platform by the Immix administrator
3. Configuration of Alerts within the Cloud VMS by the installer
4. System testing by both parties

1. Preparation of the Eagle Eye Networks System for Addition to Immix

The following steps are to be completed by an Eagle Eye Cloud VMS administrator from the installer. The Eagle Eye Immix integration needs to be enabled on a sub-account level prior to conducting the integration. Please contact support@een.com detailing the name of the sub-account (or customer account) that is to be added to an Immix system. Once integration has been enabled by Eagle Eye Networks, the Immix-specific settings detailed later in this document will be available in the Eagle Eye Cloud VMS web interface.

For the next step, It will also be necessary to generate a “refresh token” for the sub-account and pass this to the Immix administrator. A refresh token is a credential artifact that lets a client application get new access tokens without having to ask the user to log in again. If a customer has enabled two-factor authentication (2FA) on the VMS, the refresh token can be still used by applications like Immix to connect to the VMS without invoking 2FA.

This token can be generated through the following web page <https://immix.eagleeyenetworks.com/>



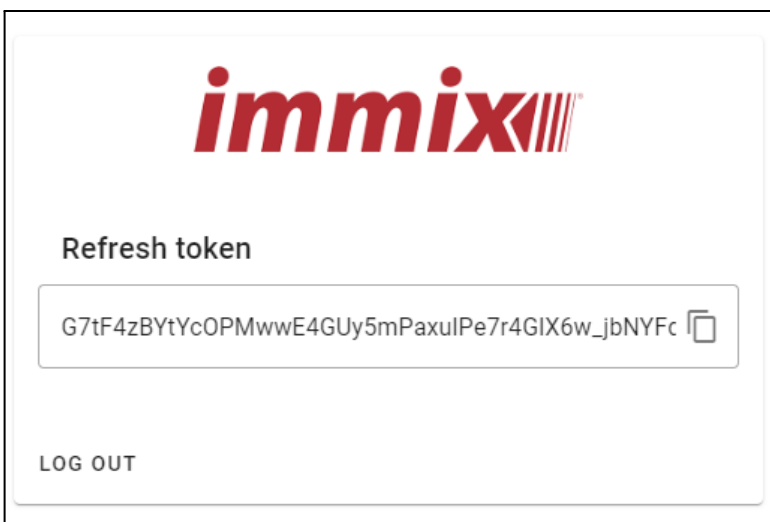
The image shows a sign-in form for Eagle Eye Networks. At the top left is the Eagle Eye Networks logo, which consists of a stylized blue eagle head icon followed by the text "EAGLE EYE NETWORKS". Below the logo is the heading "Sign in" in bold black text. Underneath the heading is the instruction "Enter an email and confirm it". There is a light blue input field with the placeholder text "Email". Below the input field is a checkbox labeled "Remember me?". At the bottom left of the form is a blue link that says "Create account". At the bottom right is a blue button with the text "Next".

You will be asked to enter the credentials for a Cloud VMS user account. **It is important to enter a user from the customer specific “sub-account,”** and not a user from the parent “reseller account.” Should you need to create a new sub-account level user for the integration, multiple accounts can be created for a single email address by using the “+” suffix when creating the account.

For example:

If your existing account uses the email address admin@Reseller.com, an additional account tied to the same email address could be created using admin+SubAccountID@Reseller.com

Once the email and password for a sub-account level user have been entered, a refresh token will be generated and can be copied to your clipboard using the button shown below. Save this token as it will need to be provided to the Immix administrator for the next step.



The image shows a screen from the Immix application. At the top center is the Immix logo, which is the word "immix" in a bold, red, italicized sans-serif font, followed by four vertical red bars of varying heights. Below the logo is the heading "Refresh token" in bold black text. Underneath the heading is a light gray input field containing a long alphanumeric string: "G7tF4zBYtYcOPMwwE4GUy5mPaxulPe7r4GIX6w_jbNYFc". To the right of the string is a small icon of a document with a checkmark, indicating a copy-to-clipboard function. At the bottom left of the screen is a link that says "LOG OUT".

Information to be passed to the Immix administrator for Step 2.

- The refresh token is generated in this step.

- A list of the camera names to be added to Immix, important if only a subset of the cameras in the sub-account are to be monitored by the Immix system.

2. Addition of System to Immix Platform

The following steps are to be conducted by an Immix administrator at the monitoring center.

Once in receipt of the information listed in the previous step from the installer, you may add the Eagle Eye Cloud VMS deployment to your Immix system. We recommend that the updates section of your Immix system is checked prior to proceeding, to ensure the latest integration package for Eagle Eye Networks is installed on your instance of Immix.

Add a new “video device” to either a newly created site or to a pre-existing one, using the details below and those provided by the installer.

EDIT DEVICES FOR: HQ AUSTIN 2

Devices > Cameras > Multiviews > Splits > Tours > Audios > Relays > Alarms > Alarm Groups > Summary

DEVICE DETAILS

Device Type Filter

- Video Devices
- Alarm Panel
- Access Control
- Show All

Device Type

Eagle Eye VMS

Title

Eagle Eye VMS

CONNECTION DETAILS

Used to connect to the device for monitoring. Obtain these details from the person who installed the device.

