

**CYBRARY** | FOR TEAMS



**Self-Service Guide**  
**to SAML 2.0 SSO Configuration**  
**for Okta, OneLogin and Azure**

# Table of Contents

## 3 Introduction

What is SAML?

What is SSO?

Benefits of SAML 2.0 SSO

## 4 Configure SAML 2.0 SSO for Okta

## 13 Configure SAML 2.0 SSO for OneLogin

## 19 Configure SAML 2.0 SSO for Azure

# 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

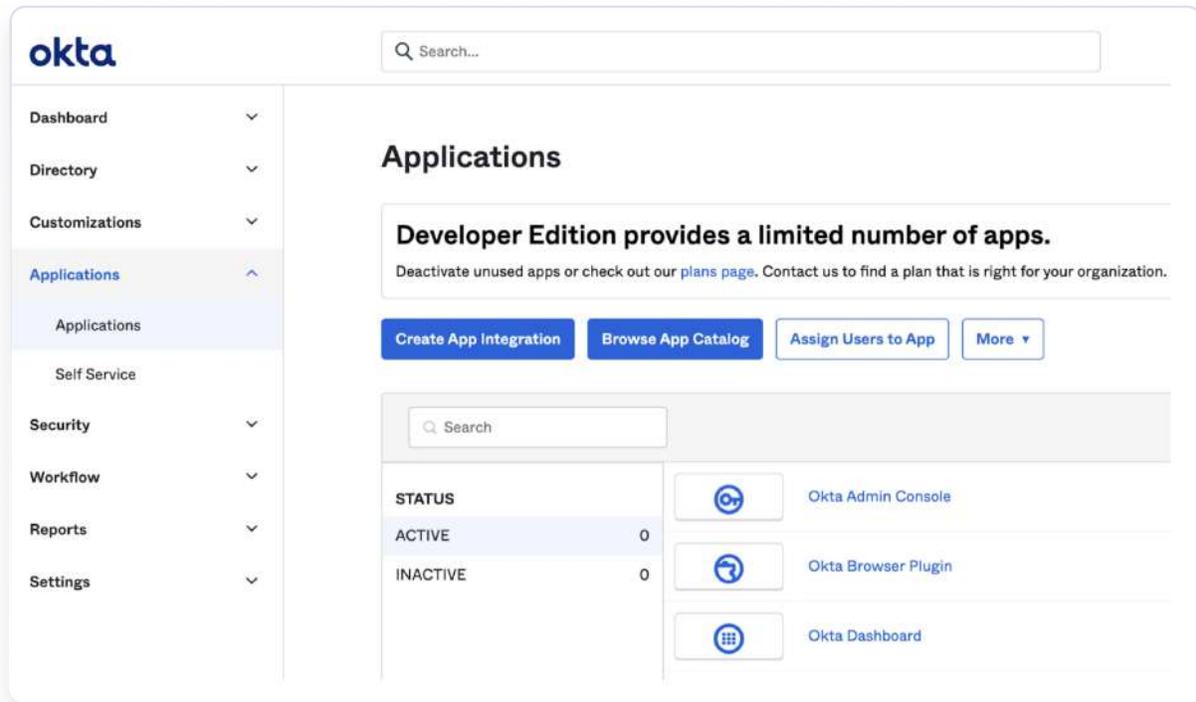


It improves the user experience as you only need to sign in once to access multiple web applications. (No need to remember multiple sets of credentials)

