# Configuring SSO with Azure

Last Modified on Oct 26, 2020

This article provides a step-by-step guide to configuring SSO between OnceHub and Azure Active Directory.

## 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 Azure AD. The person configuring in Azure AD 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 Azure AD:

**1.** In portal.azure.com, go to **Enterprise applications** -> Click on **+ New application**.

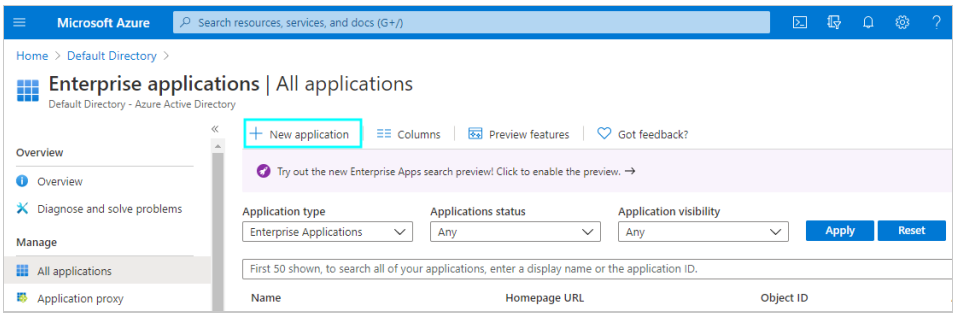


*Figure 1: New application*

**2.** On the **Add an application** page, select **Non-gallery application**.

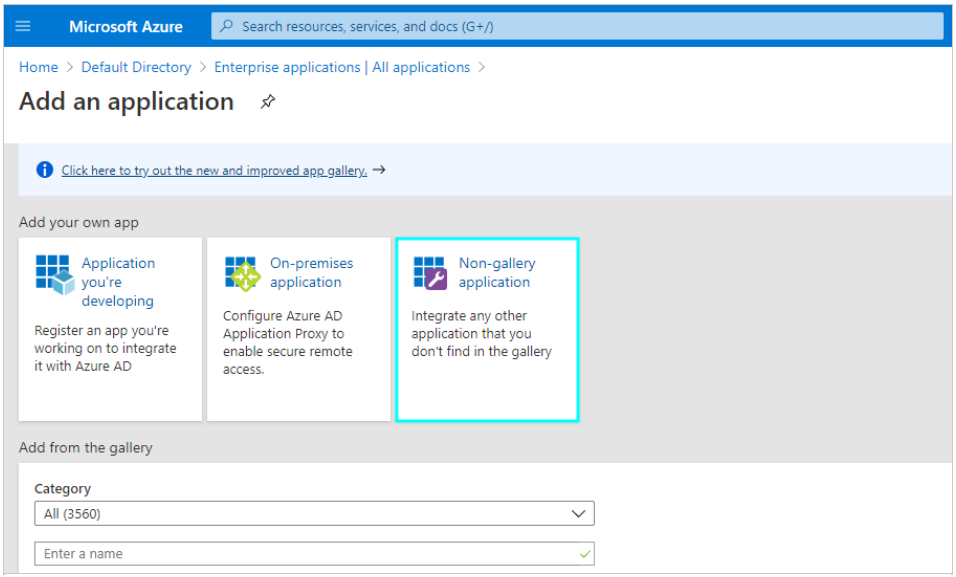