Connection details are configured via the UAC setup page.

IP/Host

Can be left blank

Port

Can be left blank

Ports must only contain numeric values.

Username

Can be left blank

Password

Can be left blank

Refresh Token

ZPNLV5v_4T8qnlF3QxHG9skQld7EjHelXXU9mbZalMXD34KOoneeXG

OAuth Eagle Eye Refresh Token

Bridge IDs

Can be left blank

Filter cameras linked to specified bridges

Camera Names

DETECT DEVICE CONFIGURATION

GET CONFIG

DONE CANCEL

fields marked with * are required

Device Type: Eagle Eye VMS

IP/Host: Can be left blank

Port: Can be left blank

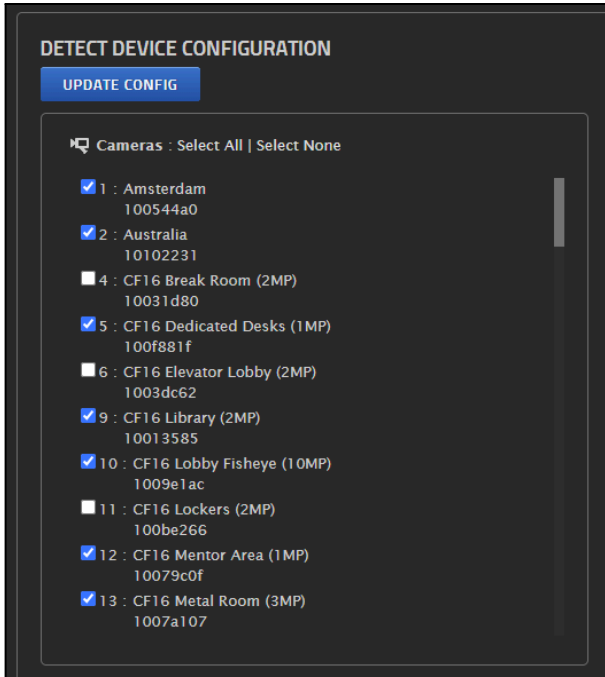
Username: Can be left blank

Password: Can be left blank

Refresh Token: Token provided by installer (this is the only information required to onboard a location to Immix)

Bridge IDs: Can be left blank, if all bridges from the account are needed. If not, add the Bridge/CMVR ESN. If multiple, the esn's must be separated by a comma. (Device ESN available in VMS by looking at Bridge settings)(Requires Immix update 1.0.0.8 for Eagle Eye VMS)

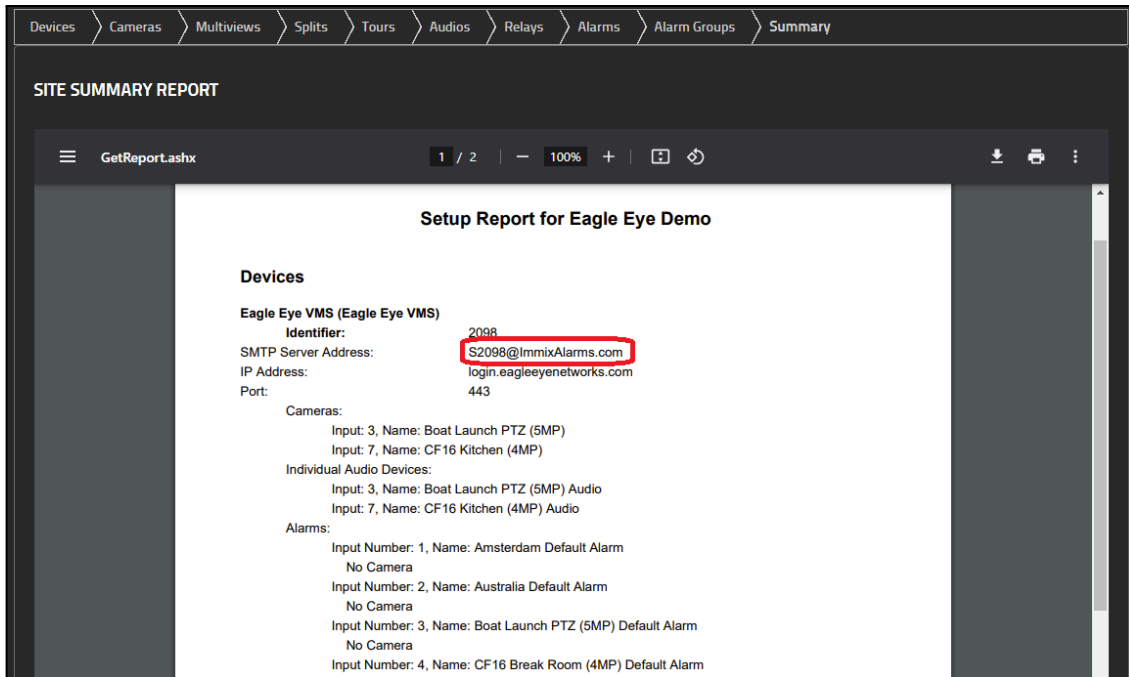
Next, click "Get Config" to retrieve a list of available cameras and audio devices to add to the Immix site. If only a subset of cameras are to be added, untick the cameras and alarm devices not required.



