Carbon Black ThreatHunter getting started guide

Version 2.0

February 18, 2020

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. Generate the Application Program Interface (API) Credentials; and
3. Configure Carbon Black ThreatHunter (CBTH) 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.

This procedure will create a user account for Expel that will keep Expel's activity separate from other activity on the CBTH console.

Create an analyst account

A. Navigate to gear icon on left-hand side and click **Users** (Figure 1); then click **Add User** on the top right of the screen

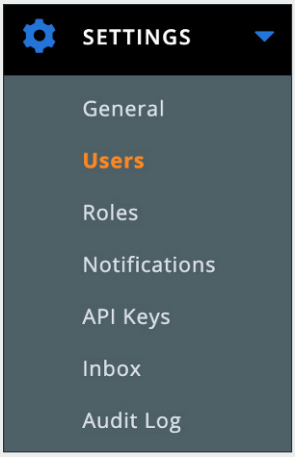

Figure 1

B. For **First name** enter *Expel* (See Figure 2 for *Steps B-F*)

C. For **Last name** enter *SOC*

D. For **Email** enter *soc+<client name>@expel.io*

E. For **Role** select *Level 2 Analyst*

F. Click **Save**

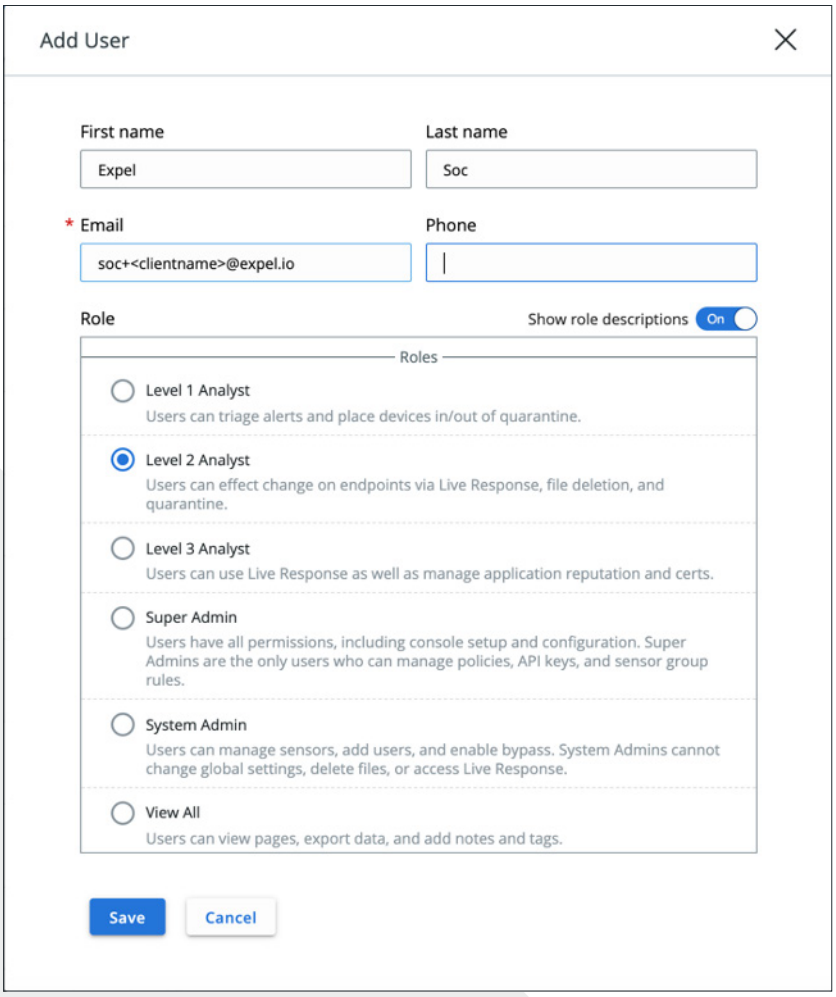

Figure 2

Step 2 — Generate API credentials

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.

