

Query for stored records

Published: 2024-11-02

You can query records that are stored in the recordstore with a standard search or with AI Search Assistant.

- [Learn more about querying records with a standard search.](#)
- [Learn more about querying for records with AI Search Assistant.](#)
- To learn how to query for a specific record, see our walkthrough for [Discovering missing web resources](#) [🔗](#).
- You can also [automate this task through the REST API](#) [🔗](#).

Next steps



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](#) [🔗](#).

Query records with a standard search

The Records page enables you to build a complex filter to search for records.

Here are some important things to know about record queries with standard search:

- You can specify multiple criteria with OR (Match Any), AND (Match All), and NOT operators.
 - You can group filters and nest them to four levels within each group.
 - You can edit a filter group after you create it to refine search results.
1. Log in to the ExtraHop system through `https://<extrahop-hostname-or-IP-address>`.
 2. At the top of the page, click **Records**.
If AI Search Assistant is not enabled, the New Record Query section is displayed. If AI Search Assistant is enabled, click **Standard Search**.

New Record Query

Last 5 minutes Record Type Any Type Group By None

MATCH IPv4 Address = [×](#)

+

[View Records](#)

AI SEARCH ASSISTANT STANDARD SEARCH

Last 5 minutes (UTC-2.5) Record Type Any Type Group By None

MATCH IPv4 Address = [×](#)

+

[View Records](#)

3. Select the time interval that you want to search.
The time interval you select changes the time set in the [global time selector](#) [🔗](#).

- From the **Record Type** drop-down menu, select one or more of the record types that your ExtraHop system is configured to collect and store.
- From the **Group By** drop-down menu, select an option to specify how you want to group the results. The displayed options are associated with the record types you selected.
For example, if you group HTTP records by client, the results table displays the clients found on the record transactions, listed by the number of times that client was found.
- From the filter criteria drop-down menu (the default is IPv4 Address), select the first criteria you want the filter to match. The displayed options are associated with the record types you selected.
- Optional: Click the plus icon and select **Add Filter** or **Add Filter Group** to specify more criteria at the top or secondary level of the filter.

A new filter group adds criteria to the result of the original filter. For example, if you search for HTTP transactions that were suspicious and contained files, you can add a filter group to narrow the results to records associated with a specified network locality.

AI SEARCH ASSISTANT **STANDARD SEARCH** Last 5 minutes (UTC-2.5) Record Type HTTP Group By None

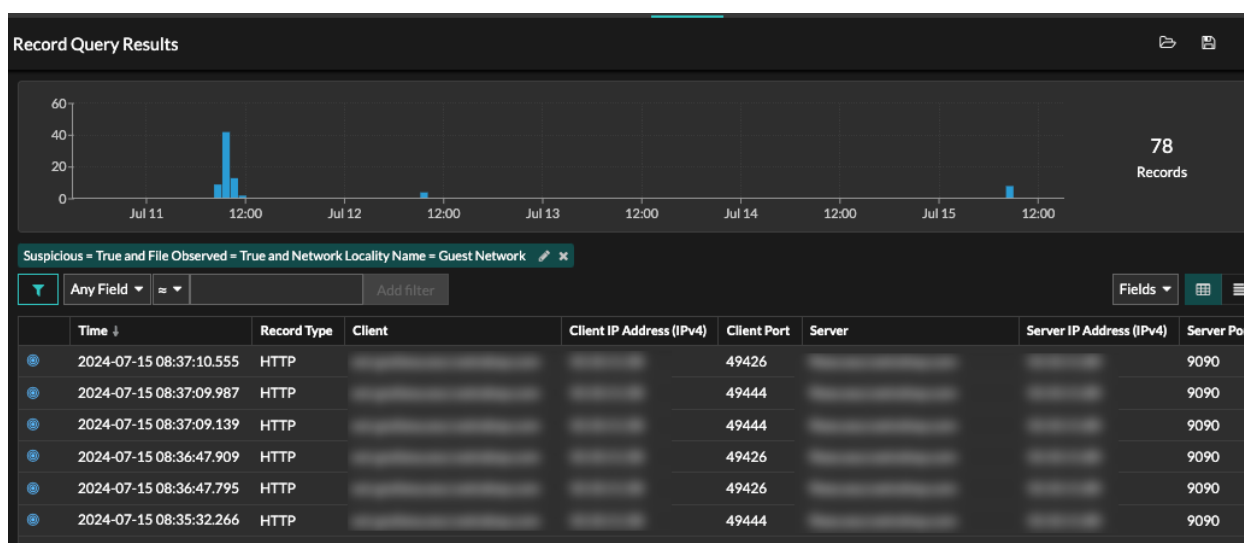
MATCH Suspicious = True

AND File Observed = True

AND MATCH Network Locality Name = Guest Network



View Records

- Click **View Records**.
Record results are displayed on the main Records page.



