AUDIT LOG SETTINGS

The Validation Platform Director has a consolidated audit log that tracks Validation Platform activity. As a general overview, the type of data in the Audit log is captured below. Each record is categorized using a Section and Action Type. For a list of Section and Action Type values, see **Audit Log Record Categorization** **(https://docs.mandiant.com/home/msv-audit-log-record-categorization)**. Some of the types of data it captures includes:

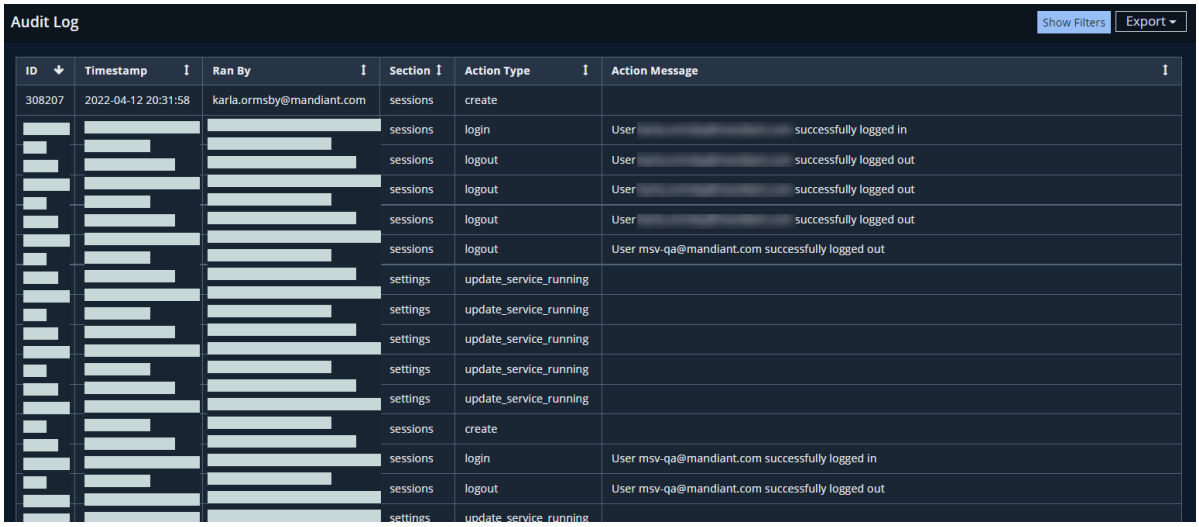
- Security Content changes: Creating, Updating, and Deleting Actions, Sequences, Evaluations, Files
- Director changes: Updating admin settings; updating network devices; adding, updating, removing notifications
- Instructions sent to the Actors: Check time sync, check version
- User Access: Login, Logout, Authentication failures
- Running Jobs
- Integrations: Adding, updating, removing Integrations
- User Actions: Users accessing reports

The audit log has a filter you can use if you're looking for a specific type of record and want to stay in the platform.

You can also do the following:

- Export the log to a csv file (MSV and MA-SV)
- Forward it to a syslog receiver (MSV only)

If you're concerned with the audit log becoming too large, you can enable email notifications for audit log storage warnings.



Audit Log Settings

Add a Syslog Receiver

1. Go to **Settings** > **Director Settings**.
2. Click **Audit Log**.
3. Scroll down and click **Add Syslog Receiver**.
4. Define the following receiver settings:
    - IP address or hostname

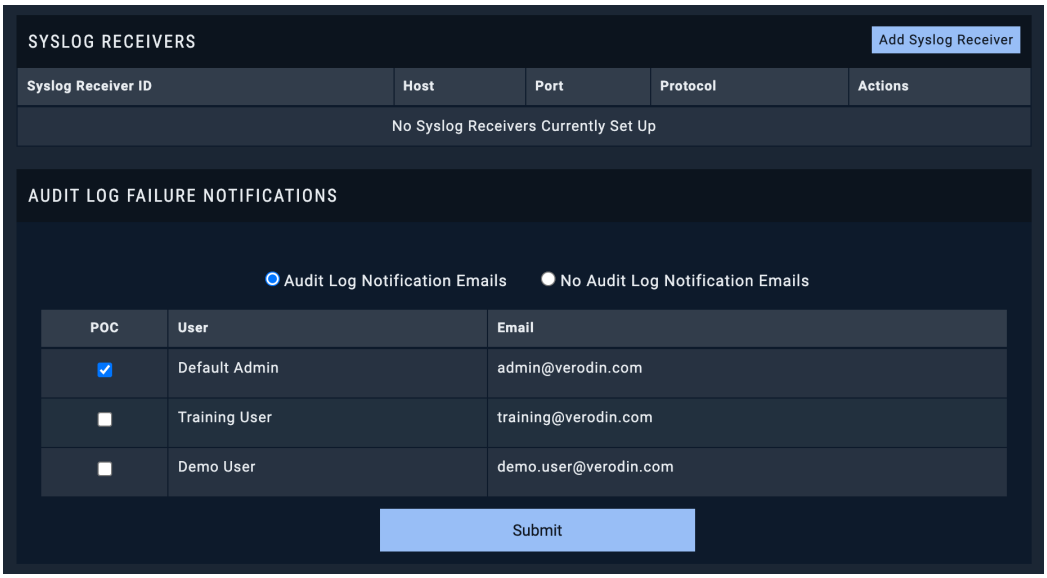
- Port
- TCP/UDP settings

5. Click **Submit**.

Enable Audit Log Failure Notifications

Users can receive email notifications when the audit log storage has less than 9 GB of storage left. Audit log failure notifications are disabled by default.

1. Go to **Settings** > **Director Settings**.
2. Click **Audit Log**.
3. Scroll down and select **Audit Log Notification Emails**.
4. Select the users you want to receive audit failure notifications.
5. Click **Submit**.



Audit Log Settings - Syslog Receivers (MSV only) and Audit Log Failure Notifications