

Odyssey Preservation Software

Configuration Guide for Single Sign-On (SSO) with Security Assertion Markup Language (SAML) 2.0

Contents

Introduction	1
Steps Common to All Identity Providers.....	2
Enable SAML Single Sign-On in Odyssey and Verify Your Email Domain.....	2
OneLogin	4
Microsoft Azure Active Directory (Azure AD)	11

Introduction

It is a best security practice to use single sign-on whenever possible to reduce the number of login credentials your users have to manage. Having multiple logins to different systems leads to dangerous password behavior, such as re-using passwords between systems. Single sign-on addresses this risk by having a single credential for an “identity provider” that allows access to multiple systems. Odyssey supports single sign-on using SAML 2.0.

Security Assertion Markup Language (“SAML”) is a protocol by which one information system can use a different system to identify valid users. Enabling SAML requires that you already have an Identity Provider (“IdP”) service, such as OneLogin or Microsoft Azure Active Directory.

These instructions address both OneLogin and Microsoft Azure AD. However, Odyssey will integrate with any Identity Provider that supports SAML 2.0. You may need to adapt the instructions below for your Identity Provider.

Steps Common to All Identity Providers

You must have account owner privileges in Odyssey to follow these steps. If you don't have account owner privileges, please request them from your current account owner.

You will also need to have access to the DNS records for your email domain. You will be adding a TXT record to confirm ownership of the domain.

Enable SAML Single Sign-On in Odyssey and Verify Your Email Domain

1. Navigate to **Administration > Single Sign-On**.
2. Toggle **Enable SAML for all users in your account** to ON.

Enable SAML for all users in your account.

3. Enter the email domain that is registered with your IdP. In our example, we use "brightpathbook.com."

Your email domain

Email domain*

brightpathbook.com

4. Click **Save** in the upper-right corner of the page. The page will reload, and you will see a yellow box asking you to verify ownership of the domain. Copy the value presented and create a new DNS TXT record for the root ("@") of your domain with the new value. (Consult with the documentation for your DNS hosting provider on how to do this. If you have existing TXT records on the domain root, pay particular attention to the DNS host's instructions for adding additional TXT records beyond the first.)
5. Wait a few minutes and refresh the SAML Setup page in Odyssey. Once the DNS change is detected, you will see a green box indicating that Odyssey has confirmed that you own the domain.

Email domain*

brightpathbook.com



You have verified ownership of **brightpathbook.com**. Please do NOT delete the DNS TXT record with the following value: **odyssey-**

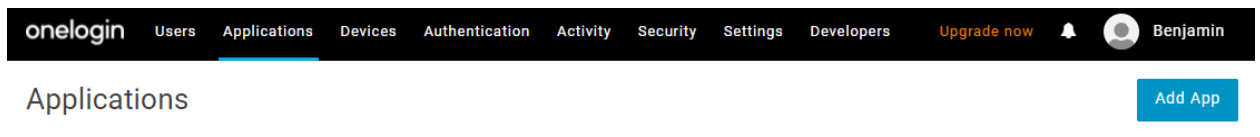
[REDACTED]

The next steps in the setup are different depending on your SAML 2.0 Identity Provider. In the following sections, we provide instructions for OneLogin and Microsoft Azure AD. If you use a different Identity Provider, please follow their setup instructions, using the values provided below. Most Identity Providers have a setup process that is similar to either OneLogin or Azure AD.

OneLogin

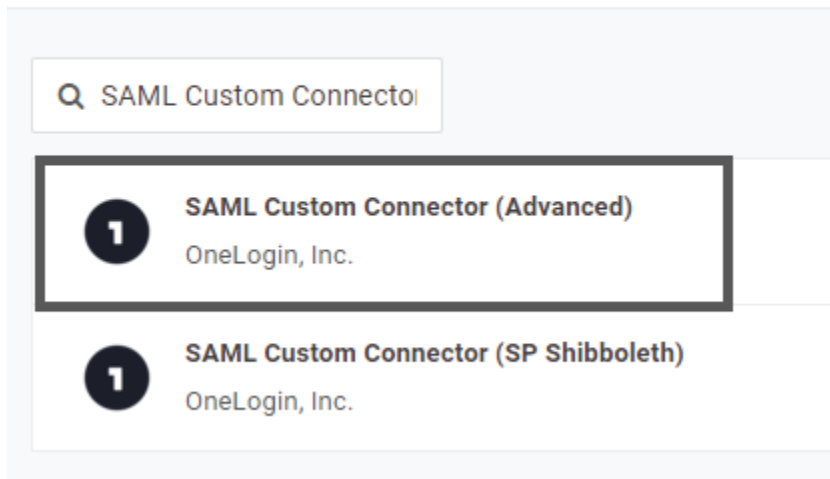
Before you begin, ensure that you have administrator privileges for your OneLogin account. Log in to OneLogin to start the setup process.

