Configuring SSO with Okta

Last Modified on Oct 26, 2020

This article provides a step-by-step guide to configuring SSO between OnceHub and Okta.

Requirements

To configure SSO in your account, you must be a OnceHub Administrator. However, you do not need a product license. Learn more

You must already have an account with Okta. The person configuring in Okta must be an administrator.

Step-by-step directions

Request access

SSO is intended for accounts with multiple users who take the extra security measure of signing into third-party applications using an identity provider. Please contact us to learn more. OnceHub can enable the SSO functionality in your account manually.

SAML configuration

You can access SAML configuration at OnceHub **Account settings** -> In the lefthand sidebar, select **Security** -> **SSO**.

OnceHub provides specific field values you can copy and configure within Okta.

Make sure you're in the Classic UI. You can select this by going to **Developer Console** -> **Classic UI**.

1. Create a New Application Integration

In Okta, go to **Applications** -> **Create New App**.

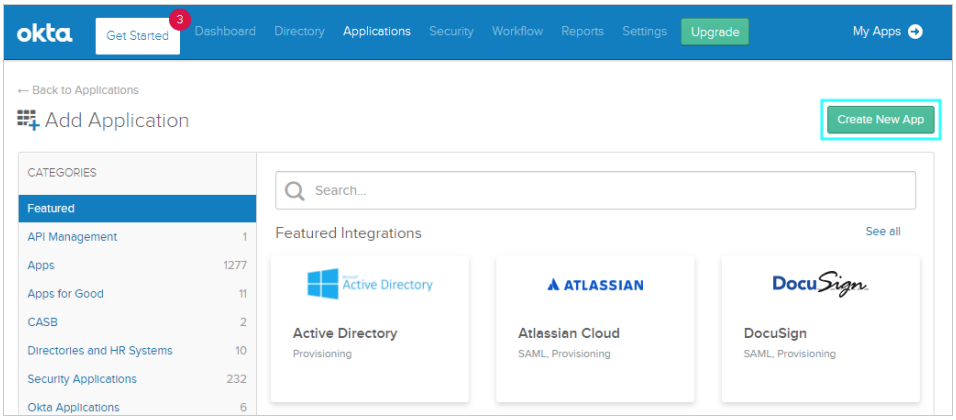

Figure 1: Create New App

In the popup, select **Web**. The sign on method should be **SAML 2.0**. Click **Create**.

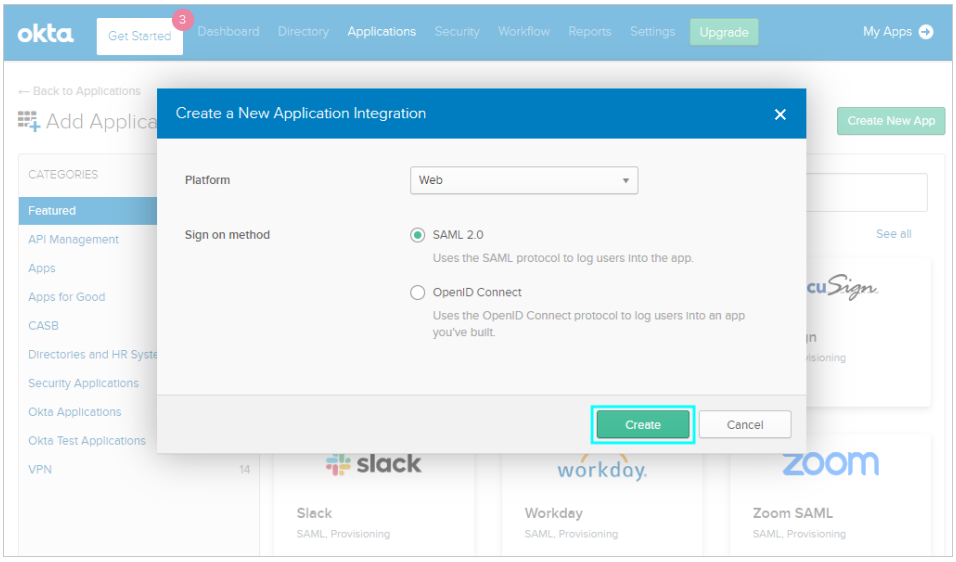

Figure 2: Create a New Application Integration

2. General Settings

On the **Create SAML Integration** page, give the app a name (for instance, OnceHub) and fill out the **General Settings**.

