Palo Alto getting started guide

Version 2.0

March 16, 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 Palo Alto 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.

Expel will connect to your Palo Alto Panorama management console (console) on port 443.

This procedure will create a user account for Expel that will keep Expel's activity separate from other activity on the Palo Alto console.

Create an admin account

A. Log onto Palo Alto device

B. On console page, navigate to **Device > Administrators** (see Figure 1)

C. Click **Add** at the bottom left of the page (see Figure 1)

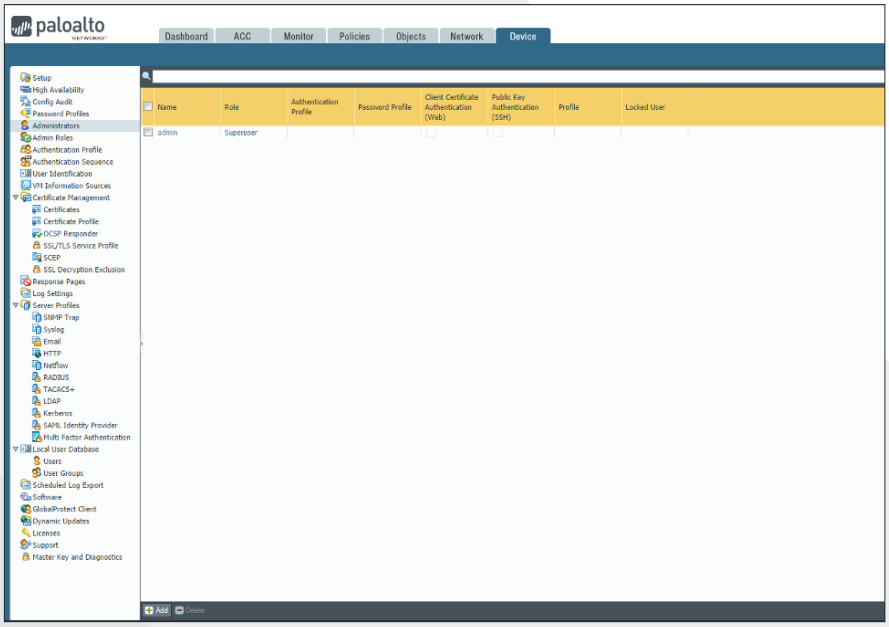

Figure 1

D. In Administrator dialog box, enter *expeluser* for **Name** (see Figure 2)

E. Enter the desired **Password** (see Figure 2)

F. Ensure the **Administrator Type** radio button is set to *Dynamic* (see Figure 2)

G. Select *Superuser (read-only)* from the dropdown below **Administrator Type** (see Figure 2)

H. Click **OK**

I. Verify that *expeluser* has been created on console page

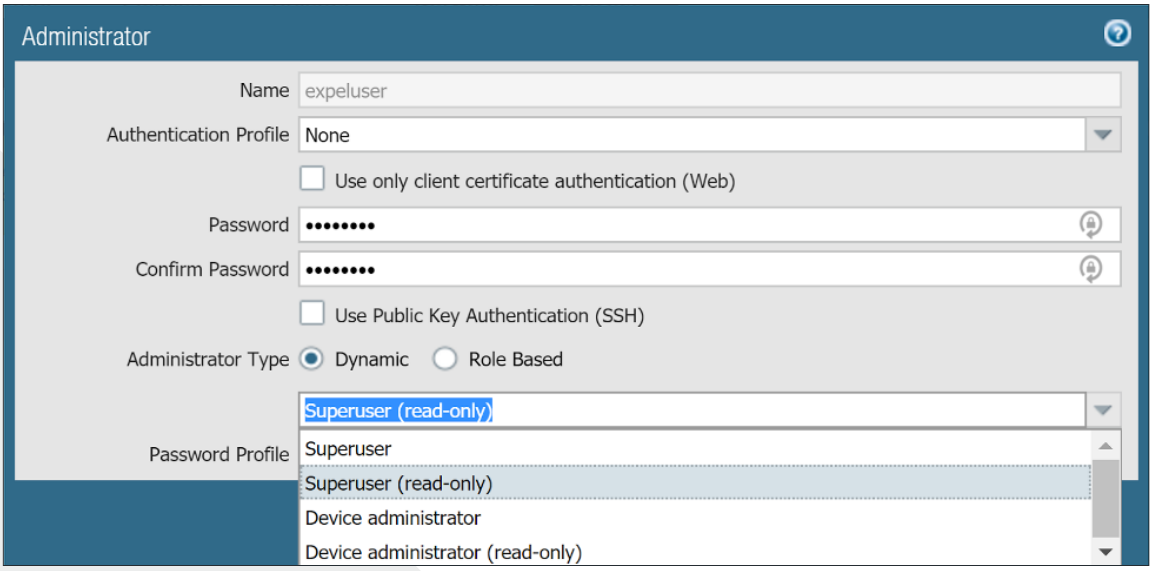

Figure 2

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*, or email customerhealth@expel.io.

