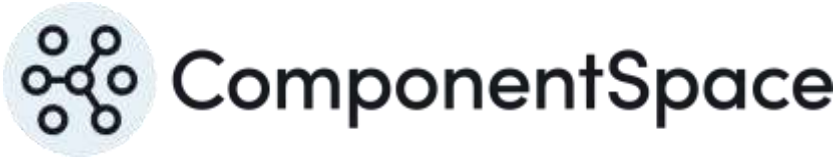


ComponentSpace
SAML for ASP.NET Core
Okta
Integration Guide

www.componentspace.com

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.

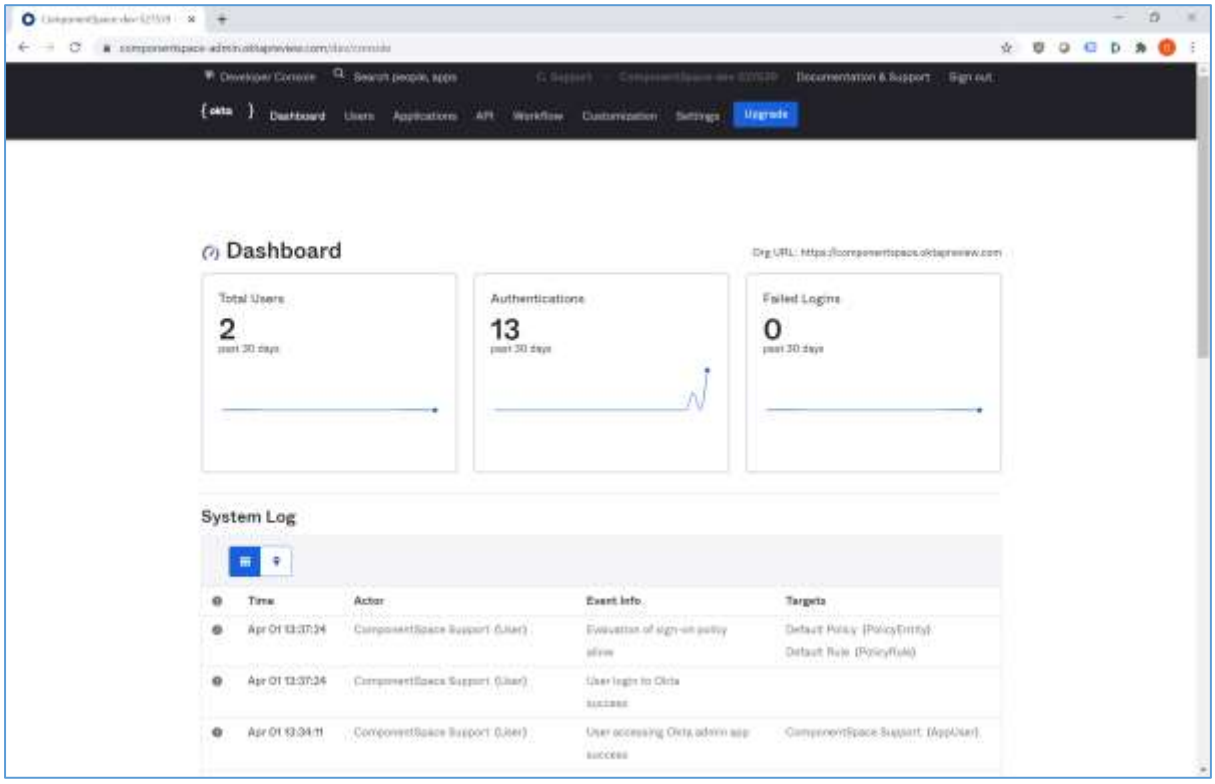
https://help.okta.com/en/prod/Content/Topics/Apps/Apps_App_Integration_Wizard_SAML.htm