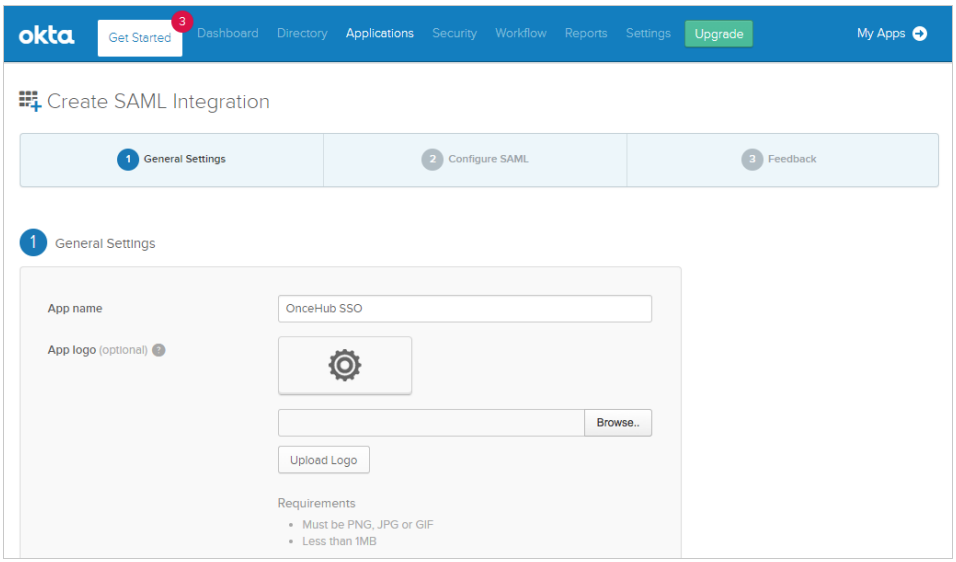

Figure 3: General Settings

3. SAML Settings from OnceHub

On the **Configure SAML** step, fill out the SAML Settings. You can grab these values in OnceHub, on the **Required by identity provider** step.