1. In Odyssey, navigate to **Administration > Single Sign-On**. Confirm that **Enable SAML for all users in your account** is set to ON, and that you have verified ownership of your email domain. If you haven't yet done this, follow the instructions in the "Steps Common to All Identity Providers," above.
2. In a new tab, log in to OneLogin. Navigate to the **Applications** section in OneLogin, and click **Add App**.



3. In the **Find Applications** screen, enter "SAML Custom Connector." From the results, click on "SAML Custom Connector (Advanced)."

Find Applications



4. Give the app a **Display Name**, such as “Odyssey Preservation Software.” You don’t need to change any other default values on this page. Click **Save** in the upper right.


App Listing / Add SAML Custom Connector (Advanced) Cancel **Save**

Configuration	Portal Display Name <input type="text" value="Odyssey Preservation Software"/>
----------------------	---


5. After the app is added, you will see additional choices on the left-hand side of the page. Choose **Parameters**.

Odyssey needs to know the first name and last name of each user. In the next steps, we’ll tell OneLogin which of its own directory values are the ‘first name’ and ‘last name’ to send to Odyssey in a SSO request.

Applications / SAML Custom Connector (Advanced)

Info Configuration Parameters Rules SSO Access Users Privileges Setup	Portal Display Name <input type="text" value="Odyssey Preservation Software"/> Visible in portal <input checked="" type="checkbox"/> Rectangular Icon 
---	--

6. Click the + icon to add a new parameter.

SAML Custom Connector (Advanced) Field	Value	
NameID value	Email	

7. For **Field name**, enter “givenname” (all lowercase, no quotes). Check **Include in SAML assertion**. Then click **Save**.

New Field

Field name

i This is the name of the field in the application's API

Flags

Include in SAML assertion

Multi-value parameter

[Cancel](#) [Save](#)

8. The panel will refresh in a different state, and you'll now see a **Value** drop-down menu. Choose **First Name** from this menu, and click **Save** again.

Edit Field givenname

Name
givenname

Value
- No default -

Q |

Email name part

External ID

First Name

First initial

Internal ID

Last Name

9. Confirm that “givenname” appears in your list of parameters, with the value First Name.

SAML Custom Connector (Advanced) Field	Value	
NameID value	Email	
givenname	First Name	custom parameter

10. Repeat this process adding the parameter “surname” and mapping it to the Last Name choice in the Value menu. When you’re done, your parameters screen should look like this:

SAML Custom Connector (Advanced) Field	Value	
NameID value	Email	
givenname	First Name	custom parameter
surname	Last Name	custom parameter

11. Now, from the left-hand navigation, choose **SSO**.

onelogin Users Applications Devices Authentication Activity Security Settings

Applications /
SAML Custom Connector (Advanced)

Info

- Configuration
- Parameters
- Rules
- SSO**
- Access
- Users
- Privileges
- Setup

Portal

Display Name

Odyssey Preservation Software

Visible in portal

Rectangular Icon

i Upload an icon with an aspect-ratio of 2.64:1 as

12. Copy the **Issuer URL** from OneLogin. (In some other Identity Providers, this is called “Federation Metadata URL” or “Federation Metadata XML.”)

Issuer URL

<https://app.onelogin.com/saml/metadata/2bdae07f-258d-4bb3-a2f4-d957d0206138>

13. Switch to Odyssey, and paste this into the Federation Metadata URL field.

Federation Metadata URL

`https://app.onelogin.com/saml/metadata/2bdae07f-258d-4bb3-a2f4-d957d0206138`

Import Values

Then click Import Values. The page will reload, and all the other SAML fields will be filled in. Don't make any other changes to these values. You don't need to click "Save" a second time; setup is now complete.

Values from your Identity Provider

Your SAML Identity Provider must *provide* the following values.

