

Eagle Eye Application Note - AN042

Configuring The Eagle Eye VMS and Immix Integration for Alarm Monitoring

2023-10-25 Revision 1.0

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 comprises 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 Networks Cloud VMS provides by design 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 Networks interface.
- **Live Video** - Live video streams from Eagle Eye Networks Cloud VMS-attached cameras can be viewed within the Immix platform.
- **Playback** - Recorded video from Eagle Eye Networks Cloud VMS-attached cameras can be viewed within the Immix platform.
- **PTZ** - Control pan, tilt, and zoom for attached PTZ-capable cameras.
- **Presets** - Go to any pre-configured pan, tilt, zoom setting.
- **Multiview** - Multiple Eagle Eye Networks VMS-attached cameras can be viewed simultaneously within the Immix platform.

- **Alarms** - Triggers based on motion, or the Eagle Eye Networks line-crossing, intrusion, and loitering analytics can be presented in the Immix platform.
- **Attached clips** - Video clips (images) of the triggering event for an alarm 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 Networks Cloud VMS system for addition to Immix by the installer
2. Addition of the Cloud VMS system 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

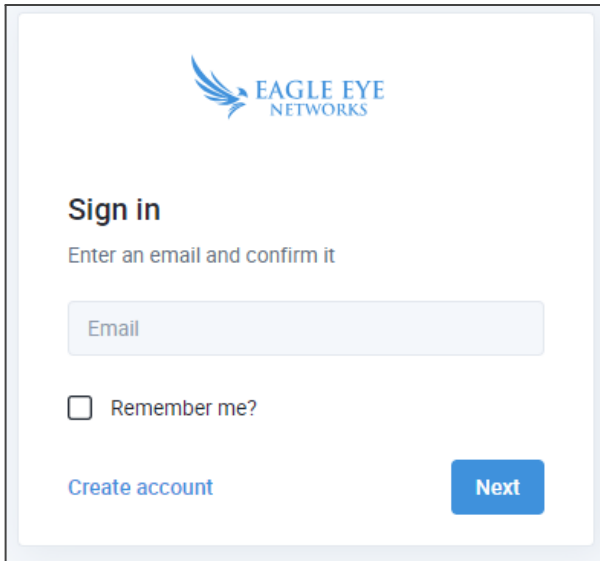
1. Preparation of the Eagle Eye Networks System for Addition to Immix

The following steps are to be completed by an Eagle Eye Networks Cloud VMS administrator from the installer.

The Eagle Eye Networks Immix integration needs to be enabled on a sub-account level prior to conducting the integration. Please contact customercare@een.com or 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 Networks 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/>



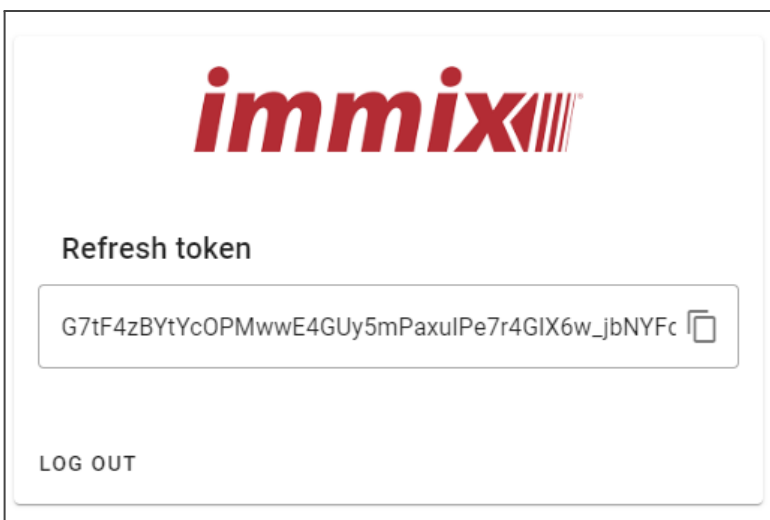
The image shows the 'Sign in' page for Eagle Eye Networks. At the top left is the Eagle Eye Networks logo. Below it, the text 'Sign in' is displayed in bold. Underneath, it says 'Enter an email and confirm it'. There is a text input field labeled 'Email'. Below the input field is a checkbox labeled 'Remember me?'. At the bottom left, there is a link 'Create account' in blue. At the bottom right, there is a blue button labeled 'Next'.

