

Azure Active Directory

1. Go to the Enterprise applications gallery:

https://portal.azure.com/#blade/Microsoft_AAD_IAM/StartboardApplicationsMenuBlade/AllApps


You can search for “Enterprise applications” in the search bar if that URL doesn’t take you there.

2. Click “New application”. It will take you to a panel like the one below:


Categories / Add an application

Add an application


Add your own app

 Application you're developing

Register an app you're working on to integrate it with Azure AD

 On-premises application









Configure Azure AD Application Proxy to enable secure remote access.

 Non-gallery application

Integrate any other application that you don't find in the gallery

Add from the gallery

Featured applications

 Box	 Concur	 Cornerstone O...	 DocuSign
 Dropbox for B...	 G Suite	 GitHub.com	 GoToMeeting

3. Click "Non-gallery application", and enter the application name, and click "Add" at the bottom of the screen.



Add your own application



Non-gallery application

Integrate any other application that you don't find in the gallery



e O...



Docusign



GoToMeeting



lou...



Netsuite

* Name

Netlify SAML

Once you decide on a name for your new application, click the "Add" button below and we'll walk you through some simple configuration steps to get the application working.

Supports:

SAML-based single sign-on

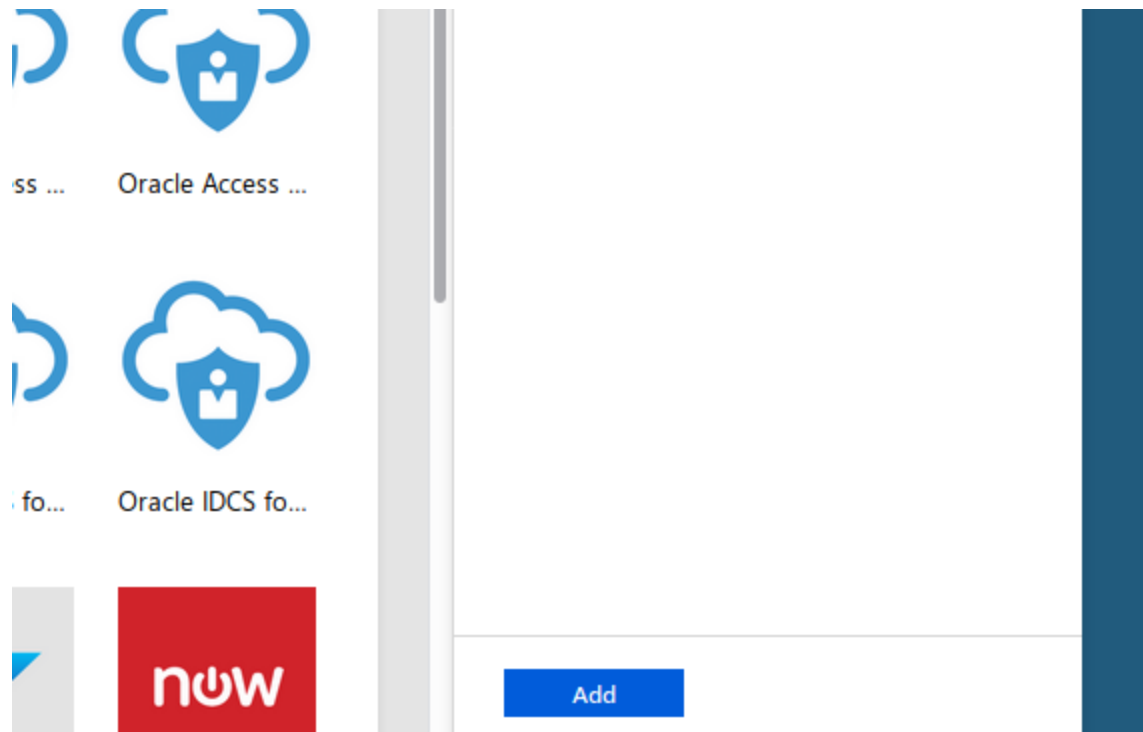
[Learn more](#)

Automatic User Provisioning with SCIM

[Learn more](#)

Password-based single sign-on

[Learn more](#)



If you're not paying for enterprise applications, it will let you start a trial. Click the option that says "Enterprise...", NOT the option that says "Mobile...".

