Splunk getting started guide

Version 2.0

February 27, 2020

www.expel.io

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 Splunk 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.

By following these steps, you'll create a user account for Expel that will keep Expel's activity separate from other activity on the Splunk console.

Create an admin account

A. Log into **Splunk**

B. Navigate to **Settings>Access Controls>Users** (Figure 1)

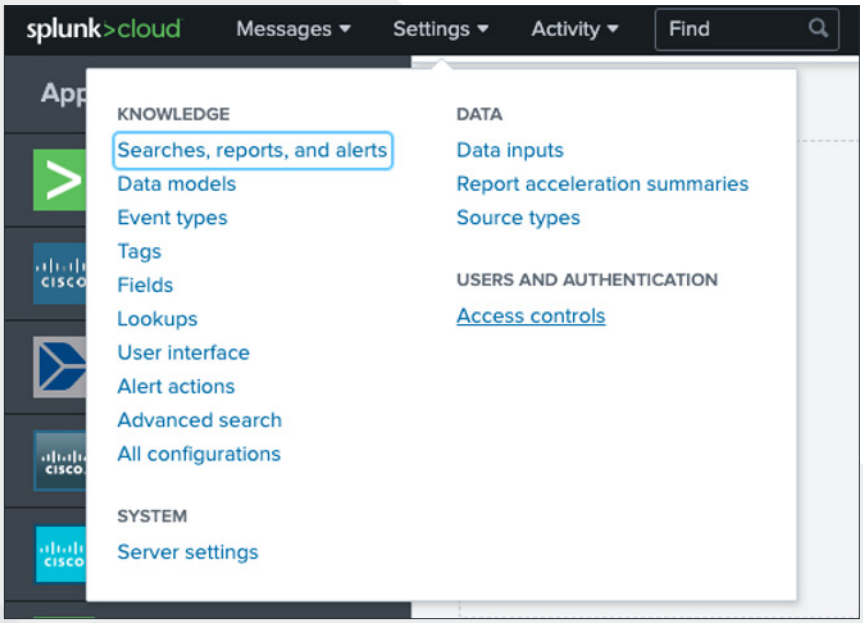

Figure 1

C. Click the **+Add new** button (Figure 2)

Figure 2

D. For **Name** enter *Expel* (See Figure 3 for *Steps D-J*)

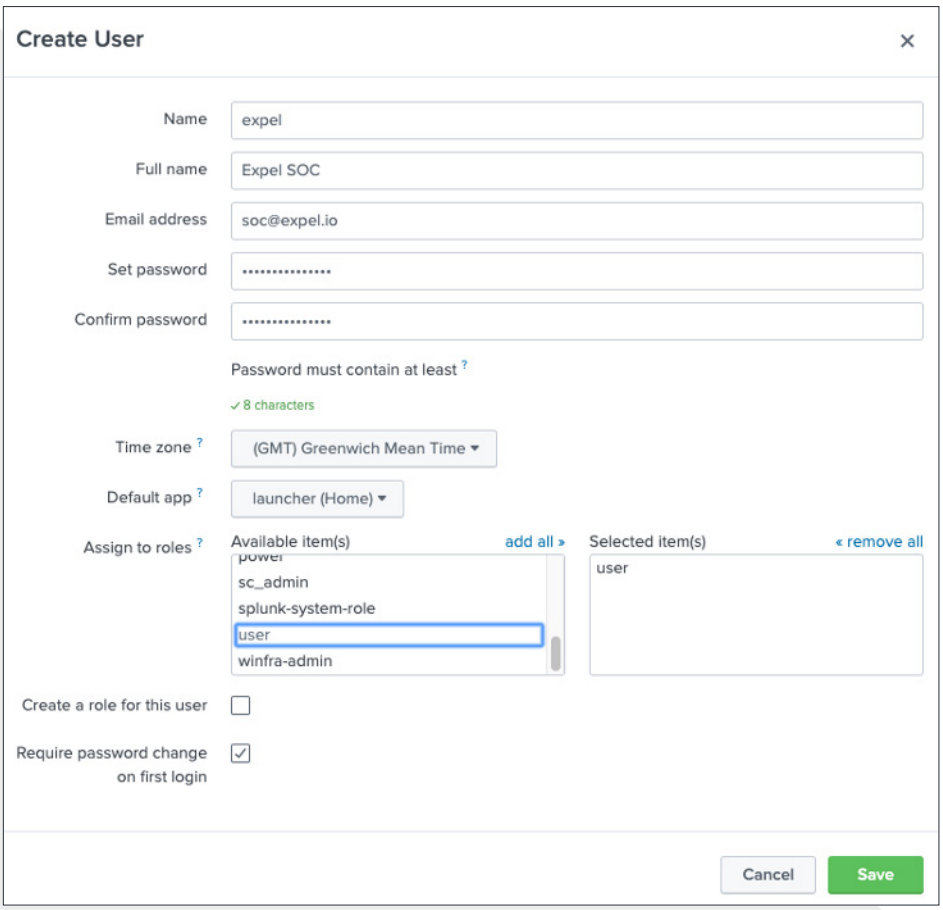

Figure 3

E. For **Full name** enter *Expel SOC*

F. For **E-mail** enter *soc@expel.io*

G. For Time Zone select *GMT (or UTC)*

H. For **Assign to roles** select *User*

I. Set the desired **Password**

J. Click **Save**

Note: The Expel Assembler will need access to the Splunk device or instance via port 8000 (UI) and 8089 (API). For cloud instances you may need to request enablement of rest API through Splunk support.

