Carbon Black Defense getting started guide

Version 2.0

January 29, 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 CB Defense 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 CB Defense 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

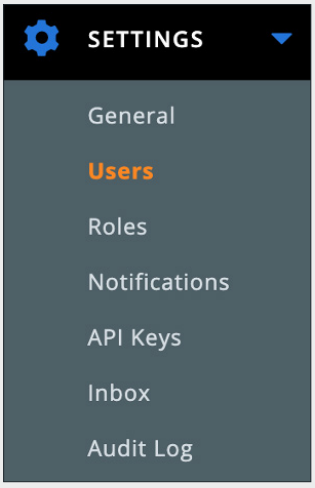

Figure 1

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**

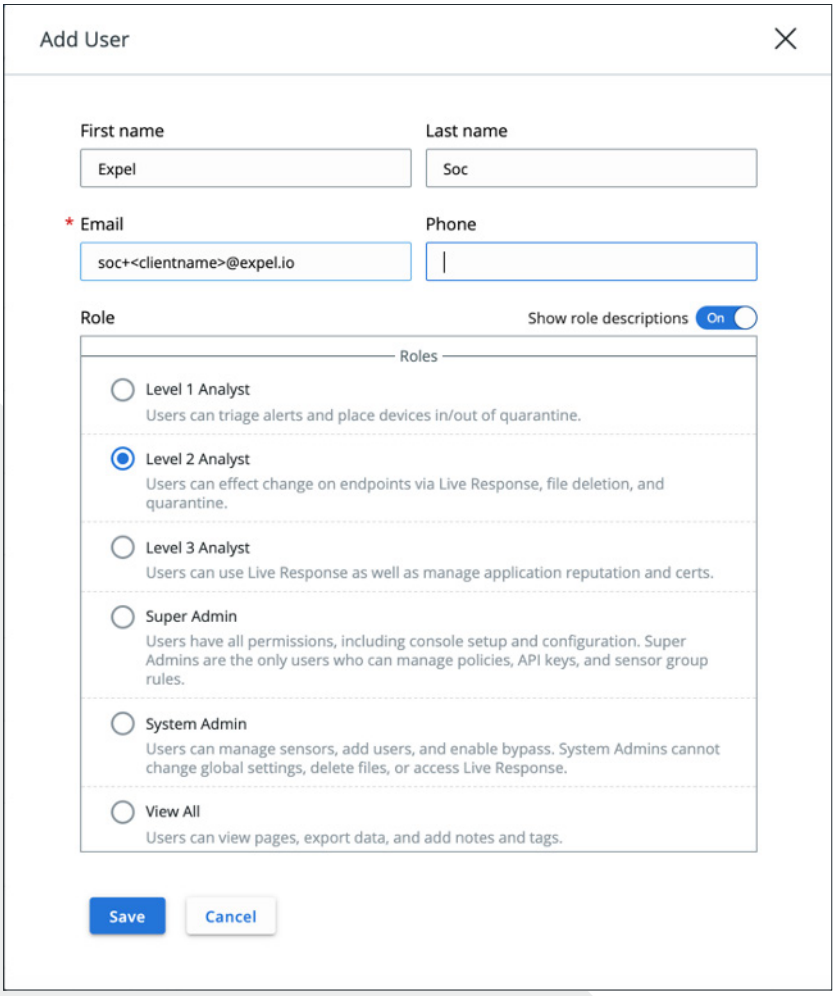

Figure 2

Step 2 — Generate API credentials and SIEM access

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.

This procedure will create an authentication token that allows the Expel Assembler to access the CB Defense API and SIEM.

