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



Configure SAML 2.0 SSO for Okta



2

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

okta		Q Search			
Dashboard	~				
Directory	~	Applications			
Customizations	~	Developer Edition provides a limited number of apps.		mited number of apps.	
Applications	^	Deactivate unused apps or	check out our	plans page. C	Contact us to find a plan that is right for your organization.
Applications		Create App Integration	Browse Ap	p Catalog	Assign Users to App More 🔻
Self Service		-			
Security	~	Q Search			
Norkflow	×	STATUS		0	Okta Admin Console
Reports	~	ACTIVE	0		
Settings	~	INACTIVE	0	0	Okta Browser Plugin
					Okta Dashboard

Select the SAML 2.0 option and click Next.

Sign-in method	OIDC - OpenID Connect
Learn More	Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through AF
	endpoints. Recommended if you intend to build a custom app integration wi the Okta Sign-In Widget.
	SAML 2.0
	XML-based open standard for SSO. Use if the Identity Provider for your
	application only supports SAML.
	SWA - Secure Web Authentication
	Okta-specific SSO method. Use if your application doesn't support OIDC or
	API Services Interact with Okta APIc using the sconed OAuth 2.0 access tokens for
	meract with Okta Aris using the scoped Okuth 2.0 access tokens for machine-to-machine authentication.
	Cancel
	Cancel

Configure SAML 2.0 SSO for Okta

y

3

4

1 General Settings	2 Configure SAML
1 General Settings	
App name	Cybrary
App logo (optional)	▲ ■

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.

General Settings	2 Configure SAML	S Feedback
A SAML Settings General		What does this form do? This form generates the XML needed
Single sign-on URL	https://cybrary.it	for the app's SAML request. Where do I find the info this form
	Use this for Recipient URL and Destination URL	needs?
Audience URI (SP Entity ID) 🛛	cybrary	The app you're trying to integrate with should have its own documentation or using SAML. You'll need to find that
Default RelayState 😡		doc, and it should outline what
	If no value is set, a blank RelayState is sent	form.
Name ID format 🛛	EmailAddress *	
Application username		

CYBRARY

5

in

Þ

<> Prev	view the SAML Assertion	
This shov	vs you the XML that will be used in	n the assertion - use it to verify the info you entered a
Previous	Cancel	

General Settings	2 Configure SAML
Help Okta Support understand	how you configured this application
	 I'm a software vendor. I'd like to integrate my app with Okta
Provinue	Fini

🖸 in f

6

y

5

CYBRARY

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.

*	Active View Logs Monitor Imports		
General Sign O	n Import Assignments		
Settings		Edit	About SAML 2.0 streamlines the end user experience by not requiring the user to
Sign on metho	ds		know their credentials. Users cannot edit their credentials when SAML 2.0 is

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

					SAML Setup
General	e new certificate				Single Sign On using SAML will not work until you configure the app to
Туре	Created	Expires	Status	Actions	trust Okta as an IdP.
		M 0022	Inesting A	Autions -	C View SAML setup instruction

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**.

4	Note: These setup instructions include certificate information for this app's most recently created SAML signing access to the app using these instructions, that certificate must be active.
The	following is needed to configure Cybrary
0	dentity Provider Single Sign-On URL:
	https://dev-590666417.okta.com/app/dev-59056417_cybrary_1/exk8ne0fr1hZj1w4M5d7/sso/saml
0	dentity Provider Issuer:
	http://www.okta.com/exk8ne0fr1hZj1w4M5d7
0	K.509 Certificate:
	BEGIN_CERTIFICATE MII0qDCCApCgAwIBAgIGAYbHLFA7MA0GCSqBSIb3DQEBCwUAMIGUHQswCQYDVQQGewJVUZETMBEG

9

8

7



10

CYBZAZY

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.

Identity Provider Configuration

Required fields are marked with an *

13

Identity Provider (IdP) Issuer URI *

http://www.okta.com/exk8ne0frlhZj1w4M5d7

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://dev-59056417.okta.com/app/dev-59056417_cybrary_1/exk8ne0frlhZj1w4M5d7/sso/saml

The binding-specific IdP Authentication Request Protocol endpoint that receives SAML AuthnRequest messages.

