Cisco AMP for Endpoints getting started guide

Version 2.0

April 29, 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 Cisco AMP for Endpoints 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 will create a user account for Expel that will keep Expel's activity separate from other activity on the Cisco AMP console.

Create a user account for console access

A. Navigate to **Accounts > Users** (Figure 1)

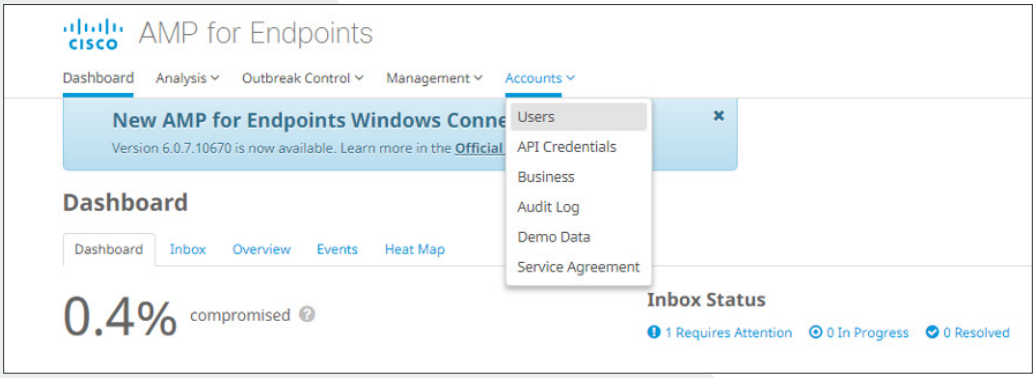

Figure 1

B. Click **+ New User** (Figure 2)

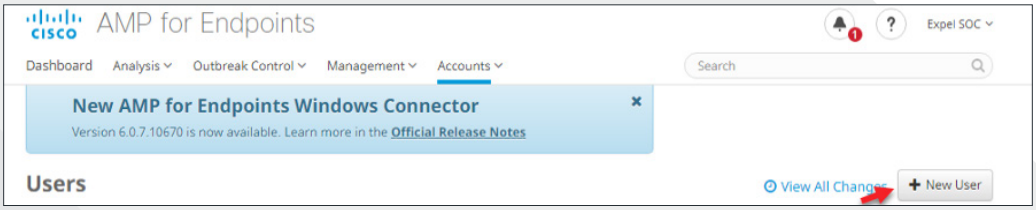

Figure 2

C. For **First Name** add *Expel* (See Figure 3 for *Steps C-G*)

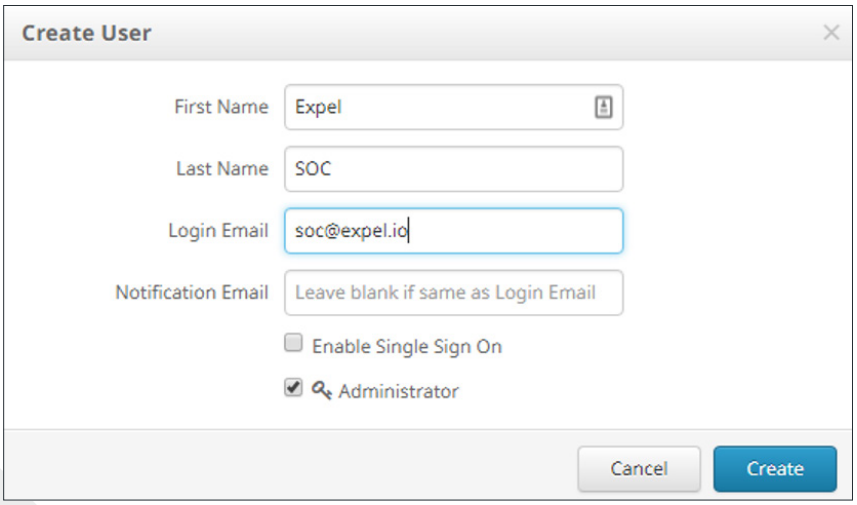

Figure 3

D. For **Last Name** add *SOC*

E. For **Login Email** add *soc@expel.io*

F. Select the **Administrator** checkbox

G. Click **Create**

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.

