FireEye HX Series getting started guide

Version 2.0

March 9, 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 FireEye HX 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 FireEye HX console.

Create an admin account

A. Navigate to **Admin>Appliance Settings** (Figure 1)

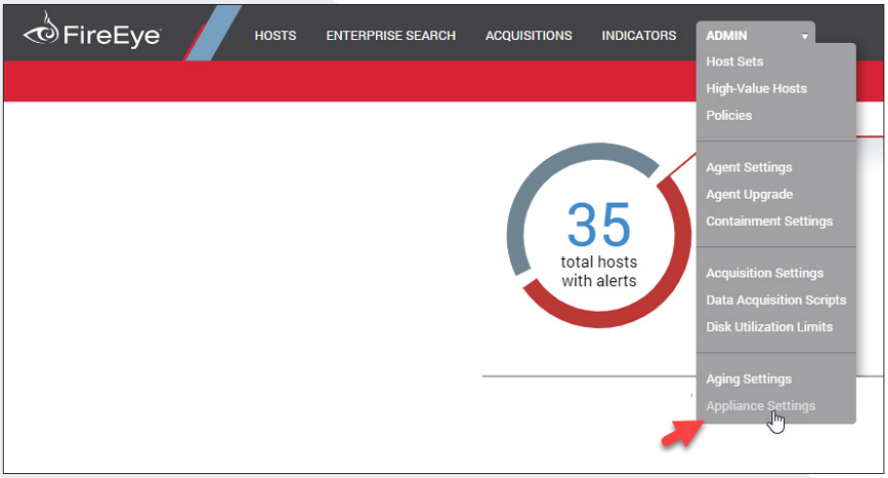

Figure 1

B. Click **User Accounts** on the left hand side (See Figure 2 for letters B-F)

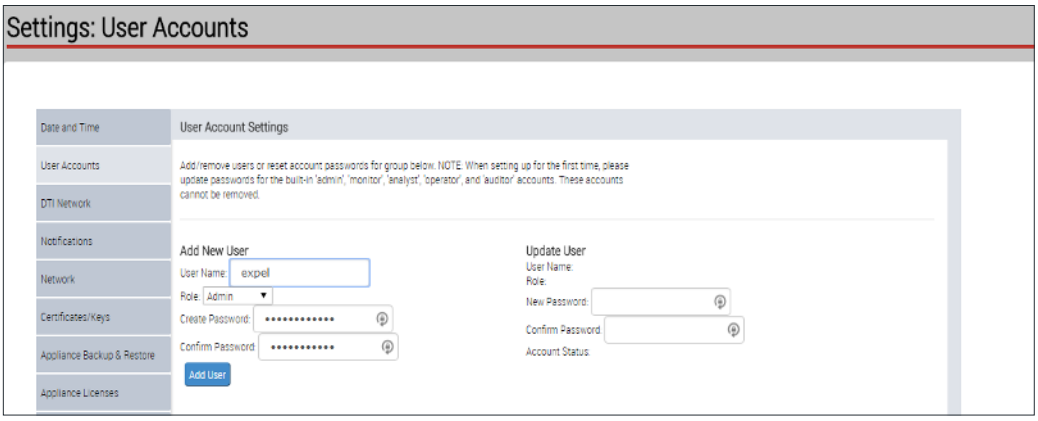

Figure 2

C. For **Username** add *Expel*

D. Ensure the **Role** dropdown is set to *Admin*

E. Enter the desired **Password**

F. Click **Add User**

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 FireEye HX API.

