

ComponentSpace

SAML for ASP.NET Core

Okta

Integration Guide

Contents

Introduction.....	1
Adding a SAML Application	1
Service Provider Configuration	8
SP-Initiated SSO	11
IdP-Initiated SSO	13
SAML Logout.....	14
Troubleshooting.....	14

Introduction

This document describes integration with Okta as the identity provider.

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

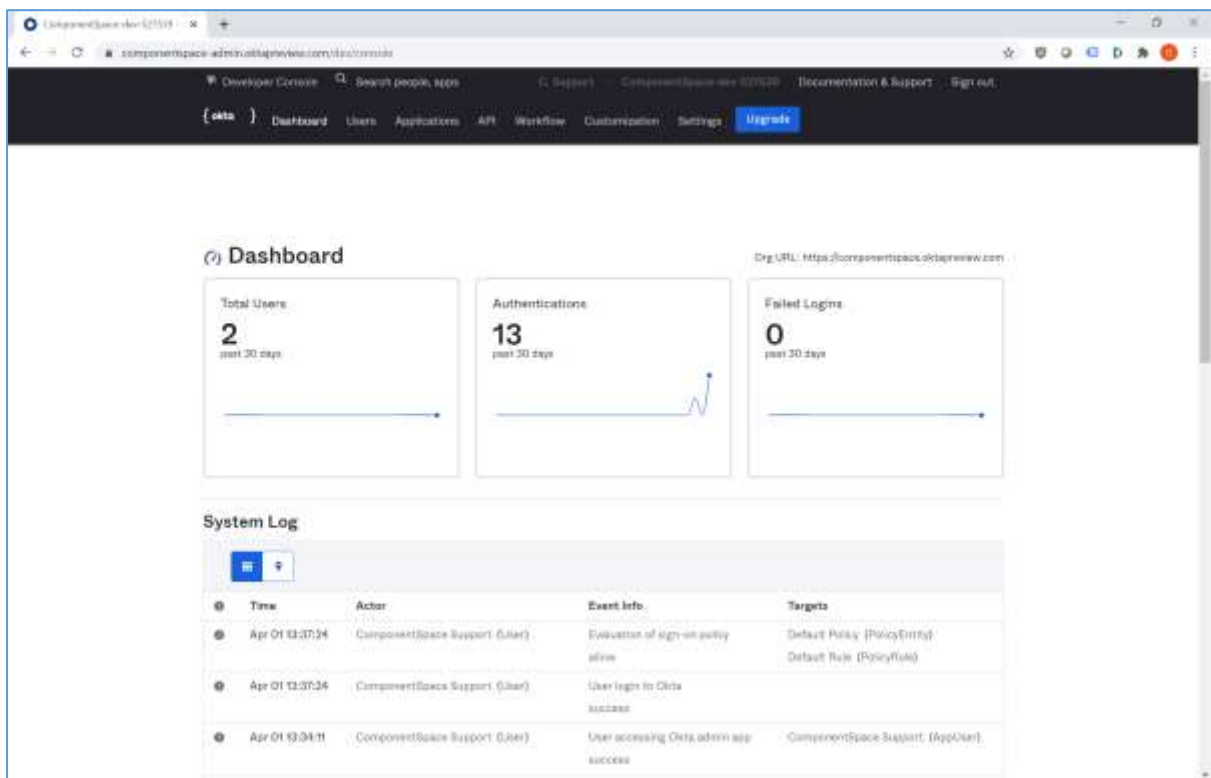
https://help.okta.com/en/prod/Content/Topics/Apps/Apps_App_Integration_Wizard_SAML.htm

Note that the developer edition of Okta was used for demonstration purposes.

Adding a SAML Application

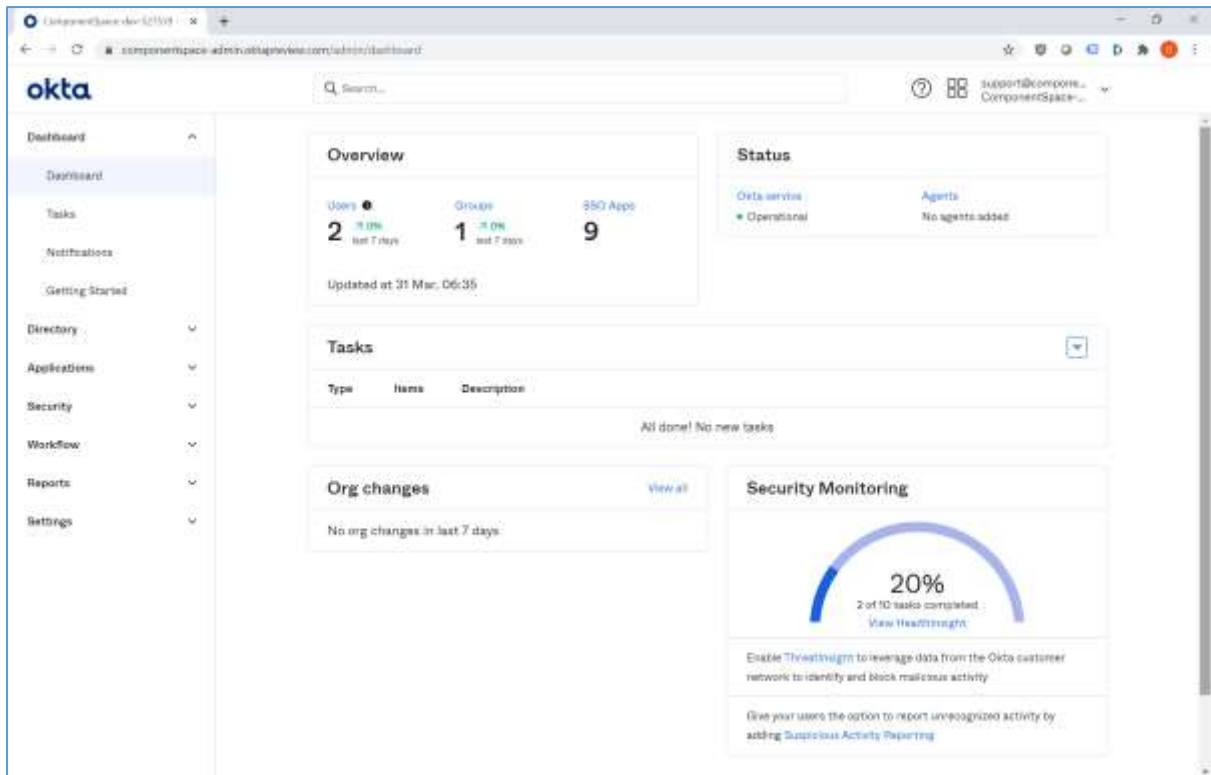
Login to Okta as an administrator.

Switch from the Developer Console to the Admin Console by selecting the Developer Console > Classic UI link in the top left corner.