Federation Metadata URL

`https://app.onelogin.com/saml/metadata/2bdae07f-258d-4bb3-a2f4-d957d0206138`

Import Values

Entity ID / Issuer URL

`https://app.onelogin.com/saml/metadata/2bdae07f-258d-4bb3-a2f4-d957d0206138`

SAML 2.0 Endpoint

`https://birney-consulting-dev.onelogin.com/trust/saml2/http-redirect/sso/2bdae07f-258d-4bb3-a2f4-d957d0206138`

Single Logout Endpoint

`https://birney-consulting-dev.onelogin.com/trust/saml2/http-redirect/sso/2bdae07f-258d-4bb3-a2f4-d957d0206138`

X.509 Certificate

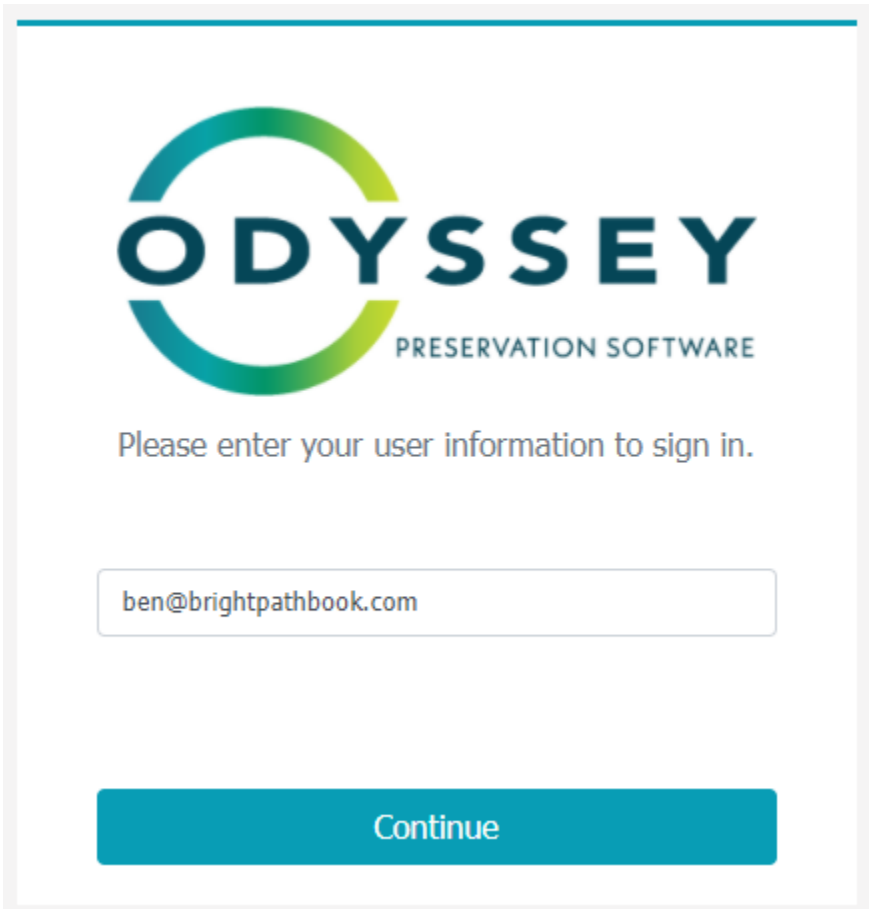
```
MIIECDCCAvCgAwIBAgIUO6ExGYNnVZO1YBb9Jz7dA13pKhkwDQYJKoZIhvcNAQEF
BQAwwGQGA1UECgVQmlybmV5IENvbnN1bHRpbmV5IENvbnN1bHRpbmV5IENvbnN1
bmVMb2dpbiBJZFAxGjAYBgNVBAMMEU9uZUxvZ2luIEFjY291bnQgMB4XDTEyMDEx
NjEwMTY1M1oXDTI3MDExNjEwMTY1M1owUzEeMBwGA1UECgVQmlybmV5IENvbnN1
bHRpbmV5IENvbnN1bHRpbmV5IENvbnN1bHRpbmV5IENvbnN1bHRpbmV5IENvbnN1
ZG90eSB0b2dpbiBJZFAxGjAYBgNVBAMMEU9uZUxvZ2luIEFjY291bnQgMB4XDTEy
```

What if that didn't work? *Only* fill in the other fields manually if the Federation Metadata URL fails to load one of them. The values for these fields can be found in the **SSO** screen in OneLogin.

14. In the OneLogin tab, click on the **Access** section for your app. Select the OneLogin Roles that should have access to Odyssey. If you are using a default OneLogin setup, then there is a single role called "Default." All users have this Role. In this setup, all OneLogin users have access to Odyssey. If this is not how you want to grant access, then create a new Role for Odyssey and

assign it on the Access screen.

15. Now we'll test your access. In an Incognito/Private Browsing/InPrivate window (depending on what your web browser calls it), navigate to odyssey.historyit.com. On the login screen, enter the email address associated your OneLogin account. Then click Continue.



ODYSSEY
PRESERVATION SOFTWARE

Please enter your user information to sign in.

ben@brightpathbook.com

Continue

16. You will be redirected to the OneLogin login experience. After authenticating with OneLogin, you should be redirected back to the dashboard associated with your Odyssey account. (You may need to accept Odyssey's terms and conditions, if no user with your OneLogin email address has previously logged in to Odyssey.)