Generate an API Key with 'view all' permissions

A. In the CBTH console, navigate to **Settings > Roles** (Figure 3)

B. Verify that a **View All** role exists. (This should be included by default) To enable the quarantine action follow *Steps B.a* through *B.e*, or else continue to *Step C*

a. Click the **Add Role** button to create a new role (see Figure 3 for *Steps Ba & Bb*)

b. Fill out name and description (we suggest the name be **Expel Custom Role**)

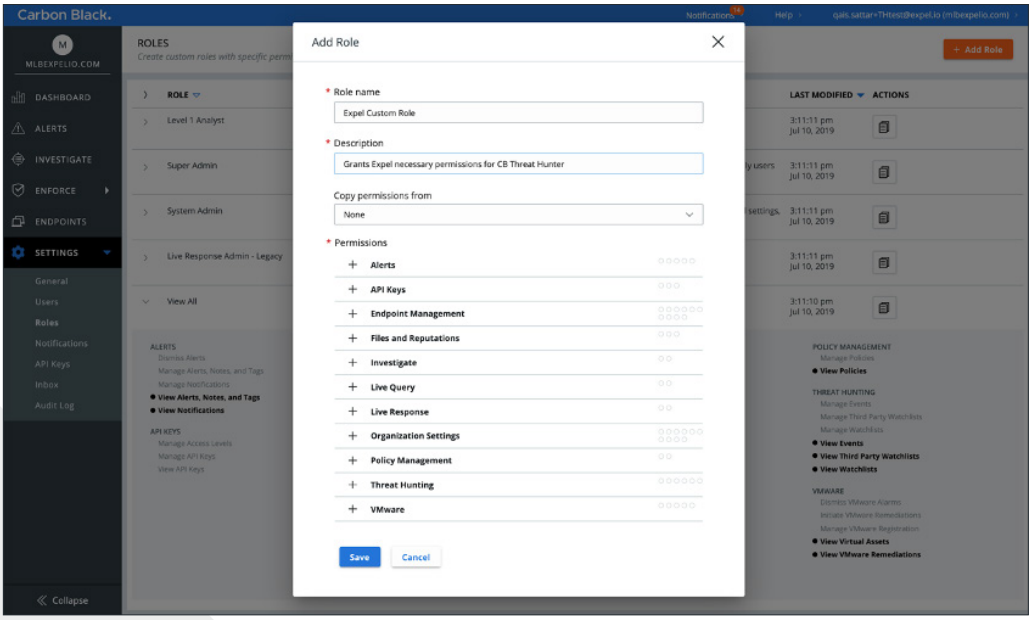

Figure 3

c. Under the **Copy Permissions** from drop down select the **View All** role (Figure 4)

