ComponentSpace SAML for ASP.NET OneLogin Integration Guide

Copyright © ComponentSpace Pty Ltd 2004-2025. All rights reserved.
www.componentspace.com

Contents

Introduction 1
Adding a SAML Application 1
Adding User Access 5
Service Provider Configuration 8
SP-Initiated SSO 9
IdP-Initiated SSO 11
SAML Logout 13

Introduction

This document describes integration with OneLogin as the identity provider.

For information on configuring OneLogin for SAML SSO, refer to the following article.

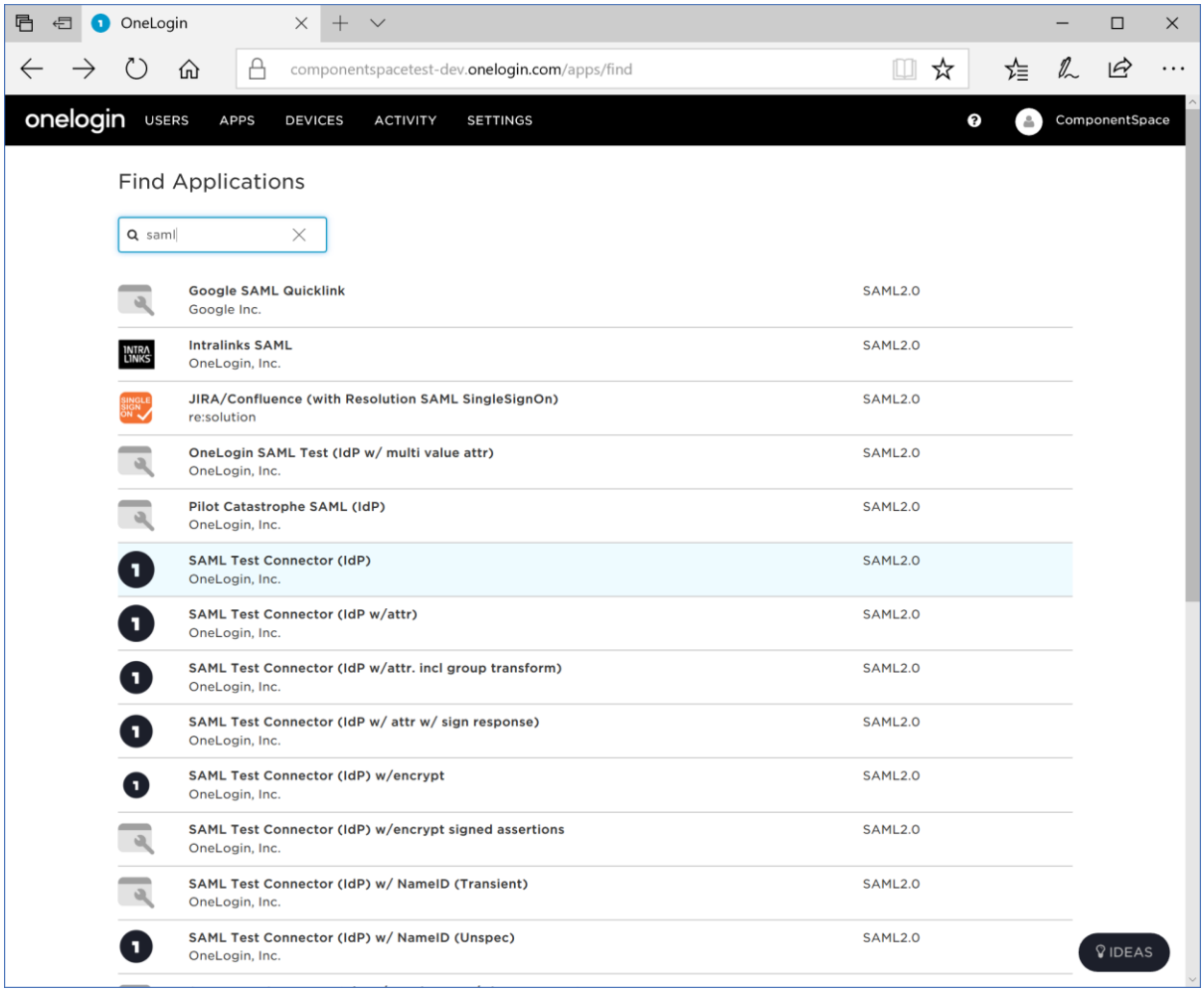
https://support.onelogin.com/hc/en-us/articles/115003638343-Configuring-SSO-for-SAML-enabled-Apps

Adding a SAML Application

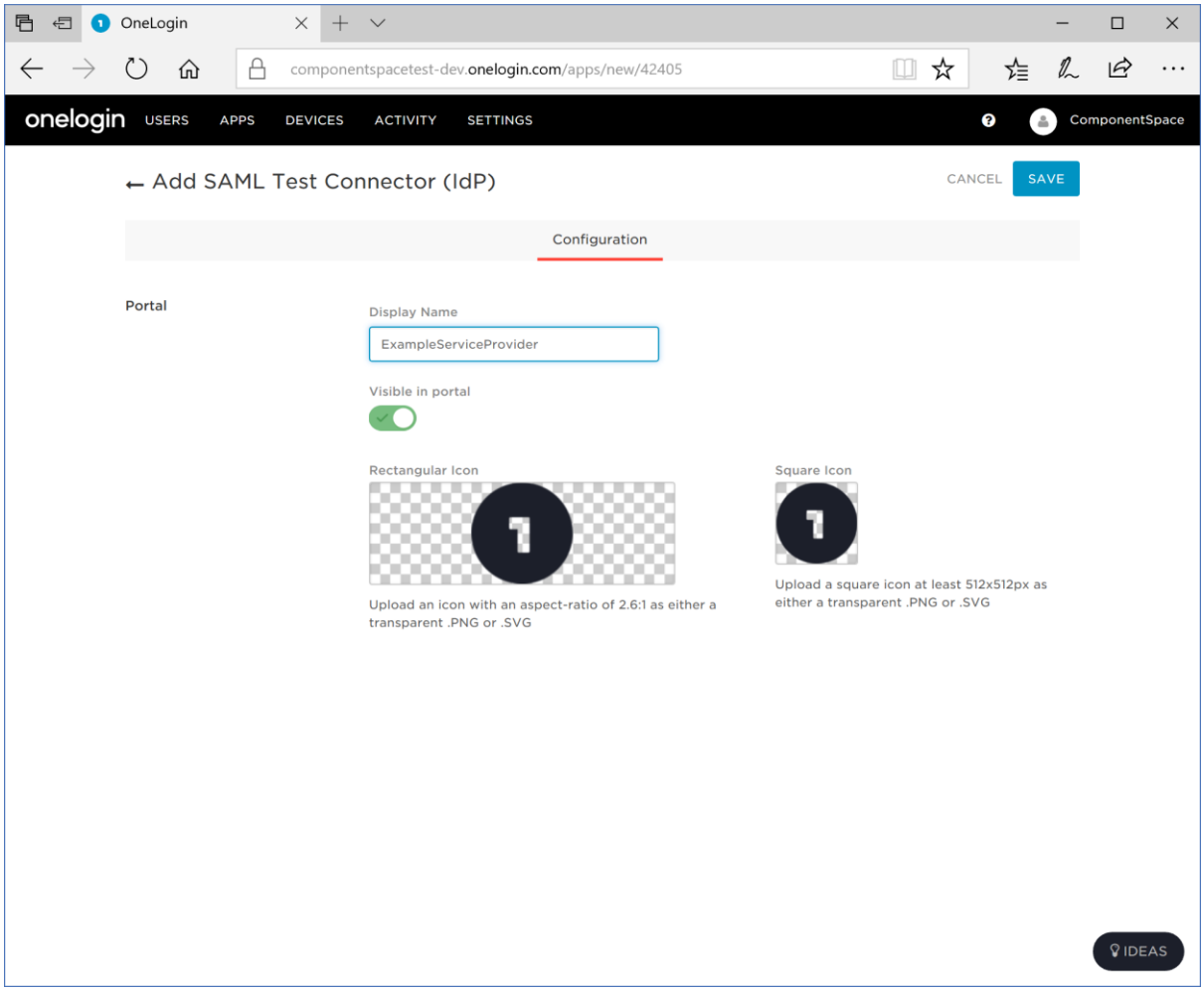
Login into OneLogin as an administrator.

