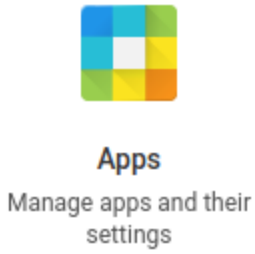
SAML Help Doc

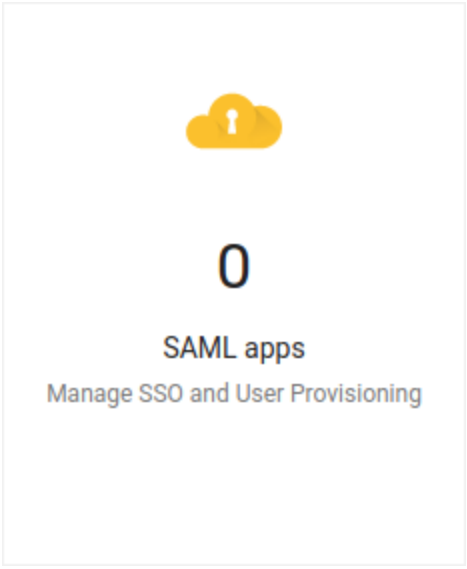
Google G Suite

To configure Netlify with Google G Suite:

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

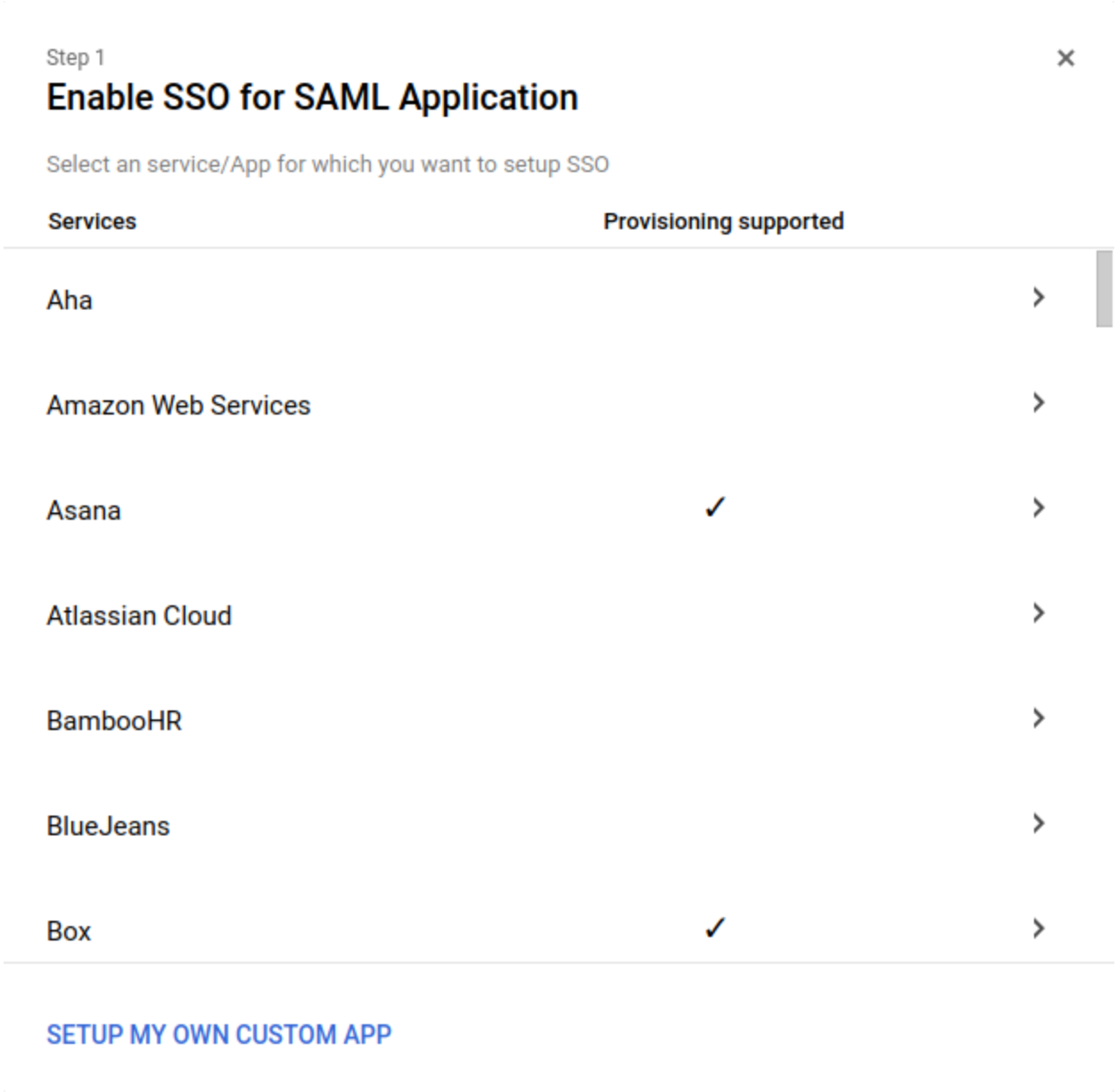


2. Select **SAML apps.**



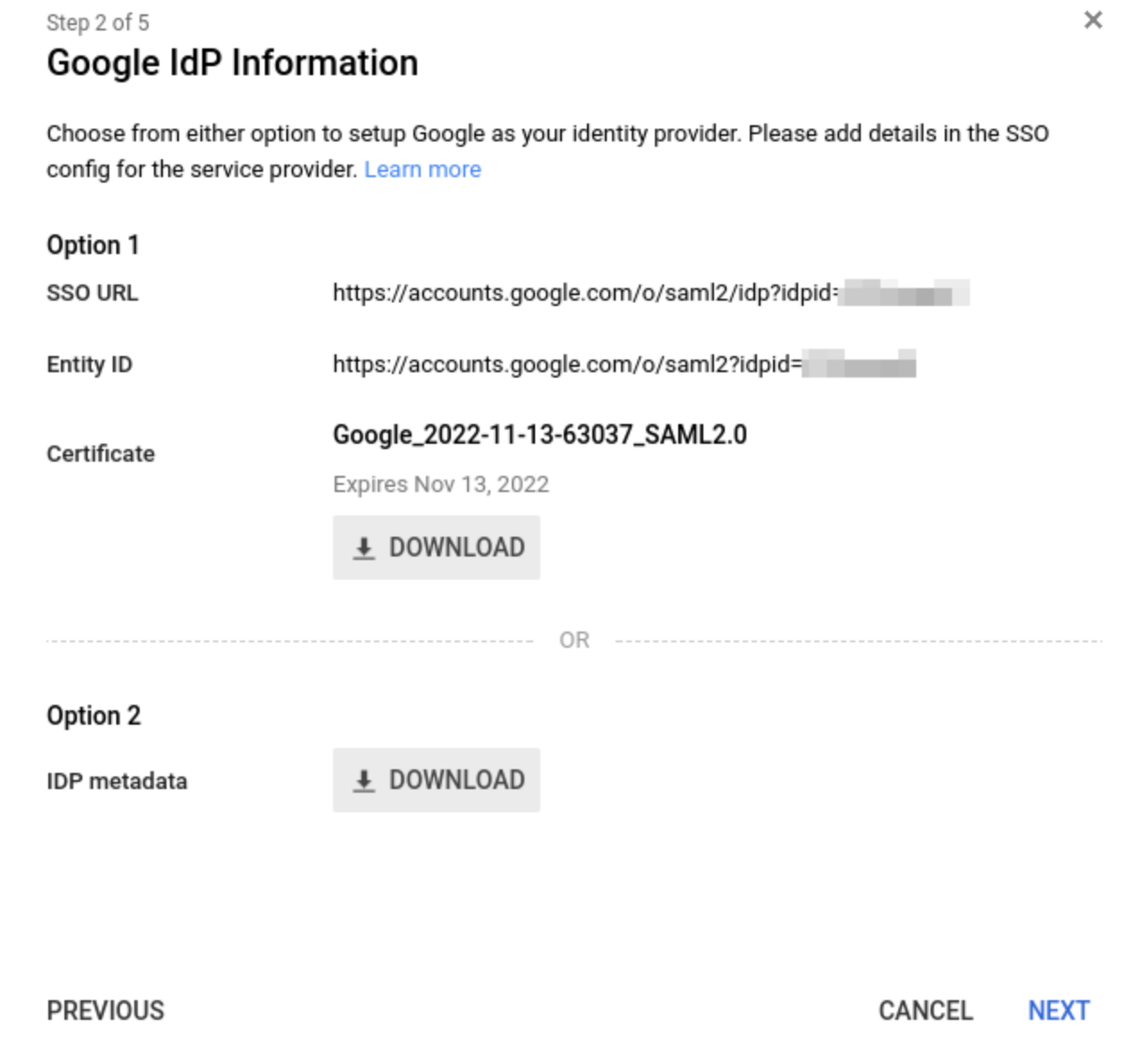
3. Click the **+** in the lower right.

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



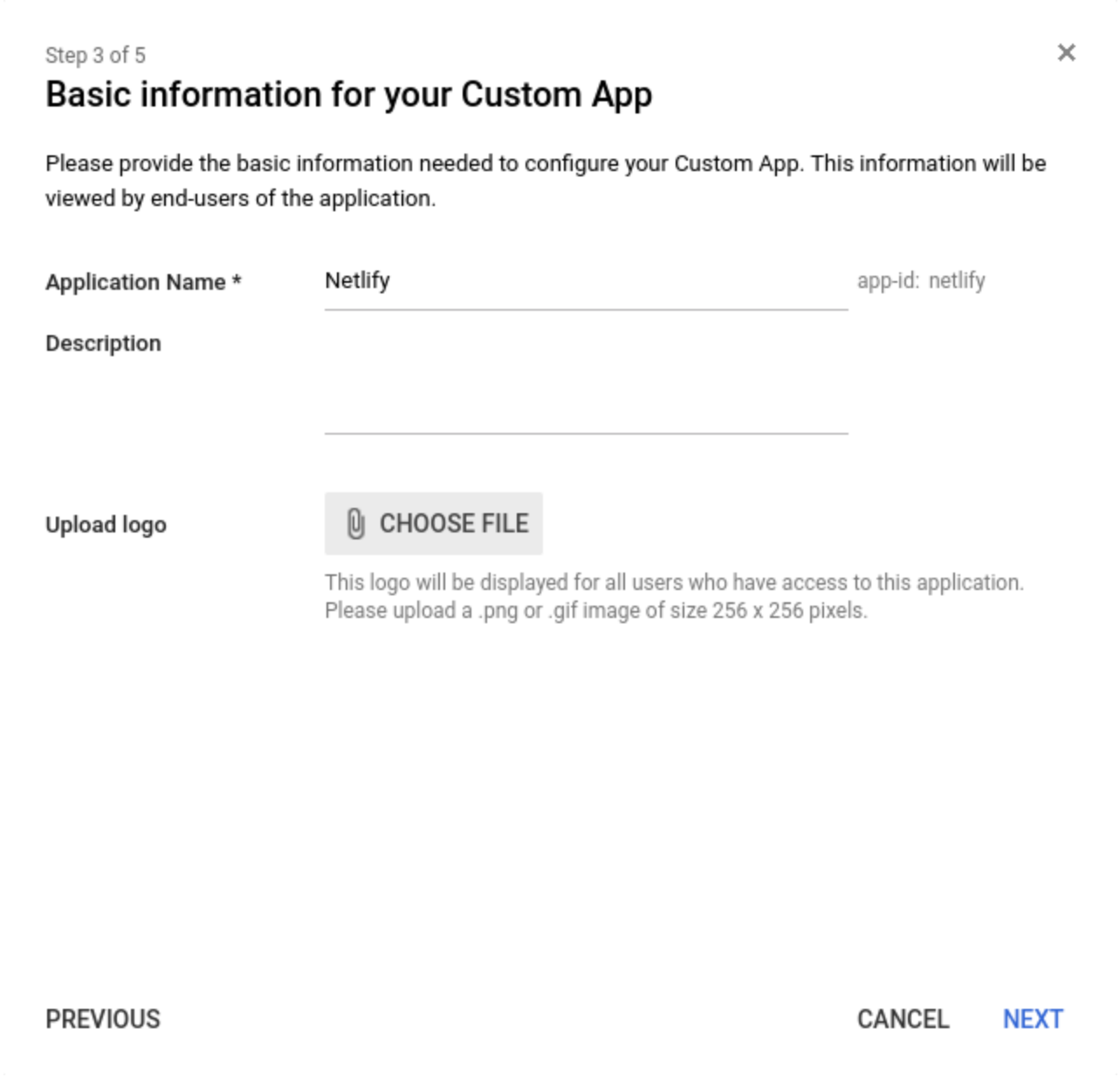
5. Under **Option 2**, select **Download** to download your Google G Suite IdP metadata. You will need to host this XML file publicly so that Netlify can access it. A good place to host it is on one of your sites deployed by Netlify.

