Configuring SSO with OneLogin

Last Modified on Oct 26, 2020

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

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 OneLogin. The person configuring in OneLogin 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 OneLogin.

1. Add SAML Test Connector (Advanced)

In OneLogin, go to **Administration** -> **Applications**. Search for **SAML Test Connector (Advanced)** and select (making sure to select the SAML 2.0 version).

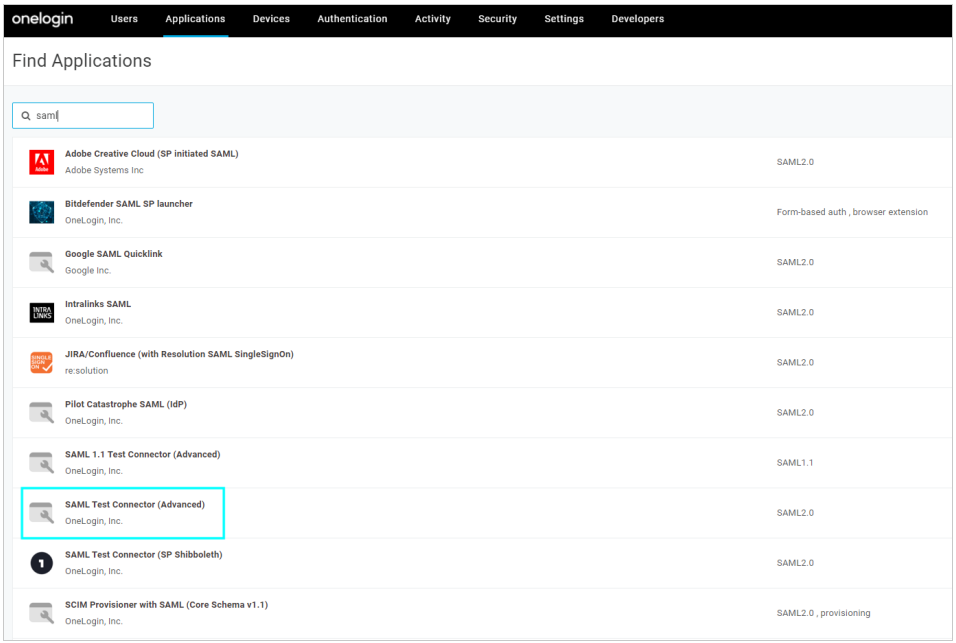

Figure 1: Select SAML Test Connector (Advanced)

2. Configuration

Give the app a name (for instance, OnceHub) and fill out the other settings.

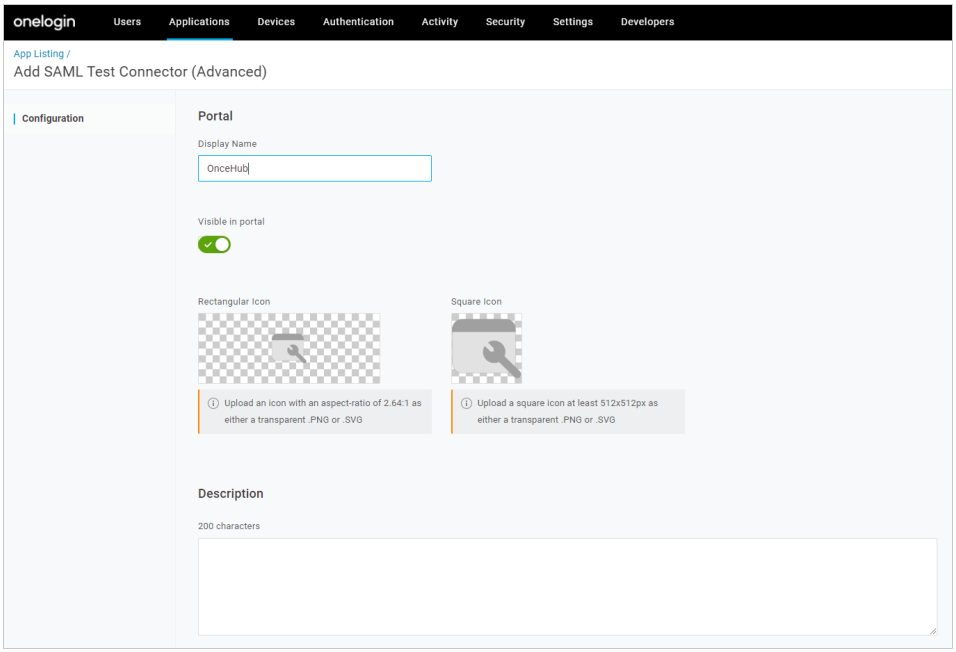

Figure 3: Display Name settings

3. Configuration - Application details

On the **Application details** page, fill out the SAML settings. You can grab these values in OnceHub, on the **Required by identity provider** step.

