DarkTrace Direct getting started guide

Version 2.0

March 4, 2020

Overview

Darktrace is an Intrusion Detection Device (“IDS”) that leverages machine learning to detect emerging threats, including insider threats, low-and-slow attacks and automated viruses.

What’s in this guide?

1. Enable and configure console access for the Expel Security Operations Center (SOC);
2. Generate the Application Program Interface (API) Credentials; and
3. Configure DarkTrace Direct 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 require a DarkTrace user account for the ability to review Alerts and Models within the console.

How to setup the user account:

A. Choose the Menu dropdown located at the top left

B. Select **Add New User**

C. Username: **Expel**

D. Password: **Set a temporary password** — this will be changed upon initial login

E. Account Permissions: **Select all available permissions, *except* User Admin** or **Group Admin**. These can be left unchecked.

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.

A. Login to the DarkTrace console

B. Navigate to **Admin > System Config** (Figure 1)

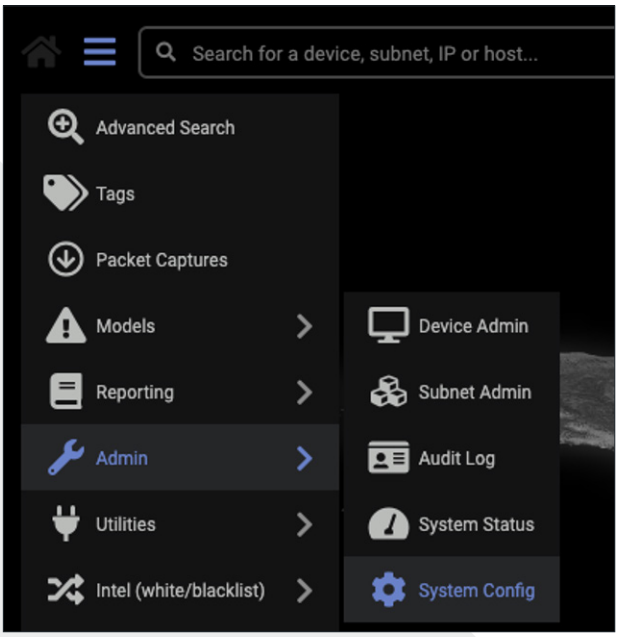

Figure 1

C. Towards the bottom of the page, under **API Token**, select **New** (Figure 2)

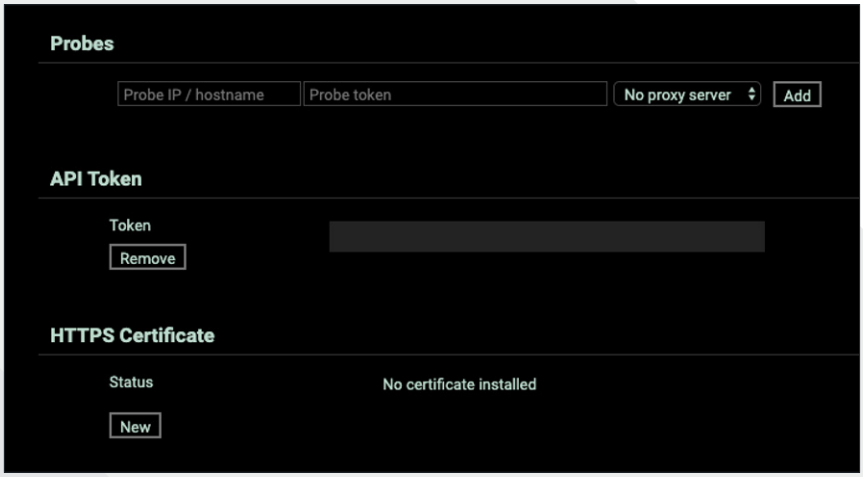

Figure 2

D. The DarkTrace system will generate a **Token** and a **Private Token**. The Private Token can only be seen once when the token pair is initially generated **(make note of the tokens for onboarding in Expel Workbench)**. The system can only have one token pair, so if one already exists and you do not have a record of this, another token pair must be generated.

Note: If a replacement Token pair is generated, other clients using the API will need to be reconfigured with the new credentials.

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.

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, **Settings** and click **Security Devices**