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.

Identity Provider Signature Certificate *

-----BEGIN CERTIFICATE-----

MIIDqDCCApCgAwIBAgIGAYbHLFA7MA0GCSqGSIb3DQEBCwUAMIGUMQswCQYDVQQGEwJVUzETMBEG A1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YTEU MBIGA1UECwwLU1NPUHJvdmlkZXIxFTATBgNVBAMMDGRIdi010TA1NjQxNzEcMBoGCSqGSlb3DQEJ ARYNaW5mb0Bva3RhLmNvbTAeFw0yMzAzMDkxNjE5MTVaFw0zMzAzMDkxNjIwMTVaMIGUMQswCQYD

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

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



15

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.

n'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)	^
Service Provider Configuration Audience URI (Service Provider Entity ID) highgarden_sp_id/saml.t_12773	Сору
Service Provider Configuration Audience URI (Service Provider Entity ID) highgarden_sp_id/saml.t_12773 Single Sign-On URL (ACS Url)	Сору

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

Cybra Active	View Logs Monitor Imports
ieneral Sign On Impor	rt 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	

in

7

f

10

16

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

18

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

1 General Settings	2 Configure SAML
1 General Settings	
App name	Cybrary
App logo (optional)	
	i©:
App visibility	Do not display application icon to users
Capacil	Nev

y

🖻 in f

11

CYBRARY

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.

General Settings	2 Configure SAML	
A SAML Settings		
General		
Single sign-on URL 🛛	ps://app.cybrary.it/auth/api/sso/saml.t_	13085/sam12/acs
	Use this for Recipient URL and Destin	ation URL
Audience URI (SP Entity ID) 🔞	highgarden_sp_id/saml.t_13085	
. Scroll down to the bottom an	nd click Next .	
. Scroll down to the bottom an • Preview the SAML Assertion This shows you the XML that will b	e used in the assertion - use it to verify the info	you entered above
. Scroll down to the bottom an Preview the SAML Assertion This shows you the XML that will b evious Cancel	e used in the assertion - use it to verify the info	you entered above
. Scroll down to the bottom an •> Preview the SAML Assertion This shows you the XML that will b evious Cancel to the bottom and click Fin	nd click Next .	you entered above

22

20

CYBRARY

Y

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.

CYBZAZY	Dashboard	oOo Teams	My Learning	Explore ~	Q	Search Cyb
	Contin	ue Le	arning			
		_				1.2.40
lf vou are an admin on	more than one	team. ma	ke sure vour co	mpany's San	dbox is s	elected in the
down on the top left. C	click on Setting	s in the se	econdary to nav	igation.		
CYBRARY	ashboard Teams	My Learning	Explore~	Search Cybrary		
Sandbox 🗸	Dashboard	People Pat	hs Goals Analy	tics Settings	Audit Log	
	Setti	inae				
	Team Loc	10		1	eam Em	ail Domains
				G	l.com	

SCIM Provisioner with S	SAML (SCIM v2 Core)	
Info Configuration	Enable SAML2.0 Sign on method SAML2.0	
Parameters	X.509 Certificate	
sso	Standard Strength Certificate (2048-bit) Change View Details	
Access	SAML Signature Algorithm	
Provisioning	Issuer URL	
Privileges	https://app.onelogin.com/saml/metadata/8e7263d3-7981-42c7-a12f-ac581d95502d	6
	SAML 2.0 Endpoint (HTTP) https://cybrary-dev.onelogin.com/trust/saml2/http-post/sso/8e7263d3-7981-42c7-a12f-ac581d95502	6

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.

~

in

f

14

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.

Λ

CYBZAZY

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-----).