   Select **NEXT.**



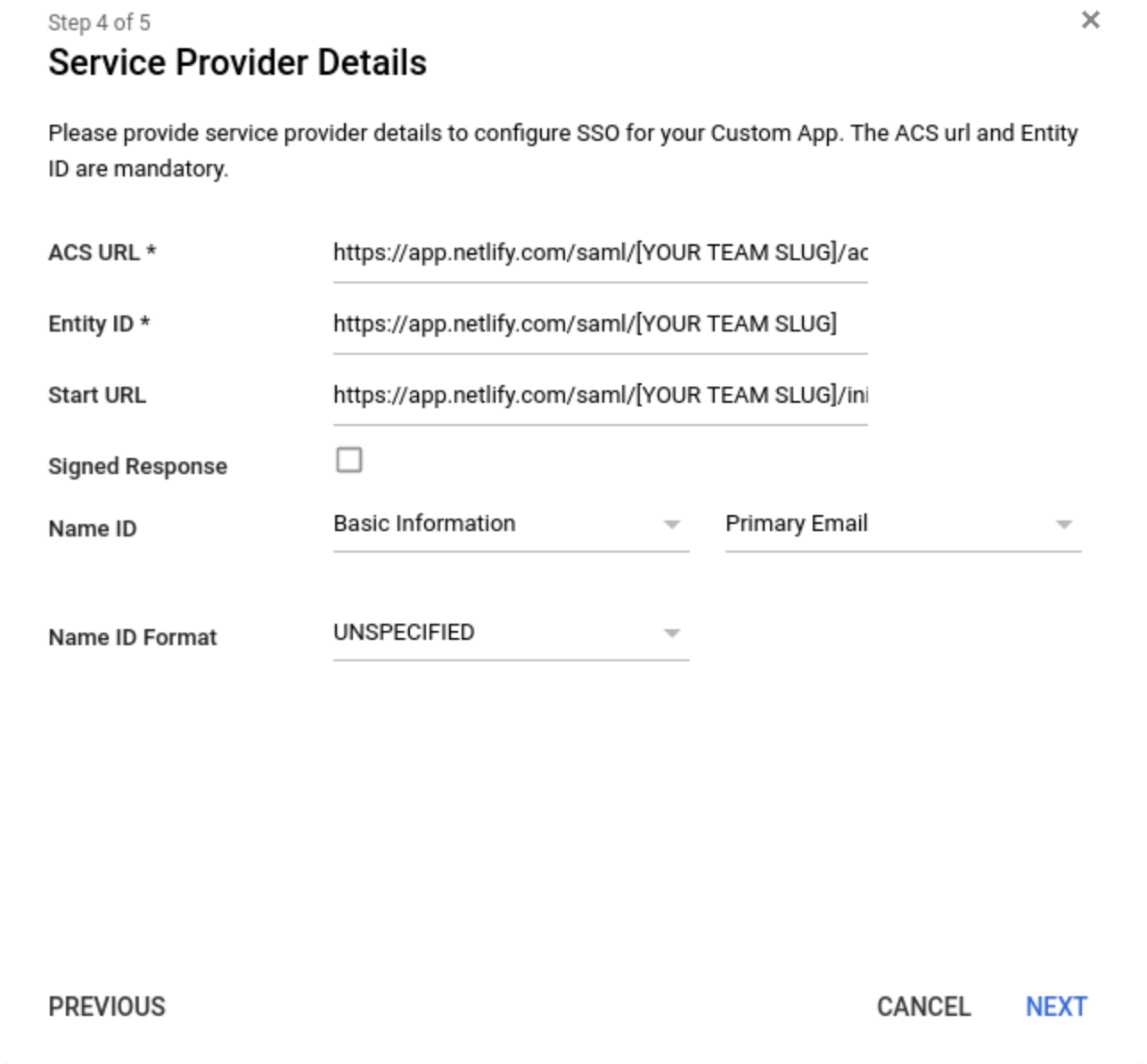
6. In **Basic information for your Custom App**:
   a. **Application Name:** Enter **Netlify.**

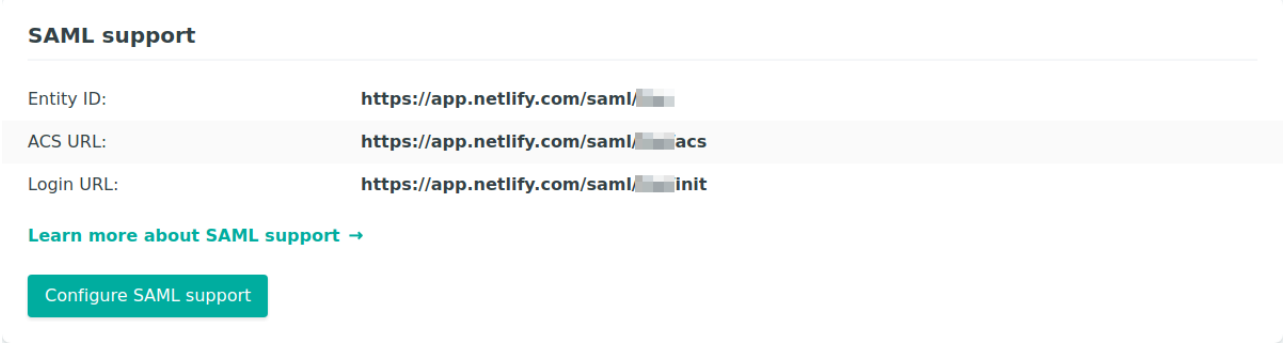
Select **NEXT**.



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.**

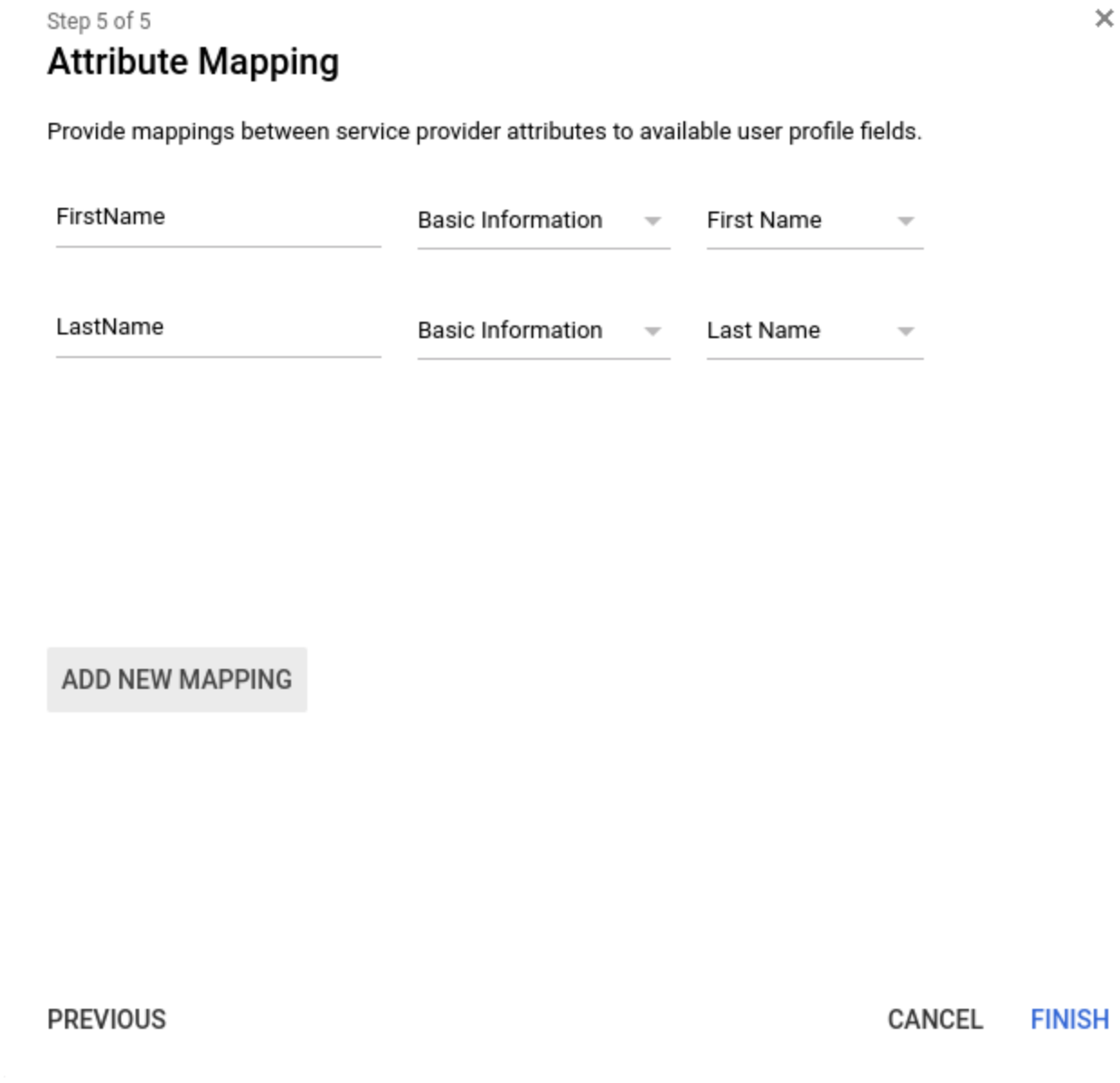

Step 4 of 5
Service Provider Details
Please provide service provider details to configure SSO for your Custom App. The ACS url and Entity ID are mandatory.
ACS URL *
https://app.netlify.com/saml/[YOUR TEAM SLUG]/ac
Entity ID *
https://app.netlify.com/saml/[YOUR TEAM SLUG]
Start URL
https://app.netlify.com/saml/[YOUR TEAM SLUG]/ini
Signed Response
Name ID
Basic Information
Primary Email
Name ID Format
UNSPECIFIED
PREVIOUS
CANCEL
NEXT



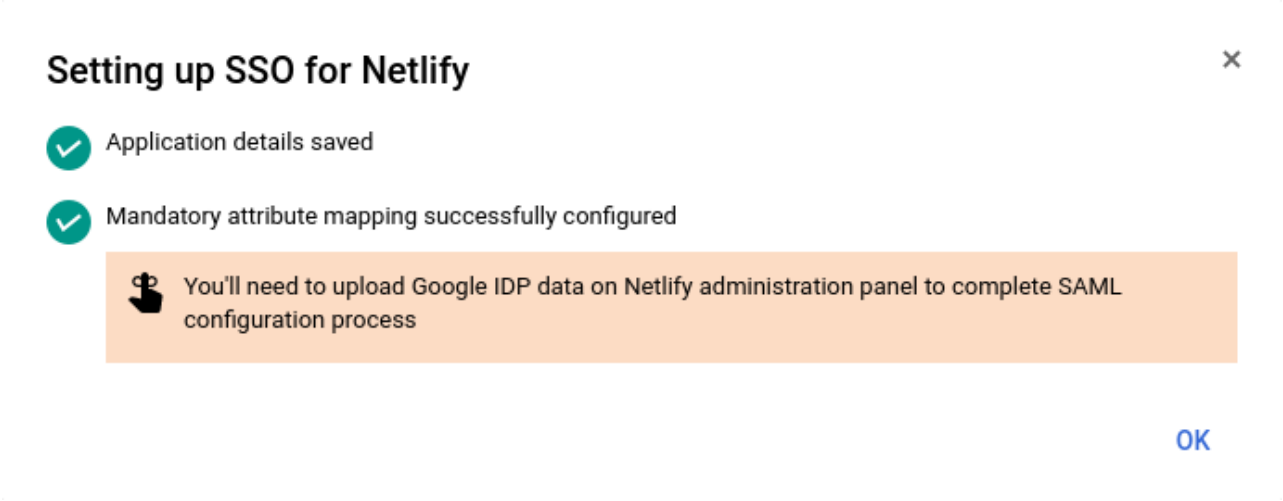
8. In **Attribute Mapping**:

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

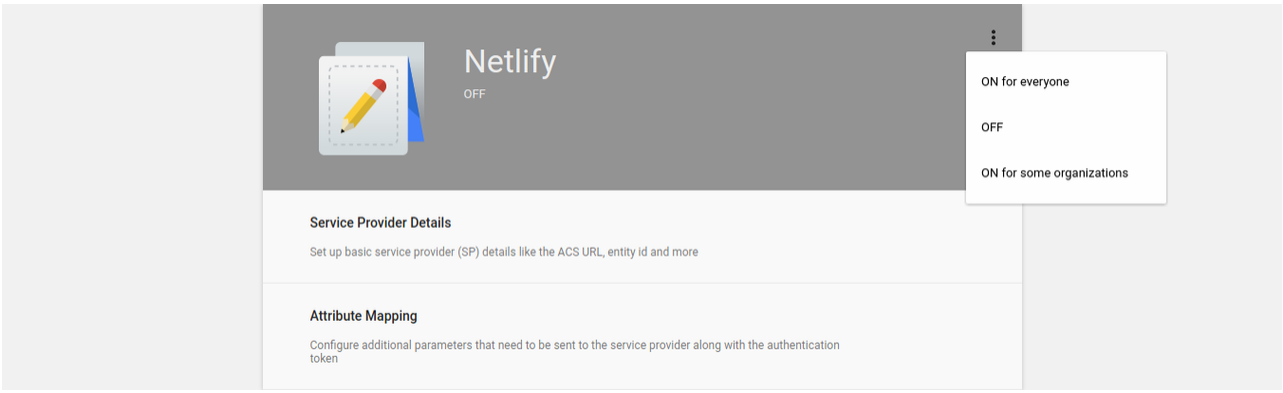
   Select **Finish**.


