CYBRARY | FOR TEAMS

Self-Service Guide

to SAML 2.0 SSO Configuration for Okta, OneLogin and Azure

Table of Contents

Introduction

Cybrary provides a seamless one-click sign-in experience using your existing SSO provider (Okta, Onelogin, Azure). This self-service integration can be easily configured using the industry standard SAML 2.0.

What is SAML?

Security Assertion Markup Language (SAML) provides the user with online security and enables the user to access multiple web applications using one set of login credentials. It works by passing authentication information in a particular format between two parties, usually an identity provider (idP) and a web application.

What is SSO?

Single sign-on (SSO) is an authentication method that enables users to securely authenticate with multiple applications and websites by using just one set of credentials.

Benefits of SAML 2.0 SSO

Increased security

Easy off-boarding

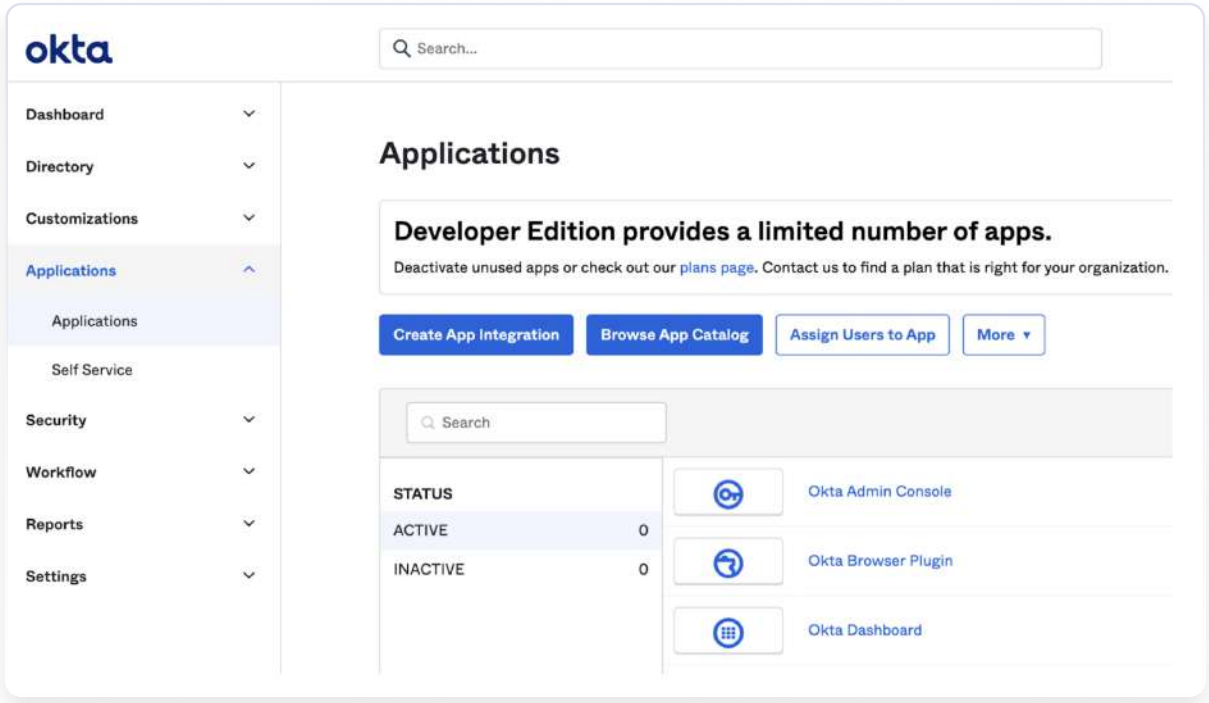
No forgotten passwords

Speeds up authentication

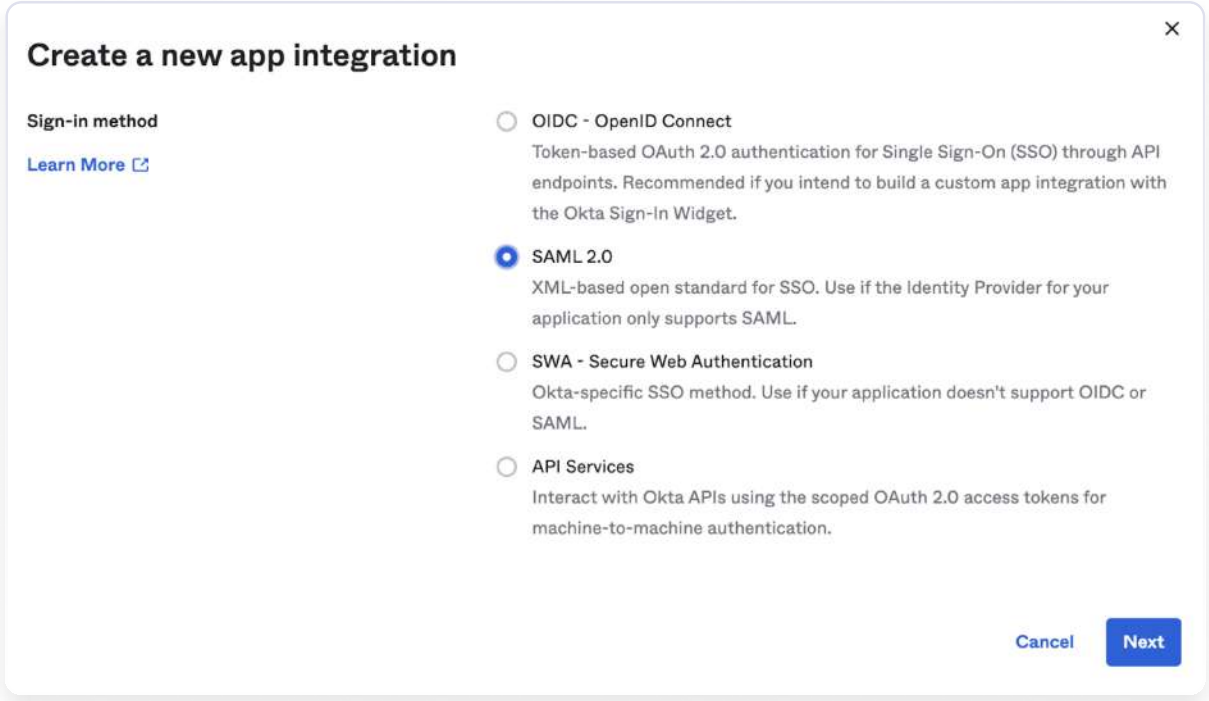
It improves the user experience as you only need to sign in once to access multiple web applications. (No need to remember multiple sets of credentials)

Configure SAML 2.0 SSO for Okta

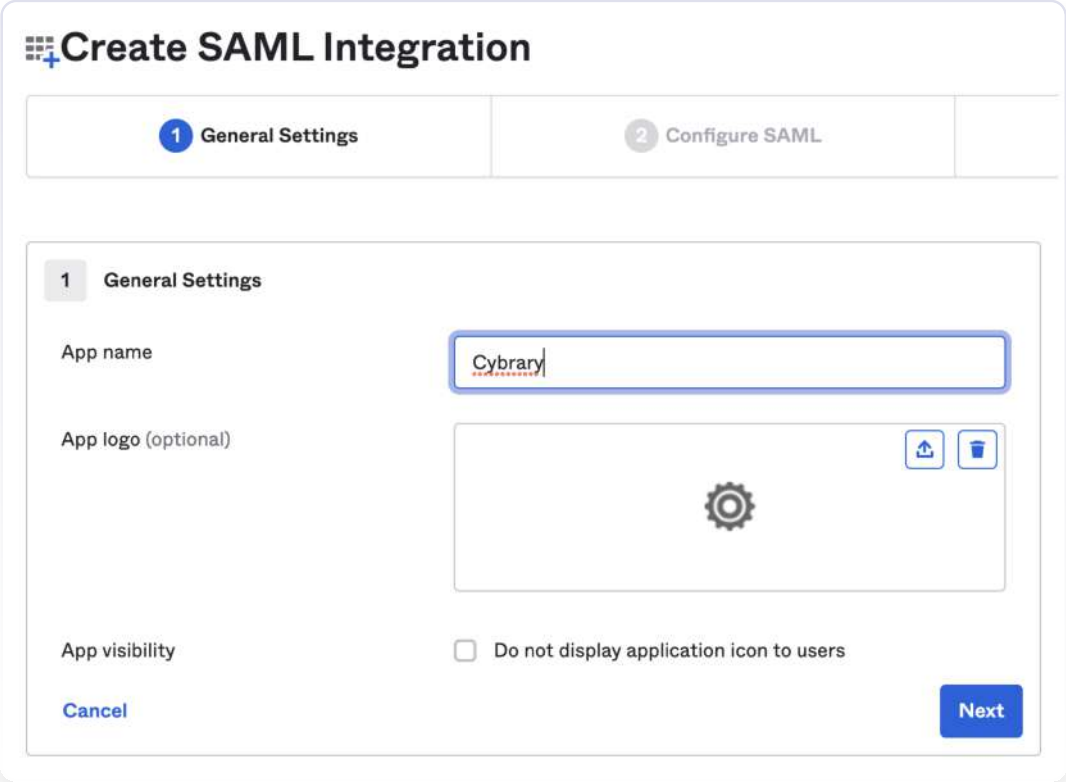
1 In your **Okta Application** navigate to the **Applications → Applications** option on the left nav and select **Create App Integration**.



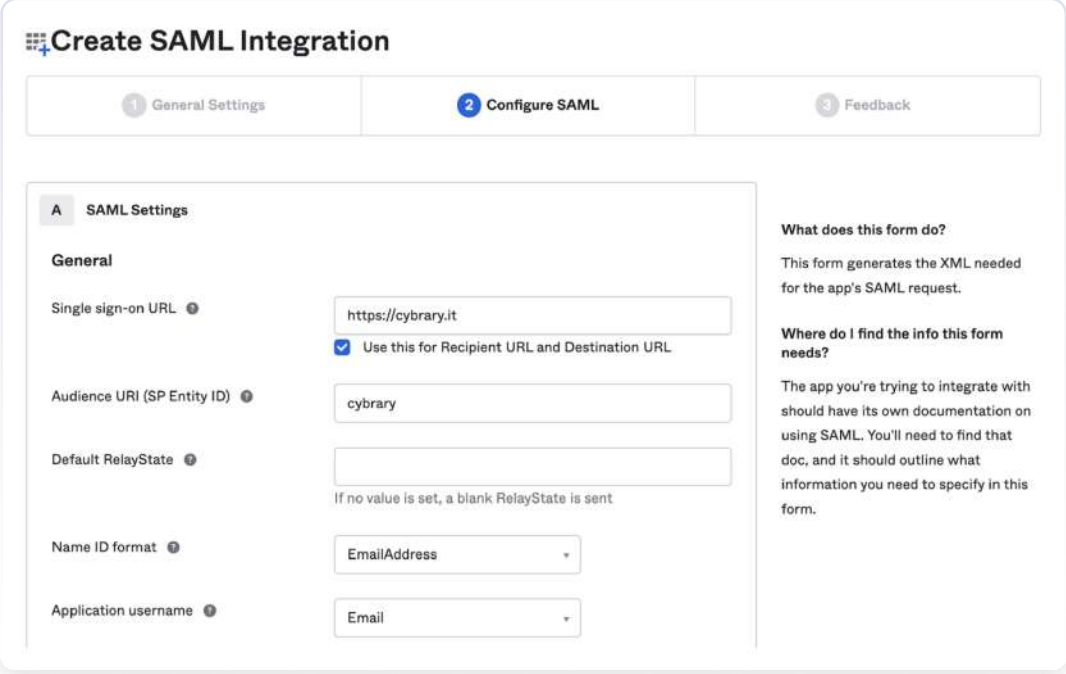
2 Select the **SAML 2.0** option and click **Next**.



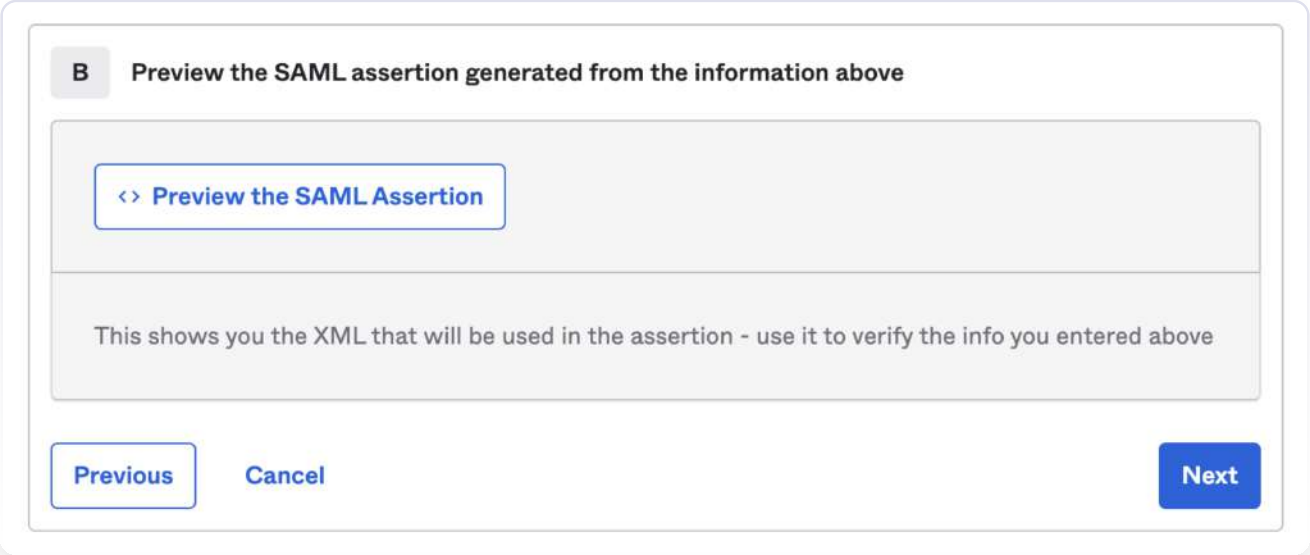
3 Enter an **App name** (eg. Cybrary) and click **Next**.



