Okta (direct) getting started guide

Version 1.0

June 23, 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 Okta (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.

A. Create a user in Okta for Expel

   a. Select **Users** and **Add Person** (Figure 1)

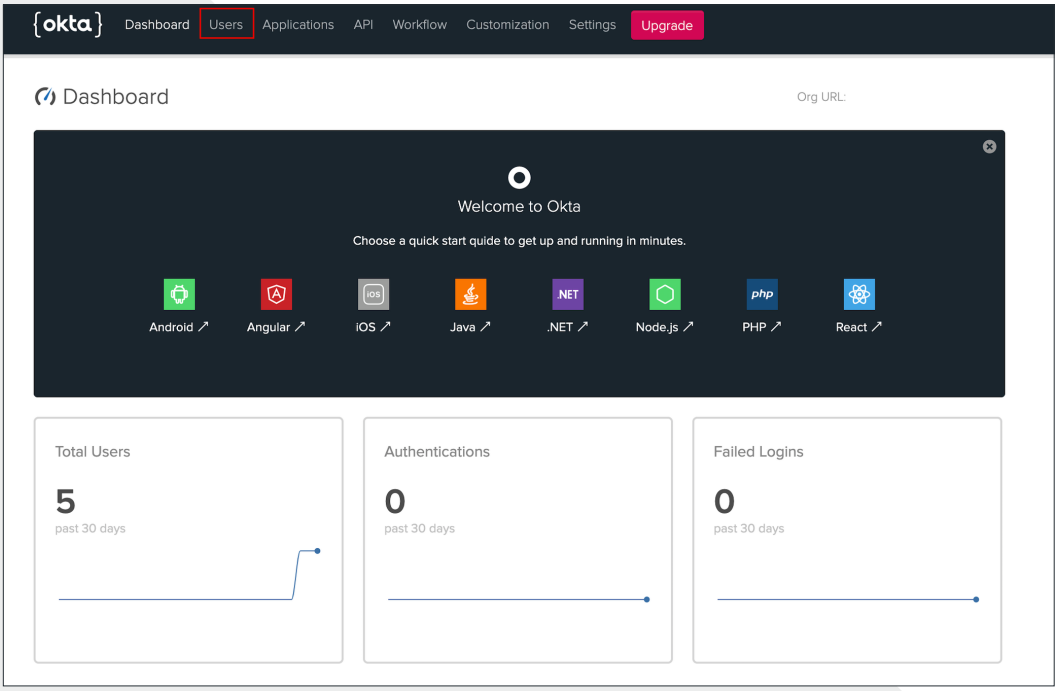

Figure 1

   i. User type: *User*
   ii. First name: *Expel*
   iii. Last name: *SOC*

iv. Username: *soc+[customer name]@expel.io*

v. Primary email: *same as username*

vi. Password: *Set by user*

vii. Checkmark *Send user activation email now* (Figure 2)

