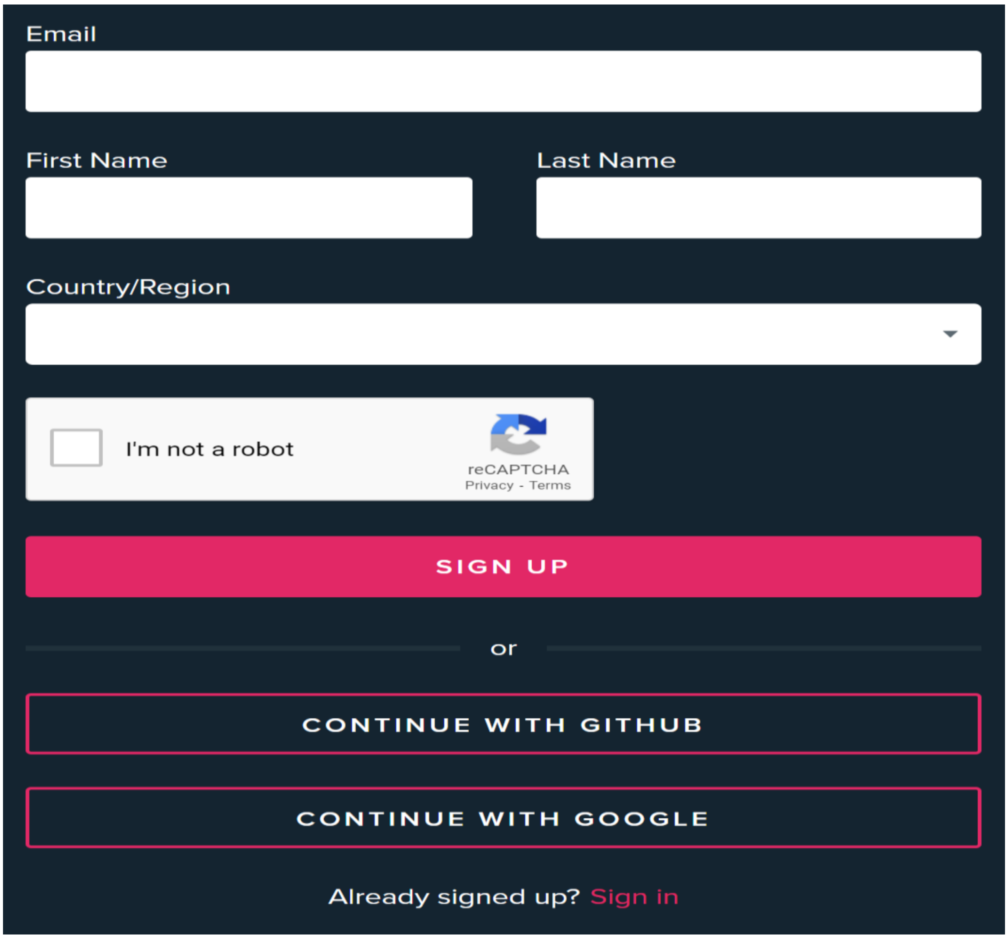
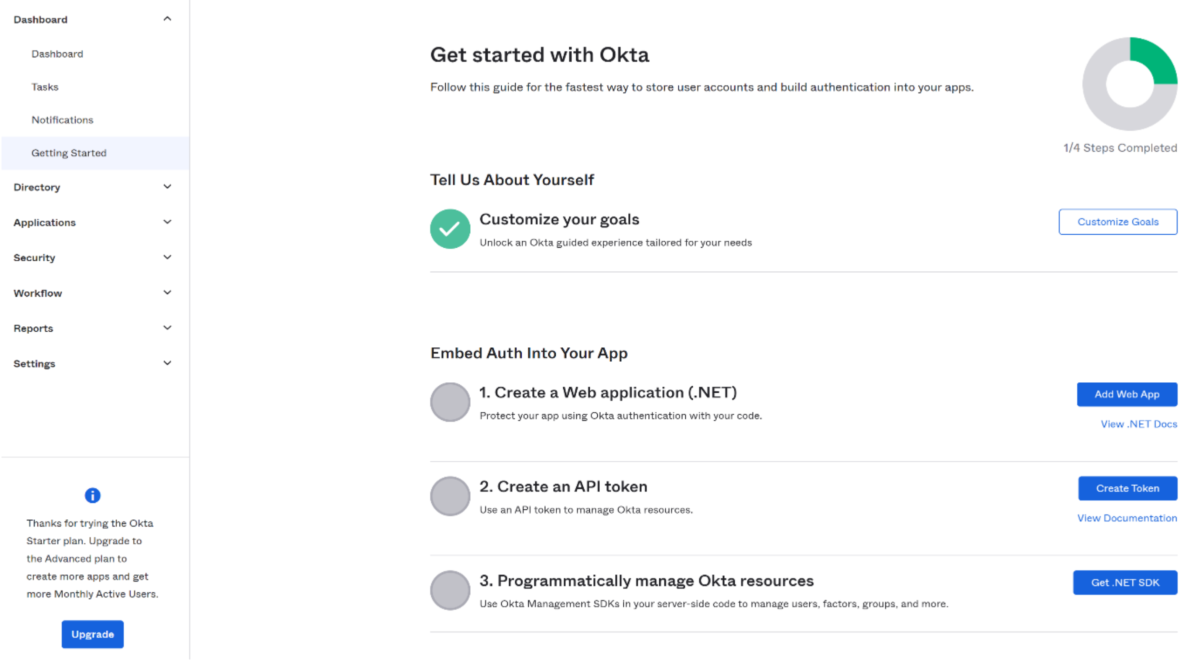
SAML Integration
In OKTA

Set up a developer account with OKTA

- OKTA is an identity provider with services like Single Sign-On, Multi-factor Authentication.
- To request a trial with OKTA, you will need a business email. But it’s also possible to request a developer account with no email restrictions from this link.
- https://developer.okta.com/signup/



- After verifying your email and logging in, you should see this page.



Thanks for trying the Okta Starter plan. Upgrade to the Advanced plan to create more apps and get more Monthly Active Users.

Get started with Okta

Follow this guide for the fastest way to store user accounts and build authentication into your apps.

1/4 Steps Completed

Tell Us About Yourself

Customize your goals

Unlock an Okta guided experience tailored for your needs

Embed Auth Into Your App

1. Create a Web application (.NET)

Protect your app using Okta authentication with your code.