C.509 Certificate	
Standard Strength Certificate (2048-bit)	
Change View Details	
X.509 Certificate	
K.509 Certificate	
BEGIN CERTIFICATE	6
MIID8jCCAtqgAwIBAgIUFeeo21j0xLHDAOo2y/wOP19J09swDQYJKoZIhvcNAQEF	
POANTDEVMPLICATILECON0021; cmEvoSP 1//CPMTEMVETATPON/PAcMDEQU7UV/721.	
BQAWIDEXMBOGATOECGWOQSTTCHIFYESBSYCBMTEMXFTATBGWYBASMDESUZOXYZZTU	
IElkUDEaMBgGA1UEAwwRT25lTG9naW4gQWNjb3VudCAwHhcNMjMwMjA3MTMwNDIØ	
IElkUDEaMBgGA1UEAwwRT25lTG9naW4gQWNjb3VudCAwHhcNMjMwMjA3MTMwNDI0 WhcNMjgwMjA3MTMwNDI0WjBMMRcwFQYDVQQKDA5DeWJyYXJ5IElUIExMQzEVMBMG	
IELKUDEaMBgGA1UEAwwRT25lTG9naW4gQWNjb3VudCAwHhcNMjMwMjA3MTMwNDIØ WhcNMjgwMjA3MTMwNDIØWjBMMRcwFQYDVQQKDA5DeWJyYXJ5IElUIExMQzEVMBMG A1UECwwMT25lTG9naW4gSWRQMRowGAYDVQQDDBFPbmVMb2dpbiBBY2NvdW5ØIDCC	
IElkUDEaMBgGA1UEAwwRT25lTG9naW4gQWNjb3VudCAwHhcNMjMwMjA3MTMwNDIØ WhcNMjgwMjA3MTMwNDIØWjBMMRcwFQYDVQQKDA5DeWJyYXJ5IElUIExMQzEVMBMG A1UECwwMT25lTG9naW4gSWRQMRowGAYDVQQDDBFPbmVMb2dpbiBBY2NvdW5ØIDCC ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALBzMzpz8jHQKvGu5uNXA2/d	

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

Identity Provider Signature Certificate *

-----BEGIN CERTIFICATE-----

MIID8jCCAtqgAwIBAgIUFeeo21jOxLHDAOo2y/wOP19J09swDQYJKoZlhvcNAQEF BQAwTDEXMBUGA1UECgwOQ3licmFyeSBJVCBMTEMxFTATBgNVBAsMDE9uZUxvZ2lu IElkUDEaMBgGA1UEAwwRT25ITG9naW4gQWNjb3VudCAwHhcNMjMwMjA3MTMwNDI0 WhcNMjgwMjA3MTMwNDI0WjBMMRcwFQYDVQQKDA5DeWJyYXJ5IEIUIExMQzEVMBMG

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

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

in

y

f

15

Submit

6

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

n't know where to get started with Single-Sign On? Talk to your IT team.	
dentity Provider Configuration	~
Service Provider Configuration	
Audience URI (Service Provider Entity ID)	
Audience URI (Service Provider Entity ID) highgarden_sp_id/saml.t_12773	Сору
Audience URI (Service Provider Entity ID) highgarden_sp_id/saml.t_12773 Single Sign-On URL (ACS Url)	Сору

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 w	ith SAML (SCIM v2 Core)
Info	Application details
Configuration	SAML Audience URL
Parameters	highgarden_sp_id/saml.t_12773
Rules	SAML Consumer URL
SSO	https://app.cybrary.it/auth/api/sso/saml.t_12773/saml2/acs

8

9

CYBRARY

🔹 in f

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 /

10

	API Connection	
Info	API Status	
Configuration	Disabled Enable	
Parameters	SCIM Base URL	
Rules	https://app.cybrary.it/auth/api/org/12773/scim/v2	
SSO	Custom Headers	
Access	1	
Provisioning		
Users		
Privileges		
	SCIM Bearer Token	

(11)

Save the OneLogin Application (top right).



