Mandiant

CROWDSTRIKE INTEGRATION WITH SECURITY VALIDATION

The integration with Crowdstrike lets you collect events generated by Crowdstrike to test the efficacy and configuration of the security control using Security Validation Jobs.

Use this document to configure the integration using one of the following methods:

- MSI (Supported and recommended for new integration configurations)
- Legacy (Supported for existing integration configurations)

Configure MSI Integration

This document covers the the MSI method of creating an integration. This method is the recommended approach for configuring new integrations in Security Validation.

To configure an integration, this document walks you through the following high-level steps:

1. Configure the third-party technology
2. Configure Security Validation
3. Verify connectivity

Configure CrowdStrike

API Calls

API	Usage
`/alerts/queries/alerts/v2`	Query alerts from Crowdstrike
`/alerts/entities/alerts/v2`	Retrieve detailed information about alerts from Crowdstrike
`/oauth2/token`	Retrieve an OAuth2 Token

Depending on your type of account, you use a specific host to access the API. Apply the relevant subdomain based upon where your account resides:

- US-1: `api.crowdstrike.com` (default)
- US-2: `api.us-2.crowdstrike.com`
- US-GOV-1: `api.laggar.gcw.crowdstrike.com`
- EU-1: `api.eu-1.crowdstrike.com`

Supported versions

- API v2 (Raptor Release)
- API v1 (deprecated)

To configure this integration, you need the following:

- A Username or Client ID
- An API Key (also referred to as a Client Secret)

Get a Client ID and API Key from Falcon

To generate a Crowdstrike Client ID and API Key, you must have the Falcon Administrator role. API Keys are only displayed when a new API Client is created or when the API Key is reset.

1. Log into the Falcon web interface.
2. Navigate to **Support and resources > API Clients and Keys** .
3. Click **Add new API Client** and fill out the dialog that appears.
4. Select the scope that is marked as **Required**:

Product area	Read	Write
Alerts	Required	Not Required

5. After clicking **Add**, make note of the Client ID and API Key (Client Secret) values that are displayed.

Configure Security Validation

Prerequisites

Information to gather before you start:

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

Configure the Crowdstrike Integration

1. Go to **Settings > Integrations**.
2. From the Integrations table, click **Add Integration > Crowdstrike**.

You can add this as either a Direct or Remote Integration.

3. Enter a meaningful **Integration Name**.
4. Optional: From the **Proxy** drop-down, choose a proxy profile if one is available. If one isn't available and all outbound connections go through a proxy, first, set up a **Proxy Rule** **(https://docs.mandiant.com/home/msv-proxy-rules)**.
5. For the **Host**, enter the appropriate value depending on your CrowdStrike environment:
   - US-1: `api.crowdstrike.com` (default)
   - US-2: `api.us-2.crowdstrike.com`
   - US-GOV-1: `api.laggar.gcw.crowdstrike.com`
   - EU-1: `api.eu-1.crowdstrike.com`
6. Enter a **Port** value. The default is **443**.
7. Enter **Client Id** and **Client Secret**.
8. Optional: Change the **Timeout** value if you want a different frequency of requests to an upstream server. The default is **30** (seconds).
9. Optional: Check **Verify Ssl** if you want this verification done for requests to an upstream server.
10. Optional: Add or modify any values in the **Query** section, as needed. The default queries are given in the web interface.
11. Optional: Modify the **Field Map** values, as necessary.

- Each field map box can hold a JSON-formatted comma-separated list of columns returned by the API to be considered for each field when translating into the normalized event object format. Example: description could be configured to be 'msg_s' or 'SyslogMessage' in some environments. The field map tries both if set to: ['msg_s','SyslogMessage'] and whichever matches first is the column that is used.
- When configuring an integration in Security Validation, you can assign additional host values in the Field Map settings. If none of the assigned fields return a valid host name, Network Actions may miss matched events from the third-party technology. Additional hosts values helps ensure the likelihood of a match between the two environments.

12. Optional: Expand **Advanced options** and update the information as necessary.

a. Update **Query Time** and **Delay Time**.

> The **Query time** is the amount of time (minutes) before and after the query runs that the platform looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the first query after a Job Action starts. For example, you configure your integration with the following values: **Query time** = 5, **Query interval** = 30 seconds, and **Delay time** = 0. When a Job Actions starts at 12:00:00, the first time the query runs, the platform looks for events from 11:55:00 to 12:00:00. Then 30 seconds later, it looks for events from 11:55:30 to 12:00:30. This interval continues, with the last query looking from 12:00:00 to 12:05:00. If you instead configured the **Delay time** to equal 10, it would run the same query, but it wouldn't start that query until 12:10:00.

