

Integrate RevealX 360 with CrowdStrike

Published: 2025-04-05

Integrate ExtraHop RevealX 360 with CrowdStrike to provide increased visibility and control over your devices.

The following options enable you to display and access information to CrowdStrike Falcon devices in the ExtraHop system.

- Display [threat intelligence](#) links that navigate to CrowdStrike Falcon. These links are displayed on detections that are marked as Suspicious based on CrowdStrike threat intelligence.
- Display device detail links that navigate to CrowdStrike Falcon. Local devices with a MAC address that are running CrowdStrike Falcon software are displayed on the [Device Overview page](#) or when you hover over a device name to view property details throughout the ExtraHop system.
- Display device properties imported from CrowdStrike Falcon. When viewing CrowdStrike Falcon devices in the ExtraHop system, the Device Overview page displays the following types of CrowdStrike properties:
 - Last user
 - Hostname
 - OS version
 - Current local and external IP addresses
 - System manufacturer and product name
 - Containment status

These CrowdStrike properties are also available as filters when [searching for devices](#).

- Contain CrowdStrike Falcon devices from detections. Users can [initiate containment of CrowdStrike devices](#) that are participants in a detection on RevealX 360. Users must be granted access through the Detections Access Control global policy and have Full Write privileges or higher to initiate containment.

After you configure the integration, CrowdStrike threat intelligence for IP addresses, domains, and hostnames are automatically enabled and indicators of compromised devices are displayed in the ExtraHop system.



Note: The integration cannot import more than 50,000 total indicators from CrowdStrike.

System Requirements

ExtraHop RevealX 360

- Your user account must have privileges on RevealX 360 for System and Access Administration or Cloud Setup.
- Your RevealX 360 system must be connected to an ExtraHop sensor with firmware version 8.8 or later. Version 8.9 or later is required to enable the integration option for device containment.
- Version 25.2 or later is required to enable the integration option to import device properties.
- Your RevealX 360 system must be [connected to ExtraHop Cloud Services](#).

CrowdStrike


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



Note: If you upgrade your ExtraHop system, you will need to enter new credentials to configure new integration options.

- To enable integration options, you must have a subscription for CrowdStrike Falcon Intelligence and the following permissions for specific options:
 - To enable the integration option for importing device properties, the scope of the CrowdStrike API client must include READ permissions for Hosts.
 - To enable the integration option for device containment, the scope of the CrowdStrike API client must include READ and WRITE permissions for Hosts.


Configure the CrowdStrike integration

1. Log in to the RevealX 360 system.
2. Click the System Settings icon  and then click **Integrations**.
3. Click the CrowdStrike tile.
4. Choose one of the following options:
 - Click **Enter Security Token** if you received a token from ExtraHop when you signed up for a free trial.
 1. Paste the security token from your welcome email into the **CrowdStrike Security Token** field.
 2. Click **Connect**.
 - Click **Enter Client ID and Secret**.
 1. Enter your CrowdStrike client ID into the API Client ID field.
 2. Enter your CrowdStrike client secret into the API Client Secret field.
 3. Select your CrowdStrike API Region Endpoint from the drop-down menu list.
 4. Click **Test Connection** to ensure that the ExtraHop system can communicate with CrowdStrike Falcon.
 5. Click **Connect**.



Note: If you see a message that your credentials are invalid, re-type your client ID and secret and click **Connect** to try again.

5. Optional: Configure any of the following integration options:

Option	Description
Display links to CrowdStrike Falcon for threat intelligence	Links are displayed on detections.
Display links to CrowdStrike for devices that have Falcon software installed	Links are displayed on the Device Overview page  for CrowdStrike devices.
Import device properties from CrowdStrike Falcon	Properties are displayed on the Device Overview page and the list of search filters.
Enable users to contain CrowdStrike devices from detections in RevealX 360	An option is displayed to initiate containment of CrowdStrike devices that are participants in a detection.

6. Click **Save**.