Next steps

- You can [view and drill down on record query results](#).
- You can [refine your record query filter](#).

- You can click the Save icon  from the top right of the page to save your filter for another time.
- You can click a packet icon next to a record to start a [packet query](#)  that is filtered by that record or click the query link at the bottom of the table to start a packet query for all displayed records.

Query records with AI Search Assistant

AI Search Assistant enables you to search for records with questions written in natural, everyday language to quickly build complex queries compared to building a standard search query with the same criteria.


For example, if you query for "Were there any suspicious HTTP transactions with files in the last 7 days?", the following AI Search Assistant query is displayed:

```
Time Interval = Last 2 days and Record Type = [HTTP]
Suspicious = True and File Observed = True
```

Here are some things to consider when searching for devices with AI Search Assistant:

- Prompts are mapped to the same record filter criteria that you specify when building a standard search.
- Prompts can include absolute and relative time ranges, such as "Show me traffic with Potential SQLi in the last 7 days". The current year is applied if a year is not included for a date.
- Prompts should be as clear and concise as possible and we recommend that you try writing a few variations to maximize your results.
- The ExtraHop system might be unable to process a query that contains requests for record information that is outside of the available filters.
- The ExtraHop system can retain user prompts for product improvement purposes; we recommend that you do not include proprietary or confidential data in your prompts.
- You can edit the query filter criteria to refine search results.

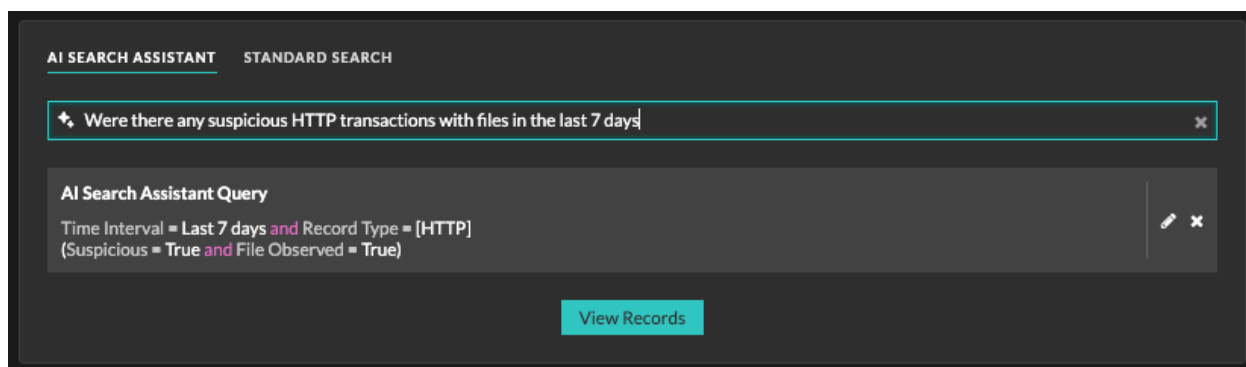
Before you begin


- Your ExtraHop system must be [connected to ExtraHop Cloud Services](#) .
 - AI Search Assistant must be enabled by your ExtraHop administrator.
1. Log in to the ExtraHop system through `https://<extrahop-hostname-or-IP-address>`.
 2. At the top of the page, click **Records**.
 3. Write a prompt in the AI Search Assistant field and press ENTER.

