

SAML Help Doc

Google G Suite

To configure Netlify with Google G Suite:

1. In Google G Suite Admin, select **Apps**.



Apps

Manage apps and their settings

2. Select **SAML apps**.



0

SAML apps

Manage SSO and User Provisioning

3. Click the + in the lower right.



4. Select **SETUP MY OWN CUSTOM APP**.

Step 1

✕

Enable SSO for SAML Application

Select an service/App for which you want to setup SSO

Services	Provisioning supported	
Aha		>
Amazon Web Services		>
Asana	✓	>
Atlassian Cloud		>
BambooHR		>
BlueJeans		>
Box	✓	>

SETUP MY OWN CUSTOM APP

- Under **Option 2**, select **Download** to download your Google G Suite IdP metadata. You will need to host this XML file publicly so that Netlify can access it. A good place to host it is on one of your sites deployed by Netlify.

Select **NEXT**.

Step 2 of 5



Google IdP Information

Choose from either option to setup Google as your identity provider. Please add details in the SSO config for the service provider. [Learn more](#)

Option 1

SSO URL [https://accounts.google.com/o/saml2/idp?idpid=\[redacted\]](https://accounts.google.com/o/saml2/idp?idpid=[redacted])

Entity ID [https://accounts.google.com/o/saml2?idpid=\[redacted\]](https://accounts.google.com/o/saml2?idpid=[redacted])

Certificate **Google_2022-11-13-63037_SAML2.0**

Expires Nov 13, 2022

 **DOWNLOAD**

OR

Option 2

IDP metadata  **DOWNLOAD**

PREVIOUS

CANCEL

NEXT

- In **Basic information for your Custom App**:
 - Application Name**: Enter **Netlify**.

Select **NEXT**.

Step 3 of 5



Basic information for your Custom App

Please provide the basic information needed to configure your Custom App. This information will be viewed by end-users of the application.

Application Name * app-id: netlify

Description

Upload logo

 **CHOOSE FILE**

This logo will be displayed for all users who have access to this application. Please upload a .png or .gif image of size 256 x 256 pixels.

[PREVIOUS](#)

[CANCEL](#)

[NEXT](#)

7. In **Service Provider Details**:

- a. **ACS URL**: Enter your **ACS URL** from **Netlify > Team settings > SAML support**.
- b. **Entity ID**: Enter your **Entity ID** from **Netlify > Team settings > SAML support**.
- c. **Start URL**: Enter your **Login URL** from **Netlify > Team settings > SAML support**.

Select **Next**.

Step 4 of 5



Service Provider Details

Please provide service provider details to configure SSO for your Custom App. The ACS url and Entity ID are mandatory.

ACS URL *	<input type="text" value="https://app.netlify.com/saml/[YOUR TEAM SLUG]/ac"/>	
Entity ID *	<input type="text" value="https://app.netlify.com/saml/[YOUR TEAM SLUG]"/>	
Start URL	<input type="text" value="https://app.netlify.com/saml/[YOUR TEAM SLUG]/ini"/>	
Signed Response	<input type="checkbox"/>	
Name ID	<input type="text" value="Basic Information"/>	<input type="text" value="Primary Email"/>
Name ID Format	<input type="text" value="UNSPECIFIED"/>	

PREVIOUS

CANCEL

NEXT

SAML support

Entity ID:	https://app.netlify.com/saml/
ACS URL:	https://app.netlify.com/saml/acs
Login URL:	https://app.netlify.com/saml/init

[Learn more about SAML support →](#)

[Configure SAML support](#)

8. In **Attribute Mapping**:

Add mappings for **FirstName** and **LastName** as shown in the screenshot.

Select **Finish**.

Step 5 of 5



Attribute Mapping

Provide mappings between service provider attributes to available user profile fields.

