

Integrate RevealX 360 with Cisco XDR

Published: 2024-10-12


Integrate ExtraHop RevealX 360 with Cisco XDR, a cloud-based detection and response tool, to enhance endpoint visibility and accelerate detection response. By creating ExtraHop REST API credentials, you can export RevealX device and detection data to Cisco XDR through ExtraHop REST API operations.

Before you begin

You must meet the following system requirements:

- ExtraHop RevealX 360
 - 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 9.8 or later.
 - Your RevealX 360 system must be [connected to ExtraHop Cloud Services](#).
- Cisco XDR
 - You must have an Administrator role on Cisco XDR.
 - You must have Cisco XDR Advantage or Cisco XDR Premium licensing tier.

1. Complete the following steps to create ExtraHop REST API credentials for the integration:

- a) Log in to RevealX 360.
- b) Click the System Settings icon  and then click **Integrations**.
- c) Click the tile of the integration you want to configure.
- d) Click **Create Credential**.
The page displays the generated ID and secret.
- e) 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 list and then click **Select**.
- f) Copy and store the ID and secret, which you will need to configure the ExtraHop app.
- g) Click **Done**.
The credential is added to the [ExtraHop REST API Credentials](#) page where you can view the credential status, copy the ID, or delete the credential.

2. Complete the following steps to [add the ExtraHop integration to Cisco XDR](#):

- a) From your Cisco XDR, click **Administration**, and then select **Integrations**.
- b) Click the **Third-Party** tab, and then click **Get Started** or **Enable** from the ExtraHop RevealX 360 card.
- c) Click the expand icon to open the integration guide.
- d) Complete the fields according to the expanded integration guide, which includes entering the ExtraHop REST API credentials that you created and copied for the integration.
- e) Click **Add**.

3. Export RevealX device and detection data to your Cisco XDR through the [ExtraHop REST API](#).