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

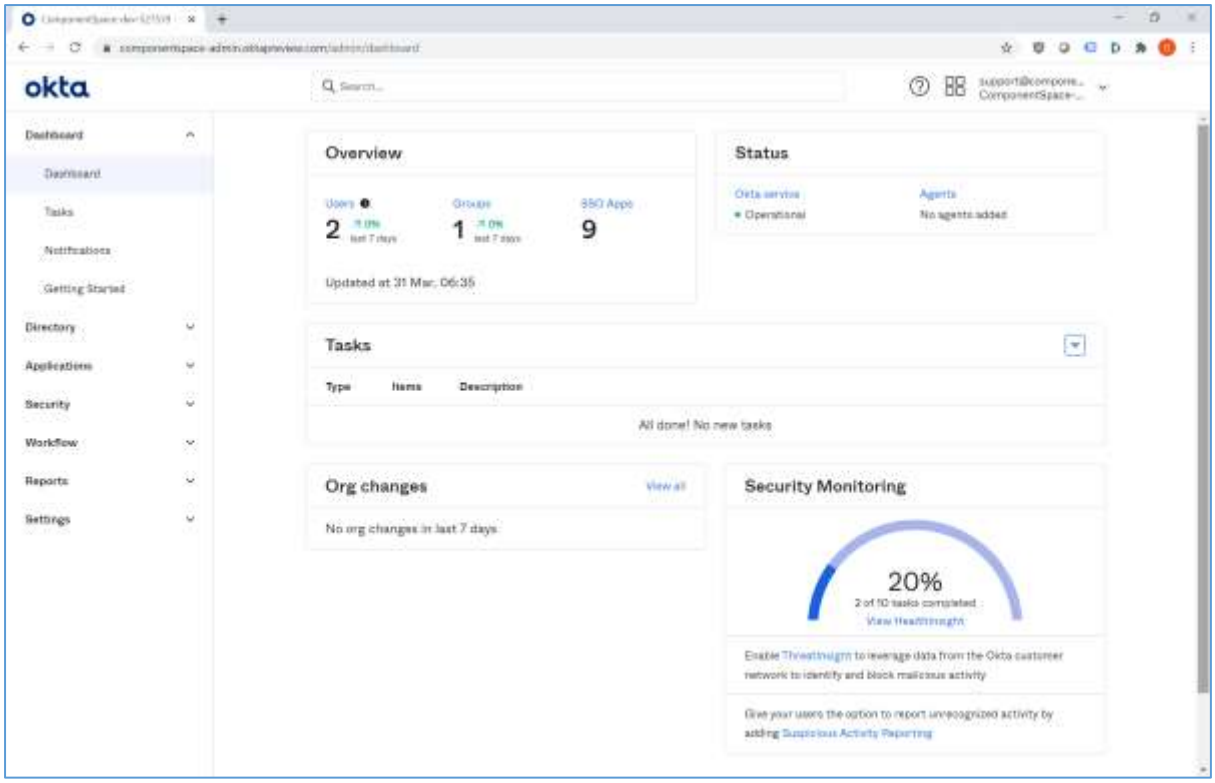
Adding a SAML Application

Login to Okta as an administrator.