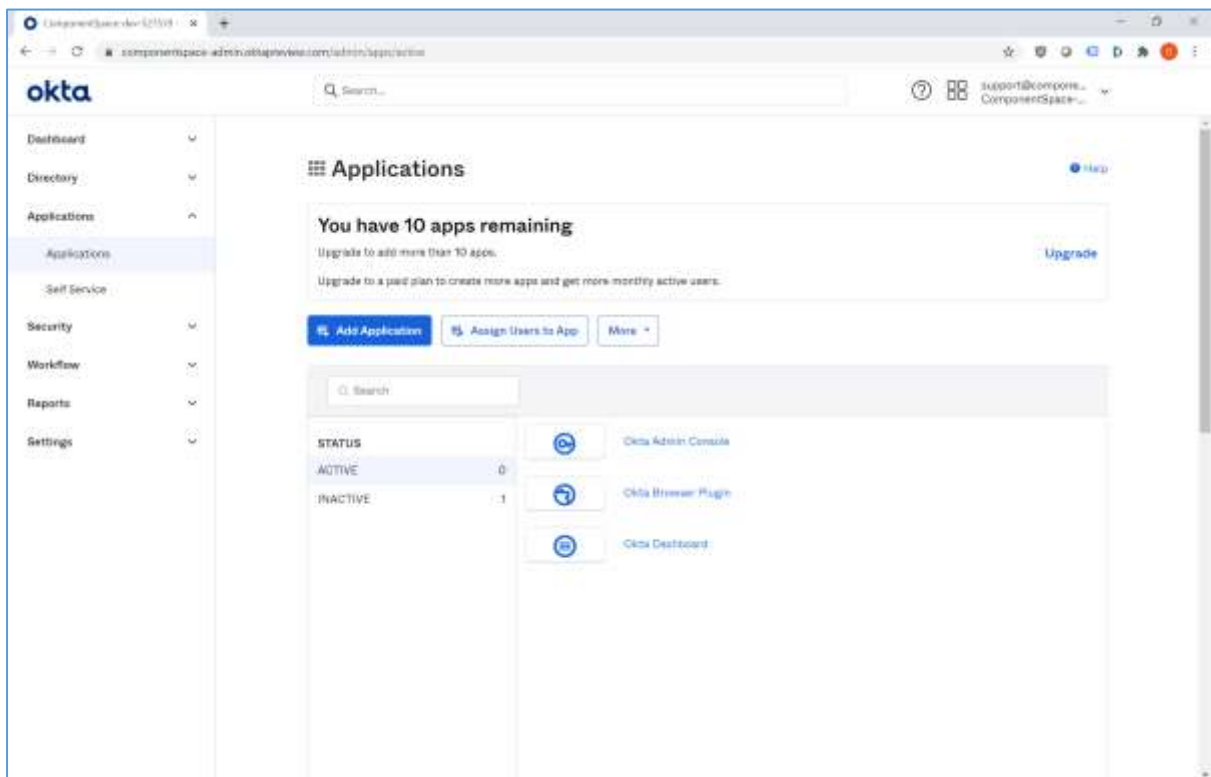


Select Applications from the menu bar.

ComponentSpace SAML for ASP.NET Core Okta Integration Guide

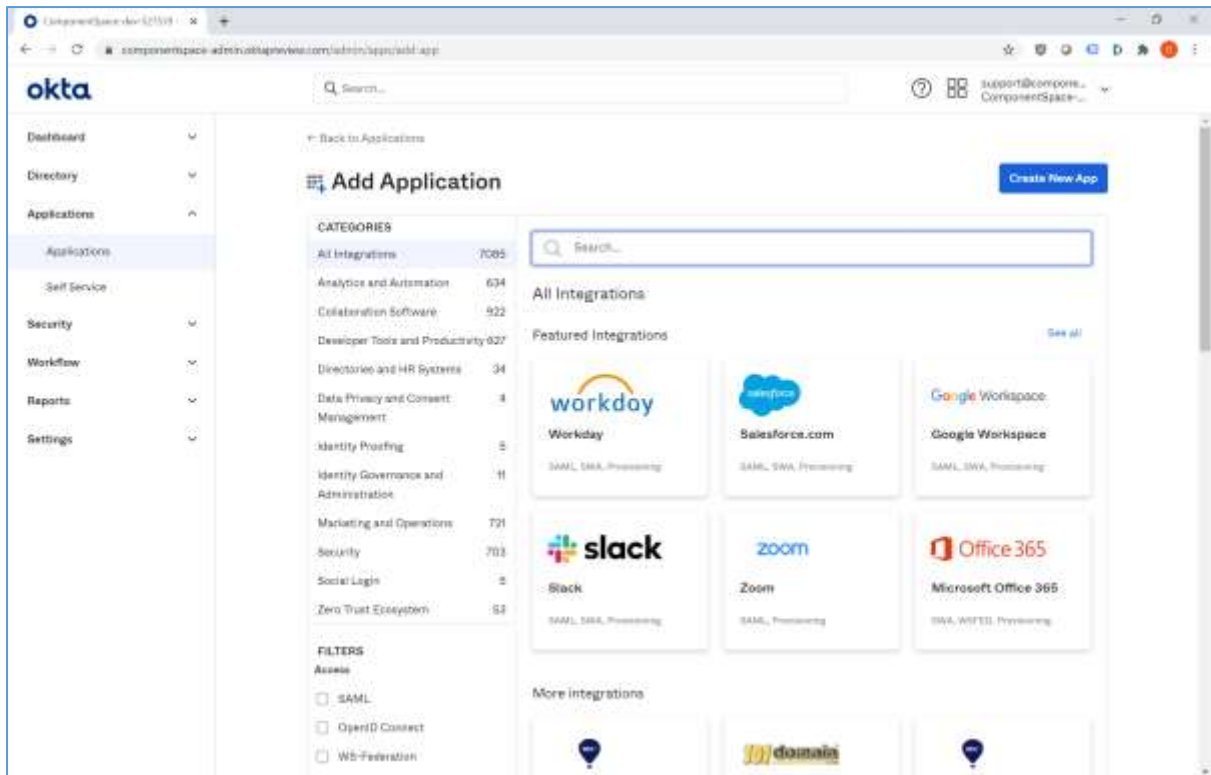


Click the Add Application button.