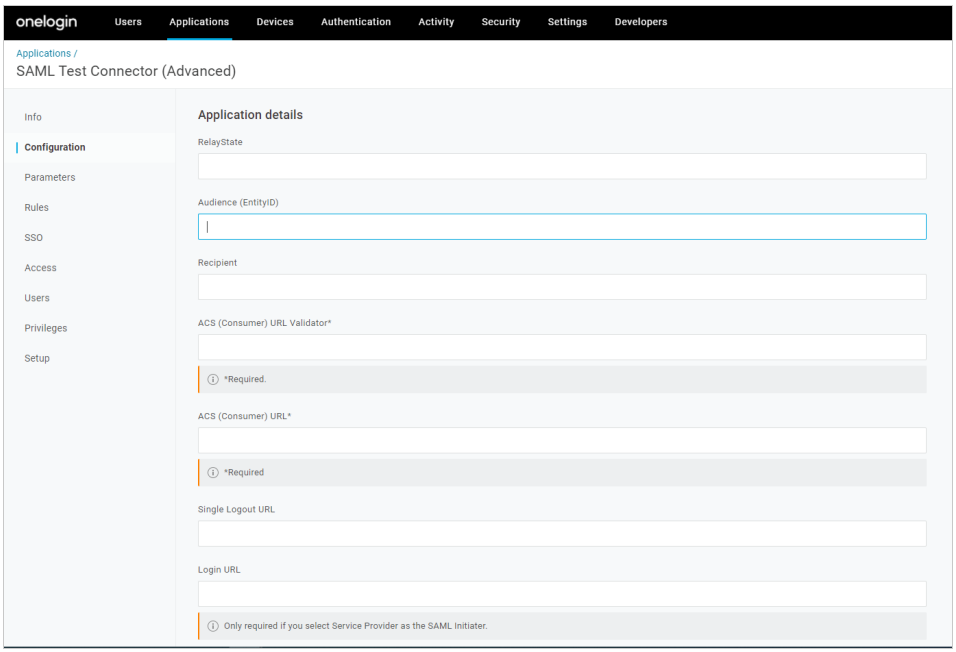

Figure 4: Configure Application details

In OneLogin	In OnceHub
Audience (EntityID)	Identifier URL
ACS (Consumer) URL Validator	ACS URL
ACS (Consumer) URL	ACS URL

[Not required; OneLogin refers to ACS URL for this function]	~~Single sign-on URL~~

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

4. Parameters

Create a new field by clicking the **+** button. For the **Field name**, use **email** (in lower case). Map this to the **Value** field **Email**. Select **Save**.