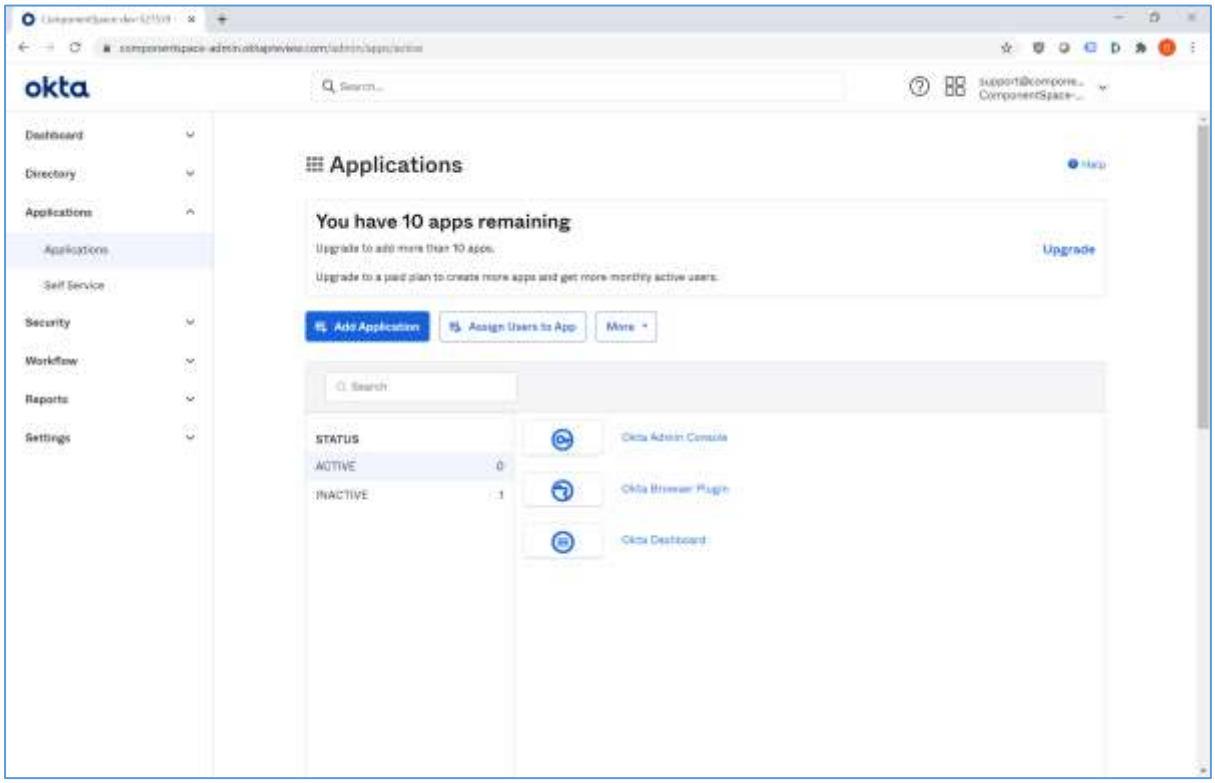
Switch from the Developer Console to the Admin Console by selecting the Developer Console > Classic UI link in the top left corner.



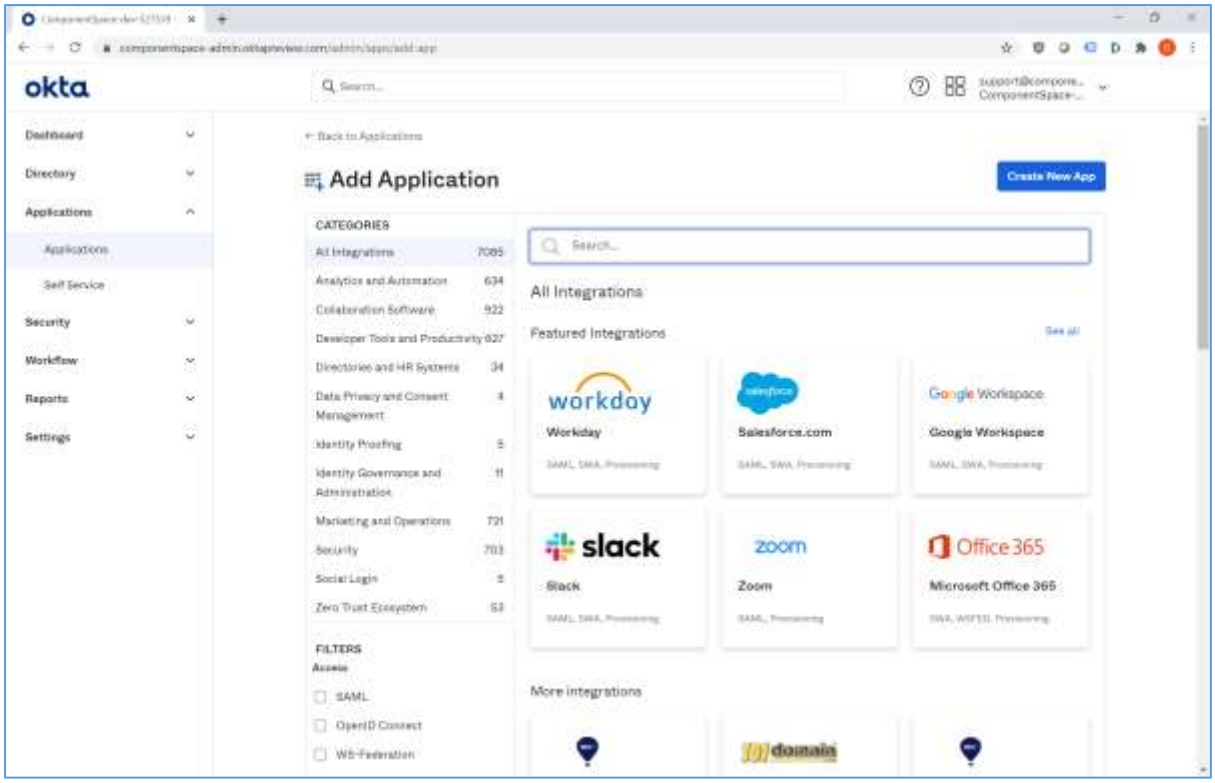
Select Applications from the menu bar.