This procedure will create an authentication token that allows the Expel Assembler to access the Palo Alto API. **Note:** Security Assertion Markup Language *(SAML)* authenticated accounts on Palo Alto cannot generate API keys

Create the API key for the '*expeluser*' account

A. In a new browser tab, access the following URL, replacing **<hostname or IP address>**, **<username>**, and **<password>** with the appropriate values for your Panorama console or the management interface of your Palo Alto Networks firewall:

https://<hostname or ip address>/api/?type=keygen&user=<username>&password=<password>

B. **<hostname or IP address>** is your Palo Alto URL from your console page (Figure 1)

C. **<username>** is the username created in *Step 1D* (expeluser)

D. **<password>** is the password entered in *Step 1E*

E. Once the URL is complete, press **Enter** (Figure 3 is an example of a completed URL)

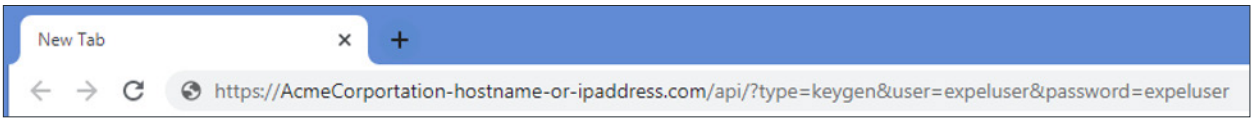

Figure 3

F. On the next screen will be the generated API key (example in Figure 4)

Figure 4

G. **Make note of the API key which will be used next for registration within Expel Workbench**

Step 3 — Configure the technology in Workbench

Now that we have the correct access configured and have noted the credentials, we can integrate Palo Alto with Expel.