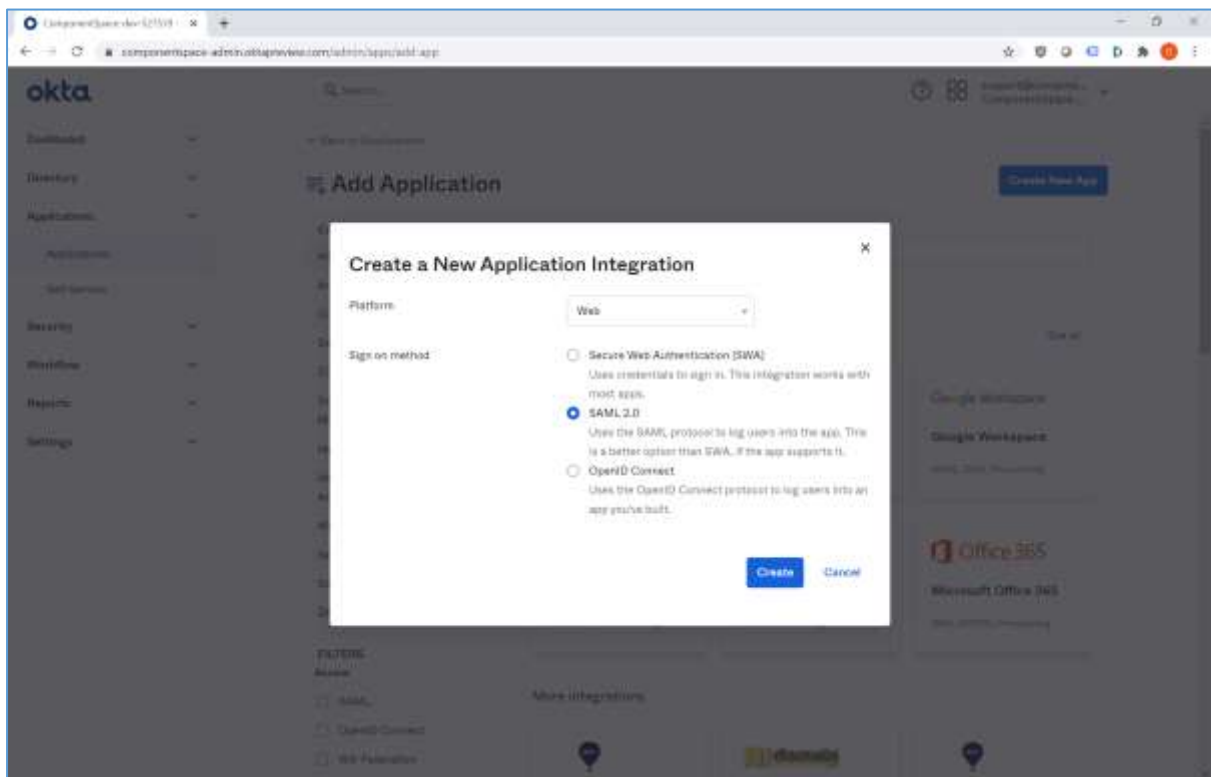


Click the Create New App button.

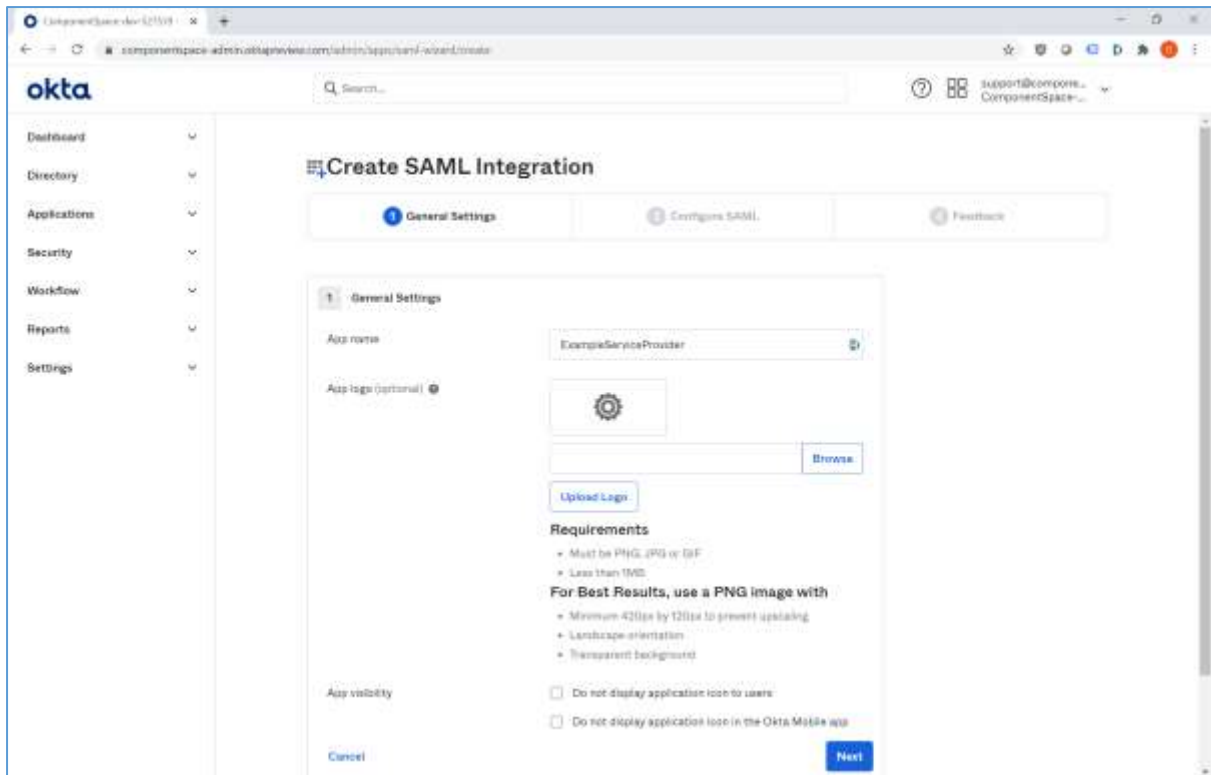
ComponentSpace SAML for ASP.NET Core Okta Integration Guide



Specify Web as the platform and SAML 2.0 as the sign-on method.



Specify an app name. This is for display purposes only.



Specify the assertion consumer service URL as the single sign-on URL.

For example:

<https://localhost:44360/SAML/AssertionConsumerService>

The same URL should be used for the recipient URL and destination URL.

Specify the service provider name as the audience URI.

For example:

<https://ExampleServiceProvider>

Relay state is not required.

The name ID format is unspecified.

The Okta username is used.

Attribute and group attribute names are not required.

ComponentSpace SAML for ASP.NET Core Okta Integration Guide

The screenshot shows the 'Create SAML Integration' page in the Okta admin console. The 'SAML Settings' section is active, and the 'General' tab is selected. The 'Single sign on URL' field is filled with 'https://localhost:44360/SAML/AssertionConsumerService'. The 'Audience URI (SP Entity ID)' field is filled with 'https://ExampleServiceProvider'. The 'Name ID format' is set to 'Unspecified'. The 'Application username' is 'Okta username'. The 'Update application username on' is set to 'Create and update'. A 'Show Advanced Settings' link is visible at the bottom right of the form.

Click the Show Advanced Settings link.

Enable single logout.

Specify the single logout URL.

For example:

<https://localhost:44360/SAML/SingleLogoutService>

Specify the SP issuer. This is the name of the service provider.

For example:

<https://ExampleServiceProvider>

Upload the service provider certificate.

For example:

Sp.cer

ComponentSpace SAML for ASP.NET Core Okta Integration Guide

The screenshot shows the Okta Admin Console interface for creating a SAML integration. The left sidebar contains navigation options: Dashboard, Directory, Applications, Security, Workflow, Reports, and Settings. The main content area is titled 'Create SAML Integration' and is currently on the 'General Settings' step. The settings are as follows:

- Response: Signed
- Assertion Signature: Signed
- Signature Algorithm: RSA-SHA256
- Digest Algorithm: SHA256
- Assertion Encryption: Unencrypted
- Enable Single Logout: Allow application to initiate Single Logout
- Single Logout URL: https://localhost:44360/SAML/SingleLogoutService
- SP Issuer: https://ExampleServiceProvider
- Signature Certificate: undefined (C:\www\ap.com) [Browse] [Upload Certificate]
- Assertion Issuance Hook: None (disabled)
- Authentication context class: PasswordProtectedTransport
- Honor Force Authentication: Yes

Click the Next button, indicate this is an internal app, and click the Finish button.