Create an API account

A. Go to the **User Accounts** section (see *Step 1, letters A & B*)

B. For **Username** add *expelapi* (see Figure 3 for letters B-E)

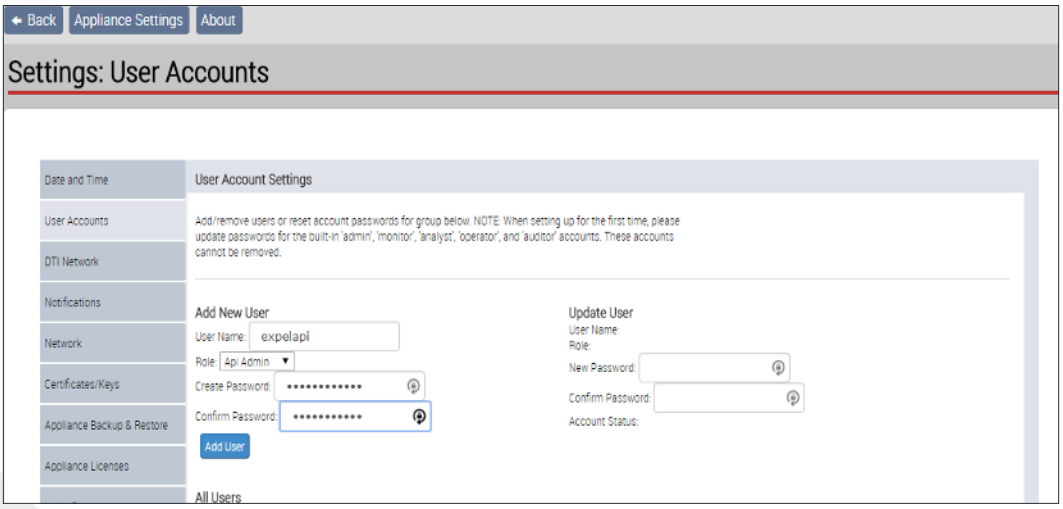

Figure 3

C. Ensure the **Role** dropdown is set to *API Admin*

D. Enter the desired **Password**

E. Click **Add User**

Step 3 — Configure the technology in Workbench

Now that we have the correct access configured and have noted the credentials, we can integrate FireEye HX with Expel.