Setup is now complete. Inform your users of the change to their login experience.

Microsoft Azure Active Directory (Azure AD)

Before you begin, ensure you have Global Admin rights on your Azure tenant.

1. Sign in to Odyssey and navigate to Administration > Single Sign-on. Confirm that **Enable SAML for all users in your account** is set to ON, and that you have verified ownership of your email domain. If you haven't yet done this, follow the instructions in the "Steps Common to All Identity Providers," above.
2. In a new tab, sign in to the Azure portal. Navigate to **Home > Azure Active Directory > Groups**. Create a user group for all users who will have access to Odyssey. Use the "Security" group type. Add the users to the group, and make sure it has an owner (you). In these instructions, the group will be called "Odyssey Users."

New Group ...

Group type * ⓘ
Security

Group name * ⓘ
Odyssey Users

Group description ⓘ
Enter a description for the group

Azure AD roles can be assigned to the group ⓘ
Yes No

Membership type * ⓘ
Assigned

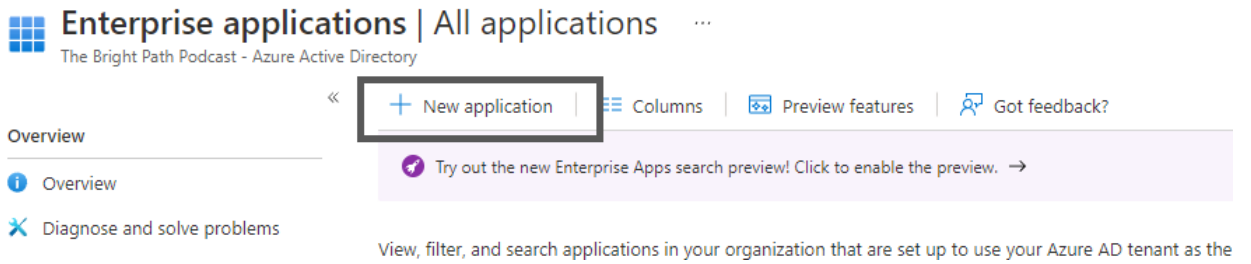
Owners
1 owner selected

Members
2 members selected

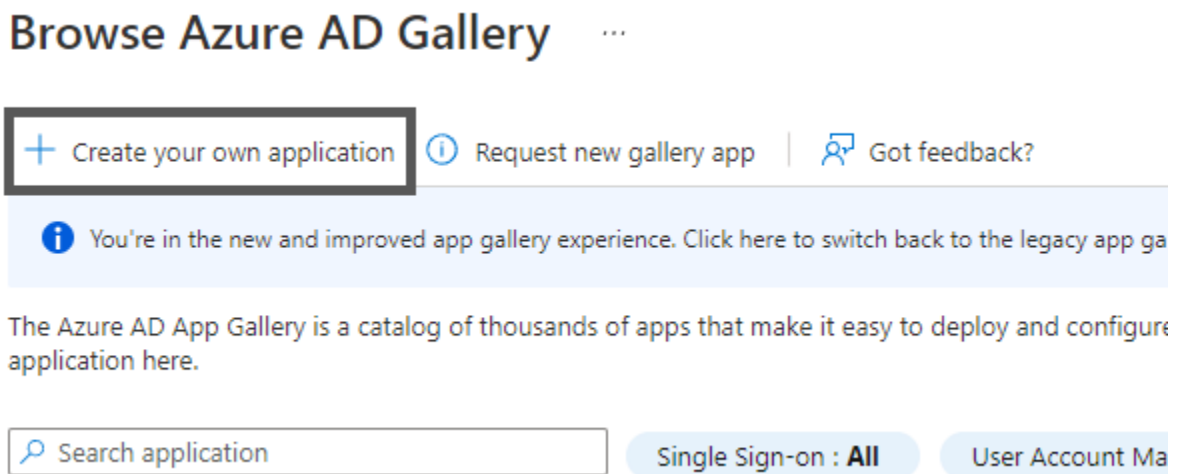
Don't forget to click **Create** at the bottom to finish creating your group. Refresh the groups index page to confirm your new group exists.

3. Navigate to **Home > Azure Active Directory > Enterprise applications**. (Do not go to the similarly-named "App registrations.")

4. Click **New Application**.




5. Click **Create your own application**.



6. Give the application a name, such as “Odyssey Preservation Software.” Check **Integrate any other application you don’t find in the gallery (Non-gallery)**.

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?

