Integrate RevealX 360 with Splunk

Published: 2025-02-12

This integration enables you to view network threat detections and behavioral insights from RevealX 360 in Splunk.

> ⚠️ **Note:** Deprecated Integration
>
> The Splunk integration has been deprecated. Please migrate your integration to the Splunk Enterprise Security SIEM ⤢ integration.

System requirements

ExtraHop RevealX 360

To configure this integration, you must create Splunk integration credentials and then add them to the configuration of the ExtraHop Add-On for Splunk.

- Your user account must have privileges ⤢ on RevealX 360 for System and Access Administration.
- Your RevealX 360 system must be connected to an ExtraHop sensor with firmware version 8.8 or later.
- Your RevealX 360 system must be connected to ExtraHop Cloud Services ⤢.

Splunk

- You must have Splunk version 8.1 or later.

Create Splunk integration credentials

1. Log in to RevealX 360.
2. Click the System Settings icon ⚙ and then click **Integrations**.
3. Click the **Splunk** tile.
4. Click **Create Credential**.
   The page displays the generated ID and secret.
5. Optional: If you have already created a credential for REST API access, you can apply it to the integration. Click **Select Existing Credential**, select a credential from the drop-down menu and then click **Select**.
6. Copy and store the ID and secret, which you will need to configure the ExtraHop Add-On for Splunk.
7. Click **Done**.

The credential is also added to the ExtraHop REST API Credentials ⤢ page where you can view the credential status, copy the ID, or delete the credential.

Next steps
Install and configure the ExtraHop Add-On for Splunk.

Install and configure the ExtraHop Add-On for Splunk

1. Download the ExtraHop Add-On for Splunk ⤢ from the SplunkBase site.
2. Install and configure the add-on according to the following documentation:

   - About Installing Splunk Add-Ons ⤢
   - ExtraHop Add-On for Splunk Details ⤢

3. In the following configuration fields, enter the credentials you created and copied for the Splunk integration:

    - **Client ID**
    - **Client Secret**

Next steps
Export RevealX 360 detections and metrics and view them in Splunk according to the instructions in the ExtraHop Add-On for Splunk Details ↗.