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

Create an API access account

A. Navigate to **Accounts > API Credentials** (Figure 4)

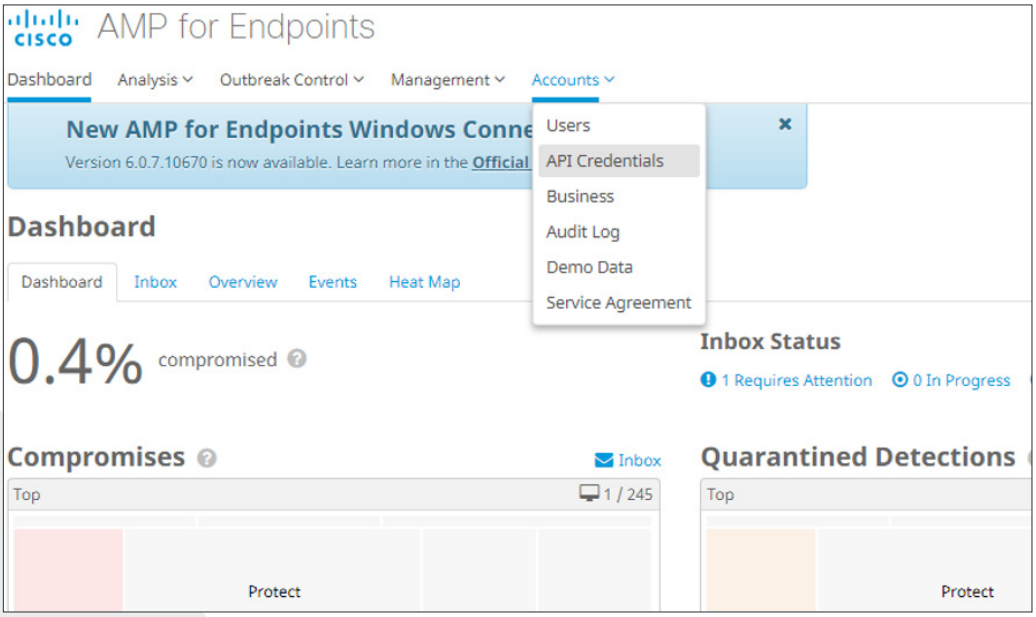

Figure 4

B. Click **+New API Credential** (Figure 5)

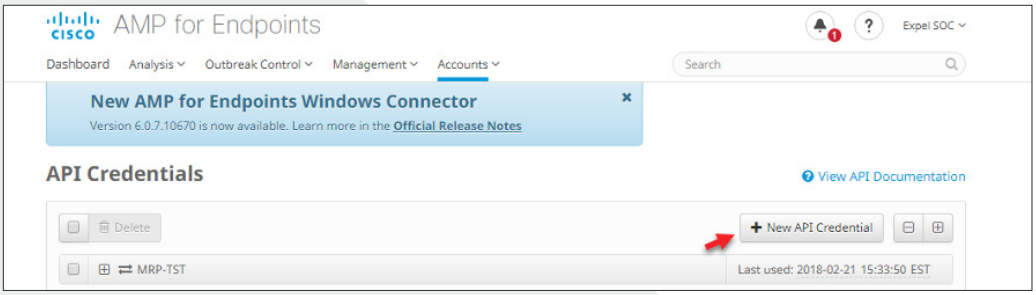

Figure 5

C. For **Application name** enter *expelapi* (See Figure 6 for *Steps C-E*)

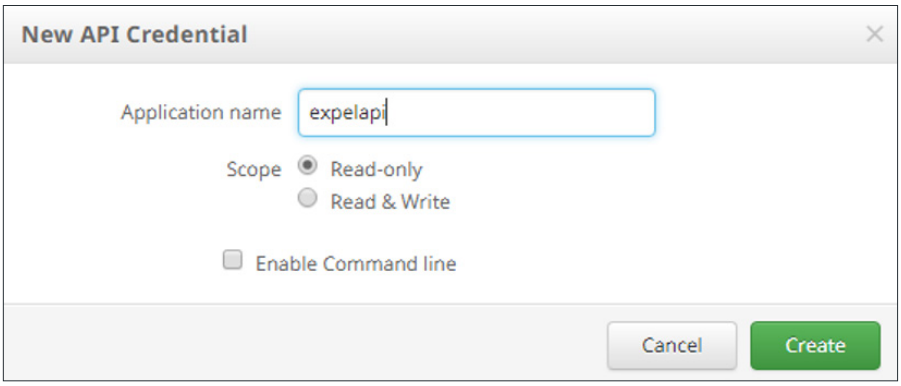

Figure 6

D. For **Scope** select *Read-Only*

E. Click **Create**