Odyssey Preservation Software ✓

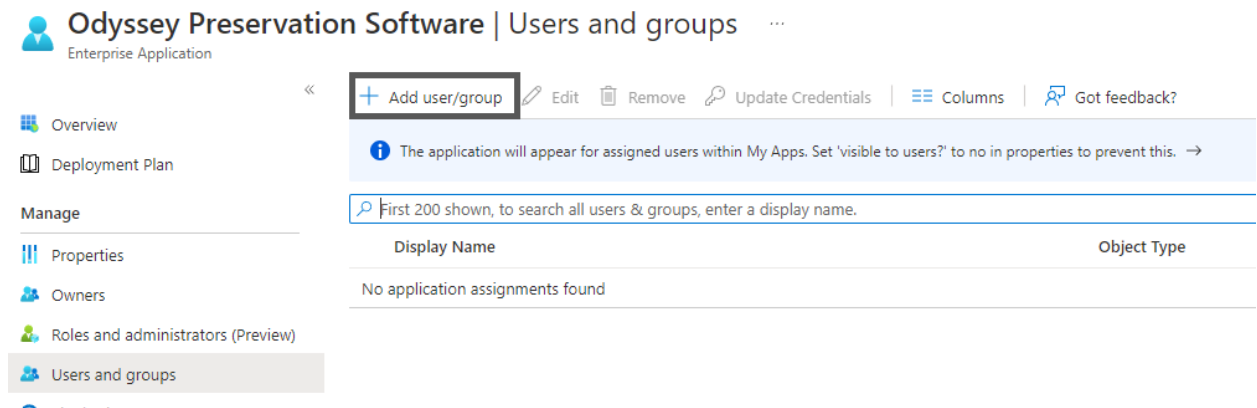
What are you looking to do with your application?

- 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)

Now click the **Create** button at the bottom of the panel.

If Azure gives you a “not found” or other error message after creating your app, navigate back to the Enterprise Applications screen, wait a minute or two, and refresh the page. Your new app should appear in the list after a short period of time. Click on the app title to go to the app settings screen for the next step.






7. From the **Overview** screen for the app, click **Assign users and groups**. (Alternatively, you can click **Users and groups** from the left-hand navigation.) Click **Add user/group**.





Odyssey Preservation Software | Users and groups ...

Enterprise Application

- Overview
- Deployment Plan
- Manage
 - Properties
 - Owners
 - Roles and administrators (Preview)
 - Users and groups**

« **+ Add user/group**   Remove  Update Credentials |  Columns |  Got feedback?

 The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this. →

 First 200 shown, to search all users & groups, enter a display name.

Display Name	Object Type
No application assignments found	

- Under **Add assignment**, click **None Selected** beneath **Users and groups**.

[Home](#) > [Odyssey Preservation Software](#) >

Add Assignment

The Bright Path Podcast

Users and groups

None Selected

Select a role

User

- In the right-hand panel, find the Odyssey Users group, and click on it. Then click **Select** at the bottom. Finally, click **Assign** in the lower right.

The screenshot shows the Microsoft Azure portal interface. The main content area displays the 'Add Assignment' page for 'The Bright Path Podcast'. A warning message is visible: 'When you assign a group to an application, only users directly in the group will be assigned. This does not cascade to nested groups.' Below this, the 'Users and groups' section shows '1 group selected.' and a 'Select a role' dropdown menu with 'User' selected. A right-hand panel titled 'Users and groups' is open, showing a search bar with 'Odyssey Users' and a list of results. The 'Odyssey Users' group is highlighted with a '1' and a 'Selected' status. Below the list, the 'Selected items' section shows 'OU Odyssey Users' with a 'Remove' button. At the bottom of the main content area, the 'Assign' button is highlighted with a '3' and the 'Select' button is highlighted with a '2'. The URL bar at the bottom shows 'https://portal.azure.com/#'.

