Configuring your Okta SSO provider with Workbench

Version 2.0

April 29, 2020

Configure Okta with Expel Workbench

A. Log into your **Okta** console

B. Navigate to **Applications** in the main top navigation

C. On the left of the page, select **Add Application**

D. On the left of the page, select **Create New App**

E. The settings should be as follows: (see Figure 1)

a. Platform: **Web**

b. Sign on method: **SAML 2.0**

c. Click **Create**

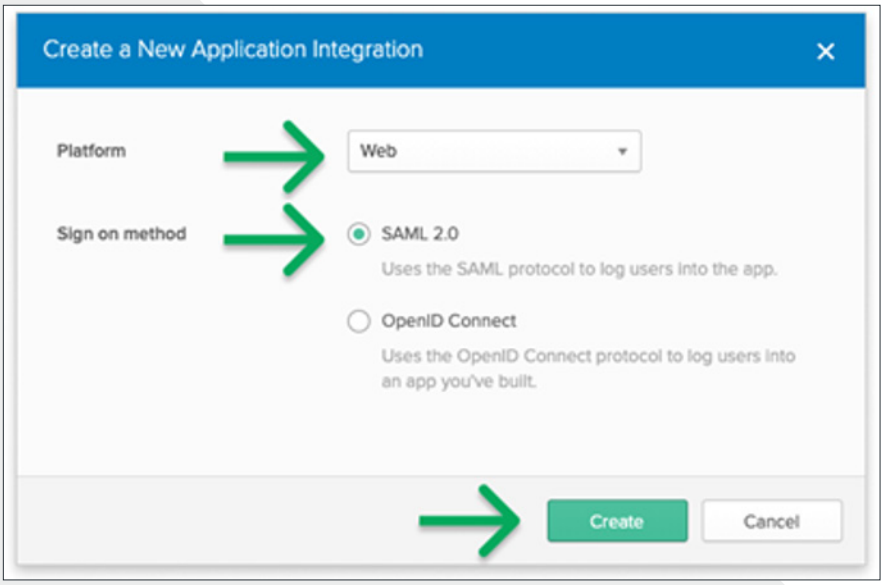


Figure 1 (Note: This screen may look slightly different depending on your Okta account)

F. Under **General Settings**

a. App name: **Expel Workbench**

b. Upload our logo, which should be provided to you by Expel

c. Click **Next**

G. You should now be on the **Configure SAML step in Okta**. You will need to copy information from Expel Workbench to complete the integration, so open a new tab or window and log into Expel Workbench (https://workbench.expel.io)

H. Navigate to **Settings > My Organizations** and select the organization. Then select the **Integrations** tab and select the **Configure SSO** link under **Single Sign-on** (Figure 2)

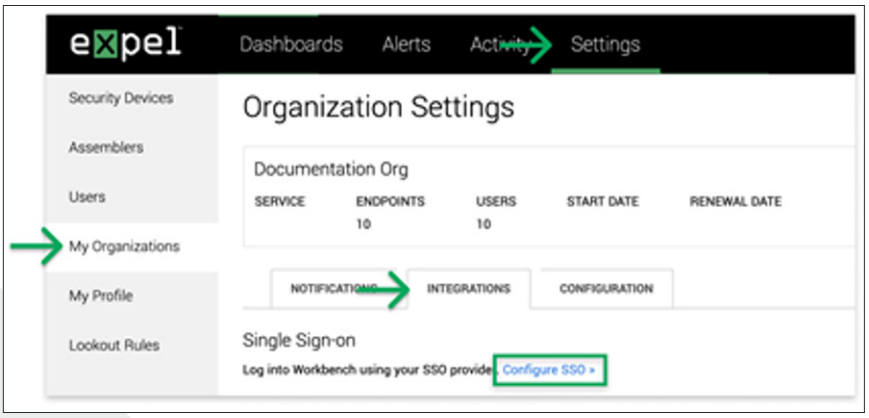


Figure 2

I. Next, copy and paste the following from Expel Workbench, into **Okta**: (Figure 3)

a. **ACS URL or Single Sign-on URL → Single sign on URL**

b. **Audience URI or Audience → Audience URI (SP Entity ID)**

c. Leave **Yes, allow users to log in locally OR via SSO** selected for local logins. This is to make initial SSO setup easier. You can change this later