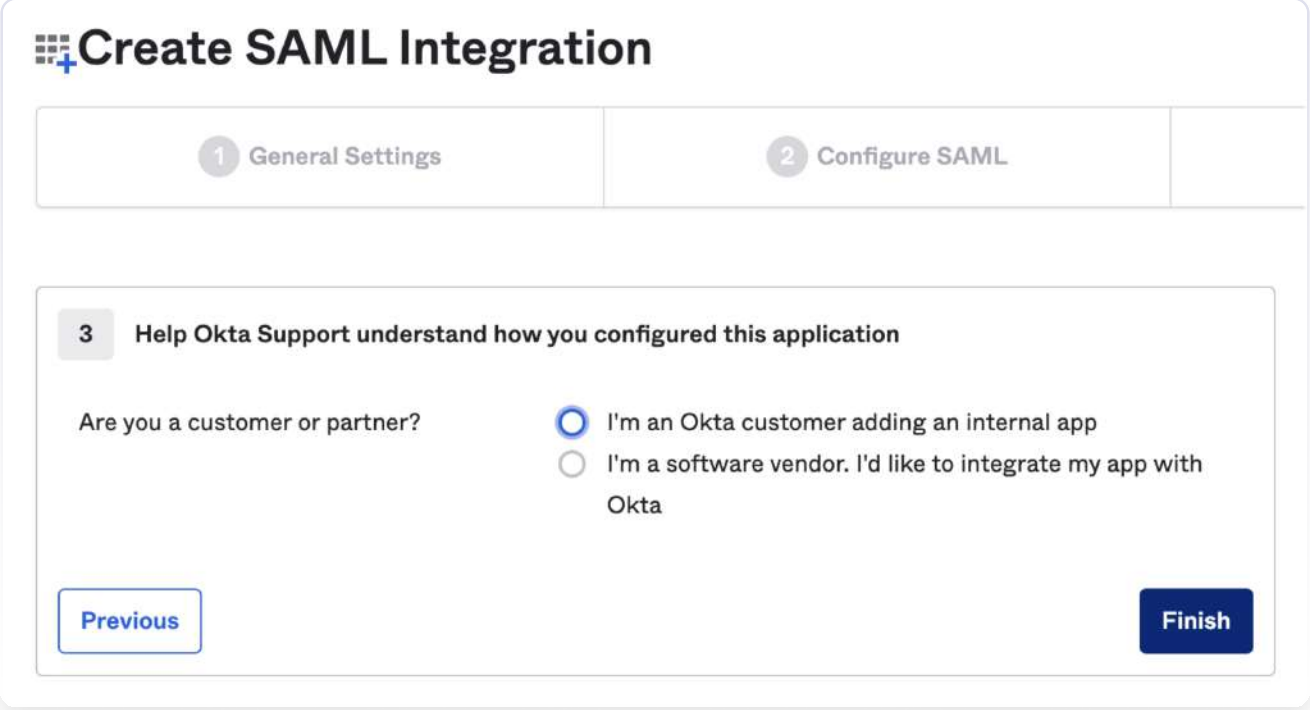
4 For **Single sign-on URL** enter https://cybrary.it and for **Audience URI** enter cybrary; these are temporary values that will be updated later on. Set **Name ID format** to EmailAddress and **Application username** to Email.



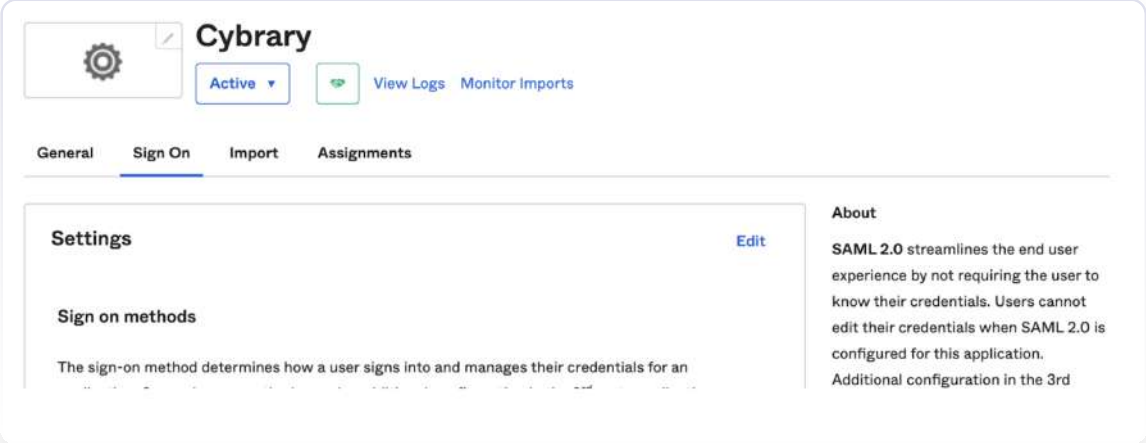
5 Scroll down to the bottom and click the **Next** button.



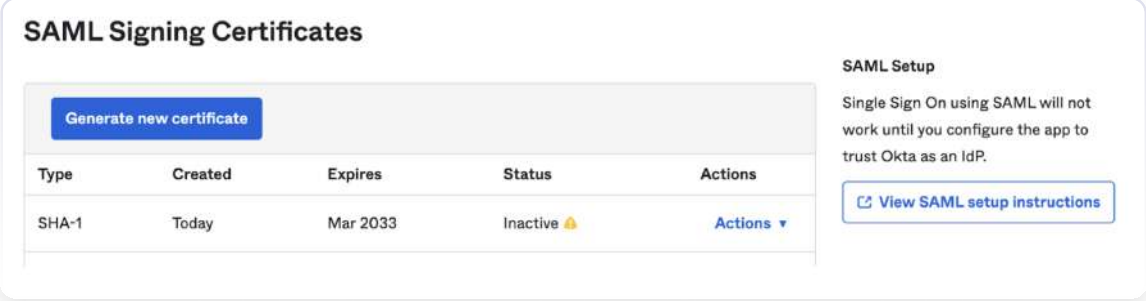
6 Select the first option: **I'm an Okta customer adding an internal app**. You can ignore the rest of the questions that appear, just scroll to the bottom and click **Finish**.



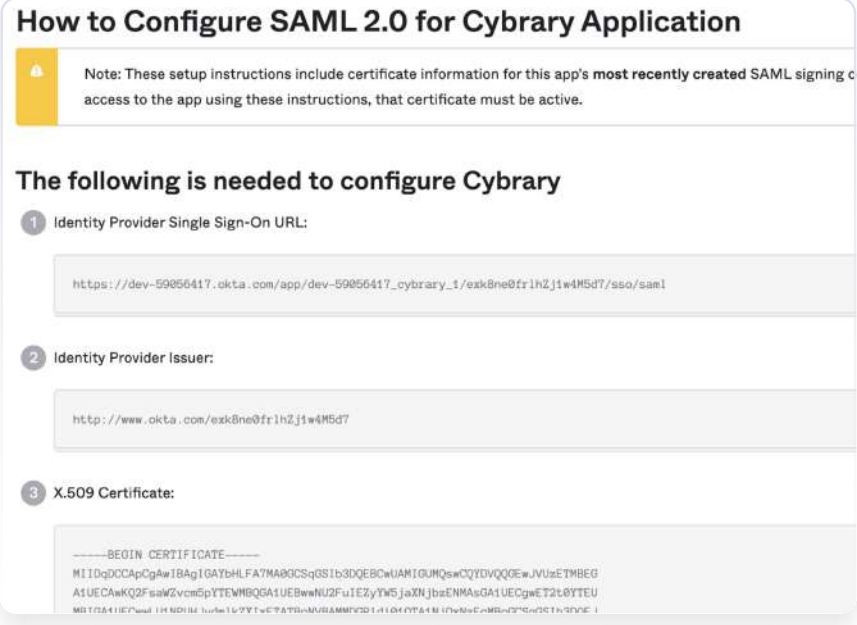
7 The Okta SSO application has now been created, now you need to update your team's SSO configuration in the Cybrary app. Navigate to the **Sign On** tab.



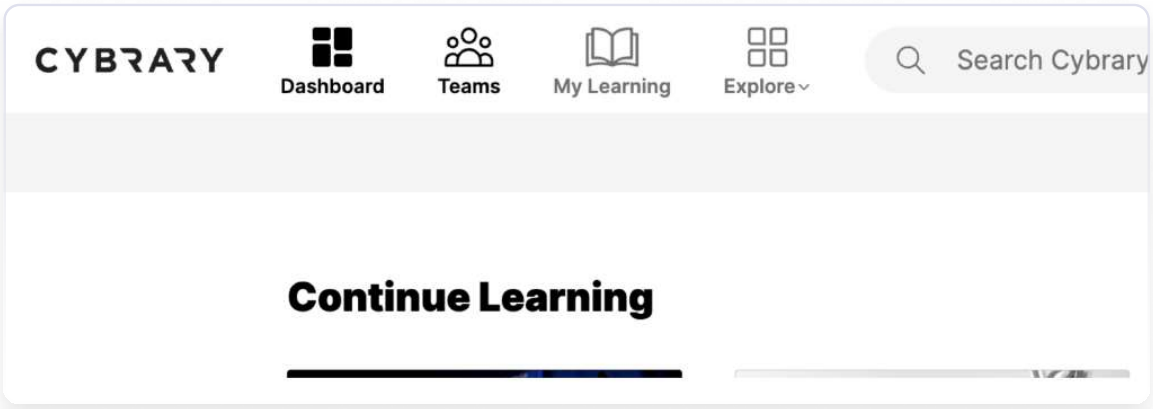
8 Scroll down until you see the **SAML Setup** section on the right. Click **View SAML setup instructions**.



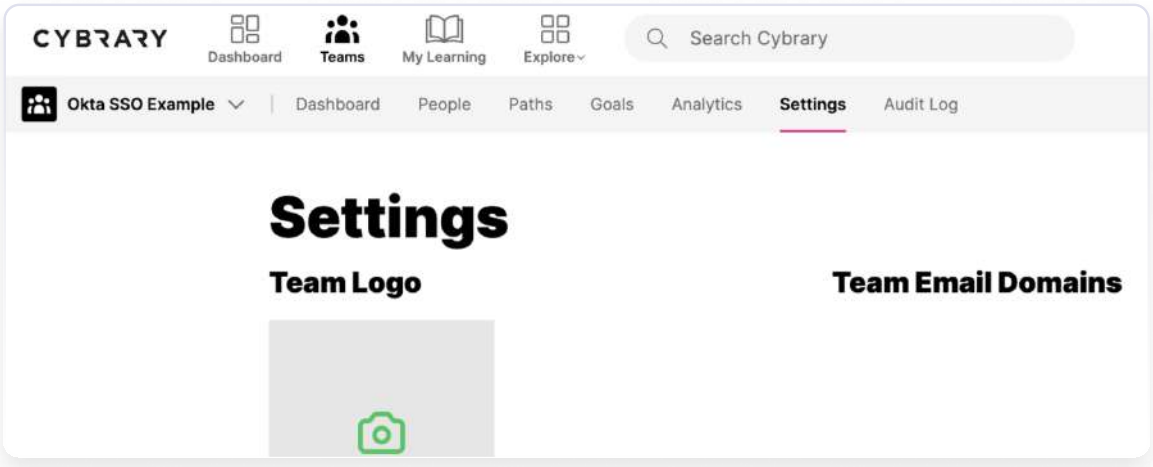
9 This page contains information you will need to copy over to the Cybrary app to enable SSO. Leave it open and **open a new tab/window**.



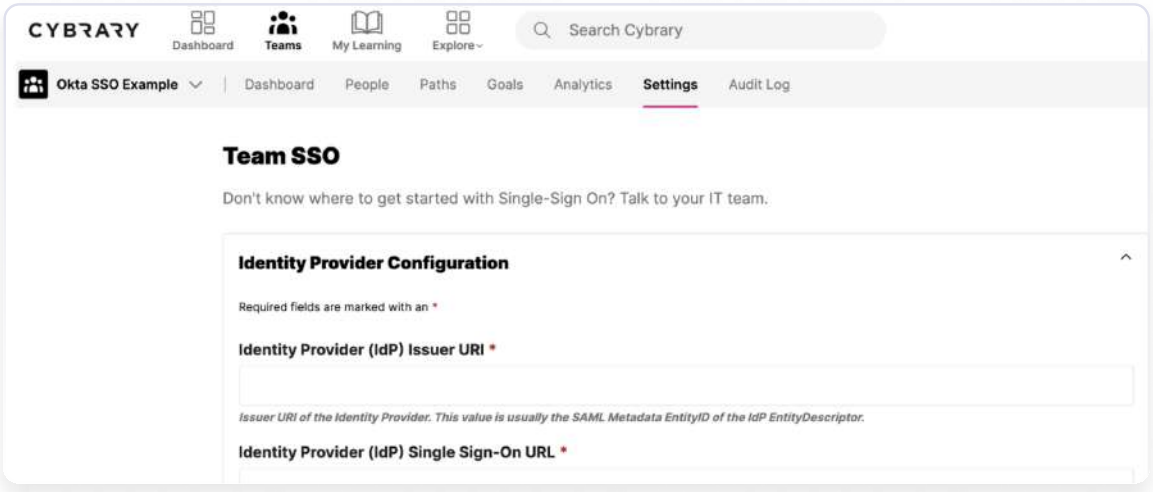
10 In the new tab/window, log in to https://app.cybrary.it and click on **Teams** in the top navigation.