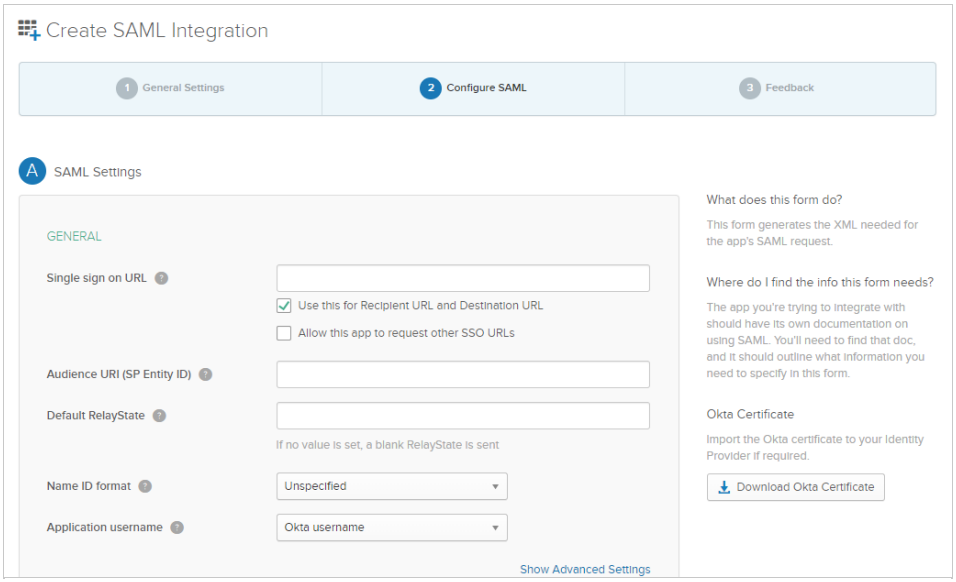

Figure 4: Configure SAML Settings

In Okta	In OnceHub
Audience URI (SP Entity ID)	Identifier URL
Single sign on URL + Select checkbox **Use this for Recipient URL and Destination URL**	ACS URL
[Not required; Okta refers to ACS URL for this function]	~~Single sign-on URL~~

These are the only required fields; the rest can be left blank.

4. Add an Attribute Statement

For the **Name** field, use **email** (in lower case). Map this to the **Value** field **user.email**.

You can keep the **Name format** on **Unspecified**.

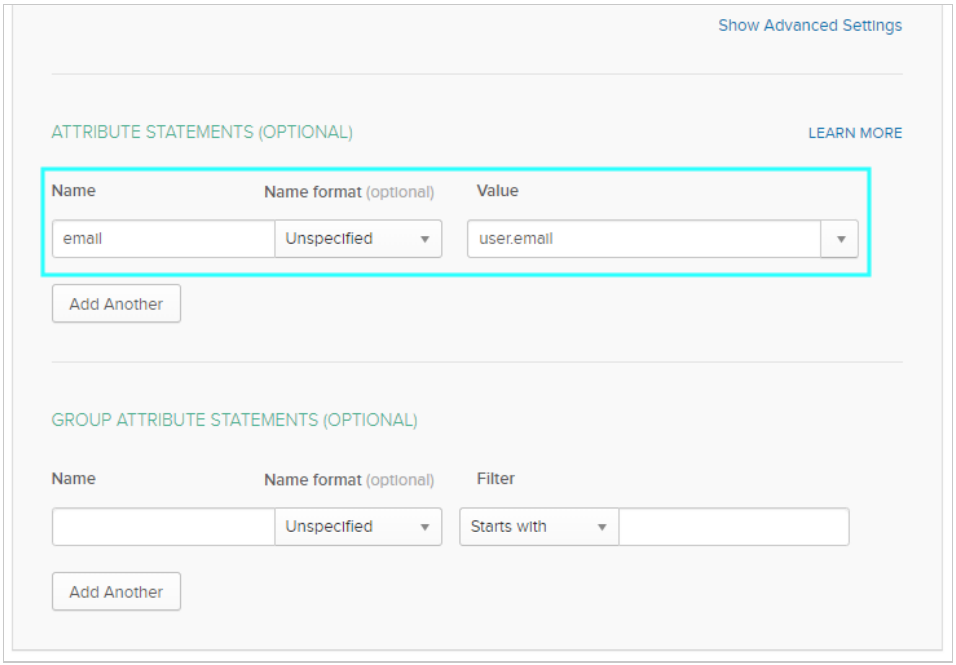

Figure 5: Attribute Statement for email

Once you're ready, click on **Next** and then **Finish**.

5. Grab information from Okta and paste in OnceHub

Click on **View Setup instructions**, which provide the information you will add in OnceHub.

