CylancePROTECT (AV) getting started guide

Version 2.0

May 27, 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 CylancePROTECT 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.

A. **Log in** to the Cylance Console **as an administrator**

B. Select **Settings > Users**

C. **Add a user** for Expel with a **Read Only** role

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 contact Expel at devicehealth@expel.io.

A. **Log in** to the Cylance Console **as an administrator**. Only administrators can create an application integration

B. Select **Settings > Integrations** (Figure 1)

C. Click **Add Application** (Figure 1)

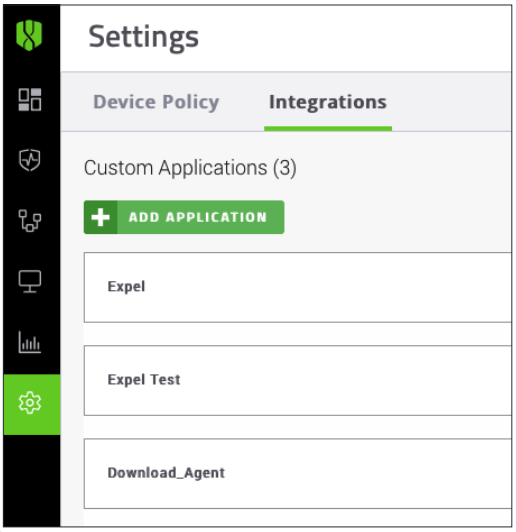

Figure 1

D. Type an **Application Name**. This must be unique within your organization (Figure 2)

E. Select **Threats READ, Devices READ,** and **Users READ** privileges (Figure 2)

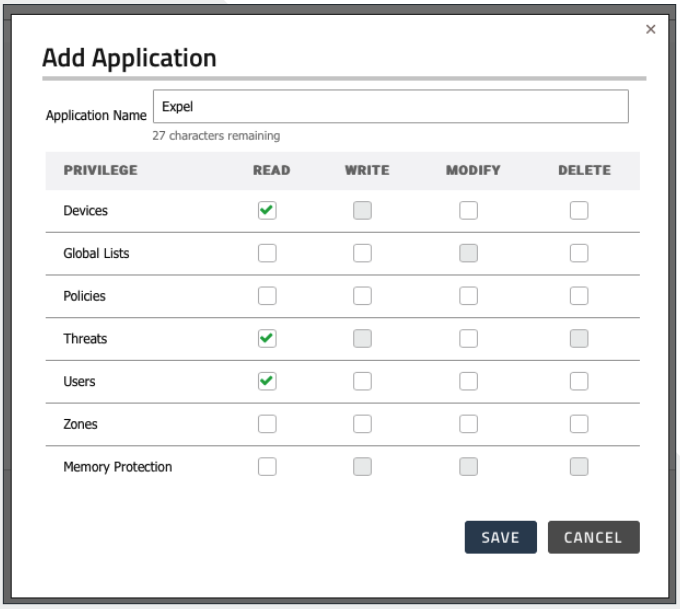

Figure 2

F. Click **Save**. The application credentials will display (Figure 3)

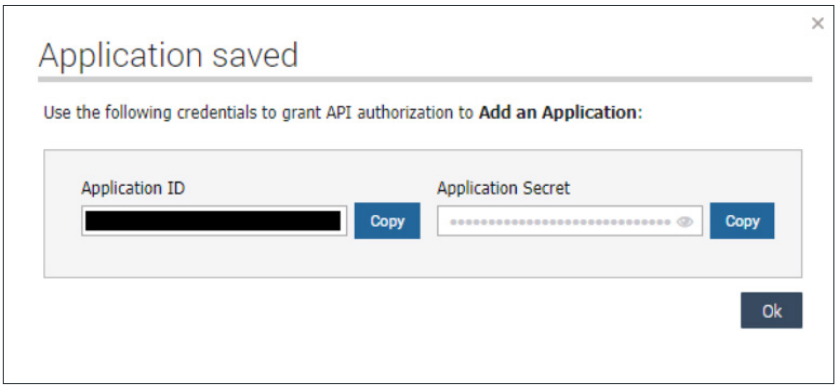

Figure 3

G. Copy the **Tenant ID** located in the **Integrations** page and save for onboarding in Expel Workbench (Figure 4)

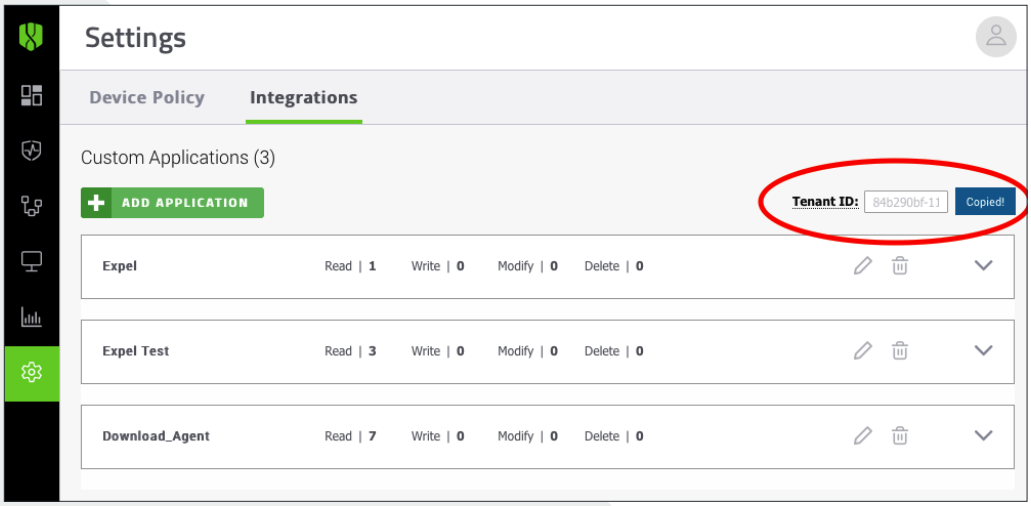

Figure 4

H. Note your Cylance **Service Endpoint**. This can be found by mapping your Cylance in the table below (Figure 5) Ex: https://protect-euc1.cylance.com would be https://protectapi-euc1.cylance.com