Obtain the API and SIEM key for the Expel account

A. Navigate to **gear icon** on left-hand side and click **API Keys** (Figure 3) then click **ADD API Keys**

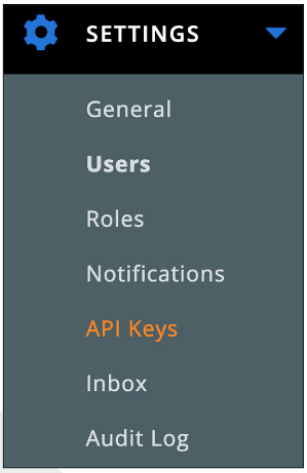

Figure 3

B. For **Name** enter *Expel* (see Figure 4 for *Steps B-F*)

C. For **Access Level** select *API*

D. For **Authorized IP** address enter the IP address of the externally facing IP of the Expel Assembler. If you are unsure, the following curl can be run on the Assembler to list the current IP:
curl -s http://ipchicken.com | egrep -o '([[:digit:]]{1,3}\.){3}[[:digit:]]{1,3}'

E. Click **Save**

F. For SIEM access follow the same *Steps B-E* above and select *SIEM* for **Access level**

G. Make note of the API, SIEM API and API IDs for each which will be used in *Step 3* for registration within Expel Workbench

