Fortinet FortiGate getting started guide

Version 1.0

August 31, 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 FortiGate 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.

The FortiGate integration polls events from the /api/v2/log/{{ alert_source }}/{{ alert_type }} endpoints. The specific route depends on where the alerts are being polled from (ex: from memory as is the case where alert_source would be memory) and the type of alert. The alert_source is configurable through Workbench. Expel currently only supports the alert_type *Anti Virus, Web Filter, and Intrusion Prevention*.

A. An API token can be created by navigating to **System > Administrators > Create New > Administrator** (Figure 1)

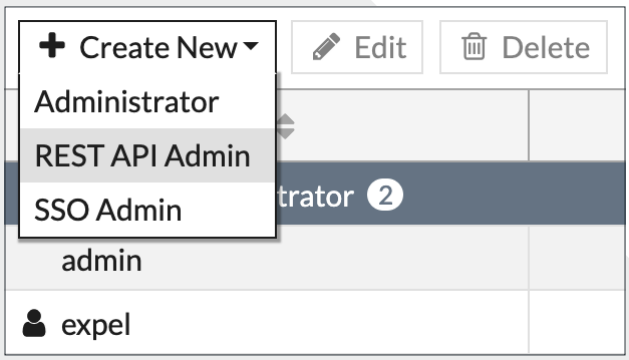

Figure 1

B. Choose the super admin read only role and optionally whitelist the IP of the assembler or the subnet the assembler is connected to if FortiGate is on premise; or whitelist the IP of Expel's Internal Proxy node if FortiGate is in the cloud

   The IP of Expel's internal proxy is: 165.227.202.51/32 (Figure 2)

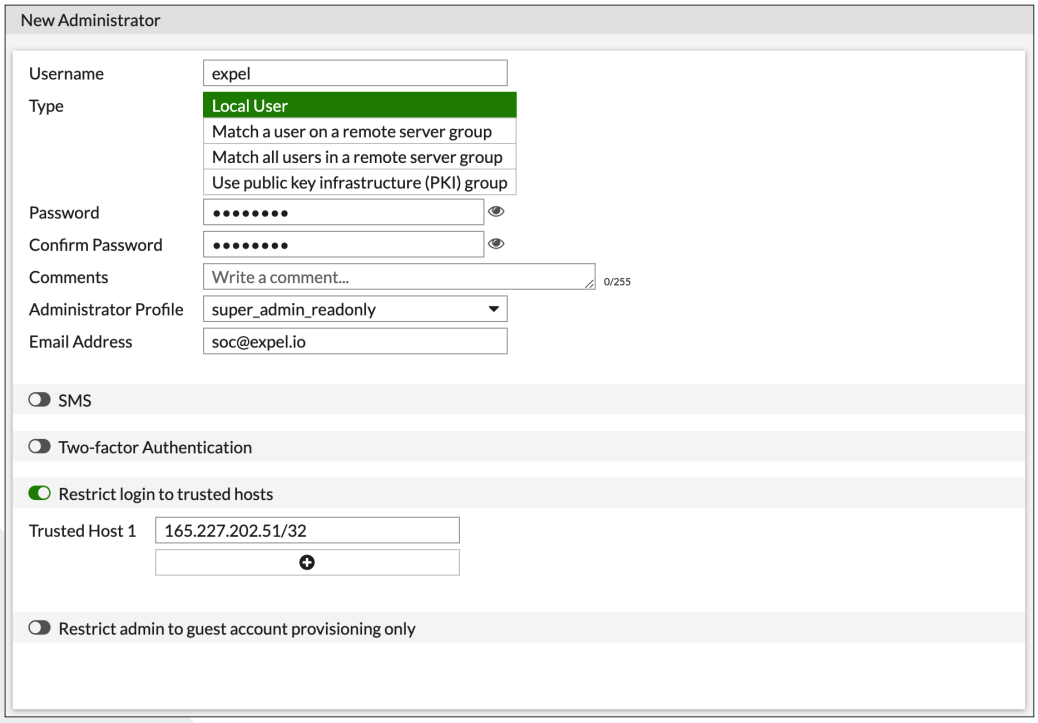

Figure 2

C. Please use the defined username and password when configuring Fortigate in Workbench

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. An API token can be created by navigating to **System > Administrators > Create New > REST API Admin** (Figure 3)

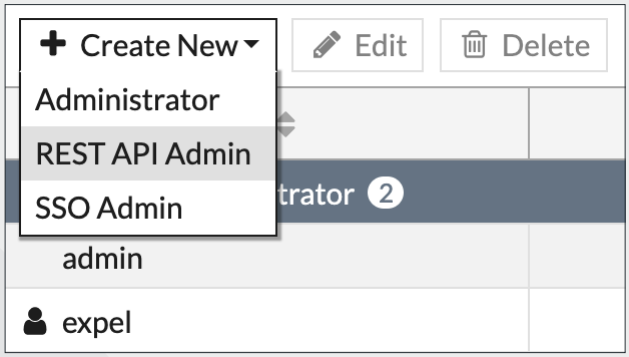

Figure 3

B. Choose the super admin read only role, disable the PKI group, and whitelist the IP of the assembler or the subnet the assembler is connected to if FortiGate is on premise; or whitelist the IPs of Expel's Task Pool nodes if FortiGate is in the cloud

The IPs of Expel's Task Pool nodes are:

104.248.229.158/32
104.248.63.128/32
134.209.113.23/32
134.209.120.9/32
134.209.71.236/32
142.93.123.9/32
142.93.196.8/32
142.93.51.126/32
142.93.55.155/32
142.93.59.117/32
142.93.59.150/32
142.93.59.250/32
157.245.129.146/32
157.245.129.151/32
157.245.129.173/32
159.203.179.53/32
159.89.229.255/32
159.89.87.151/32
159.89.87.153/32
165.227.87.38/32
165.227.91.110/32
167.99.3.128/32
174.138.42.82/32
192.241.136.143/32
204.48.18.106/32
67.205.149.216/32