# Configure SAML 2.0 SSO for Okta

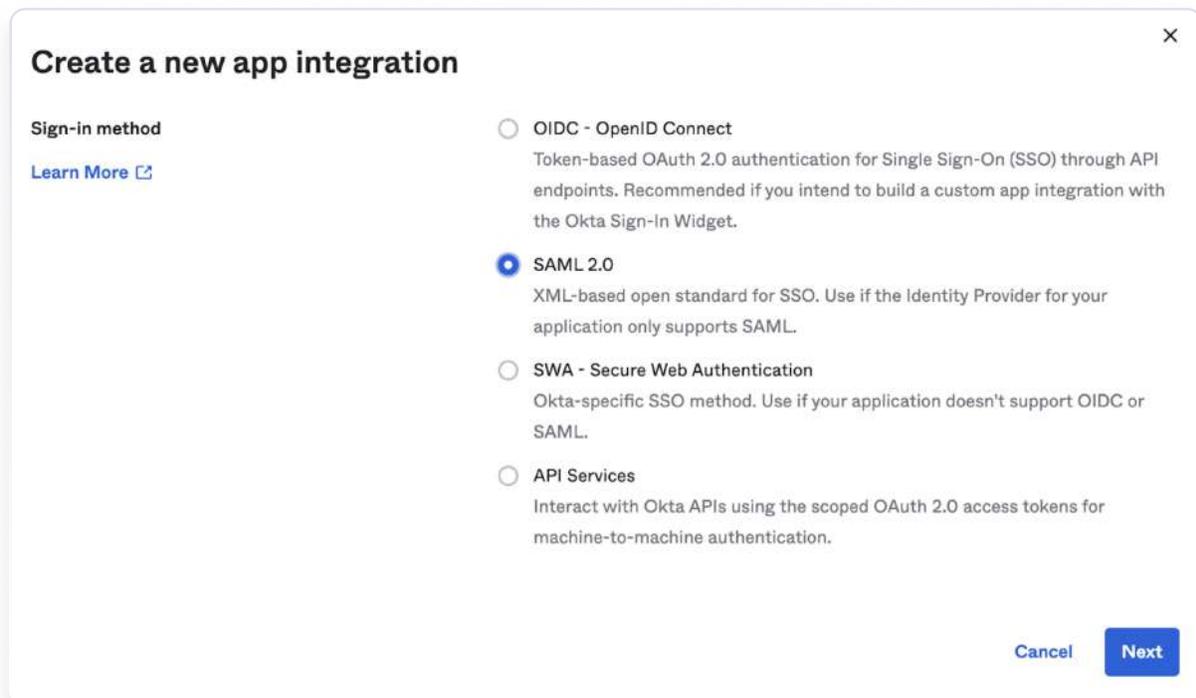
1

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**.

The screenshot shows the 'Create SAML Integration' interface. At the top, there are two tabs: '1 General Settings' (active) and '2 Configure SAML'. Below the tabs, the '1 General Settings' section contains the following fields:

- App name:** A text input field containing 'Cybrary'.
- App logo (optional):** A large empty box with a gear icon in the center and 'upload' and 'delete' icons in the top right corner.
- App visibility:** A checkbox labeled 'Do not display application icon to users', which is currently unchecked.

At the bottom left is a 'Cancel' link, and at the bottom right is a blue 'Next' button.

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.

The screenshot shows the 'Create SAML Integration' interface, now on the '2 Configure SAML' step. The '1 General Settings' tab is greyed out, and the '3 Feedback' tab is also greyed out. The main content area is titled 'A SAML Settings' and includes a 'General' section with the following fields:

- Single sign-on URL:** A text input field containing 'https://cybrary.it'. Below it is a checked checkbox labeled 'Use this for Recipient URL and Destination URL'.
- Audience URI (SP Entity ID):** A text input field containing 'cybrary'.
- Default RelayState:** An empty text input field. Below it is the text: 'If no value is set, a blank RelayState is sent'.
- Name ID format:** A dropdown menu with 'EmailAddress' selected.
- Application username:** A dropdown menu with 'Email' selected.

On the right side of the form, there is a help section:

- What does this form do?** This form generates the XML needed for the app's SAML request.
- Where do I find the info this form needs?** The app you're trying to integrate with should have its own documentation on using SAML. You'll need to find that doc, and it should outline what information you need to specify in this form.

5

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

**B Preview the SAML assertion generated from the information above**

[<> Preview the SAML Assertion](#)

This shows you the XML that will be used in the assertion - use it to verify the info you entered above

[Previous](#) [Cancel](#) [Next](#)

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**.

## Create SAML Integration

1 General Settings      2 Configure SAML

**3 Help Okta Support understand how you configured this application**

Are you a customer or partner?

I'm an Okta customer adding an internal app

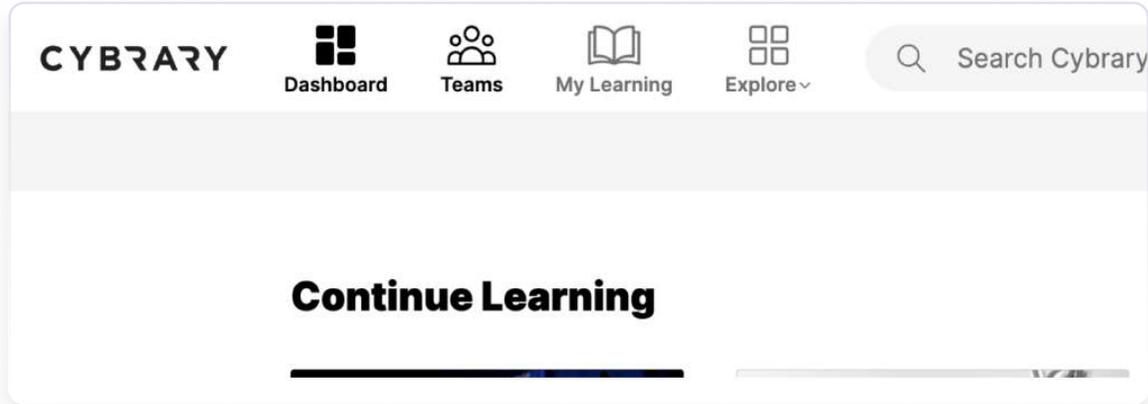
I'm a software vendor. I'd like to integrate my app with Okta

[Previous](#) [Finish](#)