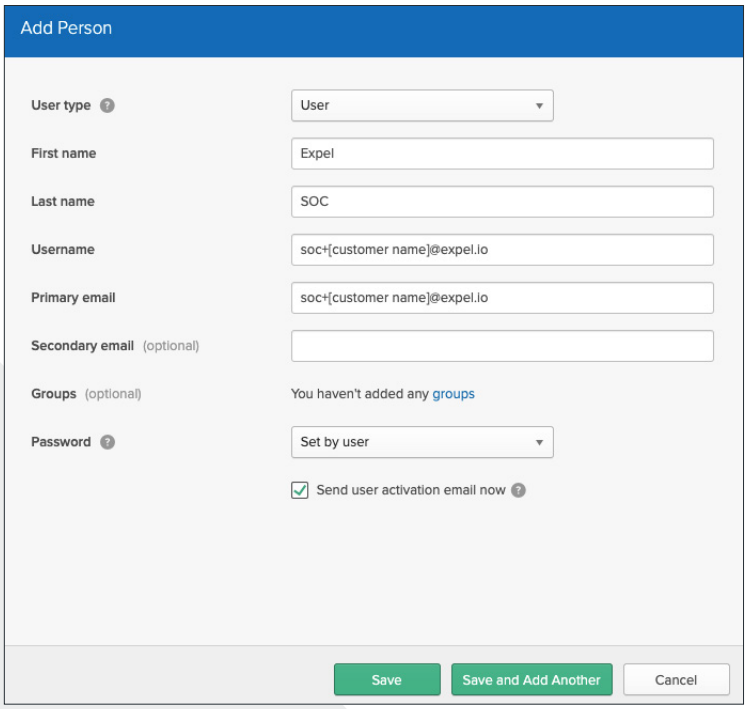

Figure 2

B. Notify your EM or CSE that the registration email has been sent

Step 2 — Generate API Credentials

In order to integrate Okta 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* via Slack, or email customerhealth@expel.io

A. Sign into your **Okta organization** as a user with **Read-Only Admin** privileges. API tokens have the same permissions as the user who creates them, and if the user permissions change, the API token permissions also change

   a. Okta permissions table https://help.okta.com/en/prod/Content/Topics/Security/Administrators.htm?cshid=Security_Administrators#Security_Administrators

B. Access the **API page**

a. If you use the **Developer Console**, select **Tokens** from the **API menu** (Figure 3)

b. If you use the **Administrator Console** (Classic UI), select **API** from the **Security menu**, and then select **Tokens**