10. Now click **Single sign-on** from the left-hand menu.

Odyssey Preservation Software | Users and groups ...
Enterprise Application

Overview
Deployment Plan

Manage

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

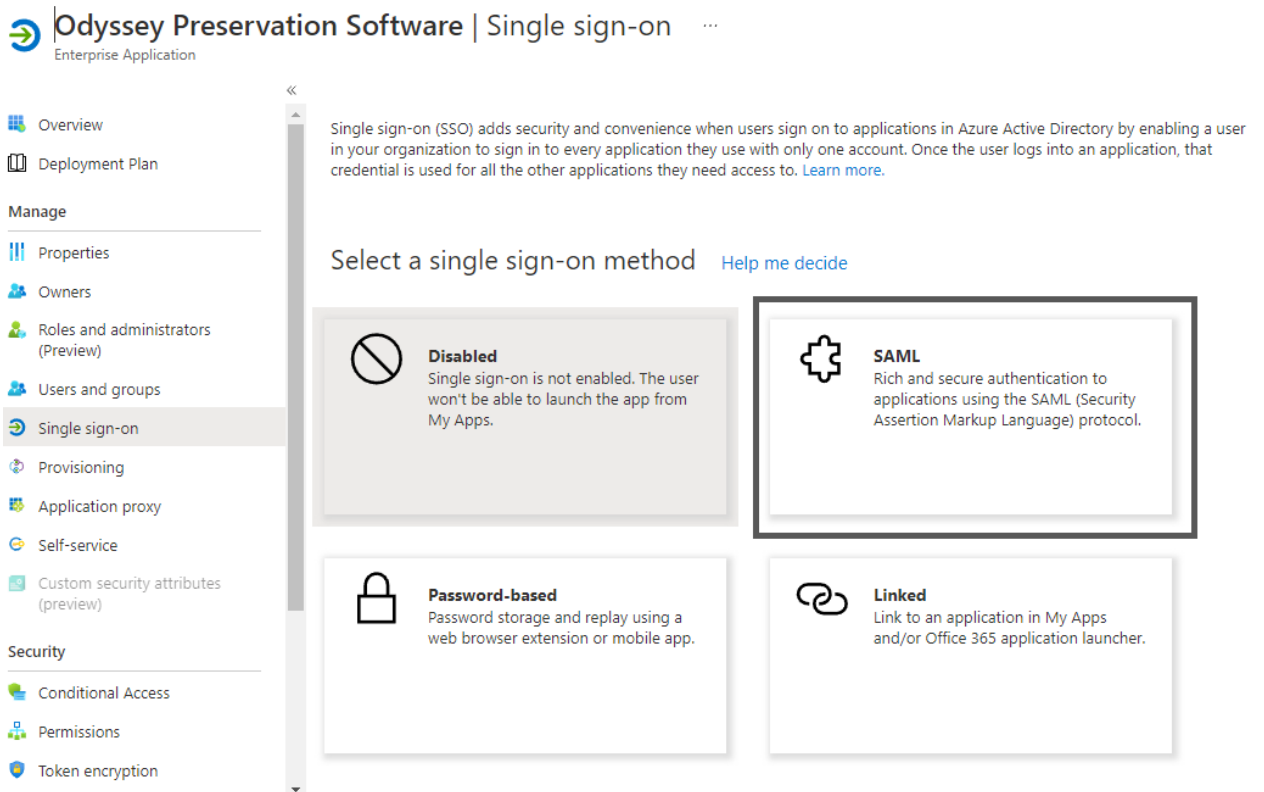
+ Add user/group Edit Remove Update Credentials

The application will appear for assigned users within My Apps. Set

First 200 shown, to search all users & groups, enter a display name

Display Name	Object Type
<input type="checkbox"/> OU Odyssey Users	Group

11. Under **Select a single sign-on method**, click **SAML**.



12. In the section labeled **Basic SAML Configuration**, click the Edit pencil.

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 Odyssey Preservation Software.

1

Basic SAML Configuration		Edit
Identifier (Entity ID)	Required	
Reply URL (Assertion Consumer Service URL)	Required	
Sign on URL	Optional	
Relay State	Optional	
Logout Url	Optional	

13. In the following steps, we will be copying and pasting values from the Odyssey **SAML Setup** screen. You will need to switch between your Odyssey and Azure AD tabs.

14. For the **Identifier (Entity ID)** field in Azure, copy the value in Odyssey's field labeled **Audience** (aka "Identifier" or "Entity ID"). Set this as the default, and click the **Delete** icon for the existing default entity ID.

Odyssey

Audience (aka "Identifier" or "Entity ID")

https://odyssey-dev-lb.historyit.com/users/saml-audience/5b08054c361162.23293524



Azure AD

Identifier (Entity ID) * ⓘ

The default identifier will be the audience of the SAML response for IDP-initiated SSO

Default

http://adapplicationregistry.onmicrosoft.com/customappssso/primary	<input checked="" type="checkbox"/>	ⓘ	🗑️
https://odyssey-dev-lb.historyit.com/users/saml-audience/5b08054c361162.23293524	<input type="checkbox"/>	ⓘ	🗑️



Default

https://odyssey-dev-lb.historyit.com/users/saml-audience/5b08054c361162.23293524	<input checked="" type="checkbox"/>	ⓘ	🗑️
--	-------------------------------------	---	----

15. For the **Reply URL (Assertion Consumer Service URL)** field in Azure, copy the value in Odyssey's field labeled **Assertion Consumer Service URL** (aka "ACS URL" or "Reply URL").