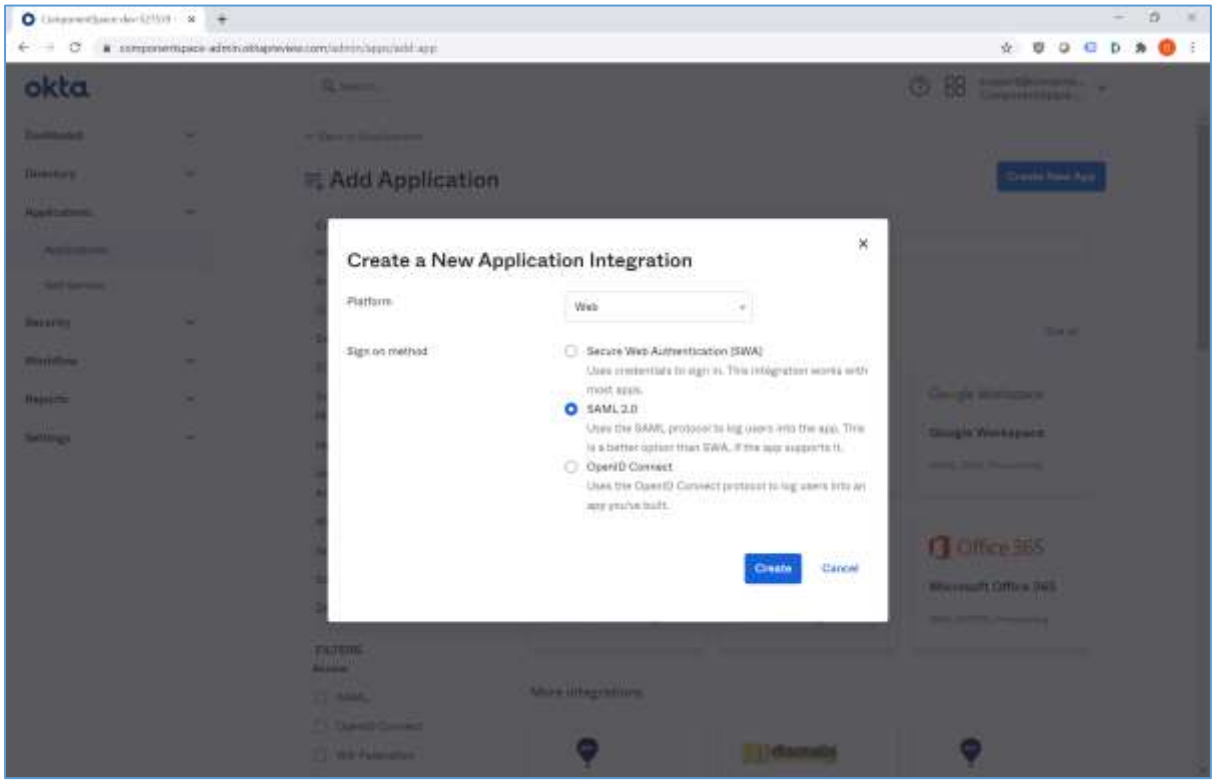
Click the Add Application button.



