Eagle Eye Application Note – AN010

Using Eagle Eye VMS Audit Log to Monitor Compliance to Standard Operating Procedures

2022-06-07 Revision 1.2

Feature Overview

In the world of security, having a proper audit trail is essential for trusting your data. Being able to track who made changes to settings and when, or who viewed (or failed to view) a video clip provides the right visibility into the Eagle Eye VMS system.

The Eagle Eye Cloud VMS provides an Audit Log that allows users to perform Audits of activity within the VMS. The data can be viewed in the browser or downloaded to a CSV file. Records for Audit logs are kept for one year and can be viewed in any date range up to that.

The Archive is available to all Editions of the VMS, with different storage limits based on the Edition (Standard, Professional, Enterprise).

Background

Almost every action performed within the Eagle Eye Cloud VMS is logged as an event and saved within the audit log. These events are saved for one year for auditing purposes, showing user actions taken along with the time the change was made.

Access to the audit log is controlled by the VMS Administrator and can be granted/revoked on a per user basis in the User Settings.

Functionality

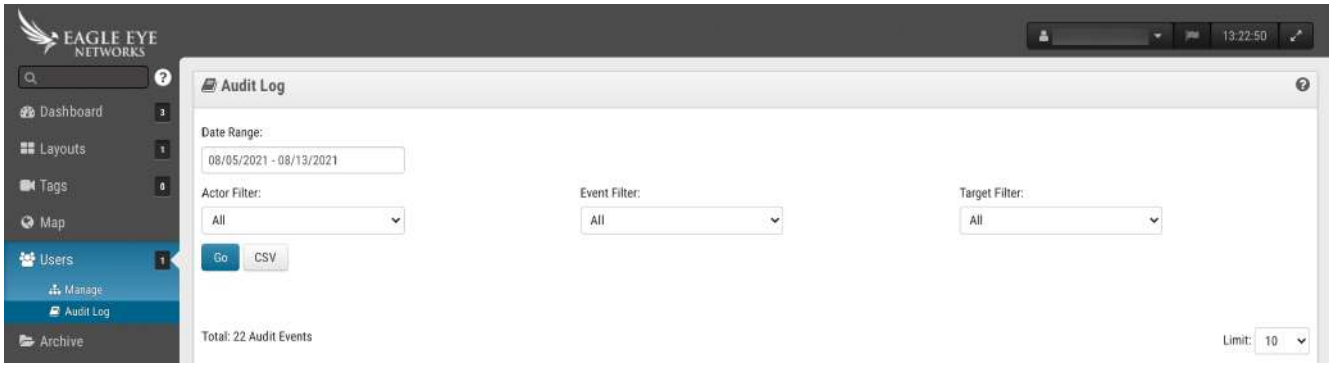

Image 1: Access the Audit Log from within the Users section of the left-side menu

- **Date Range** – Select any of the presets (today, yesterday, last 7 days, last 30 days, this month, last month), or choose a custom range up to one prior year.
- **Actor Filter** – Choose a single user or all users.
- **Event Filter** – Choose which events should be shown. There are a number of events to filter by that are broken down by the following categories:
    - **Account Events** – All events around account actions, including creating, editing, and deleting user accounts and first responder accounts.
    - **Alert Events** – All events concerning alerts, including creating and clearing alerts.
    - **Analytic Events** – All events related to Analytics.
    - **Device Events** – All device events, including bridges, CMVRs, cameras, etc.
    - **File Events** – Events associated with creating, deleting, or updating files.
    - **Layout Events** – All events concerning Layouts, including creating, deleting, modifying, etc.
    - **Notification Events** – Events that occur when notifications are sent or not sent.
    - **Plugin Events** – Any events that occur concerning plugins; creating, deleting, updating, etc.
    - **User Events** – Events that are logged when users are created or deleted, passwords are reset, or users log in/out.
    - **Video Events** – Any events around video recording, viewing, download, etc.
- **Target Filter** – Choose which target the event filter will look at. These filters are separated in the following categories:
    - **Devices** – Target events that occurred on a specific camera, bridge, CMVR, etc.
    - **Layouts** – Target events that only relate to Layouts.
    - **Videos** – Target events that only relate to videos.
- **Go** – Click this button to display the audit log generated by the selected filters in the browser window.
- **CSV** – Click this button to download a CSV file of the audit log.
- **Limit** – Change the number of events displayed per page.