*Figure 2: Non-gallery application*

**3.** Add the **Name** (for example, “OnceHub”). Click **Add**.

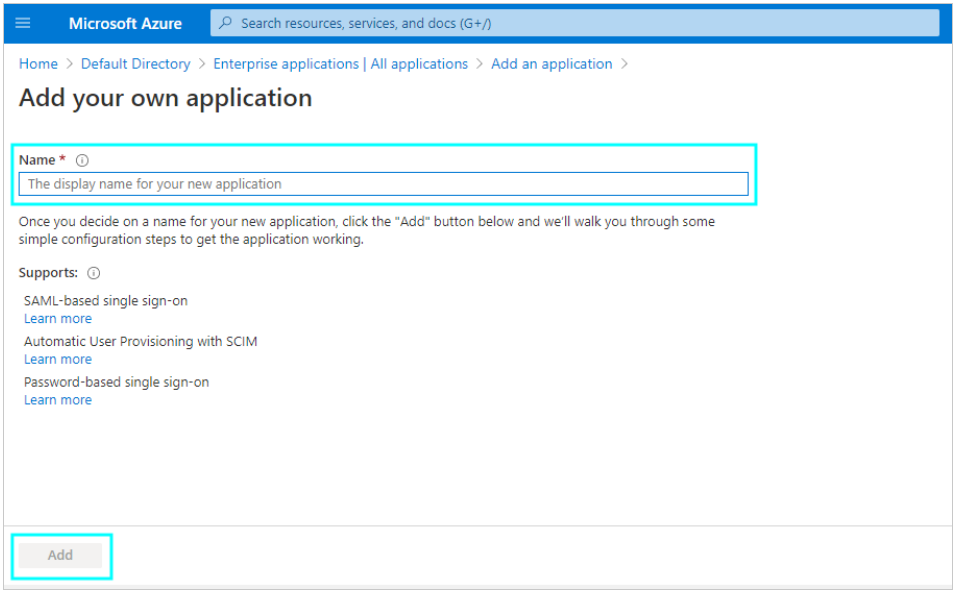


*Figure 3: Add name and click Add*

**4.** In the left menu, select **Single sign on**. Click on the **SAML** option.

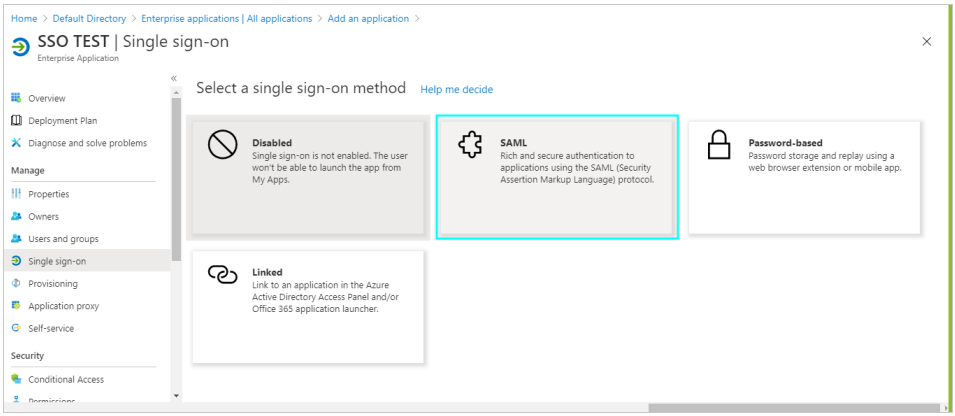


*Figure 4: SAML option*

**5.** Edit the **Basic SAML Configuration** section.

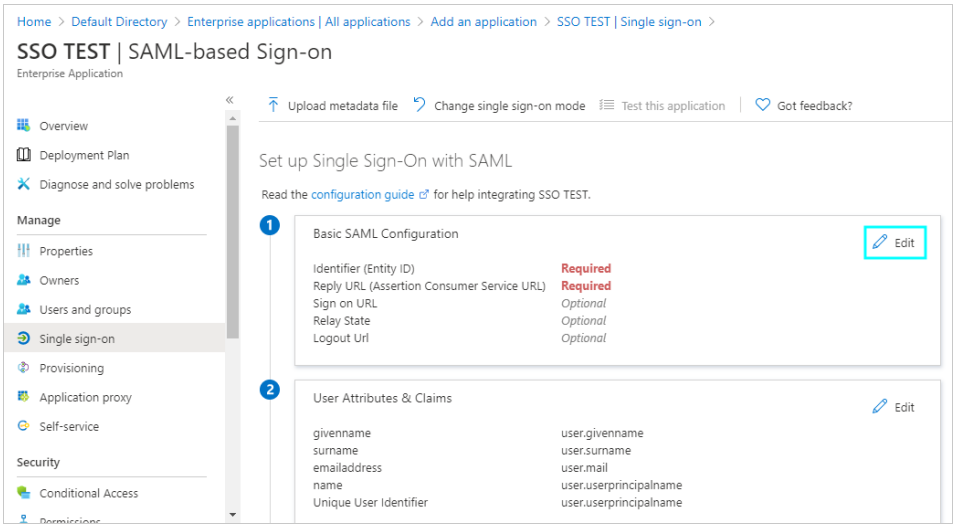


*Figure 5: Edit the Basic SAML Configuration section*

**6.** On the **Basic SAML Configuration** page, fill in the required fields and save. You can grab these values in OnceHub, on the **Required by entity provider** step.