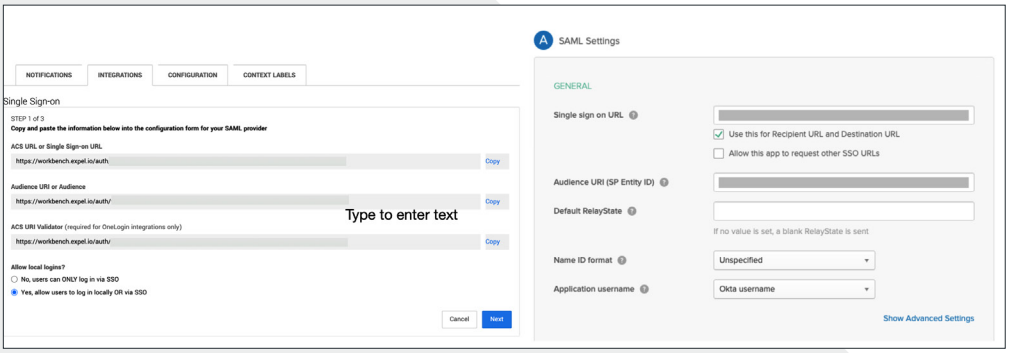


Figure 3

J. In **Okta** under **(A) SAML Settings, Attribute Statements (Optional)** — See Figure 4:

a. Enter the word “email” under **Name**, and select “user.email” from the **Value** dropdown

b. Note: **These are case sensitive**

c. Click **Next**

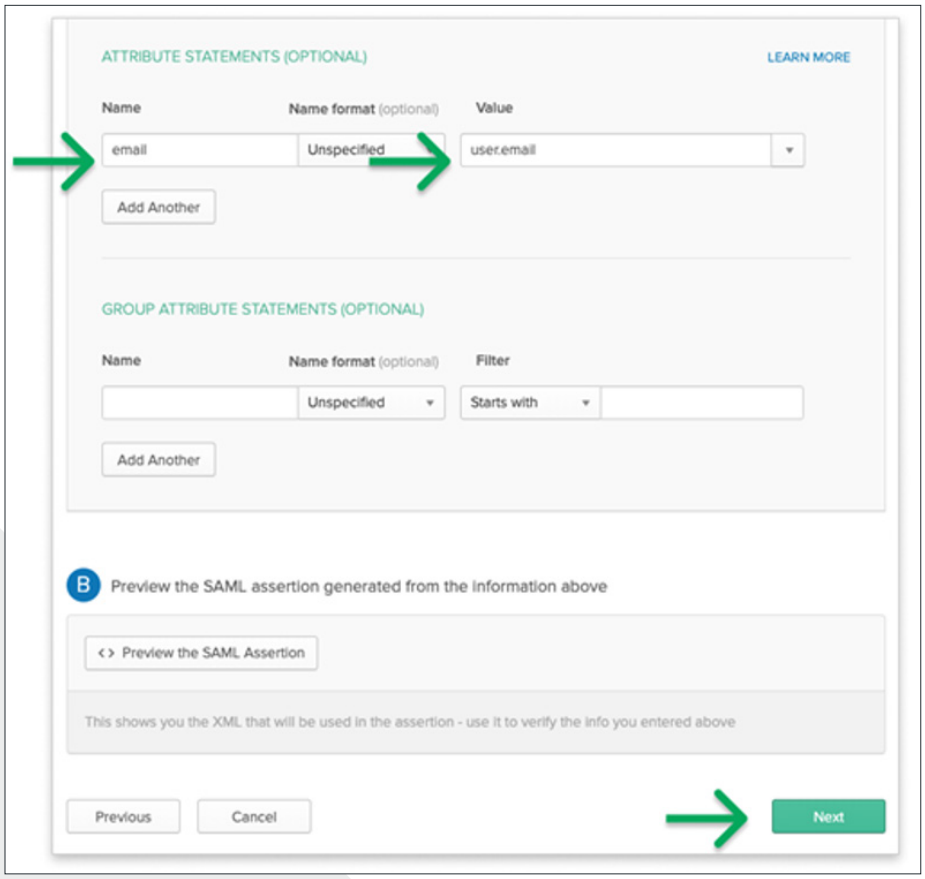


Figure 4

K. For the Okta feedback form, select '**I'm an Okta customer adding an internal app**' and fill in the following optional information as you see fit. Or select the '**This is an internal app that we have created**' checkbox. Then select **Finish**