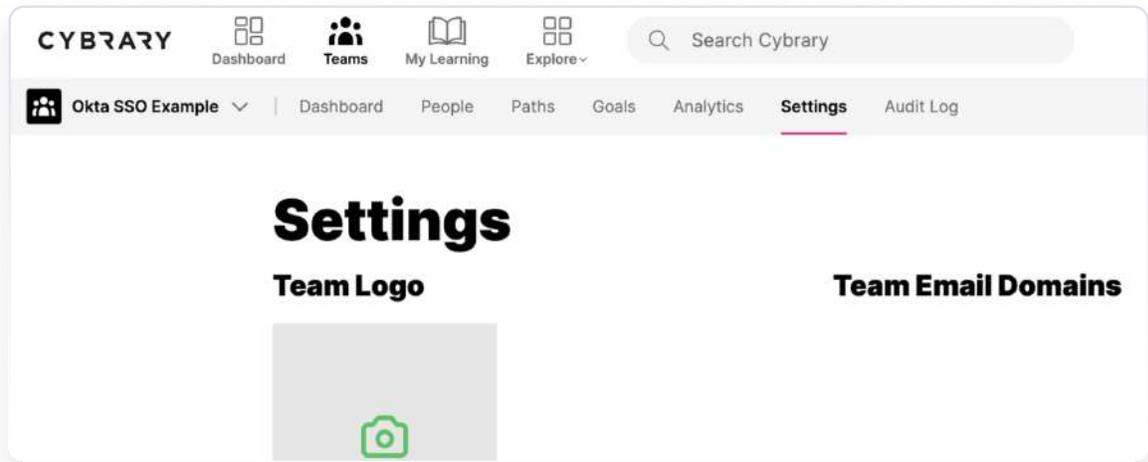
10

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



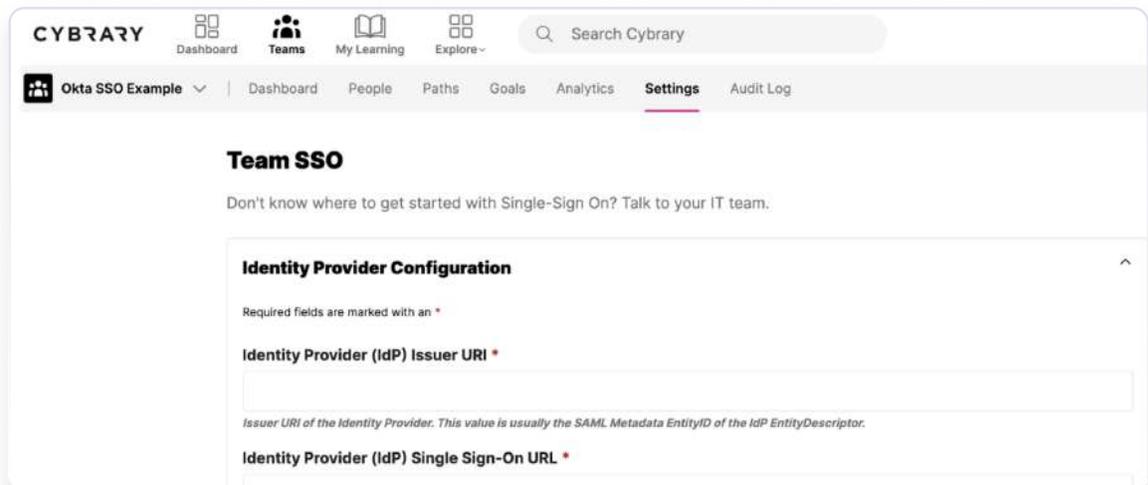
11

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.





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.

### Team SSO

Don't know where to get started with Single-Sign On? Talk to your IT team.

**Identity Provider Configuration** ▾

**Service Provider Configuration** ▲

**Audience URI (Service Provider Entity ID)**

[Copy](#)

**Single Sign-On URL (ACS Url)**

[Copy](#)

17

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



## Cybrary

[Active ▾](#) [View Logs](#) [Monitor Imports](#)

[General](#) [Sign On](#) [Import](#) [Assignments](#)

### App Settings [Edit](#)

Application label: Cybrary

Application visibility:  Do not display application icon to users

Provisioning:  Enable SCIM provisioning

Auto-launch:  Auto-launch the app when user signs into Okta.

Application notes for end users

Application notes for admins

18

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

### SAML Settings Edit

**GENERAL**

Single Sign On URL	https://cybrary.it
Recipient URL	https://cybrary.it
Destination URL	https://cybrary.it

19

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

### Edit SAML Integration

1 General Settings 2 Configure SAML

#### 1 General Settings

App name

App logo (optional)  



App visibility  Do not display application icon to users

[Cancel](#) Next

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.