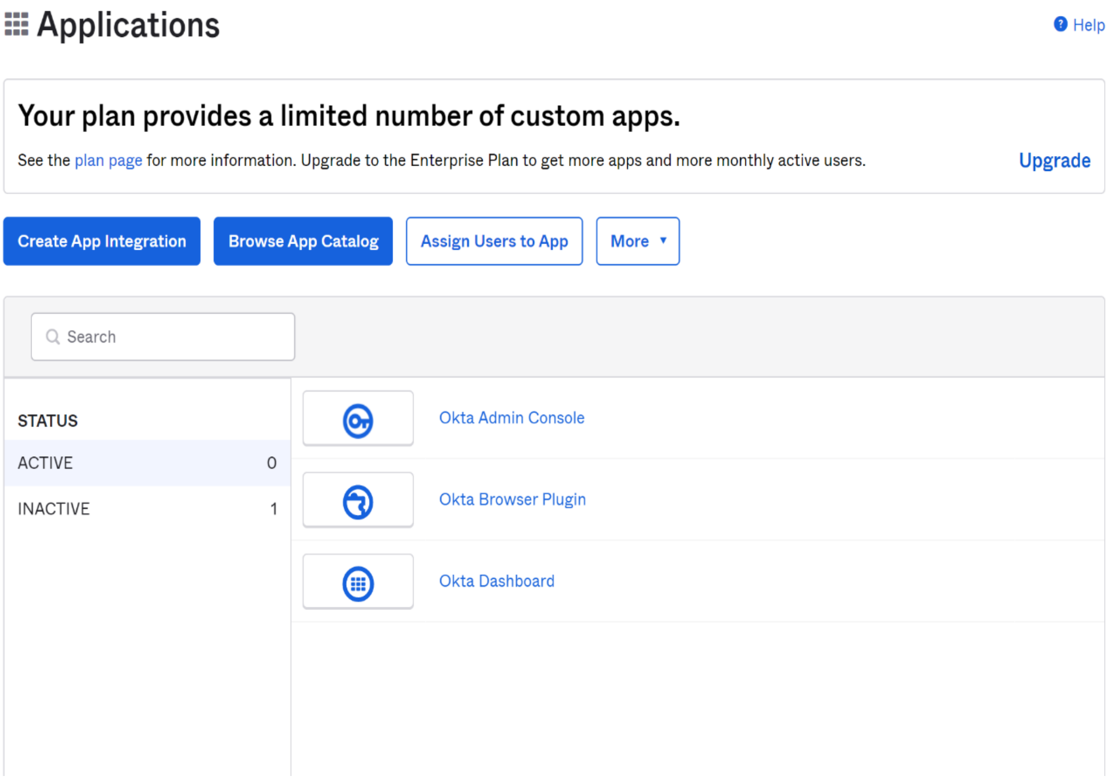
2. Create an API token

Use an API token to manage Okta resources.

3. Programmatically manage Okta resources

Use Okta Management SDKs in your server-side code to manage users, factors, groups, and more.

- Go to Applications → Applications in the left-hand side tab to open the list of applications in your organization, which should only contain the three default active apps.



Applications

Your plan provides a limited number of custom apps.

See the plan page for more information. Upgrade to the Enterprise Plan to get more apps and more monthly active users.

STATUS	
ACTIVE	0
INACTIVE	1

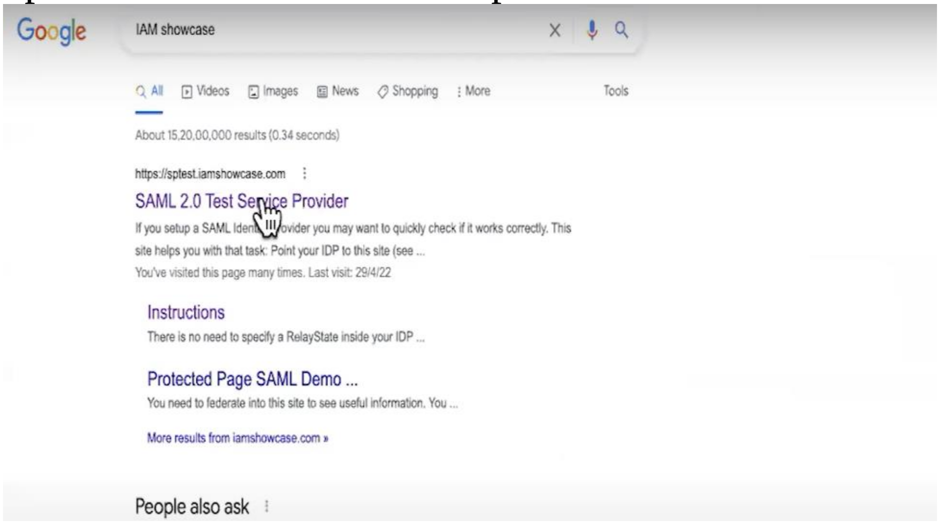
Okta Admin Console

Okta Browser Plugin

Okta Dashboard

Create a Dummy App(Metadata)

- Create a dummy application. For that go to IAM Showcase and open SAML 2.0 test service provider.



About 15,20,00,000 results (0.34 seconds)

https://sptest.iamshowcase.com

SAML 2.0 Test Service Provider

If you setup a SAML Identity Provider you may want to quickly check if it works correctly. This site helps you with that task: Point your IDP to this site (see ...

You've visited this page many times. Last visit: 29/4/22

Instructions

There is no need to specify a RelayState inside your IDP ...

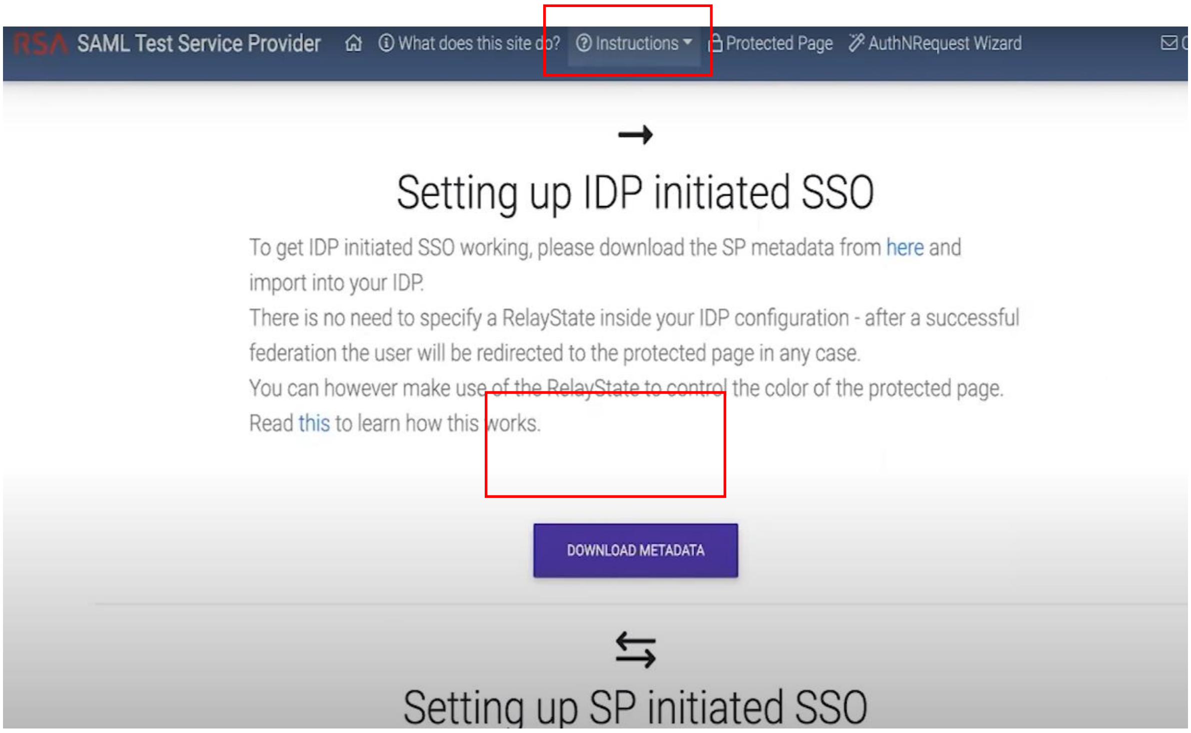
Protected Page SAML Demo ...

