Carbon Black Response getting started guide

Version 2.0

February 27, 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;
3. Enable threat feeds; and
4. Configure Carbon Black Response 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 Carbon Black Response console.

Create an admin account

A. Navigate to the **Users** icon on left-hand side panel and click **+Add User** (Figure 1)

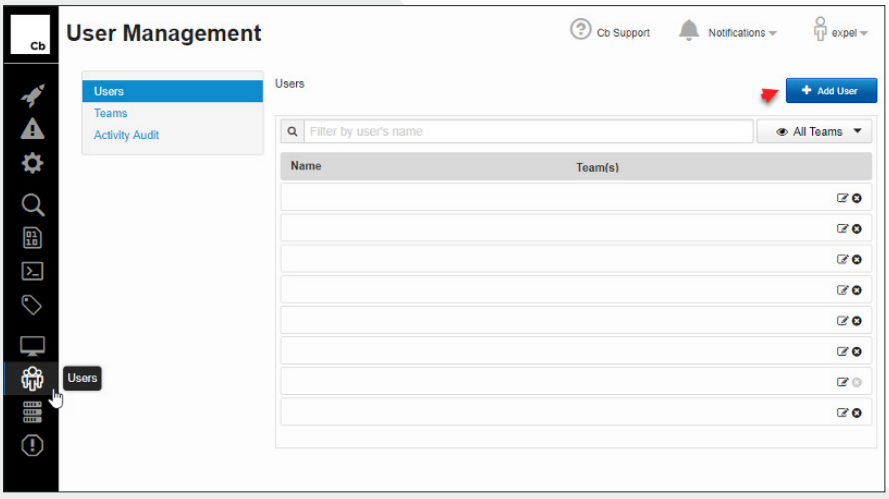

Figure 1

B. For **Username** add *expel* (Refer to Figure 2 for *Steps B-I*)

C. For **First Name** enter *Expel*

D. For **Last Name** enter *User*

E. For Email Address enter *soc@expel.io*

F. Enter the desired **Password**

G. **Assign to:** *Administrators*

H. Select the **Global administrator** checkbox (global administrator is required to perform the necessary functions within Carbon Black Response for pulling process listings, etc.)

I. Click **Save Changes**

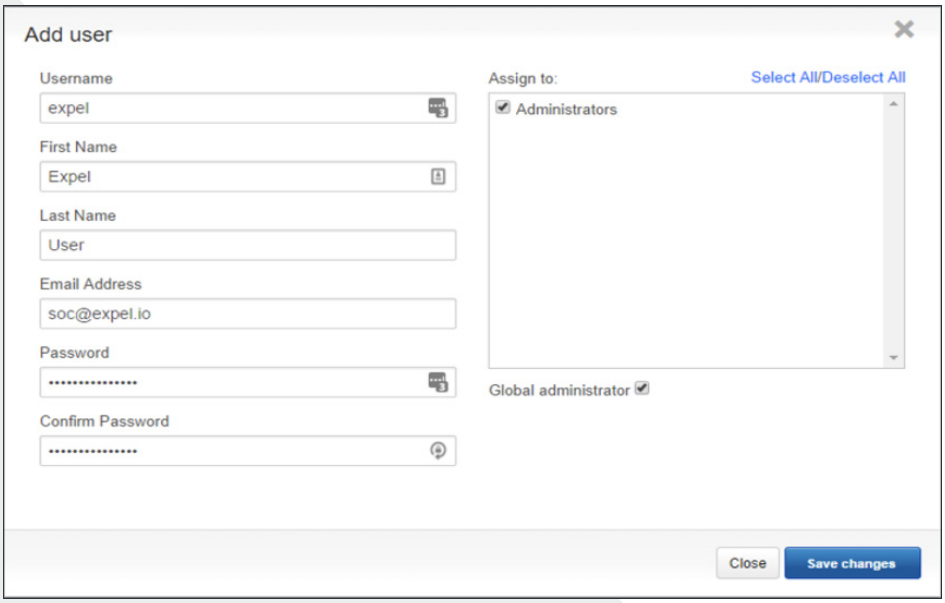

Figure 2

Verify Carbon Black Live Response is enabled

This allows Expel to interact with your endpoints (pull process listings, etc.).