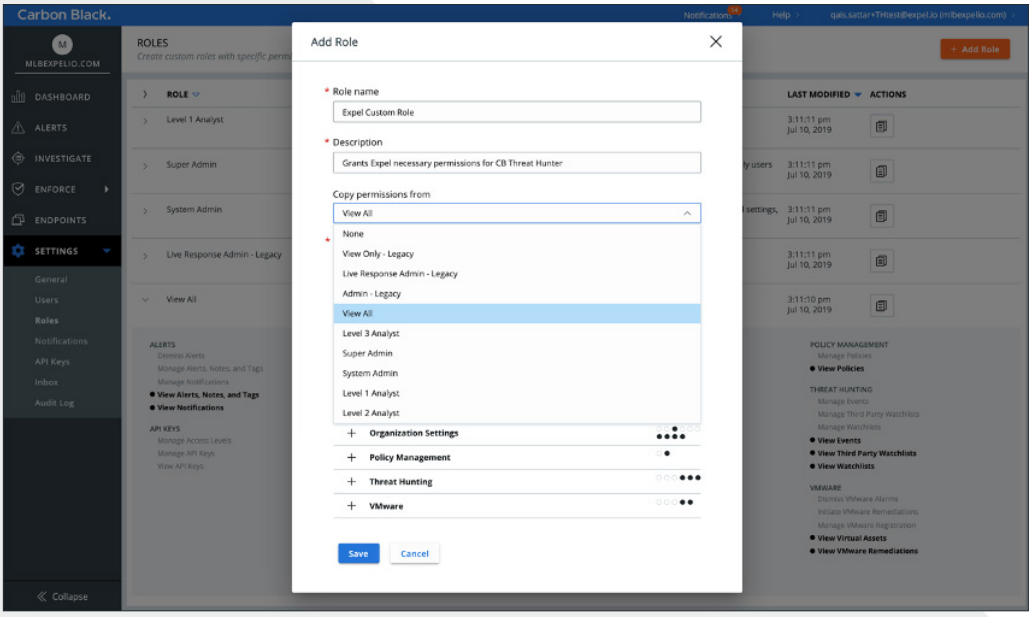

Figure 4

d. Add **Export device data, Quarantine, & View devices and sensor groups** permissions located in the Permission section under **Endpoint Management** (Figure 5)

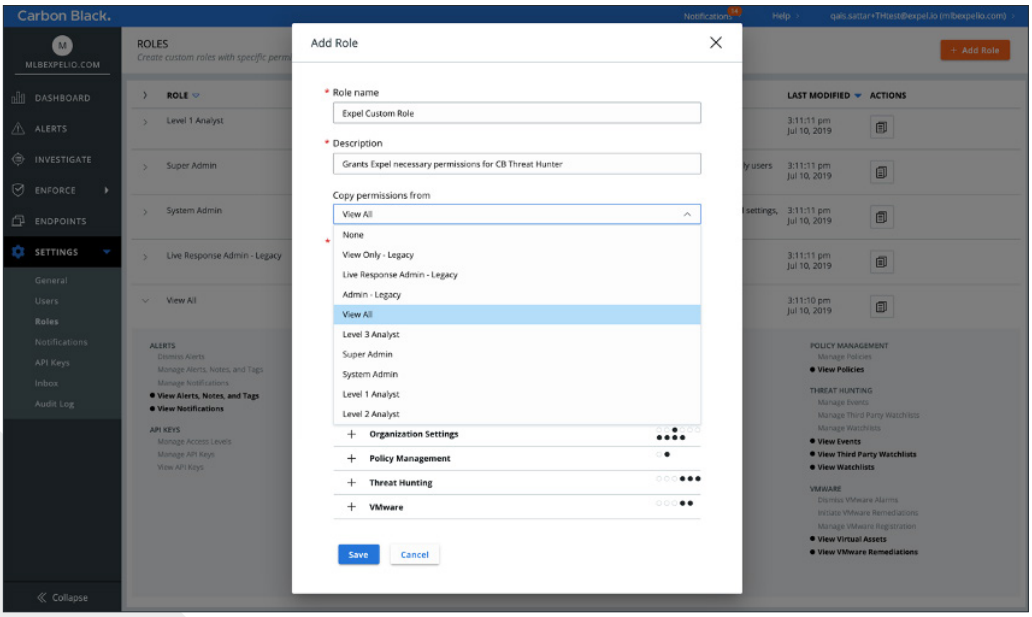

Figure 5

e. Add **Manage Events, View Events, View Third Party Watchlists & View Watchlists** permissions located in the Permission section under **Threat Hunting** (Figure 6)

