expel®

Attivo via SIEM getting started guide

Version 2.0

March 23, 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. Enable Attivo logging via Sumo Logic and Splunk; and
3. Configure Attivo via SIEM 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.

Create an admin account

A. Navigate to **Administration > User Accounts > Configure** (Figure 1)

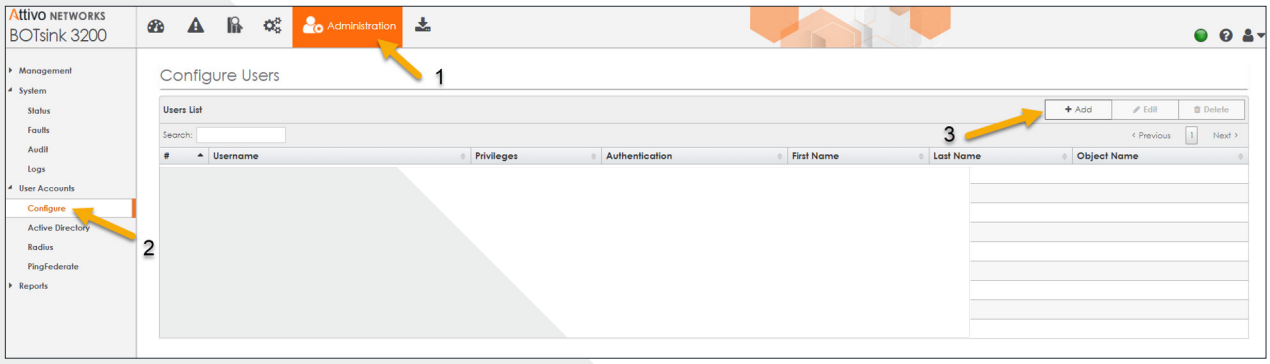

Figure 1

B. Select **+Add** within the Users List (Figure 1)

C. For **User Type** select *local* (See Figure 2 for *Steps C-I*)

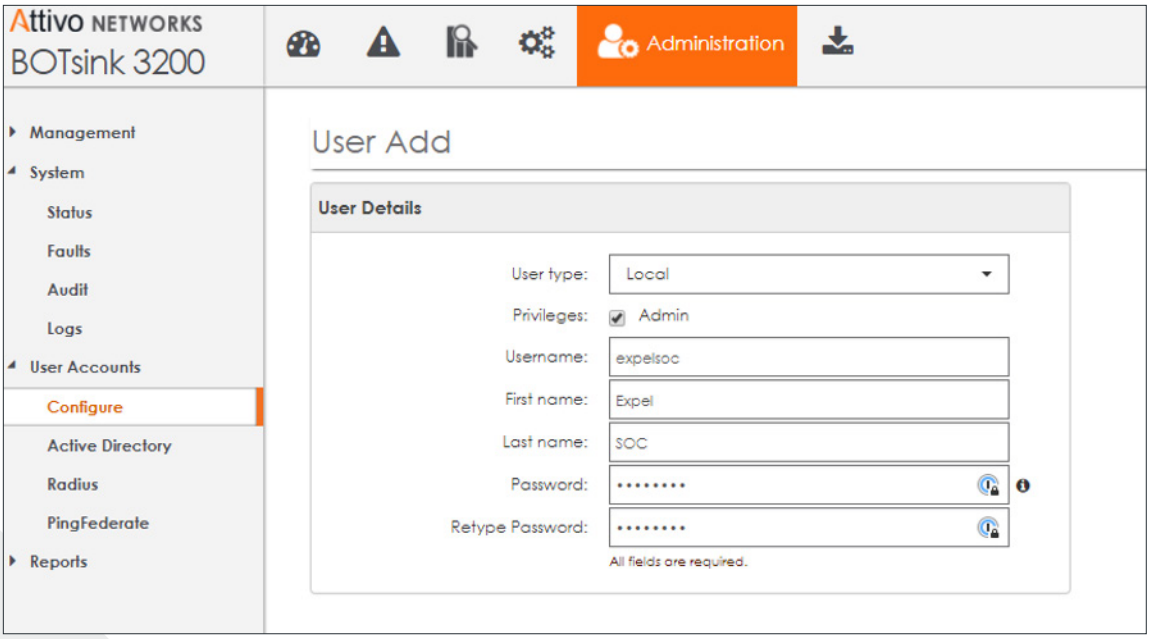

Figure 2

D. Check **Privileges** box for *Admin*

E. For **Username** enter *expelsoc*

F. For **First Name** enter *Expel*

G. For **Last Name** enter *SOC*

H. Enter the desired **Password**

I. Click **Save**

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 — Logging Attivo via Sumo Logic and Splunk

Please refer to your SIEM documentation or work with your SIEM representative to port in Attivo logs. You may also refer to the following web references for creating a new Syslog source:

Sumo Logic:
https://help.sumologic.com/Send-Data/Sources/01Sources-for-Installed-Collectors/Syslog-Source

