expel®

Cisco Umbrella getting started guide

Version 1.0

October 6, 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 SOC;
2. Generate the API Credentials; and
3. Configure the technology 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.

Adding a new user

A. Navigate to **Admin > Accounts** and click **Add**

B. Add user's email address, **soc+<org_name>@expel.io**, and select **Read Only** User Role for the account

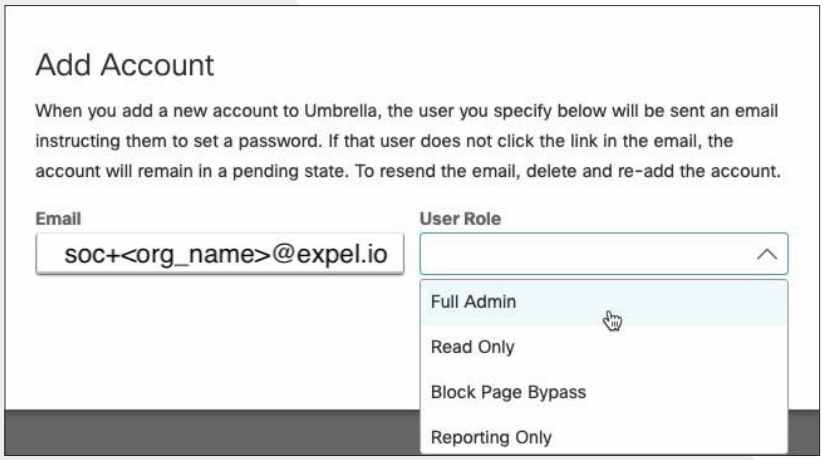

Figure 1

3. Click **Send Invitation**

   Account registration will be completed by Expel once registration email is received.

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 are unsure, please reach out to your Expel Customer Success Engineer (Tag @cse in Slack, or email customerhealth@expel.io).

A. Use your admin account to create an API Key. This can be found under **Admin > API Keys**:

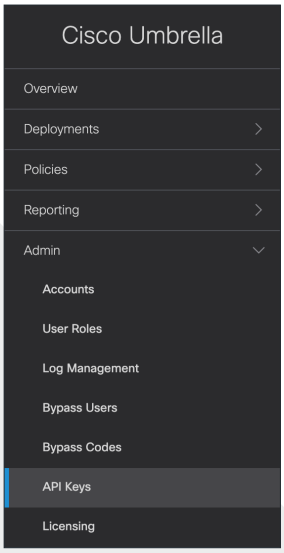

Figure 2

B. You will be asked "What should this API do?" Select **Umbrella Reporting**:

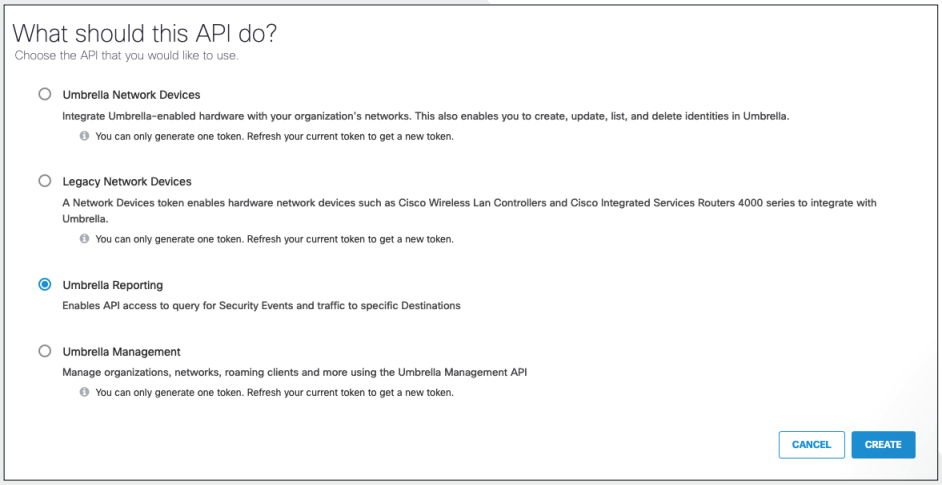

Figure 3

C. Copy both the **Key** and the **Secret** provided. Also make a note of your **Organization ID**. This can be determined by the url for your dashboard, as there will be a 7 digit number: https://dashboard.umbrella.com/o/xxxxxxx/ These will be used to configure your technology in Workbench in *Step 3*

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.

A. Login to https://workbench.expel.io

B. Navigate to **Settings > Security Devices**

C. At the top right of the page, select **Add New Device**

D. Search for and select your technology

E. Complete all fields using the credentials and information you collected in *Step 1* and *Step 2* above

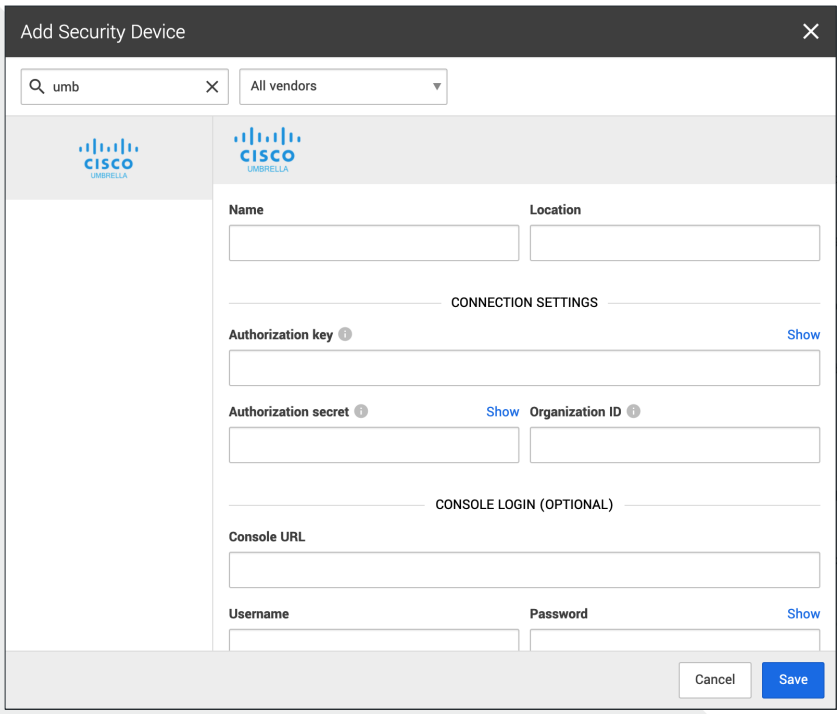

Figure 4

F. Select **Save**

G. After a few minutes (Between 1 and 15), refresh the **Security Devices** page and you should see your device reporting as *Healthy* or if there is an issue, it will provide more details of what the issue may be

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.