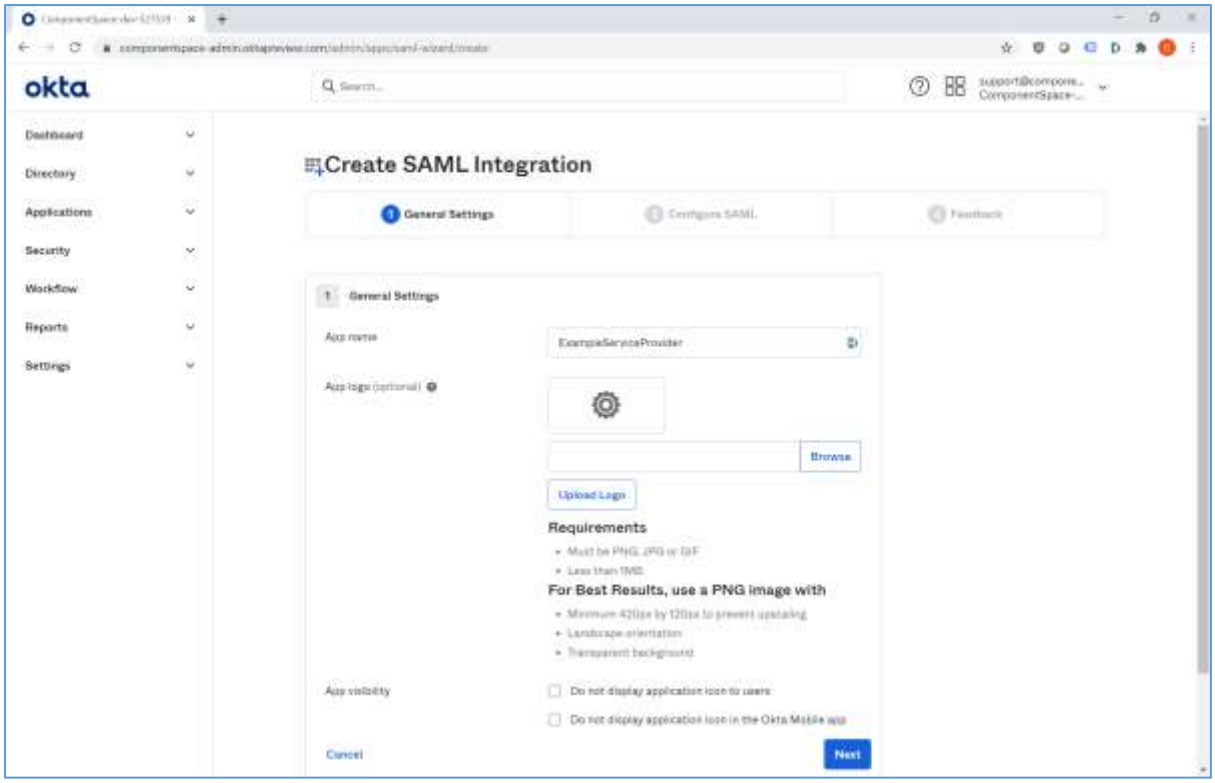
Click the Create New App button.