You need to federate into this site to see useful information. You ...

More results from iamshowcase.com »

People also ask

- Open instructions and click on download Metadata.



Setting up IDP initiated SSO

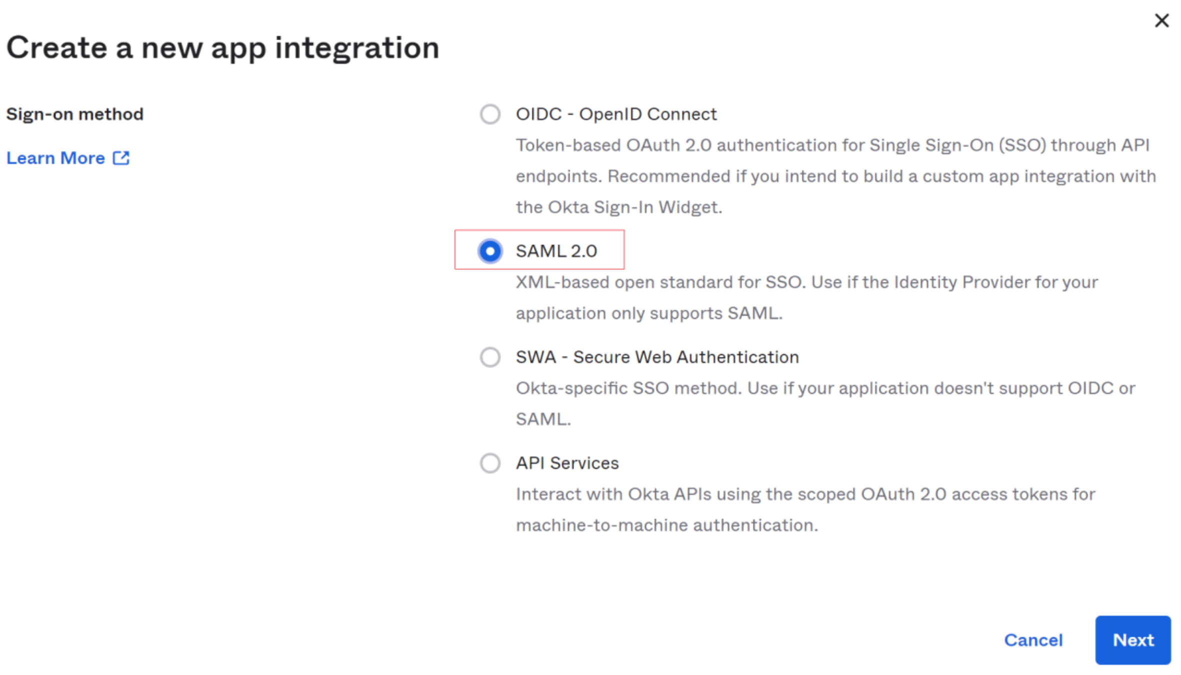
To get IDP initiated SSO working, please download the SP metadata from here and import into your IDP.
There is no need to specify a RelayState inside your IDP configuration - after a successful federation the user will be redirected to the protected page in any case.
You can however make use of the RelayState to control the color of the protected page.
Read this to learn how this works.

Setting up SP initiated SSO

- We need to create trust between our application and Okta

Create a Demo App

- From the same Okta Applications UI, select Create App Integration, choose SAML 2.0 for Sign-on method and click Next.



Create a new app integration

Sign-on method

Learn More

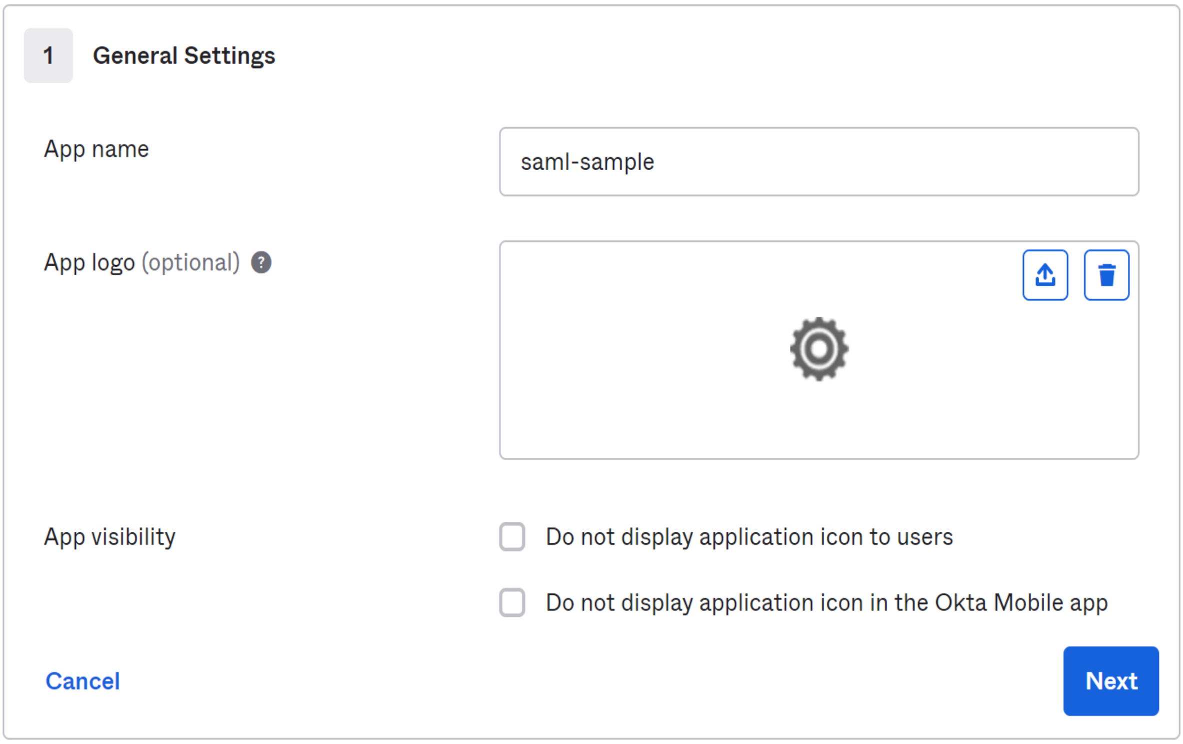
○ OIDC - OpenID Connect
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.

● 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 SAML.

○ API Services
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

- Set a name for your application and click Next.



1 General Settings

App name: saml-sample

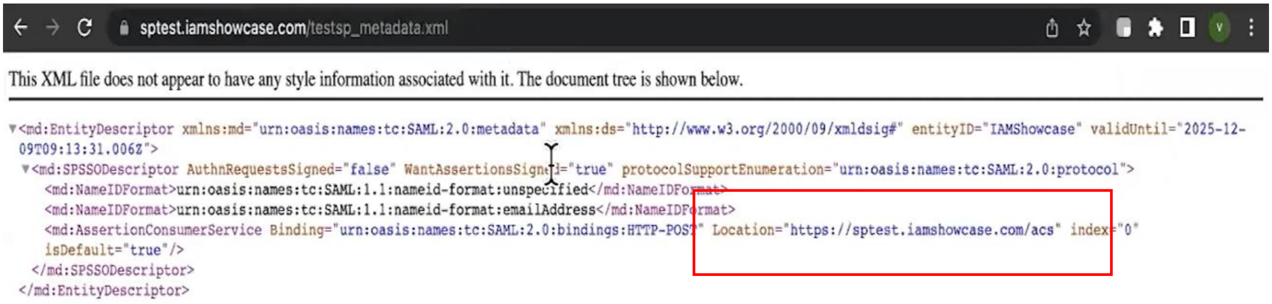
App logo (optional)

App visibility

□ Do not display application icon to users

□ Do not display application icon in the Okta Mobile app

- Now we need to add single sign on URL for that go to Metadata, where you will find the URL as mentioned below.