FirstName Basic Information ▼ First Name ▼

LastName Basic Information ▼ Last Name ▼

ADD NEW MAPPING

PREVIOUS

CANCEL FINISH

9. Select **OK**.

Setting up SSO for Netlify



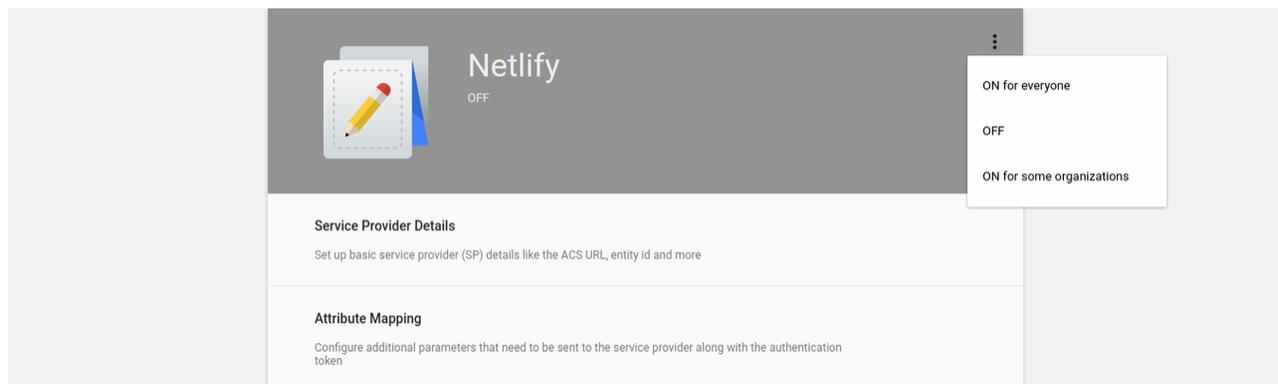
- ✓ Application details saved
- ✓ Mandatory attribute mapping successfully configured



You'll need to upload Google IDP data on Netlify administration panel to complete SAML configuration process

OK

10. Select **On for everyone** to turn the Netlify SAML app on for everyone in your organization.



11. On your Netlify Team Settings page, click the **Configure SAML Support** button under the **SAML Support** section.

Configure SAML support

12. Paste the URL of the XML file you downloaded in Step 5 and are now hosting publicly into the **Configure SAML Support** input.

Click **Save**.

Configure SAML Support

Paste in Metadata URL from your identity provider

Save Cancel

Okta

To configure Netlify with Okta:

1. In Okta Admin, select **Add Application**.

- Add Application
- Assign Applications
- Register OAuth Service

Q Search...

STATUS	
ACTIVE	0
INACTIVE	0

0110111
0011011
1100110
1000110
1000011
0100101
1011100
1100111

No active apps found

Add application and assign access to have them appear on your users' Okta home Page

2. Select **Create New App**.

Can't find an app?

Create New App

Apps you created(0) →

INTEGRATION PROPERTIES

Any

Supports SAML

Supports Provisioning

CATEGORIES

All	5573
CRM	146
CRM, Sales, Marketing	152
Collaboration	768
Consumer	209
Content Management	184
Data & Analysis	313
E-Commerce	52
ERP	65
Education	220
Finance & Accounting	529
HCM	314
Health & Benefits	201
Marketing	291
News & Research	99
Okta Applications	34
Okta Test Applications	12

Productivity	242
Security	202
Social	204
Software Development	551
Supply Chain	29
System & Network	261
Telecommunications	136
Travel & Transportation	186
Web Design & Hosting	173

3. In **Create a New Application integration**:

- a. **Platform**: Select **Web**.
- b. **Sign on method**: Select **SAML 2.0**.

Select **Create**.

Create a New Application Integration ✕

Platform

Sign on method

Secure Web Authentication (SWA)
Uses credentials to sign in. This integration works with most apps.

SAML 2.0
Uses the SAML protocol to log users into the app. This is a better option than SWA, if the app supports it.

OpenID Connect
Uses the OpenID Connect protocol to log users into an app you've built.

