CROWDSTRIKE

This document applies to Classic/Legacy Integrations. You may continue to use these integration configurations. While no active development is happening for these integrations, we continue to provide Classic/Legacy Integrations in the product. You do not have to move to MSI Integrations. If your support engineer or TSC recommends or you choose to move to MSI Integrations, you can take advantage of the latest features and functionality. For more information, see the MSI Integration documentation in the **Integrations Overview** **(https://docs.mandiant.com/home/msv-integrations-overview)**.

This integration is remote capable.

Update CrowdStrike

- Create a Username with the appropriate privileges, which requires a minimum of read on detections.
- Obtain your API key
  - Standard (Legacy) API: Contact Crowdstrike's customer support and request an API key.

    It may take a few days before they generate it and send it to you.

  - OAuth2 API key: Self-provision your API key on your portal

Update the Validation Platform

Prerequisites

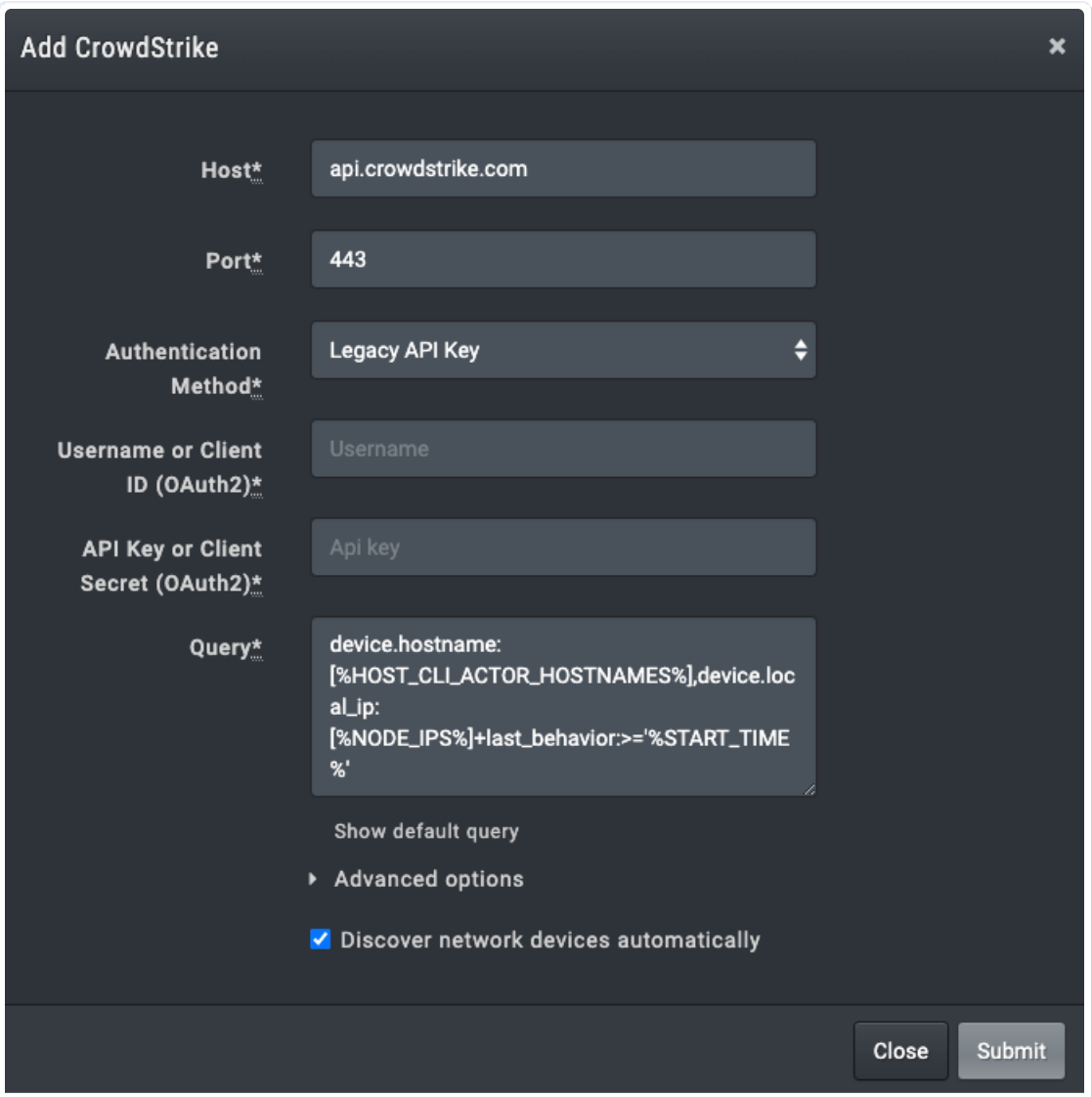
Information to gather before you start:

1. Create a Username in CrowdStrike.
2. Identify the API key.

Configuration

TO ADD THE CROWDSTRIKE INTEGRATION

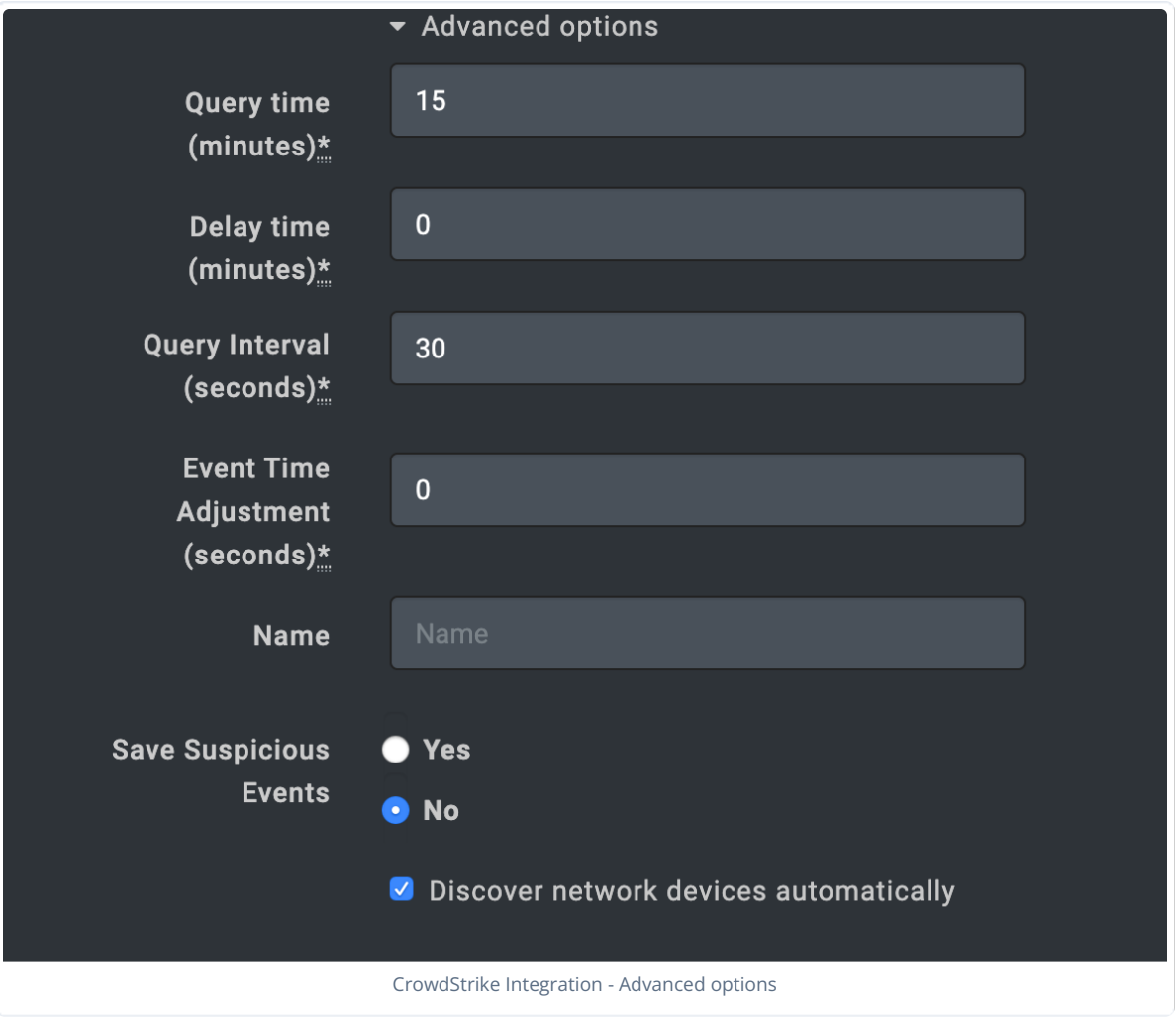
1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **CrowdStrike**.



CrowdStrike Integration

If you use the %HOST_CLI_ACTOR_HOSTNAMES% variable, the platform will substitute the plain hostname and the information from the Alternate Hostname field on the Actor configuration page.

3. Modify the **Host** and **Port**, if necessary.
4. Select your **Authentication Method**.
    a. Standard (Legacy) API: Legacy API Key
    b. OAuth2 API key: OAuth2
5. Enter Credentials for your Authentication method.
    a. Standard API: Username and API Key
    b. OAuth2: Client ID and Client Secret
6. Modify the **Query**, as necessary.
7. Expand **Advanced options**.



CrowdStrike Integration - Advanced options

8. (Optional) Select **Discover network devices automatically**.
9. Modify the **Query Interval** and **Event Time Adjustment**, if necessary.
10. (Optional) Assign a **Name**.
11. (Optional) Choose **Yes** to save suspicious events.
12. Click **Submit**.

Set up Proxy Assignment

If all outbound connections go through a proxy, you may want to set up a proxy definition and assignment for your integration. For information on setting up your proxy rules, see **Proxy Rules** **(https://docs.mandiant.com/home/msv-proxy-rules)**.

Verify Connectivity

TO VERIFY CONNECTIVITY TO CROWDSTRIKE

Click **Test** to verify that the Director can communicate with the CrowdStrike host using the provided Username and API key.