Applications / SCIM Provisioner with	SAML (SCIM v2 Core)
Info	Application details
Parameters	highgarden_sp_id/saml.t_12773
Rules	SAML Consumer URL https://app.cybrary.it/auth/api/sso/saml.t_12773/saml2/acs
Access	
Users	API Status
Privileges	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 w	ith SAML (SCIM v2 Core)	
Info	Workflow	
Configuration	Enable provisioning	
Parameters	Require admin approval before t	this action is performed
Rules	Create user Delete user	
SSO	Update user	
Access	When users are deleted in One	neLogin, or the user's app access is removed, perform the below action
Provisioning	Delete	-
Users	When user accounts are susp	pended in OneLogin, perform the following action:
Privileges	Suspend	

12

Configure SAML 2.0 SSO for Azure

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

Manage	
🚨 Users	Search your
🚨 Groups	Basic inform
External Identities	
Roles and administrators	Name
Administrative units	Tenant ID
🚸 Delegated admin partners	Primary dom
Enterprise applications	License
Devices	

Select Create your own application.

+ Create	your own application
The Azure Al connect you request using	App Gallery is a catalog of thousands of apps that make users more securely to their apps. Browse or create your the process described in this article.

1

2

in f 19

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

R Got feedbad	k?		
If you are develop application that is	ing your own application, using Application Proxy, or want to in not in the gallery, you can create your own application here.	ntegrate :	
What's the name	of your app?		
Cybrary	✓		
What are you loo	ing to do with your application?		
Configure Apple Configure A	plication Proxy for secure remote access to an on-premises app	blication	
O Register an a	oplication to integrate with Azure AD (App you're developing)		
Integrate any	other application you don't find in the gallery (Non-gallery)		
u will be redi	ected to the Overview for your new application	n. Select Single sign-on in the le	əft
u will be redi	ected to the Overview for your new application rary Overview ise Application	n. Select Single sign-on in the l	eft
u will be redi	ected to the Overview for your new application rary Overview se Application	n. Select Single sign-on in the l	eft
u will be redi	ected to the Overview for your new application rary Overview se Application « ent Plan	n. Select Single sign-on in the l	əft
u will be redi U Verviev U Deploym	ected to the Overview for your new application rary Overview ise Application « ent Plan and solve problems	n. Select Single sign-on in the l	eft
u will be redi U Cyk Enterpo U Overview Deploym X Diagnose Manage	ected to the Overview for your new application rary Overview se Application « ent Plan and solve problems	n. Select Single sign-on in the le	eft
u will be redi	ected to the Overview for your new application rary Overview se Application « ent Plan and solve problems s	n. Select Single sign-on in the l	əft
u will be redi U Cyk Enterpo U Overview Deploym C Diagnose Manage II Propertie C Owners	ected to the Overview for your new application rary Overview se Application « ent Plan and solve problems s	n. Select Single sign-on in the la	eft
u will be redi	ected to the Overview for your new application rary Overview se Application « ent Plan and solve problems s administrators	n. Select Single sign-on in the le	eft

Y

in

f

20

3

4

CYBZAZY

Single sign-on

Provisioning

Disable Single si won't be My Apps	d gn-on is not enabled. Th able to launch the app f s.	e user írom	SAML Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.
oll down to the so s section contain en and open a ne	ection labeled Set s information you w tab/window .	up Cybrary (or the will need to copy o	name of the application you entered ver to the Cybrary app to enable SS(
	a dha ana liandian da Rul		
rou II need to configur	e the application to line	k with Azure AD.	tenling com (4th 1h 10h 0200 B
Azure AD Identifier		https://iogin.microso	rtonline.com/dtb1b49b-9200
Logout URL		https://login.microso	ftonline.com/dfb1b49b-9200
he new tab/wind CYBRARY	ow, log in to <u>https:</u>	//app.cybrary.it and	d click on Teams in the top navigatio
he new tab/wind CYBRARY	ow, log in to <u>https:</u>	//app.cybrary.it and	d click on Teams in the top navigation

6

7

Configure SAML 2.0 SSO for Azure

in f 21

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.



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).