| In Azure AD | In OnceHub |
|---|---|
| Identifier (Entity ID) | Identifier URL |
| Reply URL | ACS URL |
| Sign on URL | Single sign-on URL |

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

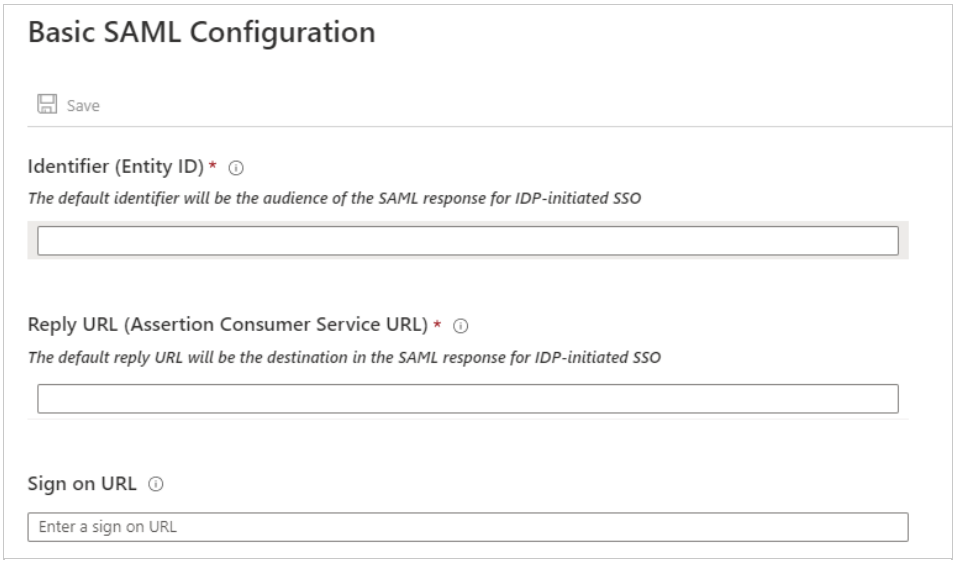


*Figure 6: Basic SAML Configuration*

**7.** Edit the **User Attributes & Claims** section**.**

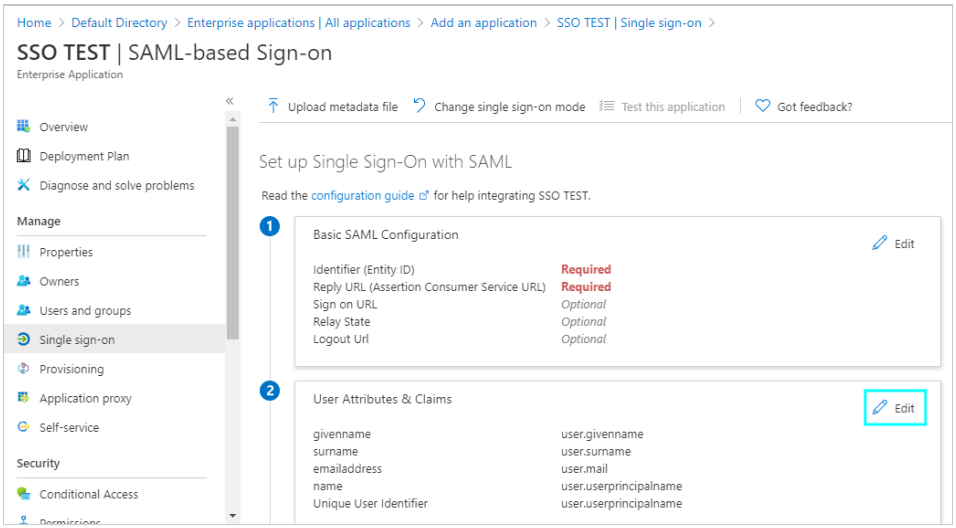


*Figure 7: Edit the User Attributes & Claims section*

**8.** Select **+ Add new claim**.

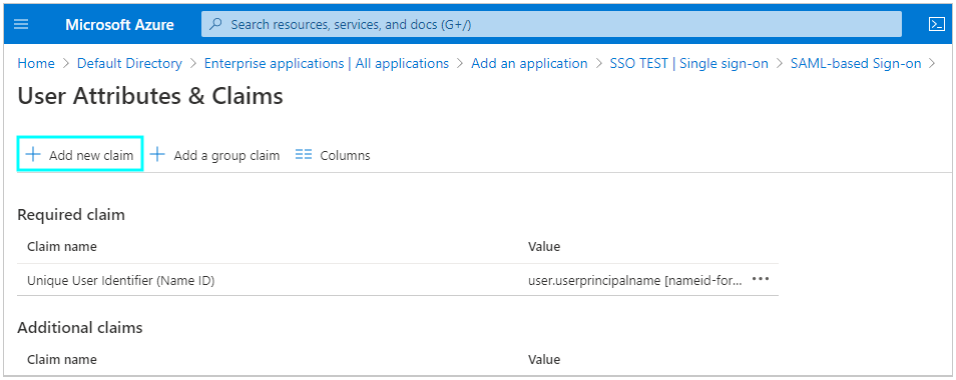


*Figure 8: Add new claim*

**9.** On the **Manage claim** page, enter these values:

Name: **email**
*Note: Write 'email' in lower-case letters only.*