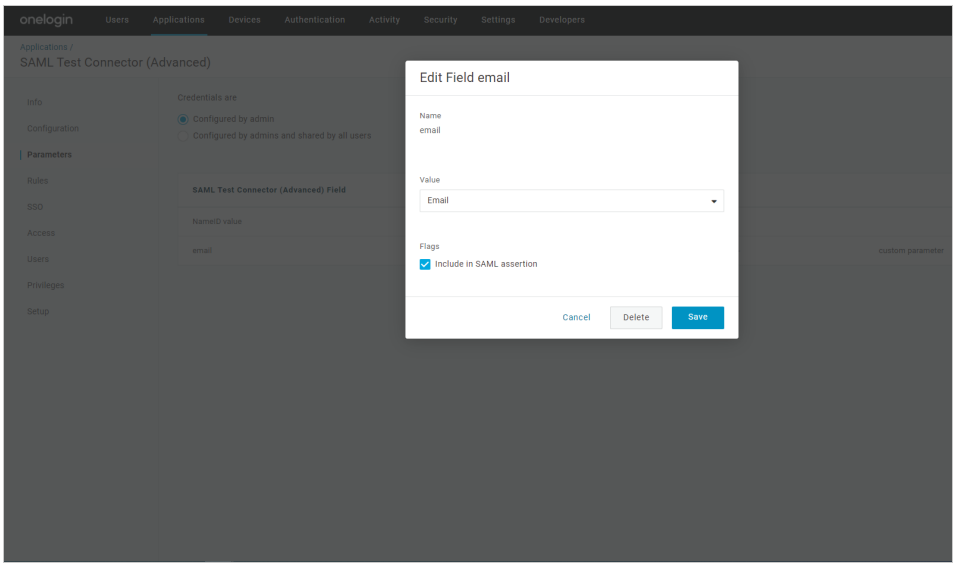

Figure 5: Select Email as the value

5. Grab information from OneLogin and paste in OnceHub

On the **SSO** step, grab the information you will add in OnceHub. Once added, go back to OneLogin before you click **Verify** in OnceHub.

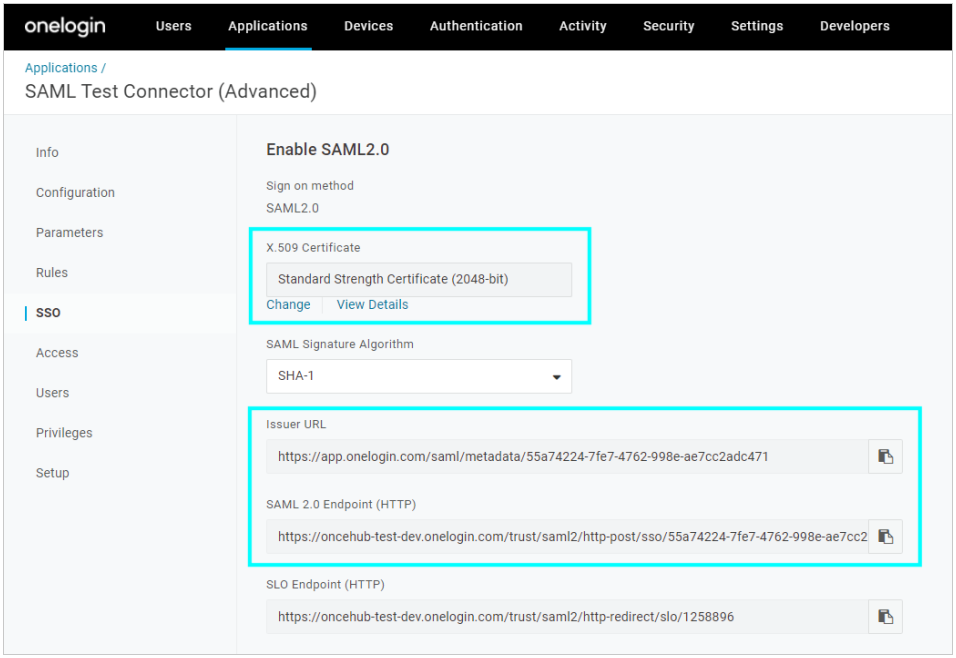

Figure 6:

Enable SAML 2.0 by grabbing information to paste in OnceHub

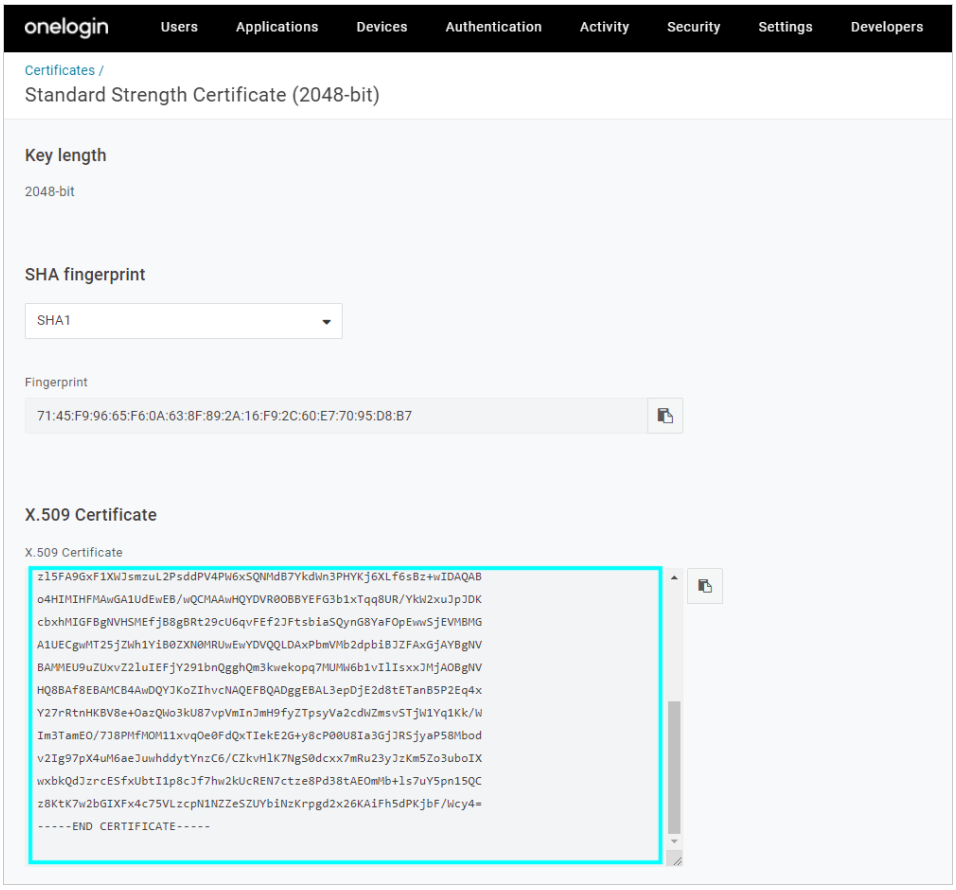

Figure 7: X.509 Certificate

In OneLogin	In OnceHub
Issuer URL	Entity ID
SAML 2.0 Endpoint (HTTP)	IDP single sign-on URL
X.509 Certificate (select **View Details** to copy)	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. Add users

On the Users step, add the relevant users in OneLogin to your new app.

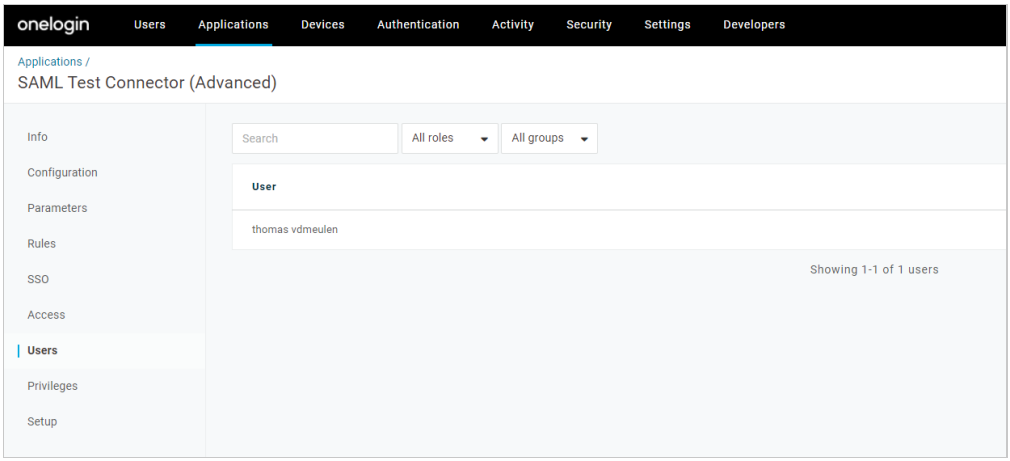

Figure 8: Add users

Follow the rest of the steps in OneLogin to complete setup.

