Crowdstrike Falcon getting started guide

Version 2.0

February 27, 2020

www.expel.io

What's in this guide?

Howdy! In this guide, you'll find instructions on how to:

1. Enable and configure console access for the Expel Security Operations Center (SOC);
2. Enable the Legacy Application Program Interface (API) Credentials;
3. Enable the OAUTH2 API; and
4. Configure Crowdstrike Falcon in Expel Workbench™.

Step 1 — Enable console access

Having read-only access to the interface of your technology allows Expel to dig deeper when performing incident investigations. Our device health team uses this access to investigate potential health issues with your tech.

Expel is a Crowdstrike Certified Managed Security Provider partner. In order to allow the Expel partner console access to your console, you need to do the following:

A. Print, complete and sign the **Crowdstrike MSP Authorization Form** (usually supplied with this guide, or request this from an Expel Customer Success Engineer)

B. Create a CrowdStrike support ticket, attaching the completed form

Step 2 — Enable the Legacy API

In order to integrate the technology with Expel, we need to create secure credentials to the API. Depending on the permissions allowed in *Step 1* above, Expel may be able to generate API credentials. If you are unsure, please reach out to your Expel *Customer Success Engineer*, or email customerhealth@expel.io.

CrowdStrike currently uses two separate API methods (Legacy API and OAuth2 API). Both APIs offer different information that provide excellent information for our service.

In order to enable the **Legacy API**, please follow the steps below:

A. Create a Crowdstrike support ticket requesting them to enable the Legacy API and to provide the API credentials

B. Crowdstrike will supply these credentials to you

C. See *Step 4* below to enter these credentials into Workbench

Step 3 — Enabling the OAuth2 API

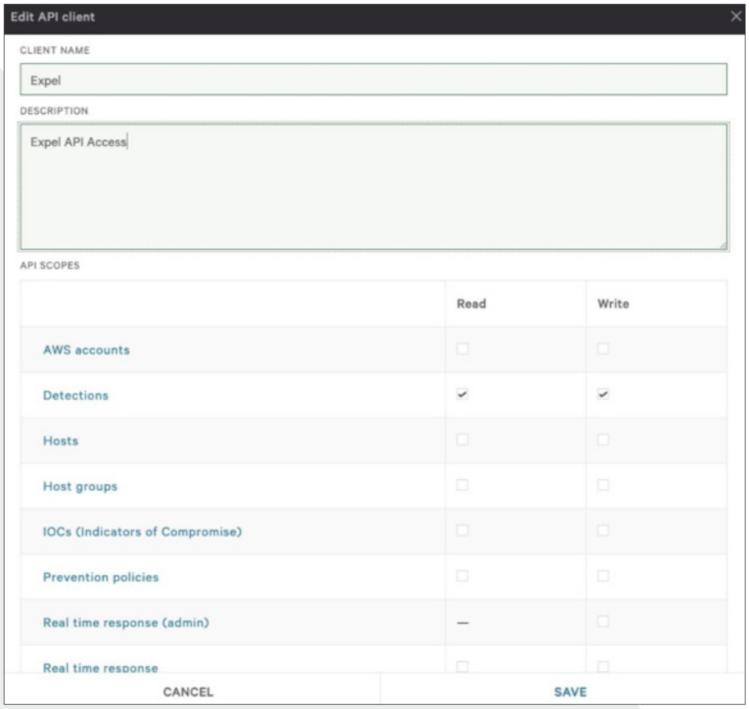
CrowdStrike currently uses two separate API methods (Legacy API and OAUth2API). Both APIs offer different information that provide excellent information for our service.

In order to enable the **OAuth2 API**, please follow the steps below:

A. When logged into the Falcon UI, navigate to **Support > API Clients and Keys**

B. Select **Add new API Client**

C. Enter **Expel** as the **Client Name** (See Figure 1 for *Steps C-F*)



Edit API client

CLIENT NAME

Expel

DESCRIPTION

Expel API Access

API SCOPES

	Read	Write
AWS accounts	□	□
Detections	☑	☑
Hosts	□	□
Host groups	□	□
IOCs (Indicators of Compromise)	□	□
Prevention policies	□	□
Real time response (admin)	—	□
Real time response	□	□

Figure 1

D. Enter **Expel API Access** as the **Description**

E. Select both **Read** and **Write** for **Detections**

F. Click **Save**

G. **Make a record of your Client ID and the Client Secret for the API**

H. Proceed to *Step 4* below to enter these credentials into Workbench

Step 4 — Configure the technology in Workbench

Now that we have all the correct access configured and have noted the credentials, we can integrate CrowdStrike Falcon with Expel.

