Send records from ExtraHop to CrowdStrike Falcon LogScale

Published: 2024-04-02

You can configure your ExtraHop Reveal(x) Enterprise system to send transaction-level records to a CrowdStrike Falcon LogScale repository for long-term storage, and then query those records from the ExtraHop system and the ExtraHop REST API.

Here are some important considerations about enabling a LogScale repository as the recordstore:

- The amount of recordstore lookback that can be queried is determined by the data retention settings configured for your LogScale system.
- You can enable a separate LogScale repository for each ExtraHop sensor.
- From an ExtraHop console, you can query records from LogScale repositories on all connected ExtraHop sensors if those repositories are associated with the same LogScale view.
- If all ExtraHop sensors send records to the same repository, you can transfer recordstore settings and manage all sensors from the ExtraHop console.
- Any triggers configured to send records through `commitRecord` to a recordstore are automatically redirected to the LogScale repository. No further configuration is required.

Enable LogScale as the recordstore

Before you begin

- Your ExtraHop system must be licensed for the LogScale recordstore.
- Your ExtraHop system must be running Reveal(x) Enterprise firmware version 9.5 or later.
- Any console and all connected sensors must be running the same ExtraHop firmware version.
- Your ExtraHop user account must have System and Access Administration privileges.
- Your LogScale system must have version 1.111.0 or later.
- Your LogScale user account must have administrator privileges.
- You must have a LogScale ingest token associated with a repository or an organization token that includes permission for ingest across all repositories within the organization.
- You must have a LogScale view token that includes data read access permission.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Records section, click **Recordstore**.
3. Select **Enable LogScale as the recordstore**.

   Important: If you are migrating to LogScale from a connected ExtraHop recordstore, you will no longer be able to access records stored on that ExtraHop recordstore.
4. In the Ingest section, specify the following information about the LogScale repository that will ingest and store records from the ExtraHop system:
   - **Ingest Hostname:** The hostname of the LogScale repository.
   - **Ingest Port:** The port over which records are sent to the repository.
   - **Repository Ingest Token:** The authentication token for ingesting data into LogScale.
5. In the Query section, specify the following details about the LogScale API server that will handle record queries from the ExtraHop system.
   - **API Hostname:** The hostname of the API server.
   - **API Port:** The port over which record queries are sent to the API.

- **View Name:** The name of the LogScale view connected to the repository.
- **View Token:** The authentication token for queries to the LogScale repository.

6. Optional: Select **Compress outgoing record payloads with gZIP** to reduce ingested file sizes.
7. Click **Test Connection** to verify that your sensor can communicate with the LogScale repository.
8. Click **Save**.

After your configuration is complete, you can query for stored records in the ExtraHop system by clicking **Records** from the top navigation menu or from the ExtraHop REST API.

Transfer recordstore settings

If you have an ExtraHop console connected to your ExtraHop sensors, you can configure and manage the recordstore settings on the sensor, or transfer the management of the settings to the console. Transferring and managing the recordstore settings on the console enables you to keep the recordstore settings up to date across multiple sensors.

Recordstore settings are configured for connected third-party recordstores and do not apply to the ExtraHop recordstore.

1. Log in to the Administration settings on the sensor through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Records section, click **Recordstore**.
3. From the **Recordstore settings** drop-down list, select the console and then click **Transfer Ownership**.

   If you later decide to manage the settings on the sensor, select **this sensor** from the Recordstore settings drop-down list and then click **Transfer Ownership**.