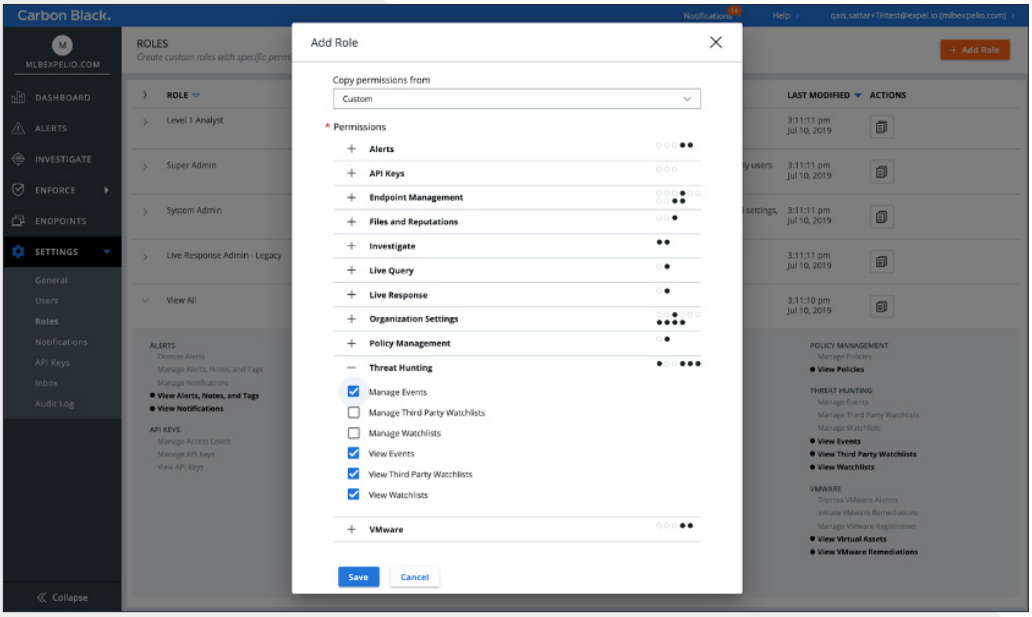

Figure 6

C. Navigate to **Settings > API Keys** (Figure 7)

D. Create a new API key by selecting **Add API Key** found in the upper right corner (Figure 7)

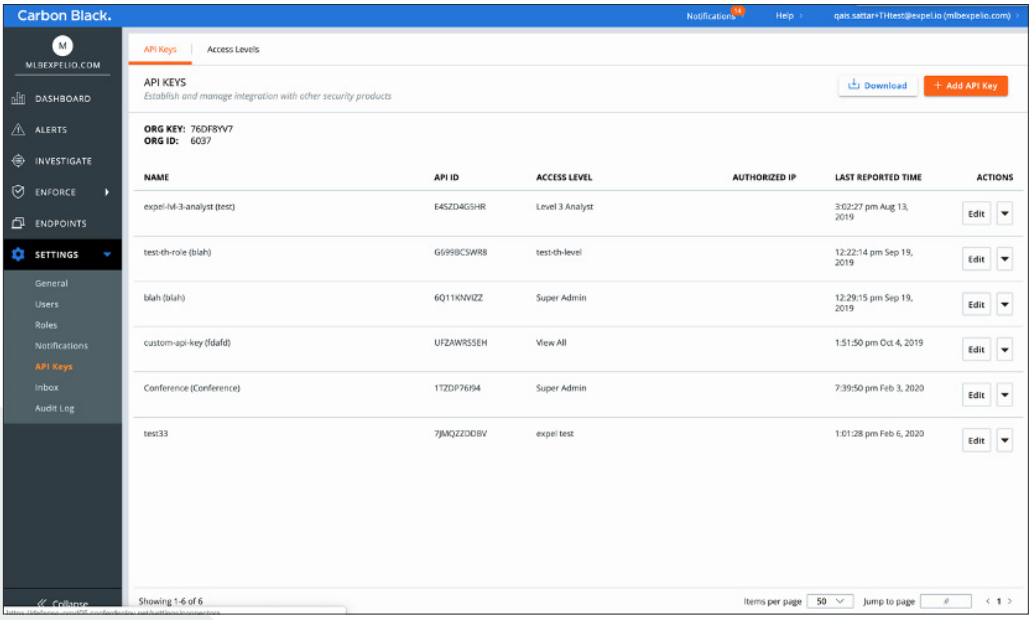

Figure 7

E. Enter a name for the new key (Anything will work, but we'd suggest **Expel SOC**). See Figure 8