4. In **General Settings**:
- a. **App Name**: Enter **Netlify**.

Select **Next**.

Create SAML Integration

1 General Settings 2 Configure SAML 3 Feedback

1 General Settings

App name

App logo (optional) 

App visibility Do not display application icon to users
 Do not display application icon in the Okta Mobile app

5. In **Configure SAML**:

- a. **Single sign on URL**: Enter your **ACS URL** from **Netlify > Team settings > SAML support**.
- b. **Audience URI (SP Entity ID)**: Enter your **Entity ID** from **Netlify > Team settings > SAML support**.

In **ATTRIBUTE STATEMENTS**:

Add mappings for **FirstName** and **LastName** as depicted in the screenshot.

Select **Next**.

Create SAML Integration

1 General Settings 2 **Configure SAML** 3 Feedback

A SAML Settings

GENERAL

Single sign on URL ?
 Use this for Recipient URL and Destination URL
 Allow this app to request other SSO URLs

Audience URI (SP Entity ID) ?

Default RelayState ?
If no value is set, a blank RelayState is sent

Name ID format ?

Application username ?

[Show Advanced Settings](#)

ATTRIBUTE STATEMENTS (OPTIONAL) [LEARN MORE](#)

Name	Name format (optional)	Value	
<input type="text" value="FirstName"/>	<input type="text" value="Unspecified"/>	<input type="text" value="user.firstName"/>	×
<input type="text" value="LastName"/>	<input type="text" value="Unspecified"/>	<input type="text" value="user.lastName"/>	×

GROUP ATTRIBUTE STATEMENTS (OPTIONAL)

Name	Name format (optional)	Filter	
<input type="text"/>	<input type="text" value="Unspecified"/>	<input type="text" value="Starts with"/>	×

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.

Okta Certificate

Import the Okta certificate to your Identity Provider if required.

B Preview the SAML assertion generated from the information above

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

ATTRIBUTE STATEMENTS (OPTIONAL)

[LEARN MORE](#)

Name	Name format (optional)	Value	
<input type="text" value="FirstName"/>	<input type="text" value="Unspecified"/> ▼	<input type="text" value="user.firstName"/> ▼	×
<input type="text" value="LastName"/>	<input type="text" value="Unspecified"/> ▼	<input type="text" value="user.lastName"/> ▼	×
<input type="button" value="Add Another"/>			

SAML support

Entity ID: <https://app.netlify.com/saml/>

ACS URL: <https://app.netlify.com/saml/acs>

Login URL: <https://app.netlify.com/saml/init>

[Learn more about SAML support →](#)

7. In Feedback:

- Are you a customer or partner?:** Select **I'm an Okta customer adding an internal app.**
- App type:** Select **This is an internal app that we have created.**

Select **Finish.**

Create SAML Integration

1 General Settings 2 Configure SAML 3 Feedback

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

i The optional questions below assist Okta Support in understanding your app integration.

App type **?** This is an internal app that we have created

Why are you asking me this?

This form provides Okta Support with useful background information about your app. Thank you for your help—we appreciate it.

Previous

Finish

8. Copy the URL from the **Identity Provider metadata** link.

SAML 2.0 is not configured until you complete the setup instructions.

[View Setup Instructions](#)

