Elastic Endpoint Security (formerly Endgame) getting started guide

Version 2.0

March 2, 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 Elastic Endpoint Security (formerly Endgame) 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 Elastic Endpoint Security console.

Create an admin account

A. Navigate to **Administration** icon on the left, click **Users** tab on the right, and click **Create New User** (Figure 1)

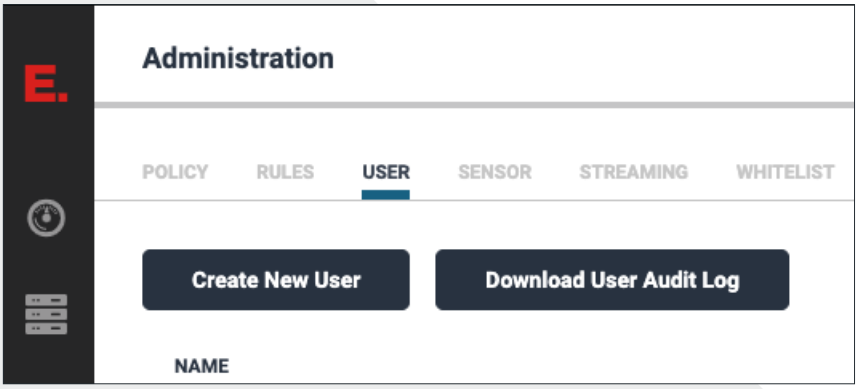

Figure 1

B. See Figure 2 for *Steps C-H*

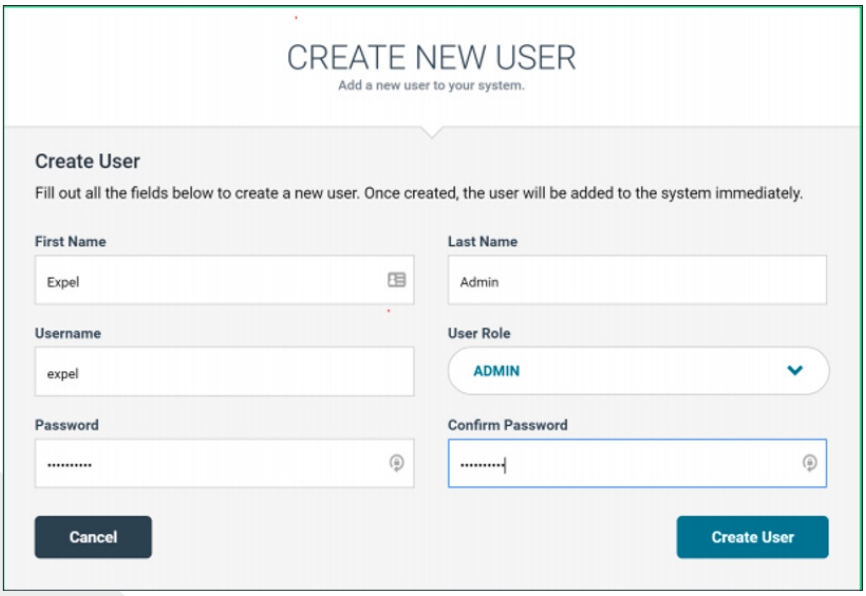

Figure 2

C. For **First name** add *Expel*

D. For **Last name** enter *Admin*

E. For **Username** enter *expel*

F. For User **Role** select *Admin**

G. Create a **Password** for Expel

H. Click **Create User**

**Note: LEVEL 3 access can be selected here although Expel will not be able to view security policies for the device to advise on best practices and configuration. Detection will remain unaffected.*

Note: Once console access is established for Expel, the remaining onboarding steps for this technology can also be performed by Expel. Please reach out to your **Engagement Manager** if this is desired and we would be happy to complete the integration!

Step 2 — Configure the technology in Workbench

Now that we have all the correct access configured and have noted the credentials, we can integrate Endgame 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 3)