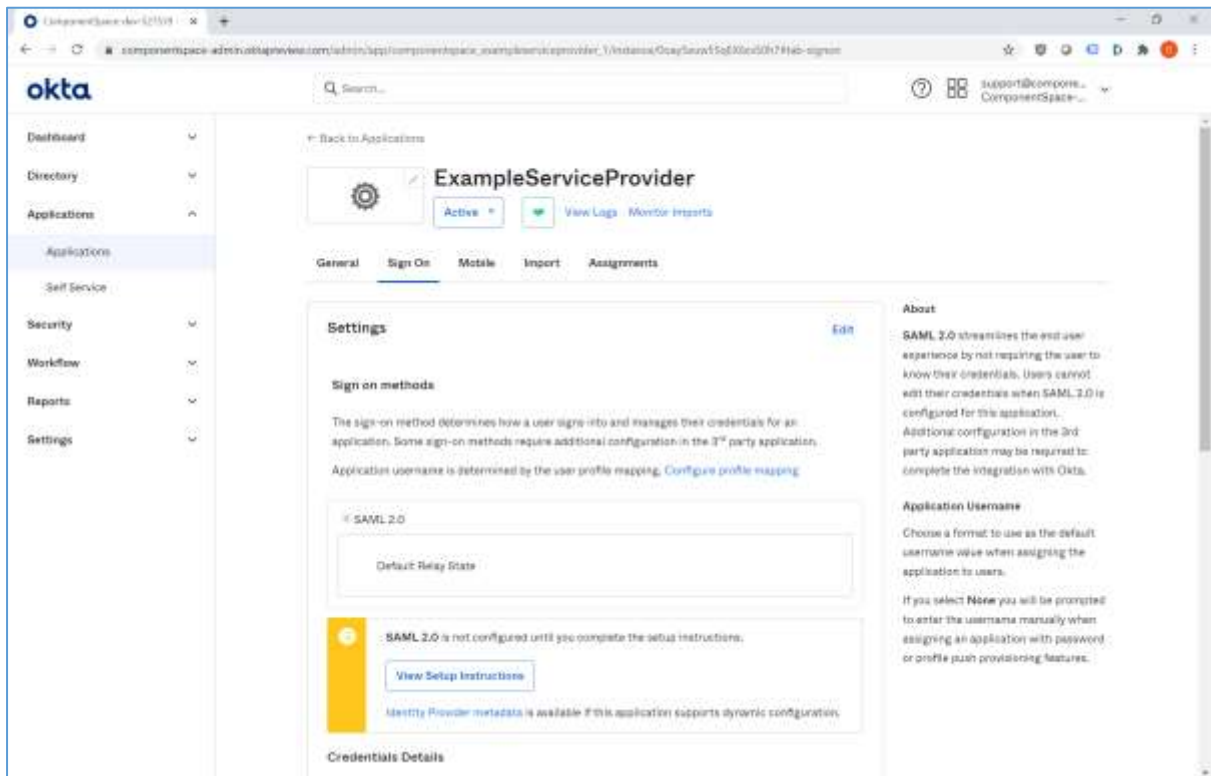
The screenshot shows the 'Create SAML Integration' page at the 'Feedback' step. The progress bar indicates three steps: 1. General Settings, 2. Configure SAML, and 3. Feedback. The main content area contains a form with the following questions and options:

- 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

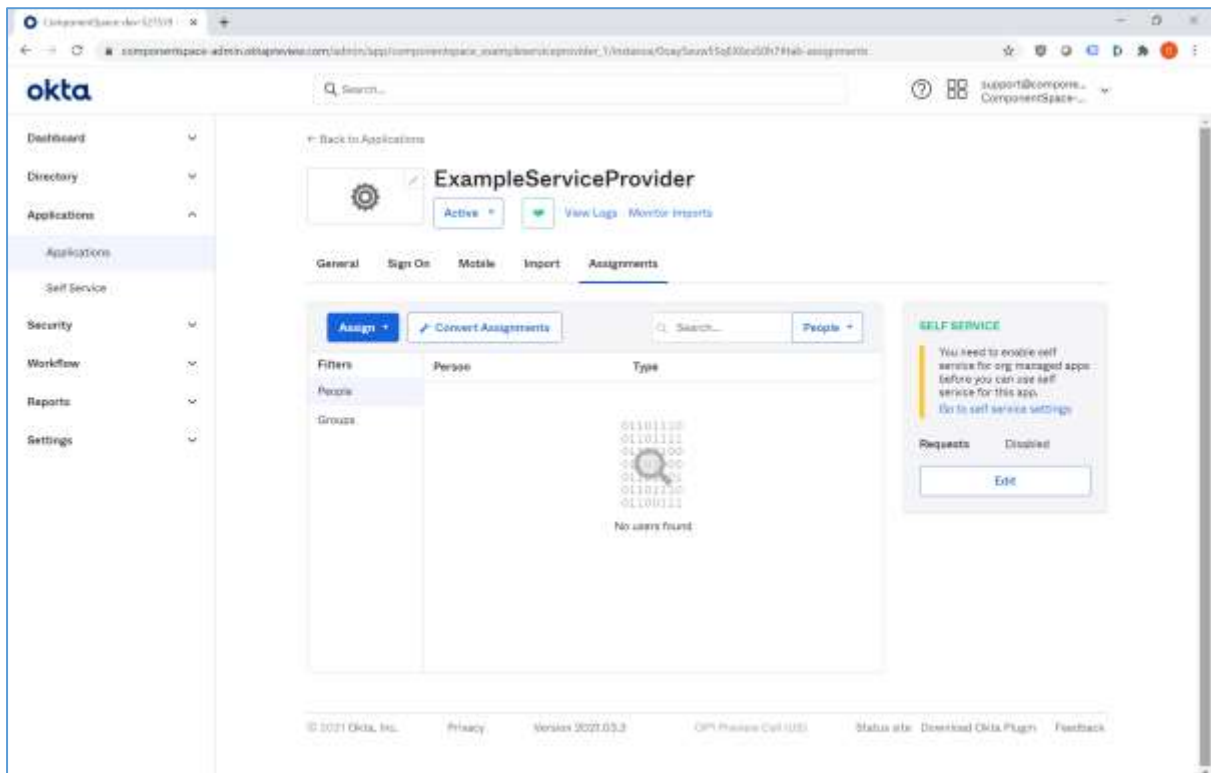
Buttons for 'Previous' and 'Finish' are visible at the bottom of the form. A help text box on the right asks 'Why are you asking me this?' and explains that the form provides background information to Okta Support.