**Edit SAML Integration**

1 General Settings      2 Configure SAML

**A SAML Settings**

**General**

Single sign-on URL ⓘ   
 Use this for Recipient URL and Destination URL

Audience URI (SP Entity ID) ⓘ

21. Scroll down to the bottom and click **Next**.

<> Preview the SAML Assertion

This shows you the XML that will be used in the assertion - use it to verify the info you entered above

Previous      Cancel      Next

22

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

Previous      Finish

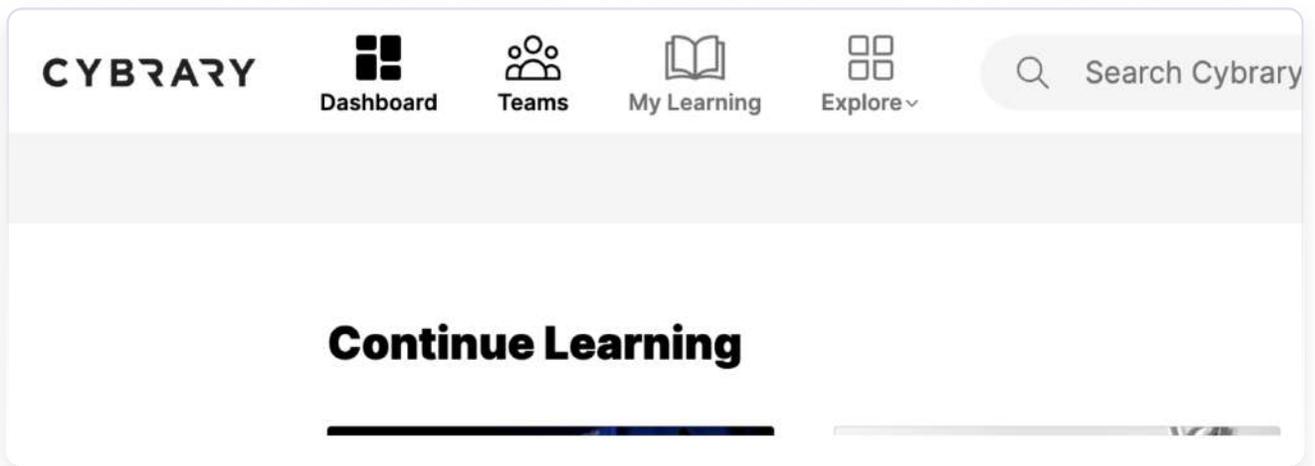


Your SSO application configuration is now complete. Once users are assigned to the application in Okta they will be able to log in with SSO.

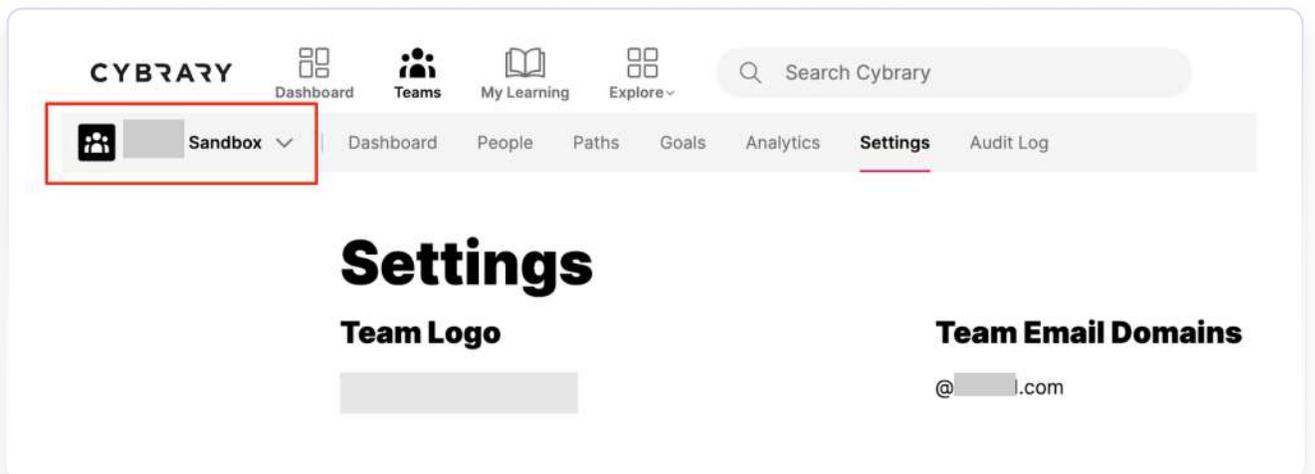
# Configure SAML 2.0 SSO for OneLogin

**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.

SCIM Provisioner with SAML (SCIM v2 Core)

Info

Configuration

Parameters

Rules

**SSO**

Access

Provisioning

Users

Privileges

### Enable SAML2.0

Sign on method  
SAML2.0

X.509 Certificate  
Standard Strength Certificate (2048-bit)  
[Change](#) [View Details](#)

SAML Signature Algorithm  
SHA-1

Issuer URL  
https://app.onelogin.com/saml/metadata/8e7263d3-7981-42c7-a12f-ac581d95502d

SAML 2.0 Endpoint (HTTP)  
https://cybrary-dev.onelogin.com/trust/saml2/http-post/sso/8e7263d3-7981-42c7-a12f-ac581d95502d

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.