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:

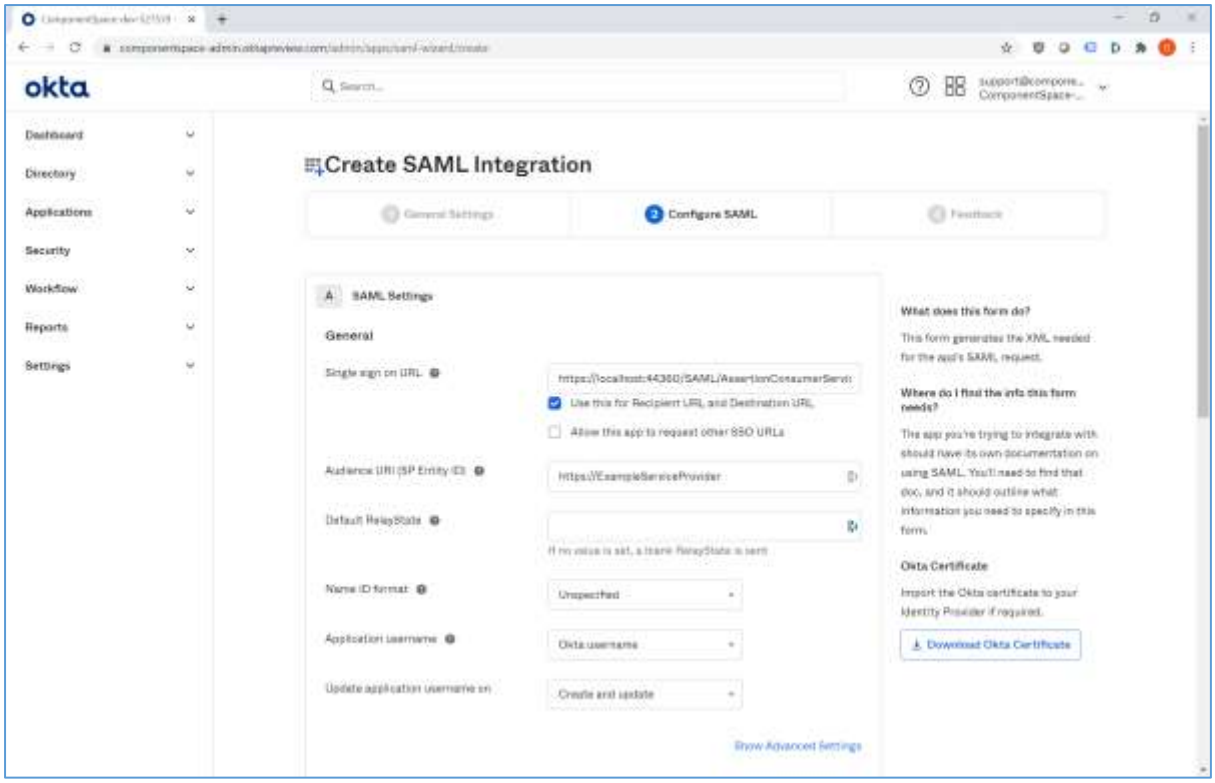
https://ExampleServiceProvider

Relay state is not required.

The name ID format is unspecified.

The Okta username is used.

Attribute and group attribute names are not required.



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.