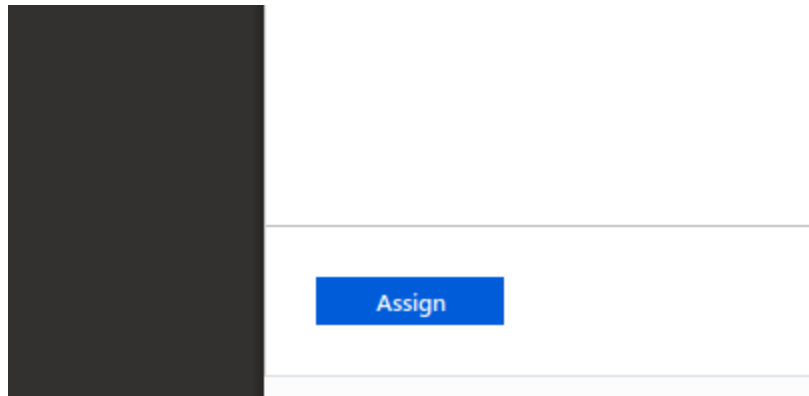
4. Click on "Assign a user for testing". This will let you choose one of your users in Azure to test the connection between Azure and Netlify.



Assign a user for testing (required)

Choose a single user account under your control to test single sign-on to Netlify SAML.

5. Click "Add user" in the top left corner and search for the user you want to test with. DO NOT FORGET to click "Assign" in the bottom left corner after selecting the user.



6. Go back to "Getting started" by using the breadcrumb menu at the top.
7. Click "Create your test user":



Create your test user in Netlify SAML (required)

You can create this user in Netlify SAML manually, or use Azure AD to provision user accounts automatically for supported apps.

8. After a few seconds with the message "Provisioning", it will show you a select box with two options, "Manual" and "Automatic". Choose "Manual" and go back to the getting started menu.
9. Click "Configure single sign-on":



Configure single sign-on (required)

Configure your instance of Netlify SAML to use Azure AD as its identity provider.

10. Click on "SAML":

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

Disabled

User must manually enter their username and password.



SAML

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



Password-based

Password storage and replacement via web browser extension or mobile app.

Linked

Link to an application in the Azure Active Directory Access Panel and/or Office 365 application launcher.

11. Click in the pencil icon to change "Basic SAML Configuration":

Set up Single Sign-On with SAML

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

1

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

2

User Attributes & Claims		
--------------------------	--	--

Those two required fields come from your Netlify Team settings, you can find them following a URL similar to this for your team:

<https://app.netlify.com/teams/YOUR-TEAM-SLUG-HERE/settings/profile#single-sign-on>

For example:

<https://app.netlify.com/teams/calavera-enterprise-inc/settings/profile#single-sign-on>

Single sign-on

You will need this information to configure SAML support for Netlify in your identity provider.

Entity ID:	https://api.netlify.com/saml/calavera-enterprise-inc
Login URL:	https://api.netlify.com/saml/calavera-enterprise-inc/init
ACS URL:	https://api.netlify.com/saml/calavera-enterprise-inc/acs

[Configure SAML](#)

Copy “Entity ID” and “ACS URL” into the configuration in Azure and click “Save” in the top:

Basic SAML Configuration

[Save](#)