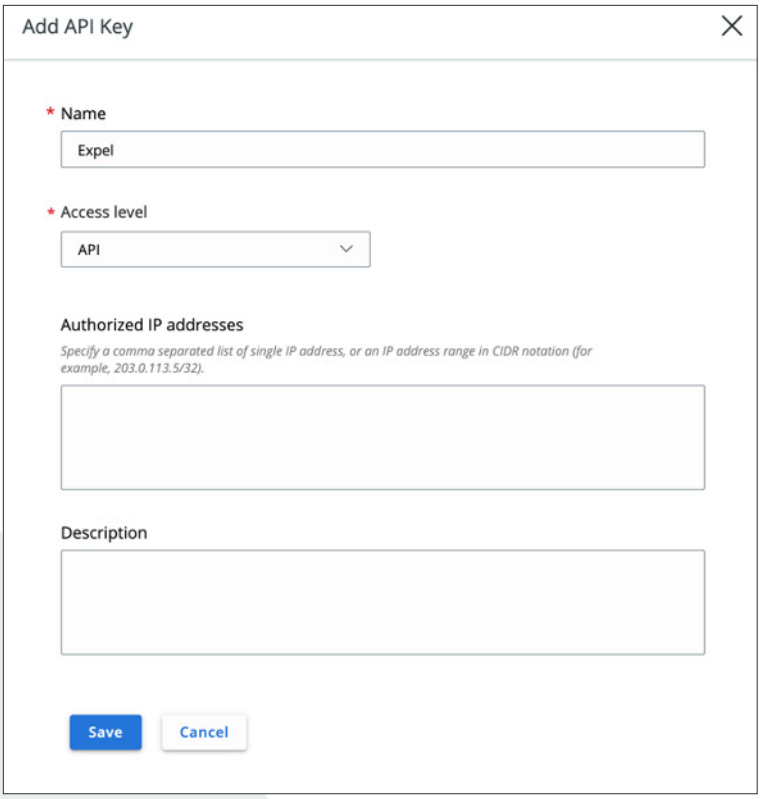

Figure 4

Subscribe to notifications

H. Navigate to **gear icon** on left-hand side and click **Notifications** then click **ADD NOTIFICATION**

I. For **Name** enter *Expel Threat* (see Figure 5 for *Steps I-M*)

J. For **Notify when** select *Threat* and select **Alert priority 3**

K. For **Policy** select *All Policies*

L. Click in **Search for API** box and search for the SIEM API Key created for Expel earlier in *Step F*

M. Click **Save**

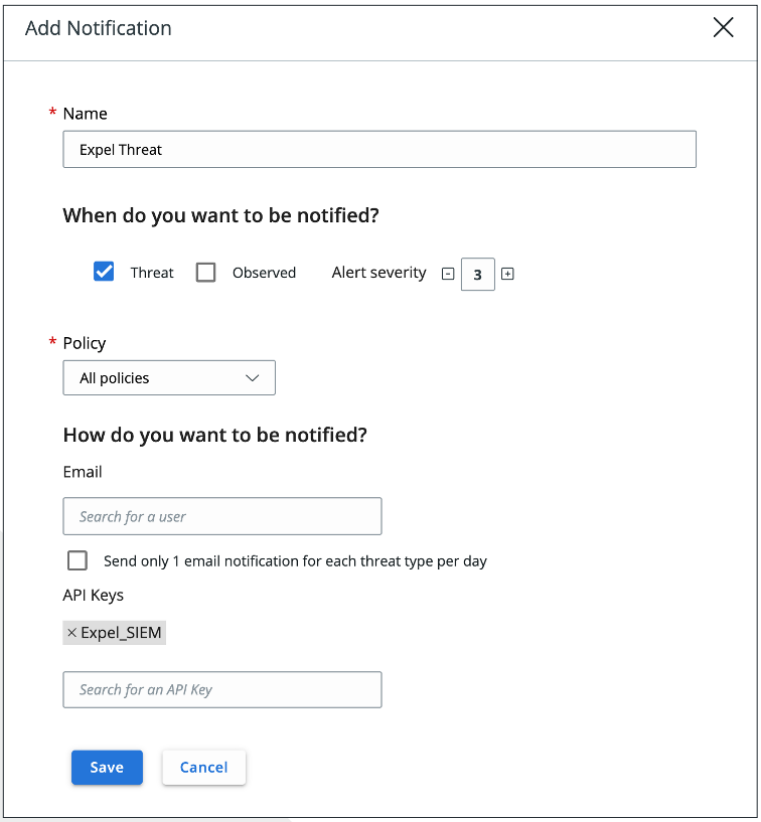

Figure 5

Step 3 — Configure the technology in Workbench

Now that we have all the correct access configured and have noted the credentials, we can integrate CB Defense 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**

E. Search for and select CB Defense (Figure 6)

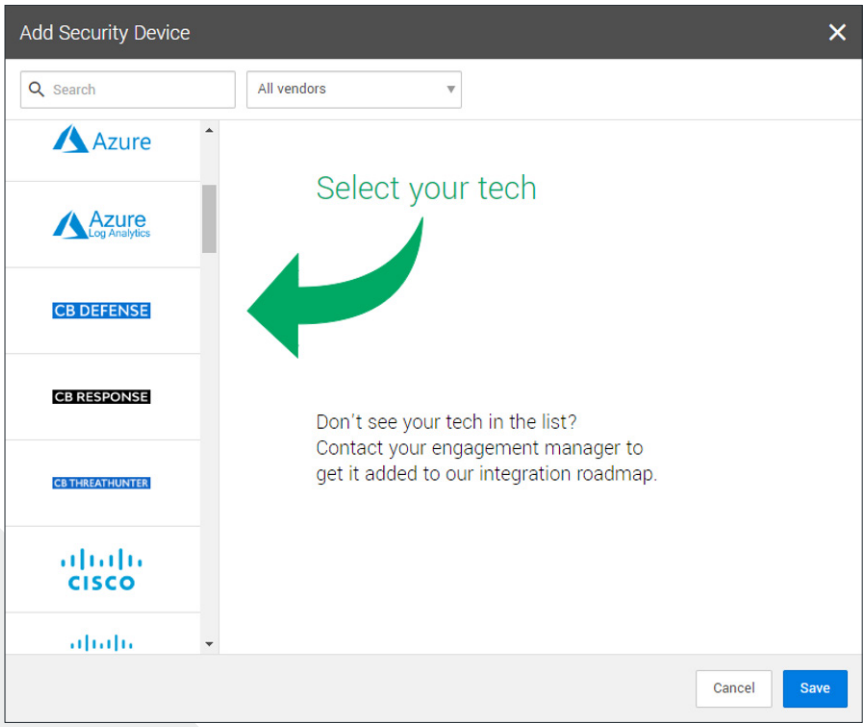

Figure 6

F. Complete all fields using the credentials and information you collected in *Step 1* and *Step 2* above (Figures 7 & 8)