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**.



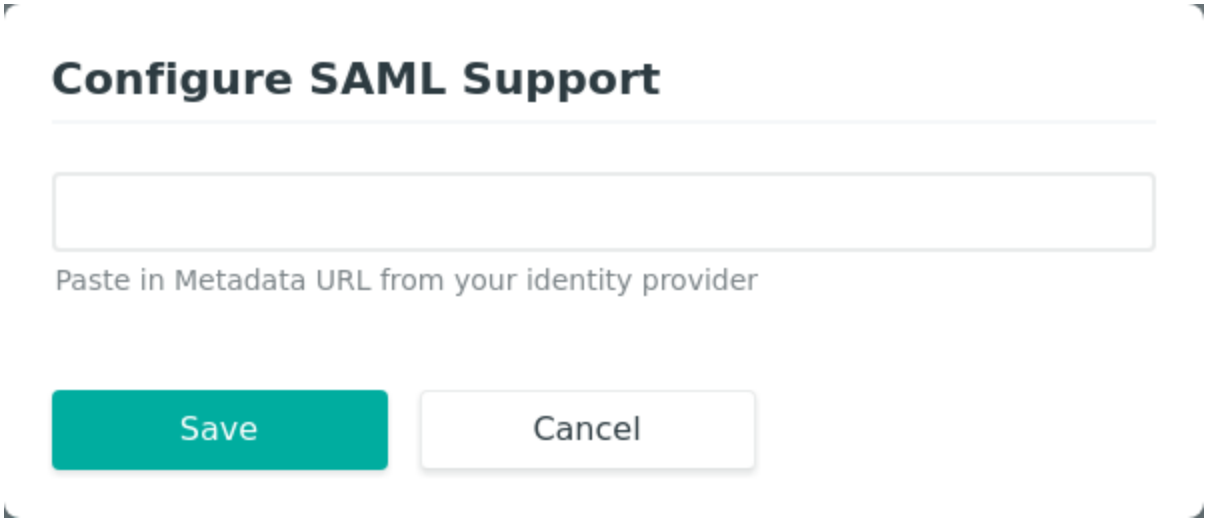
10. Select **On for everyone** to turn the Netlify SAML app on for everyone in your organization.



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

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

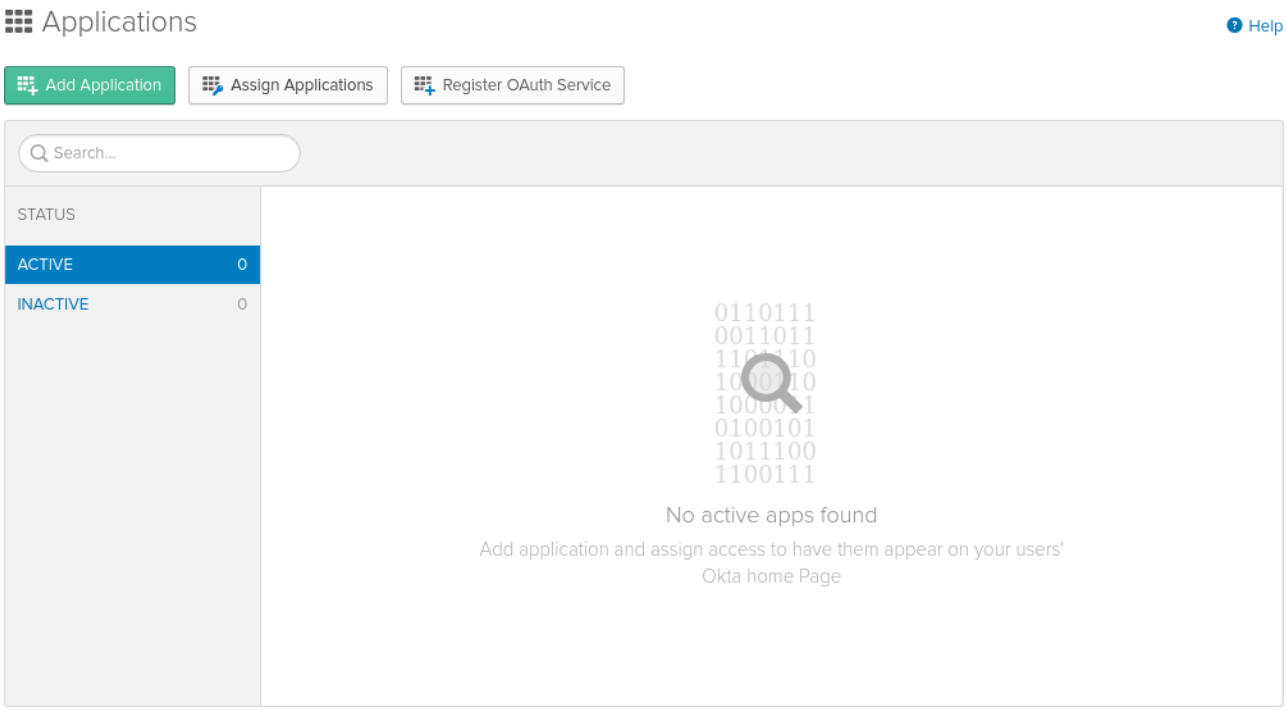
Click **Save**.



Okta

To configure Netlify with Okta:

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



2. Select **Create New App.**

Can't find an app?

Create New App

Apps you created(0) →

INTEGRATION PROPERTIES

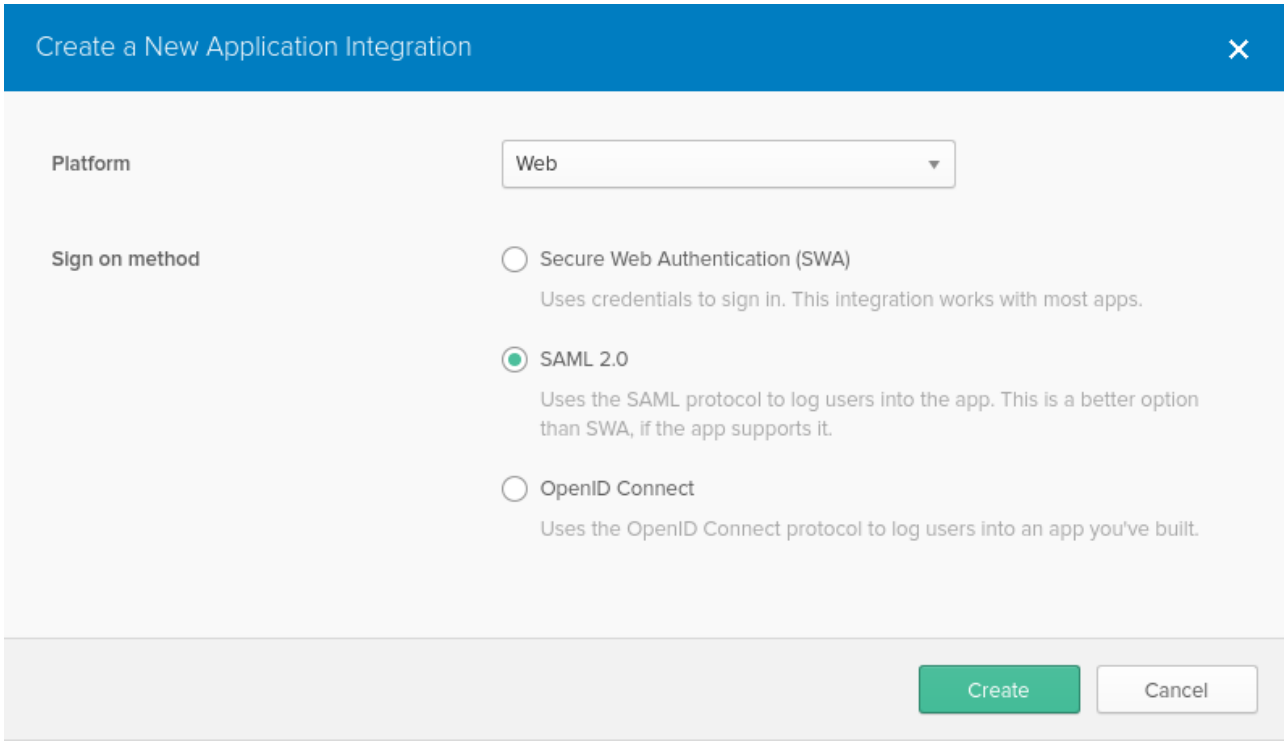
- Any
- Supports SAML
- Supports Provisioning

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

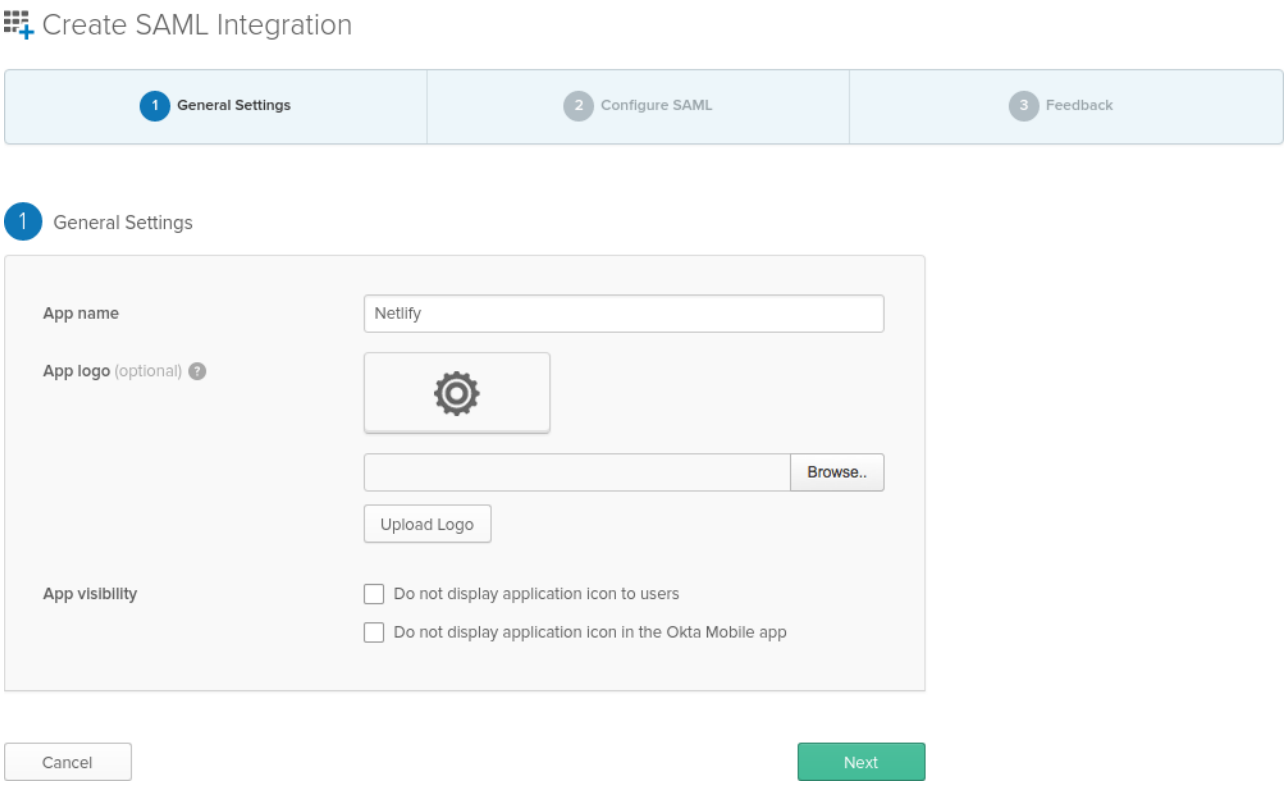
3. In **Create a New Application integration**:
   a. **Platform**: Select **Web.**
   b. **Sign on method:** Select **SAML 2.0**.

   Select **Create.**



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

   Select **Next**.



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 https://app.netlify.com/saml/[YOUR TEAM SLUG]/acs

- [x] Use this for Recipient URL and Destination URL
- [ ] Allow this app to request other SSO URLs

Audience URI (SP Entity ID) https://app.netlify.com/saml/[YOUR TEAM SLUG]

Default RelayState

If no value is set, a blank RelayState is sent

Name ID format Unspecified

Application username Okta username

Show Advanced Settings

ATTRIBUTE STATEMENTS (OPTIONAL)

LEARN MORE

Name	Name format (optional)	Value
FirstName	Unspecified	user.firstName
LastName	Unspecified	user.lastName

Add Another

GROUP ATTRIBUTE STATEMENTS (OPTIONAL)

Name	Name format (optional)	Filter
	Unspecified	Starts with

Add Another

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.

