ExtraHop Security Audit Guide

Published: 2025-06-09

Regularly auditing your ExtraHop system is important for security because your environment is constantly changing: new threats can emerge, and your system configuration state, including user roles and permissions, can be modified over time by authorized users.

Audits help you uncover misconfigurations, excessive privileges, or outdated scripts that could lead to a security event or violation of your organizational policies. Proactively addressing audit issues is far less expensive and damaging than recovering from a security incident.

Users and Privileges

Check to ensure that your configured users are valid and have appropriate privileges.

RevealX 360 consoles

Review local users and their privileges.

1. Log in to RevealX 360.
2. From the Overview page, click **System Settings** and then click **User Access**.
3. In the Users section, click **View Users**.
4. Review the list of users and verify that all users have the correct assigned privileges.

RevealX Enterprise consoles

1. Review local users and their privileges.
   a) Log in to the Administration settings on the console through `https://<extrahop-hostname-or-IP-address>/admin`.
   b) In the Access Settings section, click **Users**.
   c) Review the list of users and verify that all users have the correct assigned privileges.
   d) Return to the main Administration settings page.
2. Reset remote user connections (such as LDAP, SAML).
   a) In the Access Settings section, click **Sessions**.
   b) Click **Delete All** to log out all users and require them to log in again.

All sensors

1. Review local users and their privileges.
   a) Log in to the Administration settings on the sensor through `https://<extrahop-hostname-or-IP-address>/admin`.
   b) In the Access Settings section, click **Users**.
   c) Review the list of users and verify that all users have the correct assigned privileges.
   d) Return to the main Administration settings page.
2. Reset remote user connections (such as LDAP, SAML).
   a) In the Access Settings section, click **Sessions**.
   b) Click **Delete All** to log out all users and require them to log in again.

Triggers

Check to ensure that configured triggers are aligned with your organizational policies. Triggers can collect sensitive data from observed traffic, or modify how collected data is sanitized.

Review triggers and trigger scripts.

1. Log in to the ExtraHop system through `https://<extrahop-hostname-or-IP-address>`.
2. Click the System Settings icon and then click **Triggers**.
3. Review all triggers to verify that triggers are assigned to the expected objects and trigger scripts are performing expected actions.
4. Verify that triggers that contain Open Data Stream classes (such as `Remote.HTTP`) are sending data to expected Open Data Stream (ODS) targets.

Open Data Streams (ODS)

Check to ensure that your ODS targets are configured to send data only to intended, trusted systems.

Review ODS targets on all sensors.

1. Log in to the Administration settings on the sensor through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the System Configuration section, click **Open Data Streams**.
3. Review all ODS targets to verify that they are configured to send data to expected destinations.

RevealX 360 Integrations

Check to ensure that integrations are only configured to send data to expected, trusted endpoints.

Review configured integrations.

1. Log in to RevealX 360.
2. From the Overview page, click **System Settings** and then click **Integrations**.
3. Verify that only expected integrations are enabled.
4. Verify that the integration configuration is accurate.
5. Optional: Rotate integration credentials and cut off unauthorized access.

   You can regenerate both ExtraHop REST API credentials and credentials for an integration system from the integration configuration page.

Connected appliances

Check to ensure that each appliance is an active, managed device under your organization.

Review connections from a RevealX 360 console

1. Log in to RevealX 360.
2. From the Overview page, click **System Settings** and then click **Sensors**.
3. Verify that connected sensors appear as expected.

Review connections from a RevealX Enterprise console

1. Log in to the Administration settings on the console through `https://<extrahop-hostname-or-IP-address>/admin`.

2. In the Connected Appliance Administration section, verify the configurations in the settings for **Manage Sensors**, **Manage Recordstores**, and **Manage Packetstores** to ensure that connected appliances appear as expected.
3. Review connected third-party recordstores.
   a) In the Records section, click **Recordstore**.
   b) Review all third-party recordstore configurations to verify that recordstore targets are configured as expected to guard against unintended data exfiltration.
   c) Click **Connect ExtraHop Recordstore** to review the ExtraHop recordstore configurations and to verify that node targets appear as expected.

Review connections from sensors

1. Log in to the Administration settings on the sensor through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Connected Appliance Administration section, verify the configurations in the settings for **Connect Console**, **Connect Recordstores**, and **Connect Packetstores** to ensure that connected appliances appear as expected.
3. Review connected third-party recordstores.
   a) In the Records section, click **Recordstore**.
   b) Review all third-party recordstore configurations to verify that recordstore targets are configured as expected to guard against unintended data exfiltration.