Click Apps and then Add Apps.

Search for SAML and select the SAML Test Connector (IdP).



Set the display name to ExampleServiceProvider and click the Save button.



Click the Configuration link.

Relay state is not required.

Set the audience to the name of the service provider.

For example:

https:// ExampleServiceProvider

Set the Recipient, ACS URL and validator to the assertion consumer service endpoint URL.

For example:

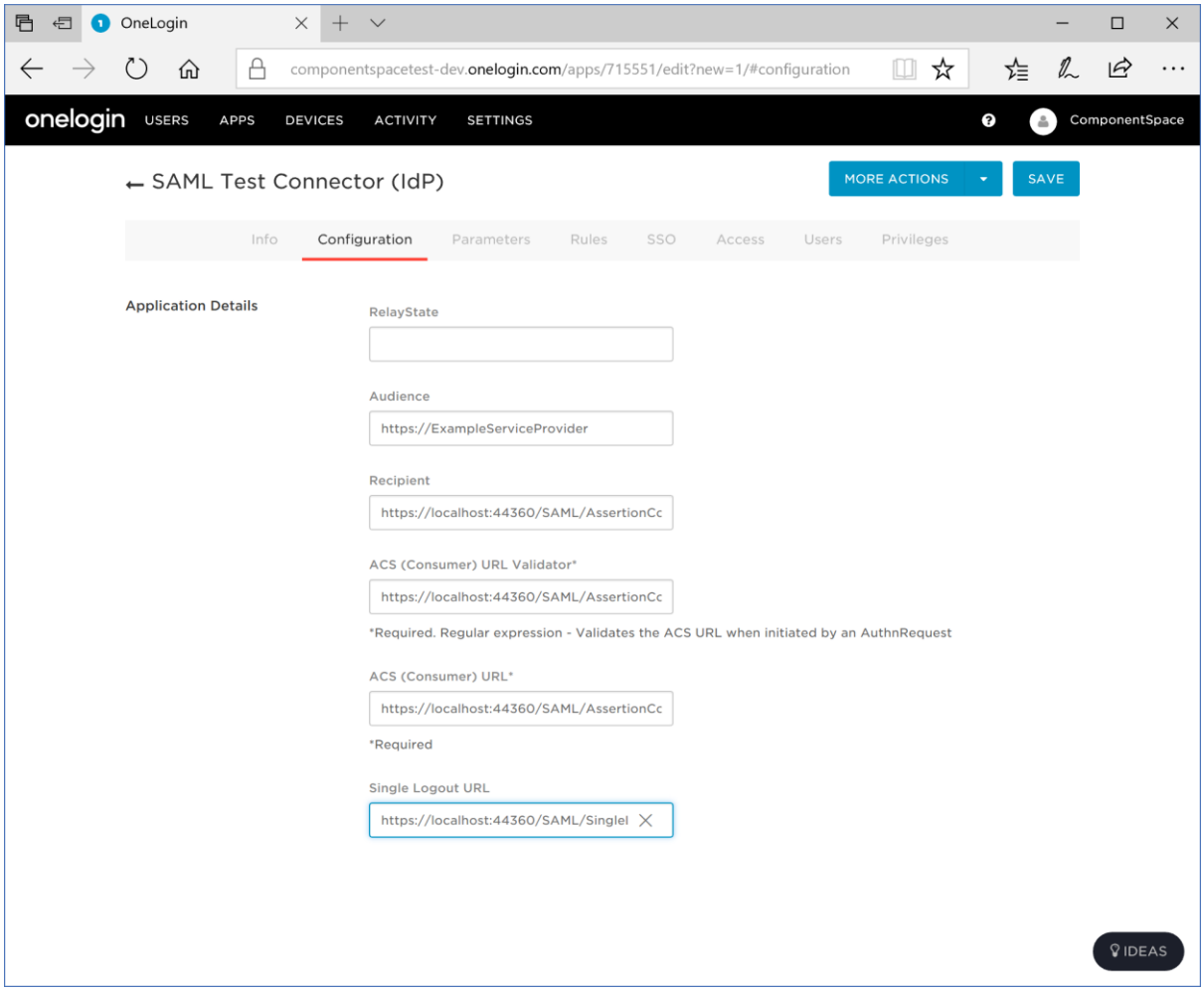
https://localhost:44360/SAML/AssertionConsumerService

Set the logout.