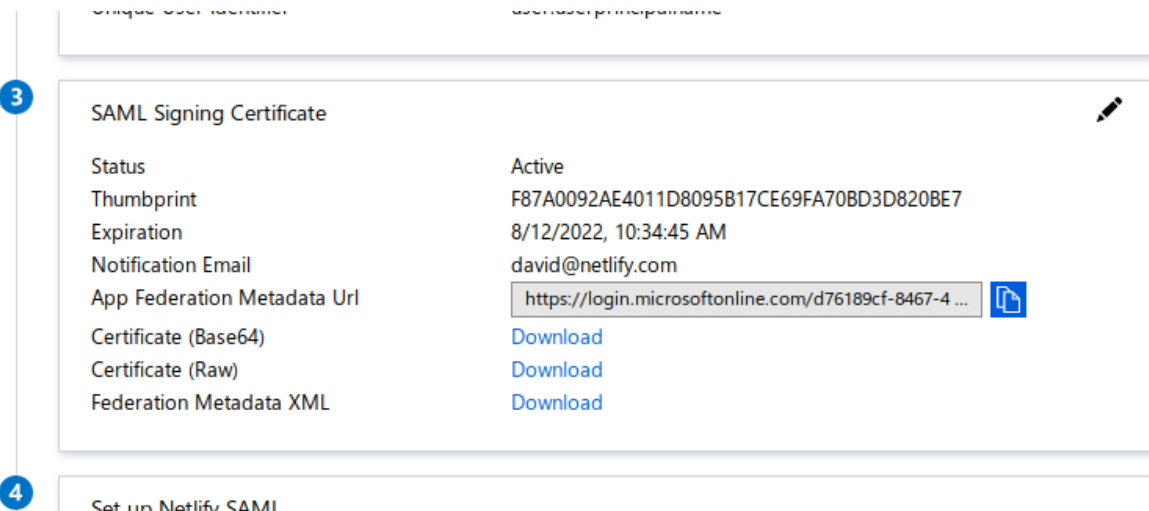
* Identifier (Entity ID) ⓘ
The default identifier will be the audience of the SAML response for IDP-initiated SSO

Default
 ✓ ⓘ 🗑

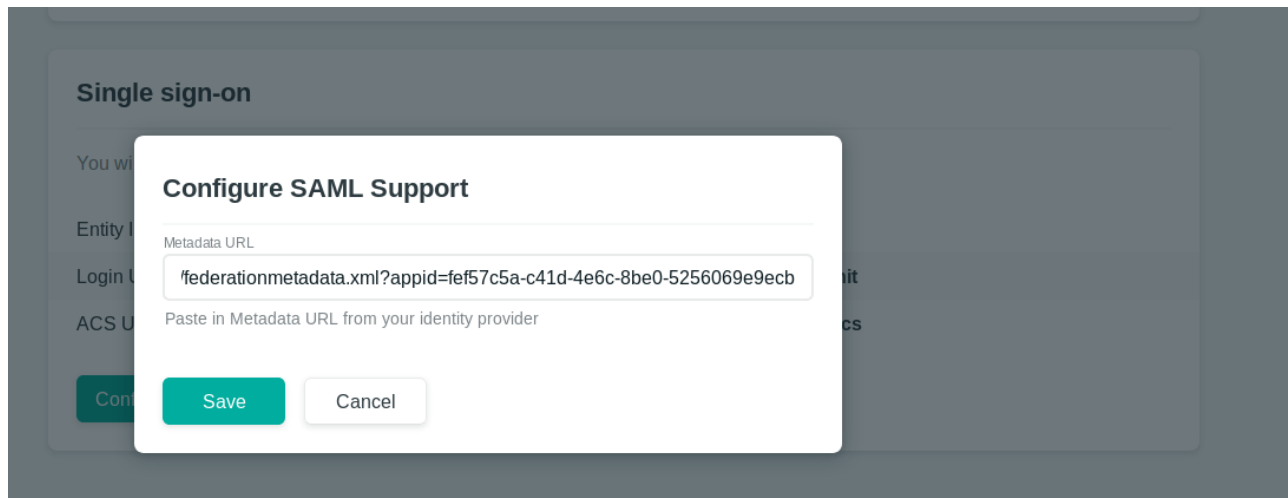
* Reply URL (Assertion Consumer Service URL) ⓘ
The default reply URL will be the destination in the SAML response for IDP-initiated SSO

Default
 ✓ ⓘ 🗑




12. Copy the “App Federation Metadata URL” from section 3 in “SAML Signing Certificate”:



13. Go to your team settings in app.netlify.com and introduce that URL in the SAML configuration:



14. Go back to Azure and click "Validate" in step 5, you'll be able to validate with the testing user you added in step 4:

Login URL	https://login.microsoftonline.com/d76189cf-8467-4 ...	
Azure AD Identifier	https://sts.windows.net/d76189cf-8467-4ab0-b0d6- ...	
Logout URL	https://login.microsoftonline.com/common/wsfede...	

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

5 Validate single sign-on with Netlify SAML

Validate to see if single sign-on is working. Users will need to be added to Users and groups before they can sign in.

[Validate](#)

If the configuration is correct, you should be redirected to Netlify's dashboard and be logged in with your user.