Send records from ExtraHop to Splunk

Published: 2024-06-12

You can configure the ExtraHop system to send transaction-level records to a Splunk server for long-term storage, and then query those records from the ExtraHop system and the ExtraHop REST API.

Here are some considerations about sending records from ExtraHop to Splunk:

- Any triggers configured to send records through `commitRecord` to a recordstore are automatically redirected to the Splunk server. No further configuration is required.
- If you are migrating to Splunk from a connected ExtraHop recordstore, you will no longer be able to access records stored on the recordstore.
- If you want to view and analyze ExtraHop data such as metrics and detections in a Splunk interface, configure a Splunk or Splunk SOAR integration.

Send records from ExtraHop to Splunk

Complete this procedure on all connected ExtraHop systems.

Important: If your ExtraHop system includes a console or Reveal(x) 360, configure all sensors with the same recordstore settings or transfer management to manage settings from the console or Reveal(x) 360.

Before you begin

- Any console and all connected sensors must be running the same ExtraHop firmware version.
- You must have version 7.0.3 or later of Splunk Enterprise and a user account that has administrator privileges.
- You must configure the Splunk HTTP Event Collector before your Splunk server can receive ExtraHop records. See the Splunk HTTP Event Collector documentation for instructions.

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 Splunk as the recordstore**.
4. In the Record Ingest Target section, complete the following fields:
   - **Splunk Ingest Host:** The hostname or IP address of your Splunk server.
   - **HTTP Event Collector Port:** The port for the HTTP Event Collector to send records over.
   - **HTTP Event Collector Token:** The authentication token you created in Splunk for the HTTP Event Collector.
5. In the Record Query Target section, complete the following fields:
   - **Splunk Query Host:** The hostname or IP address of your Splunk server.
   - **REST API Port:** The port to send record queries over.
   - **Authentication Method:** The authentication method, which depends on your version of Splunk.

   For Splunk versions later than 7.3.0, select **Authenticate with token**, and then paste your Splunk authentication token. For instructions on how to create an authentication token, see the Splunk documentation.

   For Splunk versions earlier than 7.3.0, select **Authenticate with username and password**, and then type your Splunk credentials.
6. Clear the **Require certificate verification** checkbox if your connection does not require a valid SSL/TLS certificate.

Note: Secure connections to the Splunk server can be verified through trusted certificates that you upload to the ExtraHop system.

7. In the Index Name field, type the name of the Splunk index where you want to store records.

   The default index on Splunk is called `main`, however, we recommend that you create a separate index for your ExtraHop records, and type the name of that index. For instructions for creating an index, see the Splunk documentation.
8. (ExtraHop sensor only) Click **Test Connection** to verify that the ExtraHop system can reach your Splunk server.
9. Click **Save**.

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

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 Command appliance and then click **Transfer**.

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