## Team SSO

Don't know where to get started with Single-Sign On? Talk to your IT team.

### Identity Provider Configuration

Required fields are marked with an \*

**Identity Provider (IdP) Issuer URI \***  
https://app.onelogin.com/saml/metadata/8e7263d3-7981-42c7-a12f-ac581d95502d  
*Issuer URI of the Identity Provider. This value is usually the SAML Metadata EntityID of the IdP EntityDescriptor.*

**Identity Provider (IdP) Single Sign-On URL \***  
https://cybrary-dev.onelogin.com/trust/saml2/http-post/sso/8e7263d3-7981-42c7-a12f-ac581d95502d  
*The binding-specific IdP Authentication Request Protocol endpoint that receives SAML AuthnRequest messages.*

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-----).

X.509 Certificate

Standard Strength Certificate (2048-bit)

[Change](#) [View Details](#)

### X.509 Certificate

X.509 Certificate

```
-----BEGIN CERTIFICATE-----
MIID8jCCA+qgAwIBAgIUFeeo21j0xLHDA0o2y/wOP19J09swDQYJKoZIhvcNAQEF
BQAwtDEXMBUGA1UECgwOQ3li cmFyeSBjVjCBMTEMxFTATBgNVBAsMDE9uZUxvZ2lu
IElkUDEaMBGGA1UEAwwRT25lTG9naW4gQWNjb3VudCAwHhcNMjMwNDI0
WhcNMjgwMjA3MTMwNDI0WjBMMRcwFQYDVQQKDA5DeWJyYXJ5IEIUEiExMQzEVMBMG
A1UECwwMT25lTG9naW4gSWRQMRowGAYDVQQDDDBFPbmVmb2dpbiBBY2NvdW50IDCC
ASIdDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALBz Mzpz8jHQKvGu5uNXA2/d
0eP3V1hIKCNPF0R0+7vY07xP3PcN47kew93+ig3v7uf7jG6h1vi kxThXmvFA0v00
```

6

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

**Identity Provider Signature Certificate \***

```
-----BEGIN CERTIFICATE-----
MIID8jCCA+qgAwIBAgIUFeeo21j0xLHDA0o2y/wOP19J09swDQYJKoZIhvcNAQEF
BQAwtDEXMBUGA1UECgwOQ3li cmFyeSBjVjCBMTEMxFTATBgNVBAsMDE9uZUxvZ2lu
IEIkUDEaMBGGA1UEAwwRT25lTG9naW4gQWNjb3VudCAwHhcNMjMwNDI0
WhcNMjgwMjA3MTMwNDI0WjBMMRcwFQYDVQQKDA5DeWJyYXJ5IEIUEiExMQzEVMBMG
A1UECwwMT25lTG9naW4gSWRQMRowGAYDVQQDDDBFPbmVmb2dpbiBBY2NvdW50IDCC
ASIdDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALBz Mzpz8jHQKvGu5uNXA2/d
0eP3V1hIKCNPF0R0+7vY07xP3PcN47kew93+ig3v7uf7jG6h1vi kxThXmvFA0v00
```

*The PEM encoded public key certificate of the Identity Provider used to verify SAML message and assertion signatures.*

7

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

*The PEM encoded public key certificate of the Identity Provider used to verify SAML message and assertion signatures.*

**Sign AuthN Requests**

*Generates SP Certificate and signs AuthnRequest requests. AuthnRequest request signature is verified in the returned assertion*

**Submit**

8

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

### Team SSO

Don't know where to get started with Single-Sign On? Talk to your IT team.

**Identity Provider Configuration** ▼

**Service Provider Configuration** ▲

**Audience URI (Service Provider Entity ID)**

 Copy

**Single Sign-On URL (ACS Url)**

 Copy

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**.

### SCIM Provisioner with SAML (SCIM v2 Core)

Info	<b>Application details</b>  SAML Audience URL <input type="text" value="highgarden_sp_id/saml.t_12773"/>  SAML Consumer URL <input type="text" value="https://app.cybrary.it/auth/api/sso/saml.t_12773/saml2/acs"/>
<b>Configuration</b>	
Parameters	
Rules	
SSO	

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**.

Applications /  
SCIM Provisioner with SAML (SCIM v2 Core)

Info

**Configuration**

Parameters

Rules

SSO

Access

Provisioning

Users

Privileges

**API Connection**

API Status

● Disabled Enable

SCIM Base URL

https://app.cybrary.it/auth/api/org/12773/scim/v2

Custom Headers

SCIM Bearer Token

11

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

More Actions ▼

Save

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

Applications / SCIM Provisioner with SAML (SCIM v2 Core)

Info

**Configuration**

Parameters

Rules

SSO

Access

Provisioning

Users

Privileges

**Application details**

SAML Audience URL

highgarden\_sp\_id/saml.t\_12773

SAML Consumer URL

https://app.cybrary.it/auth/api/sso/saml.t\_12773/saml2/acs

**API Connection**

API Status

● Disabled 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).