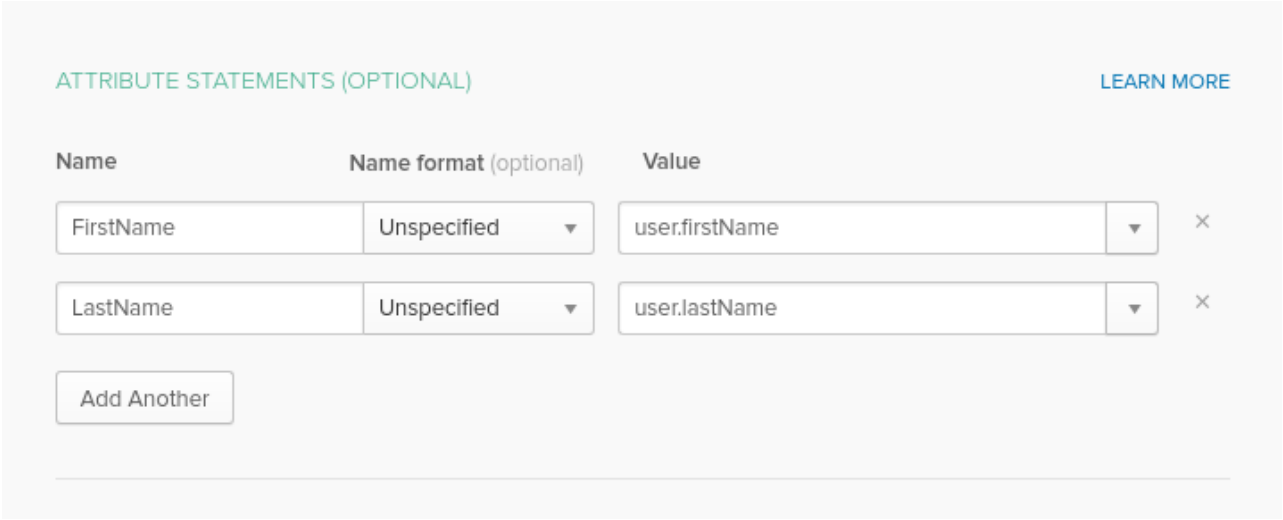
Download Okta Certificate

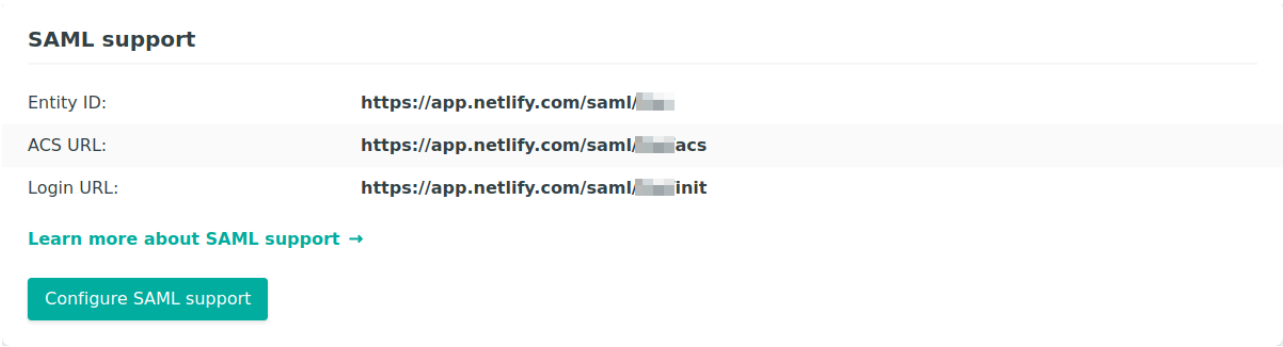
B Preview the SAML assertion generated from the information above

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

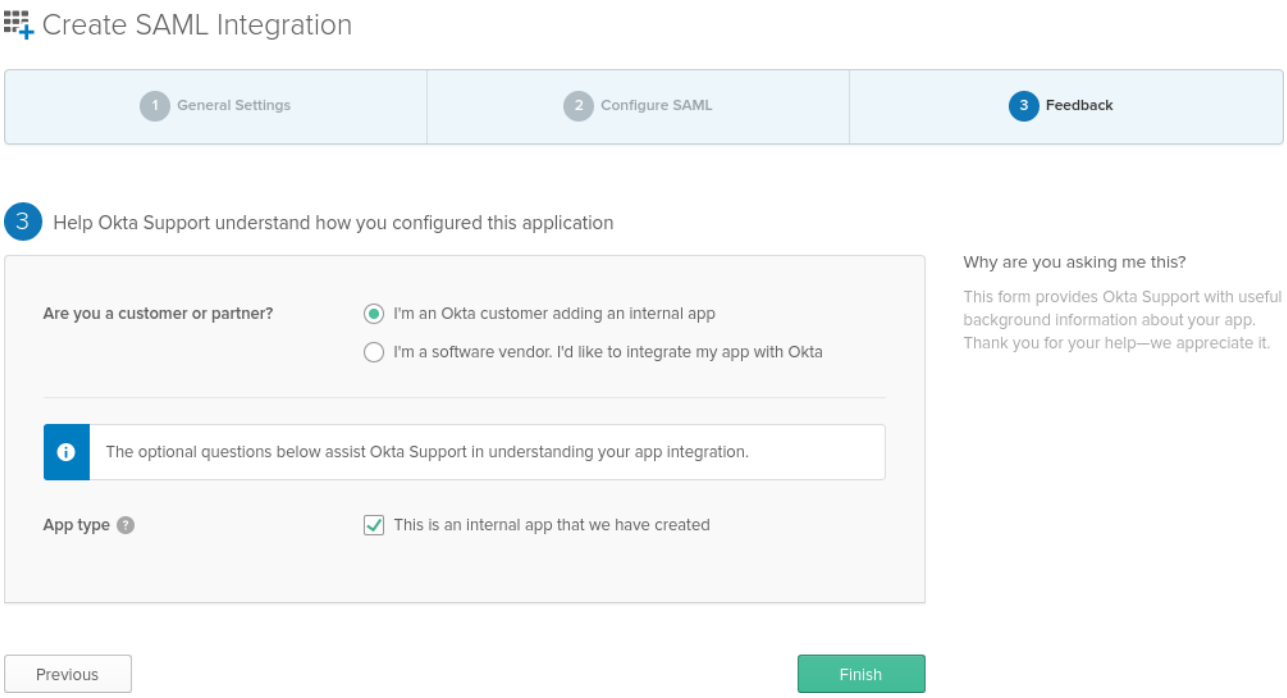
Previous | Cancel | Next



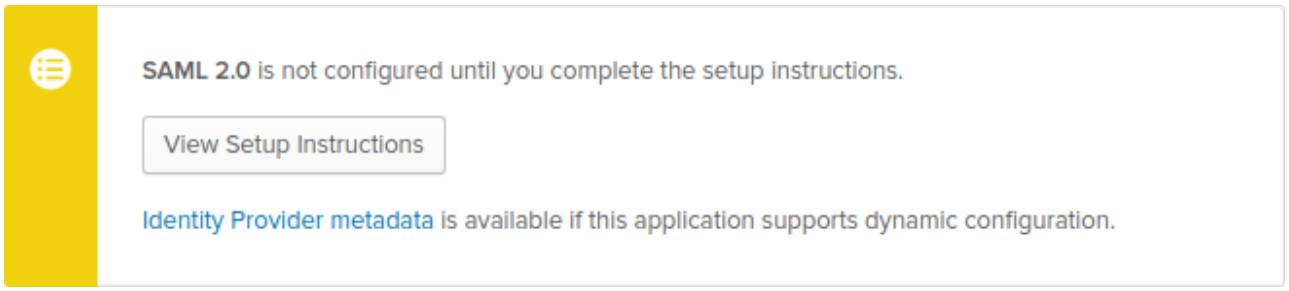


7. In **Feedback**:
   a. **Are you a customer or partner?**: Select **I'm an Okta customer adding an internal app.**
   b. **App type**: Select **This is an internal app that we have created.**

   Select **Finish.**



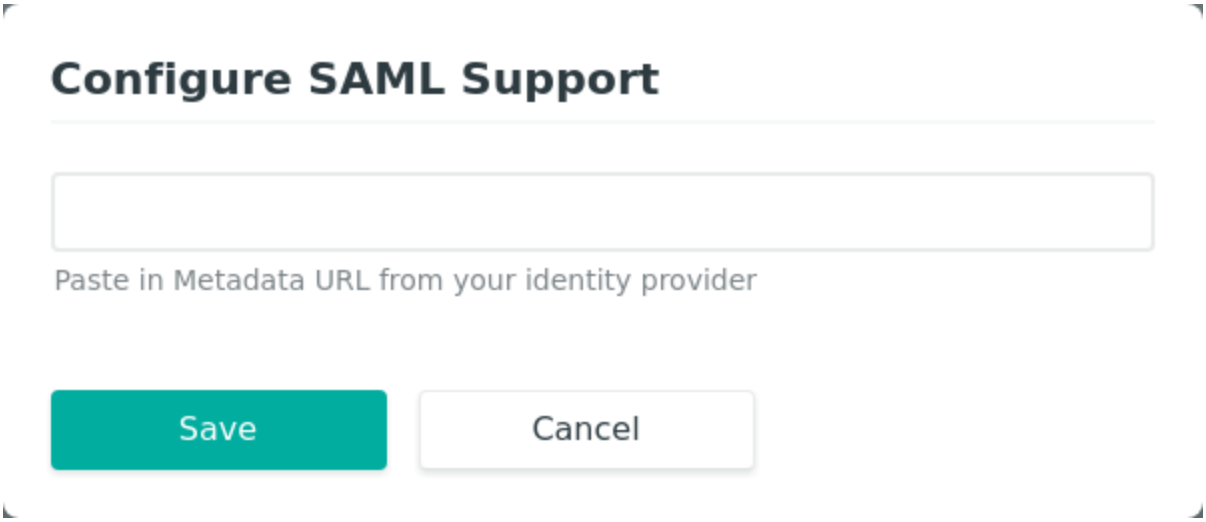
8. Copy the URL from the **Identity Provider metadata** link.



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

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

Click **Save**.



OneLogin

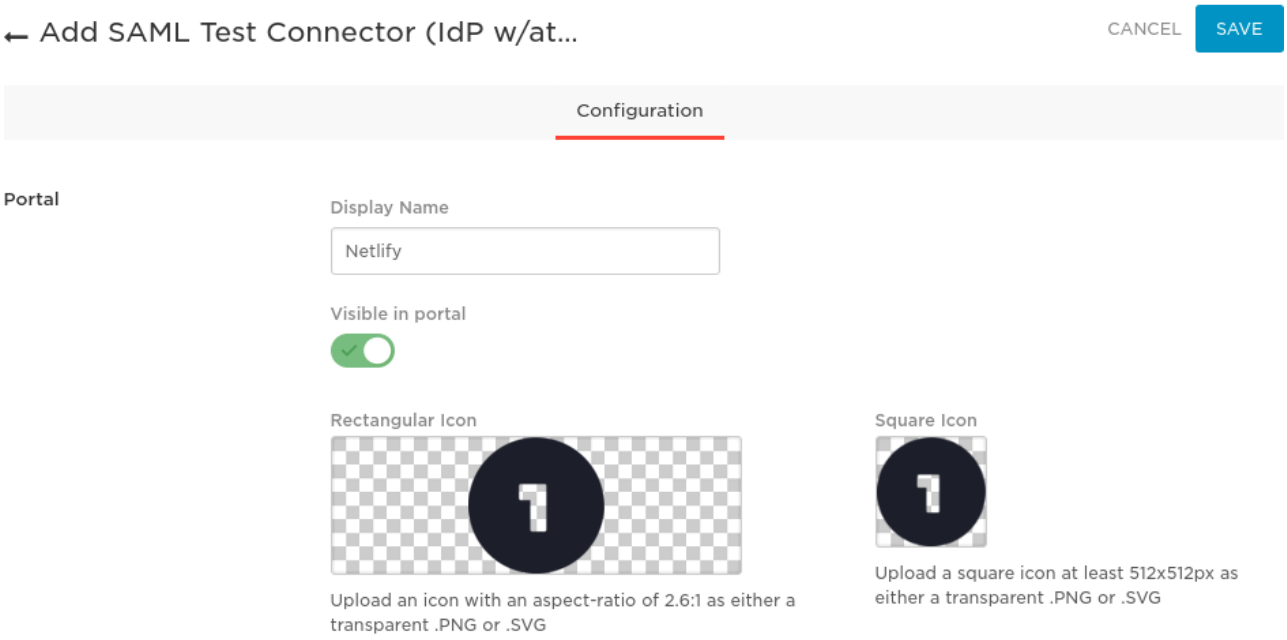
To configure Netlify with OneLogin:

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

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

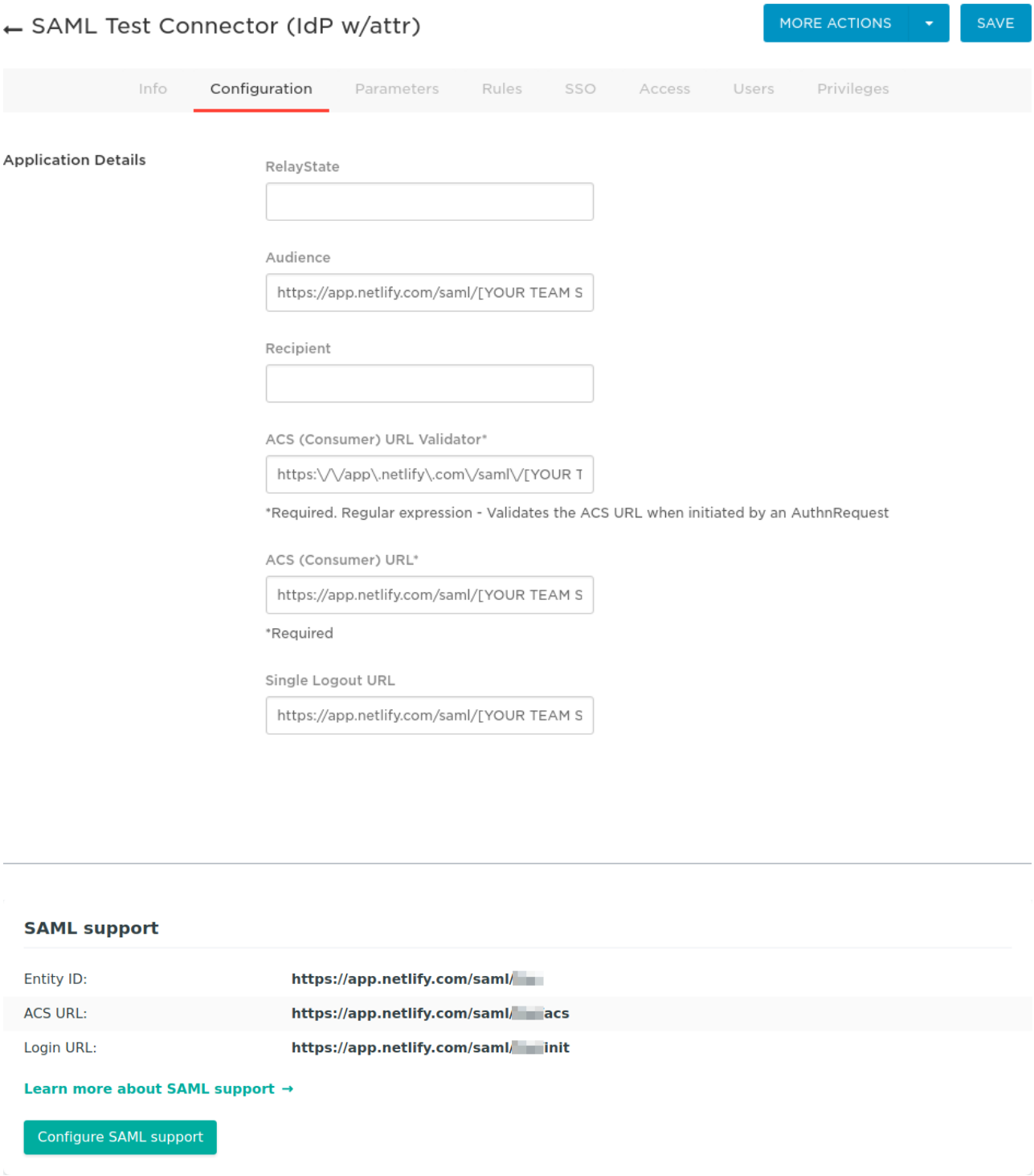
3. In **Configuration**:
   a. **Display Name**: Enter **Netlify**.

   Select **Save**.



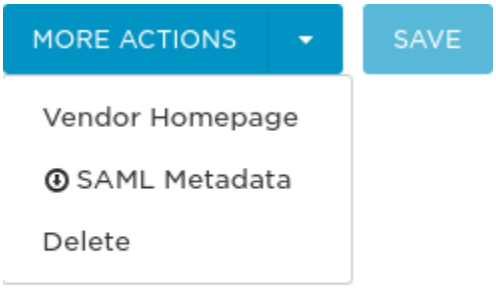
4. In **Configuration**:
   a. **Audience**: Enter your **Entity ID** from **Netlify > Team settings > SAML support**.
   b. **ACS (Consumer) URL Validator**: Enter **https:\/\/app\.netlify\.com\/saml\/YOUR TEAM SLUG\/acs** replacing YOUR TEAM SLUG with your actual team slug.
   c. **ACS (Consumer) URL**: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

   Select **Save**.



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

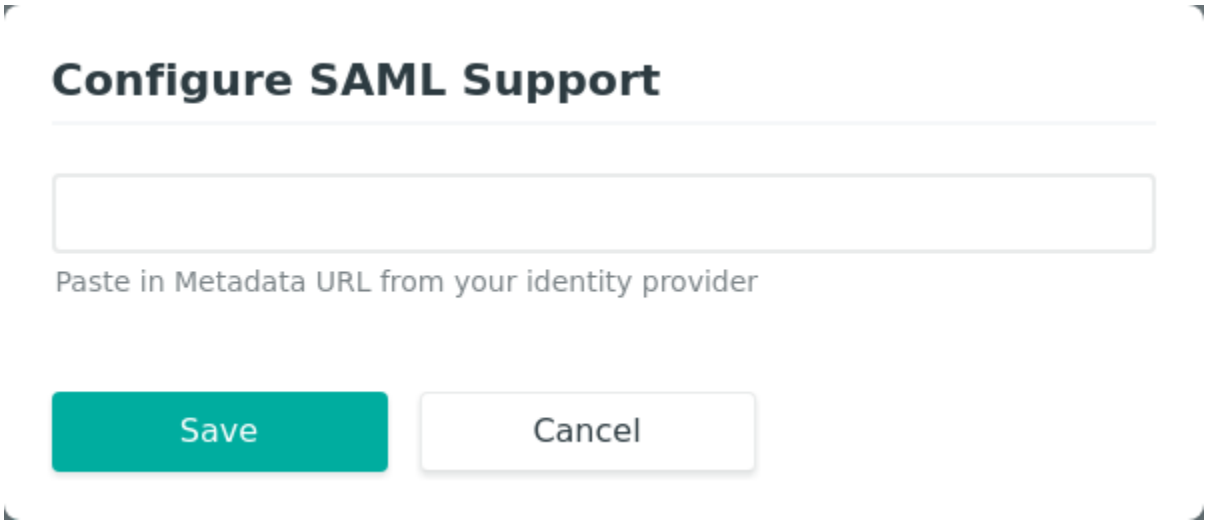
Netlify can access it. A good place to host it is on one of your sites deployed by Netlify.



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

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**.

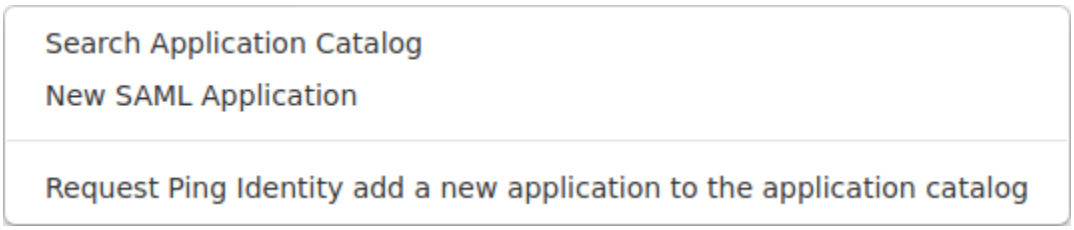


Ping Identity PingOne

To configure Netlify with Ping Identity PingOne:

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

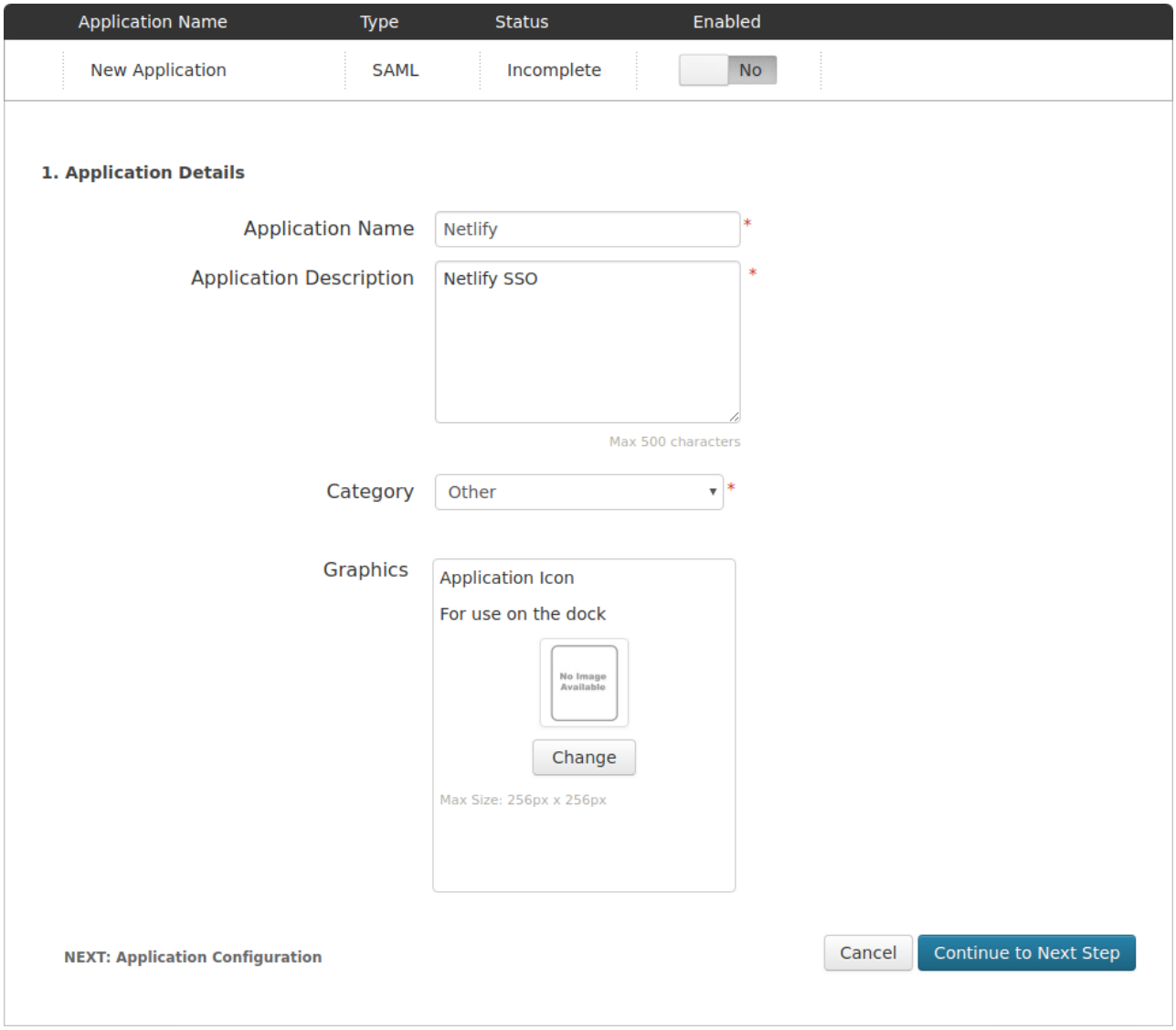
2. Select **New SAML Application**.



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**.



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	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: PingOne Account Origination 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: Select File | Or use URL

Assertion Consumer Service (ACS): https://api.netlify.com/saml/[YOUR *

Entity ID: https://api.netlify.com/saml/[YOUR *

Application URL:

Single Logout Endpoint: example.com/slo.endpoint

Single Logout Response Endpoint: example.com/sloresponse.endpoir

Single Logout Binding Type: Redirect / Post

Primary Verification Certificate: Choose File | No file chosen

Secondary Verification Certificate: Choose File | No file chosen

Signing Algorithm: RSA_SHA256

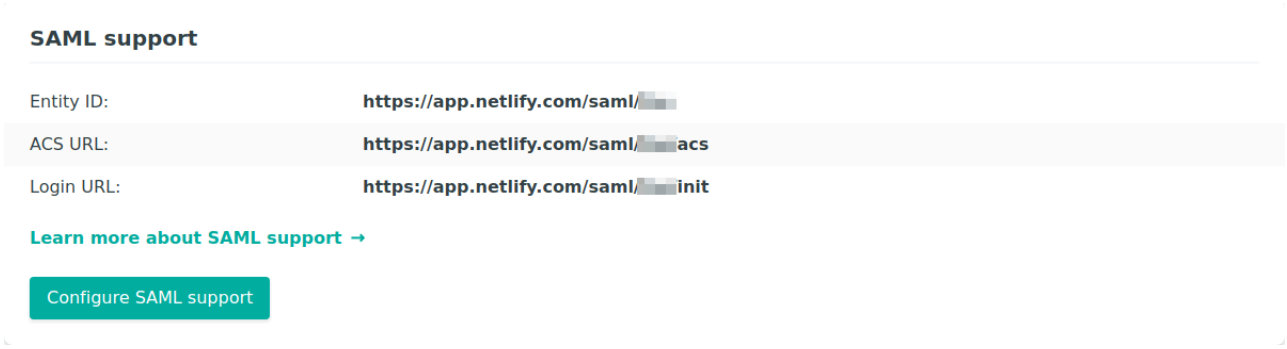
Force Re-authentication:

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

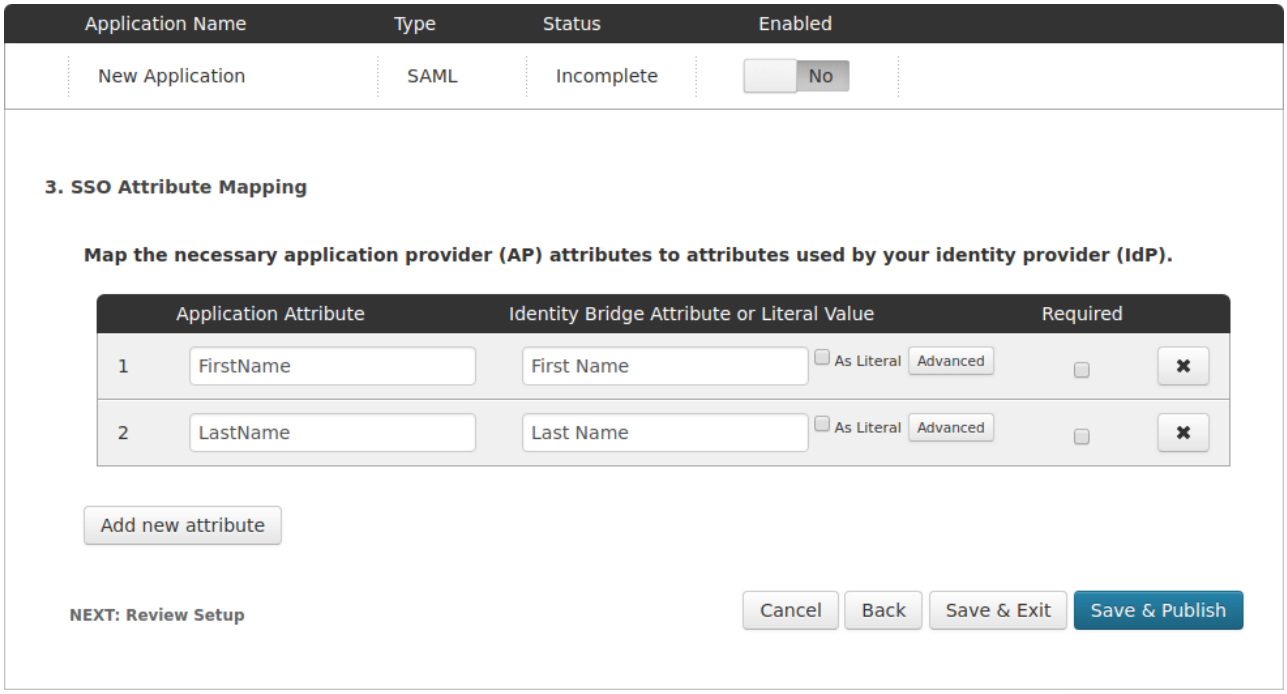
Cancel | Back | Continue to Next Step



5. In **SSO Attribute Mapping**:

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

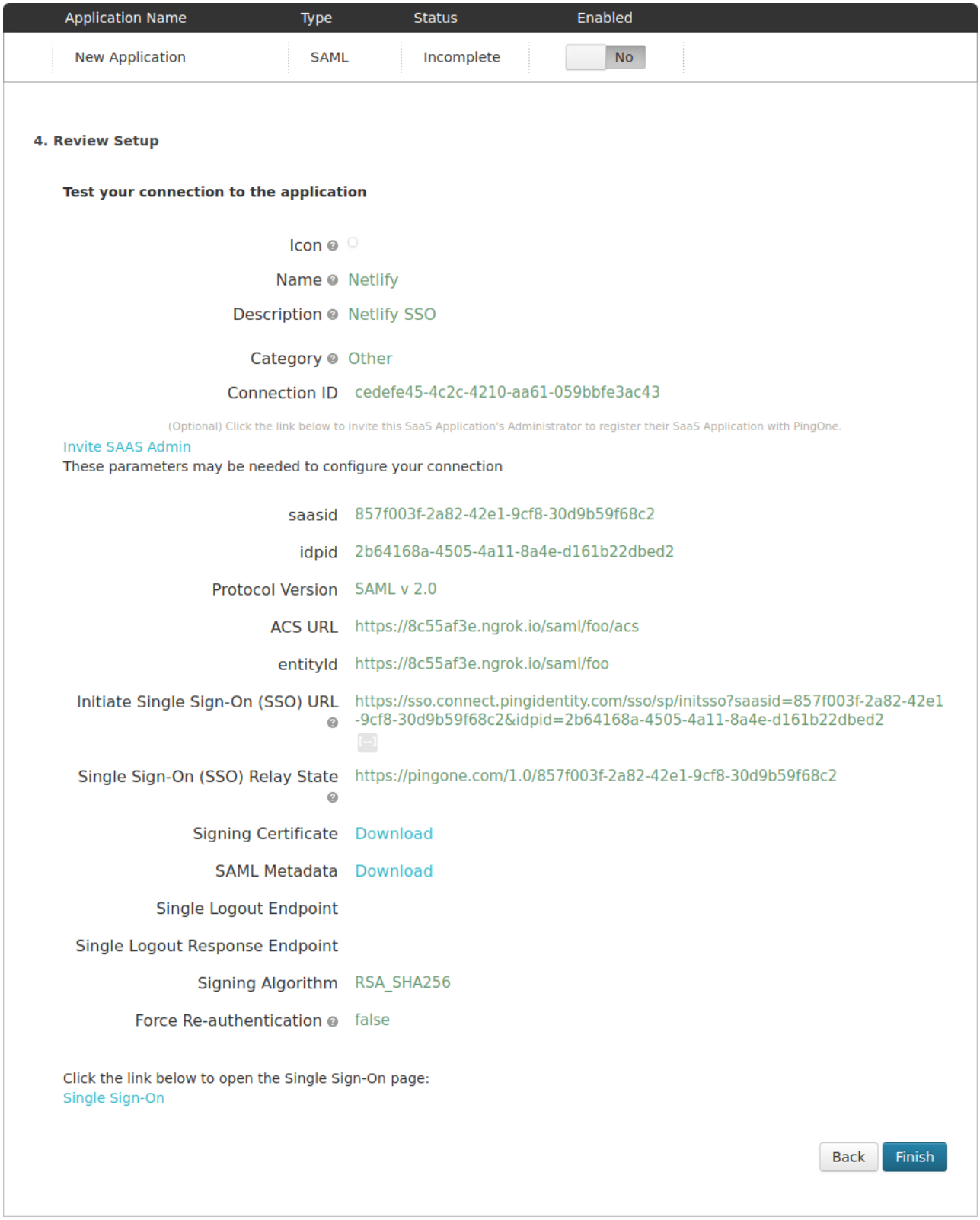
   Select **Save & Publish**.



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.

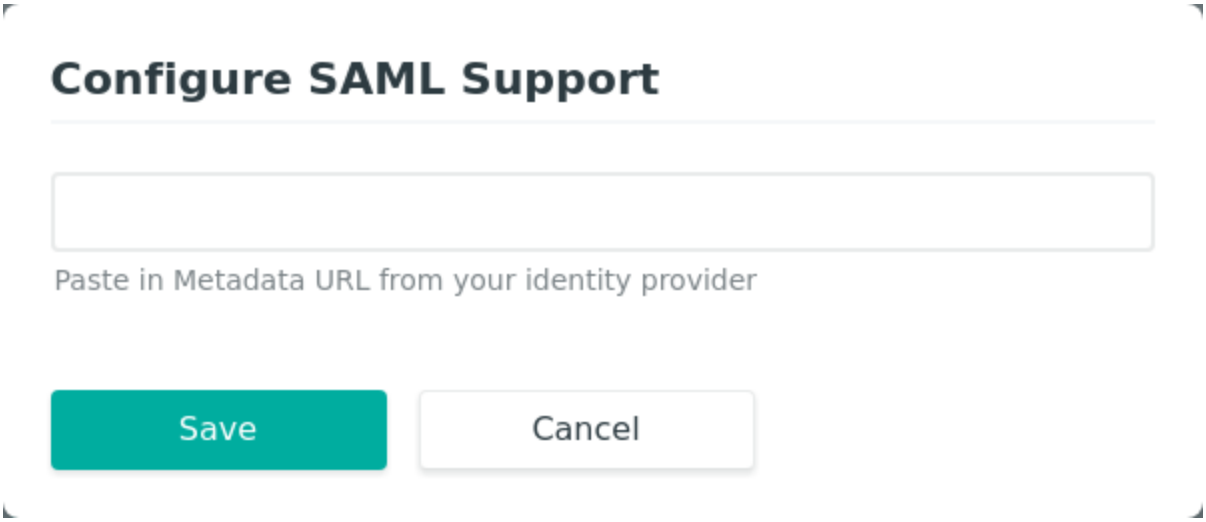
Select **Finish**.



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

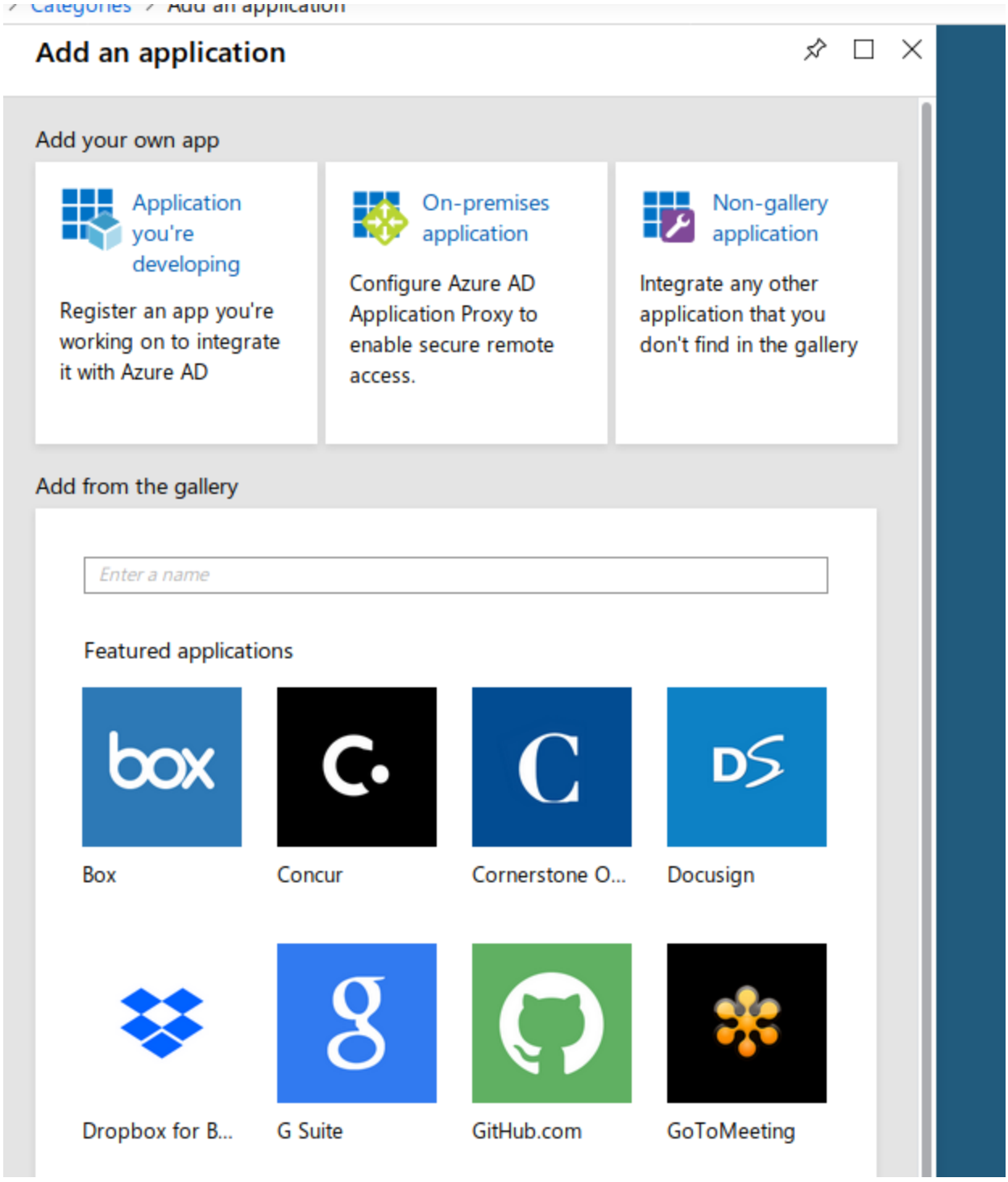
8. Paste the URL of the XML file you downloaded in Step 6 and are now hosting publicly into the **Configure SAML Support** input.

   Click **Save**.

