AI Search Assistant FAQ

Published: 2024-05-01

What is AI Search Assistant?

AI Search Assistant enables users to search for devices with questions written in natural, everyday language to quickly build complex queries. Reveal(x) 360 and Reveal(x) Enterprise administrators must opt-in to this feature, which is disabled by default.

If AI Search Assistant is enabled, users initiate searches from the Assets page ⤢ by typing a question about devices observed on the ExtraHop system. That question, or prompt, is mapped to filter criteria and the query output is displayed. For example, if the user types `Which devices have HTTP traffic with TLS v1.0?`, the following AI Search Assistant query is displayed:

```
(Activity = http_client or Activity = http_server) and (Detection Activity
 where Device Role = any and Type = weak_cipher_individual)
```

Users can modify query results to further refine filter criteria and improve search results.

What data is shared?

The ExtraHop Machine Learning Service leverages a third-party large language model (LLM) to generate asset search queries based on natural language prompts input by users. Prompts are not stored by the LLM or leveraged to train the LLM.

The Machine Learning Service retains and examines user prompts for quality assurance and to guide product improvement. We recommend that users do not include proprietary or confidential data in their prompts.

AI Search Assistant is not enabled by default on the ExtraHop system. Reveal(x) 360 and Reveal(x) Enterprise administrators must opt-in to share user prompts with the Machine Learning Service to enable AI Search Assistant.

What are the requirements for AI Search Assistant?

Here are the requirements to enable and access AI Search Assistant:

- Your ExtraHop system must be connected to ExtraHop Cloud Services ⤢.
- Your ExtraHop system must include the Network Detection and Response (NDR) module; AI Search Assistant is only available to users with NDR module access.
- Only Reveal(x) 360 and Reveal(x) Enterprise administrators can enable AI Search Assistant.
- AI Search Assistant leverages a third-party large language model (LLM) with regional limitations. AI Search Assistant cannot be enabled on ExtraHop systems that connect to ExtraHop Cloud Services from the following regions:

  - Asia Pacific (Singapore, Sydney, Tokyo)
  - Europe (Frankfurt, Paris)

Why should I enable AI Search Assistant?

Here are the ways that users benefit from AI Search Assistant:

- Simplifies searching for devices with multiple, complex criteria compared to building a standard search query with the same criteria.
- Accelerates the timeline for locating assets with anomalous behavior and detection activity.
- Displays the filter criteria of a query for easy refinement and better search performance.

Enable AI Search Assistant from Reveal(x) 360 Administration settings ⤢ or Reveal(x) Enterprise Administration settings ⤢. Your ExtraHop system must include the Network Detection and Response (NDR) module.

Can I disable AI Search Assistant?

From Administration settings, Reveal(x) 360 and Reveal(x) Enterprise administrators can opt out of the setting that enables AI Search Assistant.

The ExtraHop system displays an in-product reminder on the Assets page if no selection has been made for AI Search Assistant from the Administration settings. ExtraHop administrators can opt to disable AI Search Assistant and hide the in-product reminder.

The following settings are available:

- I agree to enable AI Search Assistant and send natural language searches to ExtraHop Cloud Services.
- I do not want to enable AI Search Assistant and do not want to see in-product reminders.