Odyssey

Assertion Consumer Service URL (aka "ACS URL" or "Reply URL")

https://odyssey-dev-lb.historyit.com/users/saml-consume-assertion/5b08054c361162.23293524



Azure AD

Reply URL (Assertion Consumer Service URL) * ⓘ

The default reply URL will be the destination in the SAML response for IDP-initiated SSO

Default

https://odyssey-dev-lb.historyit.com/users/saml-consume-assertion/5b08054c361162.23293524	<input checked="" type="checkbox"/>	ⓘ	🗑️
---	-------------------------------------	---	----

16. For the **Sign on URL** field in Azure, copy the value in Odyssey's field labeled **Sign on URL**.

Odyssey

Sign on URL

https://odyssey-dev-lb.historyit.com/users/login



Azure AD

Sign on URL ⓘ

https://odyssey-dev-lb.historyit.com/users/login ✓

17. Leave **Relay State** blank in Azure.

18. For the **Logout URL** field in Azure, copy the value in Odyssey's field labeled **Single Logout URL**.

Odyssey

Single Logout URL

https://odyssey-dev-lb.historyit.com/users/saml-single-logout/5b08054c361162.23293524



Azure AD

Logout Url ⓘ

https://odyssey-dev-lb.historyit.com/users/saml-single-logout/5b08054c361162.23293524 ✓

19. At the top of the **Basic SAML Configuration** screen (where you have been entering all these values), click **Save**.

Basic SAML Configuration



Got feedback?

20. Click the **X** button to close the Basic SAML Configuration panel. If Azure prompts you to test your SSO configuration, click **I'll do this later**. Your Basic SAML Configuration summary should now look similar to this:

1

Basic SAML Configuration Edit

Identifier (Entity ID)	https://odyssey-dev-lb.historyit.com/users/saml-audience/5b08054c361162.23293524
Reply URL (Assertion Consumer Service URL)	https://odyssey-dev-lb.historyit.com/users/saml-consume-assertion/5b08054c361162.23293524
Sign on URL	https://odyssey-dev-lb.historyit.com/users/login
Relay State	Optional
Logout Url	https://odyssey-dev-lb.historyit.com/users/saml-single-logout/5b08054c361162.23293524

21. Ensure that the **Attributes & Claims** section matches the following picture. At the time of this writing, these are the defaults for a new SAML-based Sign-On app in Azure AD, and these defaults are correct.

In particular, Odyssey expects the SAML Name ID to be the user's email address, which is almost always the Azure AD principal name. It also expects the first name and last name to be transmitted as "givenname" and "surname" respectively.


2


Attributes & Claims Edit

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

22. Scroll down to the **SAML Signing Certificate** section, and look for **App Federation Metadata URL**. Click the copy icon to the right of this value.

3

SAML Signing Certificate  Edit

Status	Active
Thumbprint	088C4C5F7AE060D51E09E785D96D1A3641774F83
Expiration	1/23/2025, 7:01:33 AM
Notification Email	ben@brightpathbook.com
App Federation Metadata Url	https://login.microsoftonline.com/29f7431b-4dd7... 
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

23. Switch to your Odyssey tab and paste this value into **Federation Metadata URL**. Then click the **Import Values** button.

Values from your Identity Provider

Your SAML Identity Provider must *provide* the following values.

Federation Metadata URL

ederationmetadata/2007-06/federationmetadata.xml?appid=ffa2f940-18bd-484c-8553-12b1a6d2168

Import Values

The page will reload, and all the other SAML fields will be filled in. Don't make any other changes to these values. You don't need to click "Save" a second time; setup is now complete.

Values from your Identity Provider

Your SAML Identity Provider must *provide* the following values.

Federation Metadata URL

https://login.microsoftonline.com/29f7431b-4dd7-4959-aaa0-44b7b0bbe463/federationmetadata/2007