The "cameras," "multiviews," "splits," "tours," "audios," "relays," and "alarms" sections can be left at default values, or configured in the usual manner for your typical deployments.

It is not necessary to create custom settings for each of the types of alarm a camera can present to Immix; the SMTP alarms sent from Eagle Eye Networks into Immix will contain information to identify their type (e.g. motion, intrusion, etc.). However, if you want to set differing priorities, actions or scripts for these alarms, you will need to configure them as usual in the "alarms" interface.

Once a site is configured to your requirements, please take note of the "SMTP server address" from the site's summary page (usually taking the form of SXXX@immixalarms.com), as it will be required by the installer for the next step.

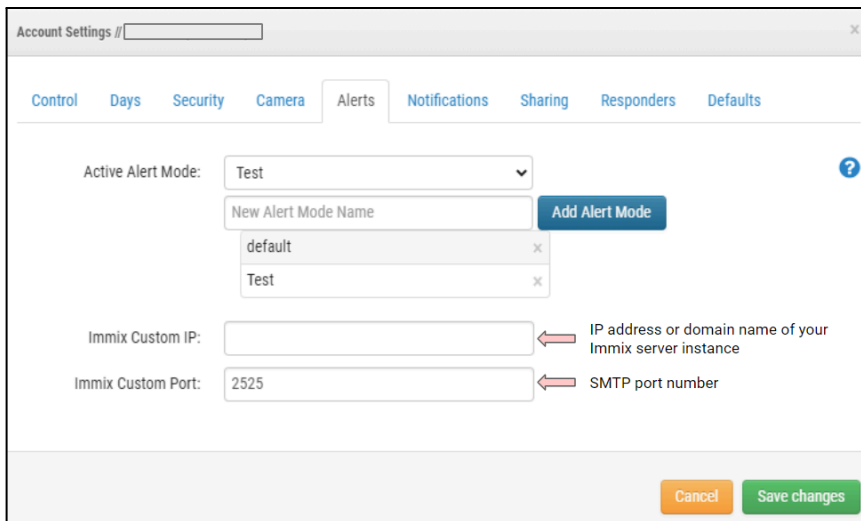


Information to be passed to the Eagle Eye Networks administrator for Step 3.

- Immix Custom IP: The domain name or public IP of your Immix Server.
- Immix Custom Port: The port on which your Immix Server is listening for alerts.
- SMTP Server Address: The email address generated in the site summary.

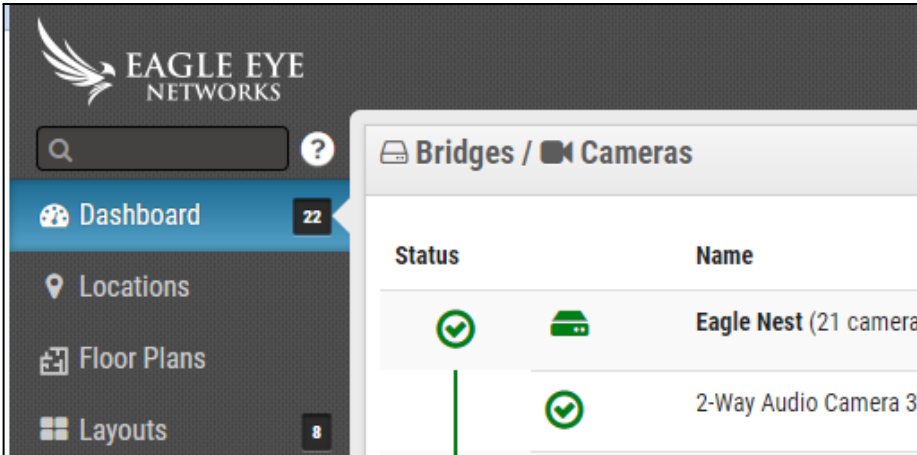
3. Configuration of Alerts Within Eagle Eye Cloud VMS

The following steps are to be completed by an admin user of the Eagle Eye Networks Cloud VMS. Once Immix integration has been enabled for the sub-account by Eagle Eye Networks' support teams (as described in Step 1), some additional fields will become available in the "alerts" tab of the "account settings" for the sub-account. Complete the fields "Immix custom IP" and "Immix custom port" with the information provided by the Immix administrator in the previous step.