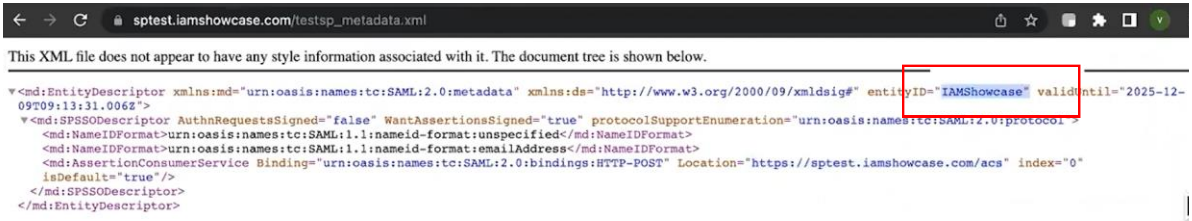


sptest.iamshowcase.com/testsp_metadata.xml

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" entityID="IAMShowcase" validUntil="2025-12-
 09T09:13:31.006Z">
  ▼<md:SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="true" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
     <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</md:NameIDFormat>
     <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</md:NameIDFormat>
     <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://sptest.iamshowcase.com/acs" index="0"
     isDefault="true"/>
   </md:SPSSODescriptor>
 </md:EntityDescriptor>
```

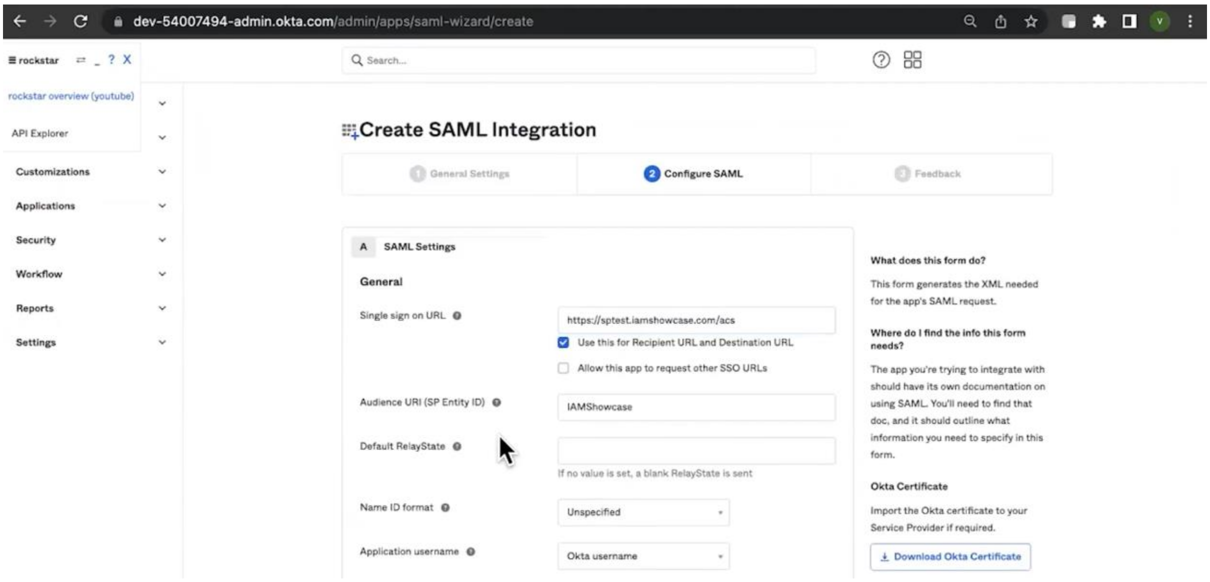
- Copy that URL and paste it in Single Sign On URL
- No similarly copy Entity Id from Metadata and paste it in Audience URI (SP Entity ID).



sptest.iamshowcase.com/testsp_metadata.xml

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" entityID="IAMShowcase" validUntil="2025-12-
 09T09:13:31.006Z">
  ▼<md:SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="true" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
     <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</md:NameIDFormat>
     <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</md:NameIDFormat>
     <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://sptest.iamshowcase.com/acs" index="0"
     isDefault="true"/>
   </md:SPSSODescriptor>
 </md:EntityDescriptor>
```



Create SAML Integration

A SAML Settings

General

Single sign on URL: https://sptest.iamshowcase.com/acs

☑ Use this for Recipient URL and Destination URL

☐ Allow this app to request other SSO URLs

Audience URI (SP Entity ID): IAMShowcase

Default RelayState:

If no value is set, a blank RelayState is sent

Name ID format: Unspecified

Application username: Okta username

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?

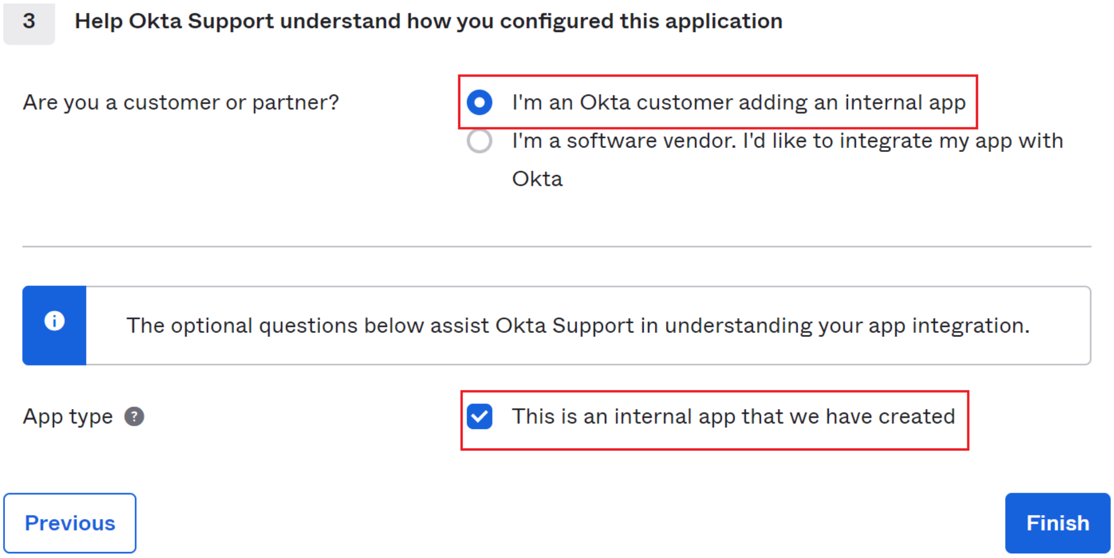
The app you're trying to integrate with should have its own documentation on using SAML. You'll need to find that doc, and it should outline what information you need to specify in this form.

Okta Certificate

Import the Okta certificate to your Service Provider if required.

Download Okta Certificate

- Click on next.
- Select I'm an Okta customer adding an internal app and This is an internal app that we have created for the next step and click Finish.