For example:

https://localhost:44360/SAML/SingleLogoutService

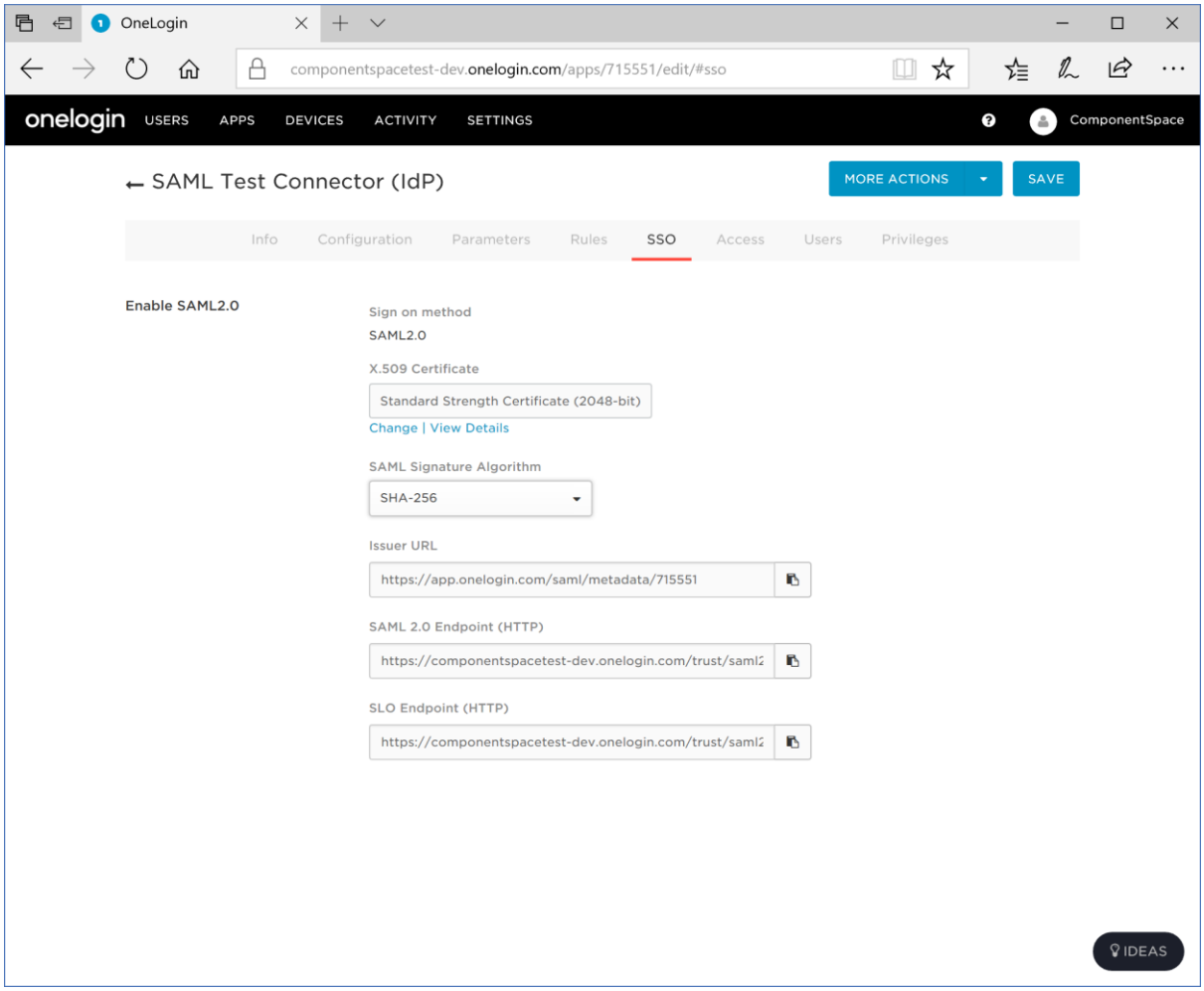
Click the Save button.



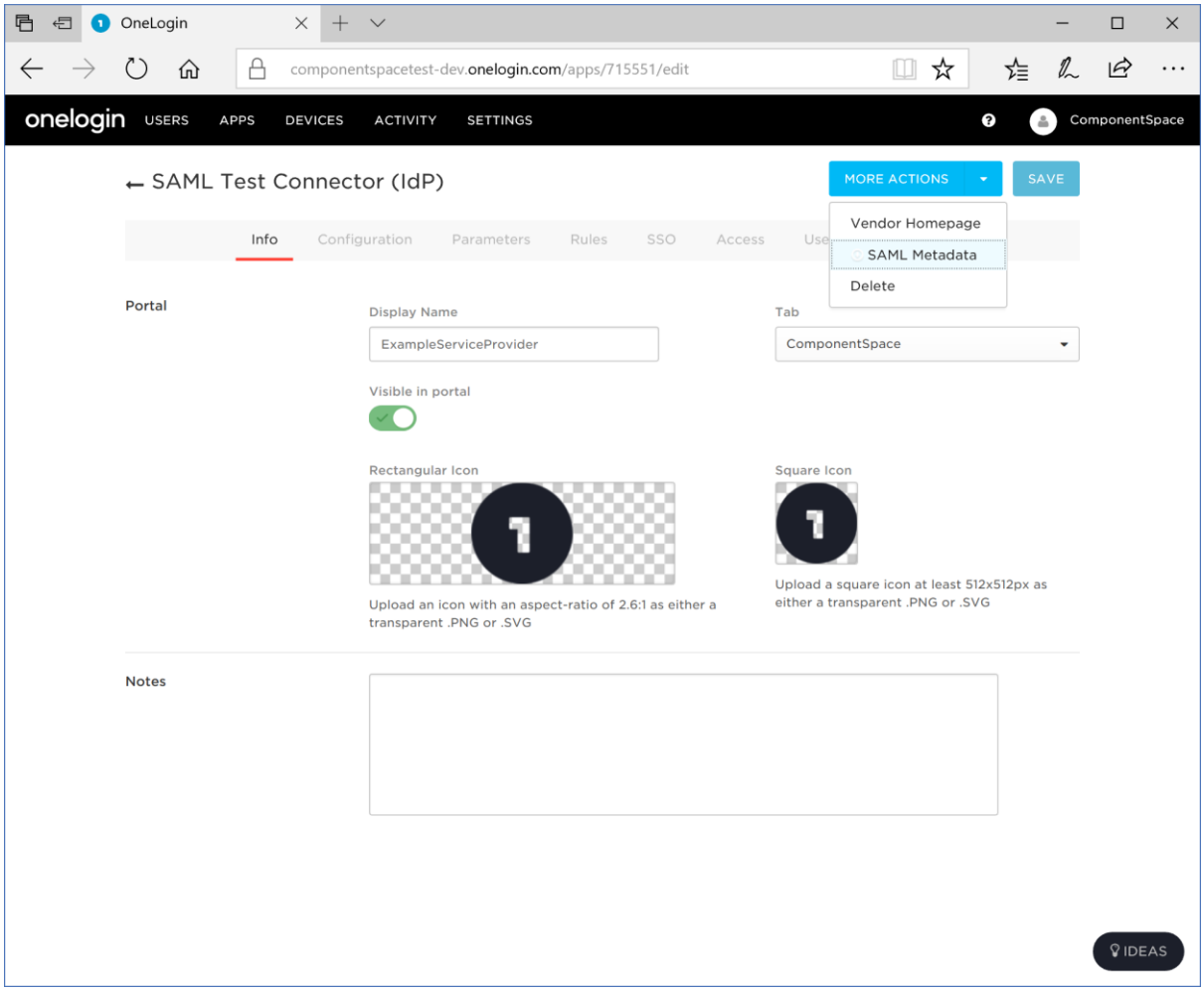
Click the SSO link.