D. At the top right of the page, select **Add Security Device** (Figure 3)

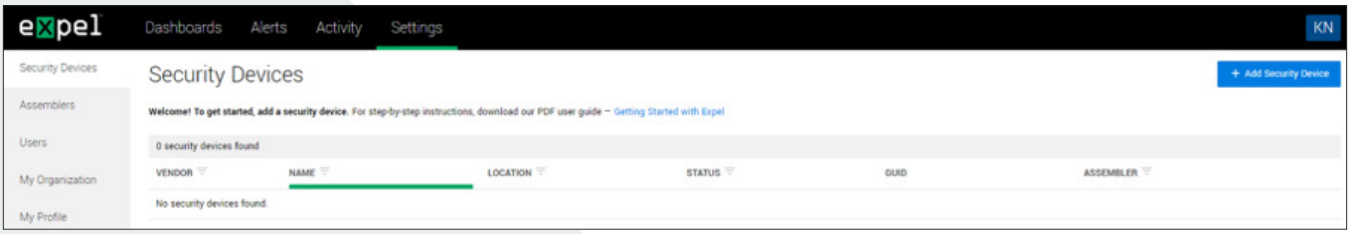

Figure 3

E. Search for and select your technology (Figure 4)

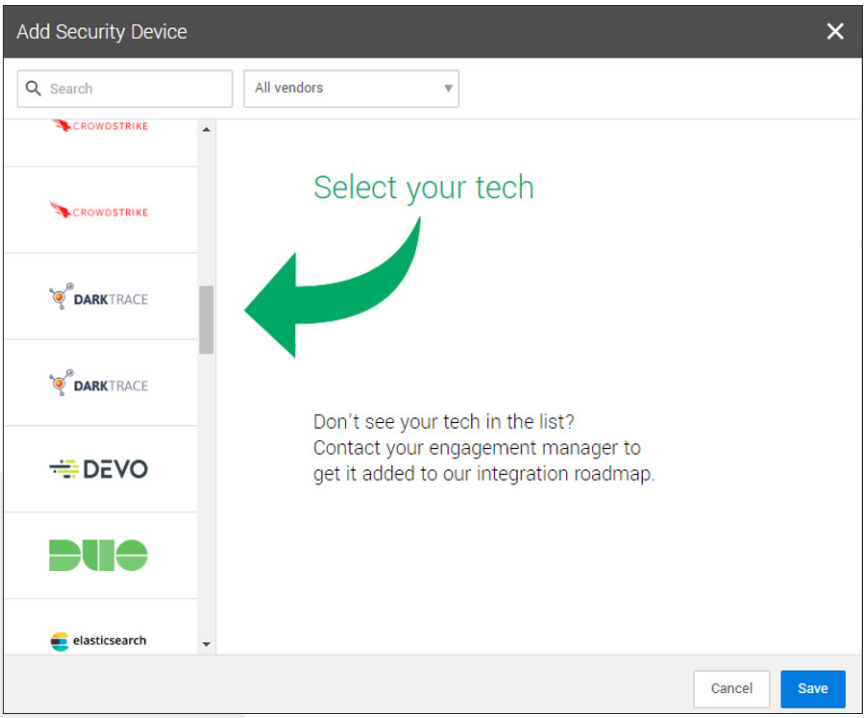

Figure 4

F. See Figure 5 when completing *Steps G-L*

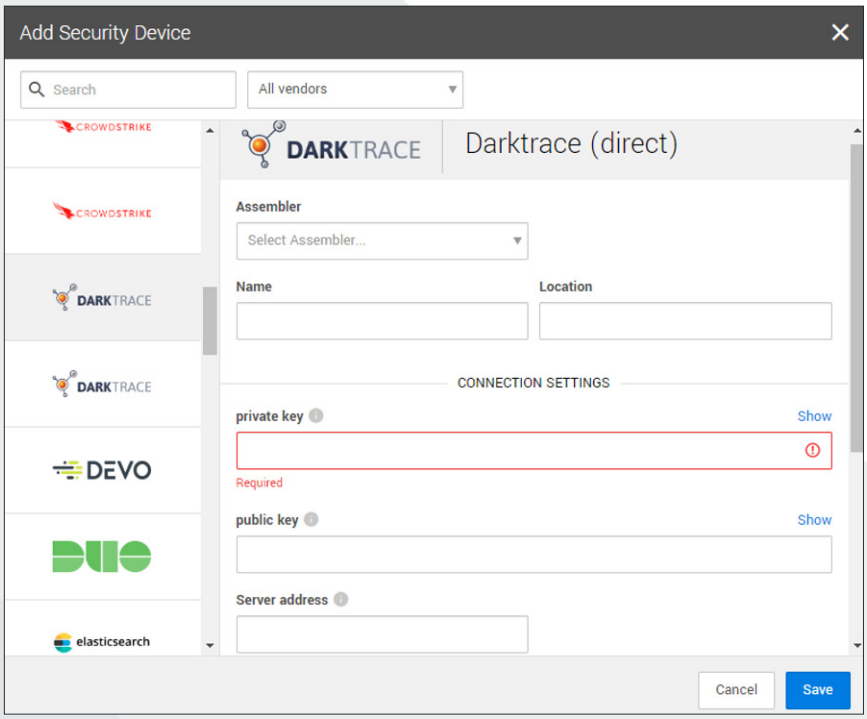

Figure 5

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 **Name** and **Location**

I. For **private key**, enter the private token used to authenticate to the device, from *Step 2, Letter D*

J. For **public key**, enter the API token used to authenticate to the device, from *Step 2, Letter D*

K. For **Server address**, enter the server address of the vendor's server, which must include the port. For example: 'https://127.0.0.1:443, or myvendordevice.acme.com:443'

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, then click the icon in the upper right to switch to grid view, then check the list for DarkTrace Direct 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.