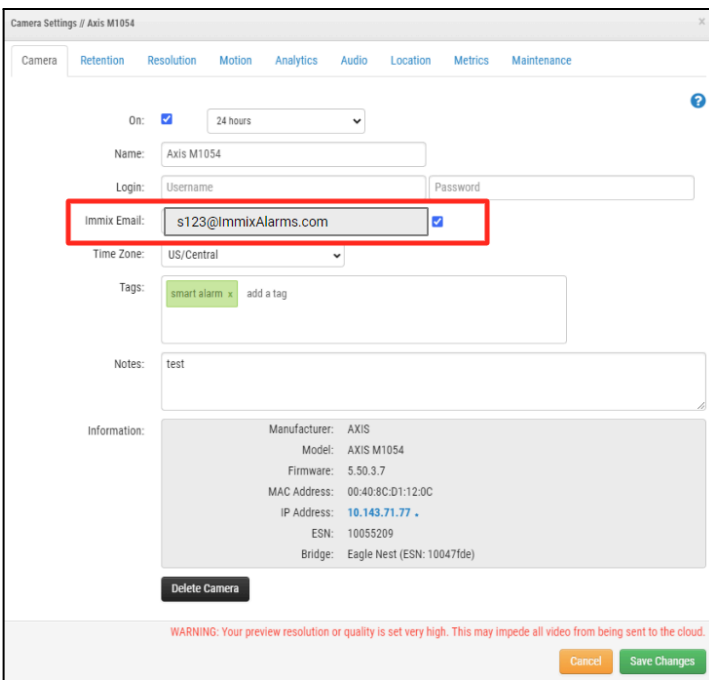


Additionally, for each camera that is to send motion or analytics alerts to Immix, enter the "SMTP Server Address" provided by the Immix administrator into the "Camera" tab of the camera's settings, accessed by clicking the gear icon from the Cloud VMS dashboard.

Go to the Camera Settings from the dashboard



Click on the gearbox for the camera you want to select



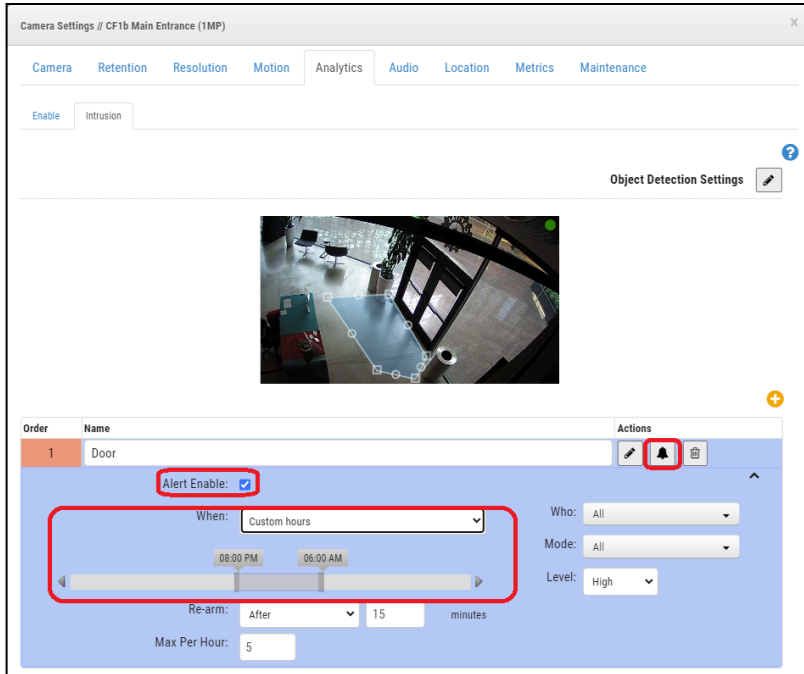
In this example, any alerts that involve this camera will be passed to your Immix system, and an email will be sent from the Eagle Eye Cloud VMS to s123@ImmixAlarms.com. This includes Motion, Intrusion, Line Crossing and Loitering alerts.

Next, either motion or analytics should be configured on the cameras that are to connect with Immix. Guides to this process can be found at the following links:

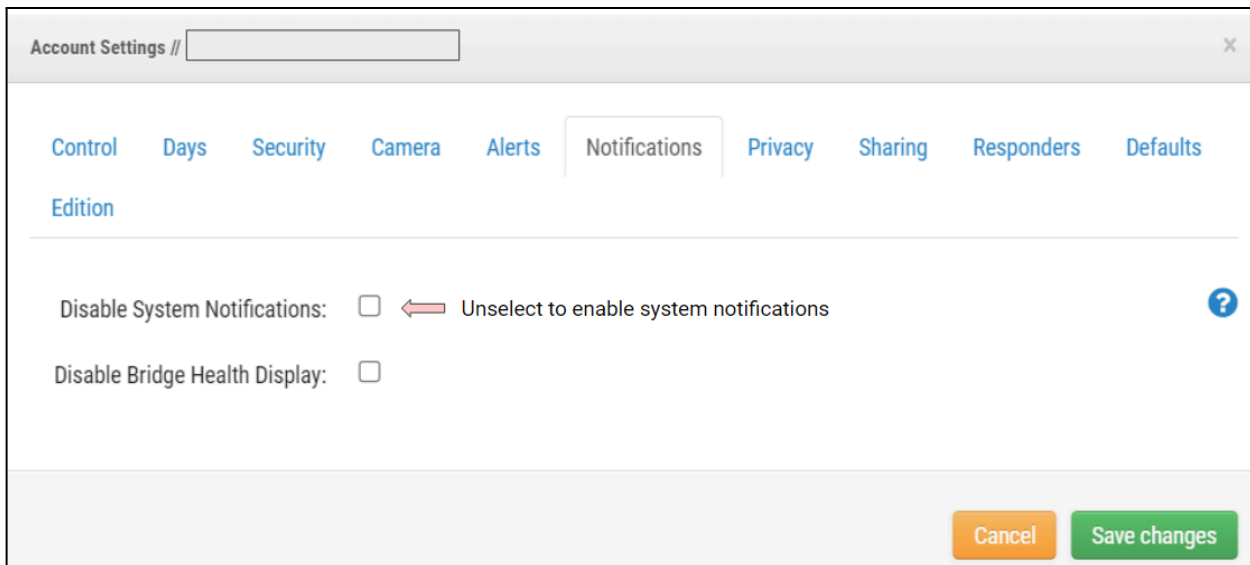
- [Blog on Adjusting Motion Settings](#)