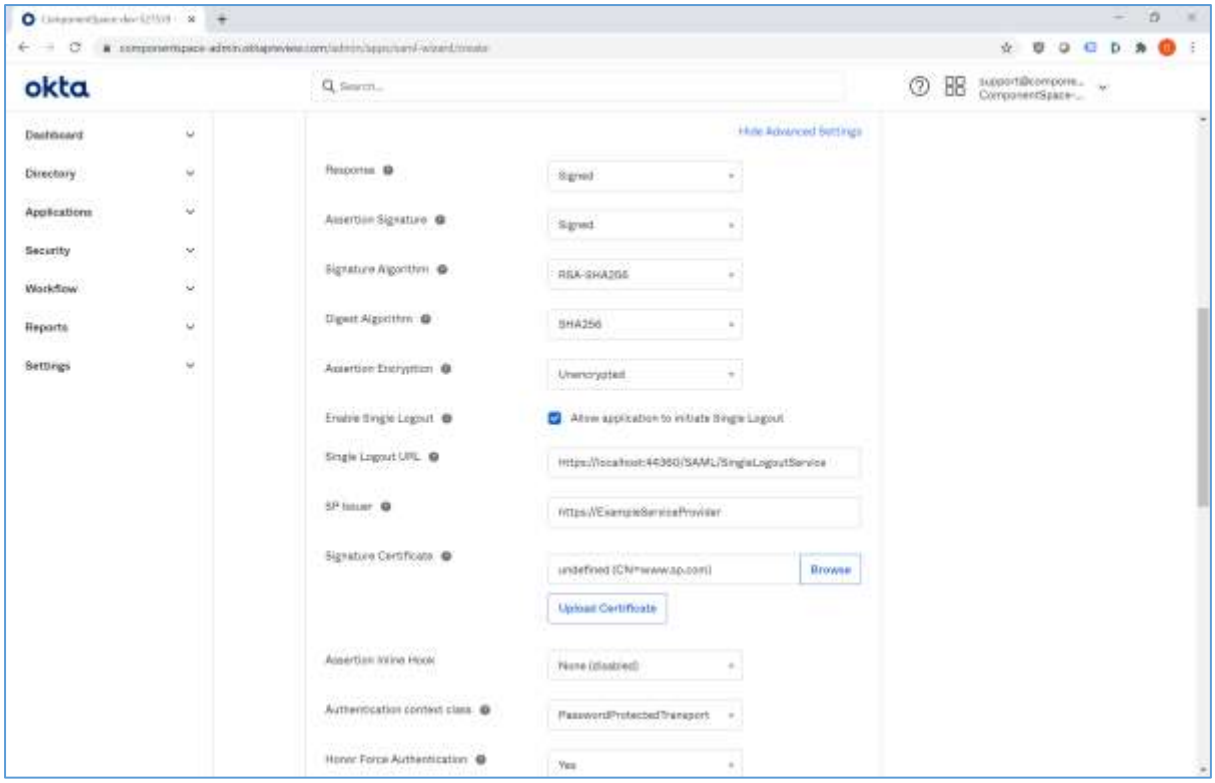
For example:

https://ExampleServiceProvider

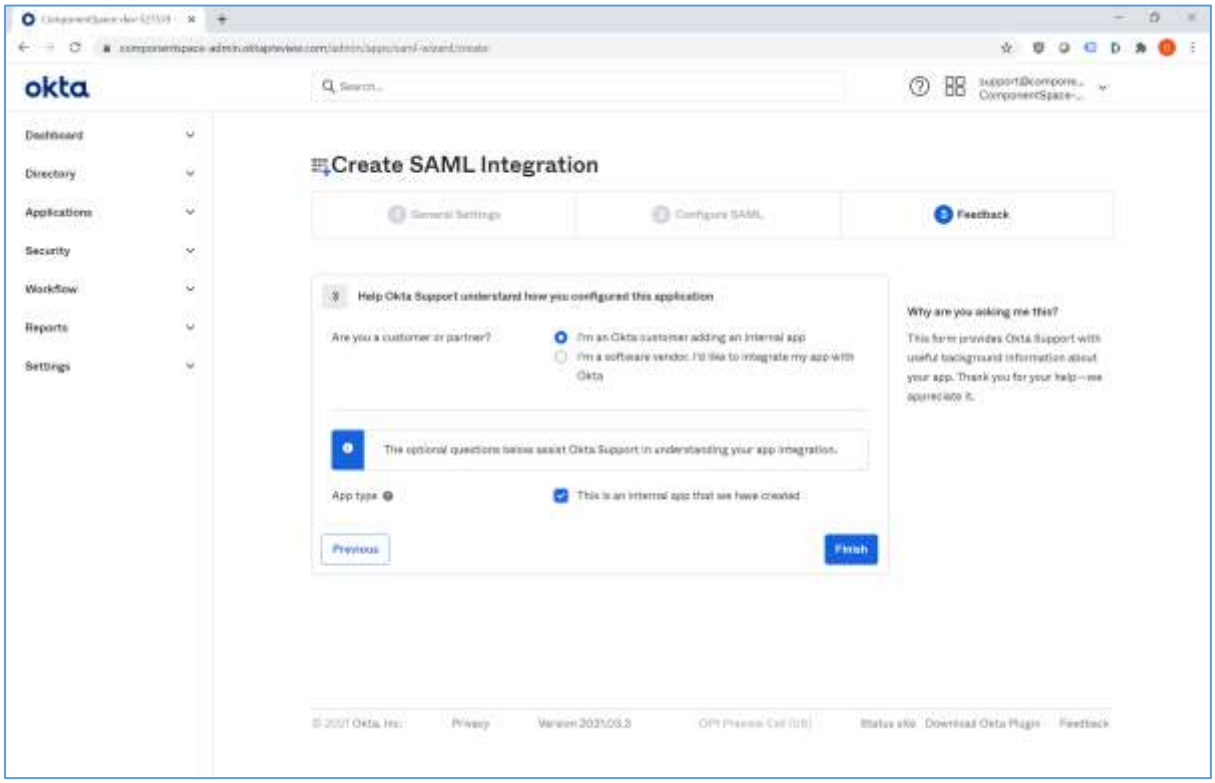
Upload the service provider certificate.

