Sumo Logic getting started guide

Version 2.1

April 15, 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 Sumo Logic 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 creates a user account for Expel that keeps Expel's activity separate from other activity happening on the Sumo Logic console.

Create an admin account

A. Log onto Sumo Logic device

B. Navigate to **Administration > Users and Roles > Users** and click the **Add User** button at the top-right of the page (See Figure 1)

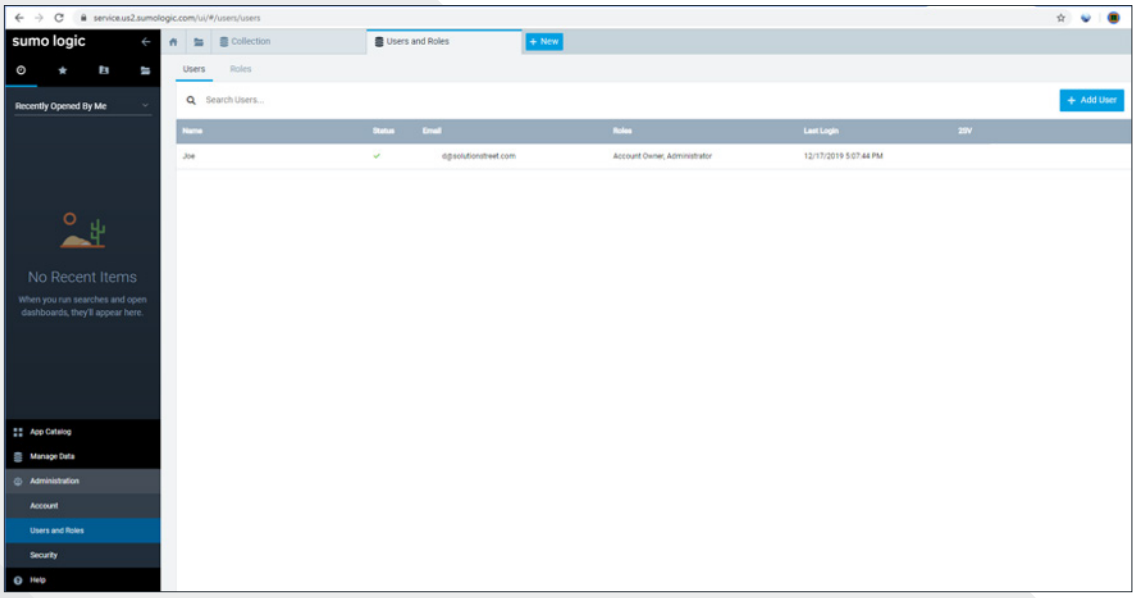

Figure 1

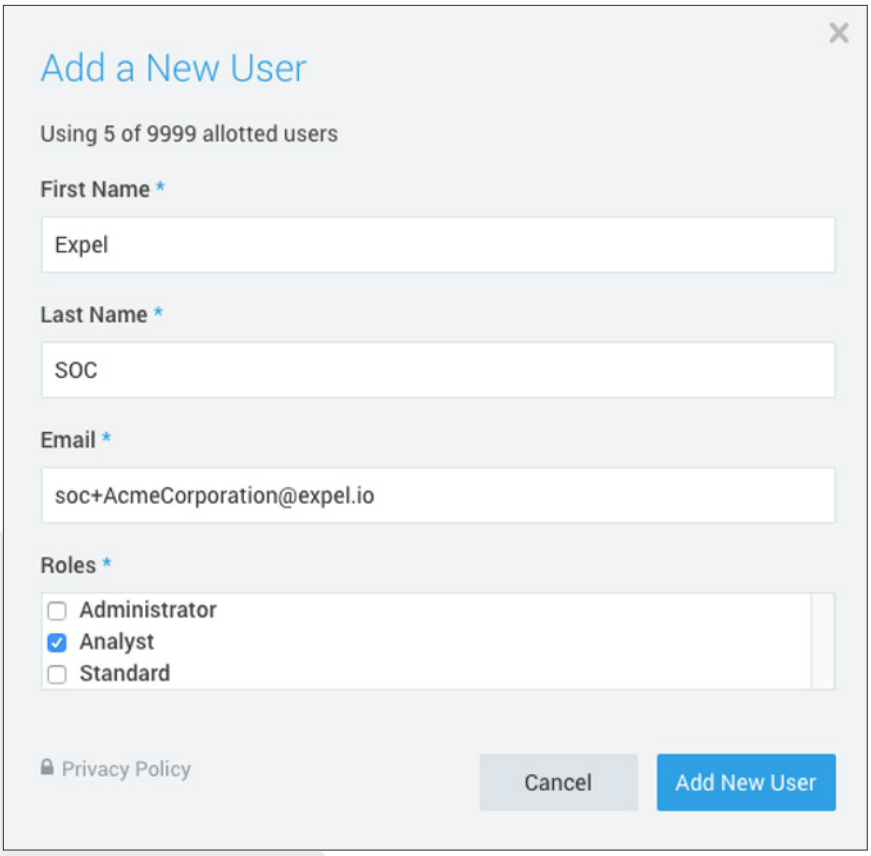

Figure 2

C. For **First Name** enter *Expel* (refer to Figure 2 for *Steps C-G*)

D. For **Last Name** enter "*SOC*"

E. For **Email** enter: soc+<Your Company Name>@expel.io

F. For **Roles** please choose the analyst role

G. Click **Add New** User

H. Verify that "Expel SOC" now appears on the Users page (this is the page shown in Figure 1)

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're unsure, please reach out to Expel at devicehealth@expel.io.

This procedure will create an authentication token that allows the Expel Assembler to access the Sumo Logic API.

Create Access ID and Access Key

A. Navigate to **Administration > Security> Access Keys** and click the **Add Access Key** button at the top-right of the page (Figure 3)