Applications / SCIM Provisioner with SAML (SCIM v2 Core)

Info

Configuration

Parameters

Rules

SSO

Access

**Provisioning**

Users

Privileges

**Workflow**

Enable provisioning

Require admin approval before this action is performed

Create user

Delete user

Update user

When users are deleted in OneLogin, or the user's app access is removed, perform the below action

Delete

When user accounts are suspended in OneLogin, perform the following action:

Suspend

# Configure SAML 2.0 SSO for Azure

1

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

**Manage**

Search your

- Users
- Groups
- External Identities
- Roles and administrators
- Administrative units
- Delegated admin partners
- Enterprise applications**
- Devices

Basic inform

Name

Tenant ID

Primary dom

License

2

Select **Create your own application**.

**Browse Azure AD Gallery** ...

+ Create your own application | Got feedback?

The Azure AD App Gallery is a catalog of thousands of apps that make it easier to connect your users more securely to their apps. Browse or create your own app or request using the process described in [this article](#).

Search application

Single Sign-on

3

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

## Create your own application

 Got feedback?

If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.

What's the name of your app?

What are you looking to do with your application?

- Configure Application Proxy for secure remote access to an on-premises application
- Register an application to integrate with Azure AD (App you're developing)
- Integrate any other application you don't find in the gallery (Non-gallery)

Create

Create

4

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

## Cybrary | Overview

Enterprise Application

<<

- Overview
- Deployment Plan
- Diagnose and solve problems

**Manage**

- Properties
- Owners
- Roles and administrators
- Users and groups
- Single sign-on
- Provisioning

5

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

### Select a single sign-on method [Help me decide](#)



**Disabled**  
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.



**SAML**  
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

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**.

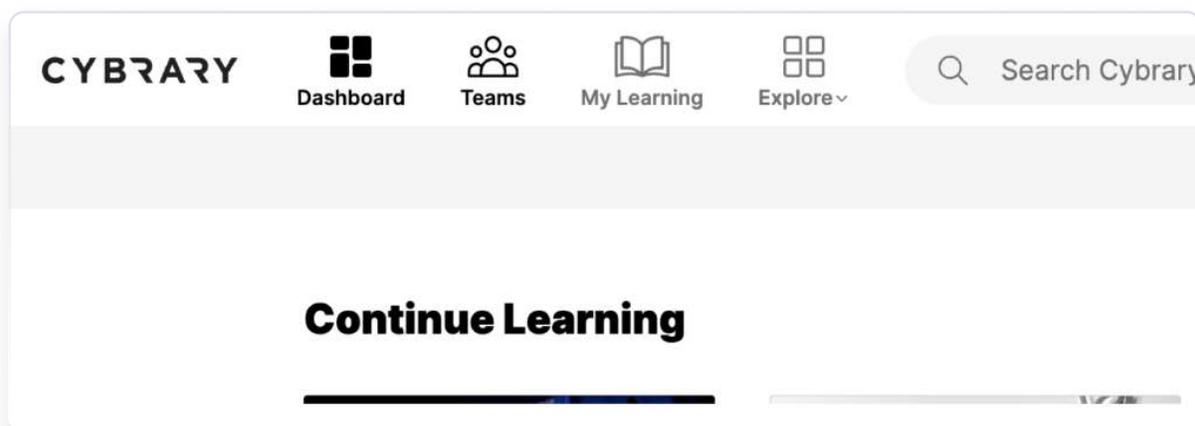
#### Set up Cybrary

You'll need to configure the application to link with Azure AD.

Login URL	<input type="text" value="https://login.microsoftonline.com/dfb1b49b-9200..."/>
Azure AD Identifier	<input type="text" value="https://sts.windows.net/dfb1b49b-9200-474e-a36..."/>
Logout URL	<input type="text" value="https://login.microsoftonline.com/dfb1b49b-9200..."/>