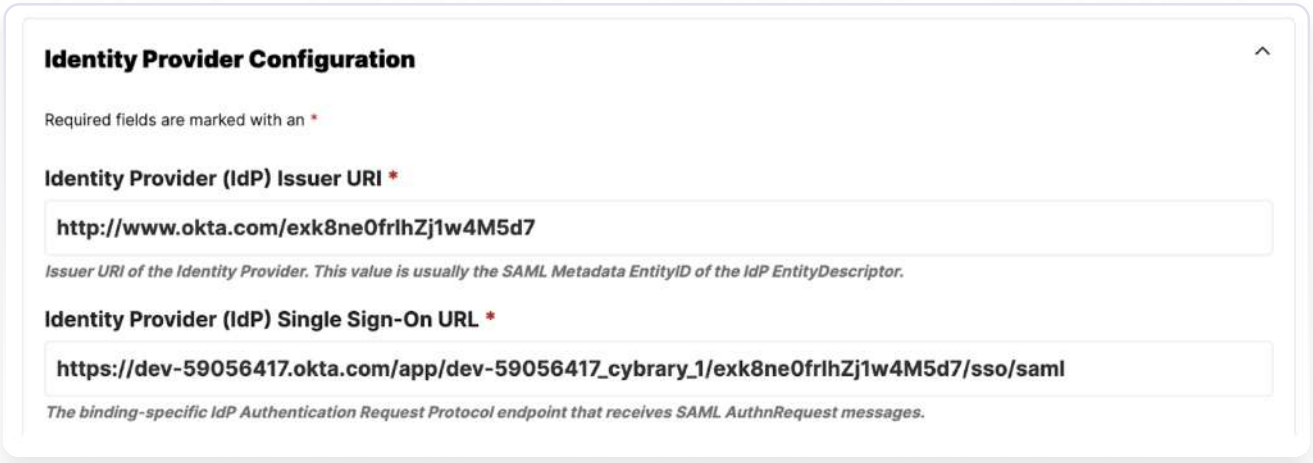
11 If you are an admin on more than one team, make sure the correct team is selected in the drop down on the top left. Click on **Settings** in the secondary to navigation.



12 Scroll down to **Identity Provider Configuration** in the **Team SSO** section.

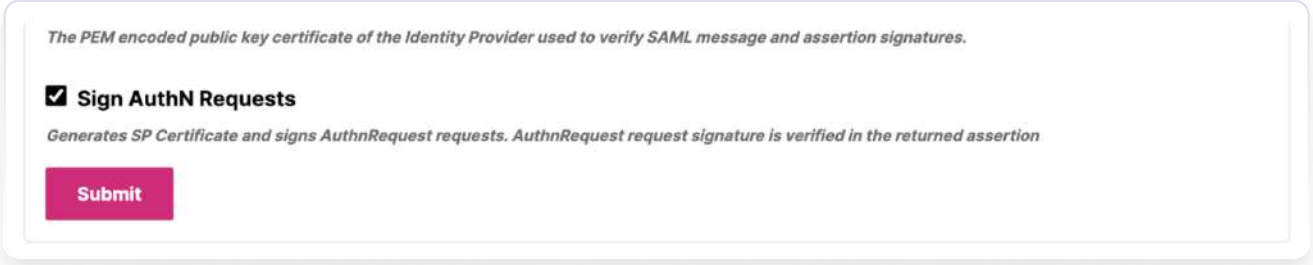


13 Enter the **Identity Provider (IdP) Issuer URI** and the **Identity Provider (IdP) Single Sign-On URL**, which can be found on the Okta page you left open. Make sure you enter the correct value for each field by matching the field names.

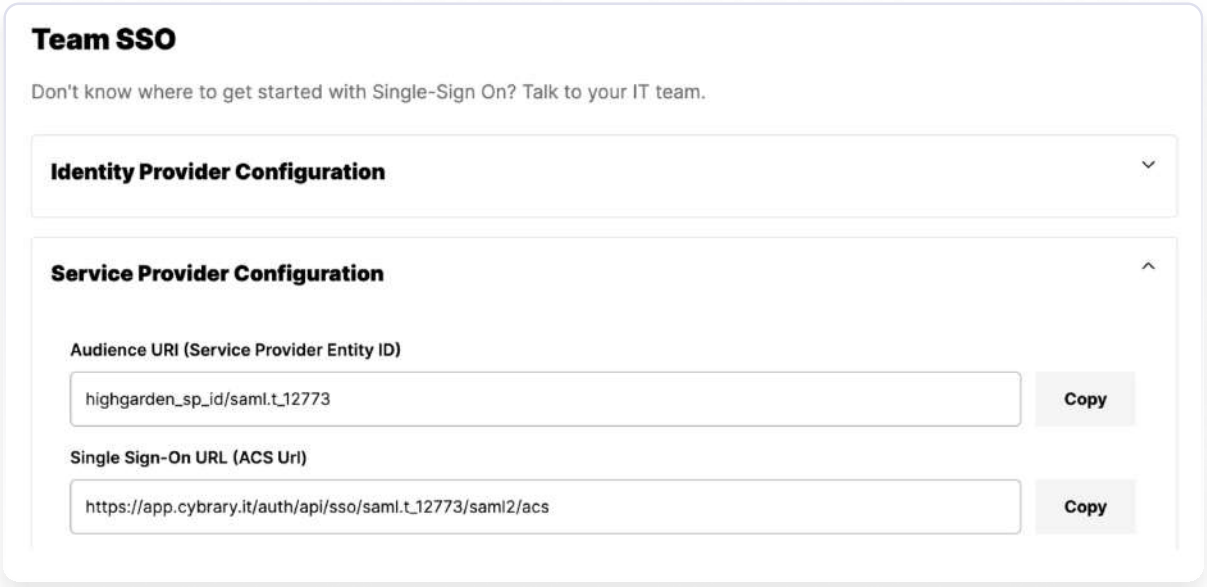


14 Copy the entire **X.509 Certificate** text (including -----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----) from the Okta page to the **Identity Provider Signature Certificate** text area in the Cybrary app.

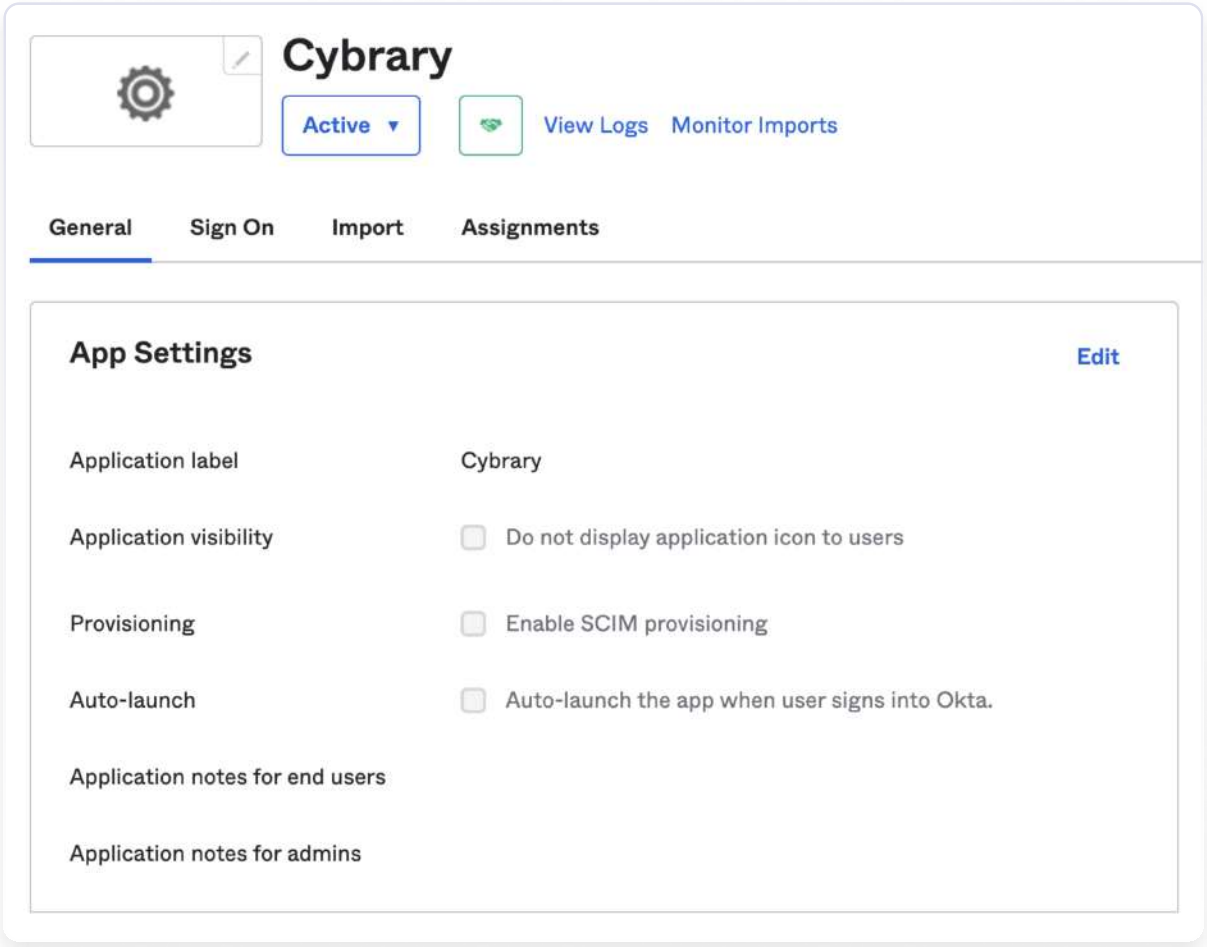
15 Check the **Sign AuthN Requests** option and click **Submit**. The page will refresh.



16 Scroll down to the **Service Provider Configuration** section in the **Team SSO** Section. You will need to copy these values over to the Okta app. Leave this page open.