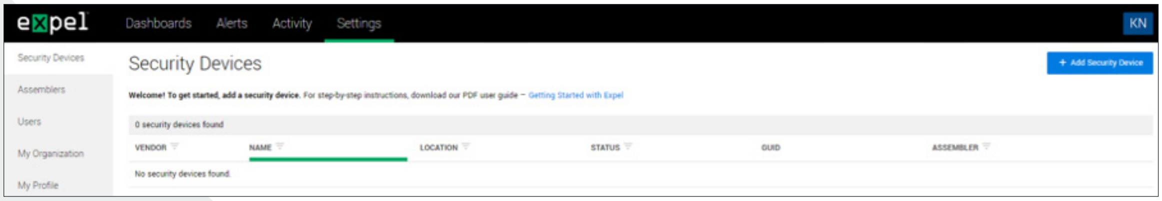
Register device in Expel Workbench

A. Login into https://workbench.expel.io

B. Enter Security Code from Google Authenticator (two-factor authentication)

C. On the console page, navigate to **Settings** and click **Security Devices**

D. At the top right of the page, select **Add Security Device** (Figure 2)



Security Devices

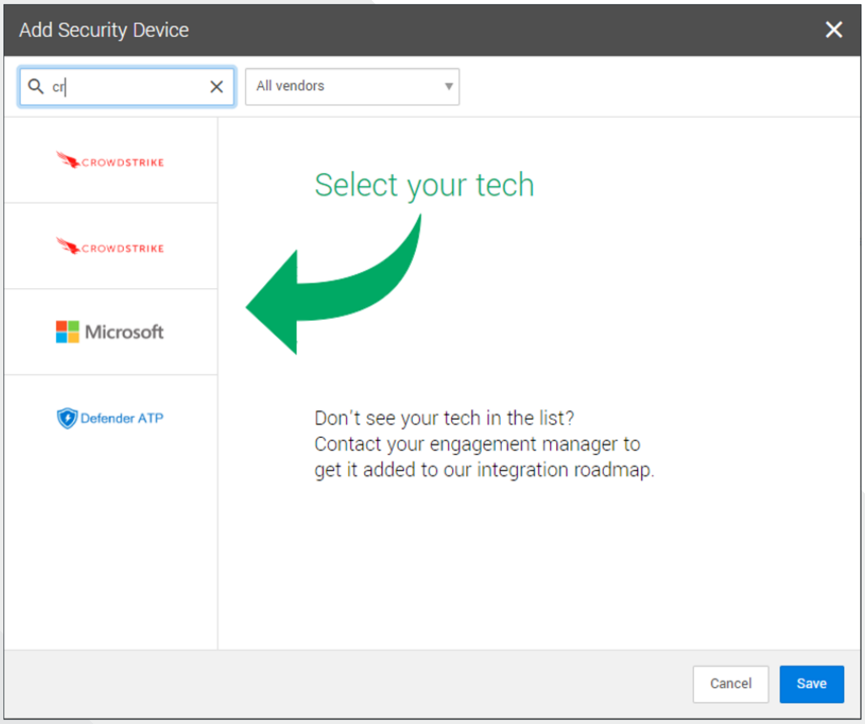
Welcome! To get started, add a security device. For step-by-step instructions, download our PDF user guide – Getting Started with Expel

0 security devices found

VENDOR	NAME	LOCATION	STATUS	GUID	ASSEMBLER
No security devices found.					

Figure 2

E. Search for and select **CrowdStrike Falcon** (Not 'Data Replicator'!). See Figure 3



Don't see your tech in the list?
Contact your engagement manager to
get it added to our integration roadmap.