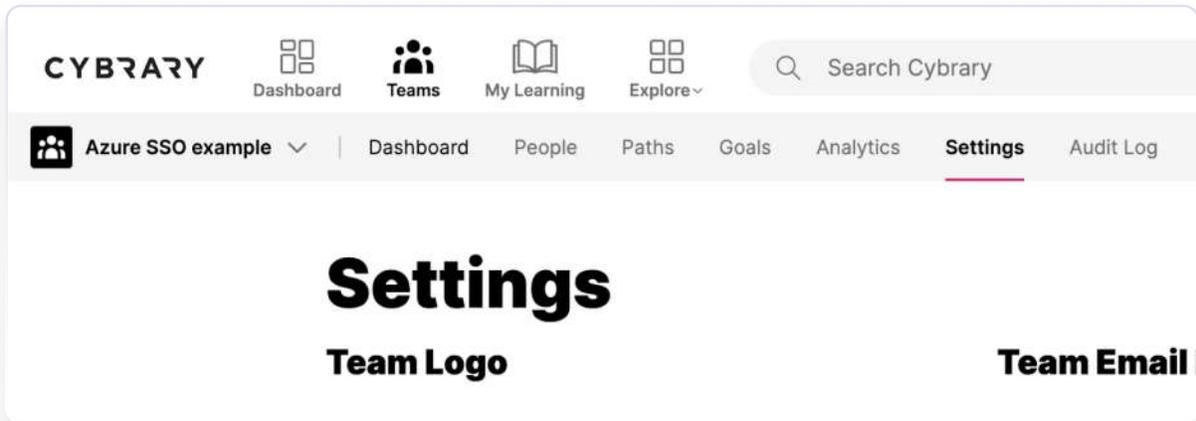
7

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



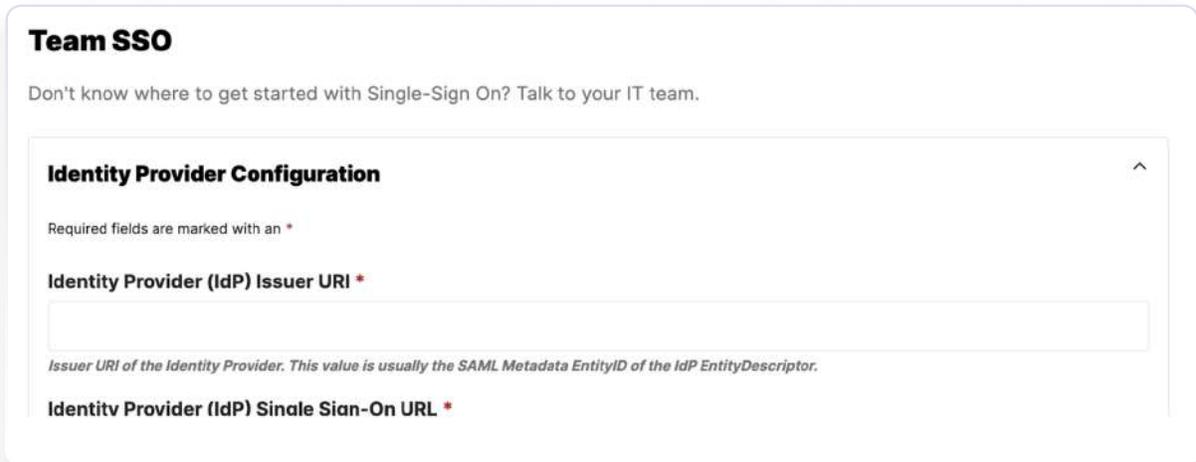
8

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.



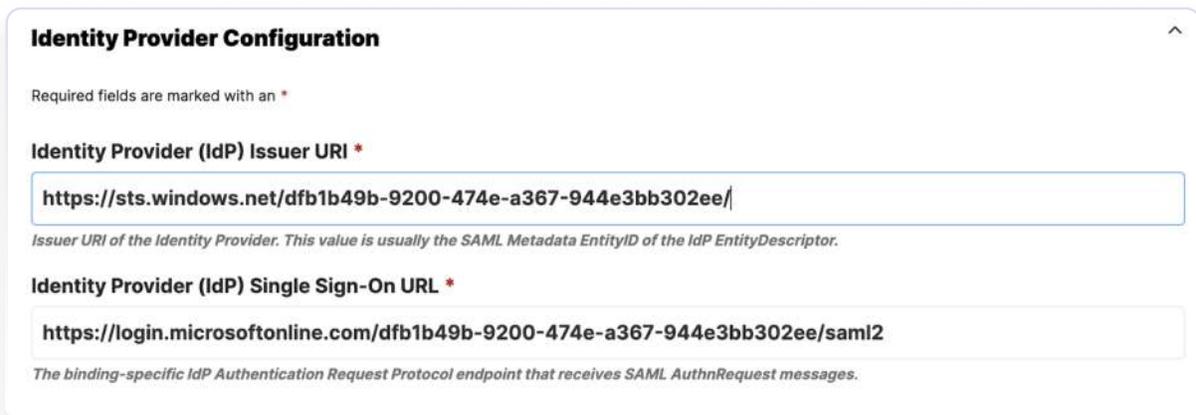
9

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**.

SAML Certificates

Token signing certificate	Active	<a href="#">Edit</a>
---------------------------	--------	----------------------

12

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

**SAML Signing Certificate**

Manage the certificate used by Azure AD to sign SAML tokens issued to your app

Save + New Certificate Import Certificate Got feedback?

Status	Expiration Date	Thumbprint
Active	3/27/2026, 7:01:54 AM	B3016AAA114C38E5D1F9FE78273CE69F2CD3C364
Inactive	3/31/2026, 4:36:28 PM	Will be displayed on save

13

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

**SAML Signing Certificate**

Manage the certificate used by Azure AD to sign SAML tokens issued to your app

Save + New Certificate Import Certificate Got feedback?