> **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 Splunk 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)

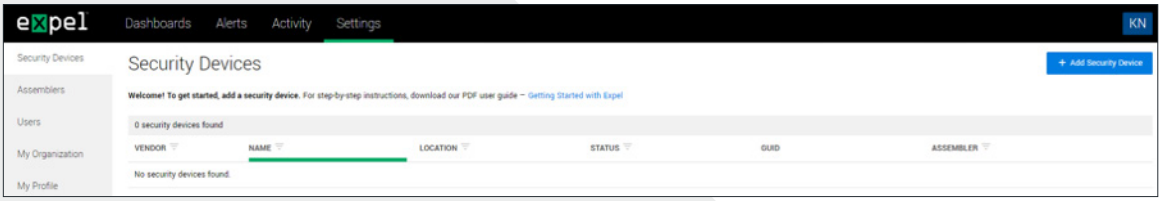

Figure 4

D. Search for and select **Splunk** (Figure 5)

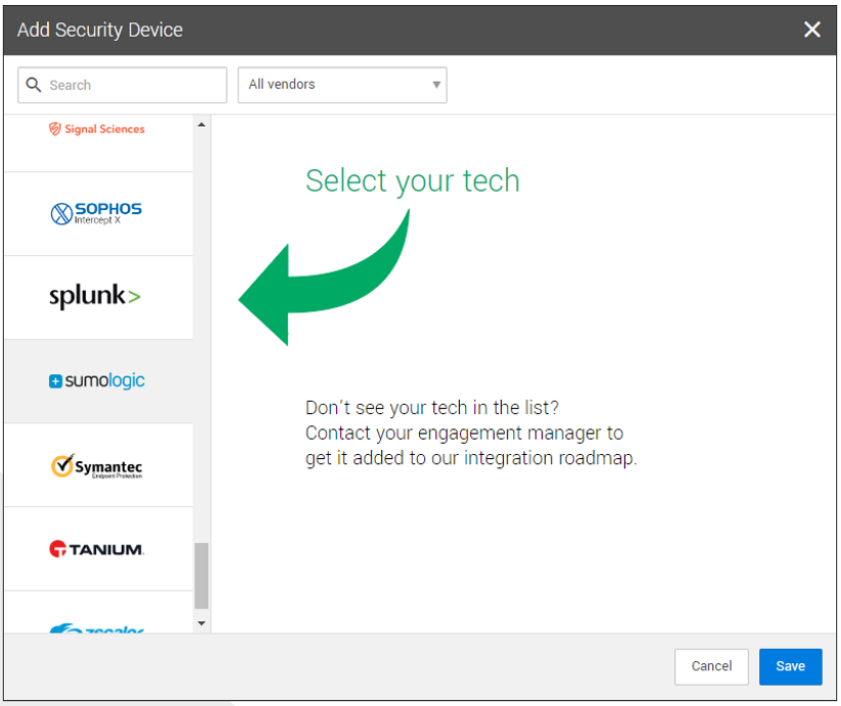

Figure 5

E. See Figure 6 for *Steps G-N*

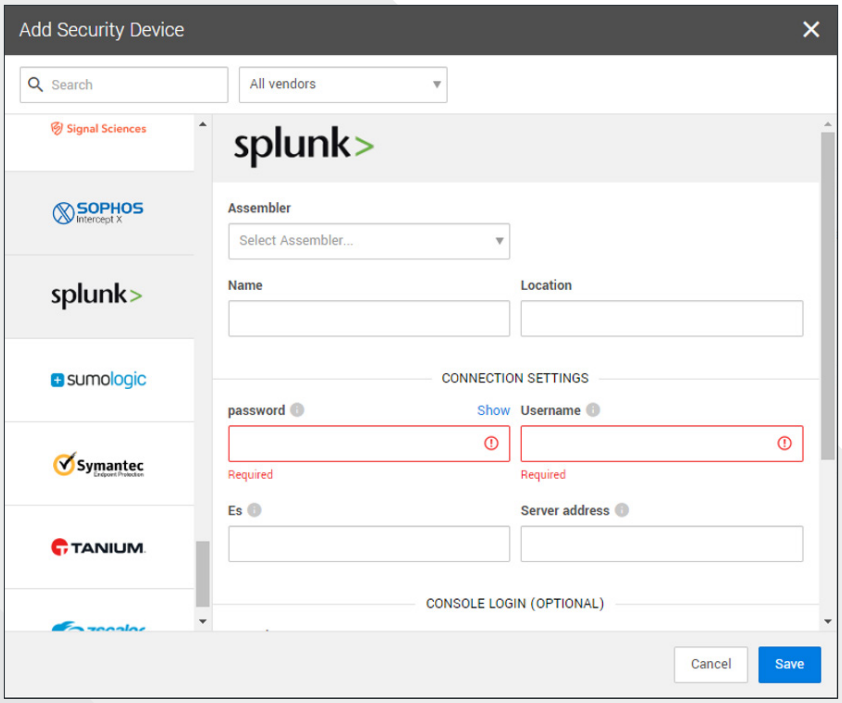

Figure 6

G. Select an **Assembler** from the drop down that has connectivity to the Splunk 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 Splunk device

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

J. For **Username** and **Password** enter the credentials used in *Step 1, letters D & I*

K. Leave the **Es** field blank. Splunk ES alerts will require review by Expel before enabling. Reach out to your *Engagement Manager* for details

L. For **Splunk on-premises** enter the Splunk console IP address and port 8089 (i.e. *https://10.10.10.10:8089/*)

M. For **Splunk Cloud** enter the Splunk server address and port 8089: (i.e. *https://<domainname>.splunkcloud.com:8089*)

N. Select **Save**

O. 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

P. 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 Splunk 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.