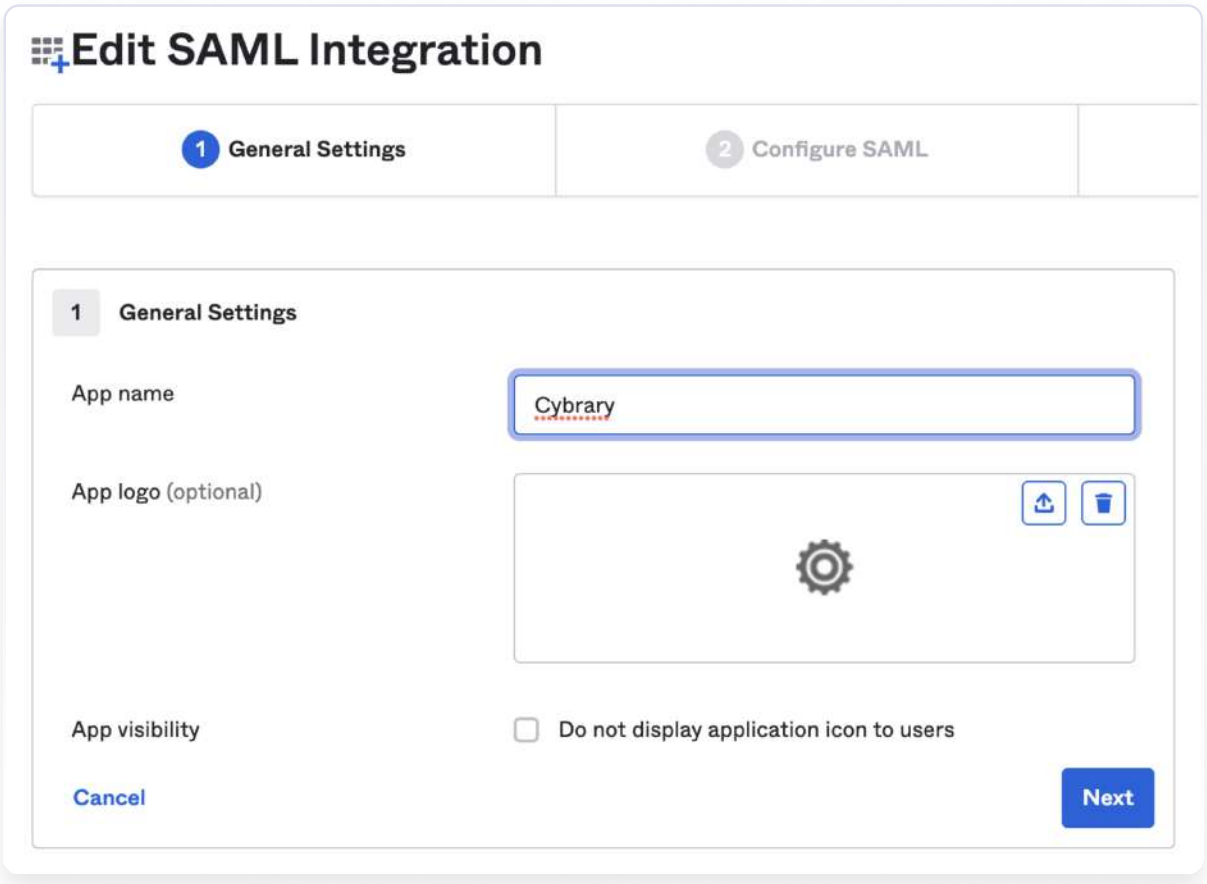


17 Back in the Okta SSO application configuration, navigate to the **General** tab.

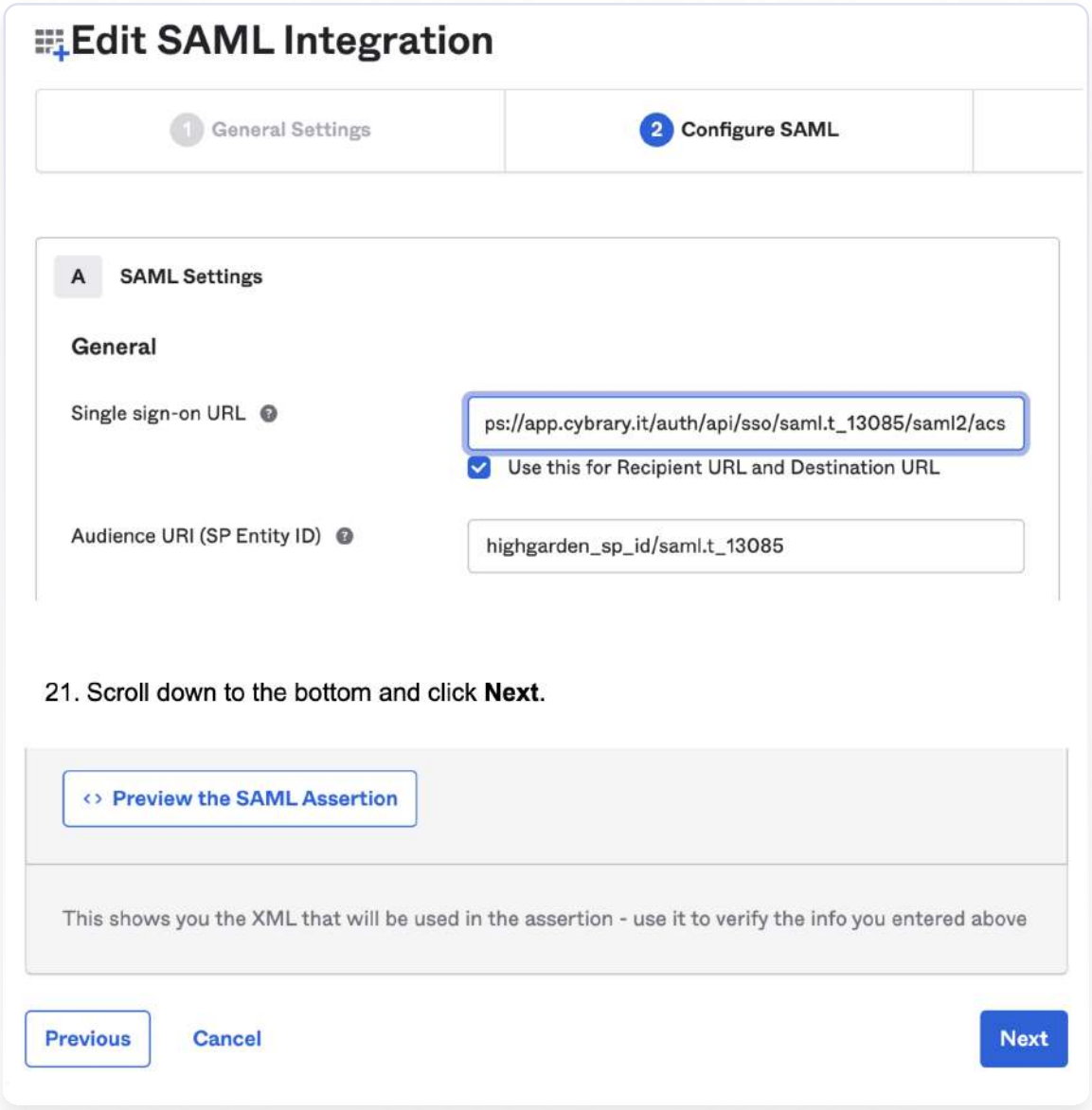


18 Scroll down to the **SAML Settings** section and click **Edit**.

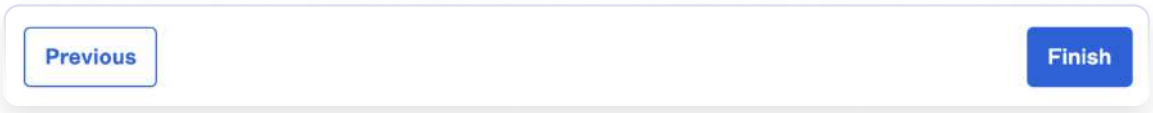
19 Click **Next** to continue to Configure SAML.



20 Update the **Single sign-on URL** and the **Audience URI (SP Entity ID)**. These values can be found back in the Cybrary page you left open in the **Service Provider Configuration** section. Make sure you enter the correct value for each field by matching the field names.



22 Scroll to the bottom and click **Finish**.

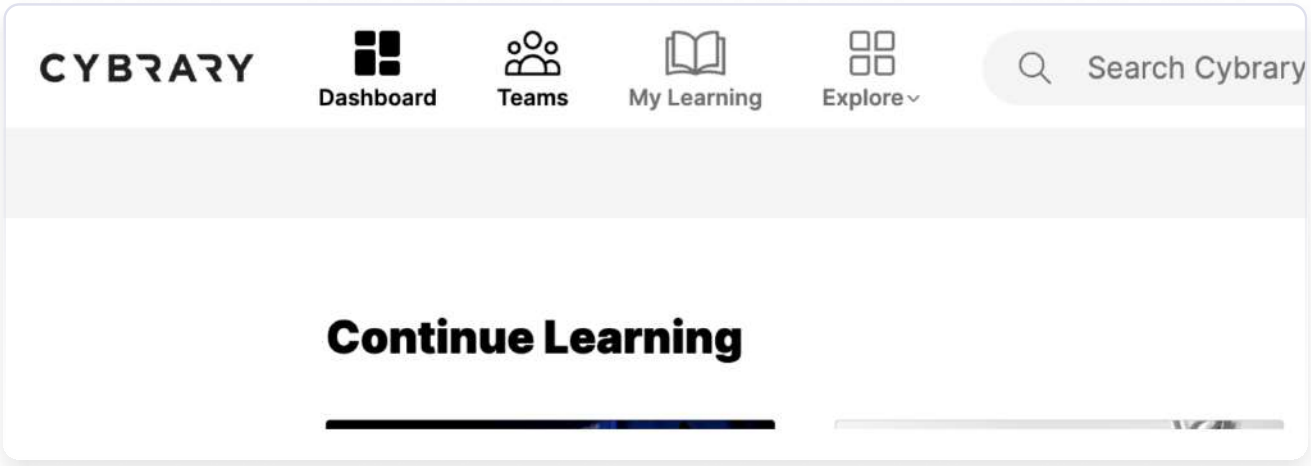


Your SSO application configuration is now complete. Once users are assigned to the application in Okta they will be able to log in with SSO.

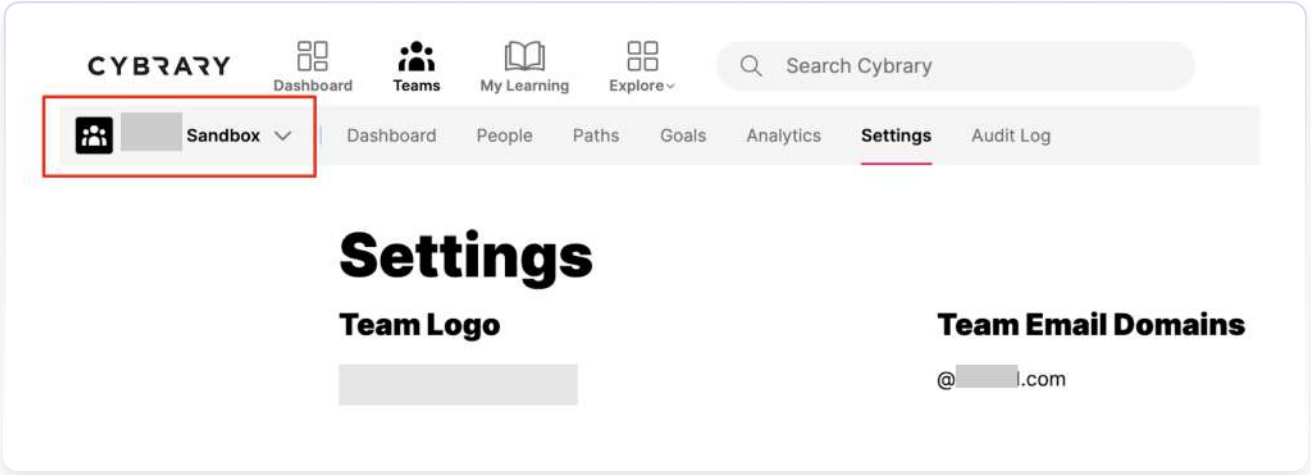
Configure SAML 2.0 SSO for OneLogin

Note: OneLogin instructions based on the SCIM Provisioner with SAML (SCIM v2 Core) application, layout and field names may vary for different applications.

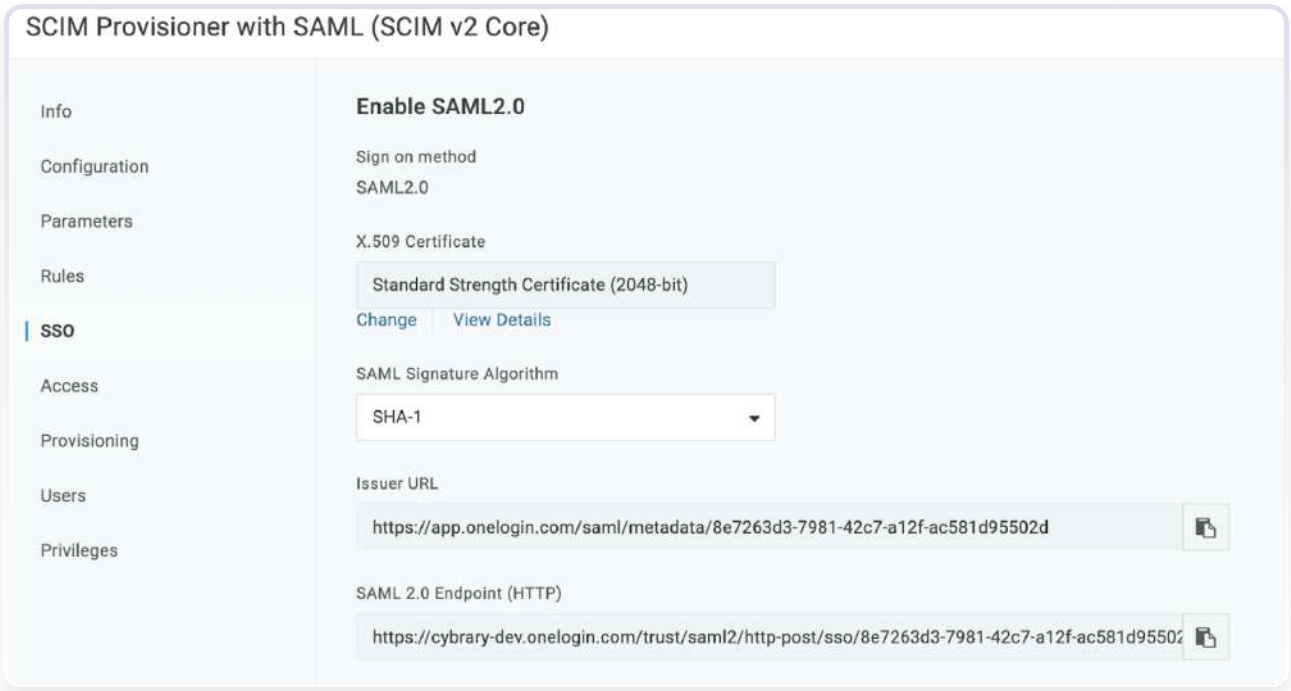
1 Log in to app.cybrary.it and click on **Teams** in the top navigation.