Select SHA-256 as the signature algorithm.

Click the Save button.



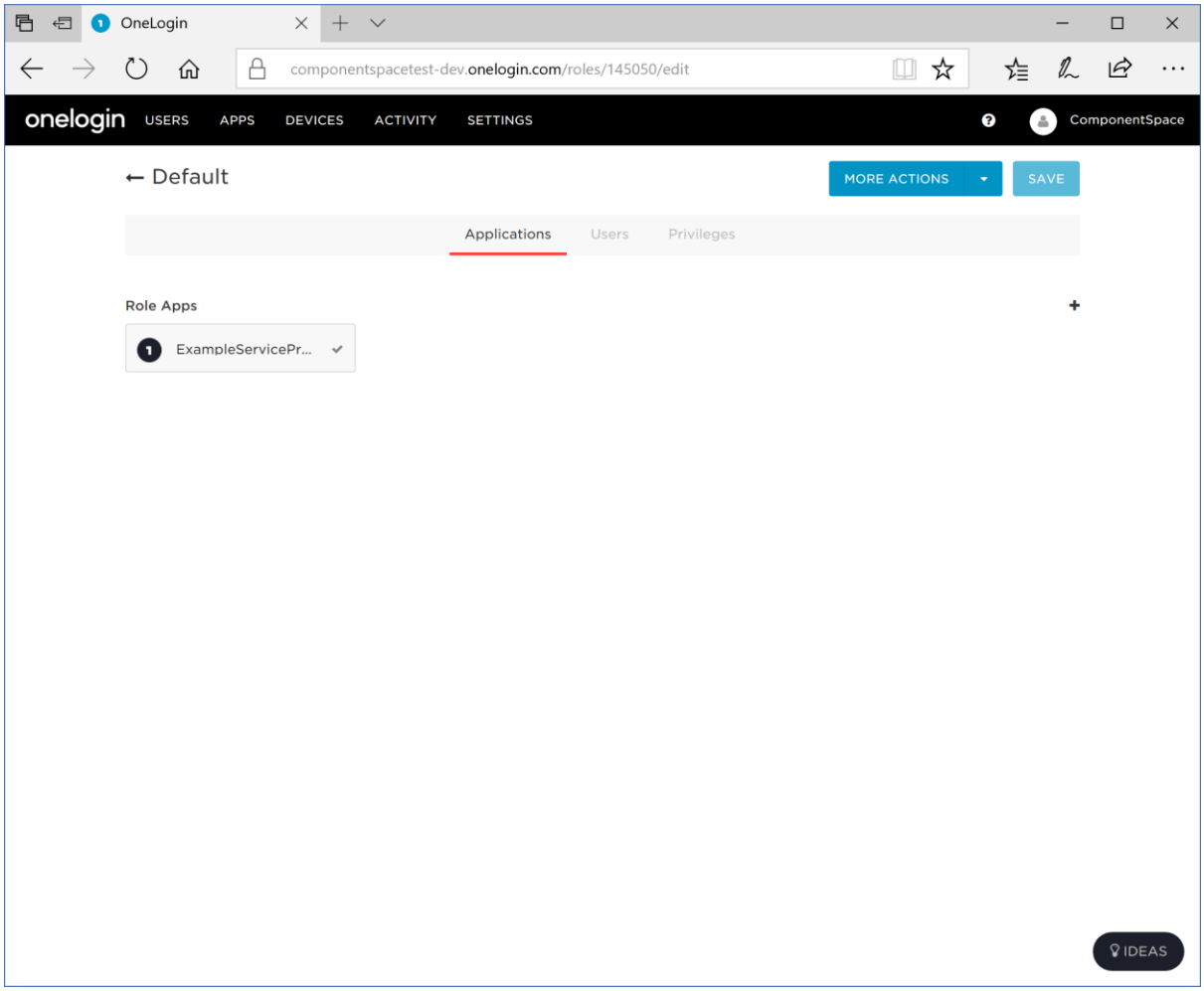
Click the More Actions and then SAML Metadata to download the identity provider metadata. This information will be used to configure the service provider.