L. In Okta, under **Sign On, Settings**, select **View Setup Instructions** (Figure 5)

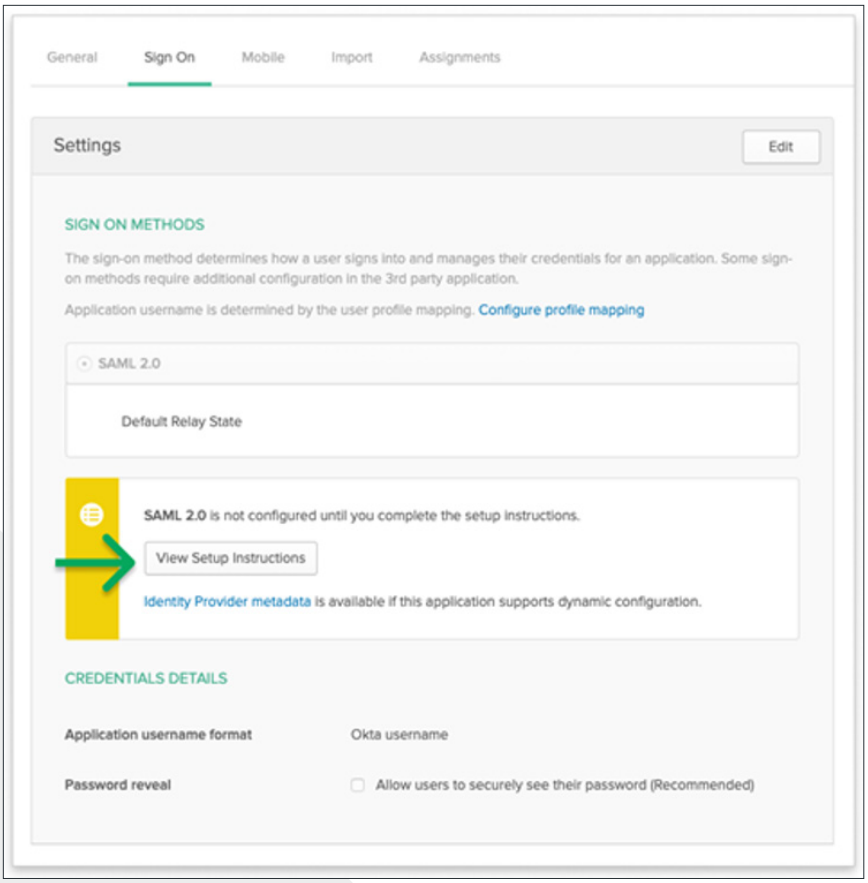
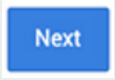


Figure 5

M. In Expel Workbench, select **Next** twice, until you see *Step 3 of 3*



N. Copy and paste the following from **Okta** into Expel Workbench (Figure 6)

   a. **Identity Provider Single-Sign-On URL → Single Sign-On URL or SAML 2.0 Endpoint**

   b. **Identity Provider Issuer → Issuer or Issuer ID**

   c. **X.509 Certificate → Certificate**

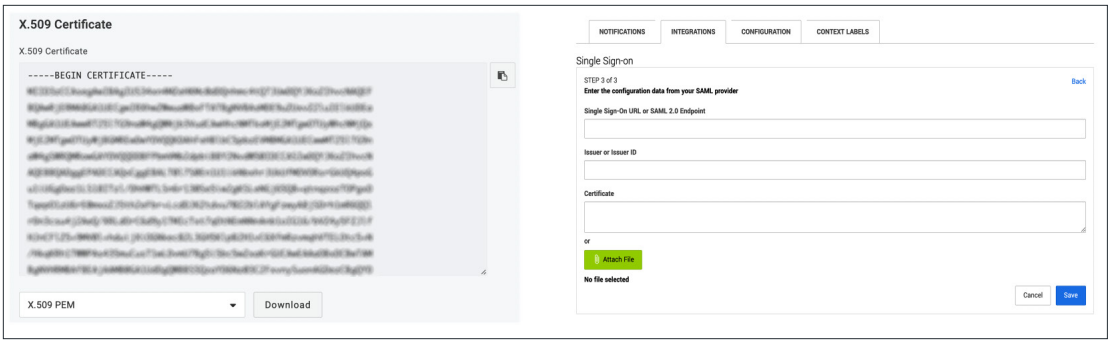


Figure 6

O. Click **Save** in Expel Workbench

Please Note

Before signing in with SSO, please make sure that:

- In Okta, the Workbench application is assigned to all intended users
- The user email addresses you have in Okta match the email that is configured for the user in Workbench; the emails are case sensitive
- New members of your organization that need access to Workbench have user accounts created in Workbench, and have the Workbench application assigned to them in your Identity Provider
- When you are completely finished testing and setting up, in Expel Workbench, you can disable local logins by selecting **Edit** from the dropdown button on the right side, and selecting **No, users can ONLY log in via SSO** (Figure 7). Then select the buttons **Next, Next, Save** to save

Figure 7

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.