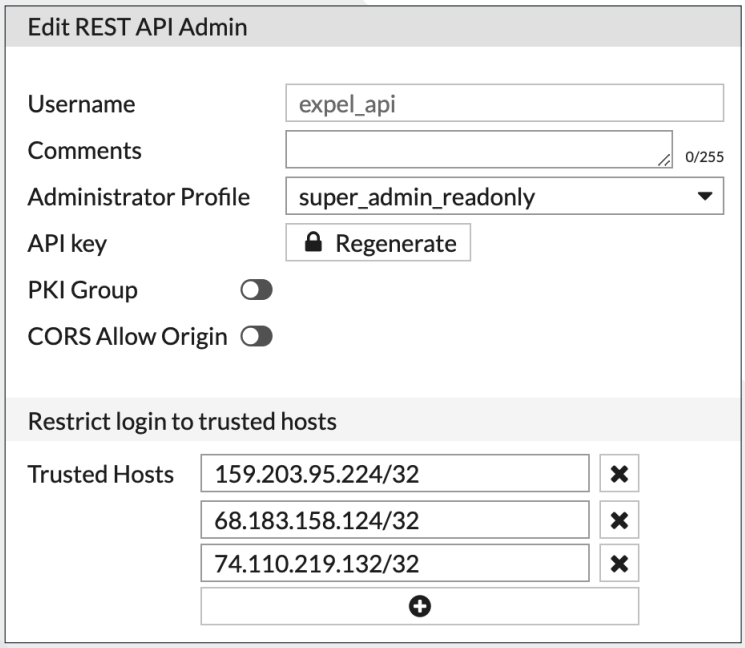

Figure 4

C. You will then be presented with an **API token**. Please use this token when configuring FortiGate in Workbench

Step 3 — Configure the technology in Workbench

Now that we have all the correct access configured and have noted the credentials, we can integrate FortiGate 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 5)

Figure 5

E. Search for and select your technology

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

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

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

I. For **Server address** enter the hostname or IP address of the FortiGate management interface (Device IP can be found in the FortiGate console under Dashboard > Status > System Information > WAN IP)

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

K. Username and Password fields can be left blank, or can be filled in with the username and password created in *Step 1*

L. Select **Save**

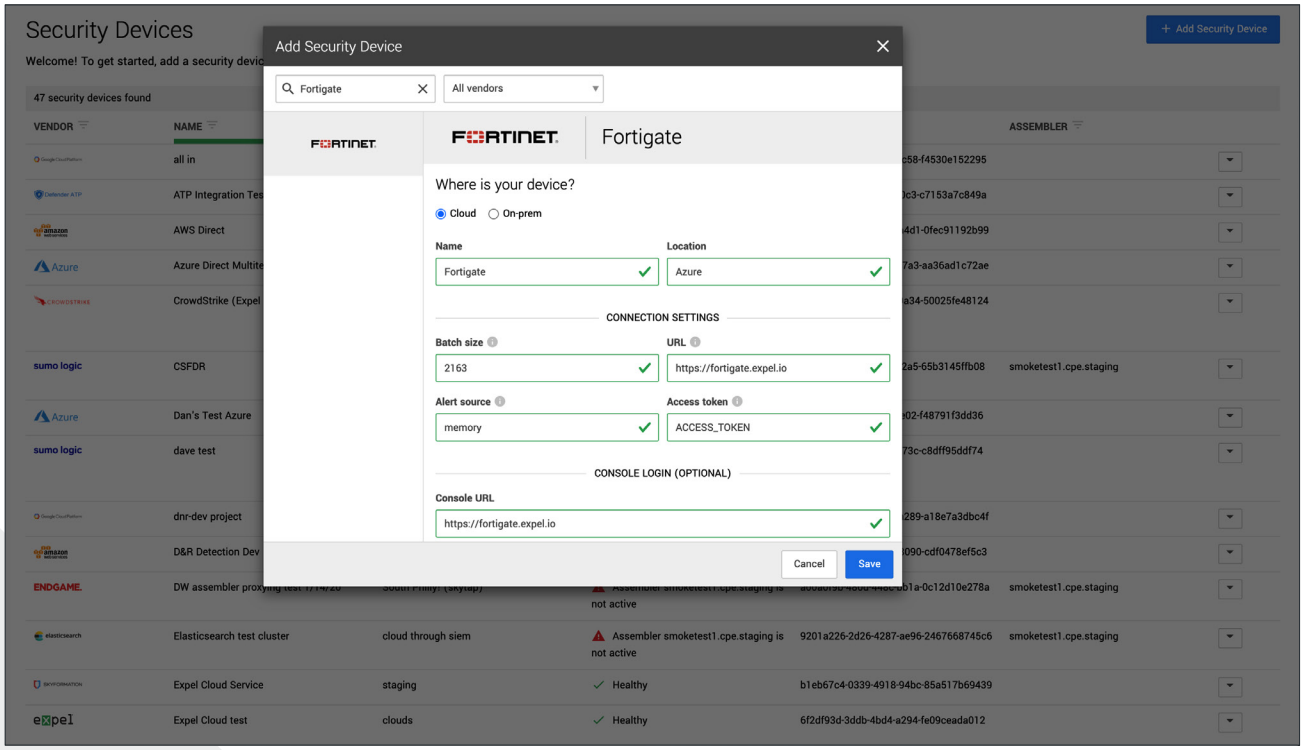

Figure 6

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 FortiGate 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.