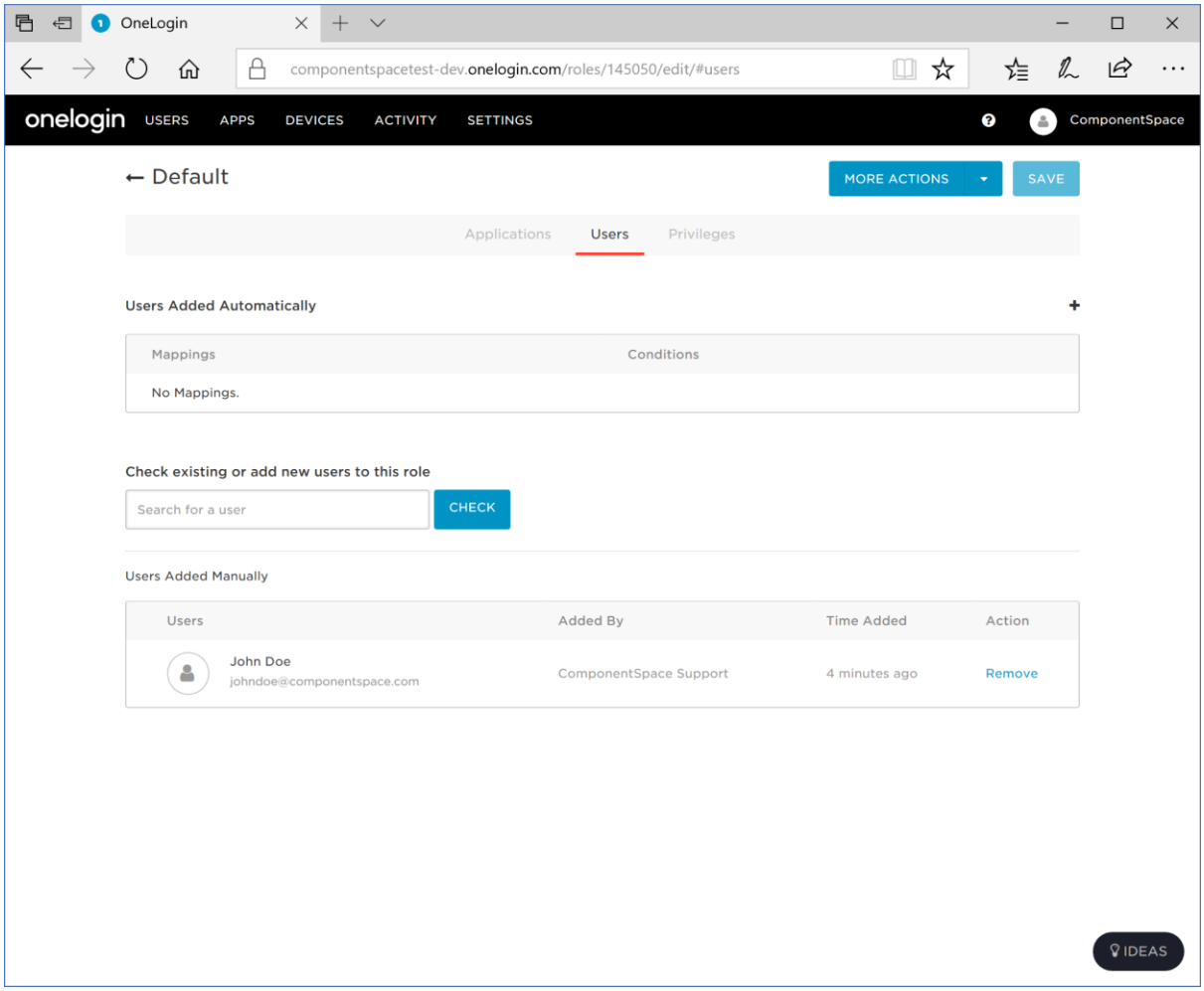
Adding User Access

Select Users and then Roles.

Edit the default role and add ExampleServiceProvider as an application.

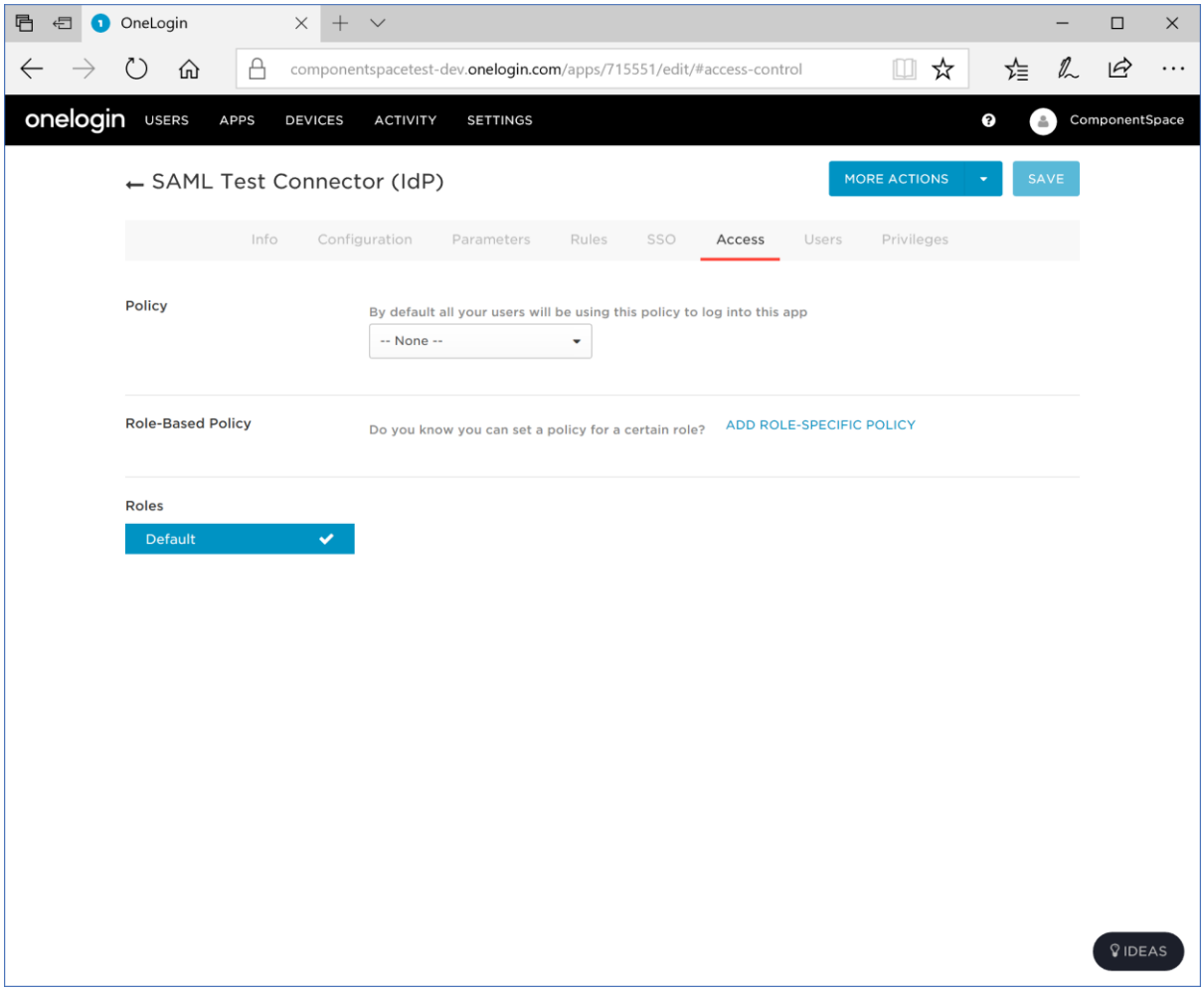


Add users to the role and save the changes.



Return to the application configuration and select the access tab.

Ensure the default role is enabled.



Select the users tab and confirm the appropriate users are listed.

Service Provider Configuration

The following partner identity provider configuration is included in the example service provider's SAML configuration.

