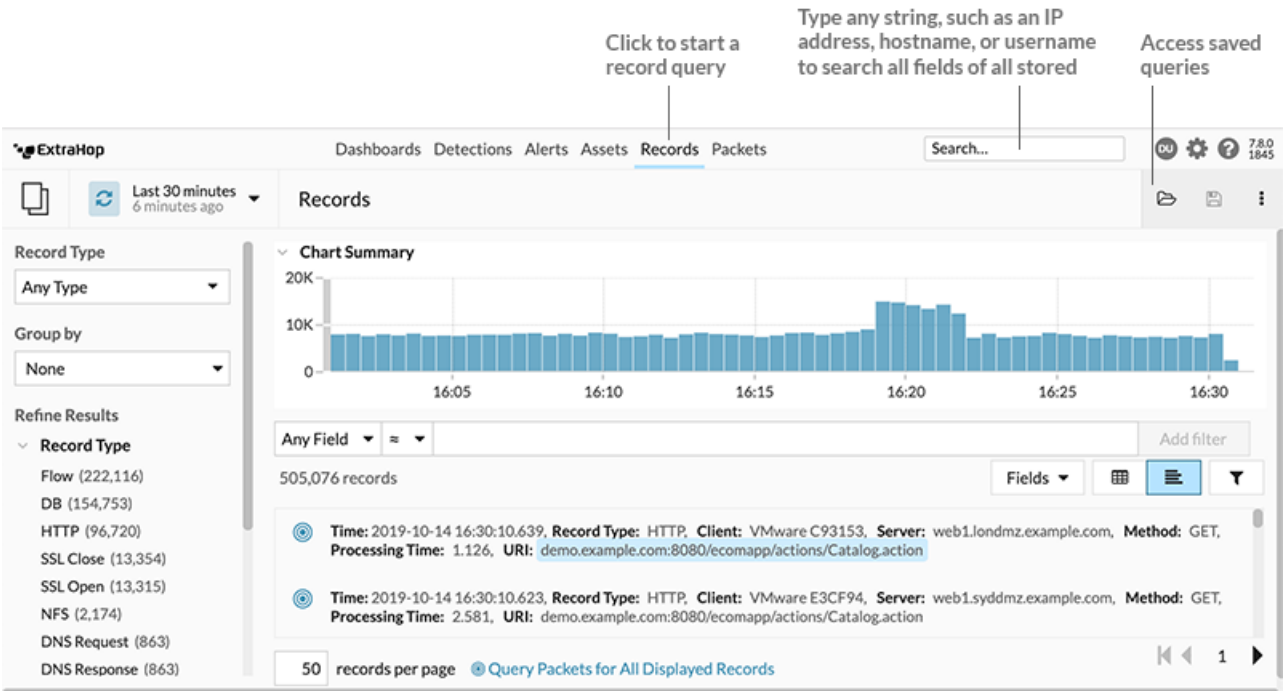
Query records with an advanced filter

Published: 2020-06-08

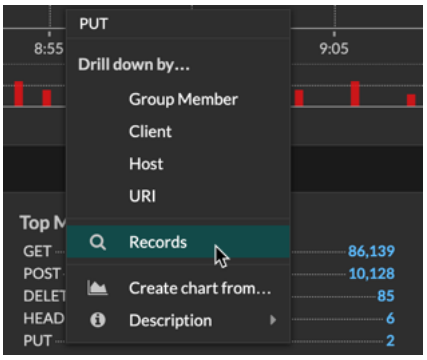
You can query records that are stored in the recordstore from multiple areas in the ExtraHop Web UI.

The following figure shows the main records page, that you access by clicking **Records** from the top menu.

Note: You can also automate this task through the REST API.



- Click **Records** from the top menu to start a new record query for all records stored on the Explore appliance or other supported recordstore.
- Click the Load icon from the top of the page to access any saved queries.
- Type a search term in the global search field at the top of the screen and click **Search Records** to start a query across all stored records.
- From a device Overview page, click **View Records** to start a query filtered by that device.
- Click the Records icon from a chart widget, as shown in the following figure.



- Click the Records icon next to a detail metric after drilling down on a top-level metric. For example, after drilling down on HTTP Responses by Server, click the Records icon to create a query for records that contain a specific server IP address.

  Note: To create a record query for a custom metric, you must first define the record relationship by linking the custom metric to a record type.