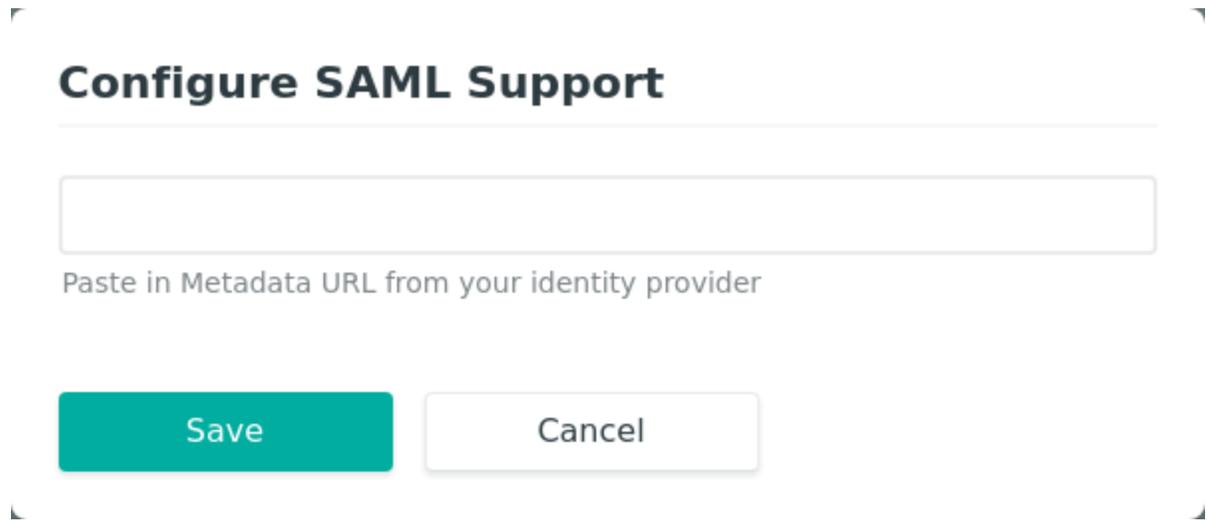
[Identity Provider metadata](#) is available if this application supports dynamic configuration.

9. On your Netlify Team Settings page, click the **Configure SAML Support** button under the **SAML Support** section.

Configure SAML support

10. Paste the URL copied in Step 8 into the **Configure SAML Support** input.

Click **Save**.



Configure SAML Support

Paste in Metadata URL from your identity provider

Save **Cancel**

OneLogin

To configure Netlify with OneLogin:

1. In OneLogin Admin, under **Apps**, select **Add App**.

Company Apps

ADD APP

🔍 search company apps...

2. Search for **SAML Test Connector (IdP w/attr)**. Select the app.

Find Applications

Q SAML Test Connector (IdP)

1

SAML Test Connector (IdP w/attr)
OneLogin, Inc.

SAML2.0

3. In Configuration:

- a. **Display Name:** Enter **Netlify**.

Select **Save**.

← Add SAML Test Connector (IdP w/at...

CANCEL **SAVE**

Configuration

Portal

Display Name

Netlify

Visible in portal



Rectangular Icon



Upload an icon with an aspect-ratio of 2.6:1 as either a transparent .PNG or .SVG

Square Icon



Upload a square icon at least 512x512px as either a transparent .PNG or .SVG

4. In Configuration:

- a. **Audience:** Enter your **Entity ID** from **Netlify > Team settings > SAML support**.
- b. **ACS (Consumer) URL Validator:** Enter **https://app.netlify.com/saml/YOUR TEAM SLUG/acs** replacing YOUR TEAM SLUG with your actual team slug.
- c. **ACS (Consumer) URL:** Enter your **ACS URL** from **Netlify > Team settings > SAML support**.

Select **Save**.

Application Details

RelayState

Audience

Recipient

ACS (Consumer) URL Validator*

*Required. Regular expression - Validates the ACS URL when initiated by an AuthnRequest

ACS (Consumer) URL*

*Required

Single Logout URL

SAML support

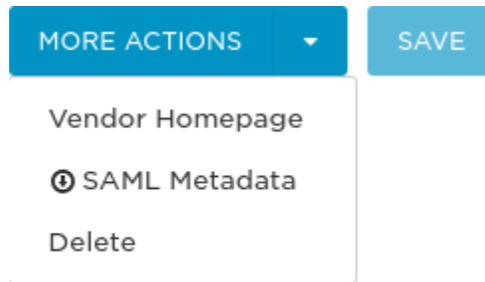
Entity ID:	https://app.netlify.com/saml/[REDACTED]
ACS URL:	https://app.netlify.com/saml/[REDACTED]acs
Login URL:	https://app.netlify.com/saml/[REDACTED]init

[Learn more about SAML support →](#)

Configure SAML support

5. Hover over the **More Actions** button and select **SAML Metadata** to download your OneLogin IdP metadata. You will need to host this XML file publicly so that

Netlify can access it. A good place to host it is on one of your sites deployed by Netlify.