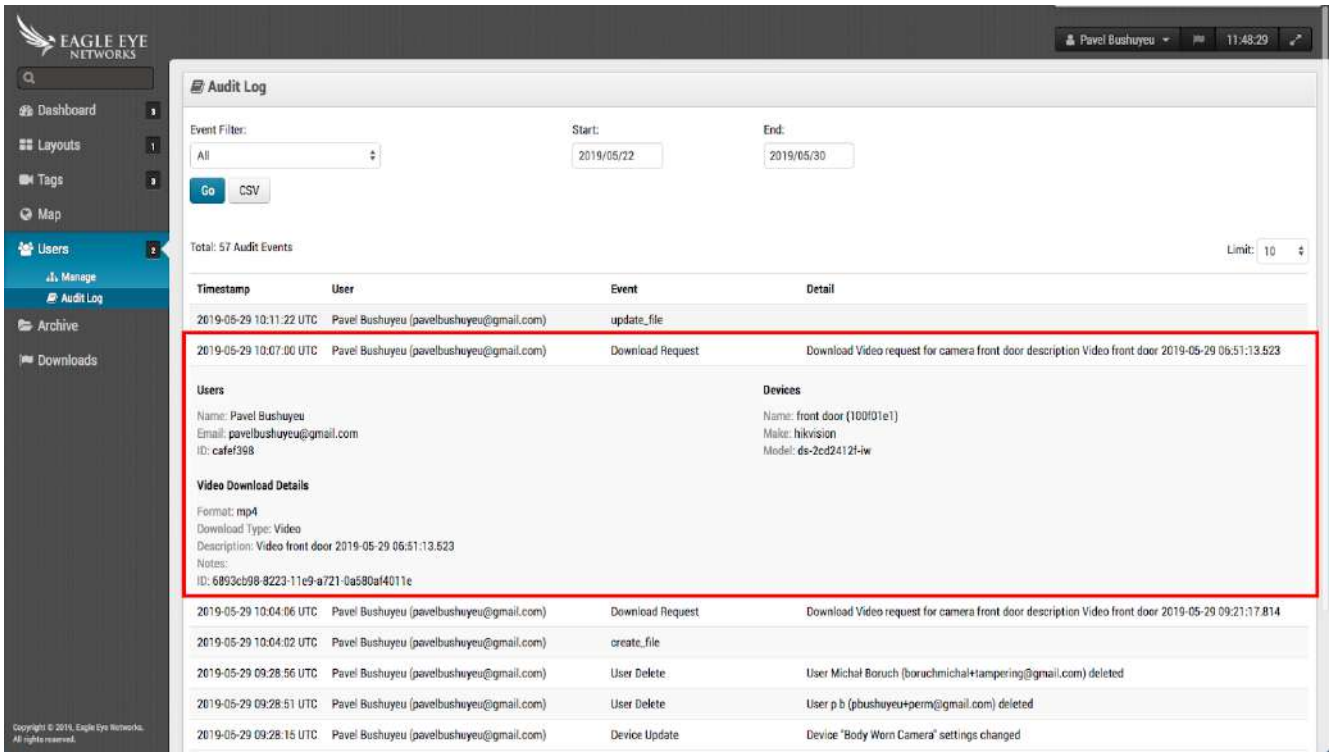

Image 2: Seeing additional details by expanding the entry within the Audit Log

Click any event to expand the entry and see additional details. When any kind of setting is changed, the detailed view will show the previous value and the value it was changed to. Click on the event again to dismiss the detailed view.

Application

Access the audit log by clicking Users on the left-side menu, then Audit Log underneath it. No setup is required (or available) to determine what events are stored. For security reasons, all events are logged.

Users that have not been granted access to the audit log will not see the menu entry. To grant or revoke access to the audit log:

1. Log in as an administrator.
2. Click Users on the left-side menu.
3. Click the Gear icon next to the user to be updated.
4. Click the Permissions tab (as shown below).

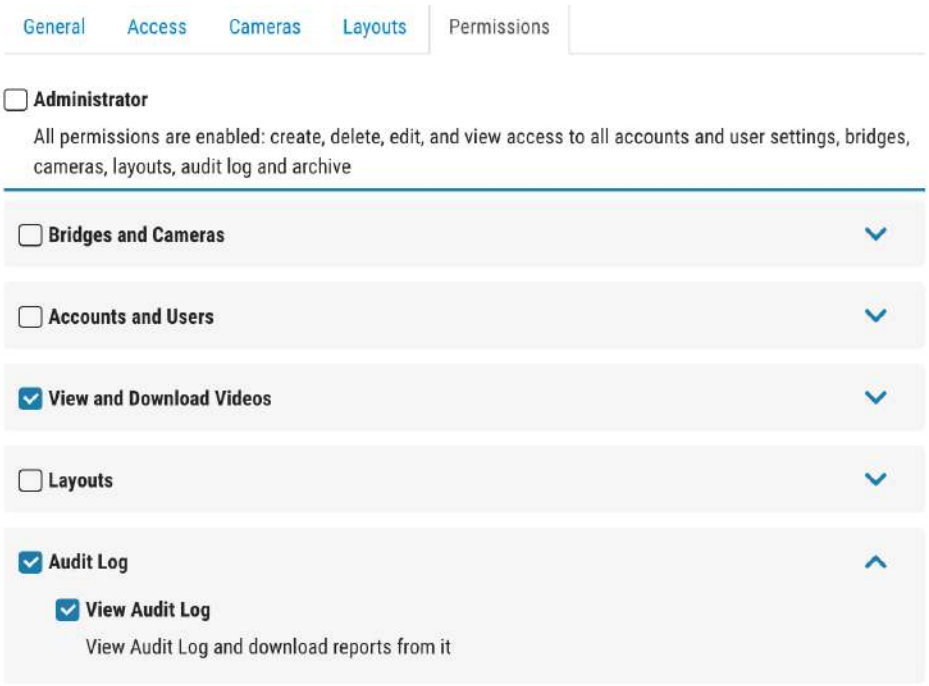

Image 3: Manage Permissions for the Audit Log from within Account Settings

5. Check the box next to Audit Log to allow the user access. Uncheck the box to revoke it.