F. Under the **Access Leve**l drop down list, select Custom (Figure 8)

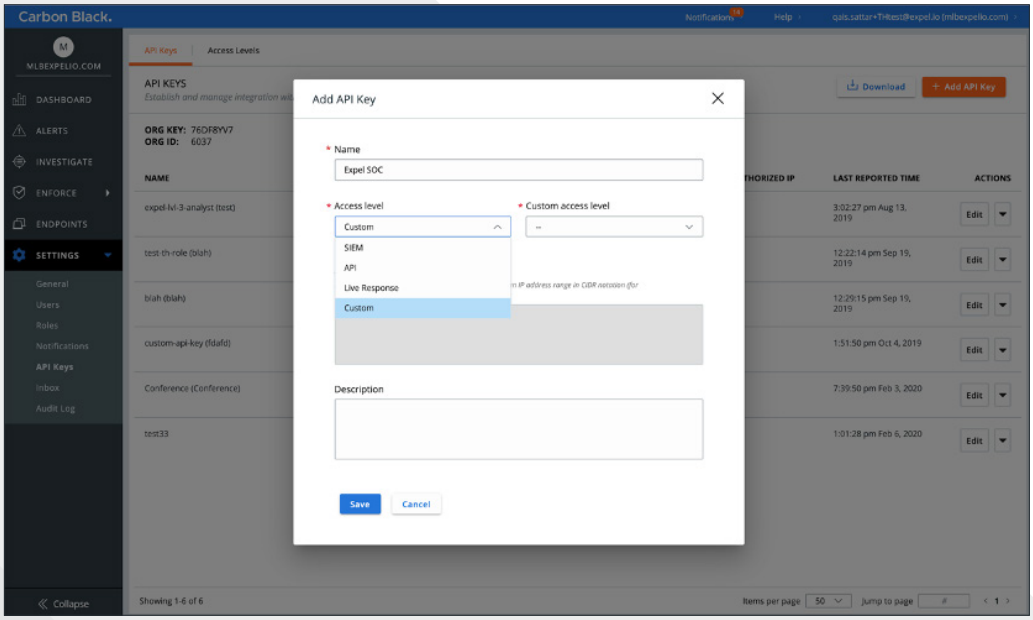

Figure 8

G. Under the **Custom Access Level** drop down list, select the either the **View All** role or the role created in *Step Ba* (Figure 9)