Status	Expiration Date	Thumbprint
Active	3/27/2026, 7:01:54 AM	B3016AAA114C38E5D1F9FE78273CE69F2CD3C364
n/a	3/31/2026, 4:36:28 PM	Will be displayed on save

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.

**SAML Signing Certificate**

Manage the certificate used by Azure AD to sign SAML tokens issued to your app

Save + New Certificate Import Certificate Got feedback?

Status	Expiration Date	Thumbprint
Inactive	3/31/2026, 4:40:02 PM	F49705BB112E7422F4D5E1274CF6FC8D2C9A7116
Active	3/31/2026, 4:39:28 PM	5447BC20B4EEA2B9D4E6AA418208

Signing Option: Sign SAML assertion

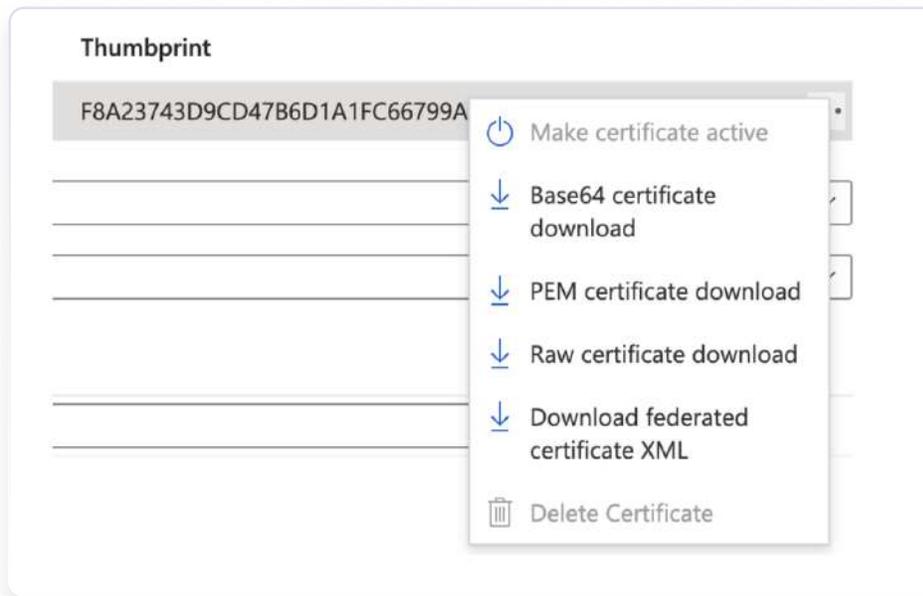
Signing Algorithm: SHA-256

Notification Email Addresses: [Empty field]

- Make certificate active
- Base64 certificate download
- PEM certificate download
- Raw certificate download
- Download federated certificate XML
- Delete Certificate

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.



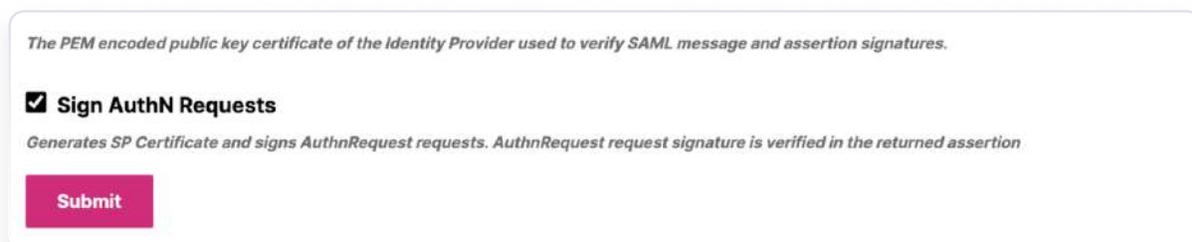
16

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.

**Service Provider Configuration**

**Audience URI (Service Provider Entity ID)**

highgarden\_sp\_id/saml.t\_13091 Copy

**Single Sign-On URL (ACS Url)**

https://app.cybrary.it/auth/api/sso/saml.t\_13091/saml2/acs Copy

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**.

Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. [Learn more.](#)

Read the [configuration guide](#) for help integrating Cybrary.

**1** Basic SAML Configuration Edit

Identifier (Entity ID)	<b>Required</b>
Reply URL (Assertion Consumer Service URL)	<b>Required</b>
Sign on URL	<i>Optional</i>
Relay State (Optional)	<i>Optional</i>
Logout Url (Optional)	<i>Optional</i>

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.

**Identifier (Entity ID) \***

*The unique ID that identifies your application to Azure Active Directory. This value must be unique across all applications in your Azure Active Directory tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.*

Default

highgarden\_sp\_id/saml.t\_13091 Add identifier

**Reply URL (Assertion Consumer Service URL) \***

*The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.*

	Index	Default
https://app.cybrary.it/auth/api/sso/saml.t_13091/saml2/acs <span style="float: right;">Add reply URL</span>	1	<input checked="" type="checkbox"/>

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**.