F. A new page will open with your API Key Details. **Save these items**, as they are not easily accessible later in the process, and they are needed for onboarding in Expel Workbench (Figure 7)

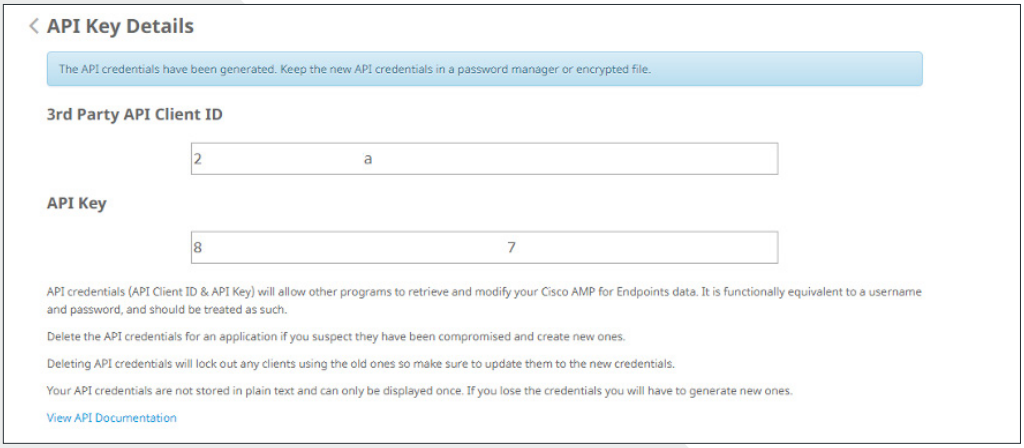

Figure 7

Step 3 — Configure the technology in Workbench

Now that we have all the correct access configured and have noted the credentials, we can integrate Cisco AMP for Endpoints 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 8)