Identity Provider Configuration	
Required fields are marked with an *	
Identity Provider (IdP) Issuer URI *	
https://sts.windows.net/dfb1b49b-9200-474e-a367-944e3bb302ee/	
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://login.microsoftonline.com/dfb1b49b-9200-474e-a367-944e3bb302ee/saml2	
The binding-specific IdP Authentication Request Protocol endpoint that receives SAML AuthnRequest messages.	

in

f

22

8

SAML Certificat	es		
Token signing o	ertificate		
Status		Active	6 Edit
lick New C o	ertificate. A new rov	v will appear. Click Save .	
SAML Sign	ing Certificate		×
Manage the certificate	used by Azure AD to sign SAML tokens is	ssued to your app	
Save + New	w Certificate 📅 Import Certificate	R Got feedback?	
Status	Expiration Date	Thumbprint	
Active	3/27/2026, 7:01:54 AM	B3016AAA114C38E5D1F9FE78273CE69F2CD3C364	
SAML Sign Manage the certificate	ing Certificate used by Azure AD to sign SAML tokens is v Certificate T Import Certificate	sued to your app ㈜ Got feedback?	×
SAML Sign Manage the certificate Save + New Status	ing Certificate used by Azure AD to sign SAML tokens is v Certificate T Import Certificate Expiration Date	sued to your app 쥿 Got feedback? Thumbprint	×
SAML Signi Manage the certificate Save + New Status Active	ing Certificate used by Azure AD to sign SAML tokens is v Certificate ↑ Import Certificate Expiration Date 3/27/2026, 7:01:54 AM	sued to your app P Got feedback? Thumbprint B3016AAA114C38E5D1F9FE78273CE69F2CD3C364	×
SAML Signi Manage the certificate Save + New Status Active n/a	ing Certificate used by Azure AD to sign SAML tokens is v Certificate	sued to your app P Got feedback? Thumbprint B3016AAA114C38E5D1F9FE78273CE69F2CD3C364 Will be displayed on save	×
SAML Signi Manage the certificate Save + New Status Active n/a Click the 3 d active. Click Active. You r his certifica	ing Certificate used by Azure AD to sign SAML tokens is v Certificate Expiration Date 3/27/2026, 7:01:54 AM 3/31/2026, 4:36:28 PM dots to the right of the Yes on the dialog wo may click the 3 dots te is not used.	sued to your app Got feedback? Thumbprint B3016AAA114C38ESD1F9FE78273CE69F2CD3C364 Will be displayed on save e new row (the one with Status I indow that appears to confirm. T of the old row (now Status Inacti	nactive). Click Make cert The new row will now have ve) and click Delete Cert
SAML Signi Manage the certificate Save + New Status Active n/a Click the 3 d ctive. Click Active. You r his certifica SAML Sign Manage the certificate Save + New	ing Certificate used by Azure AD to sign SAML tokens is v Certificate	sued to your app Got feedback? Thumbprint B3016AAA114C38E5D1F9FE78273CE69F2CD3C364 Will be displayed on save e new row (the one with Status I indow that appears to confirm. T of the old row (now Status Inacti sued to your app Got feedback?	nactive). Click Make cert The new row will now have ve) and click Delete Cert
SAML Signi Manage the certificate Save + New Status Active n/a Click the 3 d ctive. Click Active. You r his certificate SAML Sign Manage the certificate Save + New Status	ing Certificate used by Azure AD to sign SAML tokens is v Certificate Expiration Date 3/27/2026, 7:01:54 AM 3/31/2026, 4:36:28 PM dots to the right of the Yes on the dialog we may click the 3 dots te is not used. ing Certificate used by Azure AD to sign SAML tokens is w Certificate Import Certificate Expiration Date	sued to your app Free Got feedback? Thumbprint B3016AAA114C38E5D1F9FE78273CE69F2CD3C364 Will be displayed on save e new row (the one with Status I indow that appears to confirm. T of the old row (now Status Inactional) sued to your app Got feedback? Thumbprint	nactive). Click Make cert The new row will now have ve) and click Delete Cert
SAML Signi Manage the certificate Save + New Status Active n/a Click the 3 d ctive. Click Active. You r his certificate SAML Sign Manage the certificate Save + New Status Inactive	ing Certificate used by Azure AD to sign SAML tokens is v Certificate	sued to your app	nactive). Click Make cert The new row will now have ve) and click Delete Cert
SAML Signi Manage the certificate Save + New Status Active n/a Click the 3 d ctive. Click active. You r his certifica SAML Sign Manage the certificate Save + New Status Inactive Active	ing Certificate used by Azure AD to sign SAML tokens is v Certificate T Import Certificate 3/27/2026, 7:01:54 AM 3/31/2026, 4:36:28 PM Hots to the right of the Yes on the dialog we may click the 3 dots te is not used. ing Certificate used by Azure AD to sign SAML tokens is w Certificate Import Certificate Expiration Date 3/31/2026, 4:40:02 PM 3/31/2026, 4:39:28 PM	sued to your app	nactive). Click Make cert The new row will now have ve) and click Delete Cert