6. On your Netlify Team Settings page, click the **Configure SAML Support** button under the **SAML Support** section.

Configure SAML support

7. Paste the URL of the XML file you downloaded in Step 5 and are now hosting publicly into the **Configure SAML Support** input.

Click **Save**.

Configure SAML Support

Paste in Metadata URL from your identity provider

Save

Cancel

Ping Identity PingOne

To configure Netlify with Ping Identity PingOne:

1. In Ping Identity admin, click the **Add Application** button.

Add Application ▾

2. Select **New SAML Application**.

Search Application Catalog

New SAML Application

Request Ping Identity add a new application to the application catalog

3. In **Application Details**:

- a. **Application Name:** Enter **Netlify**.
- b. **Application Description:** Enter a description
- c. **Category:** Select a category

Select **Continue to Next Step**.

Application Name	Type	Status	Enabled
New Application	SAML	Incomplete	<input type="checkbox"/> No

1. Application Details

Application Name *

Application Description *
Max 500 characters

Category *

Graphics

Application Icon
For use on the dock



Max Size: 256px x 256px

NEXT: Application Configuration

- 4. In **Application Configuration:**
 - a. Select **I have the SAML configuration**
 - b. **Assertion Consumer Service (ACS):** Enter your **ACS URL** from **Netlify > Team settings > SAML support**.
 - c. **Entity ID:** Enter your **Entity ID** from **Netlify > Team settings > SAML support**.

Select **Continue to Next Step**.

Application Name	Type	Status	Enabled
New Application	SAML	Incomplete	<input type="checkbox"/> No

2. Application Configuration

I have the SAML configuration
 I have the SSO URL

You will need to download this SAML metadata to configure the application:

Signing Certificate

SAML Metadata [Download](#)

Provide SAML details about the application you are connecting to:

Protocol Version SAML v 2.0 SAML v 1.1

Upload Metadata [Or use URL](#)

Assertion Consumer Service (ACS)

Entity ID

Application URL

Single Logout Endpoint

Single Logout Response Endpoint

Single Logout Binding Type Redirect Post

Primary Verification Certificate No file chosen

Secondary Verification Certificate No file chosen

Signing Algorithm

Force Re-authentication

Keep the following in mind when creating your connection:

1. Both SP- and IdP-Initiated SSO are allowed
2. Map SAML_SUBJECT in your attribute contract, plus any attributes (configure them in PingOne later)
3. Allow outbound POST or redirect
4. Allow outbound POST

NEXT: SSO Attribute Mapping

SAML support

Entity ID: <https://app.netlify.com/saml/>
ACS URL: <https://app.netlify.com/saml/acs>
Login URL: <https://app.netlify.com/saml/init>

[Learn more about SAML support →](#)

Configure SAML support

5. In SSO Attribute Mapping:

Add mappings for **FirstName** and **LastName** as shown in the screenshot.

Select **Save & Publish**.

Application Name	Type	Status	Enabled
New Application	SAML	Incomplete	<input type="checkbox"/> No

3. SSO Attribute Mapping

Map the necessary application provider (AP) attributes to attributes used by your identity provider (IdP).