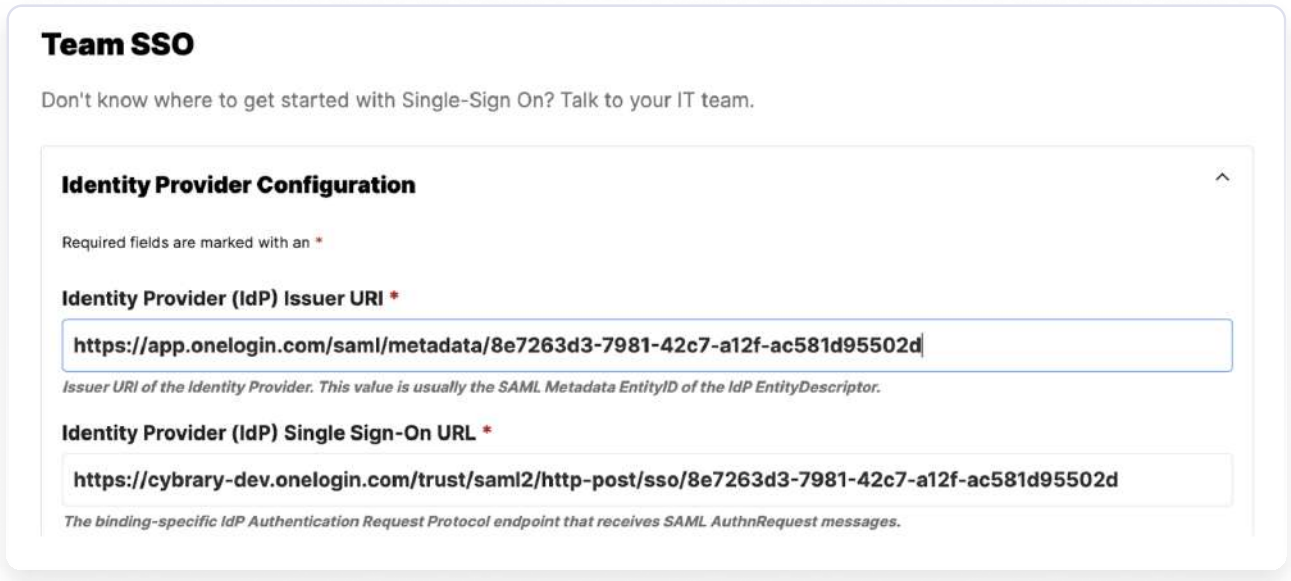
2 If you are an admin on more than one team, make sure your company's **Sandbox** is selected in the drop down on the top left. Click on **Settings** in the secondary to navigation.



3 In your **OneLogin Application** navigate to the **SSO** tab.

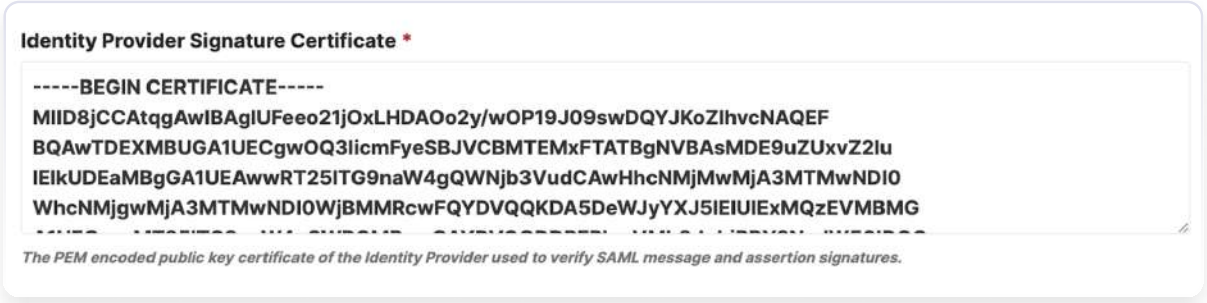


4 Back In the **Cybrary App**, scroll down to **Identity Provider Configuration** in the **Team SSO** section. Enter the **Identity Provider (IdP) Issuer URI** and the **Identity Provider (IdP) Single Sign-On URL**, and which can be found under **Issuer URL** and **SAML 2.0 Endpoint (HTTP)**, in the OneLogin Application respectively.

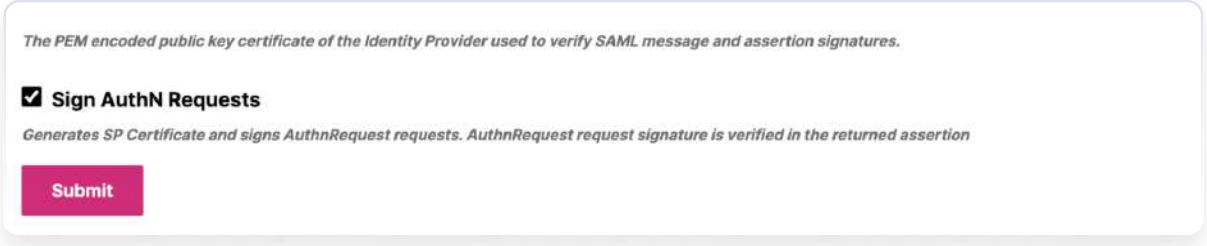


5 In the OneLogin Application click **View Details** under the **X.509 Certificate**. Copy the entire **X.509 Certificate** text (including -----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----).

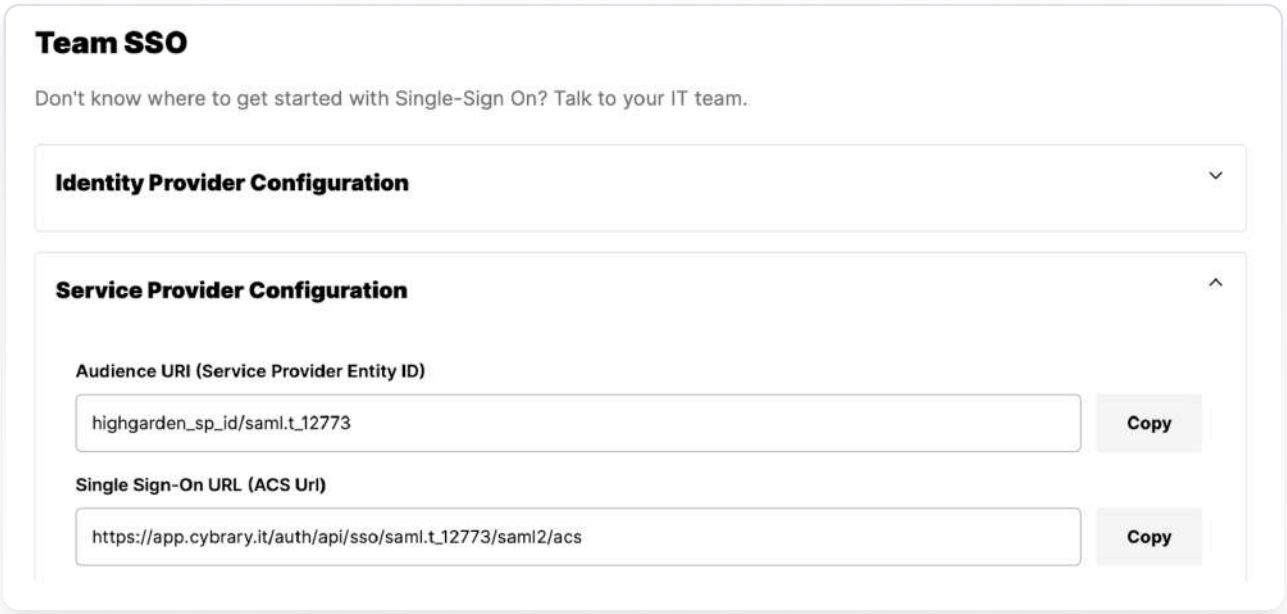
6 Paste it into the **Identity Provider Signature Certificate** text area in the Cybrary app.



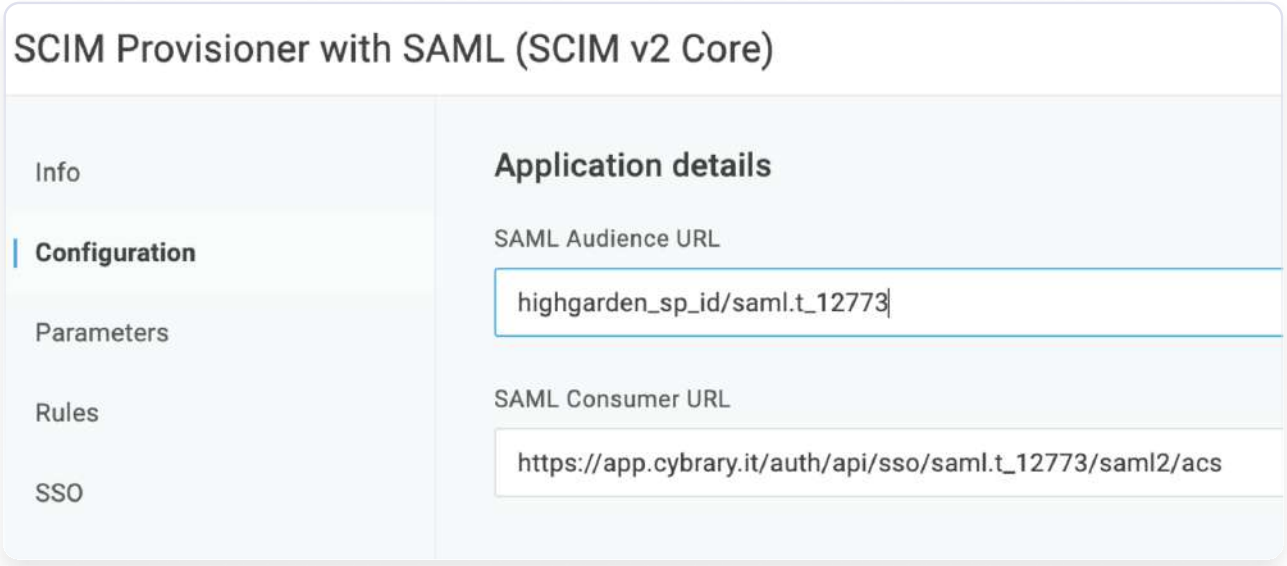
7 Check the **Sign AuthN Requests** option and click **Submit**. The page will refresh.



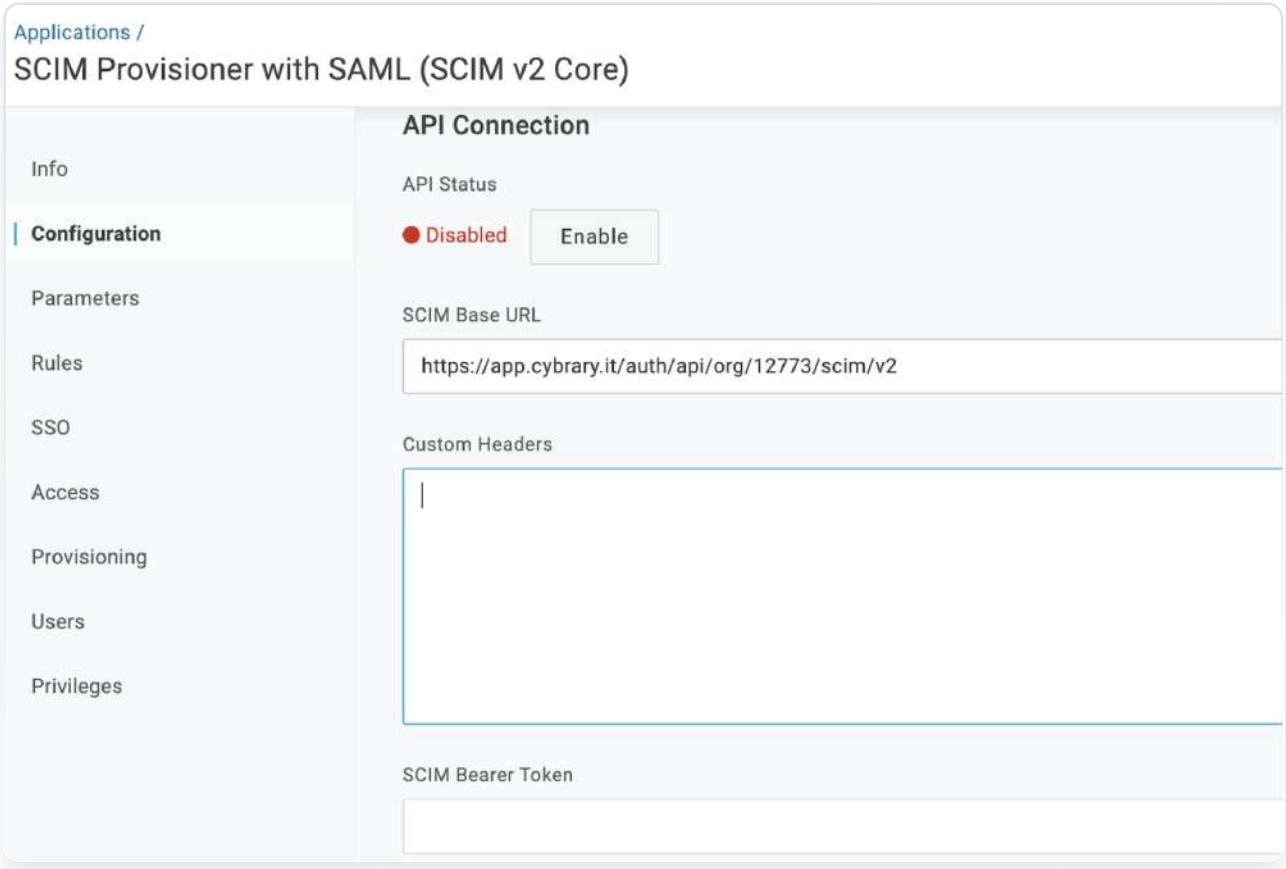
8 Scroll down to the **Service Provider Configuration** section in the **Team SSO** Section.



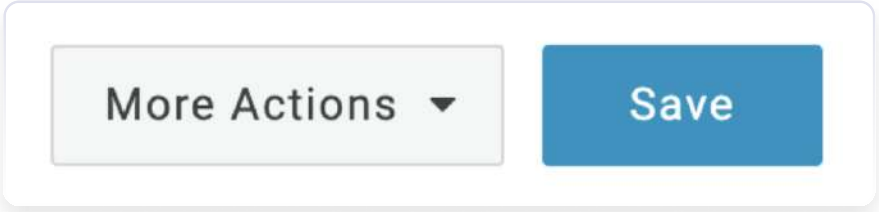
9 Copy the **Audience URI** and the **Single Sign-On URL** values to the OneLogin Application Configuration fields **SAML Audience URL** and **SAML Consumer URL**, respectively. They can be found in the **Configuration** tab at the top under **Application details**.



