

Send records from ExtraHop to Google BigQuery

Published: 2020-05-22

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.

 **Important:** If your ExtraHop system includes a Command appliance, configure all appliances with the same recordstore settings or transfer management to manage settings from the Command appliance.

1. Log in to the Administration page on the ExtraHop system through **https://<extrahop-hostname-or-IP-address>/admin**.
2. In the Records section, click **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.

Transfer recordstore settings

If you have a Command appliance connected to your Discover appliances, you can configure and manage the recordstore settings on the Discover appliance, or transfer the management of the settings to the Command appliance. Transferring and managing the recordstore settings on the Command appliance enables you to keep the recordstore settings up to date across multiple Discover appliances.

Recordstore settings are configured for connected recordstores and do not apply to the Explore appliance.

1. Log in to the Administration page on the Discover appliance 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 Discover appliance, select **this Discover appliance** from the Recordstore settings drop-down list and then click **Transfer**.