Source: **Attribute**

Source attribute: **user.mail**

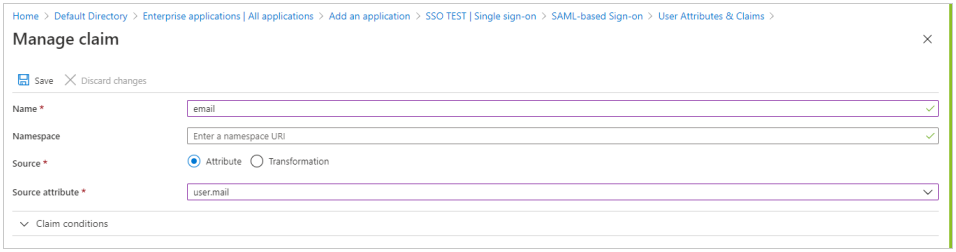


*Figure 9: Manage claim*

Once you've defined these values, click **Save**.

---

**10.** Access the SAML Signing Certificate by downloading the **Certificate (Base64)** option.

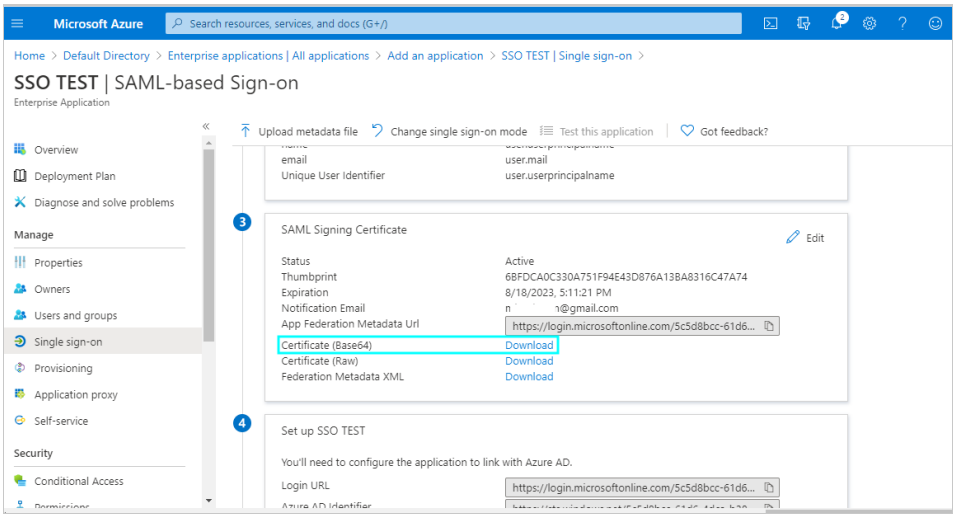


*Figure 10: Download certificate*

---

**11.** Go to OnceHub. You've already taken care of the first part, **Required by identity provider**, within Azure AD. In the second part, **Required by OnceHub**, you'll need specific field values from Azure AD that you can copy and configure within OnceHub.