J. Click on the **Sensors** icon on left-hand side panel and click any host name (Figure 3)

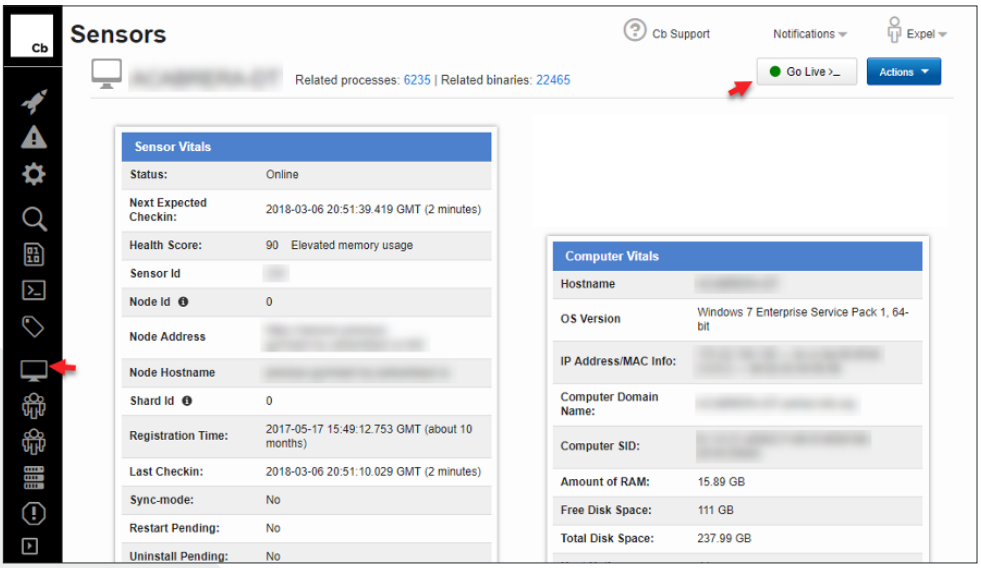

Figure 3

K. In the top-right corner, the button **Go Live** will be active if Carbon Black Live Response is enabled. If it is you are DONE!

L. If Carbon Black Live Response is **not enabled** and is **hosted on prem**:

   a. SSH into the CB appliance and perform the command "*vi /etc/cb/cb.conf*"

   b. Search for "*CbLREnabled=False*" and change the value from *False* to *True*

   c. Restart services for the change to take effect: "*service cb-enterprise restart*"

M. If Carbon Black Live Response is **not enabled** and **cloud-hosted**:

   a. You will need to submit a request to the Carbon Black Cloud Support team requesting this feature be enabled

   b. You can simply send the request with the following: "Please enable Live Response and VDI Behavior"

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.

This procedure will create an authentication token that allows the Expel Assembler to access the Carbon Black Response API.

Obtain the API Key for the Expel account

A. Log out of the Carbon Black Response Console

B. Log back into the Carbon Black Response Console, this time as the newly-created *Expel User*

C. Click **Expel User** on the top-right, then **My Profile**, then **API Token** (Figure 4)

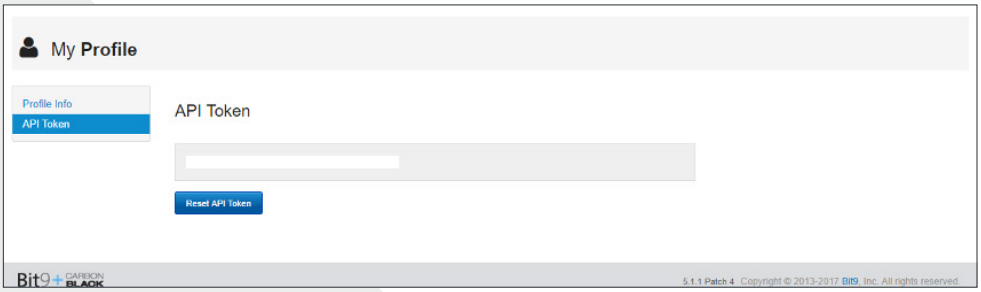

Figure 4

D. **Make note of the API token** which will be used next for registration within Expel Workbench

Step 3 — Enable threat feeds

Expel recommends the following Carbon Black threat feeds be enabled at a **minimum**:

+ CB Advanced Threat
+ CB Community
+ CB Suspicious Feed
+ CB Tamper Detection
+ CB Early Access
+ SANS Feed
+ Expel (this feed will be added and enabled by Expel)

A. Navigate to the **Threat Intelligence** icon on left-hand side panel (Figure 5)

B. Select **Enable** and the **Create Alert** options for each of the feeds referenced above (Figure 5)

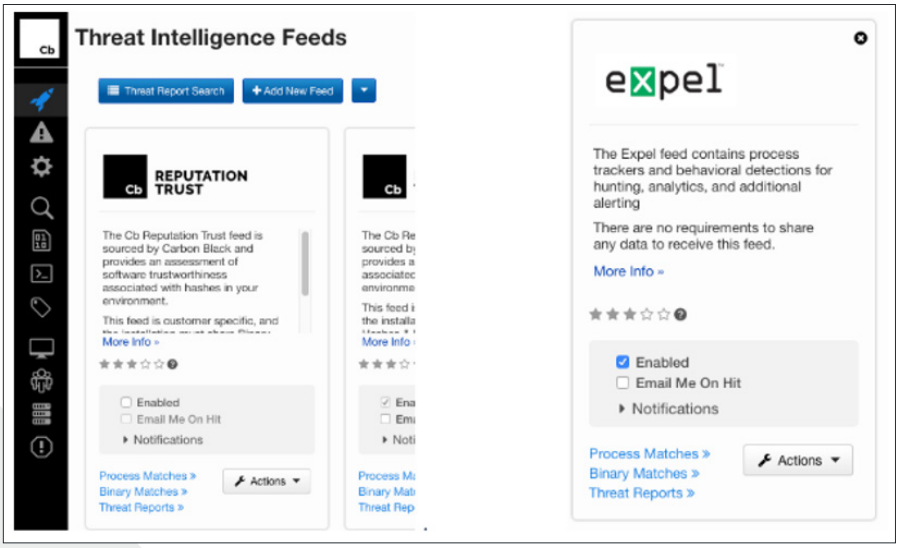

Figure 5

Step 4 — Configure the technology in Workbench

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

Register device in Expel Workbench

A. 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 6)

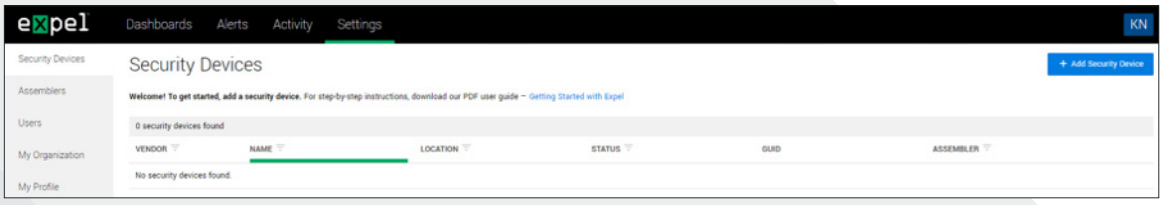

Figure 6

E. Search for and select **Carbon Black Response** (Figure 7)

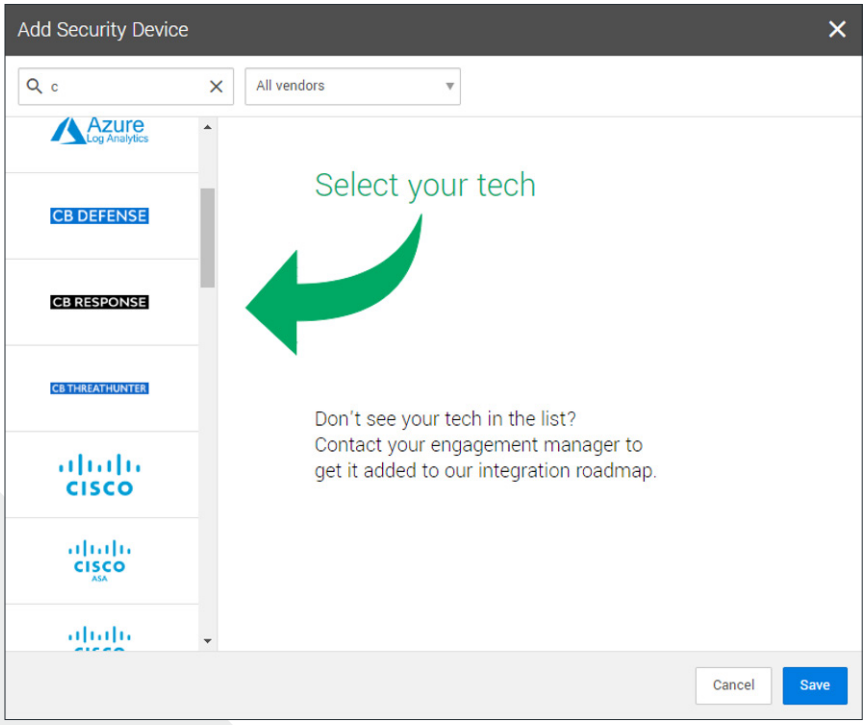

Figure 7

F. See Figure 8 for *Steps G-M*

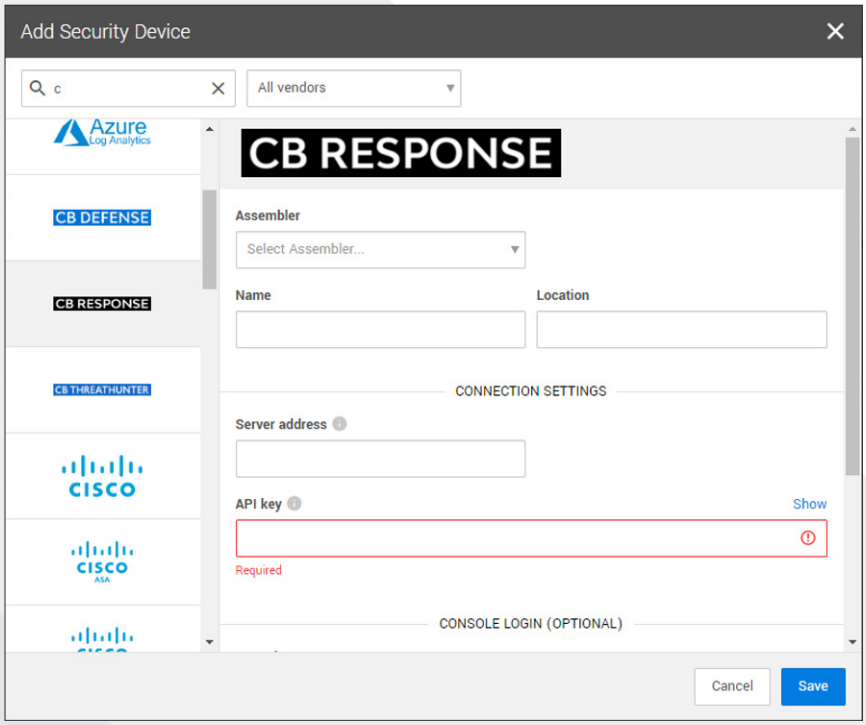

Figure 8

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. For **Name** enter the hostname of the Carbon Black Response device

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

J. For **Server address** enter the Carbon Black Response device IP or hostname in the following format: *https://10.0.0.10 or https://mycbraddress.com*

K. For **API key** enter the API generated in *Step 2, Letter D*

L. Under Console Login (Optional), **Username** and **Password** fields can be left blank, or can be filled in with the username and password created in *Step 1*

M. Select **Save**

N. After a few minutes (1–10 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

O. 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 Carbon Black Response 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.