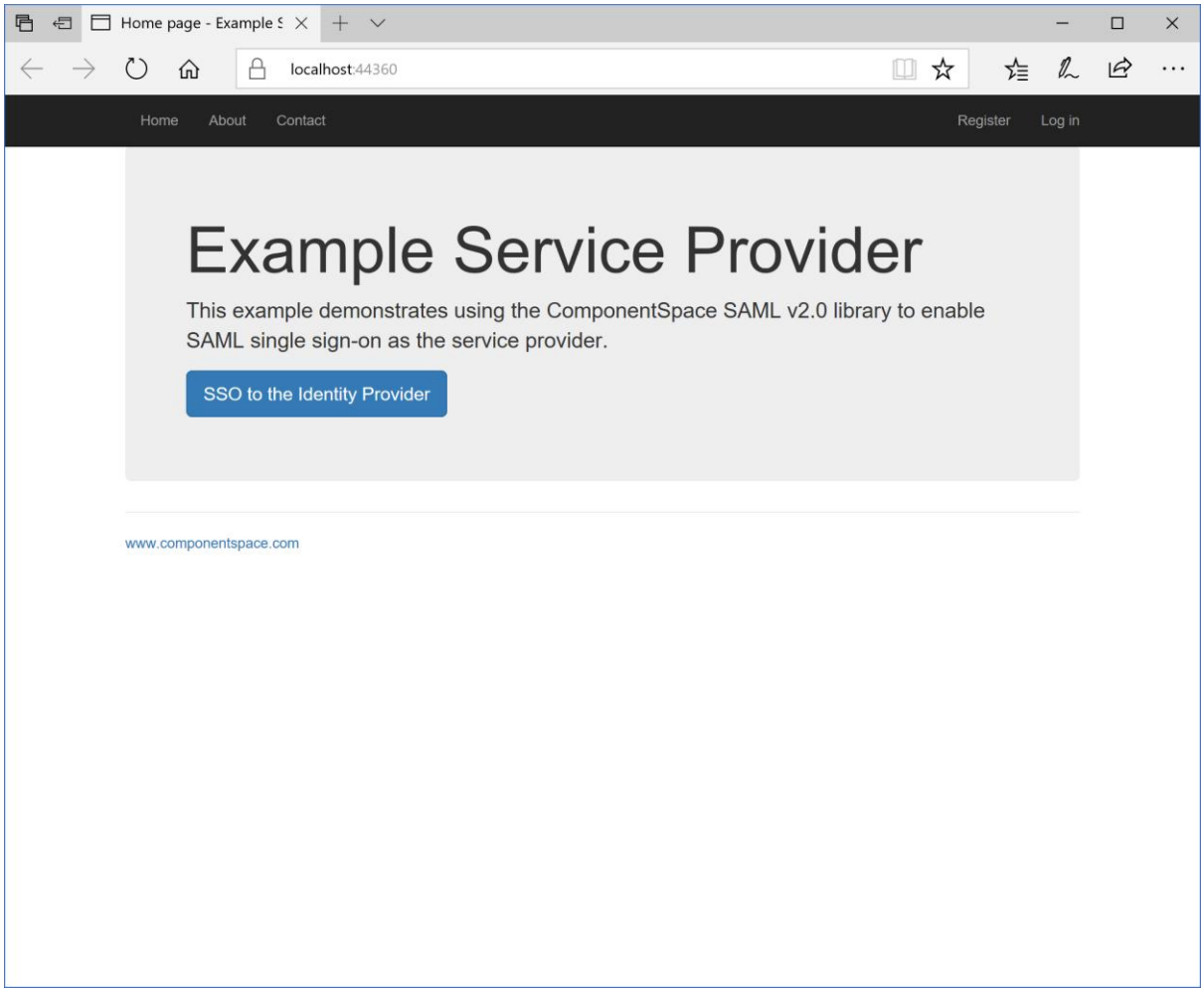
```
<PartnerIdentityProvider
 Name="https://app.onelogin.com/saml/metadata/715551"
 Description="OneLogin"
 SingleSignOnServiceUrl="https://componentspacetest-dev.onelogin.com/trust/saml2/http-post/sso/715551"
 SingleLogoutServiceUrl="https://componentspacetest-dev.onelogin.com/trust/saml2/http-redirect/slo/715551">
 <PartnerCertificates>
  <Certificate FileName="Certificates\onelogin.cer"/>
 </PartnerCertificates>
</PartnerIdentityProvider>
```

Ensure the PartnerName specifies the correct partner identity provider.

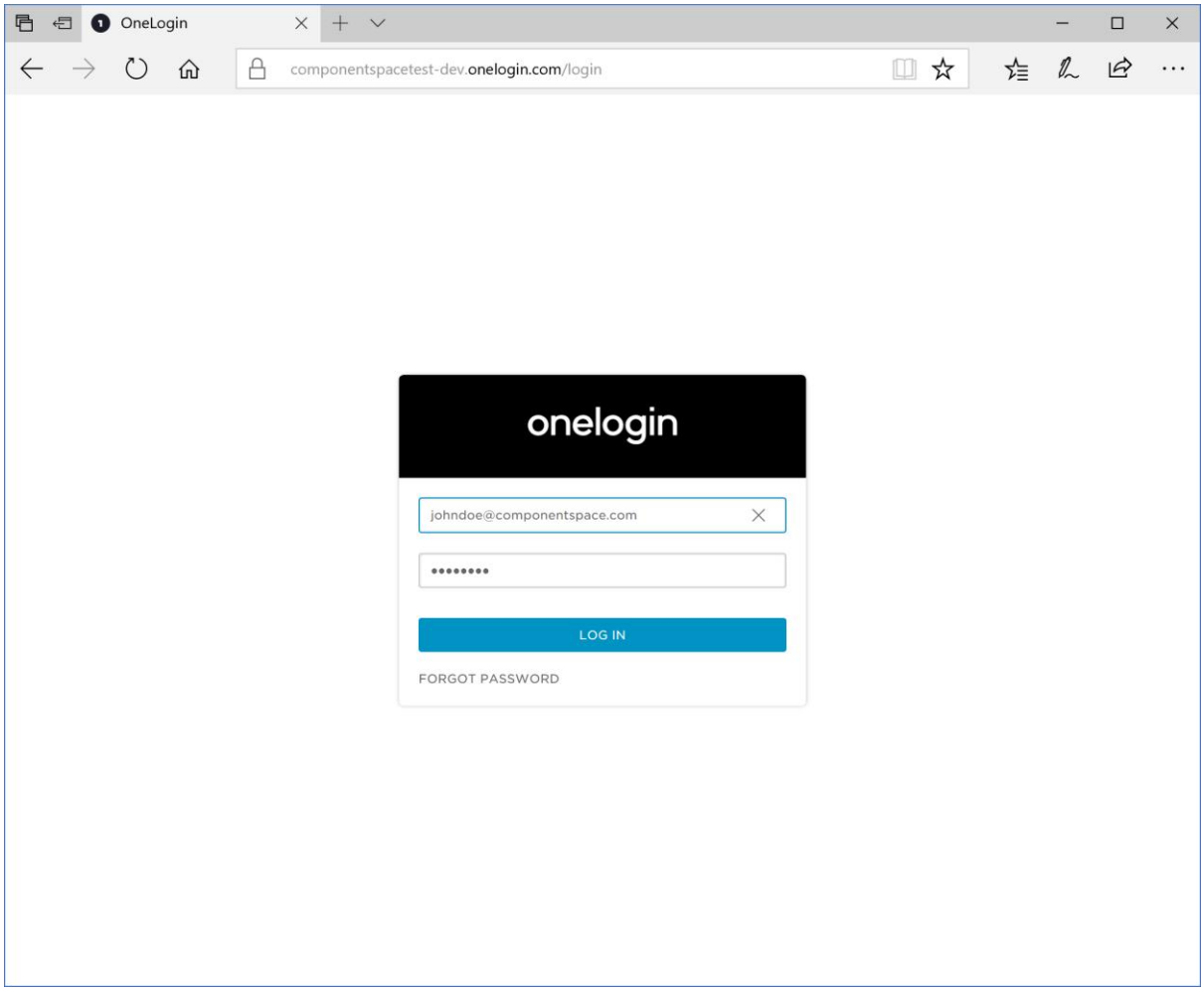
```
<add key="PartnerName" value="https://app.onelogin.com/saml/metadata/715551"/>
```