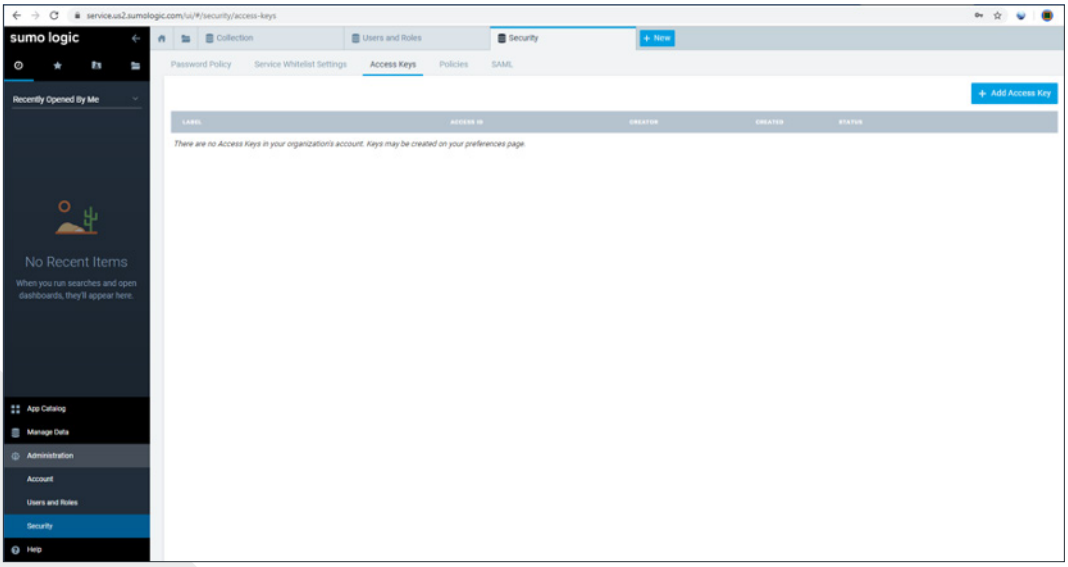

Figure 3

B. For **Name** enter *Expel-API* and click **Create Key** (Figure 4)

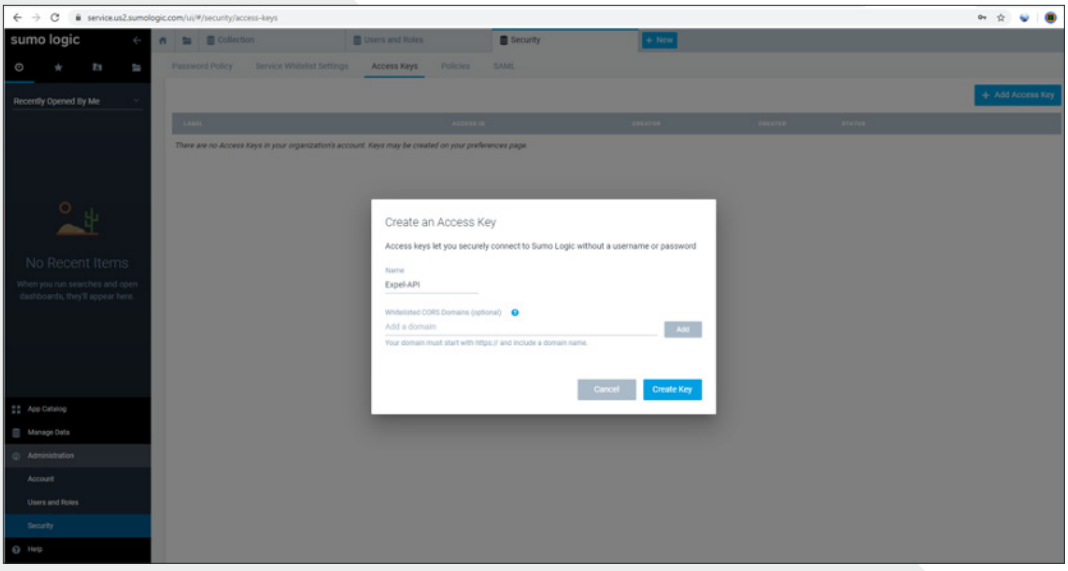

Figure 4

C. Make note of the newly generated **Access ID and Access Key** which will be used for registration within Expel Workbench in *Step 3* (See Figure 5 with sample ID and Key)