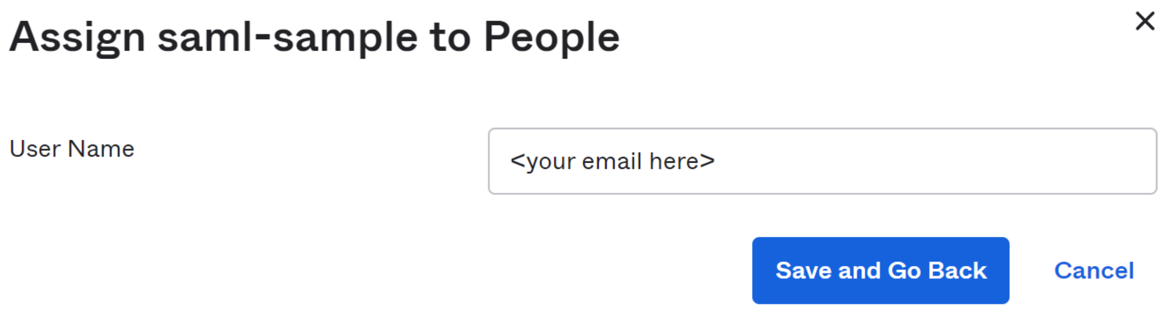
3 Help Okta Support understand how you configured this application

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

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

App type
☑ This is an internal app that we have created

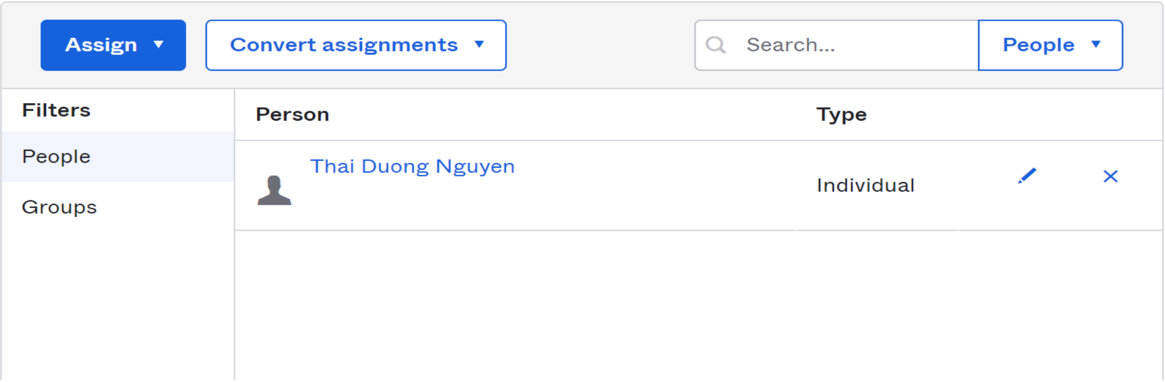
- Change to Assignments tab of your newly created app, click Assign → Assign to People to assign it to yourself.



Assign saml-sample to People

User Name <your email here>

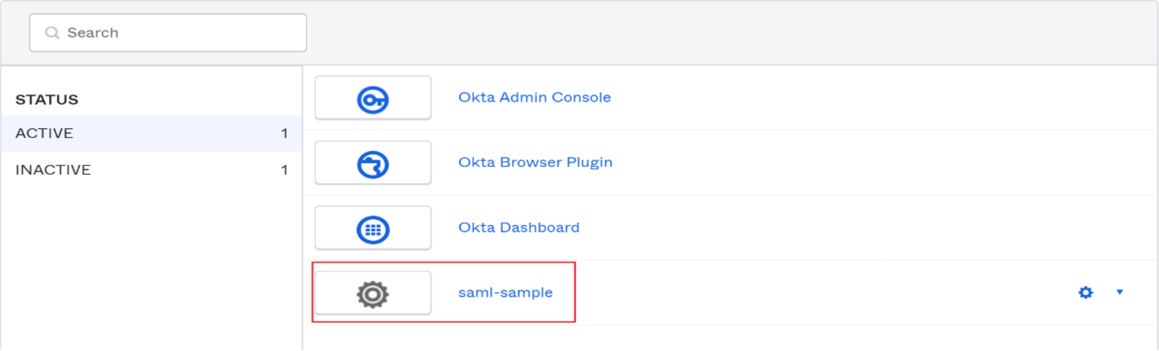
- You should be able to see your name in the list of people who have access to this app.



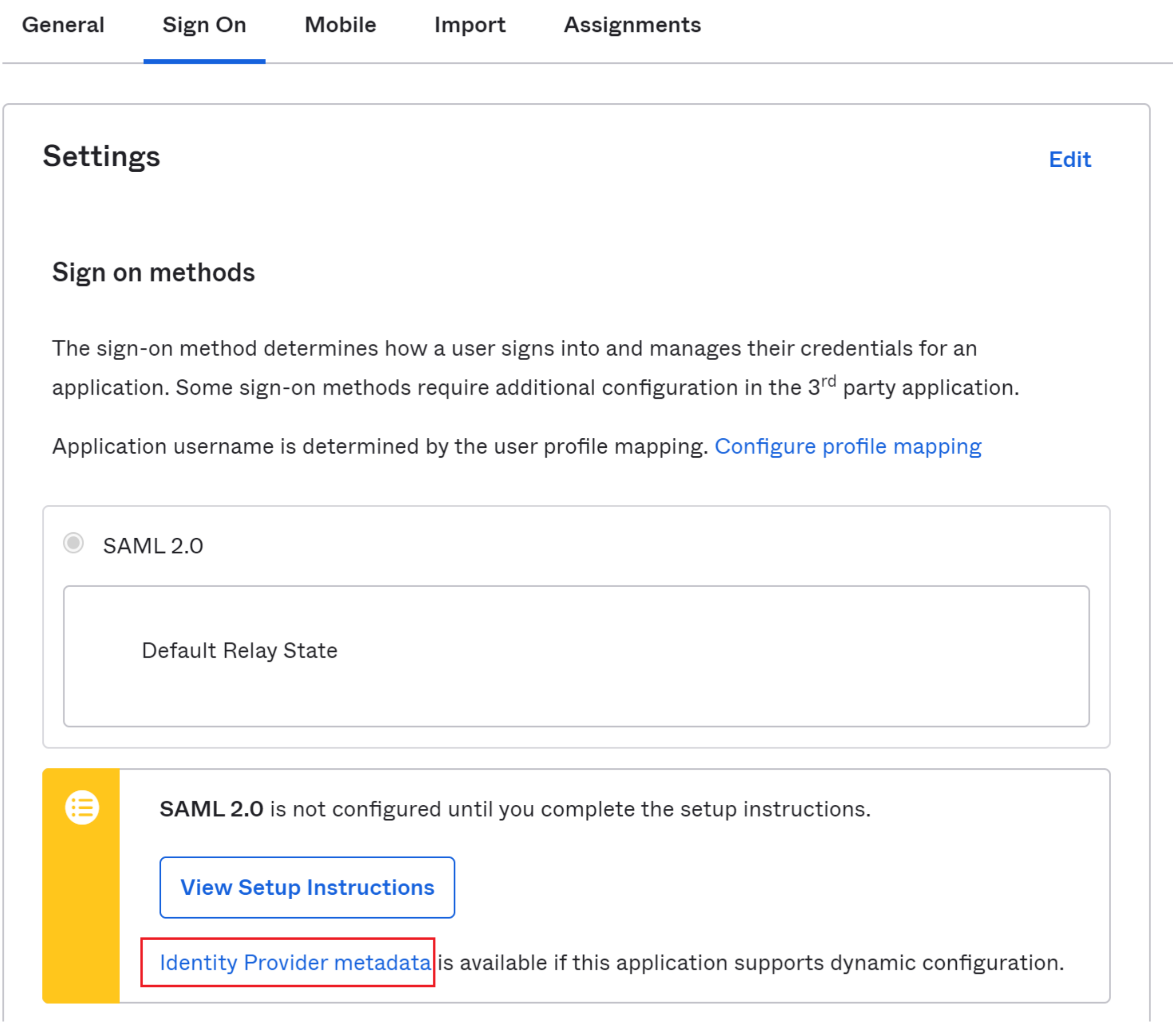
Person	Type
Thai Duong Nguyen	Individual

Get the necessary SAML information

- Select *SAML-sample* app from the list of applications.