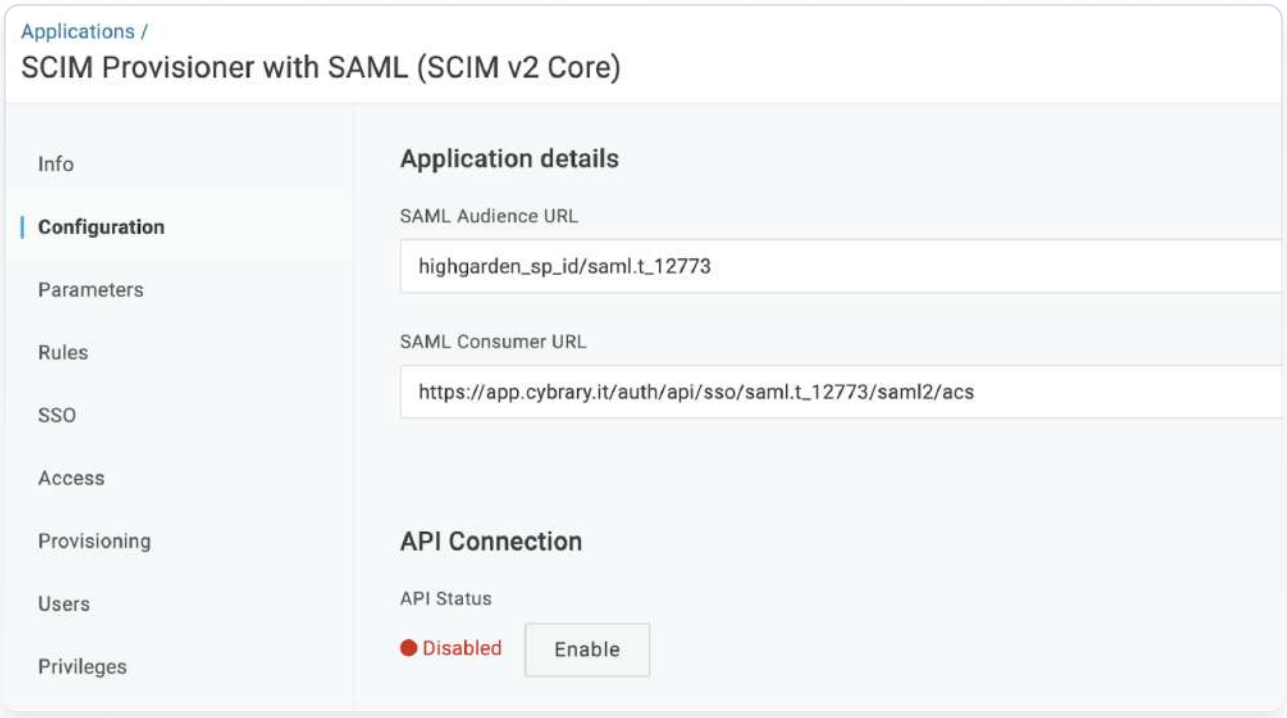
10 Further down in the OneLogin Application Configuration, under the section **API Connection**, we will provide the url and bearer token (it is custom for each team). Enter the provided url for the field **SCIM Base URL** and th provided bearer token for the **SCIM Bearer Token.**



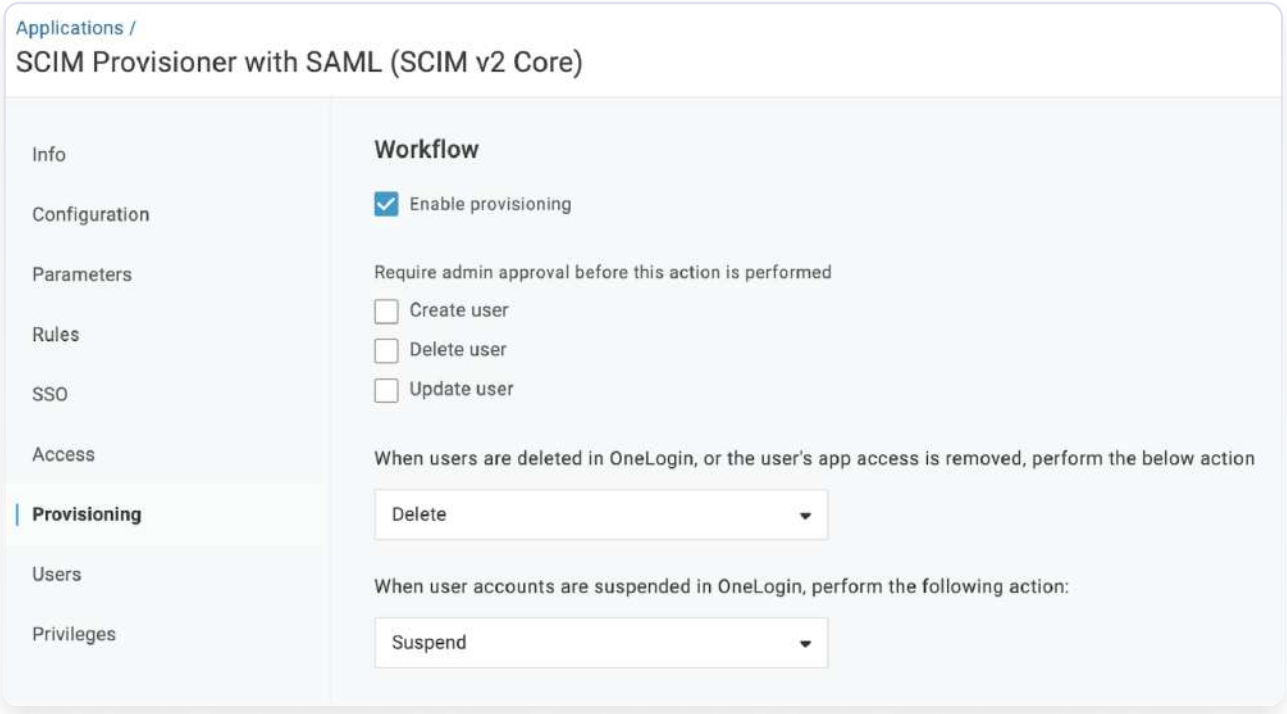
11 **Save** the OneLogin Application (top right).



12 In the **API Connection** section under **API Status** click **Enable.**

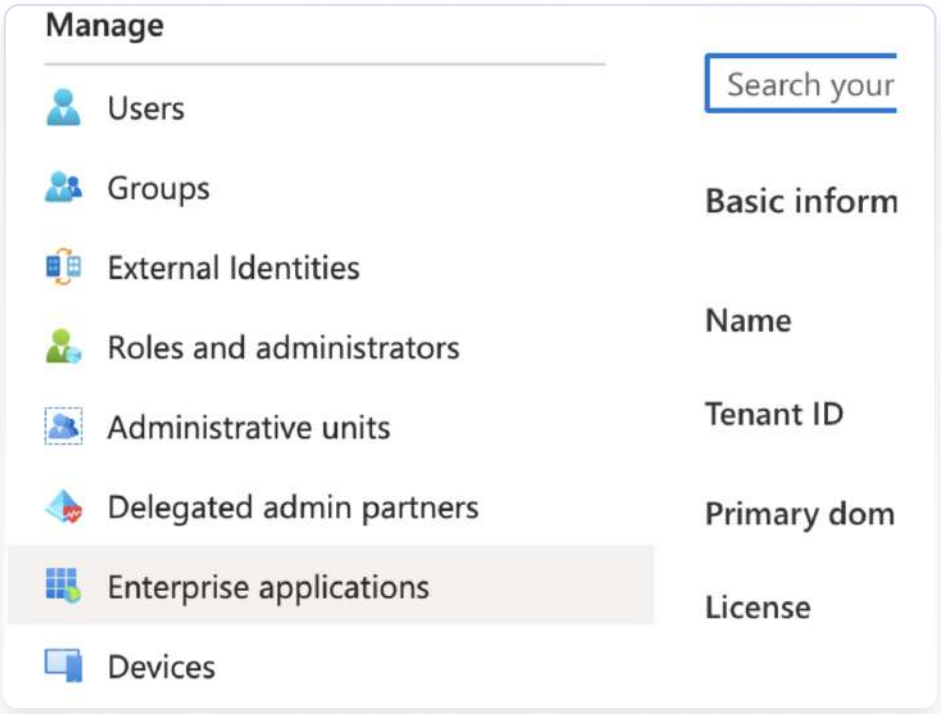


Click on the **Provisioning** tab in the OneLogin Application. Check **Enable provisioning** and **Save** the OneLogin Application. Configure provisioning settings as desired. Selecting either Delete or Suspend will result in the user being removed from the team on OneLogin account deletion (first dropdown) or suspension (second dropdown).

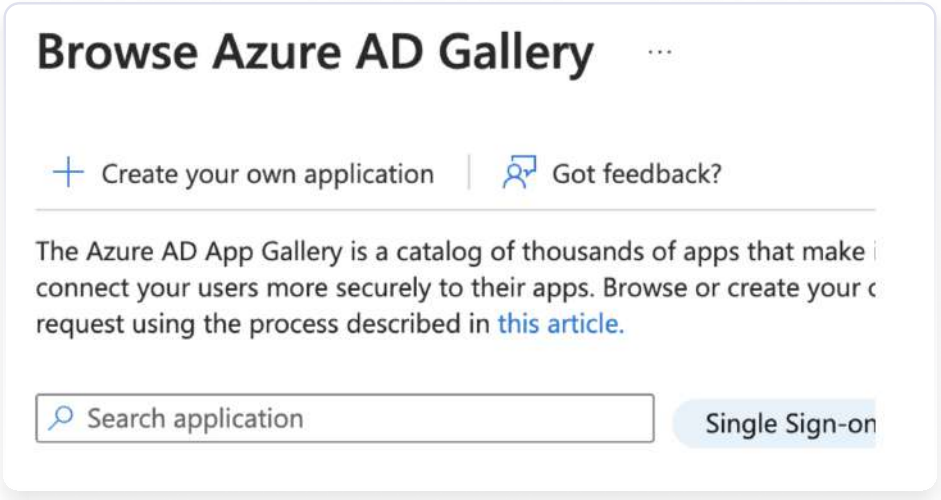


Configure SAML 2.0 SSO for Azure

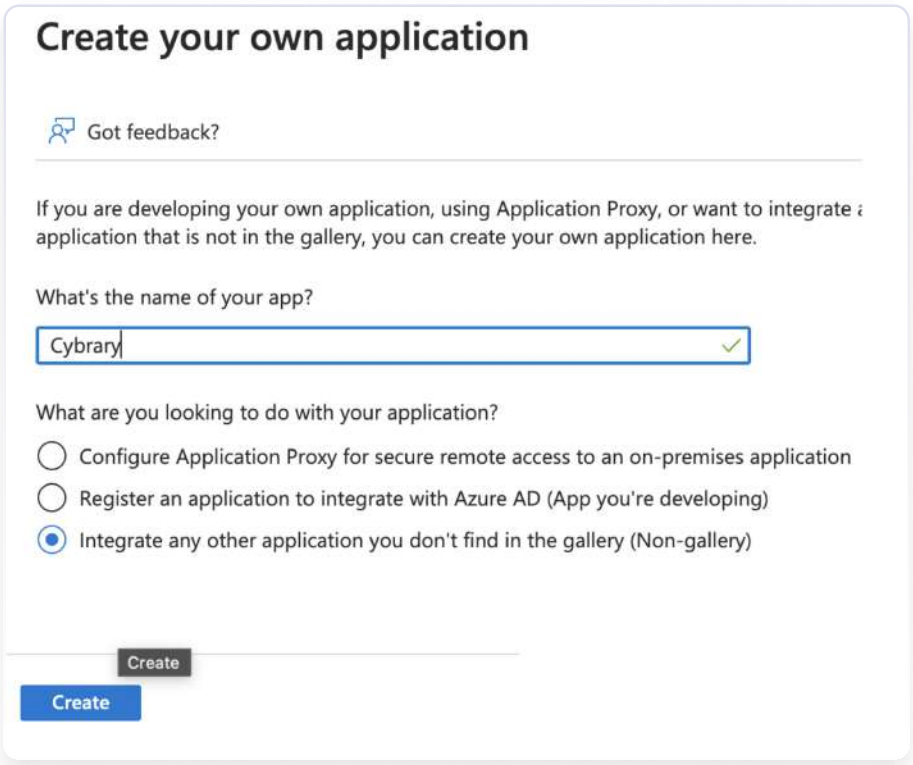
1 In **Azure Active Directory** select **Enterprise Applications** in the left nav.