URL	Service Endpoint
https://protect-apne1.cylance.com	https://protectapi-apne1.cylance.com
https://protect-euc1.cylance.com	https://protectapi-euc1.cylance.com
https://protect-au.cylance.com	https://protectapi-au.cylance.com
https://protect-sae1.cylance.com	https://protectapi-sae1.cylance.com
https://protect.us.cylance.com	https://protectapi.us.cylance.com
https://protect.cylance.com	https://protectapi.cylance.com

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 CylancePROTECT (AV) 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 6)

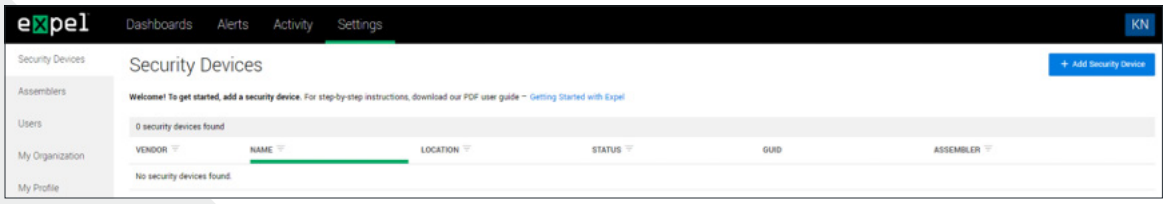

Figure 6

E. Search for and select CylancePROTECT AV (Figure 7)

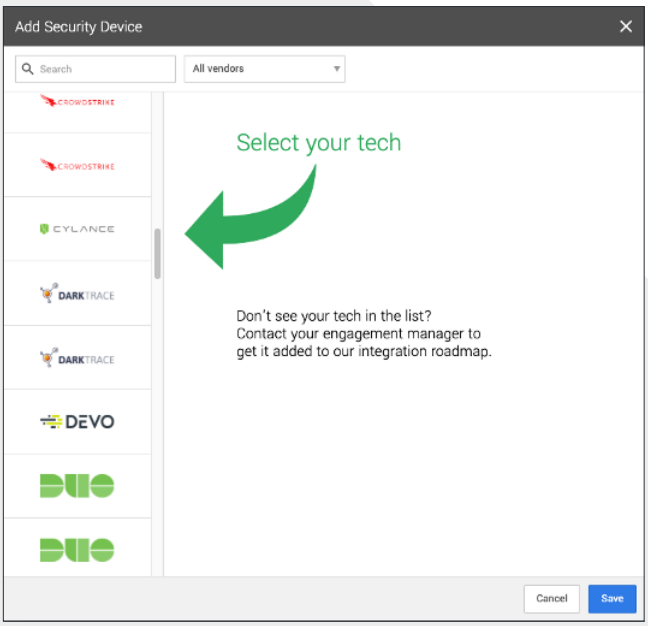

Figure 7

F. Refer to Figure 8 for *Steps G-M*

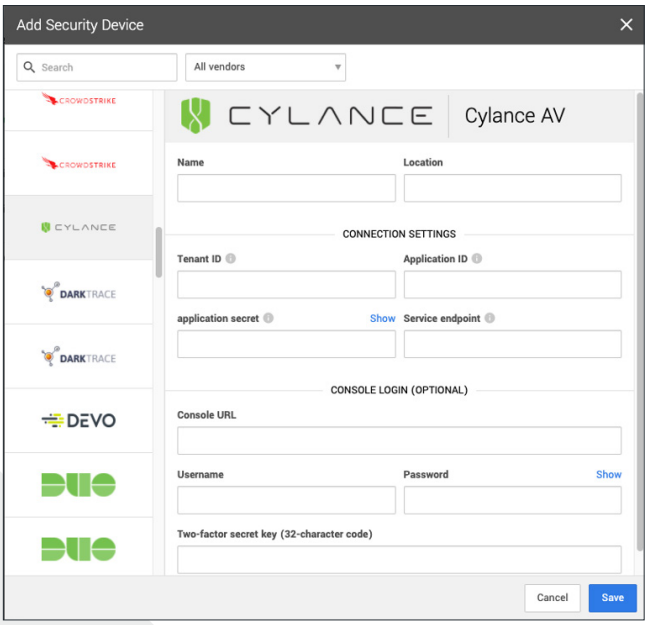

Figure 8

G. For **Name** enter the hostname of the Cylance device

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

I. For **Tenant ID** enter the Tenant ID generated in *Step 2, Letter G*

J. For **Application ID** enter the Application ID generated in *Step 2, Letter F*

K. For **application secret** enter the application secret generated in *Step 2, Letter F*

L. For **Service Endpoint** enter your correct Service Endpoint from the table in *Step 2, Letter H*

M. Select **Save**

N. 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

O. 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 CylancePROTECT (AV) 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.