D. Click **Done**

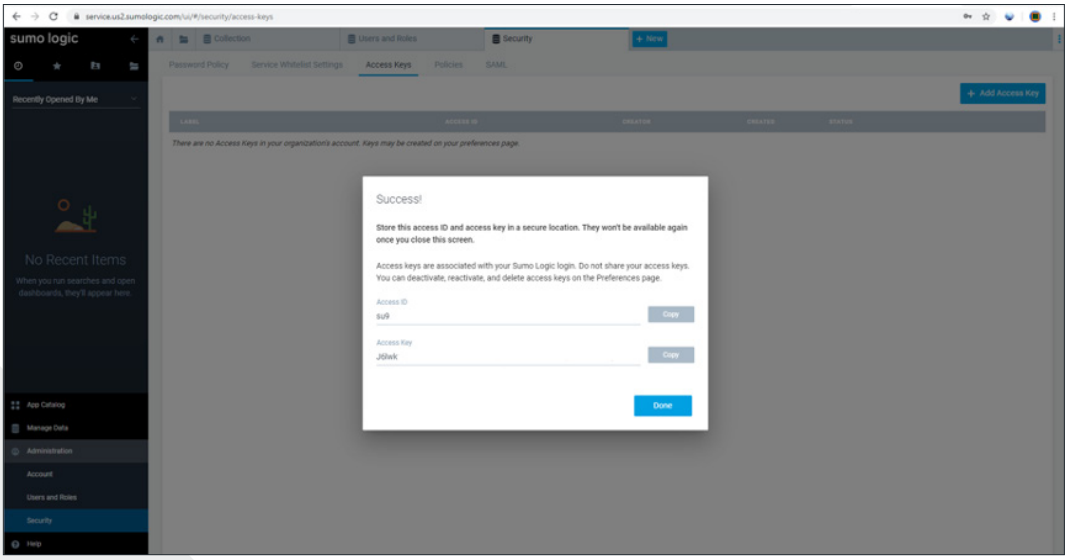

Figure 5

Step 3 — Configure the technology in Workbench

Now that we have all the correct access configured and have noted the credentials, we can integrate Sumo Logic with Expel.

Register devices 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** (see Figure 6)