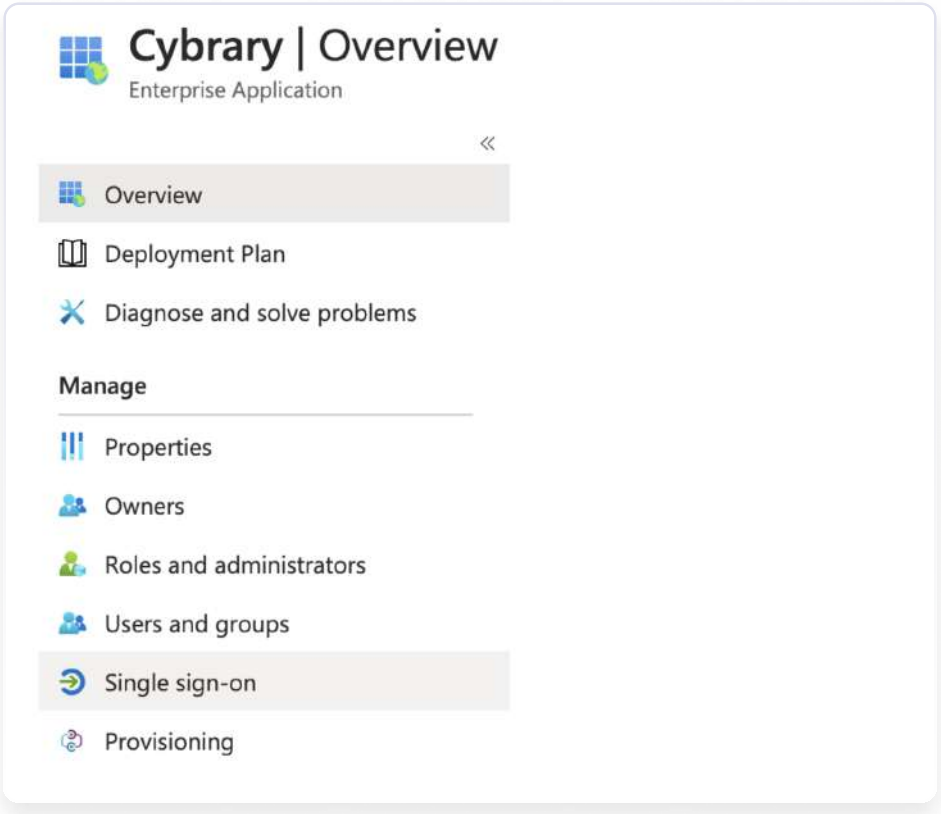
2 Select **Create your own application**.



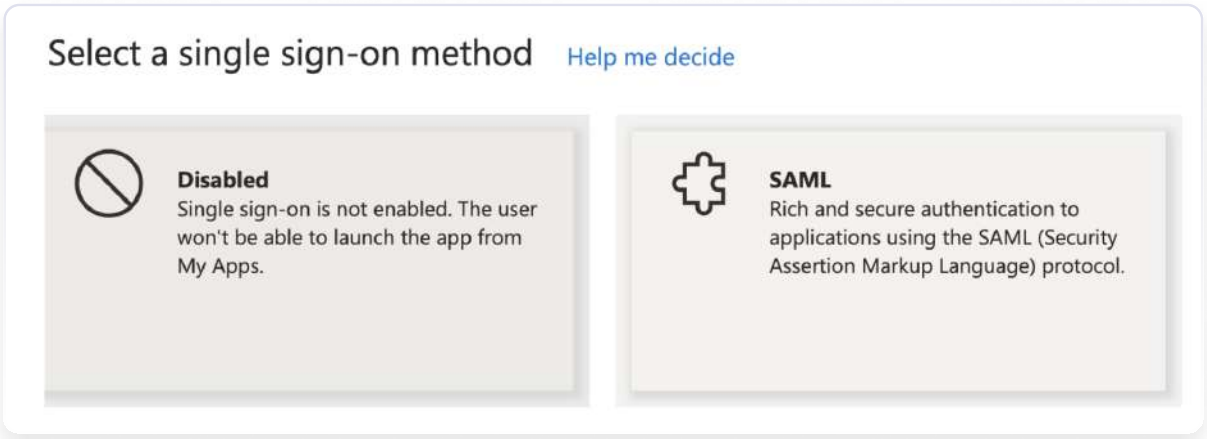
3 Enter an **App name** (eg. Cybrary) and select **Integrate any other application**. Click **Create** at the bottom.



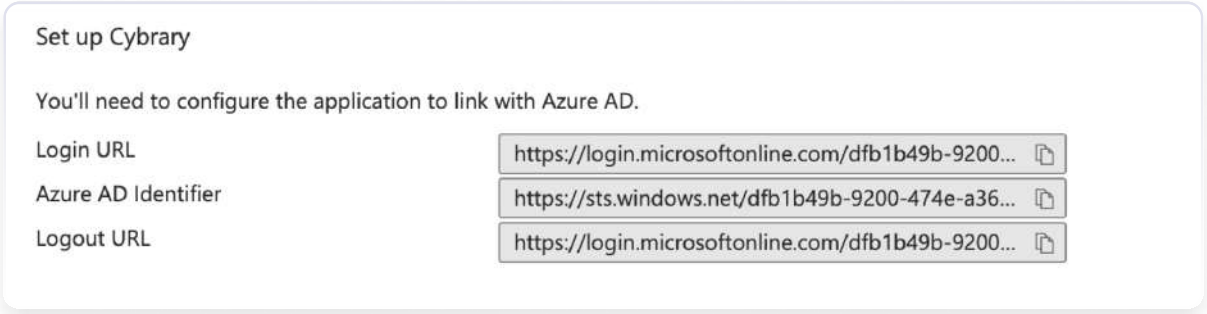
4 You will be redirected to the Overview for your new application. Select **Single sign-on** in the left nav.



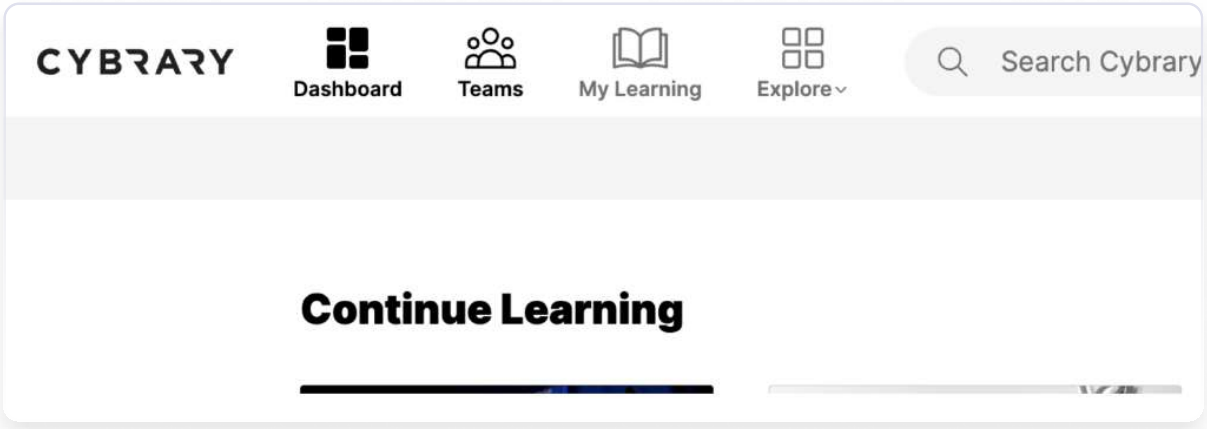
5 Select **SAML** for single sign-on method.



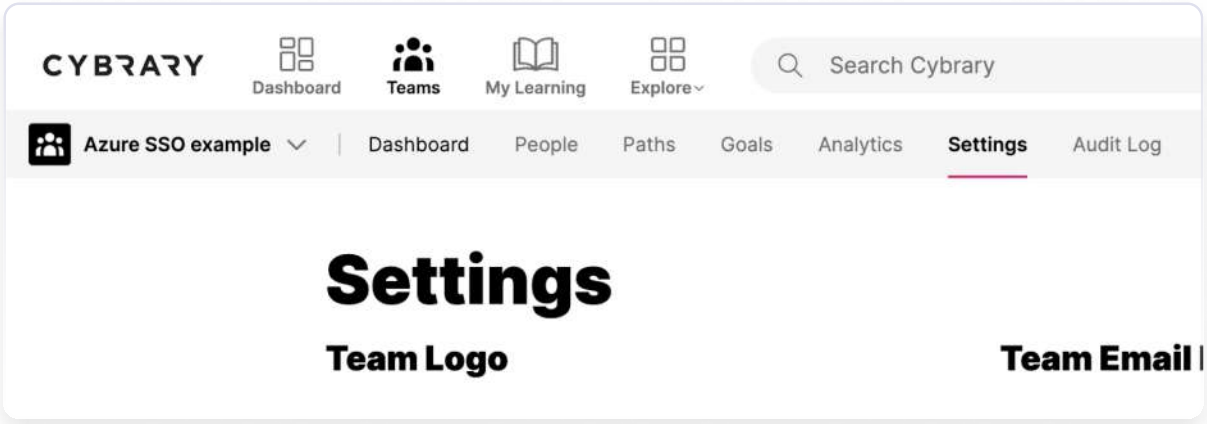
6 Scroll down to the section labeled Set up Cybrary (or the name of the application you entered in step 3). This section contains information you will need to copy over to the Cybrary app to enable SSO. Leave it **open and open a new tab/window**.



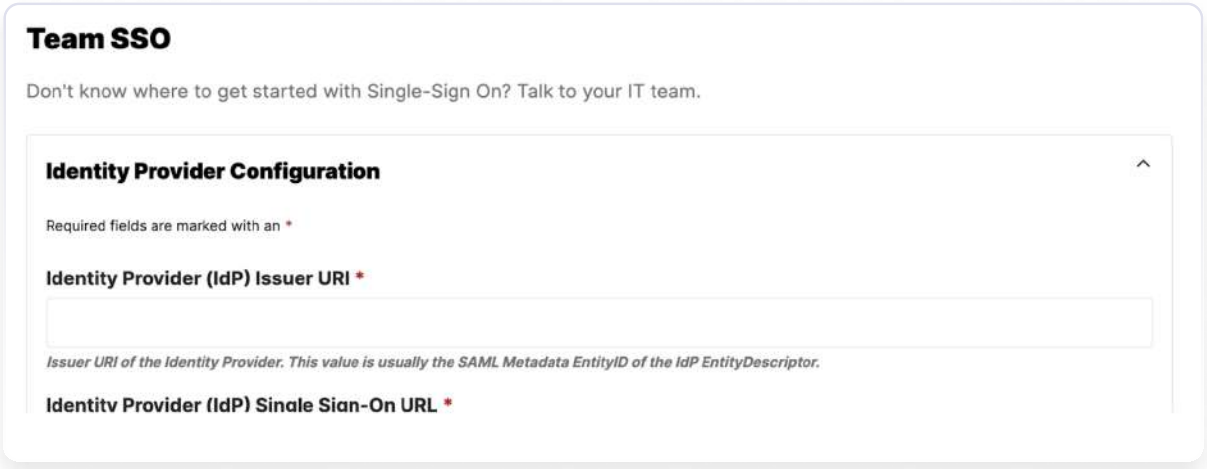
7 In the new tab/window, log in to https://app.cybrary.it and click on **Teams** in the top navigation.



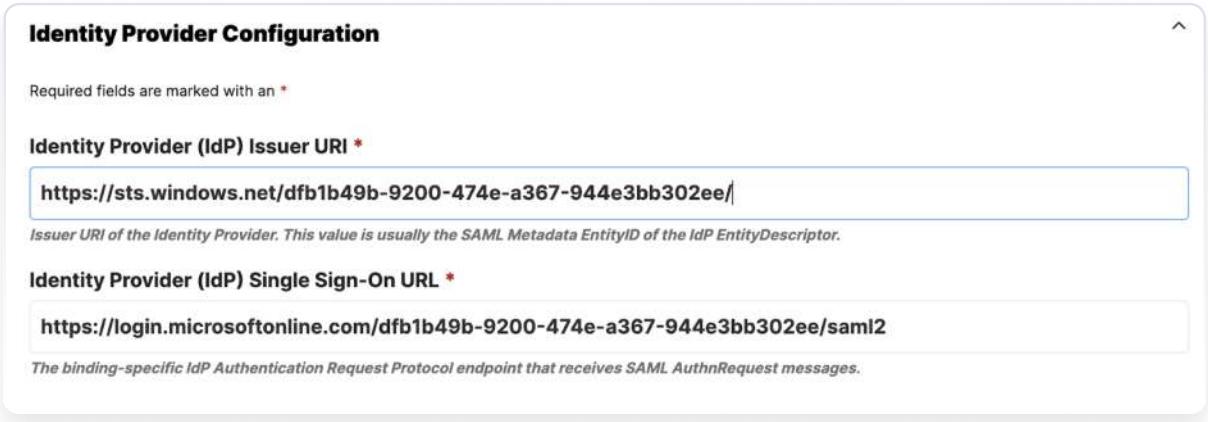
8 If you are an admin on more than one team, make sure the correct team is selected in the drop down on the top left. Click on **Settings** in the secondary to navigation.



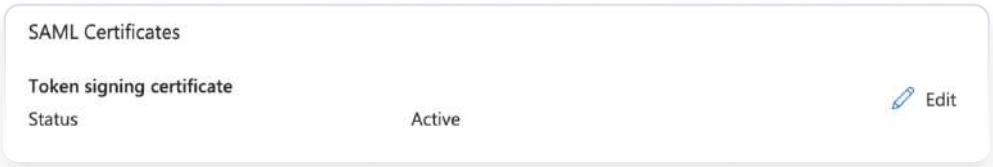
9 Scroll down to **Identity Provider Configuration** in the **Team SSO** section.