	Application Attribute	Identity Bridge Attribute or Literal Value	As Literal	Advanced	Required	
1	<input type="text" value="FirstName"/>	<input type="text" value="First Name"/>	<input type="checkbox"/>	<input type="button" value="Advanced"/>	<input type="checkbox"/>	<input type="button" value="X"/>
2	<input type="text" value="LastName"/>	<input type="text" value="Last Name"/>	<input type="checkbox"/>	<input type="button" value="Advanced"/>	<input type="checkbox"/>	<input type="button" value="X"/>

NEXT: Review Setup

6. In Review Setup

- a. Select the **Download** link to the right of **SAML Metadata** to download your PingOne IdP metadata. You will need to host this XML file publicly so that Netlify can access it. A good place to host it is on one of your sites deployed by Netlify.

Select **Finish**.

Application Name	Type	Status	Enabled
New Application	SAML	Incomplete	<input type="checkbox"/> No

4. Review Setup

Test your connection to the application

Icon

Name Netlify

Description Netlify SSO

Category Other

Connection ID `cedefe45-4c2c-4210-aa61-059bbfe3ac43`

(Optional) Click the link below to invite this SaaS Application's Administrator to register their SaaS Application with PingOne.
[Invite SAAS Admin](#)

These parameters may be needed to configure your connection

saasid `857f003f-2a82-42e1-9cf8-30d9b59f68c2`

idpid `2b64168a-4505-4a11-8a4e-d161b22dbed2`

Protocol Version `SAML v 2.0`

ACS URL `https://8c55af3e.ngrok.io/saml/foo/acs`

entityId `https://8c55af3e.ngrok.io/saml/foo`

Initiate Single Sign-On (SSO) URL `https://sso.connect.pingidentity.com/sso/sp/initssso?saasid=857f003f-2a82-42e1-9cf8-30d9b59f68c2&idpid=2b64168a-4505-4a11-8a4e-d161b22dbed2`

Single Sign-On (SSO) Relay State `https://pingone.com/1.0/857f003f-2a82-42e1-9cf8-30d9b59f68c2`

Signing Certificate [Download](#)

SAML Metadata [Download](#)

Single Logout Endpoint

Single Logout Response Endpoint

Signing Algorithm `RSA_SHA256`

Force Re-authentication false

Click the link below to open the Single Sign-On page:
[Single Sign-On](#)

7. On your Netlify Team Settings page, click the **Configure SAML Support** button under the **SAML Support** section.

Configure SAML support

8. Paste the URL of the XML file you downloaded in Step 6 and are now hosting publicly into the **Configure SAML Support** input.

Click **Save**.

Configure SAML Support

Paste in Metadata URL from your identity provider

Save Cancel

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

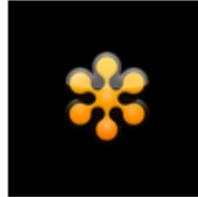
Configure Azure AD Application Proxy to enable secure remote access.

 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

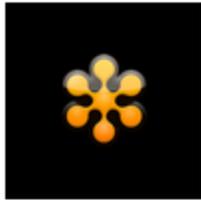
Integrate any other application that you don't find in the gallery