Splunk:
https://docs.splunk.com/Documentation/Splunk/7.0.2/Data/Monitornetworkports

Step 3 — Configure Attivo in Workbench

Now that we have the correct access configured we can integrate your Attivo 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** (Figure 3)

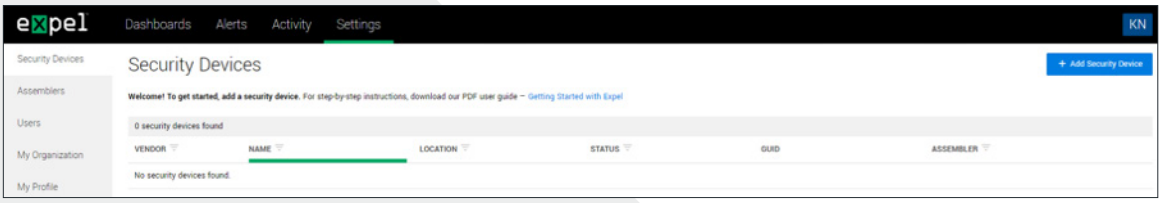

Figure 3

E. Search for and select Attivo (Figure 4)

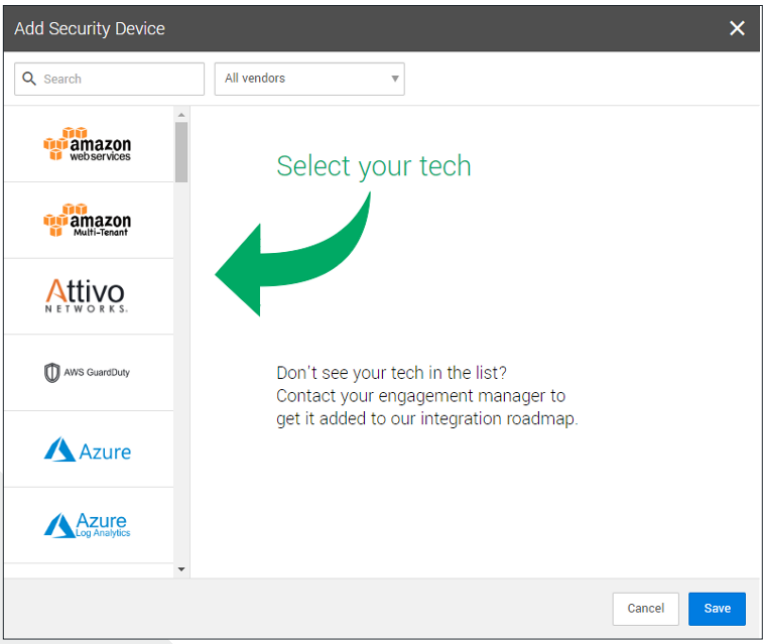

Figure 4

F. See Figure 5 for *Steps G-O*

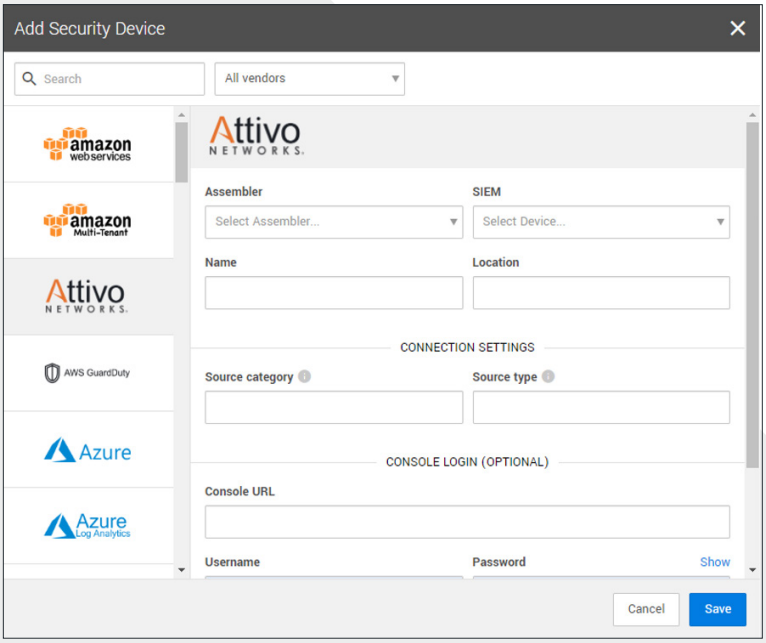

Figure 5

G. Choose the **Assembler** that has network connectivity to the Attivo device

H. For **Name** enter the hostname of the Attivo device

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

J. For **Source Category**, enter the Sumo Logic source category for this device

K. For **Source Type** (SIEM that contains the data) enter the Splunk source type for this device

L. For **Username** enter *expelsoc* from *Step 1, Letter E*

M. For **Password** enter the *expelsoc* admin password previously created in the Attivo console in *Step 1, Letter H*

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 Attivo 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.