7. Verify

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

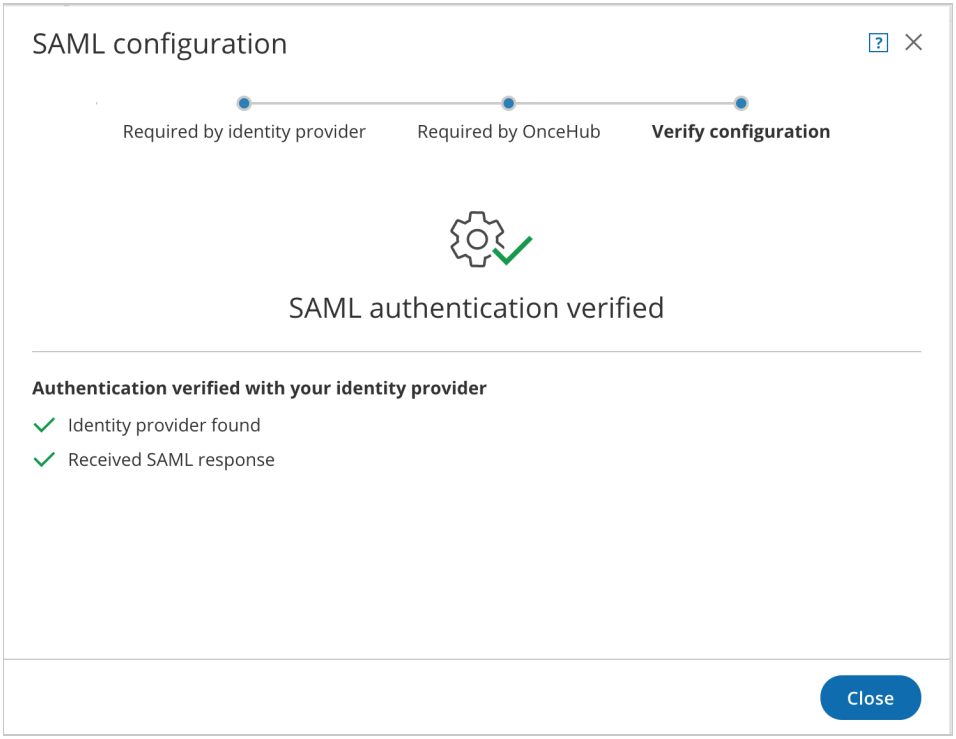

Figure 9: Verify configuration

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 OneLogin 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.

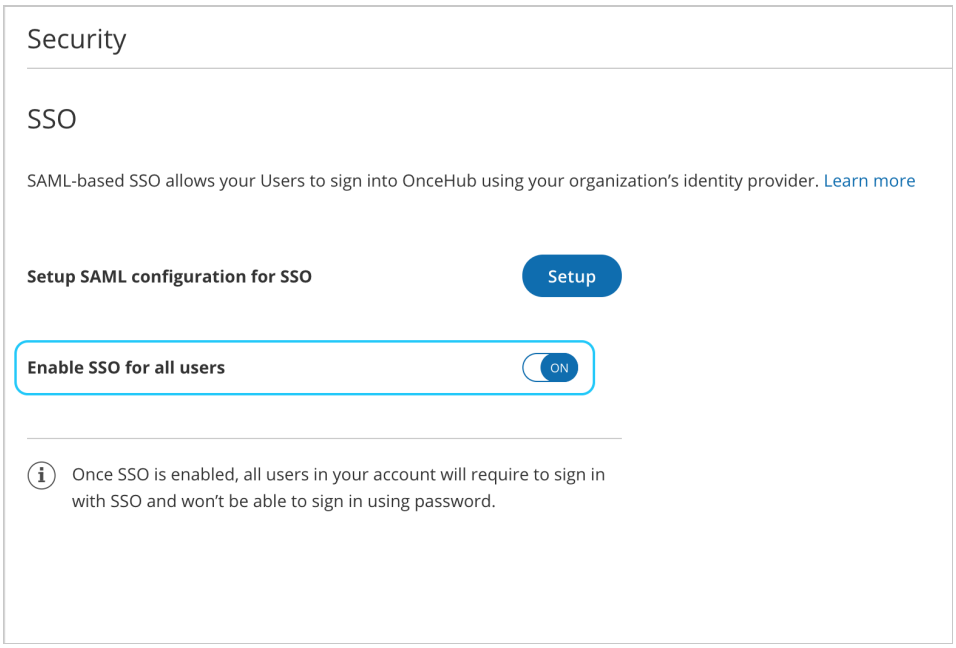

Figure 15: Enable SSO for all users

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.