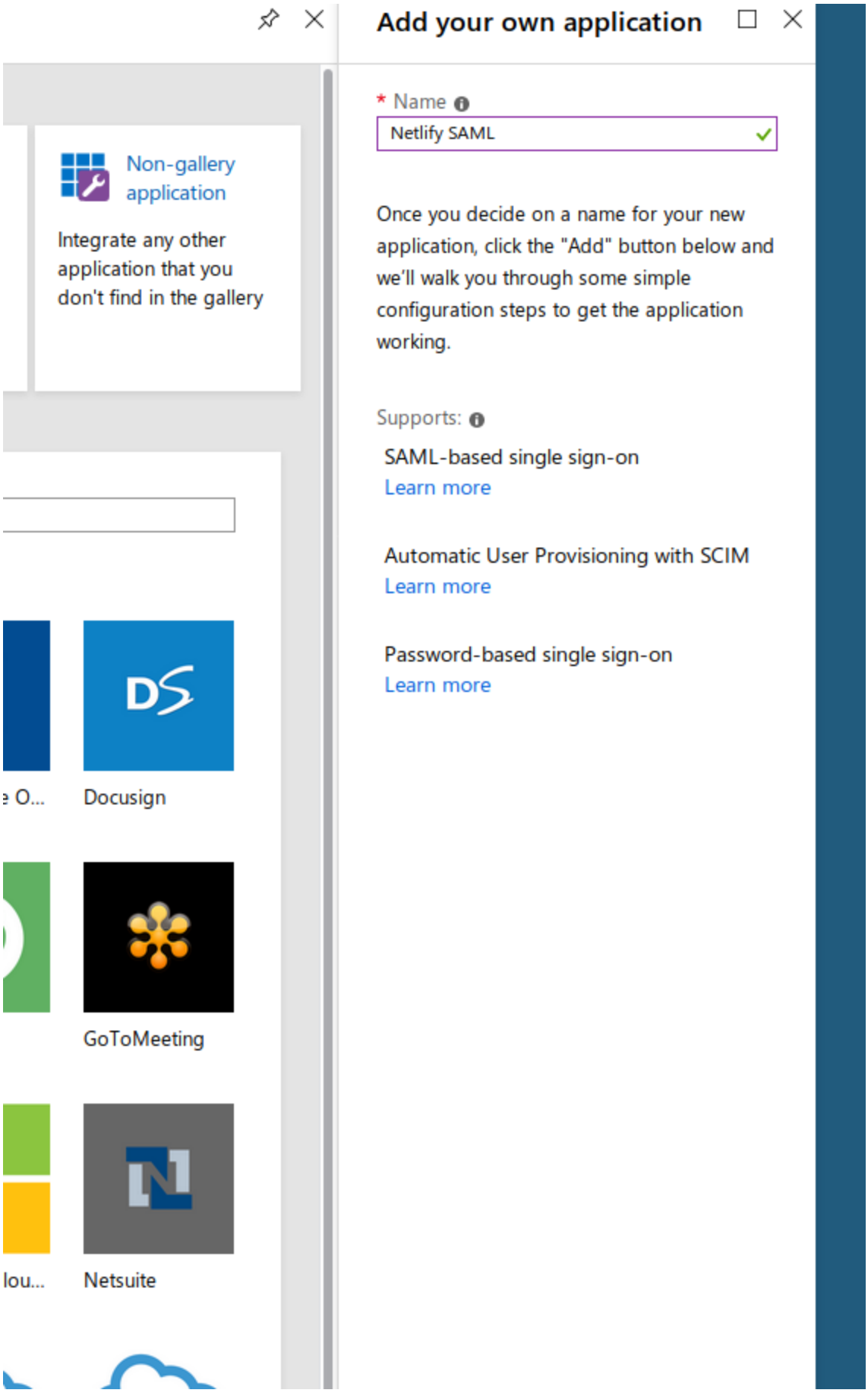


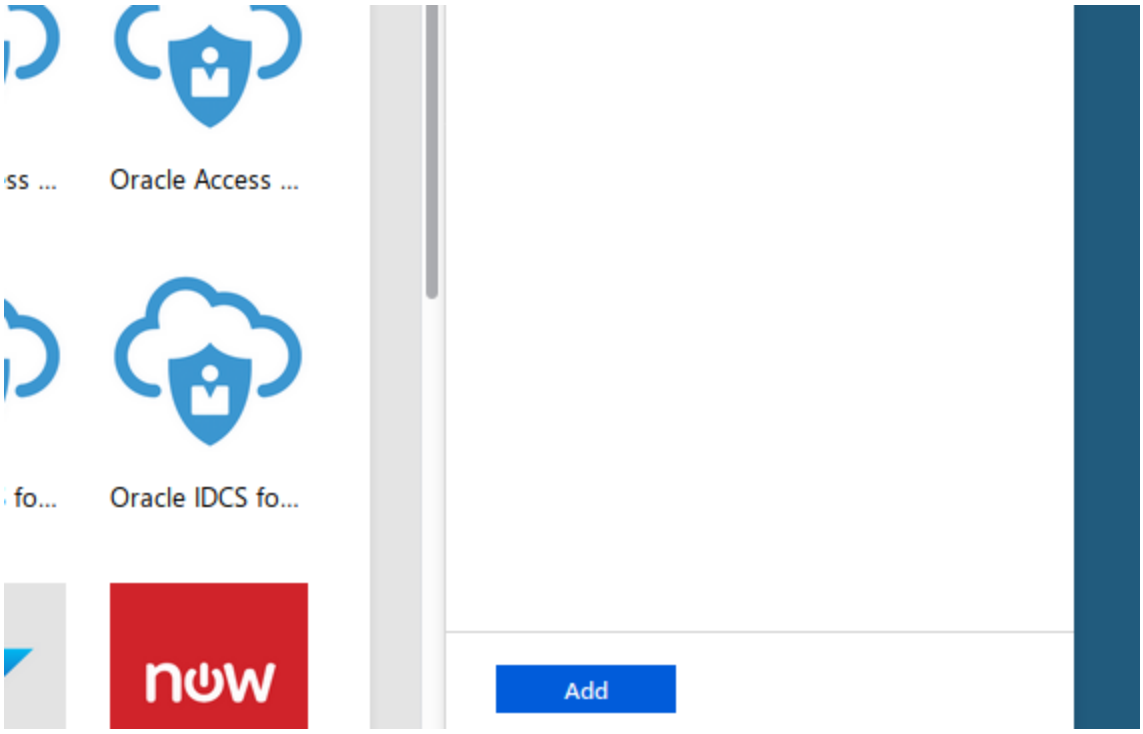
Azure Active Directory

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 onebelow:



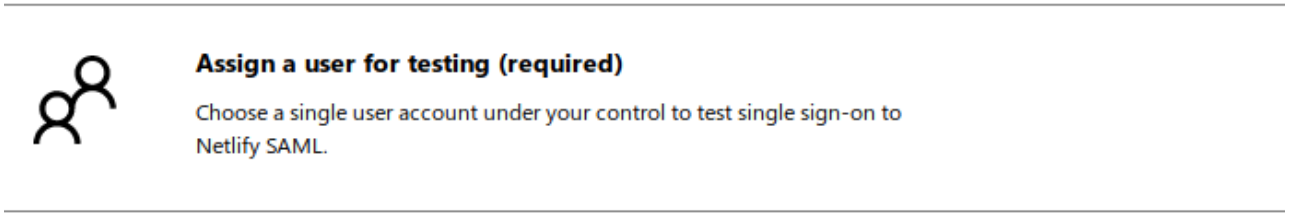
3. Click “Non-gallery application”, and enter the application name, and click “Add” at the bottom of the screen.


Non-gallery application
Integrate any other application that you don't find in the gallery
Docusign
GoToMeeting
Netsuite
Add your own application
* 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

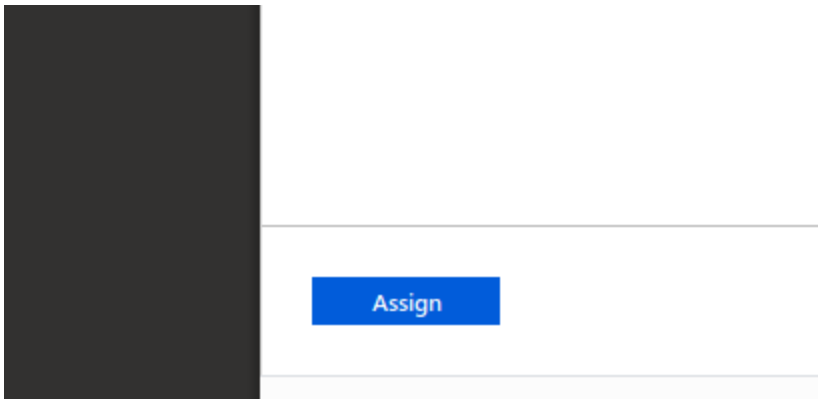


If you're not paying for enterprise applications, it will let you start a trial. Click the option that says "Enterprise...", NOT the option that says "Mobile...".

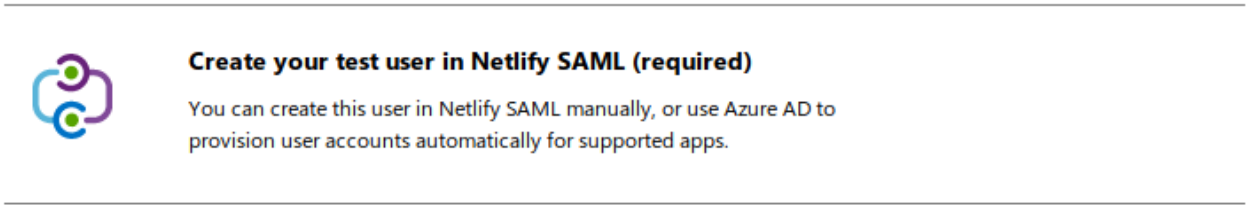
4. Click on "Assign a user for testing". This will let you choose one of your users in Azure to test the connection between Azure and Netlify.



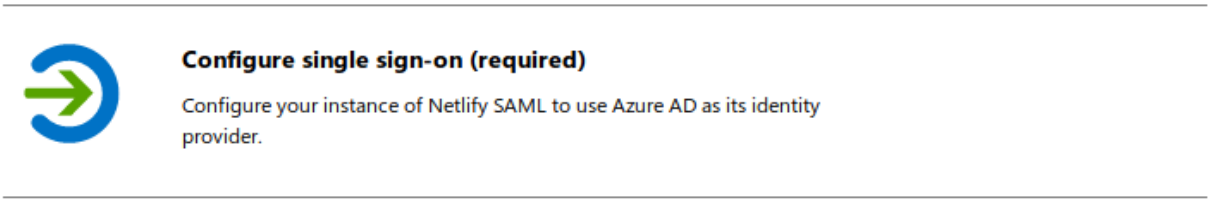
5. Click "Add user" in the top left corner and search for the user you want to test with. DO NOT FORGET to click "Assign" in the bottom left corner after selecting the user.



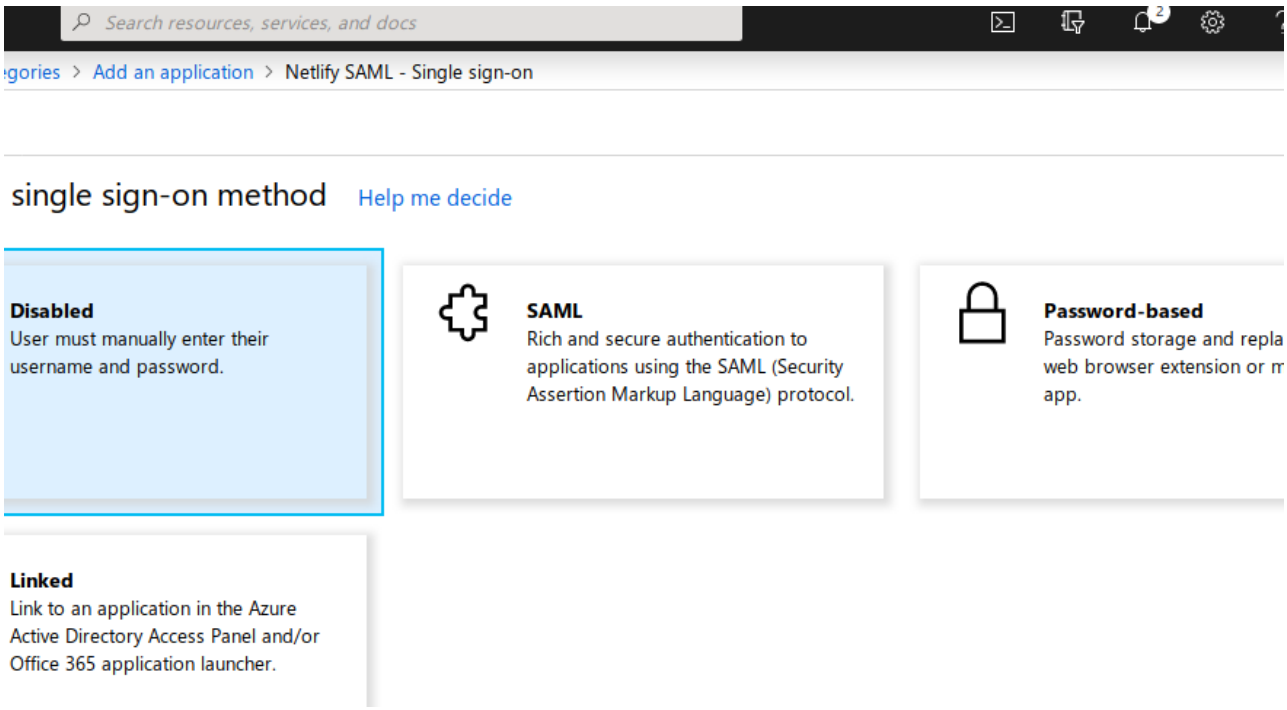
6. Go back to “Getting started” by using the breadcrumb menu at the top.
7. Click “Create your test user”:



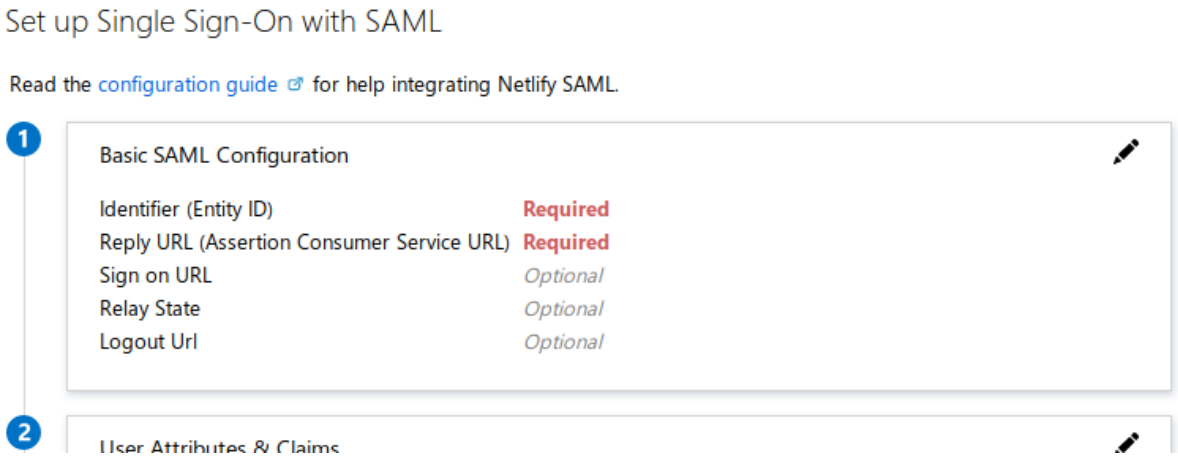
8. After a few seconds with the message “Provisioning”, it will show you a select box with two options, “Manual” and “Automatic”. Choose “Manual” and go back to the getting started menu.
9. Click “Configure single sign-on:



10. Click on “SAML”:



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

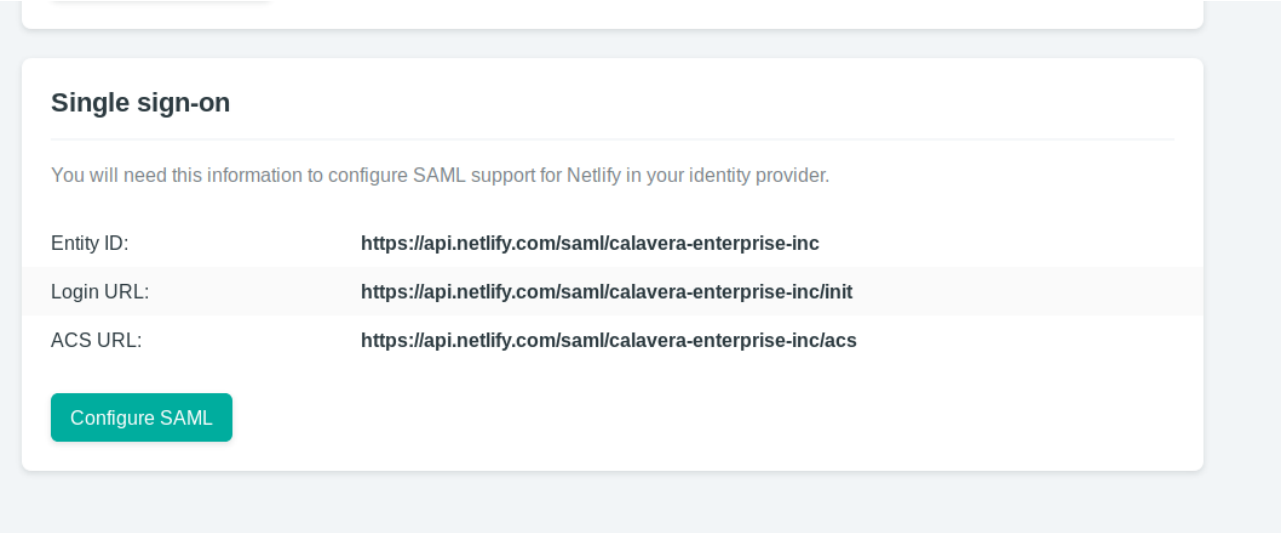


Those two required fields come from your Netlify Team settings, you can find them following a URL similar to this for your team:

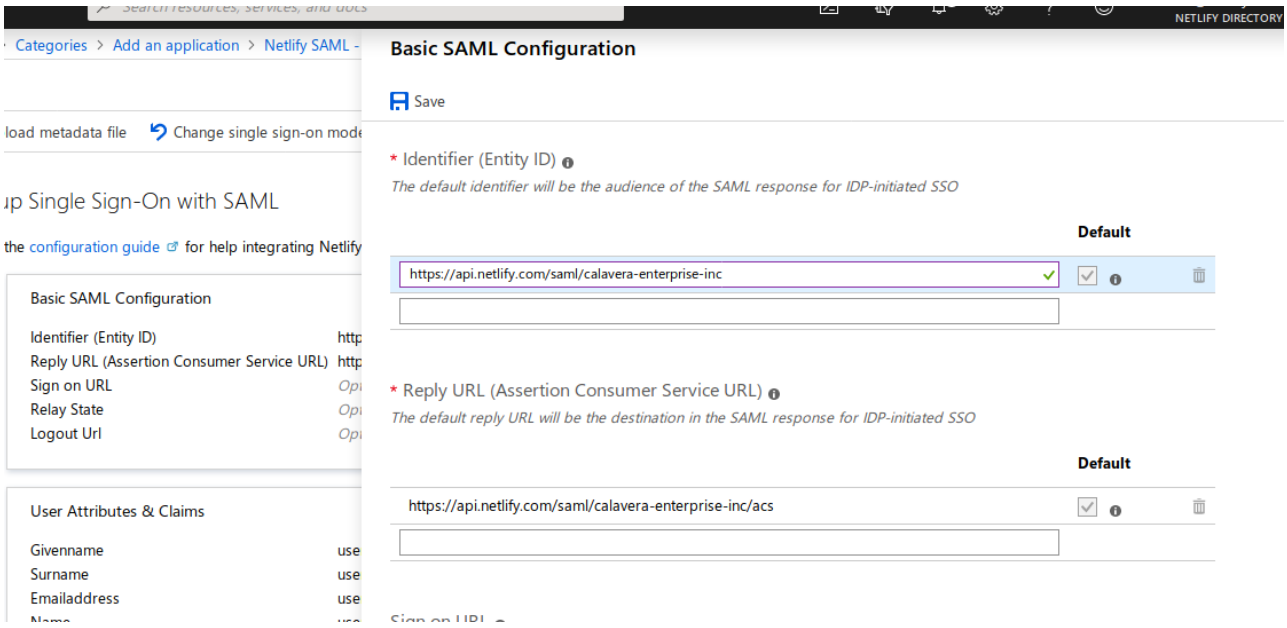
https://app.netlify.com/teams/YOUR-TEAM-SLUG-HERE/settings/profile#single-sign-on

For example:

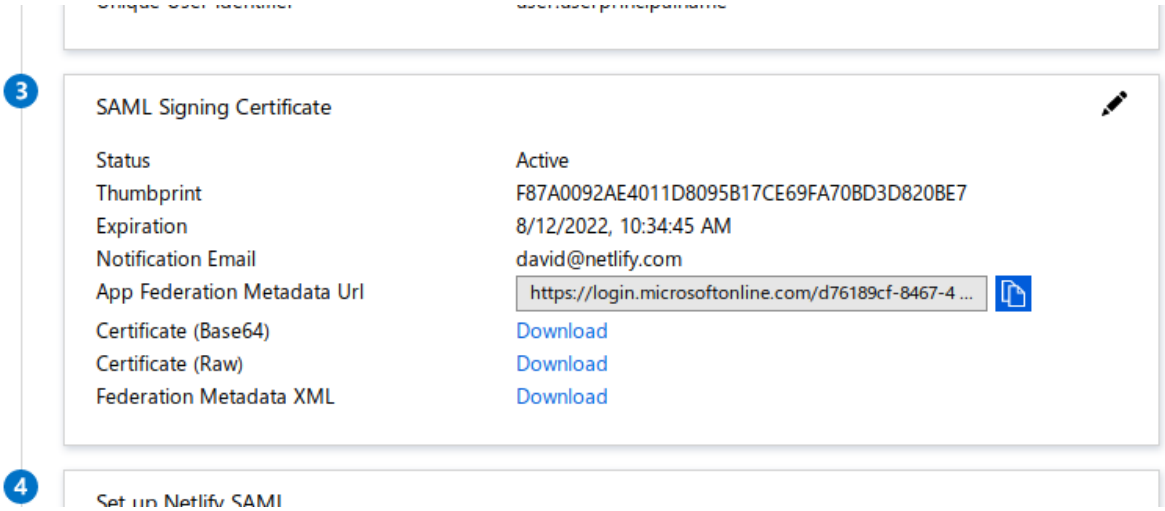
https://app.netlify.com/teams/calavera-enterprise-inc/settings/profile#single-sign-on



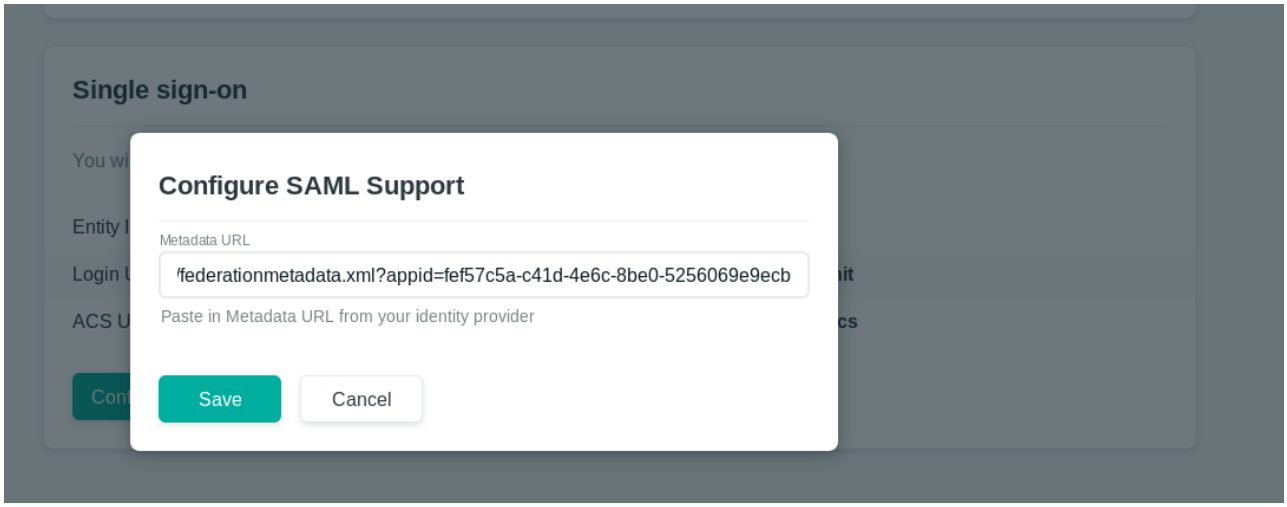
Copy “Entity ID” and “ACS URL” into the configuration in Azure and click “Save” in the top:



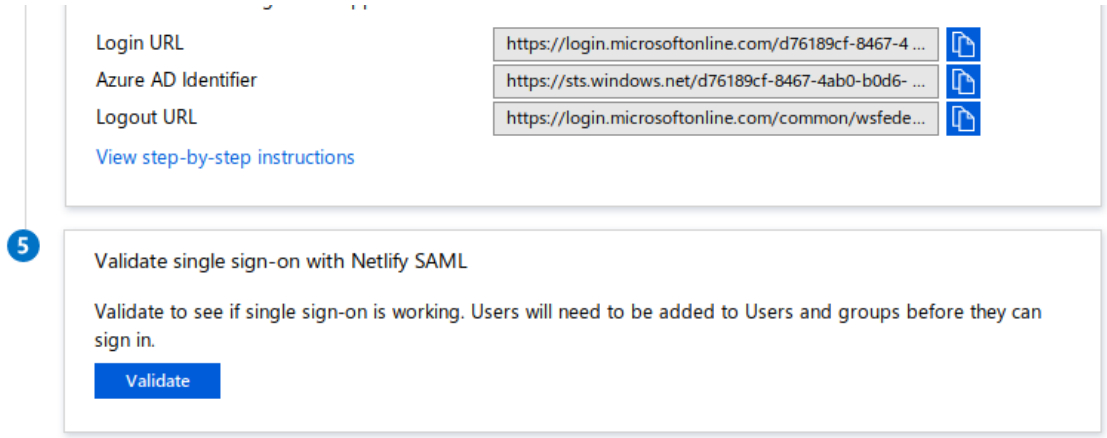
12. Copy the “App Federation Metadata URL” from section 3 in “SAML Signing Certificate”:



13. Go to your team settings in app.netlify.com and inctroduce 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:



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.