You will be asked to enter the credentials for a Cloud VMS user account. **It is important to use 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 the 'Refresh token' page in the Immix application. At the top center is the Immix logo in red. Below it, the text 'Refresh token' is displayed. Underneath, there is a text input field containing the refresh token: 'G7tF4zBYtYcOPMwwE4GUy5mPaxuIPe7r4GIX6w_jbNYFc'. To the right of the token is a copy icon. At the bottom left, there is a link '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 a pre-existing one using the details below and those provided by the installer.

EDIT DEVICES FOR: AGGREGATE INDUSTRIES

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.

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: G7HF4zBY1YcOPMmwE4G1y5mPaxulPe7r4GDX6w_jbNYFqG6r7Vul.HE
OAuth Eagle Eye Refresh Token

CAMERA PREVIEW

DETECT DEVICE CONFIGURATION
GET CONFIG

DONE CANCEL
Fields marked with * are required

Device Type: Eagle Eye VMS

IP/Host: Can be left blank

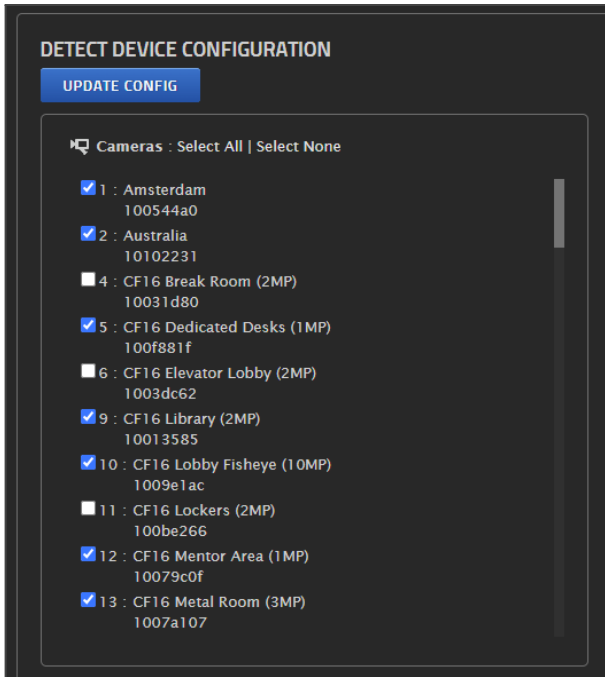
Port: Can be left blank

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)

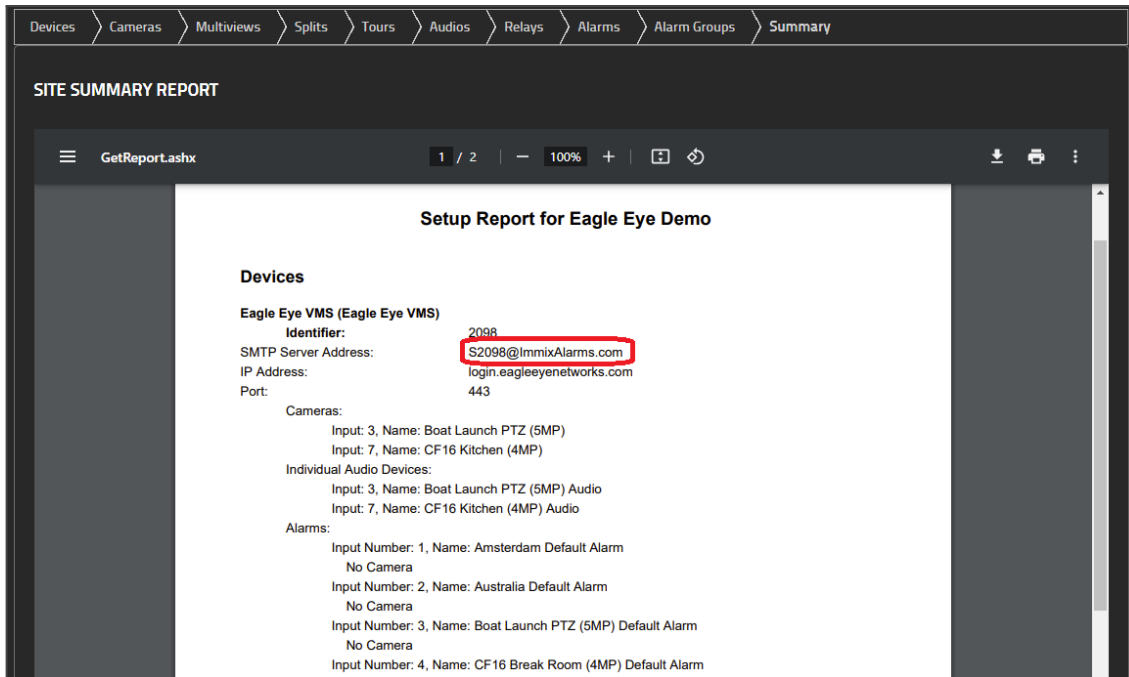
Next, click “Get Config” to retrieve a list of available cameras and alarm devices to add to the Immix site. If only a subset of cameras are to be added, untick the cameras and alarm devices not required.