ComponentSpace SAML for ASP.NET Core Okta Integration Guide

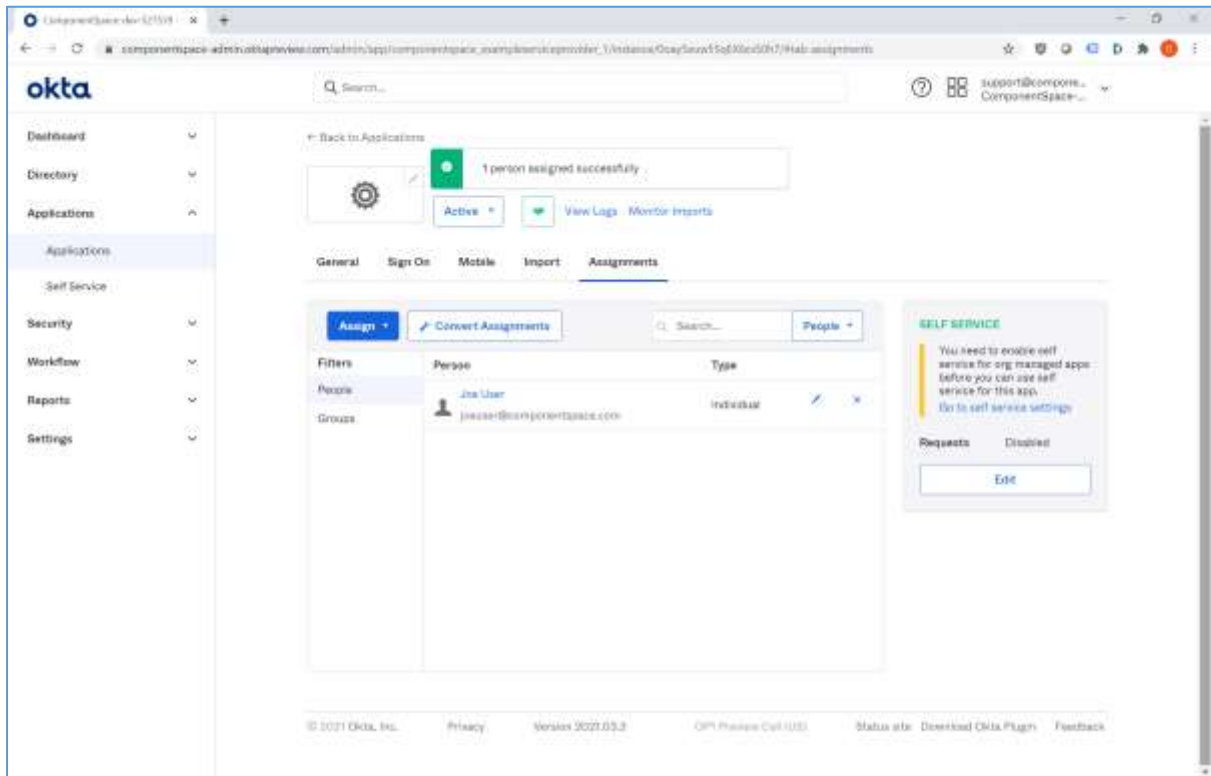
View the setup instructions or download the identity provider metadata. This information will be required when configuring the service provider.



Select the Assignments link.



Assign users or groups to the application. Only users directly assigned or assigned through group membership may SSO to the application.

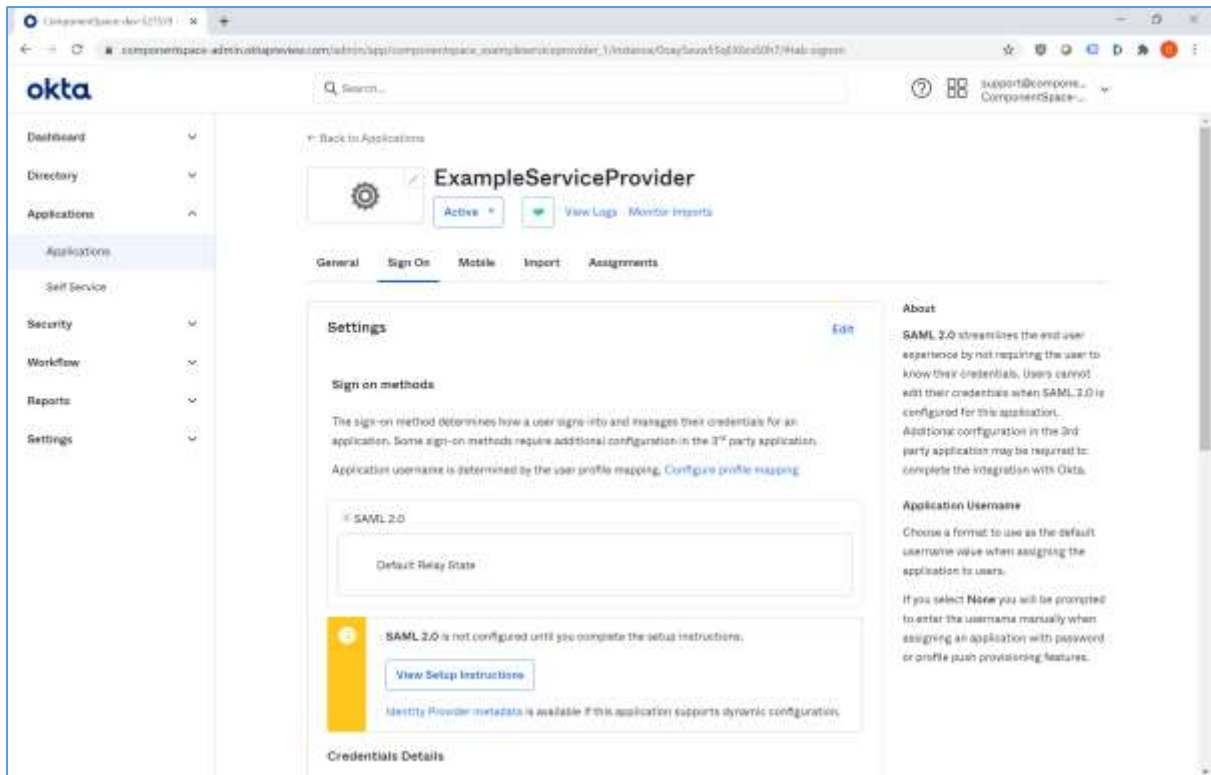


The application is now configured in Okta for SAML SSO.

Service Provider Configuration

The service provider must be configured with Okta as a partner identity provider.

The Okta SAML configuration is available using the Sign On link for the application.

