Troubleshoot recordstore connectivity

Published: 2024-11-20

Reveal(x) 360 provides a fully-hosted, cloud-based recordstore that gives you a unified view of your sensors. If the connection from a self-managed sensor to the recordstore is disabled, here are some ways to troubleshoot and restore the connection.

Create a notification rule

To learn about issues when they happen, create a notification rule ⬈ to email a recipient list whenever system events occur that are associated with recordstore connectivity issues. The email notification includes the names of affected sensors that you should investigate.

Check the sensor configuration

View sensor details to check if an affected sensor is disabled, has an invalid license, or requires newer firmware.

1. Log in to Reveal(x) 360.
2. Click the System Settings icon ⚙ and then click **Sensors**.
3. Click the sensor you want to investigate and review the Sensor Details.

   - If the sensor is offline, enable the sensor.
   - If the license is invalid, contact your ExtraHop sales representative.
   - If your firmware is outdated, complete a firmware upgrade ⬈.

Test the sensor connection from Administration settings

Test connectivity from the Administration settings of the affected sensor. If the sensor is unable to connect to the recordstore, the ExtraHop system displays error messages about the cause, such as firewall or BigQuery ingest API issues.

1. Log in to the Administration settings on the affected sensor through https://<extrahop-hostname-or-IP-address>/admin.
2. From the Records section, click **Recordstore**.
3. Click **Test Connection**. The system displays a success message or a detailed error message that can help you troubleshoot the connection.

Verify access to ExtraHop Cloud Services and the recordstore

A sensor might not receive records if it cannot resolve DNS queries to Google BigQuery domains or traffic to those domains is blocked.

If your ExtraHop system is deployed in an environment with a firewall, you must open access to ExtraHop Cloud Services. Verify that your environment enables sensors to resolve DNS queries for *.extrahop.com and allows TCP 443 (HTTPS) access on one of the following IP addresses that corresponds to your sensor license:

- 35.161.154.247 (Portland, U.S.A.)
- 54.66.242.25 (Sydney, Australia)
- 52.59.110.168 (Frankfurt, Germany)

For Reveal(x) 360 systems that are connected to self-managed sensors, you must also open access to the ExtraHop Cloud Recordstore. Verify that your environment allows sensors to access these fully-qualified domain names through outbound TCP 443 (HTTPS):

- `bigquery.googleapis.com`
- `bigquerystorage.googleapis.com`

- `oauth2.googleapis.com`
- `www.googleapis.com`
- `www.mtls.googleapis.com`
- `iamcredentials.googleapis.com`

Ensure correct proxy configuration

Recordstore connections might have issues if your ExtraHop system is connected to a proxy server that is improperly configured. Ensure that the proxy is configured to verify SSL/TLS connections to Google BigQuery domains and that the proxy server CA certificate is added to the secure certificate store.

Allow gRPC traffic

Records cannot be created if the gRPC (Remote Procedure Call) protocol is blocked on a sensor. Check your environment to ensure that gRPC traffic to Google BigQuery domains is allowed.