- Switch to Sign On tab, click Identity Provider Metadata and copy its URL.



Sign on methods

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

Application username is determined by the user profile mapping. Configure profile mapping

○ SAML 2.0

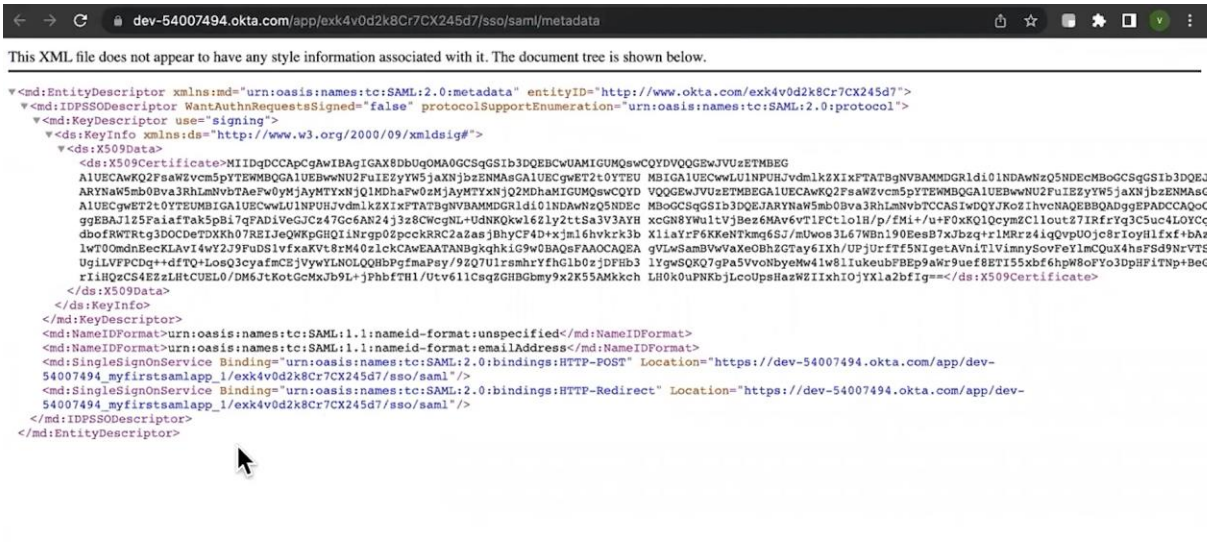
Default Relay State

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.

- This is the link to the metadata file we will use to integrate OKTA with our web app.