D. At the top right of the page, select **Add Security Device**

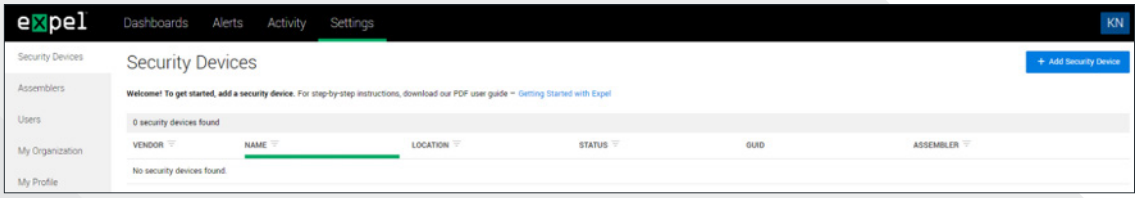

Figure 6

E. Search for and select Sumo Logic (Figure 7)

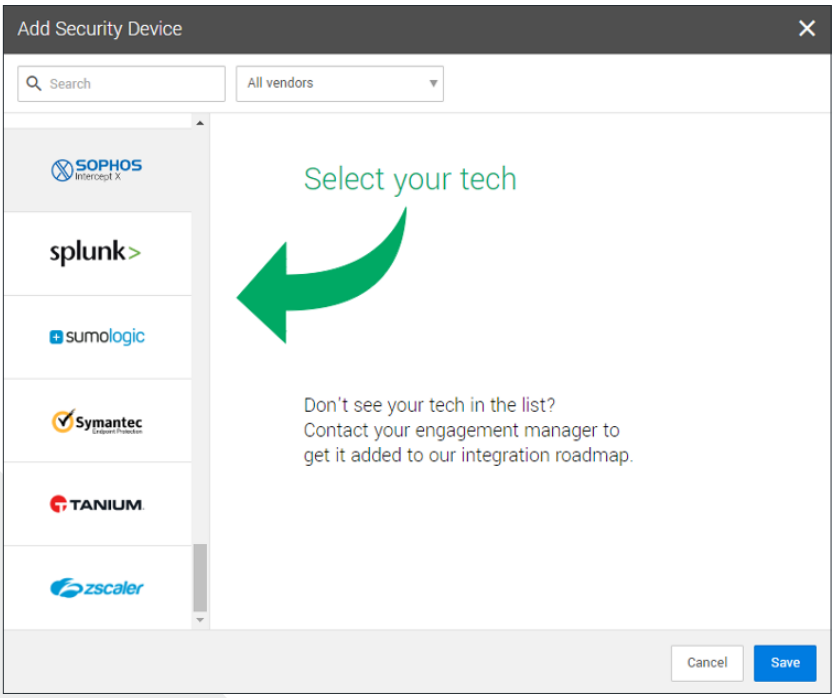

Figure 7

F. Select an **Assembler** from the drop down (Choose the **Assembler** you set up in *Step 2* of the Getting Started with Expel guide)

G. Enter **Assembler Name** and **Location** (see Figure 8, example Sumo Logic and Expel Lab)

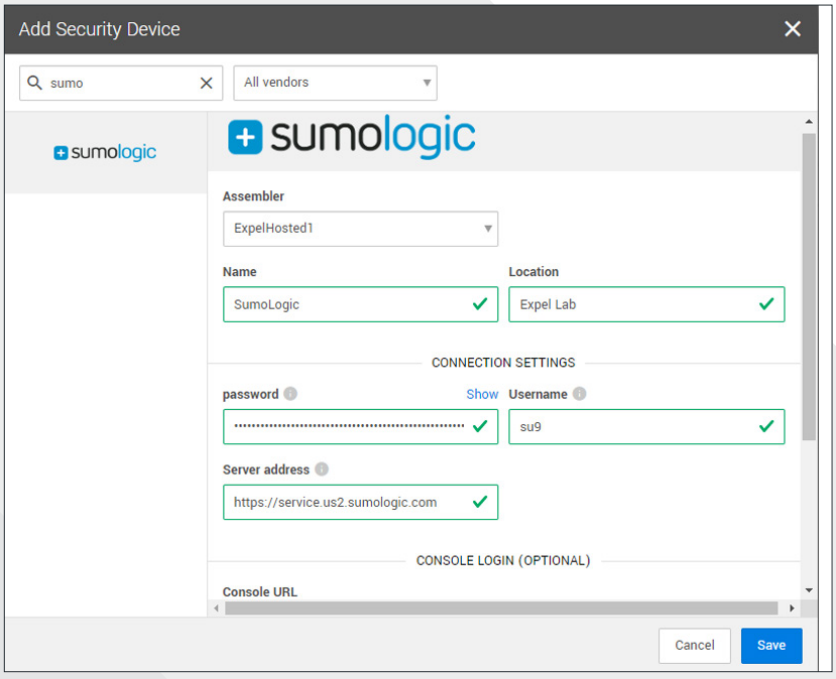

Figure 8

H. In the Connection Settings section, enter the **Access ID** from *Step 2C* for the **Username**

I. In the Connection Settings section, enter the **Access Key** from *Step 2C* for the **Password**

J. For **Server address** enter https://service.us2.sumologic.com. Alternatively, it can be https://service.sumologic.com. Please see https://help.sumologic.com/APIs/General-API-Information/Sumo-Logic-Endpoints-and-Firewall-Security for assistance

K. The optional **Console Login** section can be left blank

L. Select **Save**

M. 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 (see Figure 9)

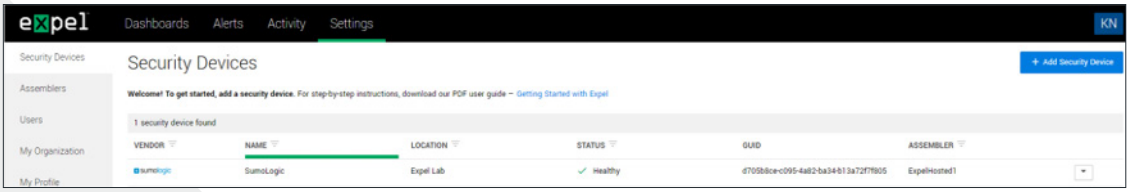

Figure 9

N. 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 Sumo Logic 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.