This includes the **Entity ID**, **Single sign-on URL**, and the **Public x509 certificate**. You've already downloaded the certificate. You can grab the other values in Azure AD next to the **4**.

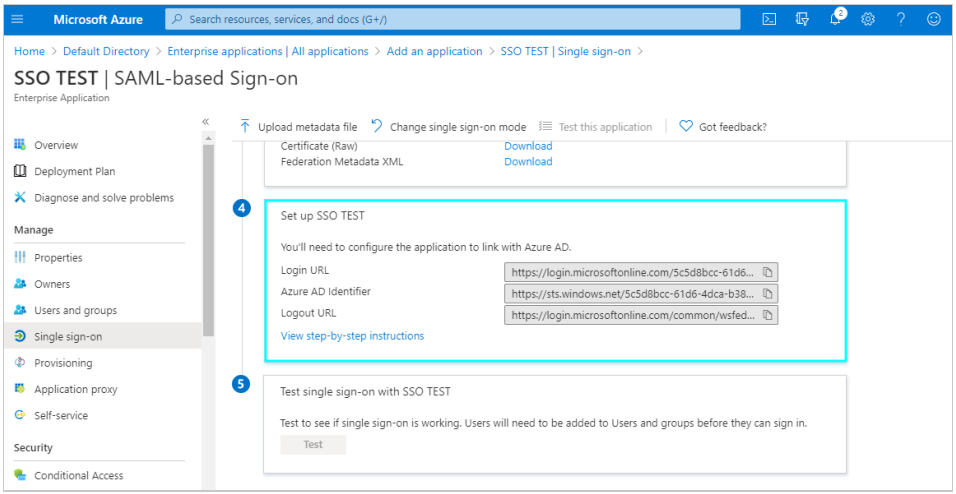


*Figure 11: Required by OnceHub step*

| In Azure AD | In OnceHub |
|---|---|
| Azure AD Identifier | Entity ID |
| Login URL | IDP single sign-on URL |
| Certificate (Base64) - Download and copy/paste whole contents | Public x509 certificate |

**12.** For the certificate field, open the downloaded certificate and copy all contents.

> **Important:**
>
> Include the **-----BEGIN CERTIFICATE-----** and **-----END CERTIFICATE-----** syntax in your selection.


*Figure 12: Copy whole contents of certificate text*

**13.** In Azure AD, go to the left menu and select **Users and groups**. On that page, select **+ Add user**.

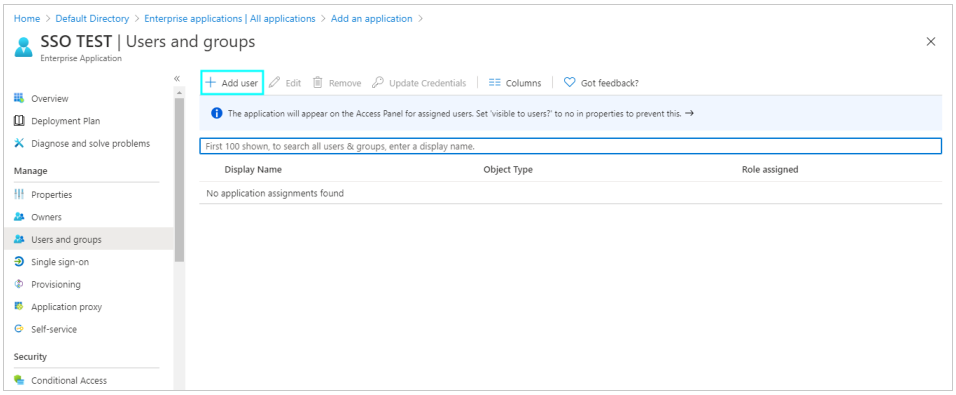


*Figure 13: Add user*

---

**14.** On the **Add Assignment** page, search for relevant users or groups. Select them and click **Assign** when ready.

---

## Verify configuration

OnceHub will speak to your identity provider and verify that the configuration has the correct values on both sides to proceed.

