

Integrate Reveal(x) Enterprise with Splunk

Published: 2024-03-26

This integration enables you to view network threat detections and behavioral insights from Reveal(x) Enterprise into Splunk.

Before you can configure this integration, you must [generate an ExtraHop REST API key](#) and then add the key when you [configure the ExtraHop Add-on for Splunk](#).

System requirements

ExtraHop Reveal(x) Enterprise

- Your user account must have [full write privileges](#) or higher on Reveal(x) Enterprise.
- Your Reveal(x) Enterprise system must be connected to an ExtraHop sensor with firmware version 8.8 or later.
- Your Reveal(x) Enterprise system must be [connected to ExtraHop Cloud Services](#).
- Your Reveal(x) Enterprise system must be [configured to allow REST API key generation](#).

Splunk

- You must have Splunk version 8.1 or later.

Generate a REST API key

You must generate an ExtraHop API key before you can configure the ExtraHop Add-on for Splunk. The API key enables you to gain access to the integration and perform operations from Splunk.

1. Log in to the ExtraHop system through <https://<extrahop-hostname-or-IP-address>>.
2. Click the User icon at the top right corner of the page, and then click **API Access**.
3. In the Generate an API Key section, type a description for the new key, and then click **Generate**.
4. Scroll down to the API Keys section and copy the API key that matches your description.

Install and configure the ExtraHop Add-on for Splunk

1. Download and install the [ExtraHop Add-on for Splunk](#) from the SplunkBase site according to the [Splunk Add-Ons and Apps](#) documentation.
2. From the installed app, click **Configuration**, and then click **Add** from the Account tab.
3. Type a unique **Account Name**.
4. From the Instance Type drop-down list, select **On Prem Instance**.
5. Type the **Hostname** of the Reveal(x) Enterprise system that this account will connect to.
6. Enter the key that you generated from your Reveal(x) Enterprise system in the **API Key** field.
7. Complete the configuration of the account according to the [ExtraHop Add-on for Splunk documentation](#) available from the Details tab on the download page.