Figure 3

F. Select an **Assembler** from the drop down (Choose the **Assembler** you set up in *Step 2* of the Getting Started with Expel guide). See Figure 4 for *Steps F-H*

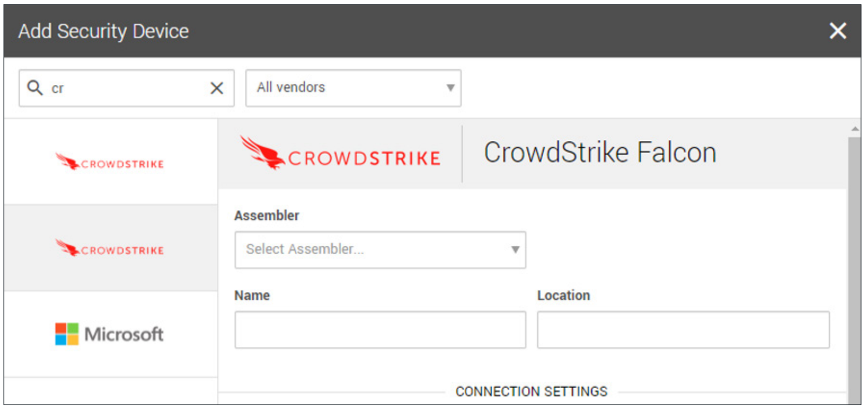


Figure 4

G. For **Name** enter the hostname of the device

H. For **Location** enter the geographic location of the appliance

I. After entering the name and location, complete the remaining fields using the credentials and information you collected in *Steps 2 or 3* above. See Figure 5

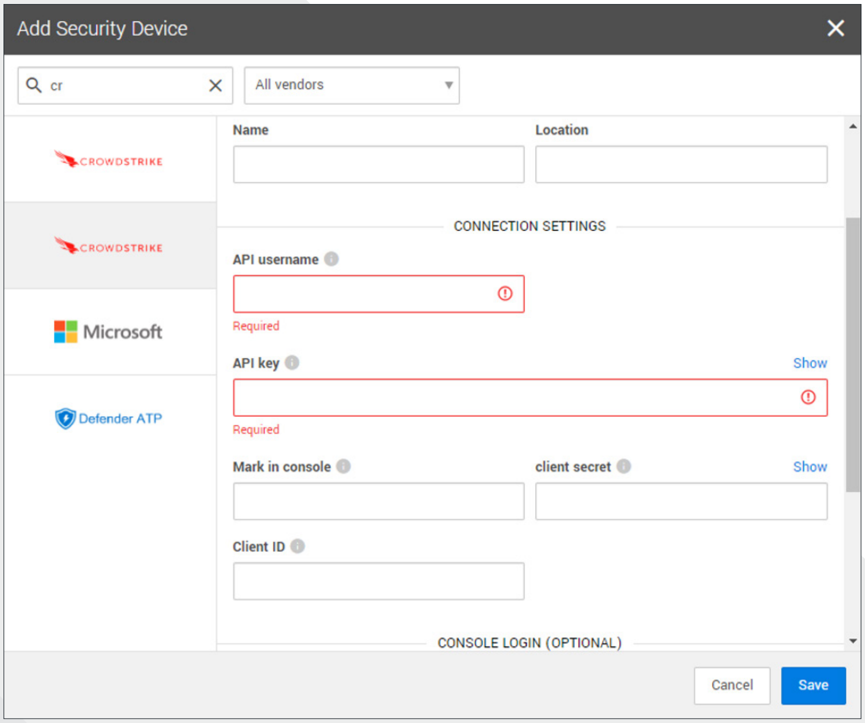


Figure 5

J. If using Legacy API, for **API username**, enter the credentials obtained in *Step 2*

K. If using Legacy API, for For **API key**, enter the credentials obtained in *Step 2*

L. For **Mark in console**, enter **y = yes** to mark the events on the console to in progress status

M. If using OAuth2 API, for **client secret**, enter the secret from *Step 3, letter G*

N. If using OAuth2 API, for **Client ID**, enter the ID from *Step 3, letter G*

O. Select **Save**

P. After a few minutes, refresh the **Security Devices** page and you should see your device status reporting as *Healthy*, or if there is an issue, it will provide more details of what the issue may be

Q. To check and see if alerts are coming through, navigate to **Alerts** on the console page. Click the icon in the upper right to switch to grid view, then check the list for Crowdstrike Falcon alerts

That's it! Give yourself a pat on the back — you're done!

If you have any issues, concerns, questions or feedback,
please don't hesitate to contact Expel at devicehealth@expel.io.