

Integrate Reveal(x) 360 with CrowdStrike

Published: 2021-12-14


Integrate Reveal(x) 360 with CrowdStrike to provide increased visibility and threat intelligence about your devices.

Before you begin

- You must have the security token provided by ExtraHop in your welcome email or your CrowdStrike API client ID, client secret, and endpoint.



Note: The scope of the CrowdStrike API client must include read access to the Indicators (Falcon X) API.

- Log in to the Reveal(x) 360 system with an account that has OktaAdmin or ApplianceAdmin (cloud setup) privileges.
- Click the System Settings icon  and then click **All Administration**.
- Click **Integrations**.
- Click the CrowdStrike tile.
- Choose one of the following options:
 - Click **Add Security Token** if you received a token from ExtraHop when you signed up for a free trial.
 - Paste the security token from your welcome email into the **Security Token** field.
 - Click **Connect**.
 - Click **Add Client ID and Secret**.
 - Enter your CrowdStrike client ID into the API Client ID field.
 - Enter your CrowdStrike client secret into the API Client Secret field.
 - Select your CrowdStrike API Region Endpoint from the drop-down list.
 - Click **Test Connection** to ensure that the ExtraHop system can communicate with CrowdStrike Falcon.
 - Click **Connect**.
- Optional: Configure any of the following integration options:
 - Select **Display links to CrowdStrike for devices that have Falcon software installed**. Devices must be local and have a MAC address. Links appear on the device overview page in Reveal(x) 360.
 - Select **Import Threat Intelligence for IP addresses from CrowdStrike Falcon**. A visual cue appears in the Reveal(x) 360 system for any activity that matches an entry in the CrowdStrike threat collection.
 - Select **Import Threat Intelligence for domains and hostnames from CrowdStrike Falcon**. A visual cue appears in the Reveal(x) 360 system for any activity that matches an entry in the CrowdStrike threat collection.
- Click **Save**.