Microsoft Cloud Application Security getting started guide

Version 2.1

October 1, 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 the technology in Expel Workbench™.

Step 1 — Enable console access

Having global reader access to the interface enables Expel to go above and beyond. This access is used by our Analysts to dig deeper when performing Incident Investigations and allows our Device Health Team to investigate potential health issues with your technologies. You can create either a local account or an AD user via portal.azure.com.

A. Go to admin.microsoft.com to create a new user

B. Scroll down to **Users** and click on **Active Users**

C. Select **Add a user**

D. Set **Expel** as first name and **SOC** as last name

E. Scroll to the bottom and grant **global reader** role for the user

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 your Expel Customer Success Engineer or email customerhealth@expel.io.

A. Access MCAS portal http://portal.cloudappsecurity.com/ using the account credentials created in *Step 1* above

B. Go to the **Settings** menu and select **Security extensions** and then **API tokens** (Figure 1)

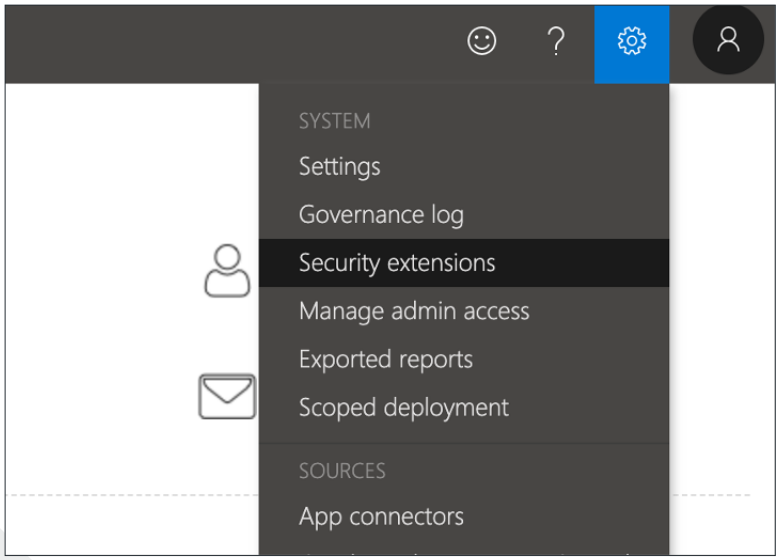

Figure 1

C. Generate a new token and provide a name to identify the token and click **Next**

D. **Copy the token value and save it somewhere safe**

E. After you generate a new token, you'll be provided with a new URL to use to access MCAS (Microsoft Cloud Application Security); be aware the token has the privileges of the user (created in *Step 1*) who issued it

Step 3 — Configure the technology in Workbench

Now that we have all the correct access configured and have noted the credentials, we can integrate your tech 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 2)