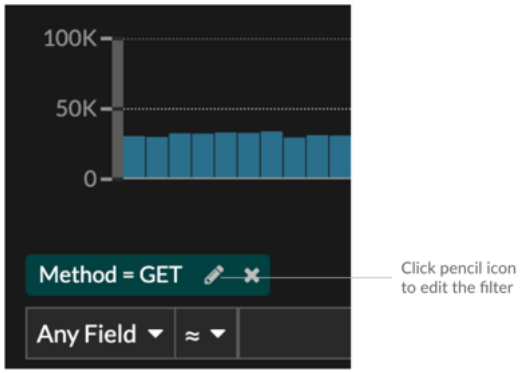
No matter where you start your query from, you might have a large set of records results. You can narrow down your results by applying filters to find the specific record you need.

Next steps

- Filter your record query
- To learn how to query for a specific record, see our walkthrough for Discovering missing web resources.

Filter your records with advanced query rules

For advanced queries, you can create and modify complex filters by clicking the Add Advance Filter button or by clicking the pencil icon next to any filter that you have added.



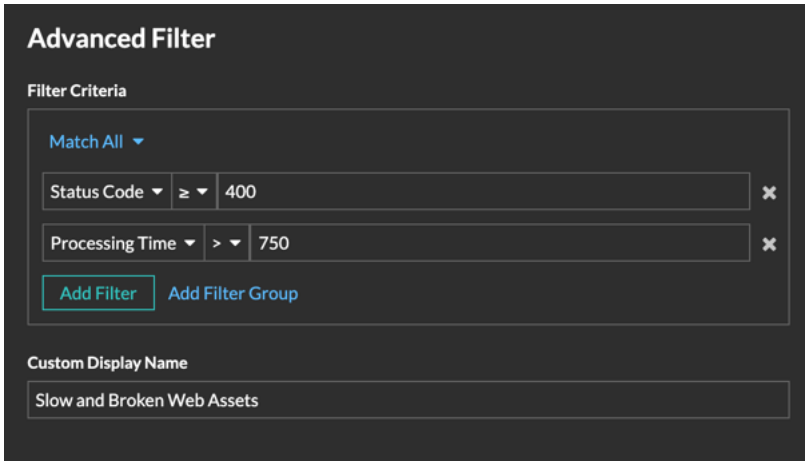
Here are some important things to know about advanced queries:

- You can specify multiple criteria with OR (Match Any), AND (Match All), and NONE operators
- You can group filters and nest them to four levels within each group
- You can edit a filter group after you create it
- You can create a descriptive name to identify the general purpose of the query

Create a complex filter with AND and OR operators

The following example shows how you can create an advanced query to filter your records with complex criteria. We will create a filter to return results for all HTTP records that include two URIs plus a status code greater than or equal to 400 or a processing time greater than 750 milliseconds.

Important: To try this example on your own Discover appliance, you must have HTTP traffic on your network.

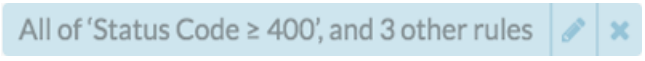


1. Click **Records** from the top menu.
2. In the left pane, select **HTTP** from the Refine Results section. Only available records are displayed in the Refine Results section. This step ensures that you have available records for this query.

   Note: Record types do not appear as filters; they are displayed in the left pane.
3. Click the Add Advanced Filter button . The button is on the right side of the page, above the records search results.
4. Under Filter Criteria, select **Match All** from the drop-down. Match All is an AND operator and will let us search for criteria that matches the status code and the processing time criteria.
5. Select **Status Code**, the greater than or equal to sign (**≥**), and then type `400` in the number field.
6. Click **Add Filter** to add a filter for processing time.
7. Select **Processing Time**, the greater than sign (**>**), and then type `750` in the number field.

   In the next steps, we will add a group of criteria that applies specifically to the fields we added.
8. Click **Add Filter Group**.

   We are keeping **Match Any** for this group. Match Any is an OR operator and will let us search for criteria that matches either of our URIs.
9. Click **Add Filter** to add a filter to the group.
10. Click the **Any Field** drop-down and select **URI**.
11. Select the includes (**≈**) symbol.
12. Type a URI for one of your web servers in the text field. We will add `assets.example.com`.
13. Click **Add Filter** to add a second URI filter to the group.
14. Click the **Any Field** drop-down and select **URI**.
15. Select the includes (**≈**) symbol.
16. Type a URI for one of your web servers in the text field. We will add `media.example.com`.
17. In the Custom Display Name field, type a descriptive name to make the filter easy to identify on the results page, otherwise the display name shows the first filter and the number of other applied rules:

    We will type “Slow and Broken Web Assets” in the field.
18. Click **Save**.

After you click **Save**, the query automatically runs, and returns records that match either URI and that have either a status code equal to or greater than 400 or a processing time that is greater than 750 milliseconds.

Next steps
You can click the Save icon from the top right of the page to save your criteria for another time.