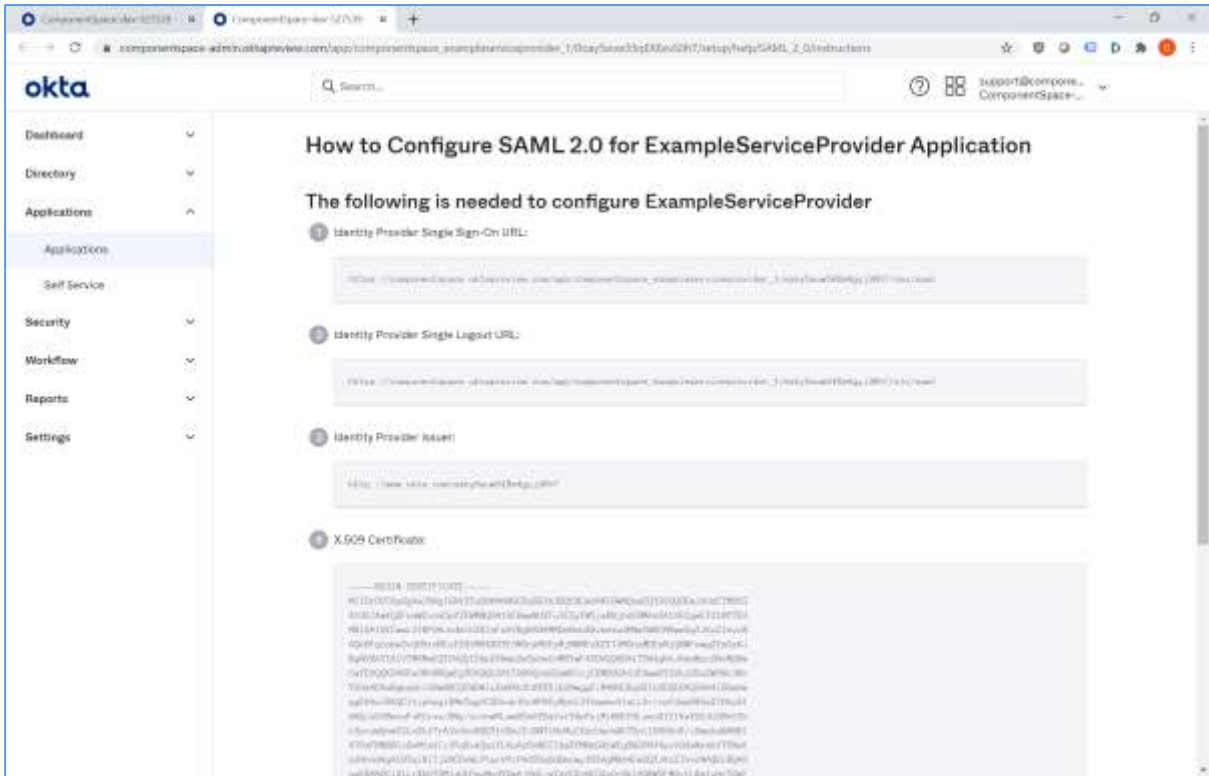


There are two options for setting up the partner identity provider configuration in the example service provider's SAML configuration.

The first option is to download Okta's SAML metadata and import this into the example service provider's SAML configuration. Please refer to the SAML Metadata Guide for more information.

The second option is to manually add a partner identity provider configuration using the information provided by Okta.

The identity provider single sign-on and single logout URLs are self-explanatory. The identity provider issuer corresponds to the partner identity provider name. The X.509 certificate is the partner certificate.



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

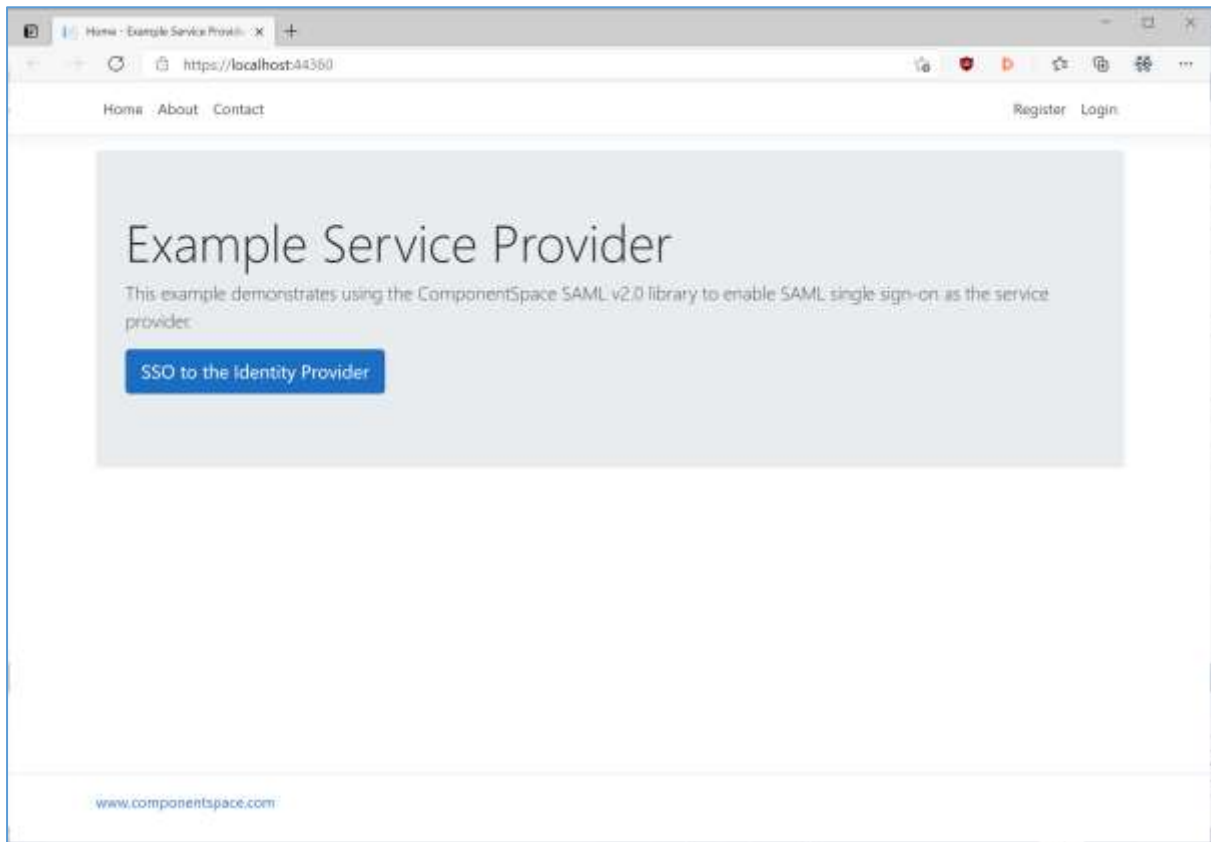
```
{
  "Name": "http://www.okta.com/exky5euw54Xm4gyj30h7",
  "Description": "Okta",
  "SignAuthnRequest": true,
  "SignLogoutRequest": true,
  "SignLogoutResponse": true,
  "SingleSignOnServiceUrl":
  "https://componentspace.oktapreview.com/app/componentspace_exampleserviceprovider_1/exky5euw54Xm4gyj30h7/sso/saml",
  "SingleLogoutServiceUrl":
  "https://componentspace.oktapreview.com/app/componentspace_exampleserviceprovider_1/exky5euw54Xm4gyj30h7/slo/saml",
  "PartnerCertificates": [
    {
      "FileName": "certificates/okta.cer"
    }
  ]
}
```

Ensure the PartnerName specifies the correct partner identity provider.

```
"PartnerName": "http://www.okta.com/exky5euw54Xm4gyj30h7"
```