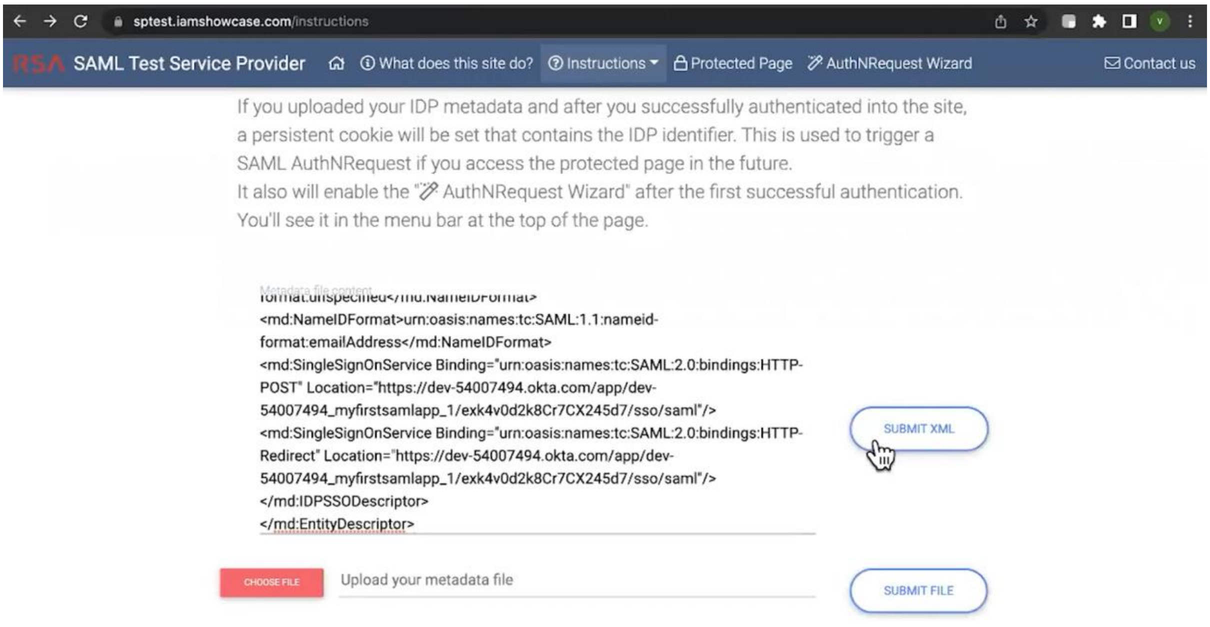


dev-54007494.okta.com/app/exk4v0d2k8Cr7CX245d7/sso/saml/metadata

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="http://www.okta.com/exk4v0d2k8Cr7CX245d7">
 ▼<md:IDPSSODescriptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
  ▼<md:KeyDescriptor use="signing">
   ▼<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    ▼<ds:X509Data>
      <ds:X509Certificate>MIIDqDCCApCgAwIBAgIGAX8DbUqOMA0GCSqGSIb3DQEBCwUAMIGUMQswCQYDVQQGEwJVUzETMBEG
      A1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YTEU MBIGA1UECwwLU1NPUHJvdmlkZXIxFTATBgNVBAMMDGRldi01NDAwNzQ5NDEcMBoGCSqGSIb3DQEJ
      ARYNaW5mb0Bva3RhLmNvbTAeFw0yMjAyMTYxNjQ1MDhaFw0zMjAyMTYxNjQ2MDhaMIGUMQswCQYD VQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsG
      A1UECgwET2t0YTEUMBIGA1UECwwLU1NPUHJvdmlkZXIxFTATBgNVBAMMDGRldi01NDAwNzQ5NDEc MBoGCSqGSIb3DQEJARYNaW5mb0Bva3RhLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
      ggEBAJ1Z5FaiafTak5pBi7qFADiVeGJCz47Gc6AN24j3z8CWcgNL+UdNKQkwl6Zly2ttSa3V3AYH xcGN8YWultVjBez6MAv6vT1FCtlolH/p/fMi+/u+F0xKQ1QcymZC1loutZ7IRfrYq3C5uc4LOYCq
      dbofRWTRtg3DOCDeTDXKh07REIJeQWKpGHQIiNrgp0ZpcckRRC2aZasjBhyCF4D+xjml6hvkrk3b XliaYrF6KKeNTkmq6SJ/mUwos3L67WBn190EesB7xJbzq+r1MRrz4iqQvpUOjc8rIoyHlfxf+bAz
      lwT0OmdnEecKLAvI4wY2J9FuDSlvfxaKVt8rM40zlckCAwEAATANBgkqhkiG9w0BAQsFAAOCAQEA gVLwSamBVwVaXeOBhZGTay6IXh/UPjUrfTf5NIgetAVniTlVimnySovFeYlmCQuX4hsFSd9NrVTS
      UgiLVFPCDq++dfTQ+LosQ3cyafmCEjVywYLNOLQQHbPgfmaPsy/9ZQ7UlrsmhrYfhGlb0zjDFHb3 lYgwSQKQ7gPa5VvoNbyeMw41w8lIukeubFBEp9aWr9uef8ETI55xbf6hpW8oFYo3DpHFiTNp+BeG
      rIiHQzCS4EZzLHtCUEL0/DM6JtKotGcMxJb9L+jPhbfTH1/Utv611CsqZGHBGbmy9x2K55AMkkch LH0k0uPNKbjLcoUpsHazWZIIxhIOjYXla2bfIg==</ds:X509Certificate>
    </ds:X509Data>
   </ds:KeyInfo>
  </md:KeyDescriptor>
  <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</md:NameIDFormat>
  <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</md:NameIDFormat>
  <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://dev-54007494.okta.com/app/dev-
  54007494_myfirstsamlapp_1/exk4v0d2k8Cr7CX245d7/sso/saml"/>
  <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://dev-54007494.okta.com/app/dev-
  54007494_myfirstsamlapp_1/exk4v0d2k8Cr7CX245d7/sso/saml"/>
 </md:IDPSSODescriptor>
</md:EntityDescriptor>
```

- Copy this Metadata URL and scroll below in Metadata instruction page and paste it in metadata file content. And hit Submit XML

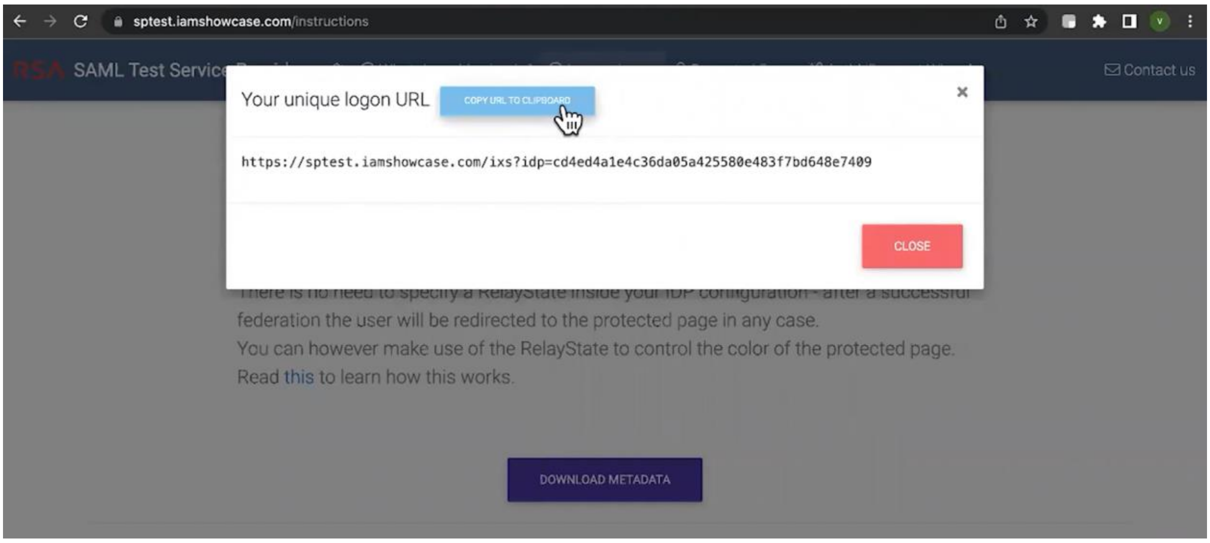


If you uploaded your IDP metadata and after you successfully authenticated into the site, a persistent cookie will be set that contains the IDP identifier. This is used to trigger a SAML AuthNRequest if you access the protected page in the future.
It also will enable the "AuthNRequest Wizard" after the first successful authentication.
You'll see it in the menu bar at the top of the page.

Metadata file content

```
format:unspecified</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-
format:emailAddress</md:NameIDFormat>
<md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
POST" Location="https://dev-54007494.okta.com/app/dev-
54007494_myfirstsamlapp_1/exk4v0d2k8Cr7CX245d7/sso/saml"/>
<md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
Redirect" Location="https://dev-54007494.okta.com/app/dev-
54007494_myfirstsamlapp_1/exk4v0d2k8Cr7CX245d7/sso/saml"/>
</md:IDPSSODescriptor>
</md:EntityDescriptor>
```

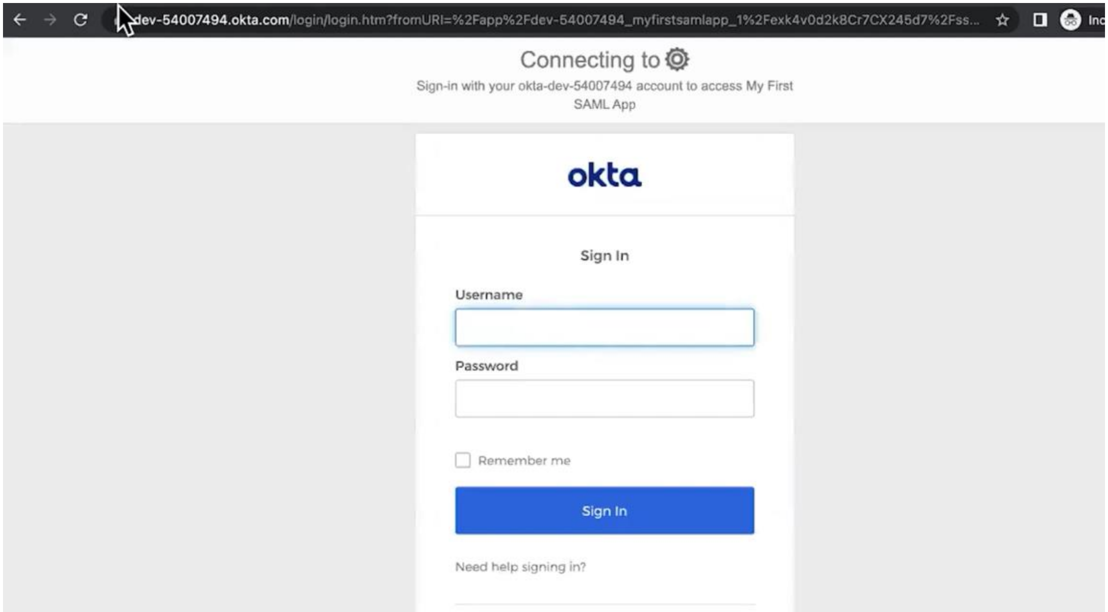
- You will get a URL which the application has provided to you.
- Copy that URL paste it in New Incognito Window