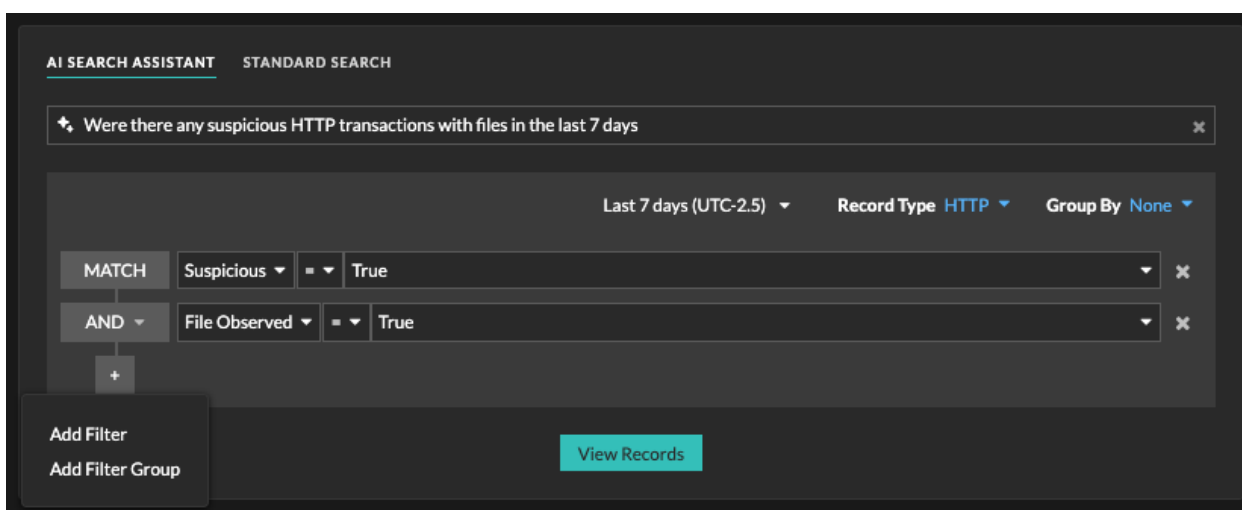


Tip: Click the search prompt field to select a recent query or suggested search.

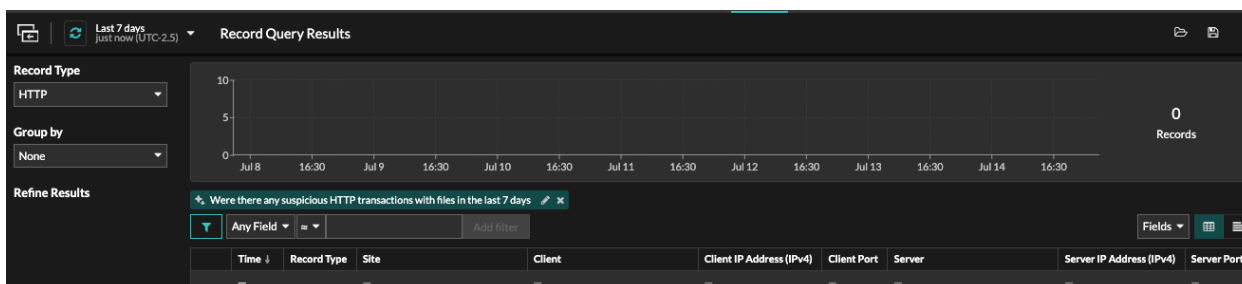
The AI Search Assistant query filter is displayed.



4. Optional: From the AI Search Assistant Query section, click the edit icon  to refine your query filter criteria.



- a) In the top row, edit the time interval, **Record Type** or **Group By** options.
 - b) Click the plus icon and select **Add Filter** or **Add Filter Group** to specify more criteria at the top or secondary level of the filter.
 A new filter group adds criteria to the result of the original filter. For example, if you search for HTTP records that were suspicious and contained files, you can add a filter group to narrow the results to records associated with a specified network locality.
 - c) Click **Done**.
5. Click **View Records**.
 Record results are displayed on the main Records page. The display name of the AI Search Assistant filter is the prompt that you entered and is shown above the tri-field.



Next steps

- You can [view and drill down on record query results](#).
- You can [refine your record query filter](#).
- You can click the Save icon from the top right of the page to save your filter for another time.
- You can click a packet icon next to a record to start a [packet query](#) that is filtered by that record or click the query link at the bottom of the table to start a packet query for all displayed records.