SP-Initiated SSO

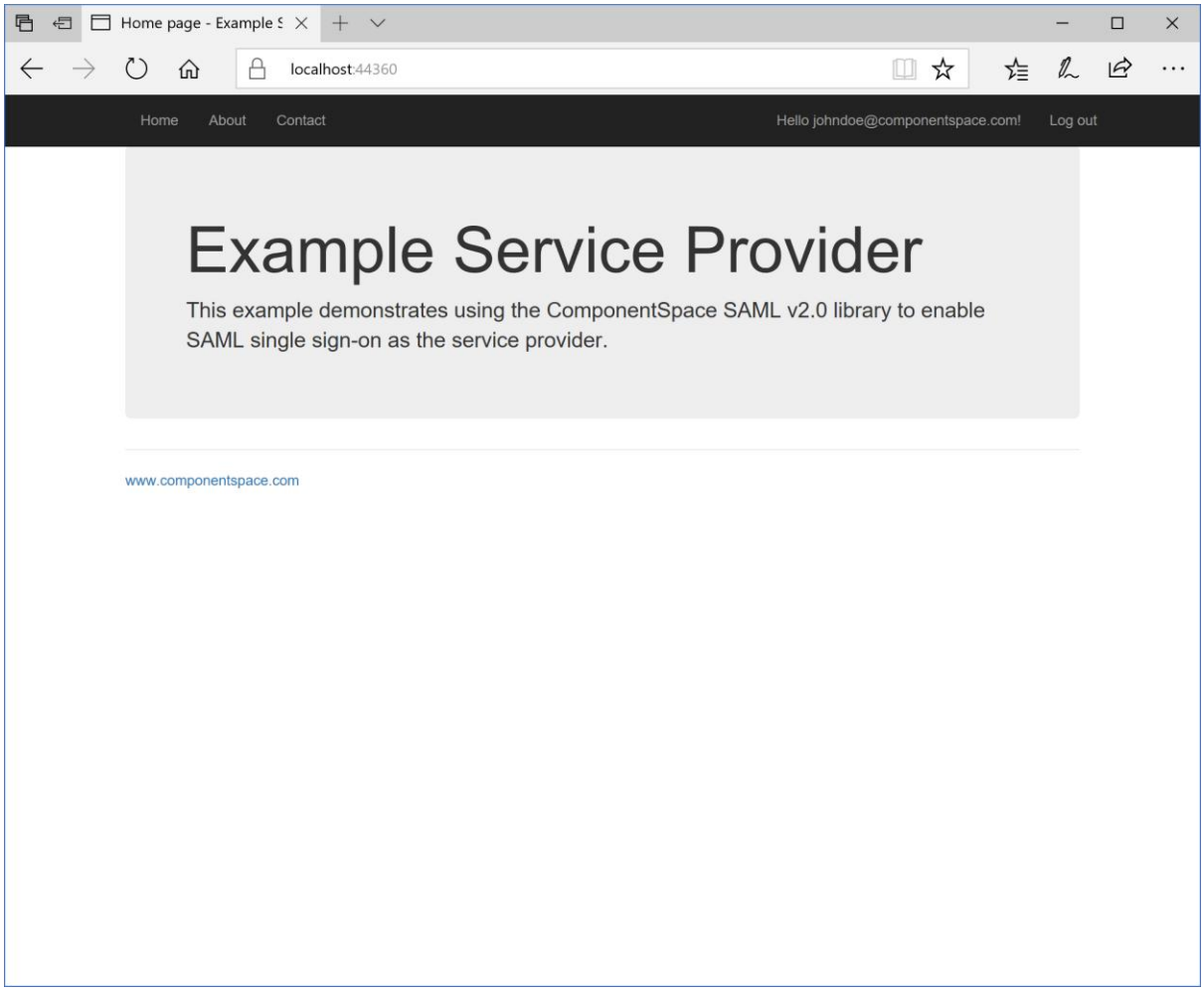
Browse to the example service provider and click the button to SSO to the identity provider.



Log into OneLogin.