Register device in Expel Workbench

A. In a new browser tab, log into 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** (Figure 5)

D. At the top right of the page, select **Add Security Device**

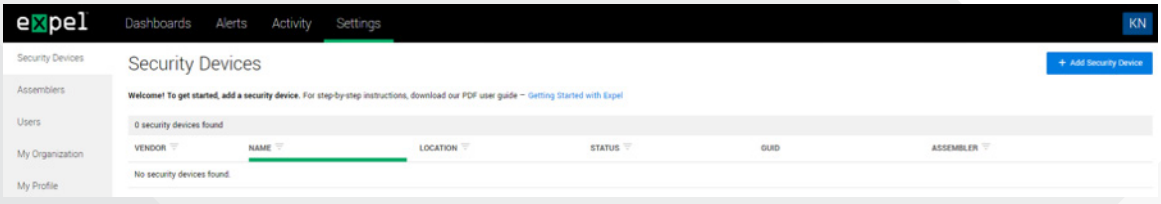

Figure 5

E. Search for and select Palo Alto (Figure 6)

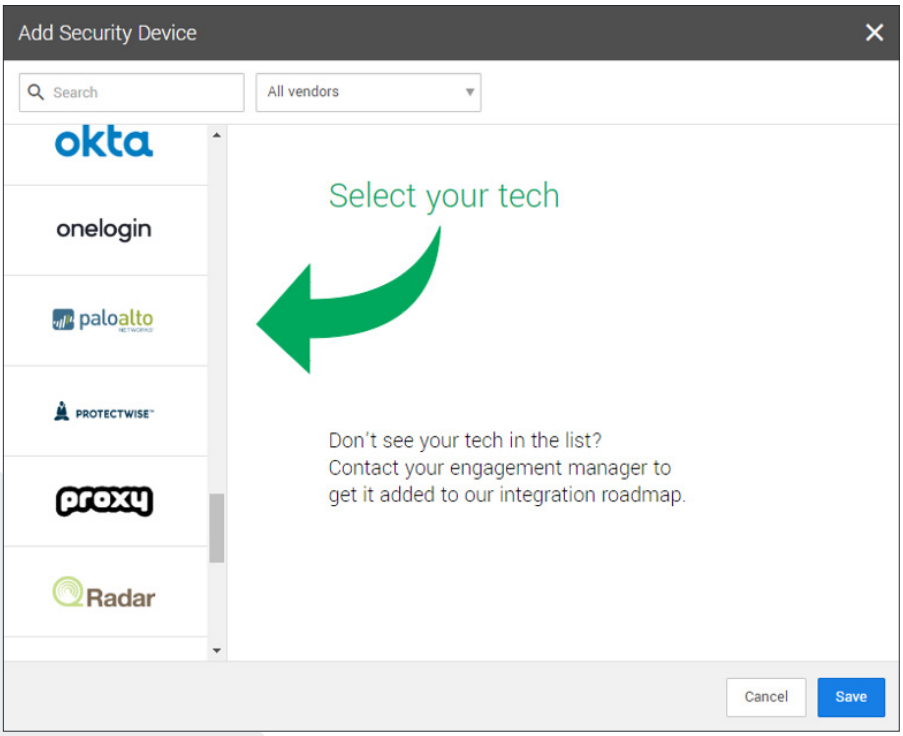

Figure 6

F. Refer to Figure 7 for *Steps G-M*

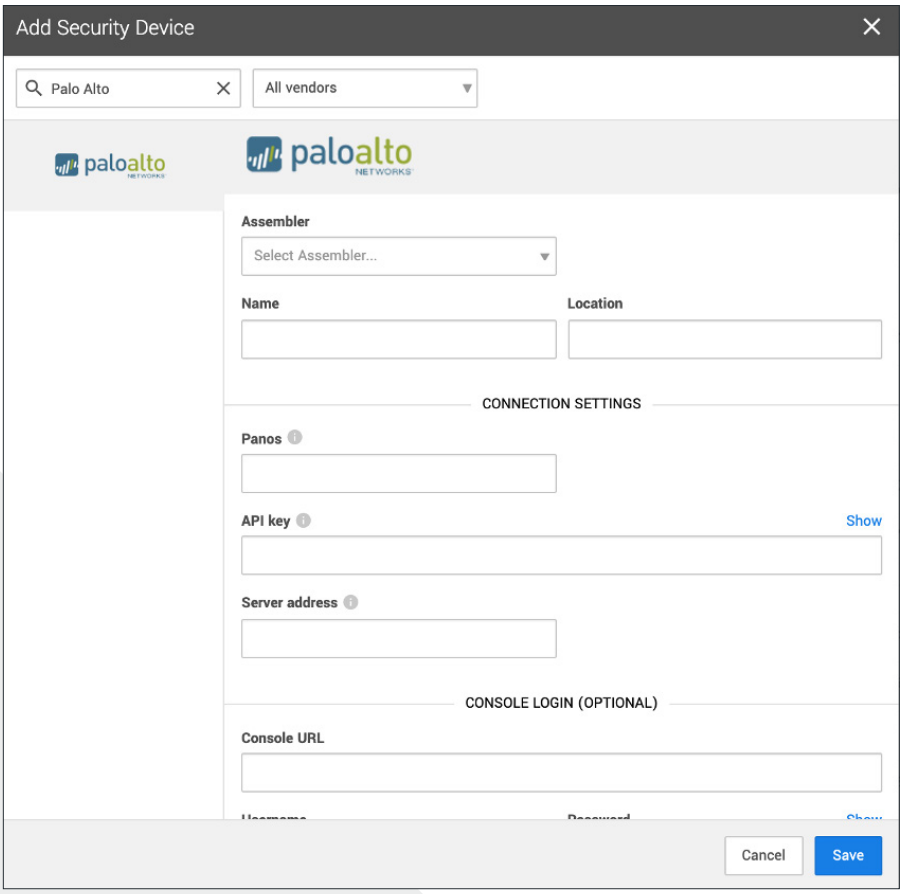

Figure 7

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. Enter Assembler **Name** and **Location** (example: *Palo Alto* and *Expel Lab*)

I. For **PanOS**, OS version must be specified if OS version is <= 6

J. For **API key** enter the API generated in *Step 2F*

K. For **Server address** enter the hostname or IP address of the Palo Alto management interface *(Device IP can be found in the console under Dashboard >> General Information >> MGT IP Address)*

L. **Username** and **Password** (in the optional Console Login section) fields can be left blank, or can be filled in with the username and password created in *Step 1D* and *1E*

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 Palo Alto 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.