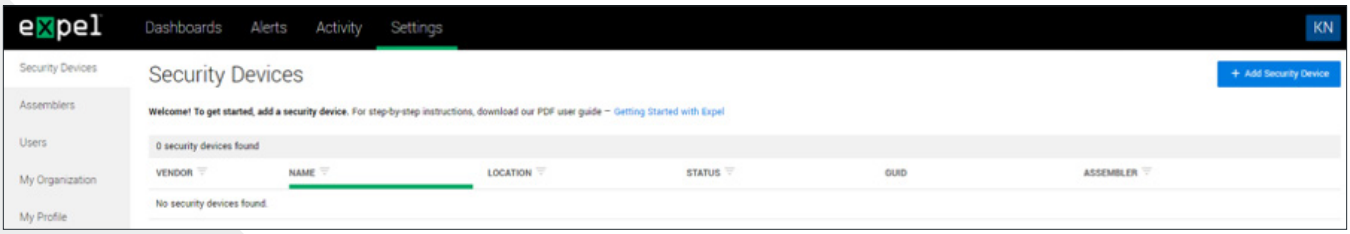

Figure 3

E. Search for and select Endgame (Figure 4)

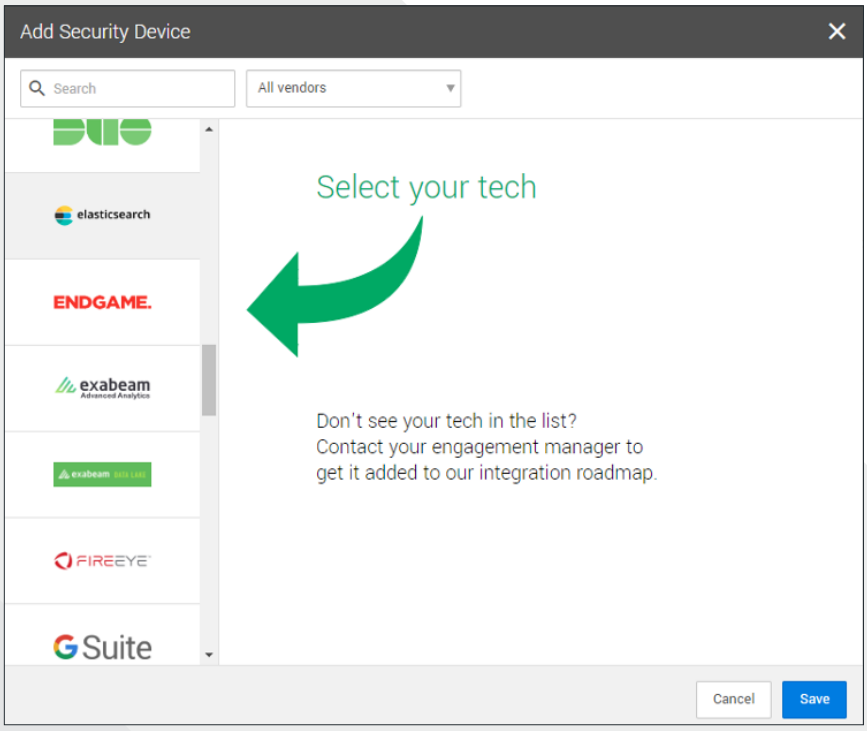

Figure 4

F. See Figure 5 to complete *Steps G-N*

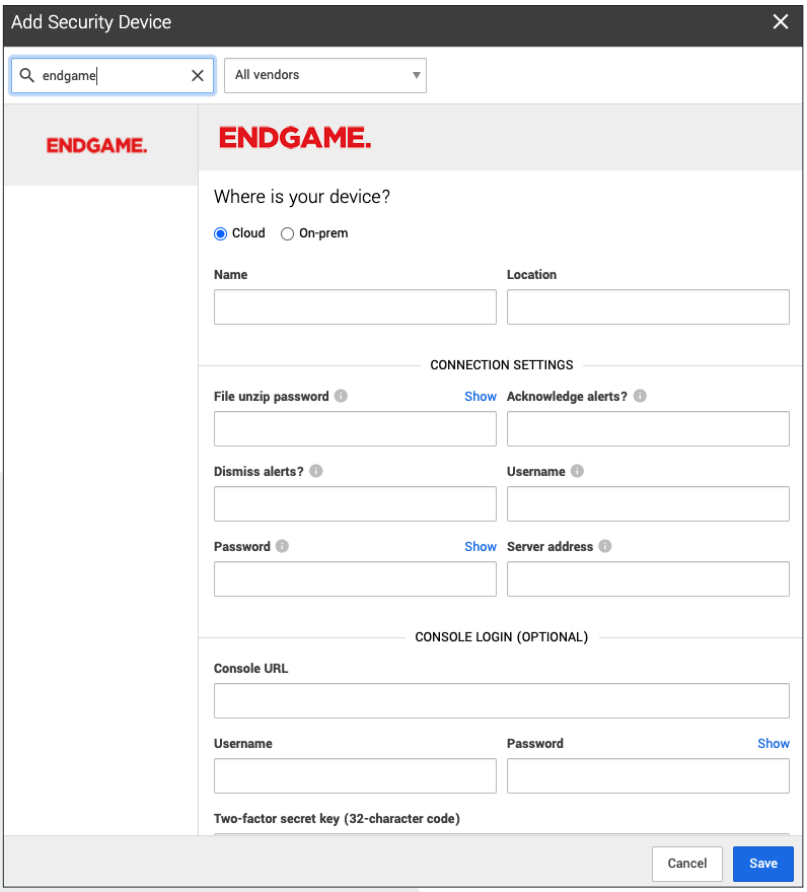

Figure 5

G. For **Name**, enter the hostname of the Elastic Endpoint Security device

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

I. For **Username**, enter *expel* (from *Step 1, Letter E*)

J. For **Ack alerts**, enter **"y"** to have Endgame alerts marked as "viewed" when Expel processes them

K. For **Server address** enter the management/console IP address of the device to be connected via https (i.e. https://127.0.0.1)*

L. For **Password**, enter the password used in *Step 1, Letter G*

M. Select **Save**

N. 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

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 Endgame alerts

**Note: The Expel Assembler will need access to this address on port 443. Please reach out to your* Expel *Engagement Manager if more information is needed on the Assembler.*

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.