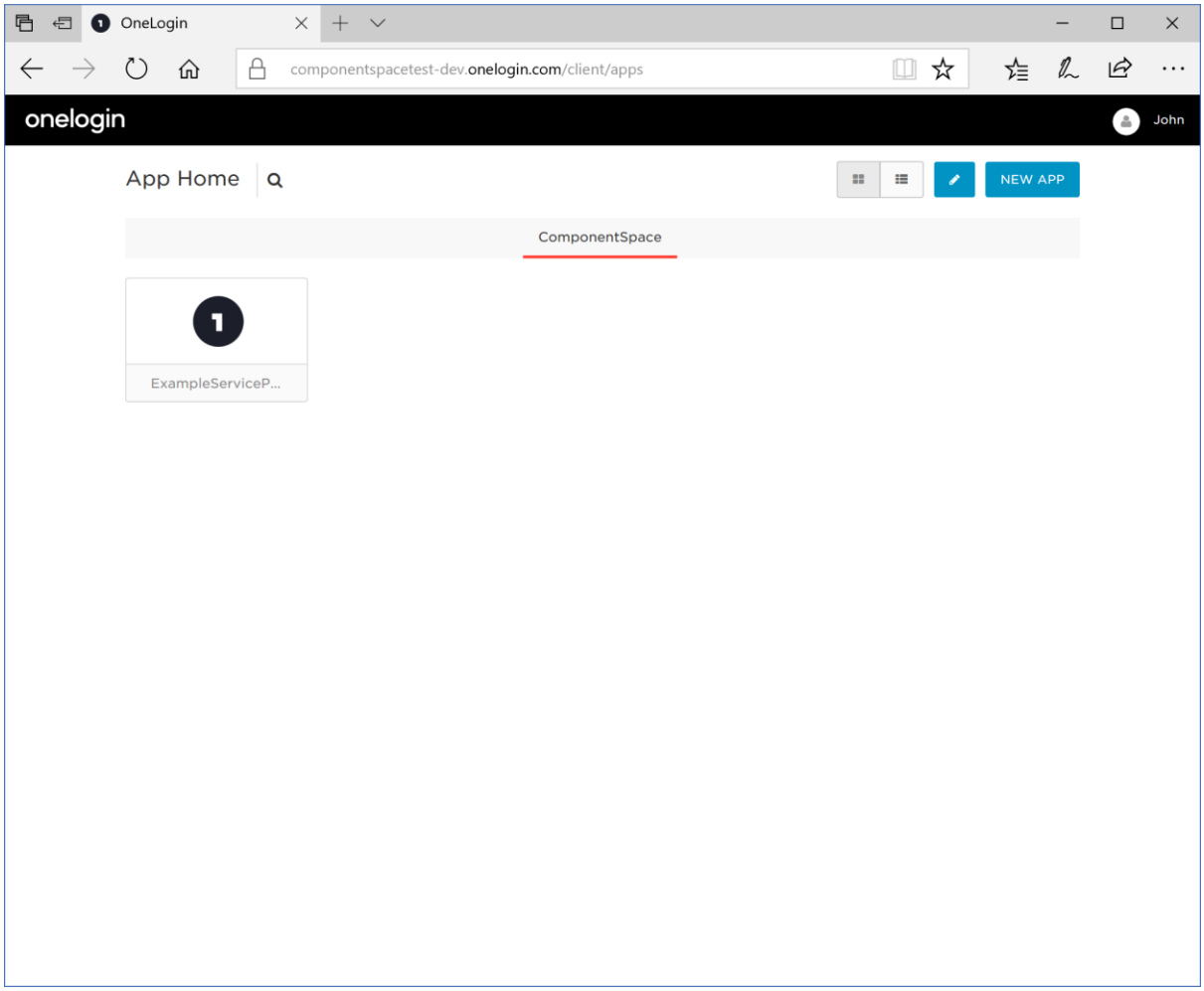
The user is automatically logged in at the service provider.



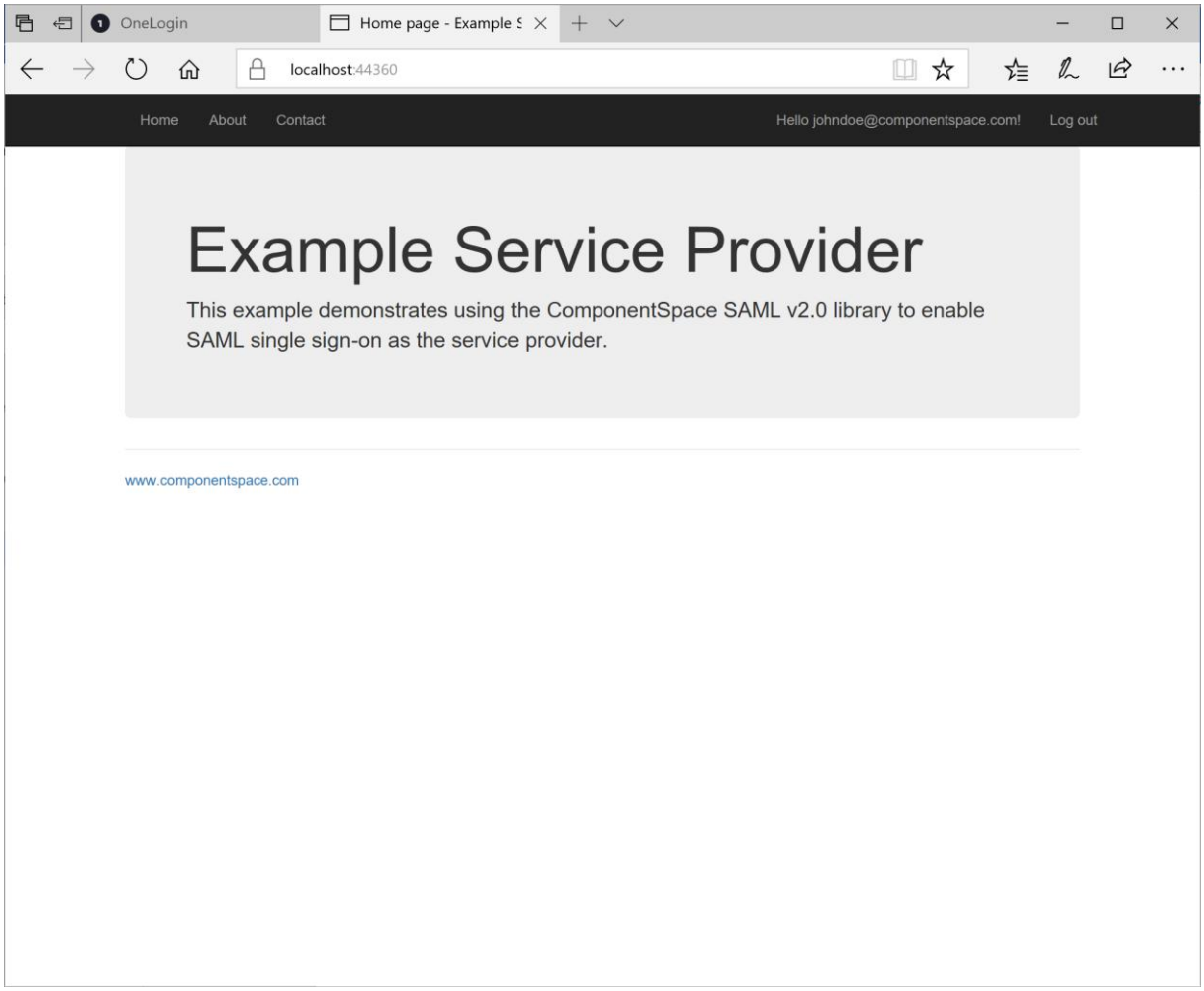
IdP-Initiated SSO

Log into OneLogin.

Click the ExampleServiceProvider button.



The user is automatically logged in at the service provider.



SAML Logout

OneLogin supports both IdP-initiated and SP-initiated SAML logout.