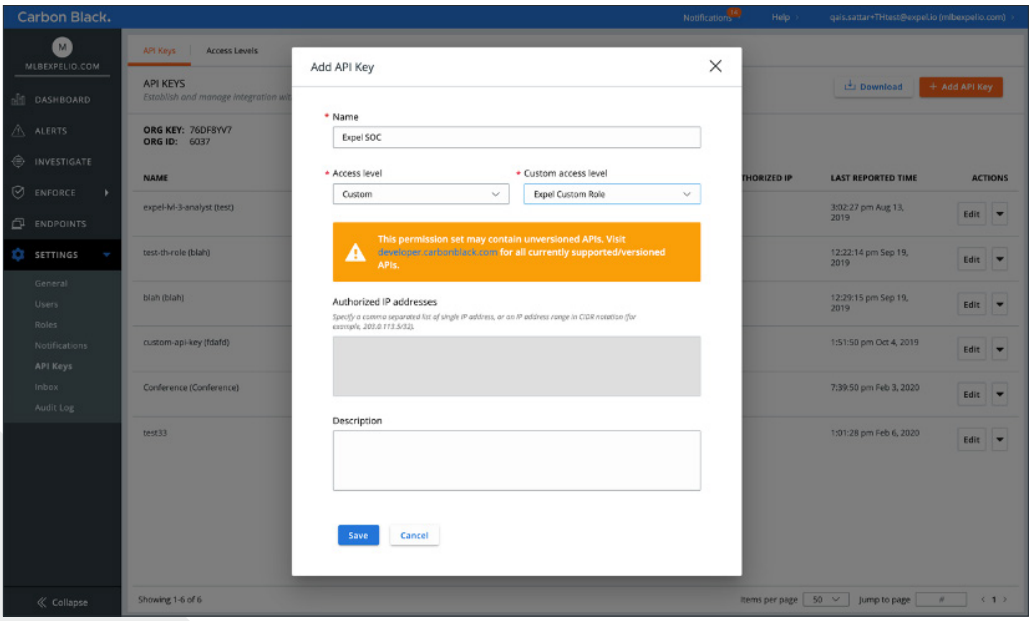

Figure 9

H. Complete the rest of the information and click **Save** to create the new key

I. Make a record of the **API ID** and **API Secret Key** for later

Step 3 — Configure the technology in Workbench

Now that we have all the correct access configured and have noted the credentials, we can integrate Carbon Black ThreatHunter with Expel.

