Azure Log Analytics getting started guide

Version 2.0

April 30, 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 Azure Log Analytics in Expel Workbench™.

Overview

Azure Log Analytics (ALA) aggregates and provides search capabilities over data in an Azure deployment. ALA functions as a data store for Azure applications, but can also be queried manually. Depending on policy and configuration, ALA can contain all kinds of data relevant to a security team. Most notably, when security audit policies are enabled on Azure VMs, they feed log data to ALA where it can be queried in the Analytics Portal.

Step 1 — Set up Azure AD Account for access to Log Analytics

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.

A. **Create an account** for Expel in Azure AD and provide access to the **Log Analytics** application

B. **expelsoc@[your AD domain]** can be used for naming convention

Step 2 — Setting up the Azure Log Analytics REST API

The Azure Log Analytics REST API lets you query the full set of data collected by Log Analytics using the same query language used throughout the service. To get started, follow these steps. These steps provide a simple way to get started, but a lot more options are available. For full details, make sure to review the Using the API section, as well as Microsoft's reference.

Please follow the documented instructions from *Steps 1-1.2* provided by Windows:
https://dev.loganalytics.io/documentation/1-Tutorials/Direct-API

Step 3 — Configure Azure Log Analytics in Workbench

Now that we have all the correct access configured and have noted the credentials, we can integrate Azure Log Analytics with Expel Workbench.

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 1)

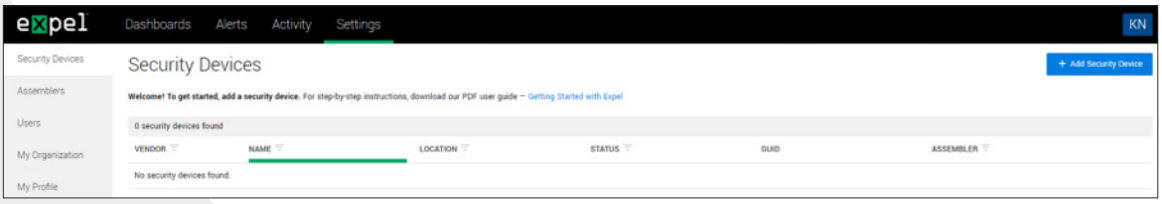

Figure 1

E. Search for and select Azure Log Analytics (Figure 2)

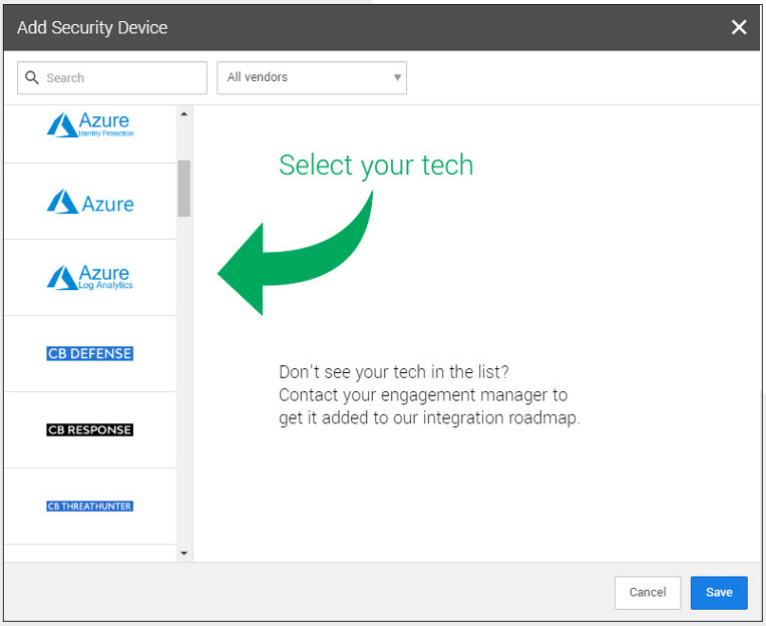

Figure 2

F. Refer to Figure 3 for *Steps G-N*

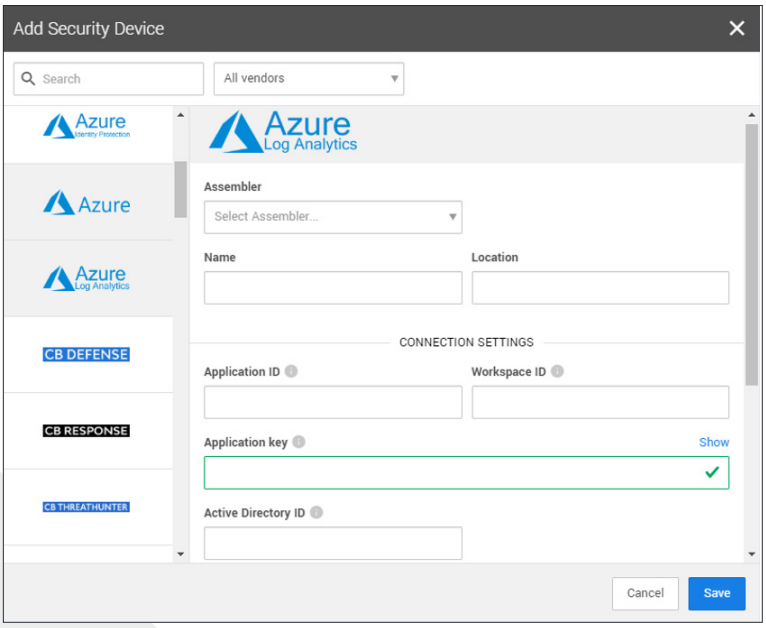

Figure 3

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

H. For **Name** enter the hostname of the Microsoft ALA device

I. For **Location** enter Cloud

J. For **Application ID**, enter the ID of the application with access to Azure Log Analytics

K. For **Workspace ID**, enter the ID of the workspace within Azure Log Analytics

L. For **Application key**, enter the key used to authenticate the application

M. For **Active Directory ID**, enter the ID of the Azure Active Directory (tenant) in the cloud instance

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 Microsoft Azure Log Analytics 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.