> If your monitors are set to run more frequently than the query time, this configuration impacts the pass/fail results for AEDA monitors.

b. Update **Query Interval** (seconds).
c. Configure correlation queries:
   i. Select **Correlation Query Enabled** and fill in the **Correlation Query**.
   ii. Modify the **Correlation Query Interval**, if necessary (minutes).
d. Select **Discover network devices automatically**, the default and recommended option.

> If unselected, reported events won't include product information for any matching network security technology.

e. Select **Save Suspicious Events**.
f. Modify the **Event Time Adjustment** (seconds). The default is **0**.
g. Modify the **Limit** value if you need to prevent a flood of results. This value is set to **10000** by default. This limit applies to both events and alerts individually, so if you set it to **10**, you can still see a maximum of 10 events and 10 alerts.

13. Click **Save**.

Verify connectivity

1. Go to **Settings > Integrations**.
2. From the Direct Integrations table, click ⋮ **> Test** to verify that:
   - The Director can communicate with the integration host on the port and protocol specified.
   - The integration credentials are valid and working.

For more information on setting up queries, see **Manage Integrations** (https://docs.mandiant.com/home/msv-managing-integrations).

Configure Legacy Integration

> 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)**.

To configure an integration, this document walks you through the following high-level steps:

1. Configure the third-party technology
2. Configure Security Validation
3. Verify connectivity

Update CrowdStrike

API Calls

API	Usage
`/detects/queries/detects/v1`	Query detections from Crowdstrike
`/detects/entities/summaries/GET/v1`	Retrieve detailed information about detections from Crowdstrike
`/oauth2/token`	Retrieve an OAuth2 Token

Depending on your type of account, you use a specific host to access the API. Apply the relevant subdomain based upon where your account resides:

- US-1: `api.crowdstrike.com` (default)
- US-2: `api.us-2.crowdstrike.com`
- US-GOV-1: `api.laggar.gcw.crowdstrike.com`
- EU-1: `api.eu-1.crowdstrike.com`

To configure this integration, you need the following:

- A Username or Client ID
- An API Key (also referred to as a Client Secret)

Get a Client ID and API Key from Falcon

To generate a Crowdstrike Client ID and API Key, you must have the Falcon Administrator role. API Keys are only displayed when a new API Client is created or when the API Key is reset.

1. Log into the Falcon web interface.
2. Navigate to **Support** > **API Clients** and then click **Keys**.
3. Click **Add new API Client** and fill out the dialog that appears.
4. After clicking **Add**. make note of the Client ID and API Key (Client Secret) values that are displayed.