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

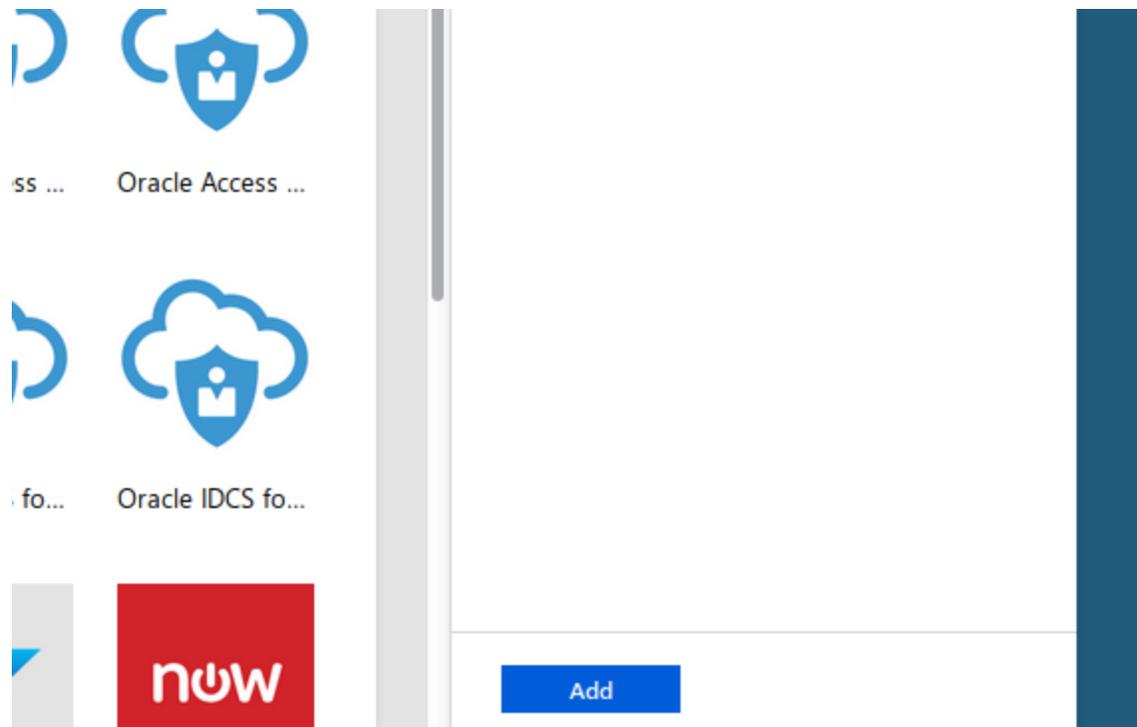
[Learn more](#)

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...".

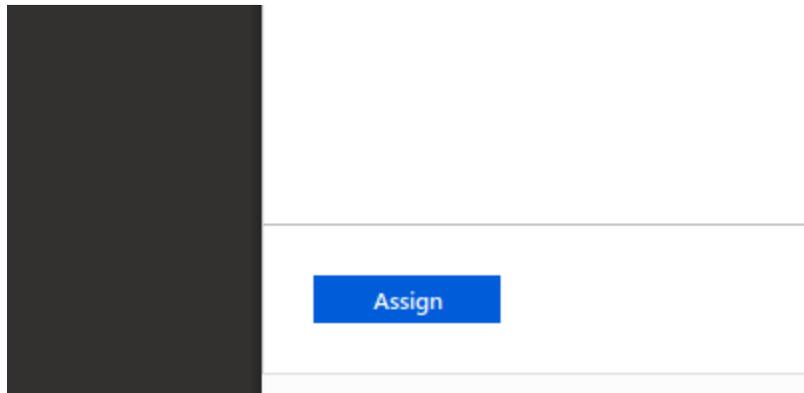
4. Click on "Assign a user for testing". This will let you choose one of your users in Azure to test the connection between Azure and Netlify.



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](#)