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 Networks 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.

Account Settings // []

Control Days Security Camera Alerts Notifications Sharing Responders Defaults

Active Alert Mode: Test [v] ?

New Alert Mode Name [] Add Alert Mode

default [x]

Test [x]

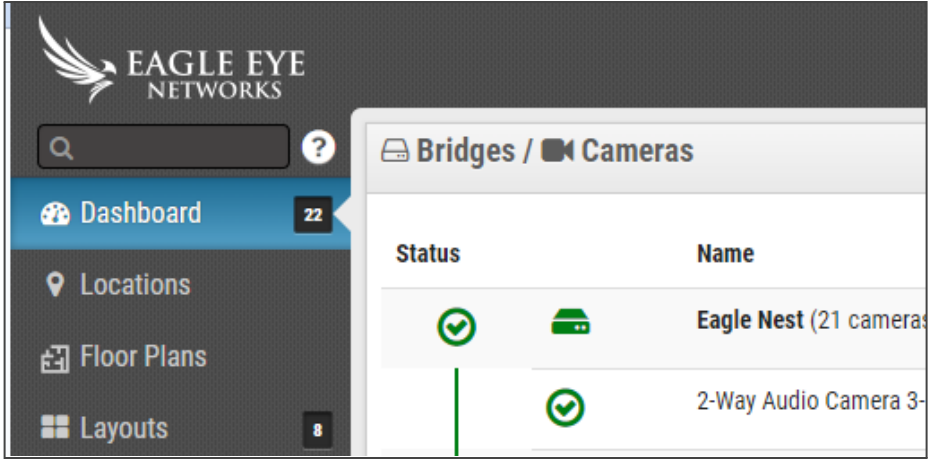
Immix Custom IP: [] ← IP address or domain name of your Immix server instance

Immix Custom Port: 2525 [] ← SMTP port number

Cancel Save changes

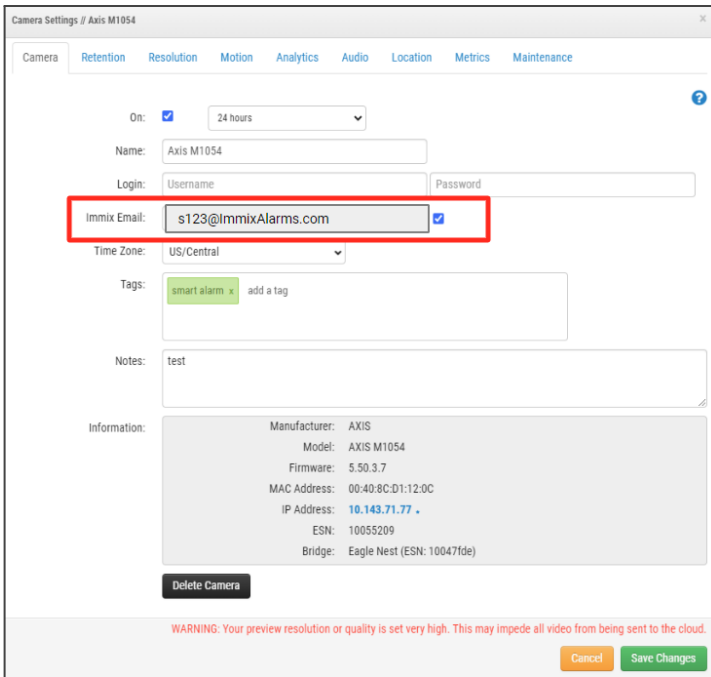
Additionally, for each camera that is to send motion or analytics alerts to Immix, enter the “SMTP Server Address” provided by the Immix administrator into the “Camera” tab of the camera’s settings, accessed by clicking the gear icon from the Cloud VMS dashboard.