- [Application Note on Eagle Eye VMS Analytics](#)

It is important to ensure that the “Alert Enable” checkbox is selected and an appropriate schedule is set from the notification settings for each analytic or motion zone enabled, as shown below:



It is also possible to forward system notifications for health events concerning the added cameras to the Immix system. To enable this functionality, ensure the “Disable System Notifications” checkbox in the notification tab of the account settings is unticked.



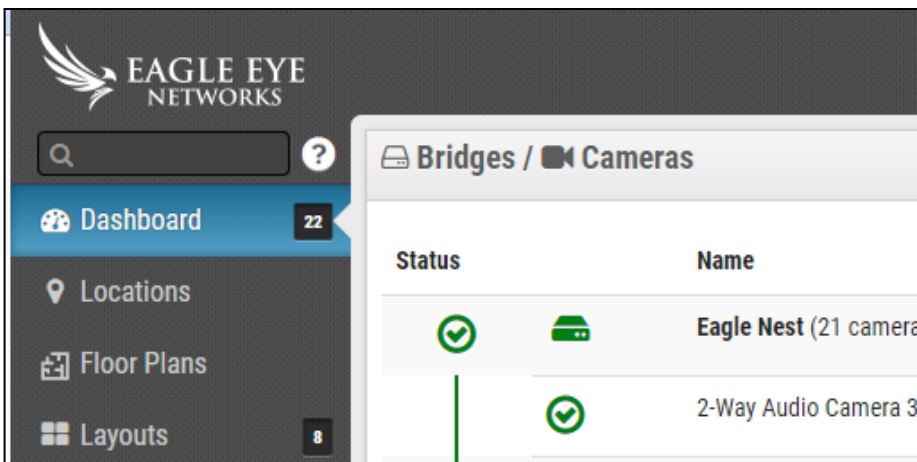
With this unticked, any health notifications concerning the cameras attached to Immix will be automatically sent to the Immix system. With these steps complete, any configured motion, analytic or health events should now be sent via SMTP to the Immix platform.

4. Configuration of Eagle Eye AI Alert Filtering in Cloud VMS

The following steps are to be completed by an admin user of the Eagle Eye Networks Cloud VMS. Eagle Eye Networks AI Alert Filtering needs to be enabled on a sub-account level prior to conducting the next steps. It would be advisable to have this done at the same time as the Immix integration enablement described in Step 1. Eagle Eye Networks AI Alert Filtering is a per-camera addition to the camera subscription. Please contact your Eagle Eye Networks sales team or sales@een.com to discuss the cost for enabling this feature on the camera.

Once Immix integration and AI Filtering has been enabled for the sub-account by Eagle Eye Networks' support teams, the sub-account can be configured to use Eagle Eye Networks AI Alert Filtering, in place of or in addition to the Alerts settings from Step 3. Eagle Eye Networks AI Alert Filtering allows for false alarm reduction to Immix, by isolating the alerts generated by the camera to only "Person" or "Vehicle" (or both) events, instead of any motion detected by the camera.

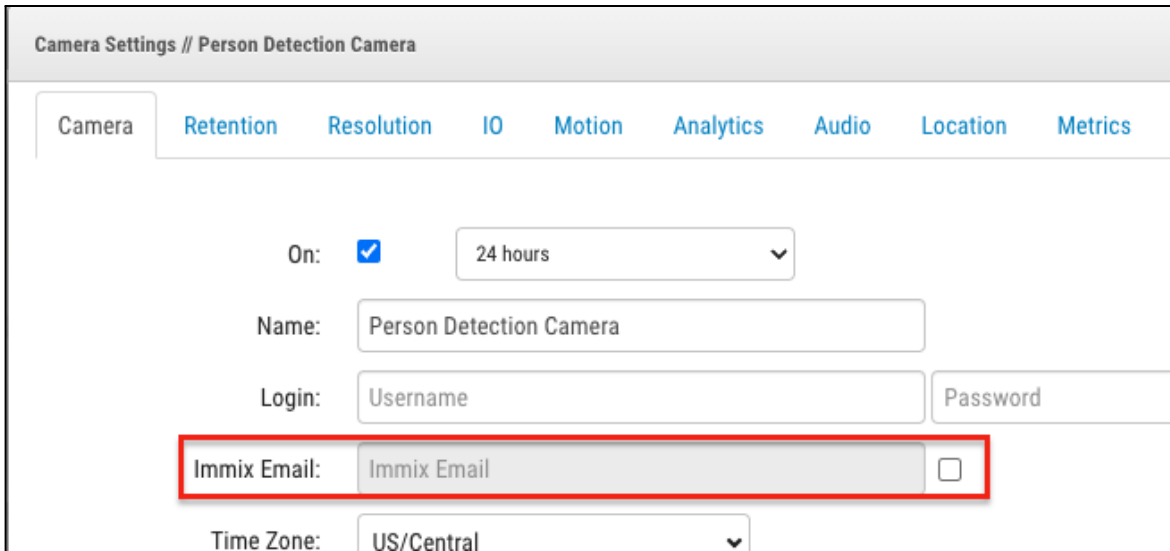
Go to the Camera Settings from the dashboard