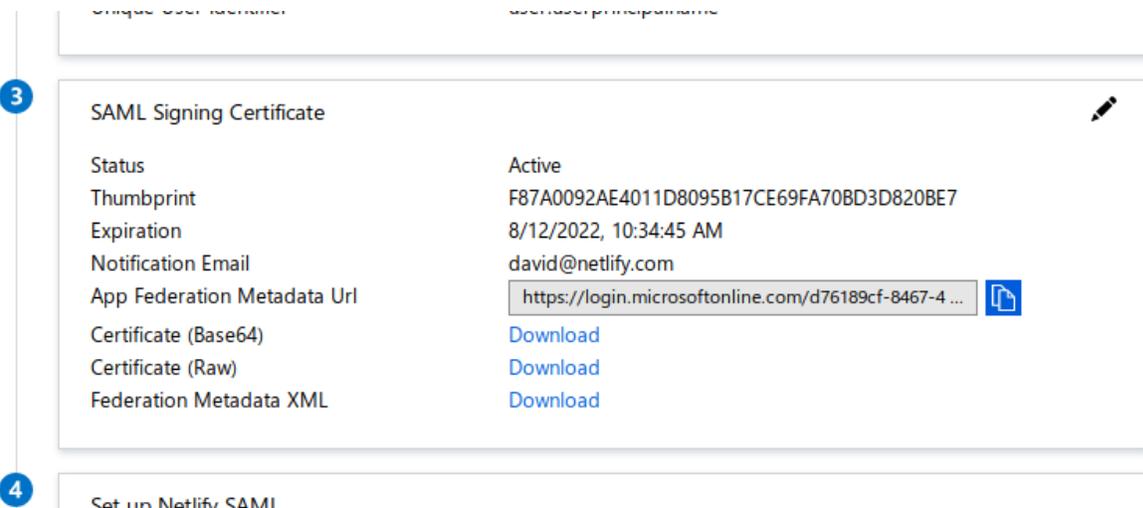
* Identifier (Entity ID) ⓘ
The default identifier will be the audience of the SAML response for IDP-initiated SSO

Default

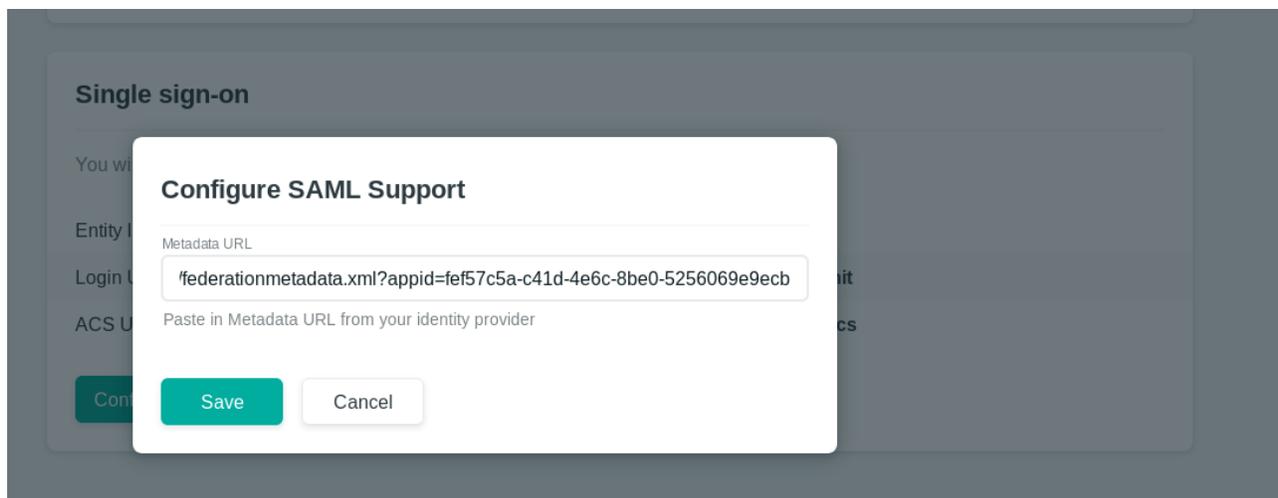
* Reply URL (Assertion Consumer Service URL) ⓘ
The default reply URL will be the destination in the SAML response for IDP-initiated SSO

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.

Other Provider

Most SAML 2.0 compliant identity providers require the same information from the service provider (Netlify in this case) for setup/configuration. These values are specific to your Netlify Team and are available from the **SAML Support** section in the **Team Settings** of the Netlify Team where you want to enable SAML.

Identity Provider Value	Netlify Value
ACS/SSO URL	ACS URL
Entity ID/Audience	Entity ID
Login/Start URL	Login URL

You will also need to provide Netlify with your Identity Provider’s metadata XML which should be publicly accessible online by either your Identity Provider or on one of your own sites.