Configure Security Validation

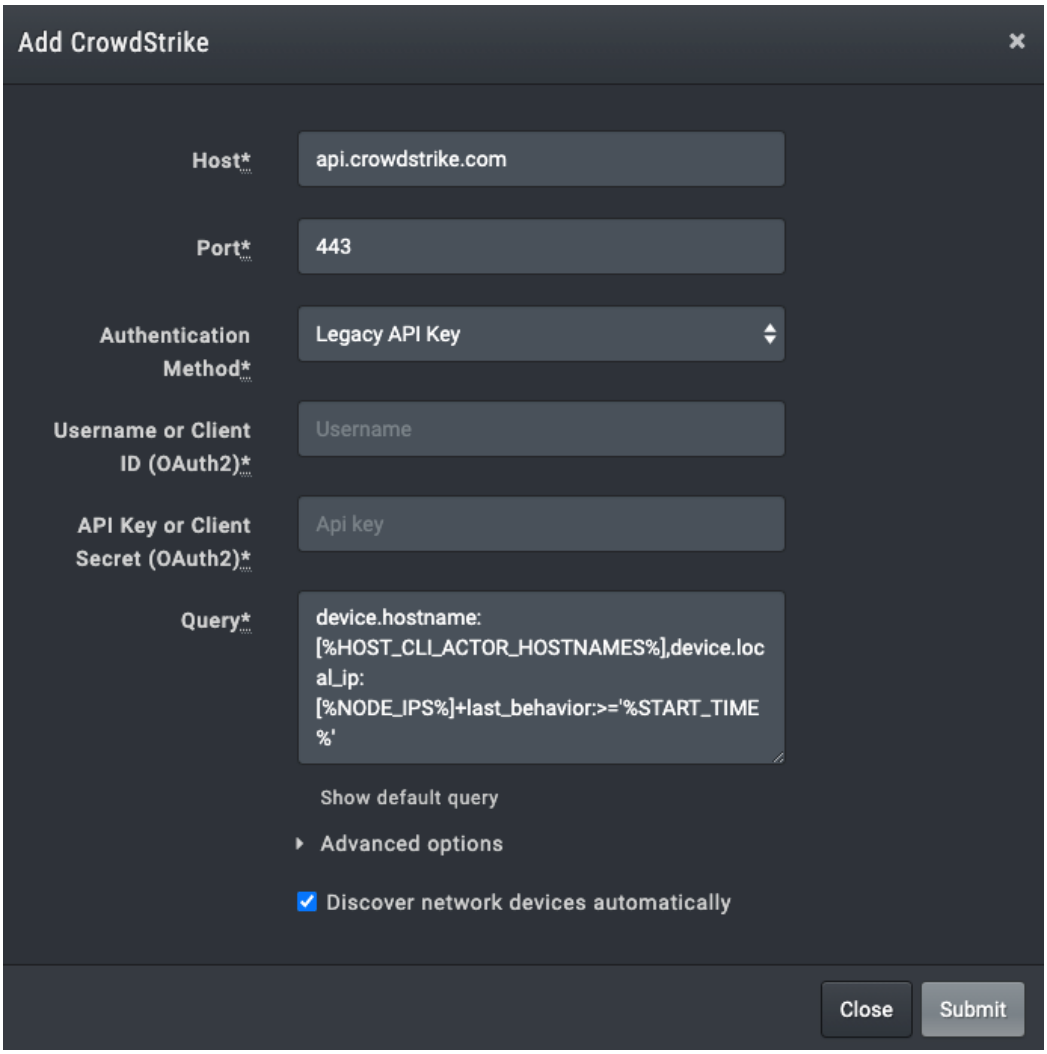
Prerequisites

Information to gather before you start:

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

Configuration

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

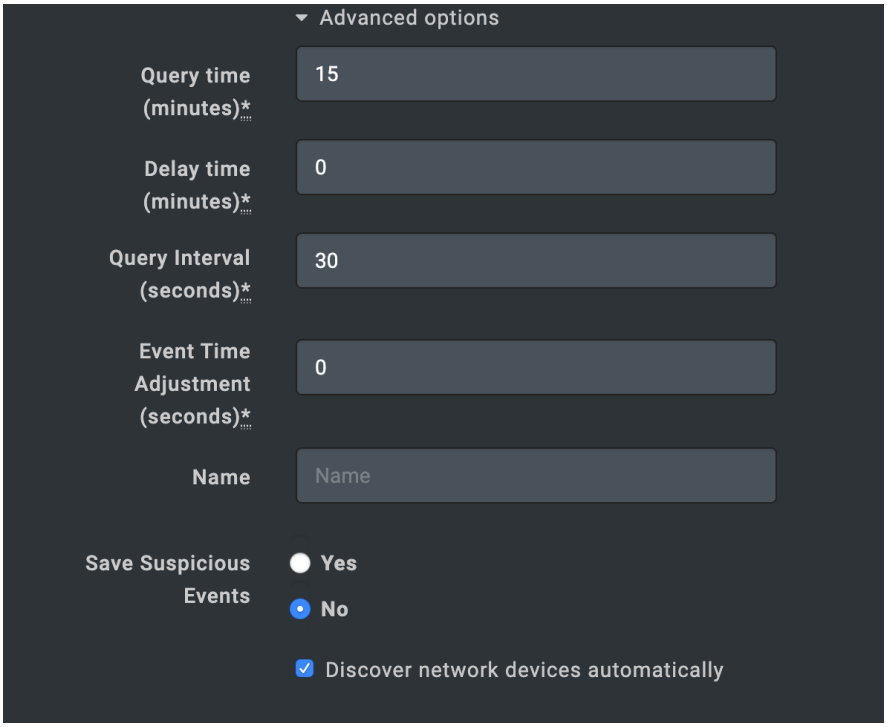


CrowdStrike Integration

> 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

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