Register device in Expel Workbench

A. In a new browser tab, login to 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 10)

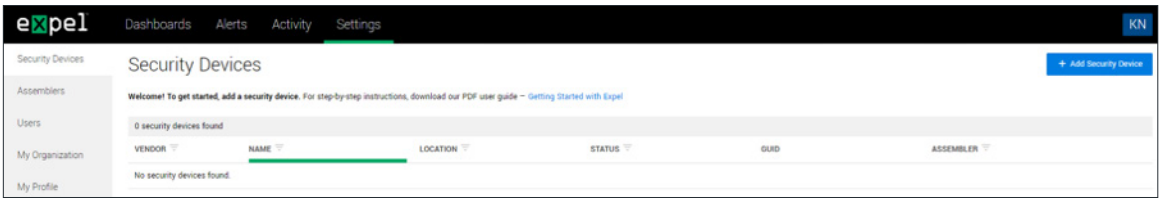

Figure 10

E. Search for and select CB ThreatHunter (Figure 11)

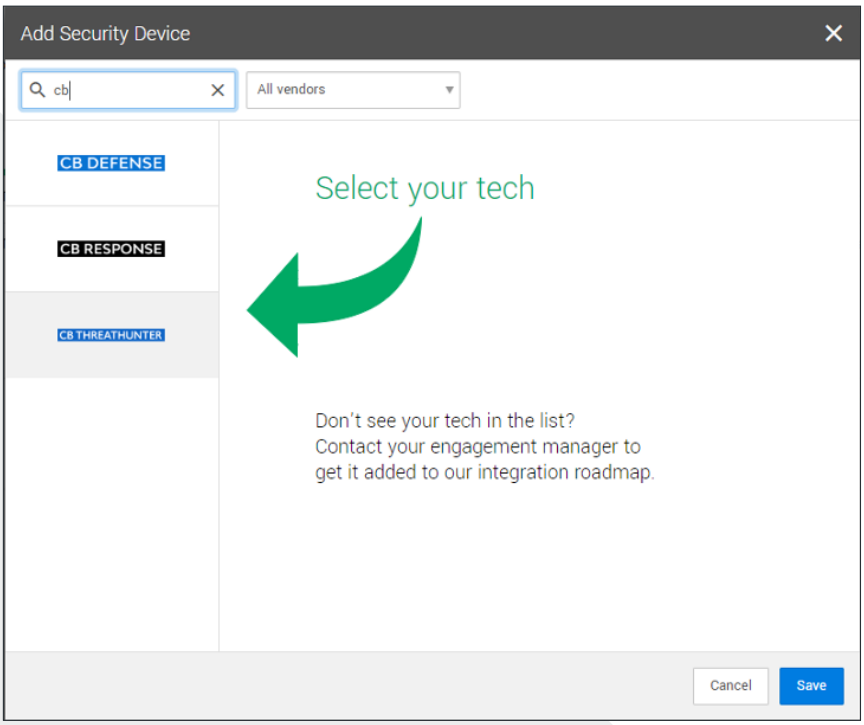

Figure 11

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 12 for *Steps F-H*

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

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

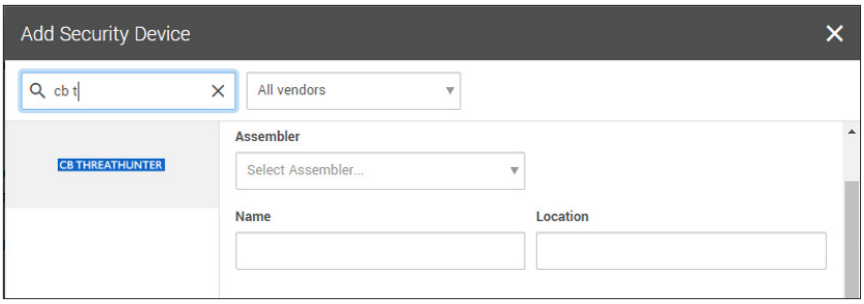

Figure 12

I. Refer to Figure 13 for *Steps J-O*

J. For **Org Key**, enter the Org Key (from the upper left hand corner of figure 7)

K. For **Org ID**, enter your CB Organization ID which can be found in the upper left hand corner of Figure 7

L. For **Server Address**, enter the CBTH server address (which is usually https://defense-prod05.conferdeploy.net/)

M. For **API ID** enter the API ID created in *Step 2, letter I*

N. For **API Key**, enter the API Secret Key created in *Step 2, Letter I*

O. Select **Save**

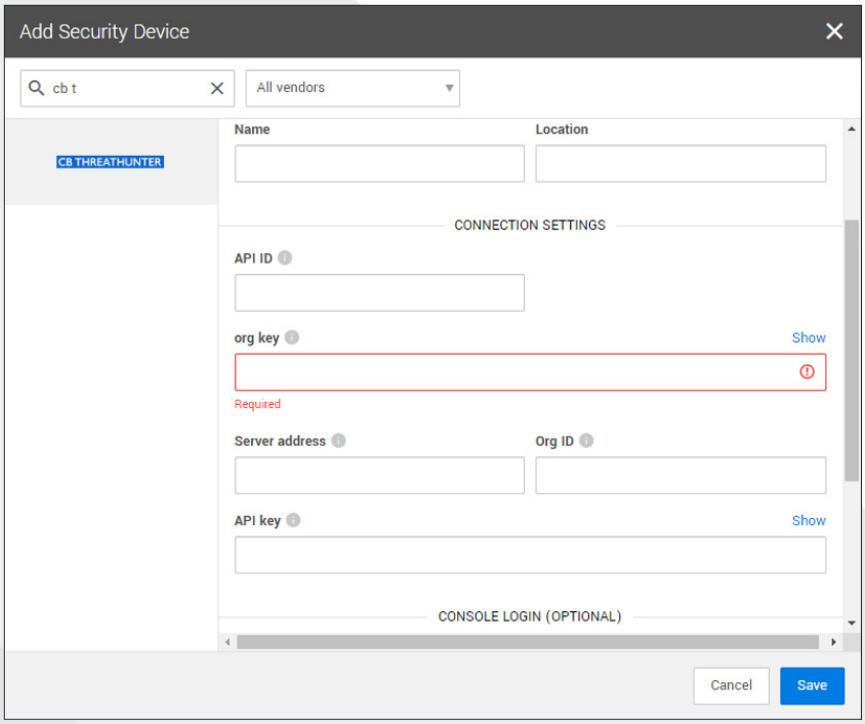

Figure 13

P. After a few minutes (1–10 min), 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. The device should be active in Expel Workbench within 30 minutes

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 CB ThreatHunter 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.