Click on the gearbox for the camera you want to select

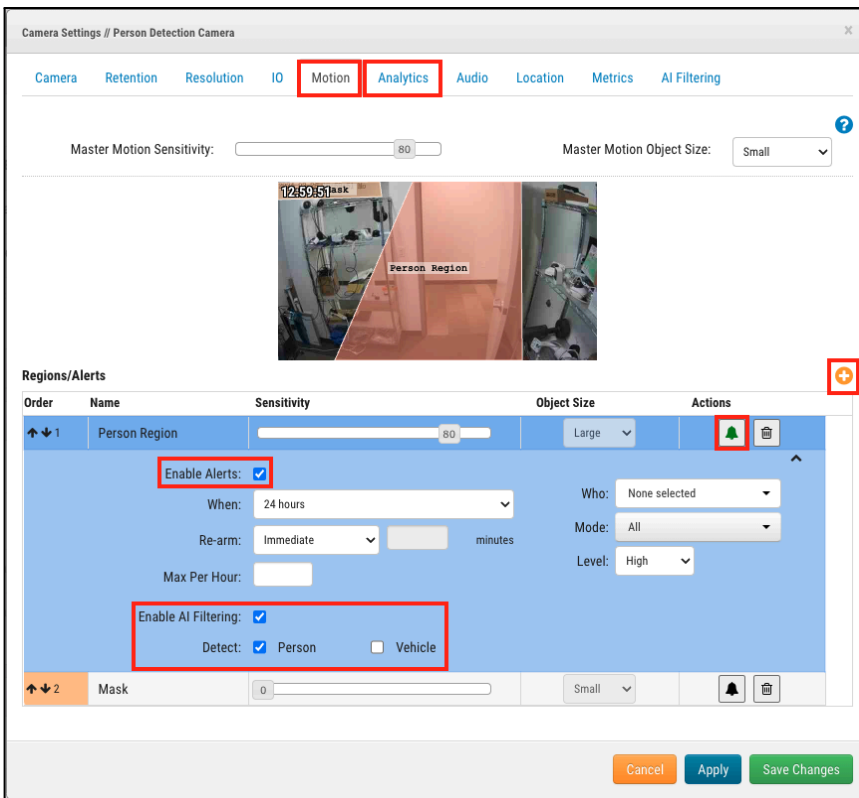


Using AI Filter allows you to leave this Immix Email empty; the email will be used in the next steps. Keep the Immix Email here to receive Alerts that do not include "Person" or "Vehicle" AI Filters.



To enable AI Filtering, navigate to either the Motion or Analytics tab in the Camera settings. Guides to this process can be found at the following links:

- [Blog on Adjusting Motion Settings](#)
- [Application Note on Eagle Eye VMS Analytics](#)