Import Values

Entity ID / Issuer URL

https://sts.windows.net/29f7431b-4dd7-4959-aaa0-44b7b0bbe463/

SAML 2.0 Endpoint

https://login.microsoftonline.com/29f7431b-4dd7-4959-aaa0-44b7b0bbe463/saml2

Single Logout Endpoint

https://login.microsoftonline.com/29f7431b-4dd7-4959-aaa0-44b7b0bbe463/saml2

X.509 Certificate

```
MIIC8DCCAdigAwIBAgIQTLx FbqfDTK1ICqs z7LwVTDANBgkqhkiG9w0BAQsFADA0MTIwMAYDVQQDEYlNaWNyb3NvZnQgQXp1cmUgRmVkdXJhdGVkIFNTTyBDZXJ0aWZpY2F0ZTAeFw0yMjAxMjMxMjAxMzFwNTAxMjMxMjAxMzNaMDQxMjAwBgNVBAMTKU1pY3Jvc29mdCBBenVybSBGZWRIcmF0ZWQgU1NPIENlcnRpZmljYXRIMllBljANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvgTjdb2Cgf2TjBOC2bY3mvf/T2q+Xdyq5eEXNn6BK3unrjsmc0I3zvyHOMyNHM+CLL/IFGBIguz6ei8AieTGUomeI29vBLSII5LY4khTjzflb7nrXlxfjBI5HHI2S8z9PfAxPR7OYpfVK
```

24. **What if that didn't work?** *Only* fill in the other fields manually if the Federation Metadata URL fails to load one of them. The values for these fields can be in the panel labeled **Set up [name of your app]**.

4

Set up Odyssey Preservation Software

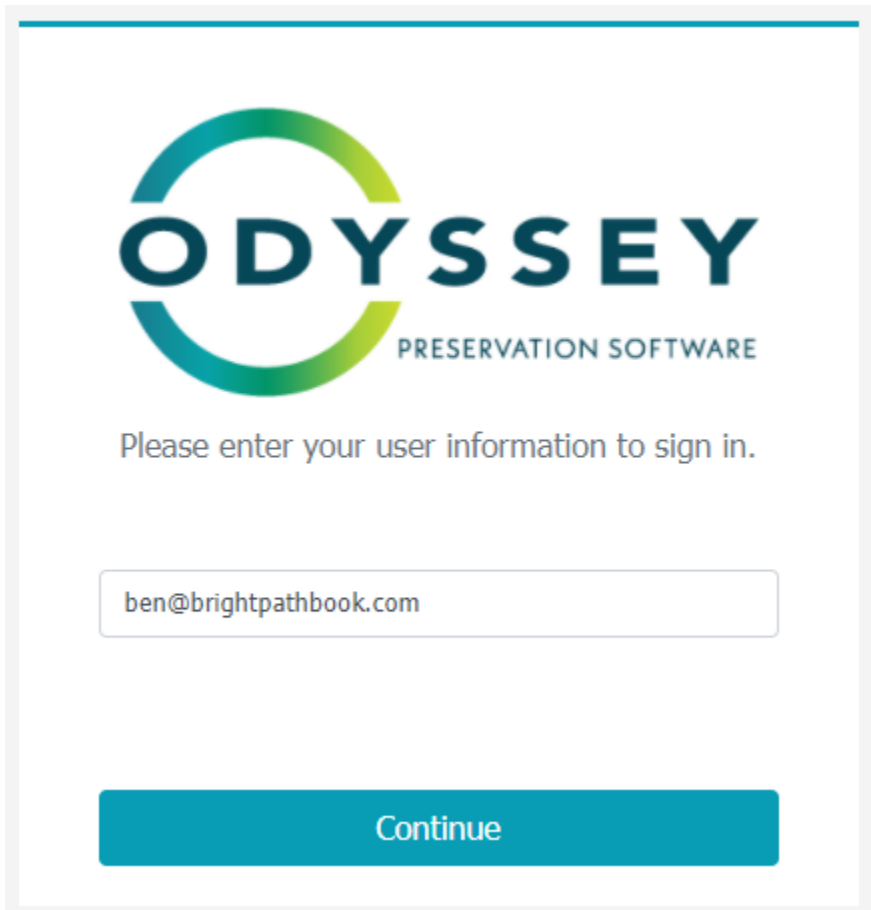
You'll need to configure the application to link with Azure AD.

Login URL	<code>https://login.microsoftonline.com/29f7431b-4dd7...</code>
Azure AD Identifier	<code>https://sts.windows.net/29f7431b-4dd7-4959-aaa...</code>
Logout URL	<code>https://login.microsoftonline.com/29f7431b-4dd7...</code>

[View step-by-step instructions](#)

Copy and paste these into the similarly-named fields in Odyssey. (The **Azure AD Identifier** goes in the **Entity ID** field.)

25. Now we'll test your access. In an Incognito/Private Browsing/InPrivate window (depending on what your web browser calls it), navigate to odyssey.historyit.com. On the login screen, enter the email address associated with your Azure AD identity. Then click Continue.



26. You will be redirected to the Azure AD login experience. After authenticating with Azure AD, you should be redirected back to the dashboard associated with your Odyssey account. (You may need to accept Odyssey's terms and conditions, if no user with your Azure AD email address has previously logged in to Odyssey.)

Setup is now complete. Inform your users of the change to their login experience.