```
https://sptest.iamshowcase.com/ixs?idp=cd4ed4a1e4c36da05a425580e483f7bd648e7409
```

There is no need to specify a RelayState inside your IDP configuration - after a successful federation the user will be redirected to the protected page in any case.
You can however make use of the RelayState to control the color of the protected page.
Read this to learn how this works.

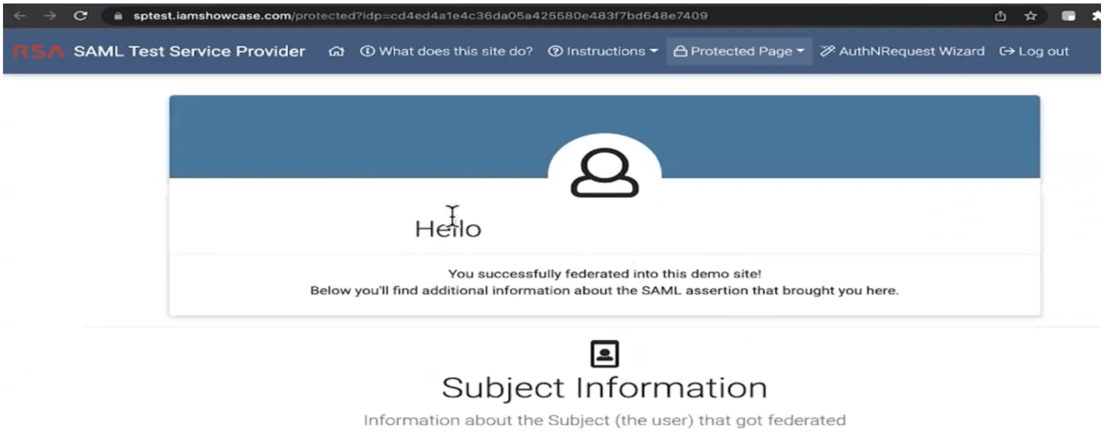
- Copy that URL paste it in New Incognito Window.



dev-54007494.okta.com/login/login.htm?fromURI=%2Fapp%2Fdev-54007494_myfirstsamlapp_1%2Fexk4v0d2k8Cr7CX245d7%2Fss...
Connecting to
okta
Sign In
Username
Password
Remember me
Sign In
Need help signing in?

Sign-in with your okta-dev-54007494 account to access My First SAML App

- You will get redirected to Okta. Once the authentication is done you will be redirected to application.
- Click on View Setup Instructions, on the next screen, note down the value in Identity Provider Issuer field.

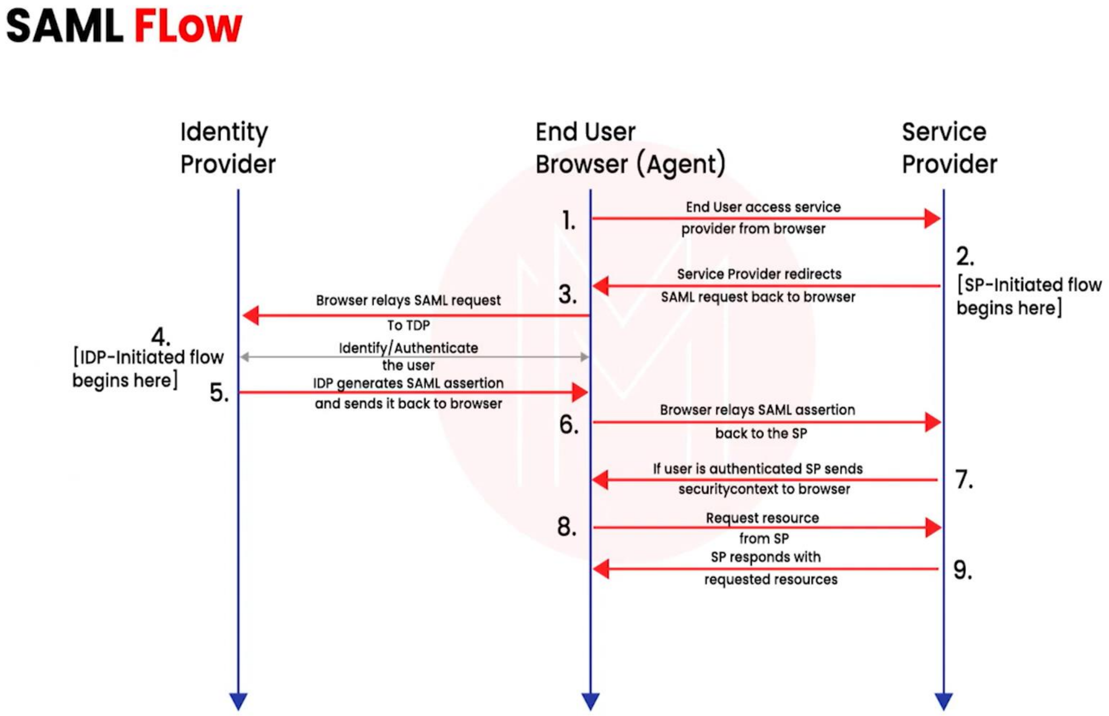


sptest.iamshowcase.com/protected?idp=cd4ed4a1e4c36da05a425580e483f7bd648e7409
SAML Test Service Provider
What does this site do?
Instructions
Protected Page
AuthNRequest Wizard
Log out
Hello
Subject Information

You successfully federated into this demo site!
Below you'll find additional information about the SAML assertion that brought you here.

Information about the Subject (the user) that got federated

SAML Flow


SAML FLow
Identity Provider
End User Browser (Agent)
Service Provider
1.
End User access service provider from browser
2.
[SP-Initiated flow begins here]
Service Provider redirects SAML request back to browser
3.
Browser relays SAML request To TDP
4.
[IDP-Initiated flow begins here]
Identify/Authenticate the user
5.
IDP generates SAML assertion and sends it back to browser
6.
Browser relays SAML assertion back to the SP
7.
If user is authenticated SP sends securitycontext to browser
8.
Request resource from SP
9.
SP responds with requested resources

- We want to access the service provider on any application so as an end user we go to the browser and hit the url of the application.
- Now if we are going to the link of application that means we are going to step 2. And from there our SP Initiate flow is going to begin.
- From service provider it will redirect the SAML request back to the browser & from the browser, browser will relay SAML request to the identity provider as SAML is going to authenticate the user.
- In SP Initiate flow there is always redirection from this service provider to the identity provider.
- In this place our IDP-Initiated flow will begin. IDP will identify and authenticate the user. Once the identity provider is satisfied it will generate a SAML assertion.

- SAML assertion is being generated and is sent back to the browser. Now browser has got nothing to do with the assertion because browser cannot consume that assertion. So, it will got to the service provider.
- At service provider it will check, it will pass decrypt the search. It will decrypt because service provider has some of the information which okta has already provided, or the identity provider is already provided. It is happening because there was a metadata exchange between the service provider and the identity provider.
- If the user is authenticated service provider sends the security context to the browser. From the browser it requests resource from the service provider and then requested resource is being granted to the user.
- For IDP-Initiated flow we don’t have 1,2,3 steps, it will directly flow from Step 4 to Step 9.
- For SP -Initiated flow we have 1,2,3 steps.
- There is no comparison between these two flows. It is based on requirement of the application team.