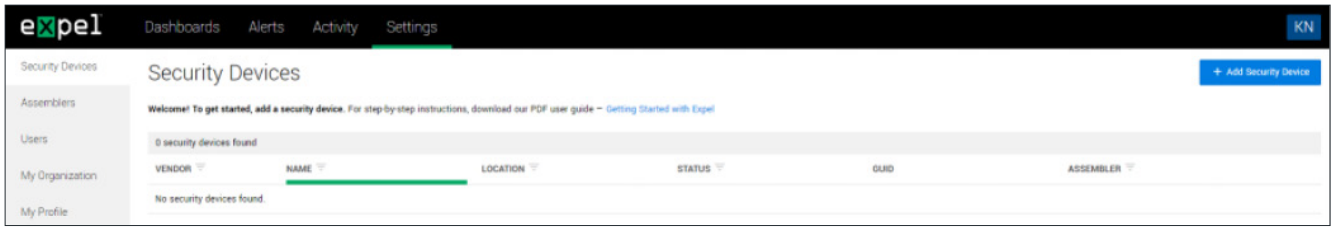

Figure 2

E. Search for and select your technology (Figure 3)

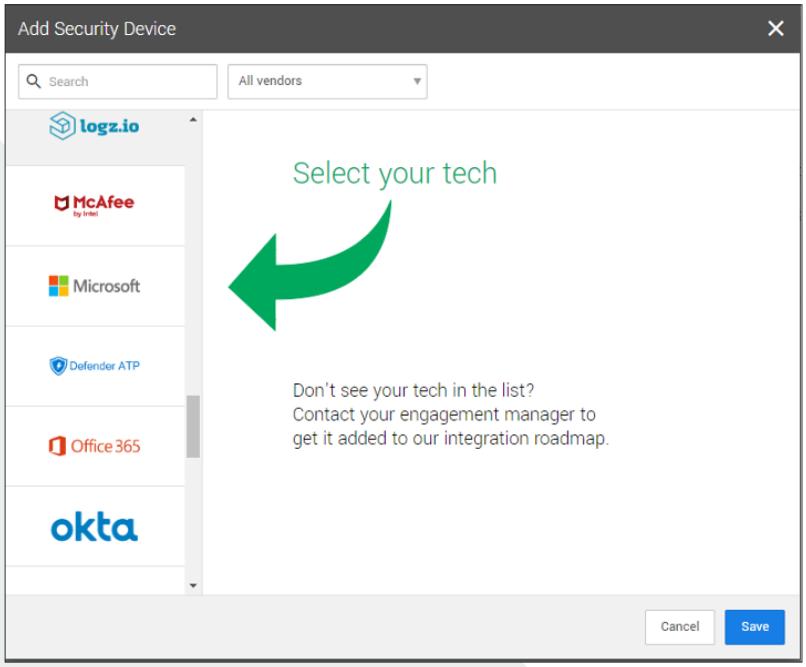

Figure 3

F. Refer to Figure 4 for Steps G-L

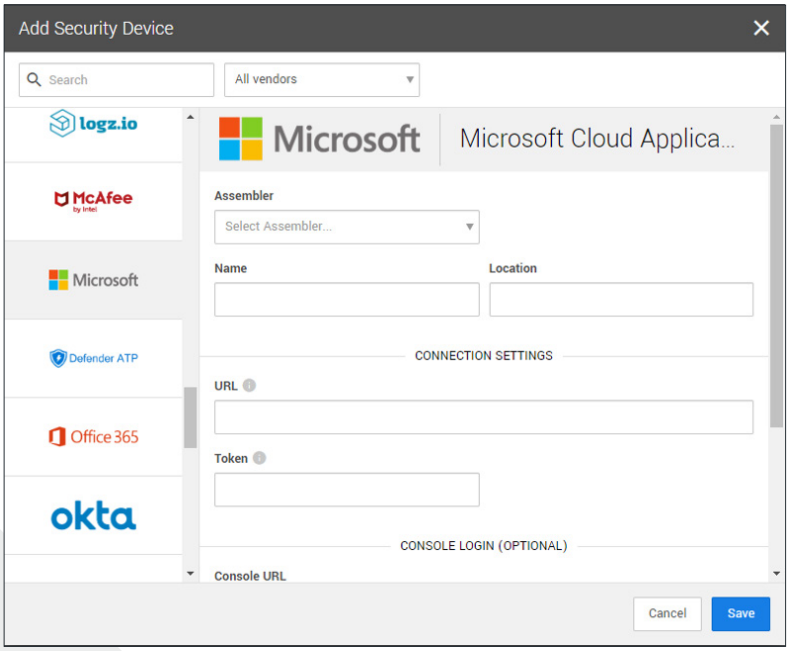

Figure 4

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 MS Cloud Application Security device

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

J. For **URL**, enter from *Step 2, Letter E*

K. For **Token**, enter from *Step 2, Letter C*

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

N. To check and see if alerts are coming through, navigate to **Alerts** on the console page, then click the icon in the upper right to switch to grid view, then check the list for MS Cloud Application Security 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 your assigned *Engagement Manager*, or our friendly *Customer Success Engineers* by email to devicehealth@expel.io.