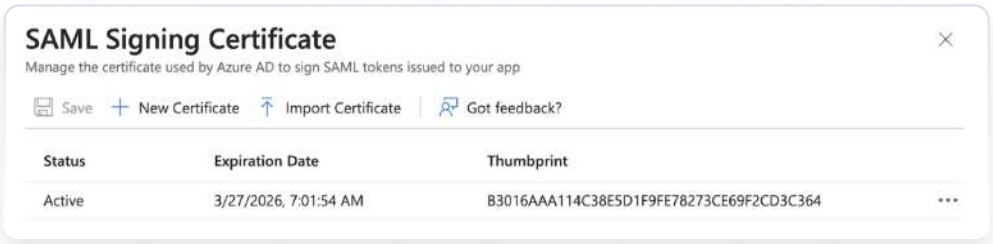
10 Enter the **Identity Provider (IdP) Issuer URI** (Azure AD Identifier) and the **Identity Provider (IdP) Single Sign-On URL** (Login URL), which can be found in the Set up Cybrary section of the Azure page you left open. Make sure you enter the correct value for each field by matching the field names listed above **Cybrary field** (Azure AD field).



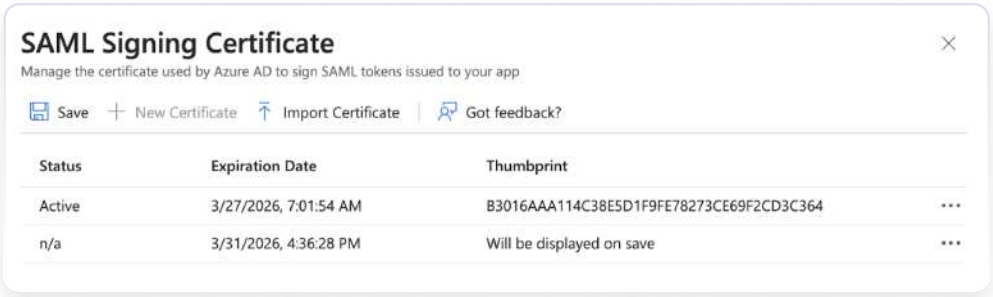
11 Back in the **Azure tab**, scroll up to the SAML Certificates section and click **Edit**.



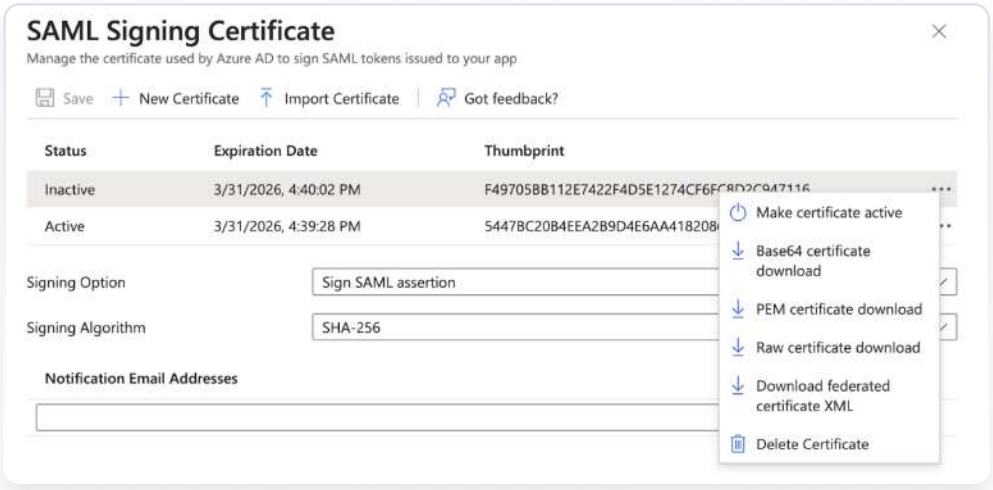
12 Click **New Certificate**. A new row will appear. Click **Save**.



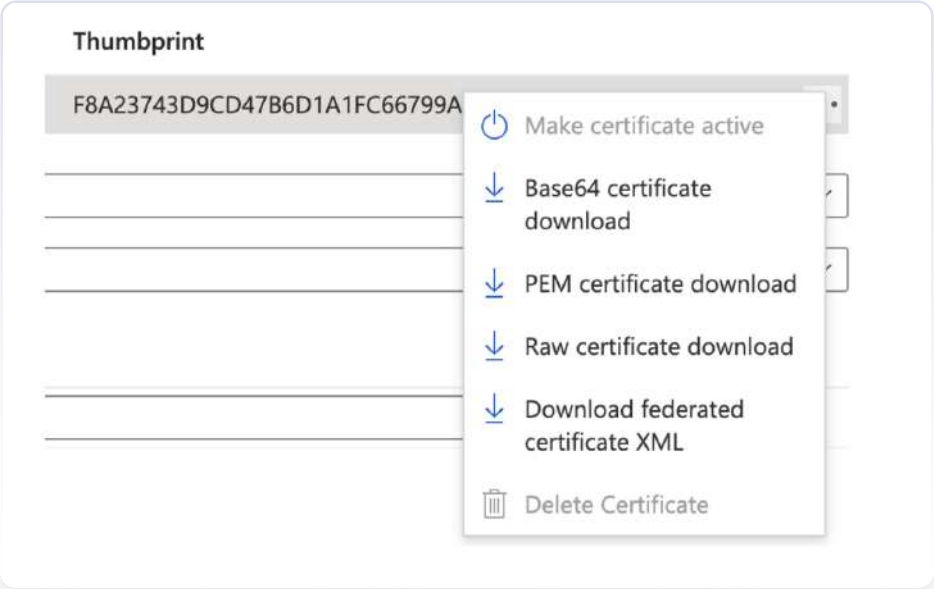
13 Click **Save**. The new certificate row will now have Status Inactive.



14 Click the 3 dots to the right of the new row (the one with Status Inactive). Click **Make certificate active**. Click **Yes** on the dialog window that appears to confirm. The new row will now have status Active. You may click the 3 dots of the old row (now Status Inactive) and click **Delete Certificate**, this certificate is not used.

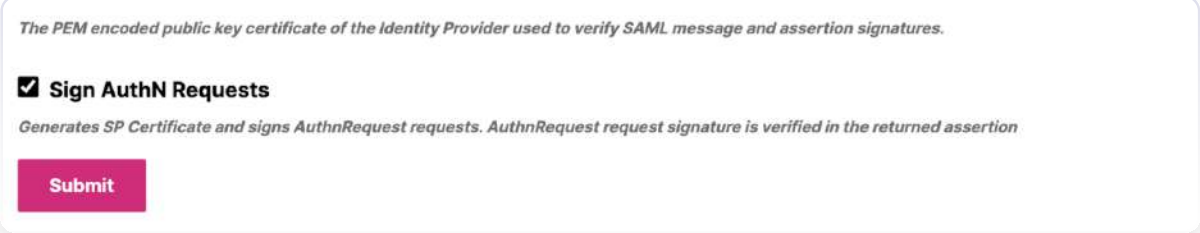


15 Click the 3 dots to the right of the new row and select **Base64 certificate download**. You will need to open this file in a text editor and copy the entire contents.



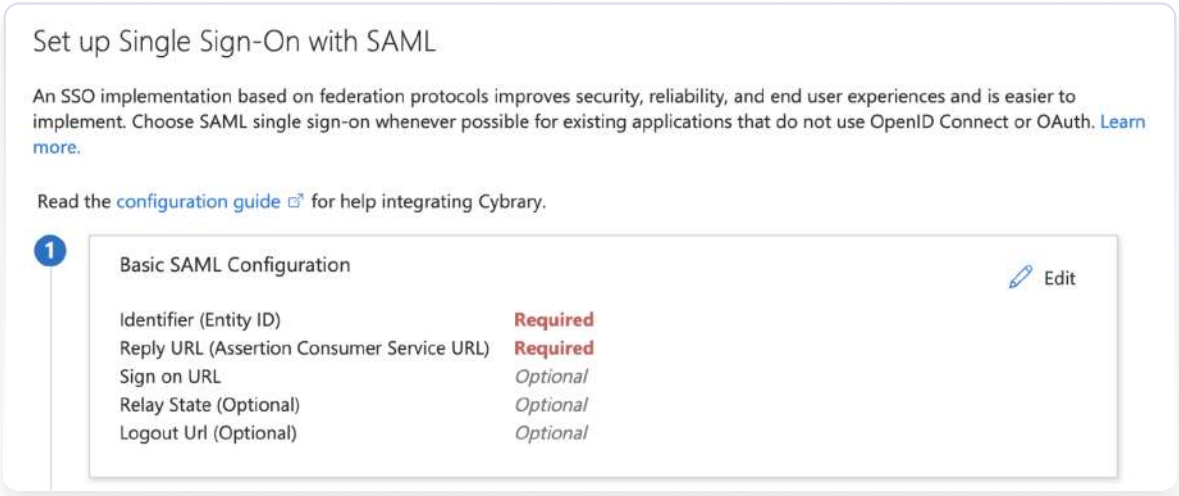
16 Back in the **Cybrary app**, paste the certificate contents into the **Identity Provider Signature Certificate** text area.

17 Check the **Sign AuthN Requests** option and click **Submit**. The page will refresh.

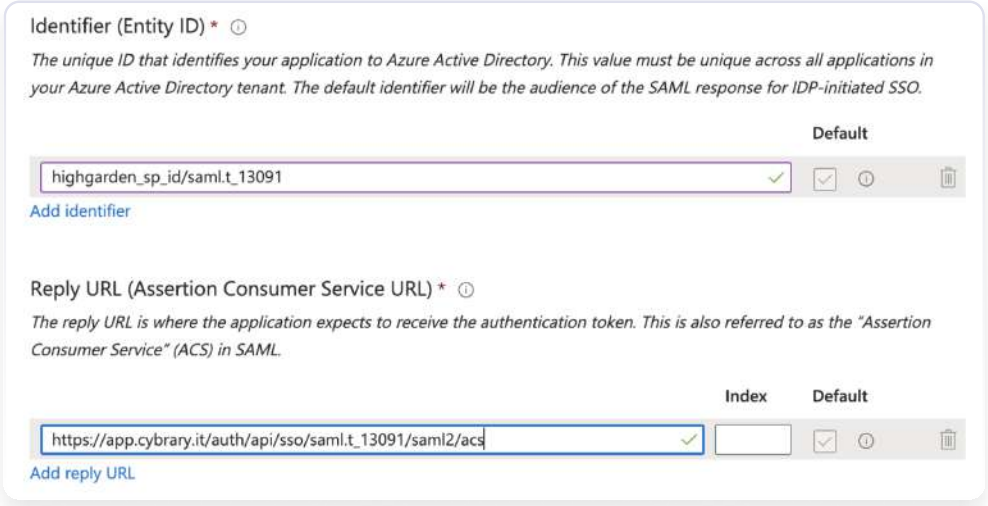


18 Scroll down to the **Service Provider Configuration** section in the **Team SSO** Section. You will need to copy these values over to the Azure AD app. Leave this page open.

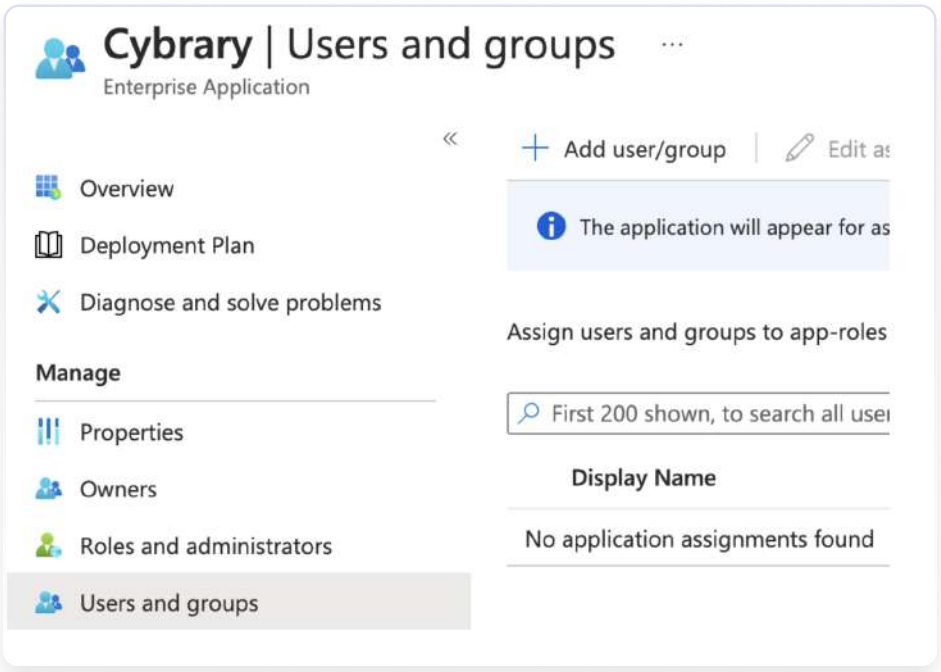
19 Back in the Azure AD SSO application configuration, close the certificate editor and scroll up to the top and find the **Basic SAML Configuration** section. Click **Edit**.



20 Click **Add identifier** and copy over the Audience URI value from the Cybrary app. Click **Add reply URL** and copy over the Single Sign-on URL value from the Cybrary app. Click **Save** at the top.



21 Your SSO application configuration is now complete, you will need to assign users to the application to test SSO with Cybrary. You can do this by clicking **Users and groups** in the left nav.



If you wish to enable SCIM, select **Provisioning** in the left nav. Change the Provisioning Mode to **Automatic**. Cybrary will provide you with the values for Tenant URL and Secret Token. Click **Save**.