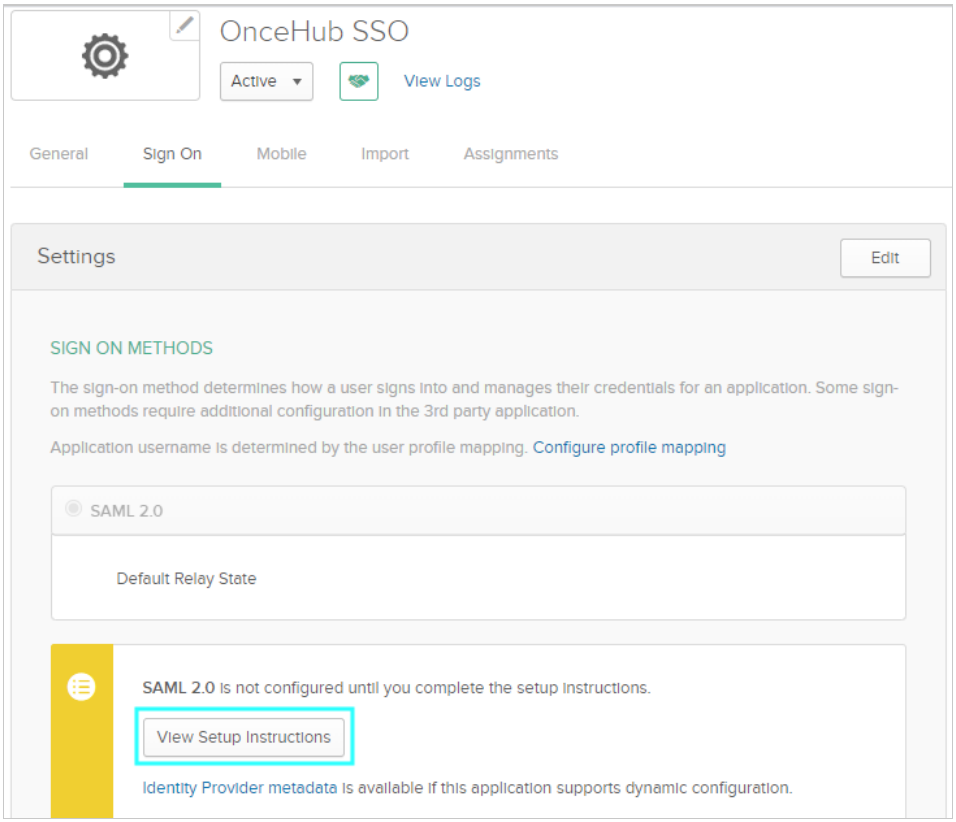

Figure 6: View Setup Instructions

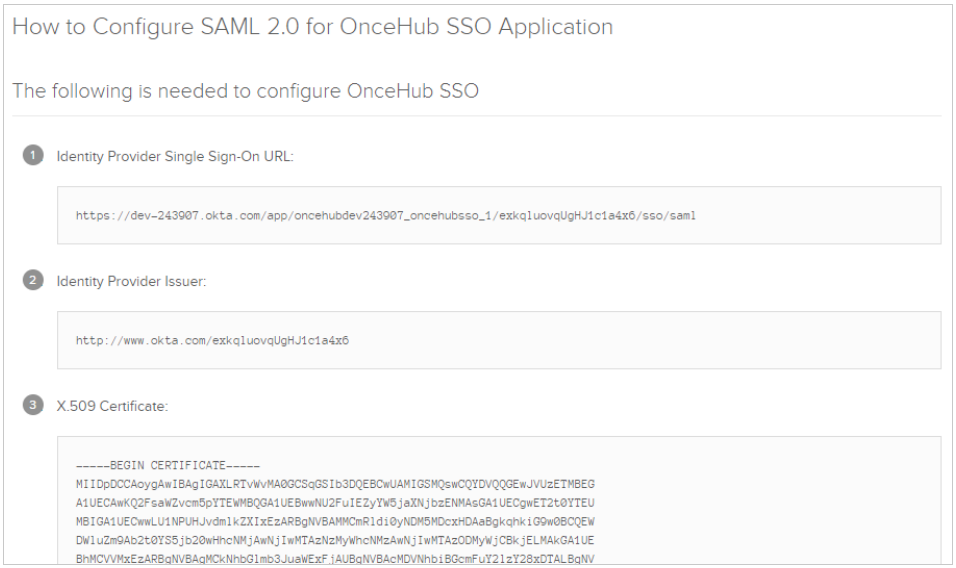

Figure 7: Information from Okta required in OnceHub

In Okta	In OnceHub
Identity Provider Issuer	Entity ID
Identity Provider Single Sign-On URL	IDP single sign-on URL
X.509 Certificate	Public x509 certificate