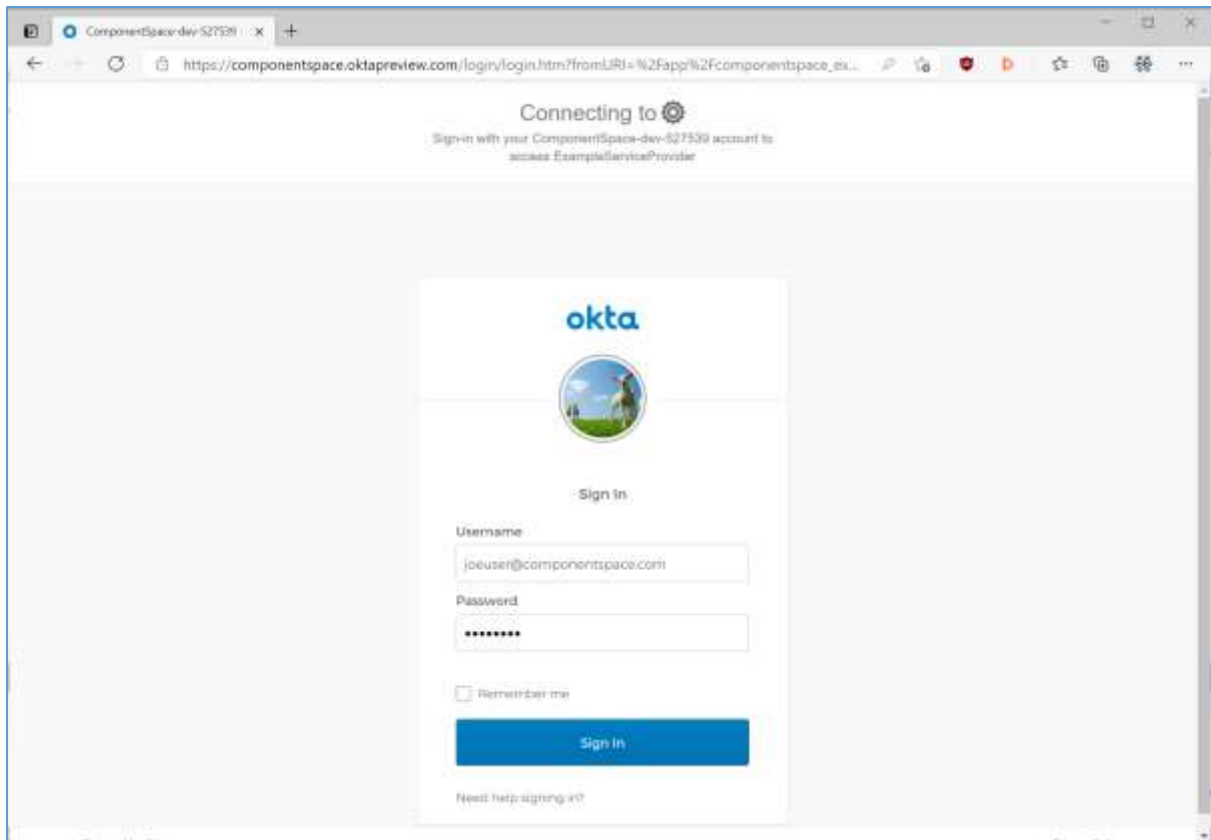
SP-Initiated SSO

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

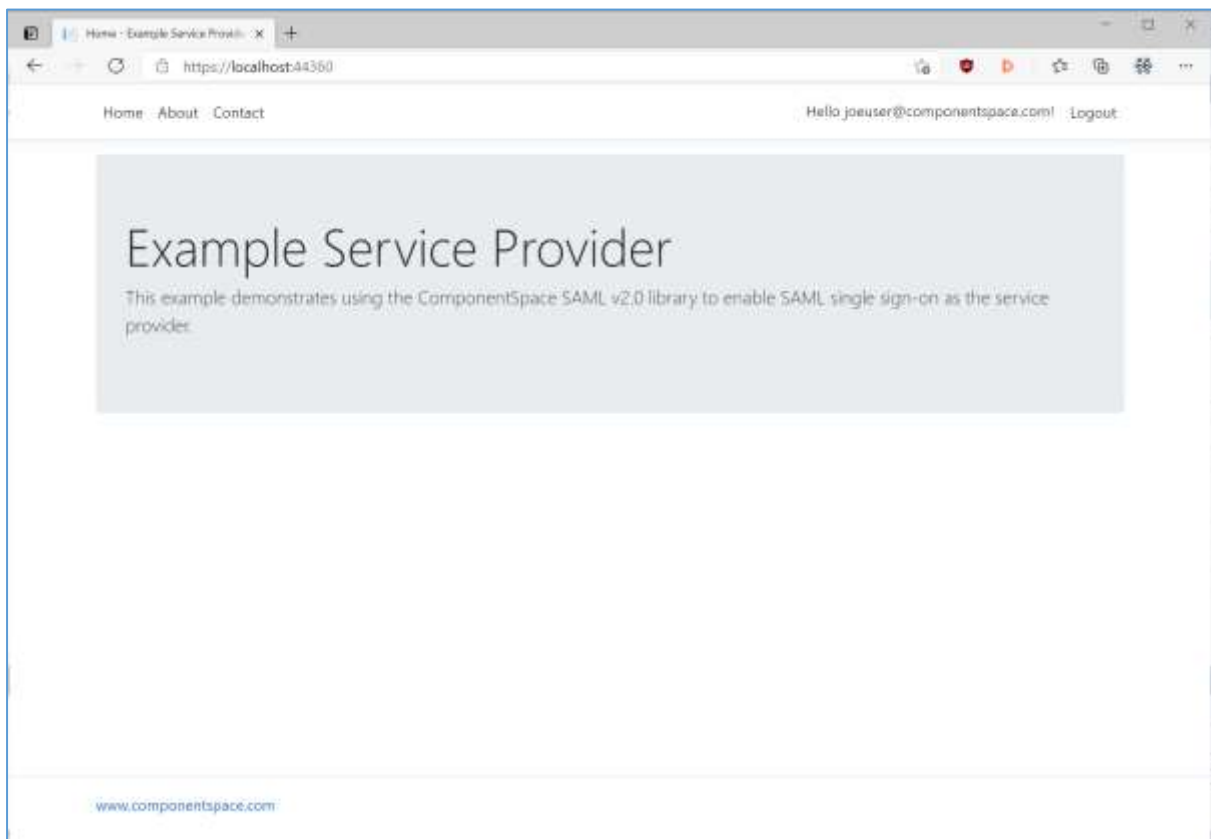


Login to Okta.

