

Send records from ExtraHop to Google BigQuery

Published: 2020-02-23

You can configure your Discover appliance to send transaction-level records to a Google BigQuery server for long-term storage, and then query those records from the ExtraHop Web UI and the ExtraHop REST API.

Before you begin

- You need the BigQuery project ID
- You need a credential JSON file from your BigQuery API authentication page



Note: Any triggers configured to send records through **commitRecord** to an Explore appliance are automatically redirected to the BigQuery. No further configuration is required.

Send records from ExtraHop to BigQuery

Complete this procedure on all connected Command and Discover appliances.

1. Log into the Admin UI on the ExtraHop appliance.
2. In the Records section, click **Third-party Recordstore**.
3. Select **Enable BigQuery as the recordstore**.



Important: If you are migrating to BigQuery from a connected Explore appliance, you will no longer be able to access records stored on the Explore appliance.

4. In the Project ID field, type the ID for your BigQuery project. The project ID can be found in the BigQuery API console.
5. In the JSON Credential File field, click **Choose File** and select the credential JSON file saved from your BigQuery project.
6. Click **Test Connection** to verify that your Discover appliance can communicate with the BigQuery server.
7. Click **Save**.

After your configuration is complete, you can query for stored records in the ExtraHop Web UI by clicking **Records**.



Important: Do not modify or delete the table in BigQuery where the records are stored. Deleting the table deletes all stored records.



Note: The **Chart Summary** and **Group by** selector are not available on the Records page.