Important:

For the Public x509 certificate, include the **-----BEGIN CERTIFICATE-----** and **-----END CERTIFICATE-----** syntax in your selection and paste it all into the OnceHub field.

6. Assignments

Before clicking Verify in OnceHub, go back to Okta and access **Assignments**. Click on the **Assign** dropdown and select **Assign to People**.

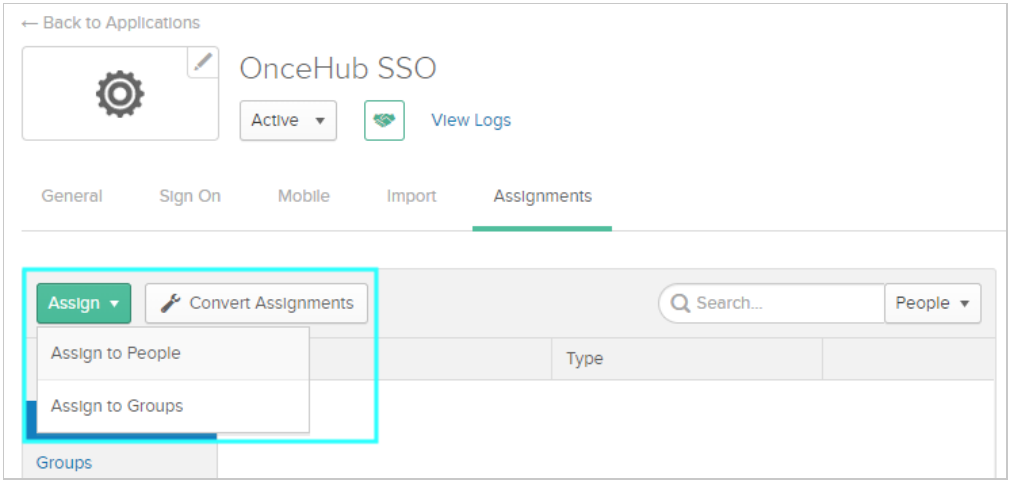

Figure 8: Assign to People

Assign your new OnceHub SAML 2.0 application to the relevant people in Okta.

7. Verify

In OnceHub, click **Verify** to confirm that SAML authentication is verified.