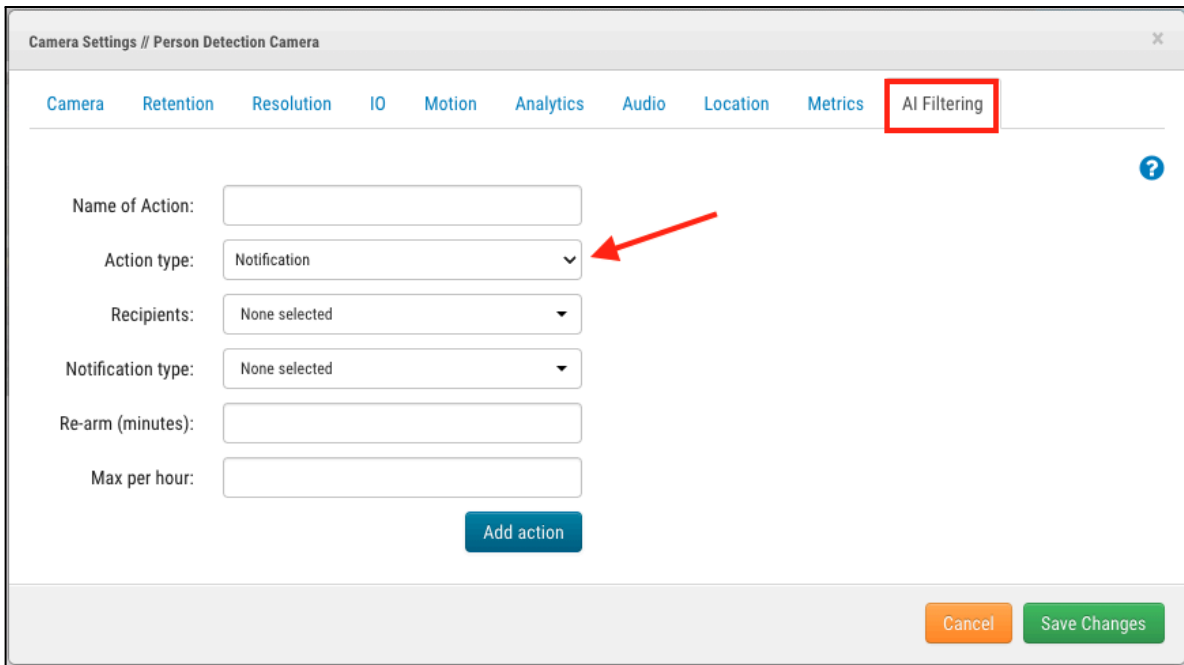


Once you have created a Region of Interest (ROI) where the camera needs to detect people, vehicles, or both (the ROI can encompass the entire field of view if needed), make sure to check the “Enable Alerts” checkbox, and enable the “AI Filtering” checkbox and checkboxes for whichever item needs to

be detected. Using this feature does not require additional settings for Re-Arm, or Max per hour, and you do not need to select a person to notify from the Who dropdown, or change the Level. When utilizing an Analytic for the camera, i.e. "Line Cross" or "Intrusion," it is necessary to have a Motion ROI set for the same region as the Analytic.

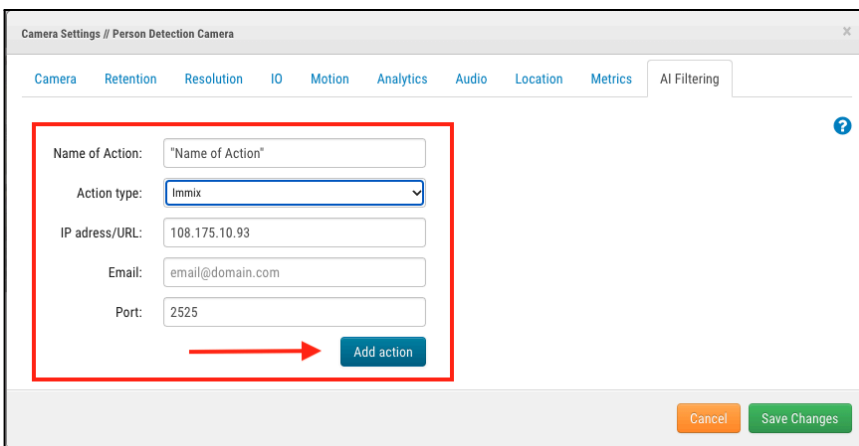
Once these settings are confirmed, you can navigate to the AI Filtering tab from the camera's settings.

Select the Action Type dropdown and select "Immix."



Name the Action and complete the fields for "Immix custom IP" "Immix custom port" and "Email" (SMTP Server Email) provided by the Immix administrator in the previous steps.

Make sure to click the "Add Action" button before clicking "Save Changes" at the bottom of the settings menu.



The saved Action will be displayed above the settings for additional AI Filter Actions.

Camera Settings // Person Detection Camera

Camera Retention Resolution IO Motion Analytics Audio Location Metrics AI Filtering

Alert actions:

Name of Action:

Action type:

Recipients:

Notification type:

Re-arm (minutes):

Max per hour:

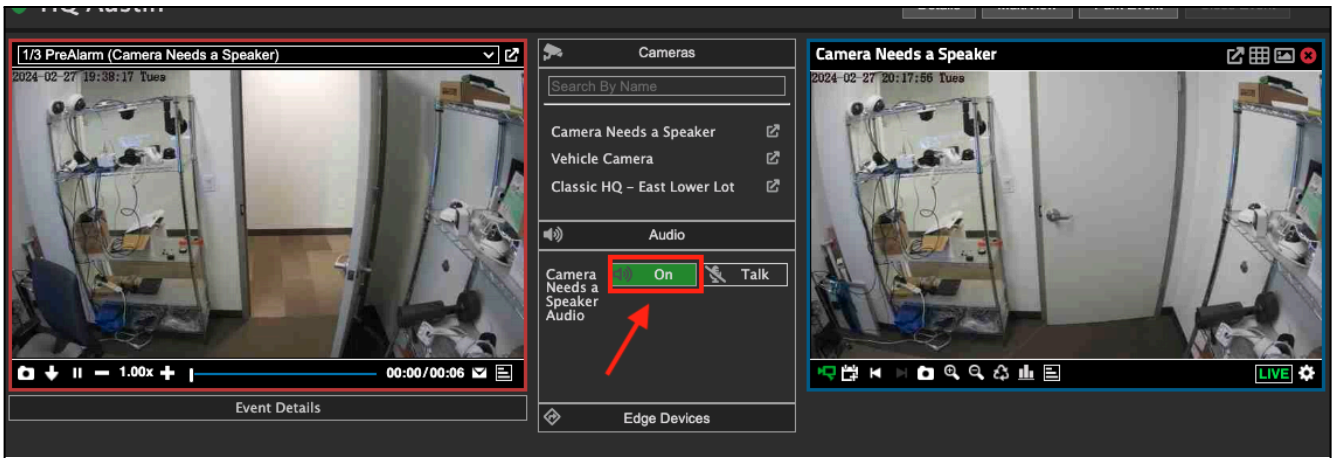
5. Using Audio in Immix from compatible Cameras and IP Speaker devices added to Eagle Eye Networks Cloud VMS