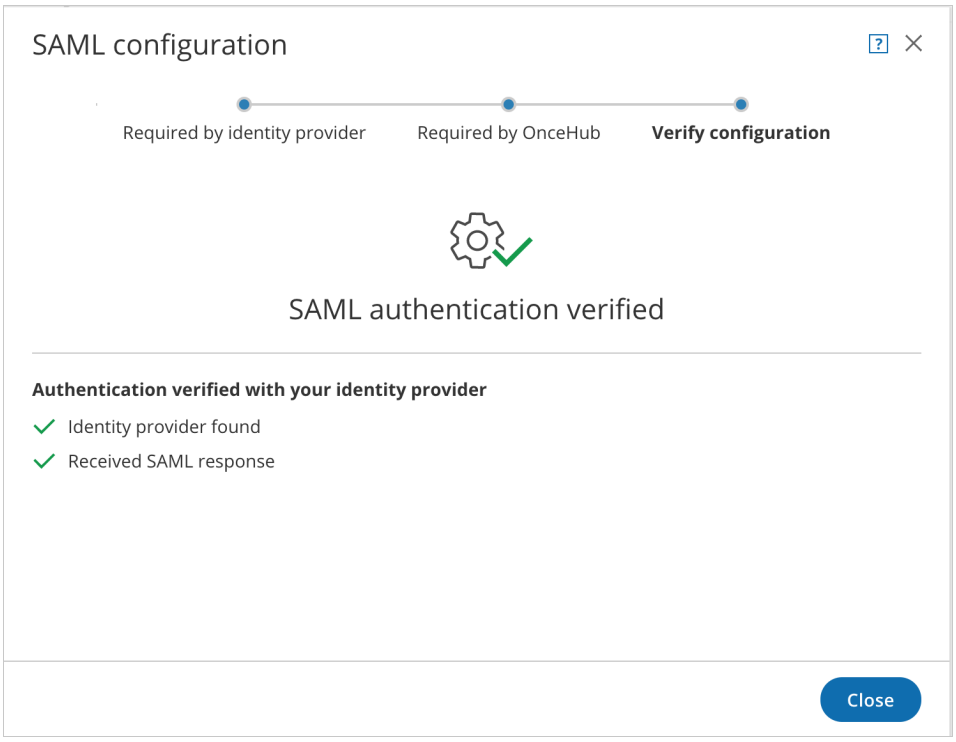


*Figure 14: Verify configuration*

---

## 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 Azure 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.

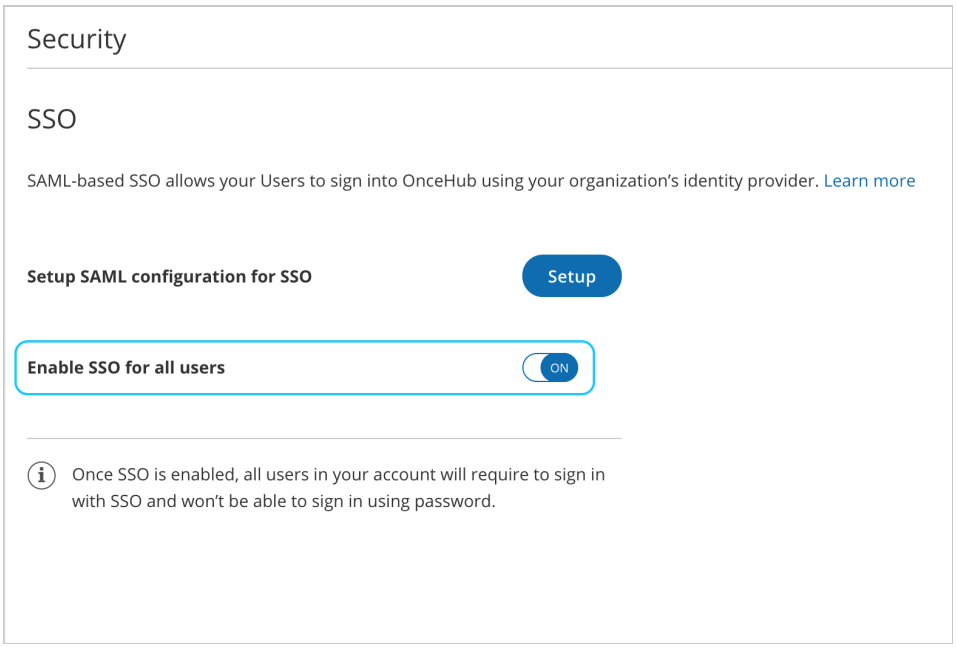


*Figure 15: Enable SSO for all users*

**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.