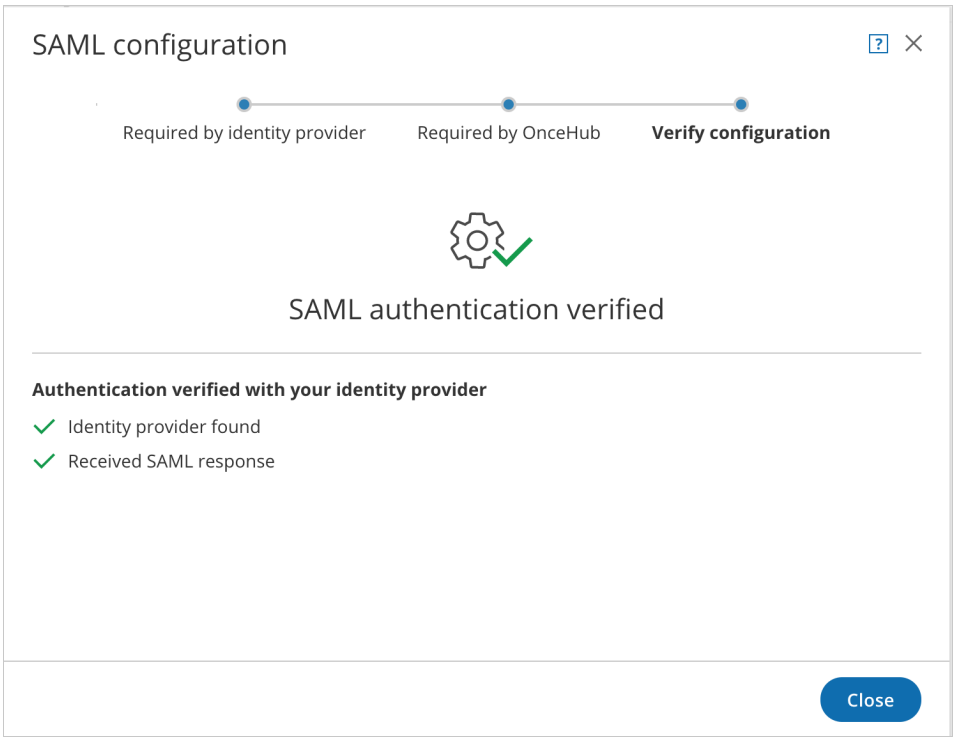

Figure 9: Verify configuration

8. Enable SSO for all users

Once you've verified your SSO configuration, you can select the **Enable SSO for all users** toggle. All Users in your OnceHub account can now access their account using SSO.

Important:

Before you enable the account, make sure all your Users have matching email addresses for their OnceHub User profile and their Okta profile.

Once SSO is enabled, they **will not** be able to change their OnceHub email.

If their OnceHub email does not match the email in their IDP profile, they **will not** be able to log in.

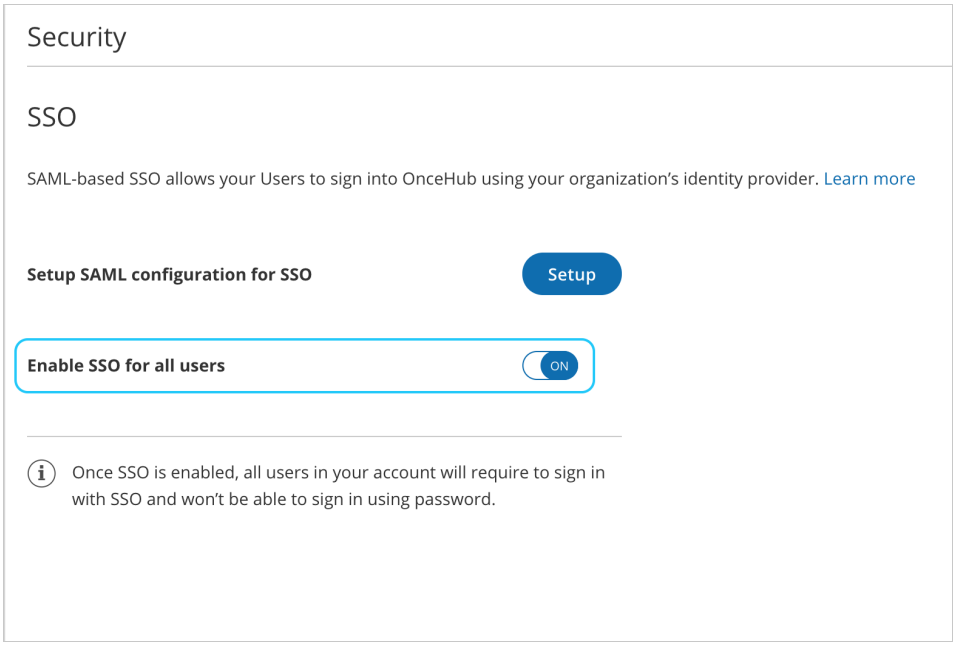

Figure 15: Enable SSO for all users

Note:

If existing Users were already signing into OnceHub using an email and password, they will no longer be able to do so. They will only be able to sign in using SSO.