

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 \(https://docs.mandiant.com/home/msv-audit-log-record-categorization\)](https://docs.mandiant.com/home/msv-audit-log-record-categorization). Some of the types of data it captures includes:

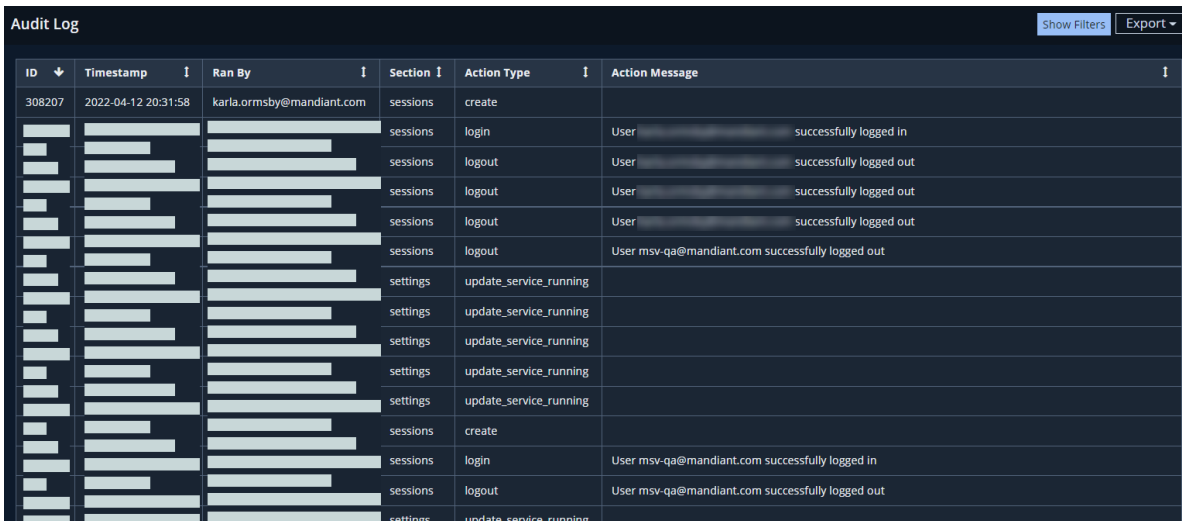
- Security Content changes: Creating, Updating, and Deleting Actions, Sequences, Evaluations, Files
- Director changes: Updating admin settings; updating network devices; adding, updating, removing notifications
- Instructions sent to the Actors: Check time sync, check version
- User Access: Login, Logout, 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.



ID	Timestamp	Ran By	Section	Action Type	Action Message
308207	2022-04-12 20:31:58	karla.ormsby@mandiant.com	sessions	create	
			sessions	login	User [redacted] successfully logged in
			sessions	logout	User [redacted] successfully logged out
			sessions	logout	User [redacted] successfully logged out
			sessions	logout	User [redacted] successfully logged out
			sessions	logout	User msv-qa@mandiant.com successfully logged out
			settings	update_service_running	
			settings	update_service_running	
			settings	update_service_running	
			settings	update_service_running	
			settings	update_service_running	
			sessions	create	
			sessions	login	User msv-qa@mandiant.com successfully logged in
			sessions	logout	User msv-qa@mandiant.com successfully logged out
			settings	update_service_running	

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

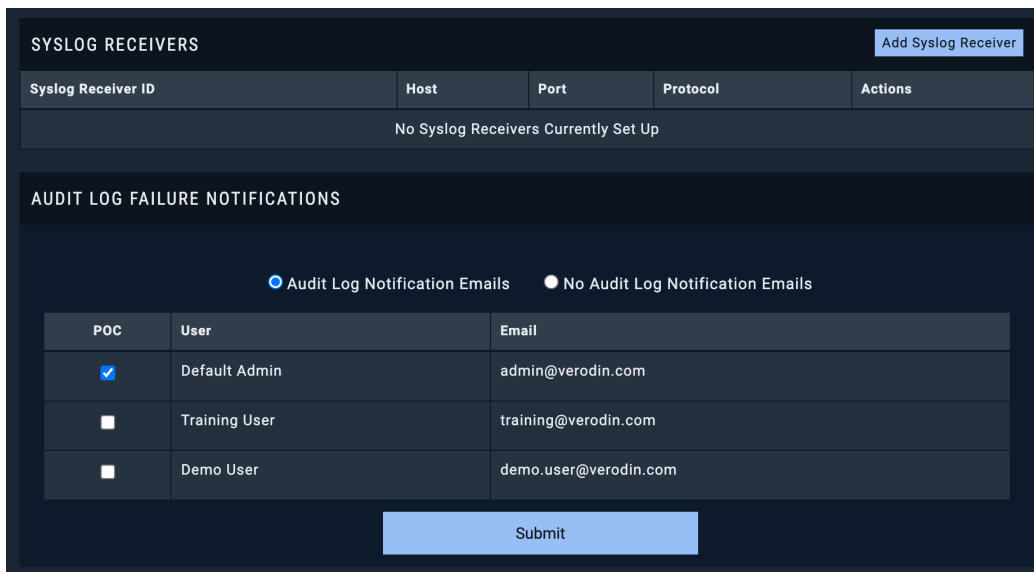
- Port
- TCP/UDP settings

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**.



The screenshot displays two sections of the Mandiant configuration interface. The top section, titled "SYSLOG RECEIVERS", includes a table with columns for Syslog Receiver ID, Host, Port, Protocol, and Actions. Below the table, a message states "No Syslog Receivers Currently Set Up". The bottom section, titled "AUDIT LOG FAILURE NOTIFICATIONS", features two radio buttons: "Audit Log Notification Emails" (which is selected) and "No Audit Log Notification Emails". Below these buttons is a table with three columns: POC, User, and Email. The table lists three users: Default Admin (checked), Training User, and Demo User. A "Submit" button is located at the bottom of the form.

Syslog Receiver ID	Host	Port	Protocol	Actions
No Syslog Receivers Currently Set Up				

Audit Log Notification Emails No Audit Log Notification Emails

POC	User	Email
<input checked="" type="checkbox"/>	Default Admin	admin@verodin.com
<input type="checkbox"/>	Training User	training@verodin.com
<input type="checkbox"/>	Demo User	demo.user@verodin.com

Submit

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