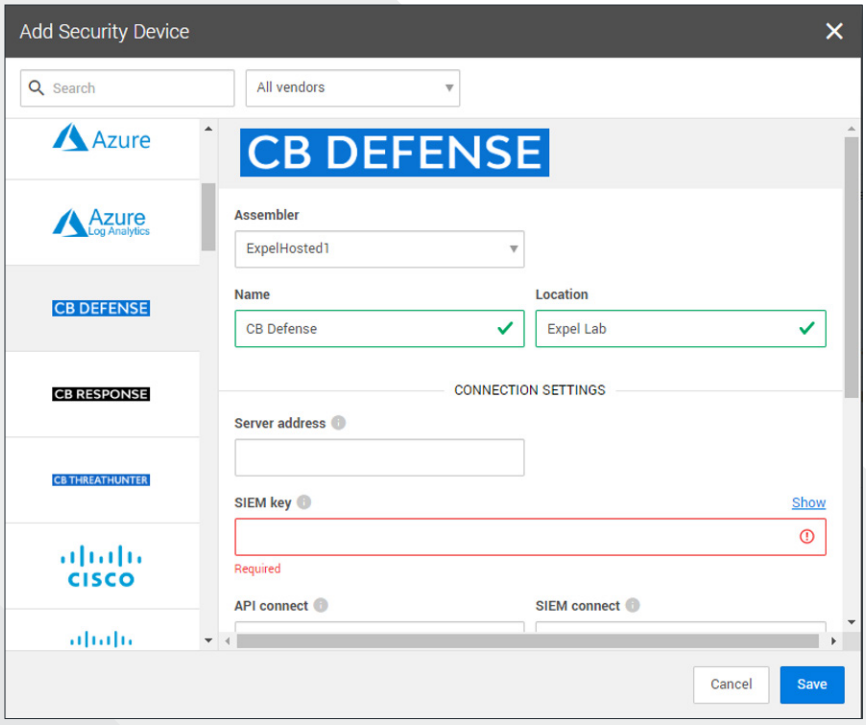

Figure 7

G. Select an **Assembler** from the drop down (Choose the **Assembler** you set up in *Step 2* of the Getting Started with Expel guide)

H. Enter Assembler Name and Location (example: *CB Defense and Expel Lab*)

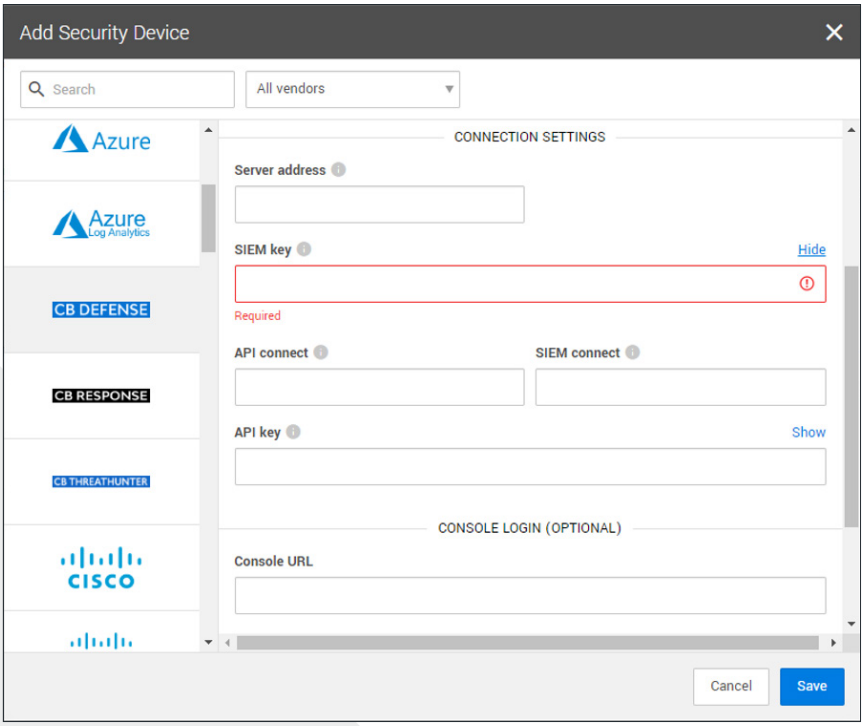

Figure 8

I. For **Server address** enter the url for the Cb Defense server, including the port

J. For **SIEM key**, enter the SIEM API Key generated in *Step 2*

K. For **API connect**, enter API ID generated in *Step 2*

L. For **SIEM connect**, enter SIEM's API ID generated in *Step 2*

M. For **API key** enter the API generated in *Step 2*

N. **Username** and **Password** fields are optional and can be left blank

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 CB Defense 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.