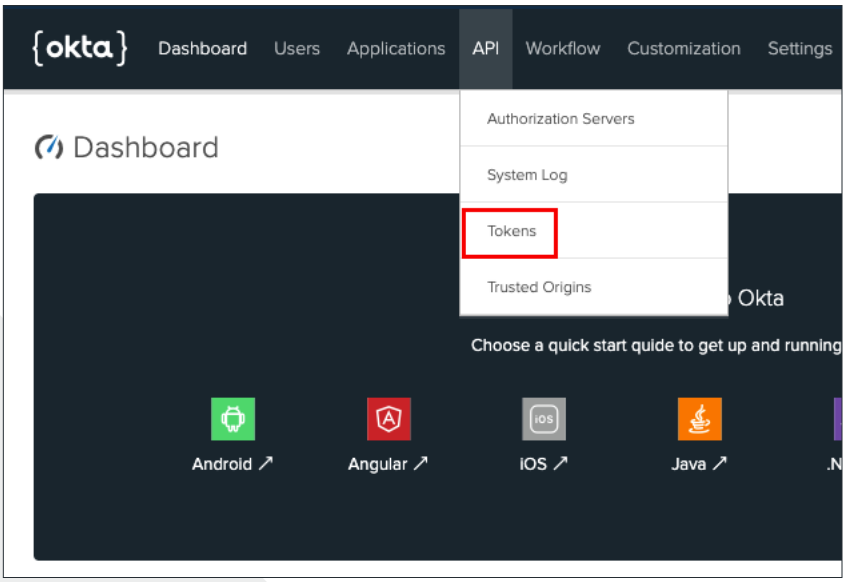

Figure 3

C. Click **Create Token** (Figure 4)

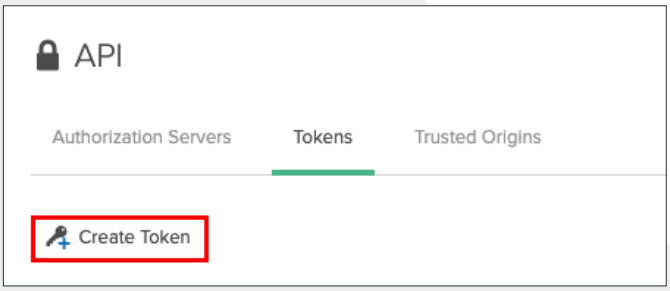

Figure 4

D. Name your token “ExpelAPI” and click **Create Token** (Figure 5)

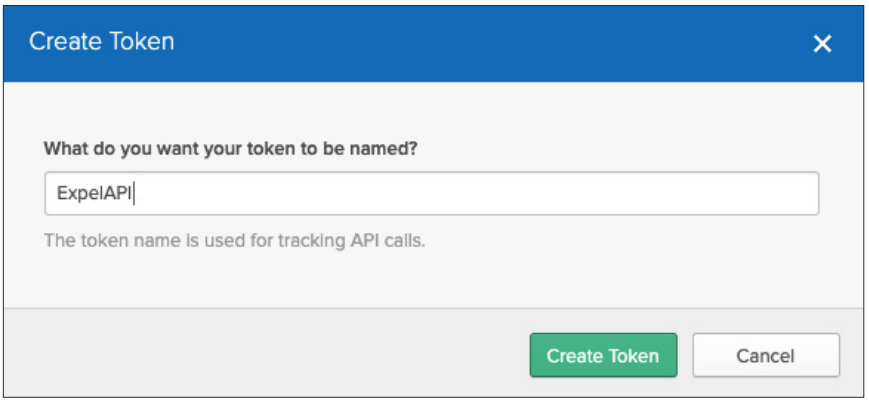

Figure 5

E. Make note of your API token, as you only see it one time

F. Collect your **Okta URL** (also called an Okta domain)

   a. Sign in to your Okta organization with your administrator account

   b. Look for the **Okta domain** in the top right corner of the dashboard

Step 3 — Configure the technology in Workbench

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

A. Log into 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 **Okta Direct** (1st option) — Figure 6

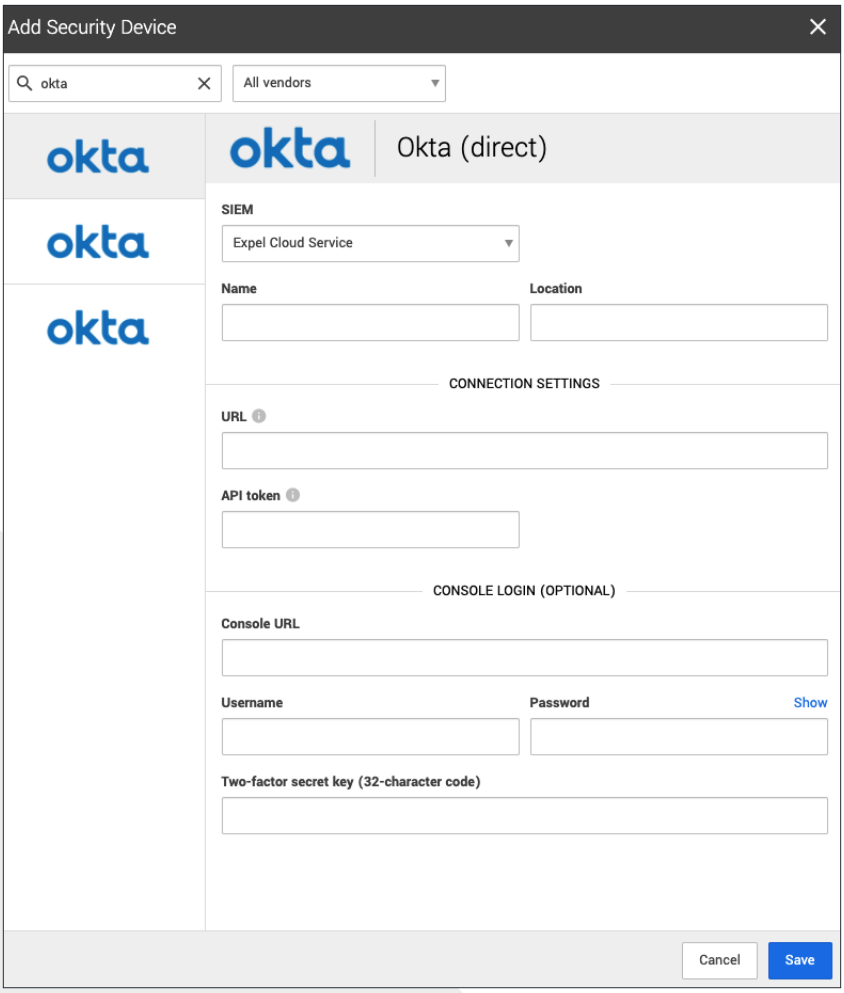

Figure 6

E. Select **Expel Direct Cloud Service** for the SIEM

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

G. Select **Save**

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

I. 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 Okta 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.