ComponentSpace SAML for ASP.NET Core Okta Integration Guide



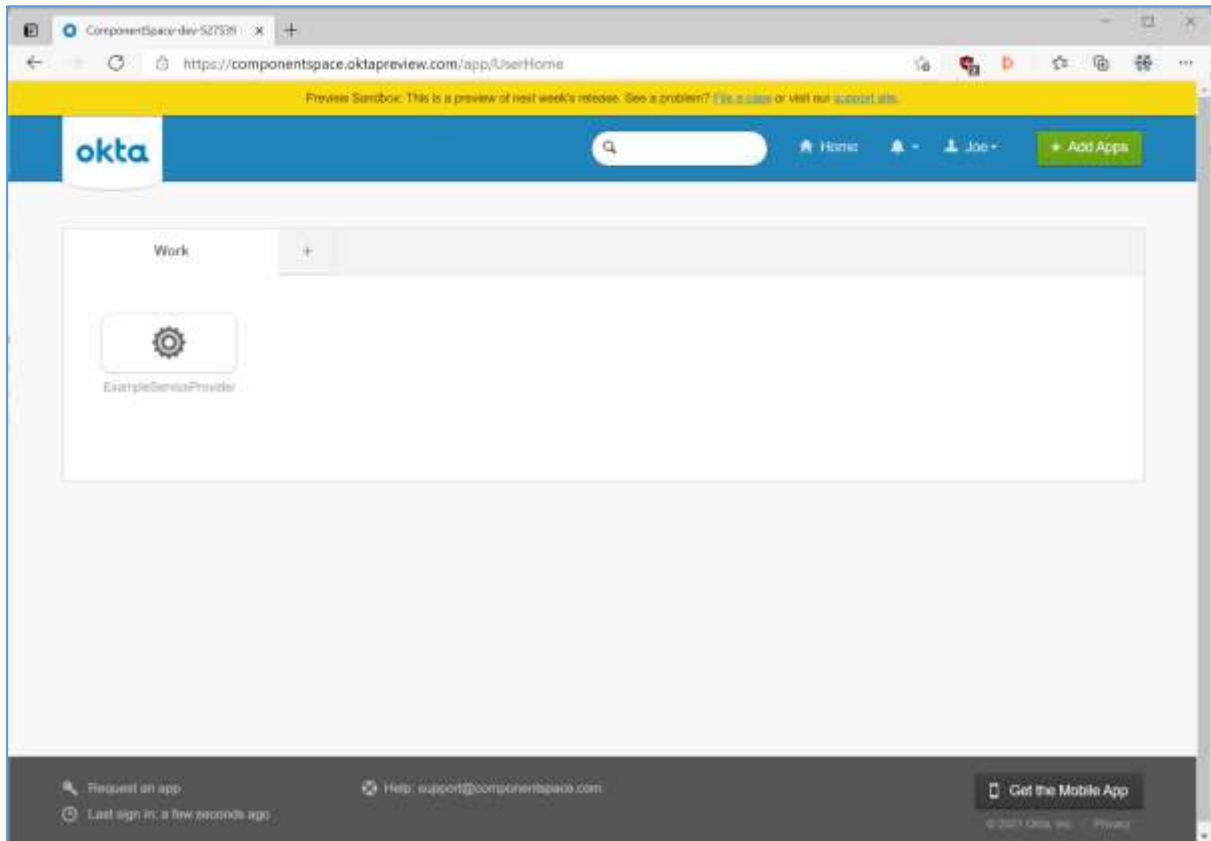
The user is automatically logged in at the service provider.



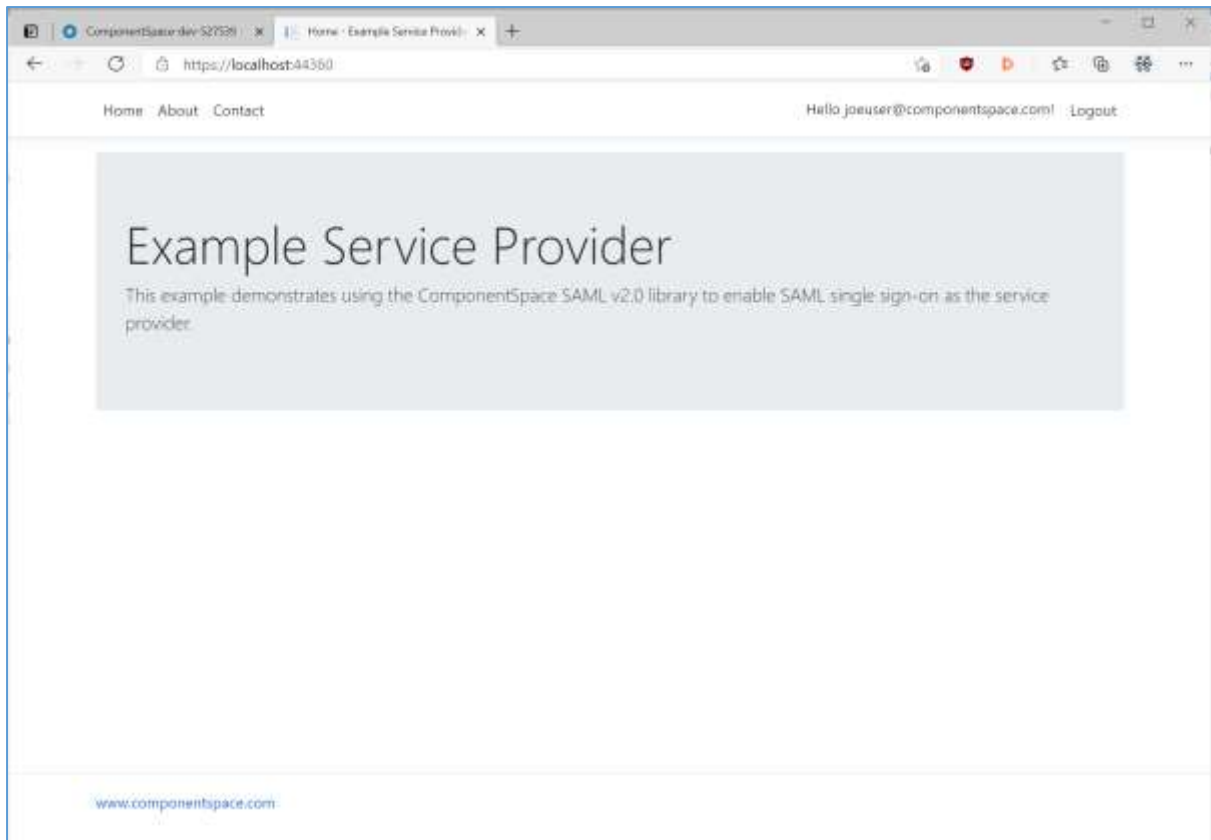
IdP-Initiated SSO

Login to Okta.

Click the ExampleServiceProvider button.



The user is automatically logged in at the service provider.



SAML Logout

Okta supports SP-initiated SAML logout only.

If logged into a service provider and the user logs out from Okta, no SAML logout request is sent to the service provider.

Troubleshooting

Most issues result from configuration mismatches. Ensure that the Okta configuration and the service provider configuration are consistent with each other.

The Okta system log may contain additional information.

ComponentSpace SAML for ASP.NET Core Okta Integration Guide

The screenshot displays the Okta System Log interface. At the top, there is a search bar and a navigation menu on the left. The main content area is titled "System Log" and includes a filter section with "From" and "To" date and time pickers. Below the filters is a search input field and a "Count of events over time" bar chart. A section titled "Show event trends by category" is followed by a table of events. The table has columns for "Time", "Actor", "Event Info", and "Targets".

Time	Actor	Event Info	Targets
Apr 03 09:24:41	ComponentSpace Support: [User]	User accessing Okta admin app: success	ComponentSpace Support: [App/Dev]
Apr 03 09:24:41	Okta Administration: [PublicClientApp]	OIDC access token is granted: success	[User] Access Token: [access_token]
Apr 03 09:24:41	ComponentSpace Support: [User]	User single sign on to app	Okta Admin Console: [App/Instance]