The following steps are to be conducted by an Immix administrator at the monitoring center. Eagle Eye Cloud VMS supports Talk-Down through compatible SIP enabled IP speakers. Read [AN072 Configure 2-Way Audio to Communicate Remotely Through the Eagle Eye Cloud VMS](#) for more information.

These devices may be included in the integration to Immix for monitoring, and can be controlled through the Alarms interface.

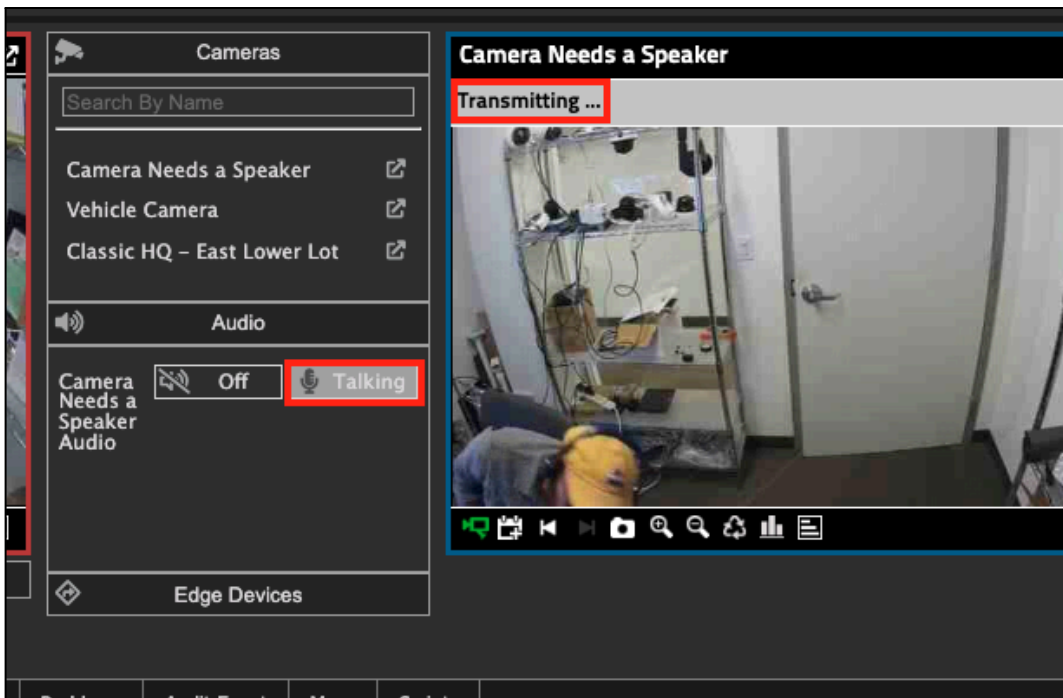
Cameras that have built in microphones or a mic input which is supported by Eagle Eye Cloud VMS will be able to send audio to the operator while viewing the camera Live stream.

In the Alarms interface, a camera that has a microphone can play audio by clicking on the Audio button (has a speaker icon). Click once to enable, and click the button again to turn audio off.



For Talk Down audio, if there is an IP Speaker or Horn enabled in the Eagle Eye Cloud VMS, and added as an Audio device in Immix with an associated camera, you can use the Talk icon to initiate communication to the Speaker.

Press and hold the Talk button; once you see “Transmitting” displayed on screen, you can speak through your device's microphone (computer mic or headset for example). Once you are done speaking, release the Talk button.



There is a delay before your message is played at the site. If you are attempting to speak down to a person in view, it may take a moment before they hear the message. Long messages can delay the transmission further, so the Talk feature is best used for short and succinct messages.

6. Testing

To be conducted by both installer and Immix administrator/operators.

As with any professionally monitored surveillance solution, it is important to test that alarms and videos are being received properly prior to arming a site for monitoring.

The installer, after ensuring the site is placed on test within the Immix platform, should intentionally trigger all configured motion and analytic alarms and confirm receipt by the monitoring center. It may be necessary to temporarily change any schedules set for motion and analytics notifications if these tests are being conducted outside of the configured schedules.

The Immix 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 working live view.

Once confirmed, the integrated site is ready to arm for ongoing monitoring within Immix.