CYBRARY

y

Delete Certificate

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.

F8A23743D9CD47B6D1A1FC66799A	() Make certificate active
	o make certificate delive
	\downarrow Raw certificate download
	✓ Download federated certificate XML
	Delete Certificate

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

Identity Provider Signature Certificate *

-----BEGIN CERTIFICATE-----

MIIDBTCCAe2gAwIBAgIQGQ6YG6NIeJxJGDRAwAd/ZTANBgkqhkiG9w0BAQsFADAtMSswKQYDVQQD EyJhY2NvdW50cy5hY2NIc3Njb250cm9sLndpbmRvd3MubmV0MB4XDTIyMTAwMjE4MDY0OVoXDTI3 MTAwMjE4MDY0OVowLTErMCkGA1UEAxMiYWNjb3VudHMuYWNjZXNzY29udHJvbC53aW5kb3dzLm5I dDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALSS+Ig9iVLMS8jXsz0IdSes5+sEqAwI

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

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



16

17

🕑 🖸 in f 24

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.

ervice Provider Configuration	^
Audience URI (Service Provider Entity ID)	
highgarden_sp_id/saml.t_13091	Сору
Single Sign-On URL (ACS Url)	
https://app.cybrary.it/auth/api/sso/sami.t_13091/sami2/acs	Сору

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 a for help integrating Cybrary.

susie of the configuration		6 Edit
Identifier (Entity ID)	Required	
Reply URL (Assertion Consumer Service URL)	Required	
Sign on URL	Optional	
Relay State (Optional)	Optional	
Logout Url (Optional)	Optional	

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.

in

f

25

The unique ID that identifies your application to Azure Active Directory. This valu your Azure Active Directory tenant. The default identifier will be the audience of	ue must be unique acro f the SAML response foi	ss all application IDP-initiated S	ns in SO.
		Default	
hiskearden en id/samlt 13001			100
Add identifier Reply URL (Assertion Consumer Service URL) * ①] [] []	III
Add identifier Reply URL (Assertion Consumer Service URL) * ① The reply URL is where the application expects to receive the authentication toke Consumer Service" (ACS) in SAML.	✓ en. This is also referred	to as the "Asser	tion
Add identifier Reply URL (Assertion Consumer Service URL) * ① The reply URL is where the application expects to receive the authentication toke Consumer Service" (ACS) in SAML.	en. This is also referred	to as the "Asser Default	tion



19 [`]

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.

	Add user/group Add u
J Overview	
Deployment Plan	1 The application will appear for a
X Diagnose and solve problems	Assign users and groups to app releas
Manage	Assign users and groups to app-roles
Properties	$ \mathcal{P} $ First 200 shown, to search all use
Sources Sources	Display Name
8 Roles and administrators	No application assignments found
Licors and groups	

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**.

	🧉 🔚 Save 🗙 Discard
0 Overview	
Pa Provision on demand	Provisioning Mode
Managa	Automatic \checkmark
Provisioning	Use Azure AD to manage the creation and synchronization of user accounts in Cybrary based on user and group assignment.
Expression builder	
Monitor	∧ Admin Credentials
Provisioning logs	Admin Credentials
Audit logs	Azure AD needs the following information to connect to Cybrary's API and synchronize user data.
💡 Insights	Tenant URL * 🛈
Troubleshoot	
Rew support request	Secret Token

Configure SAML 2.0 SSO for Azure

f

in