Register device in Expel Workbench

A. In a new browser tab, log 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 4)

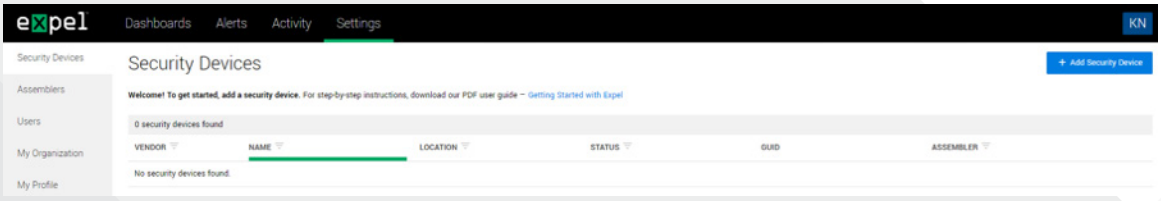

Figure 4

E. Search for and select FireEye HX (Figure 5)

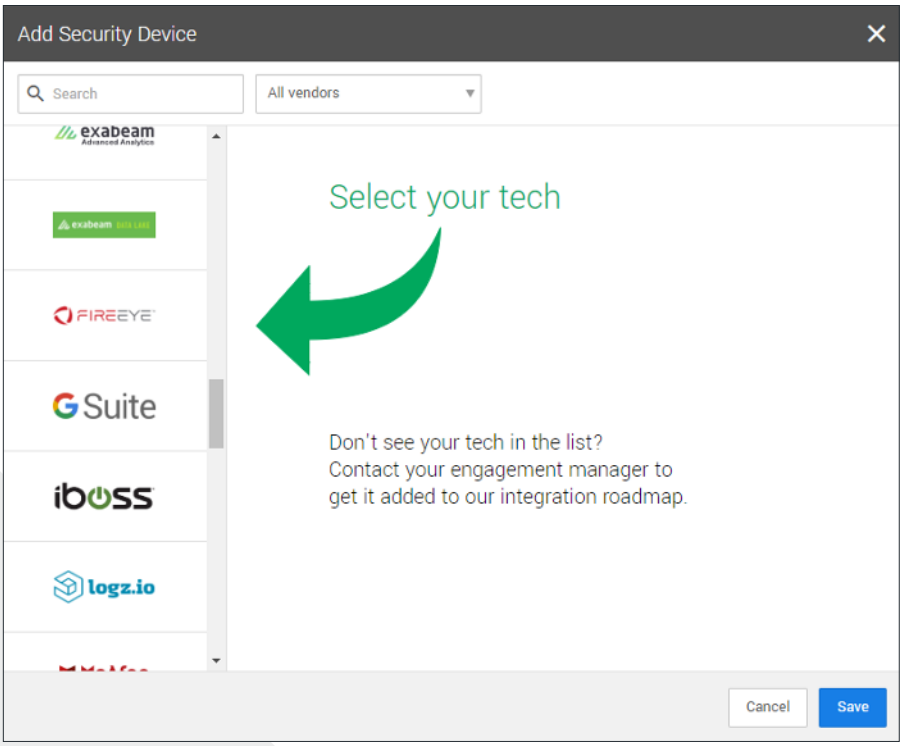

Figure 5

F. Refer to Figure 6 for *Steps G-M*

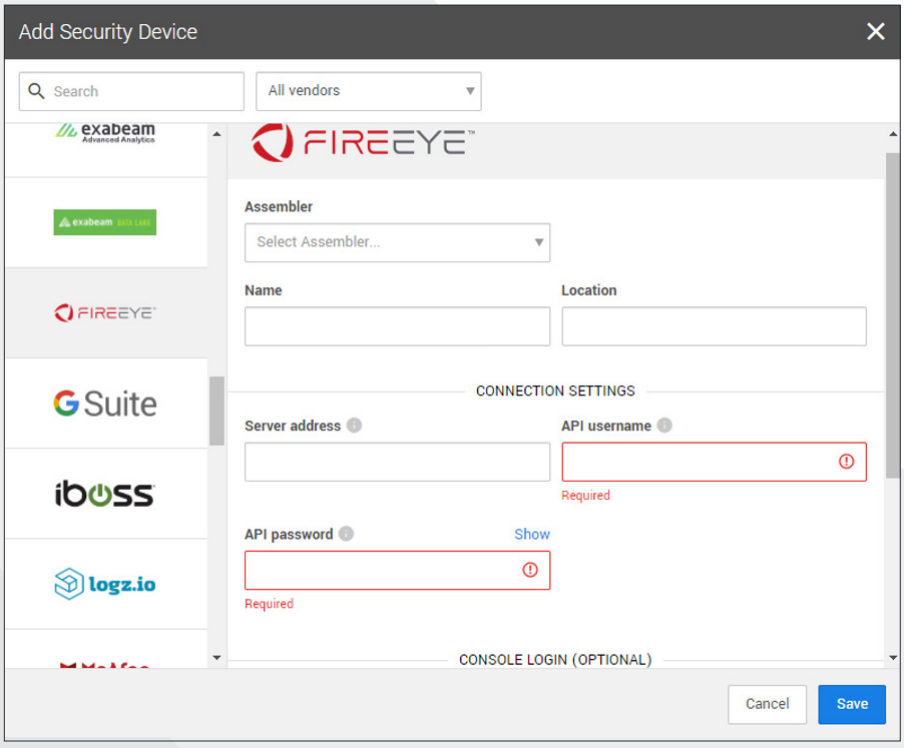

Figure 6

G. Select an **Assembler** from the drop down that has network connectivity to the FireEye HX device (Choose the **Assembler** you set up in *Step 2* of the Getting Started with Expel guide)

H. For **Name** enter the hostname of the FireEye HX device

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

J. For **Server address** enter the FireEye HX device IP and communications port in the following format: *https://<serverip>:3000 (Device IP can be found in the FireEye console > Admin> Appliance Settings > Network)*

K. For **Api Password** and **Api Username** enter the *API Admin* credentials previously created in the FireEye console in *Step 2*

L. In the optional Console Login section, for **Username** and **Password** enter the *Admin* credentials previously created in the FireEye console 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 FireEye HX 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.