Go to the Camera Settings from the dashboard



Click on the gearbox for the camera you want to select

test 8	test	Warehouse	[] [] [] []
test 7		Warehouse	[] [] [] []

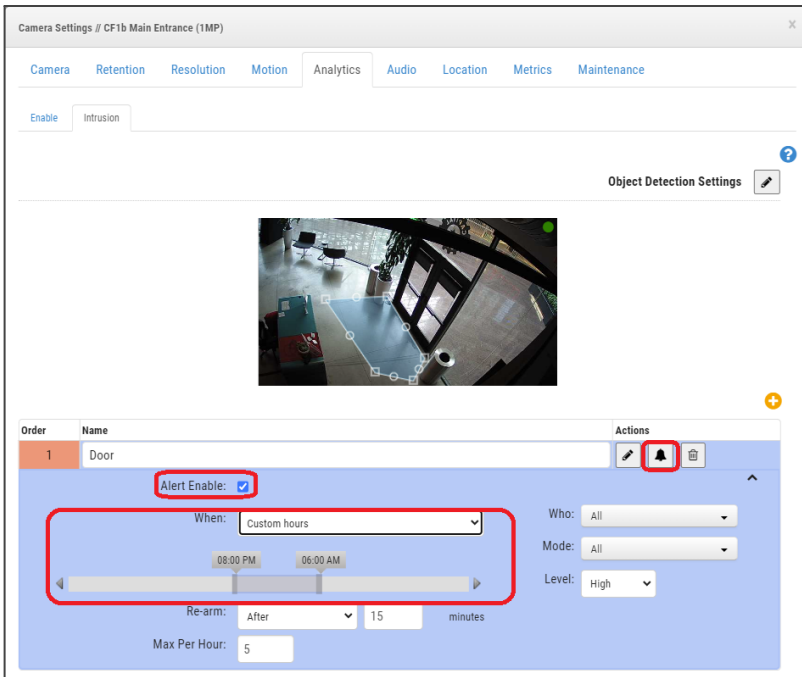


In this example, any alerts that involve this camera will be passed to your Immix system, and an email will be sent from the Eagle Eye VMS to s123@ImmixAlarms.com. This includes Motion, Intrusion, Line Crossing and Loitering alerts.

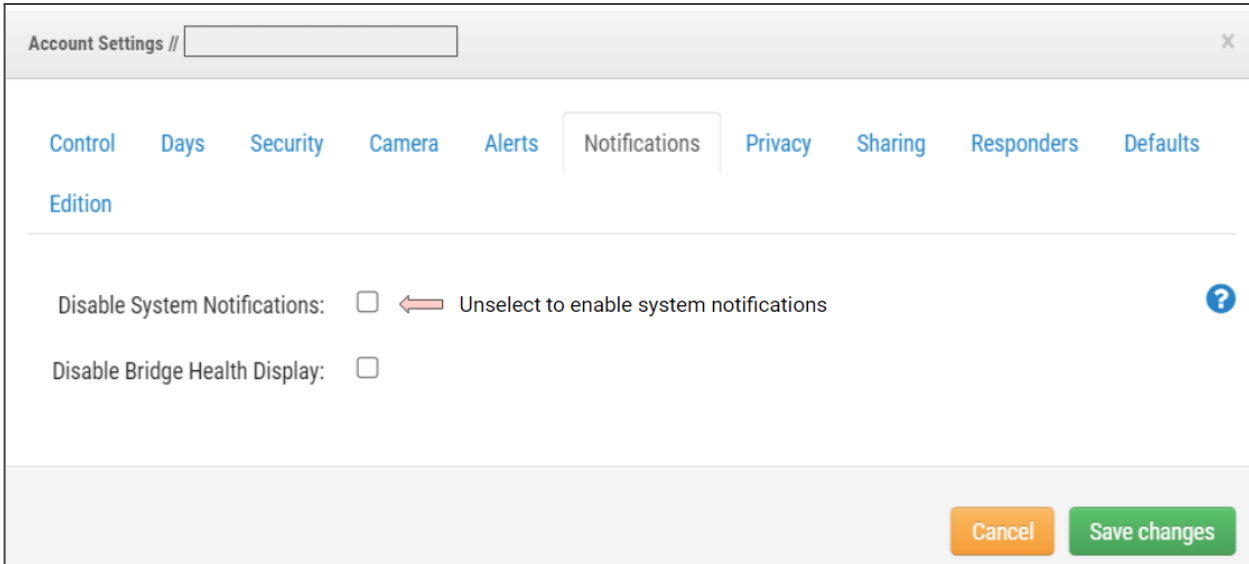
Next, either motion or analytics should be configured on the cameras that are to connect with Immix. Guides to this process can be found at the following links:

- [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. 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.