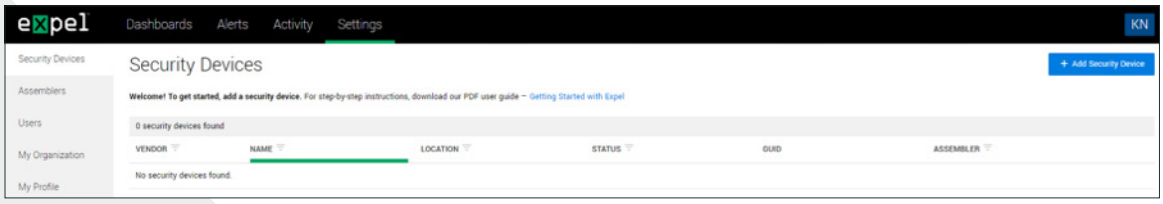

Figure 8

E. Search for and select **Cisco** (Figure 9)

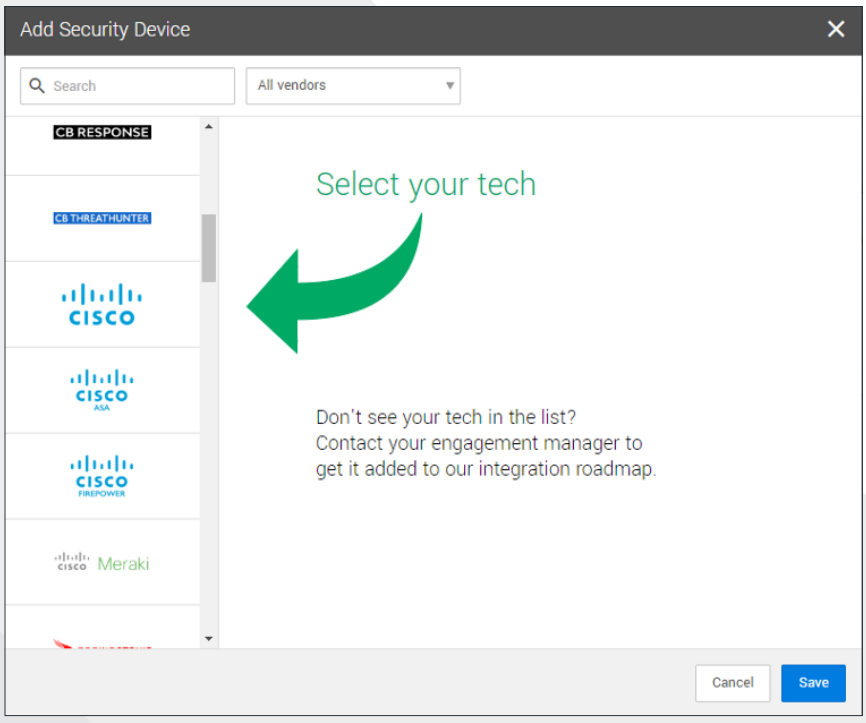

Figure 9

F. Use Figure 10 to for *Steps G-L*

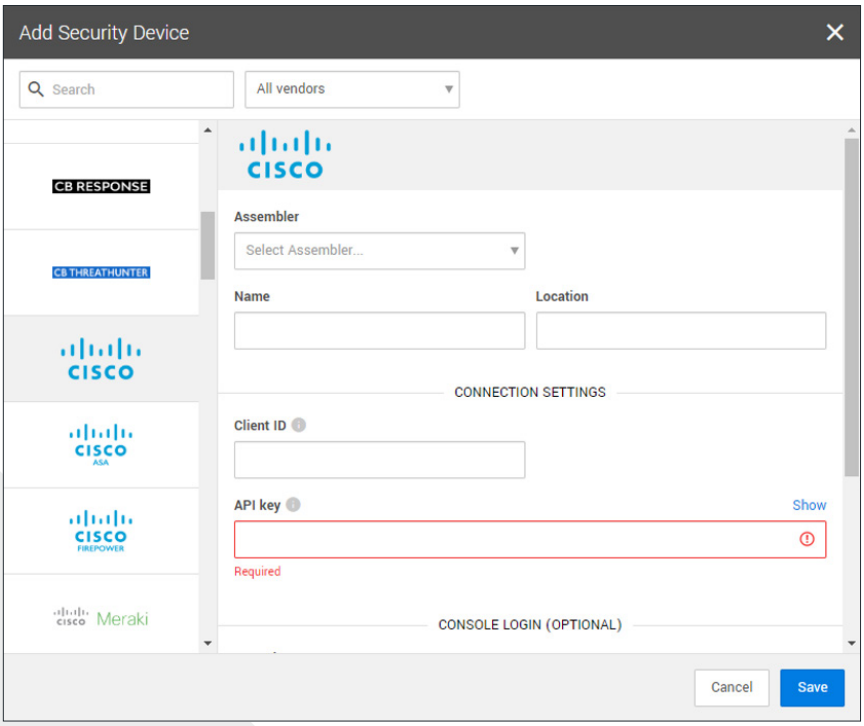

Figure 10

G. Select an **Assembler** from the drop down that has network connectivity to the Cisco AMP device (Choose the **Assembler** you set up in *Step 2* of the Getting Started with Expel guide)

H. For **Name** enter the hostname of the Cisco AMP device

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

J. For **API key** and **Client ID**, enter the API credentials generated in *Step 2, Letter F*

K. For **Username** and **Password** enter credentials previously created in the Cisco AMP console

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. Click the icon in the upper right to switch to grid view, then check the list for Cisco AMP for Endpoint 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.