For example:

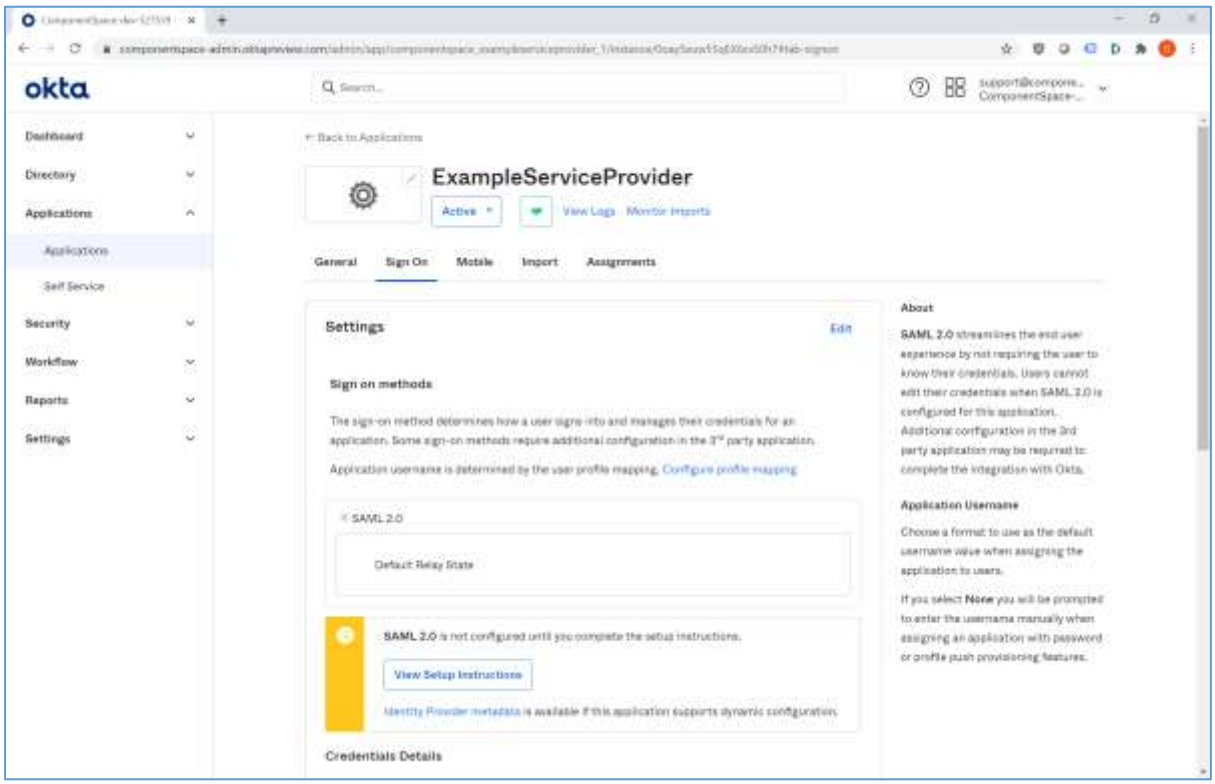
Sp.cer



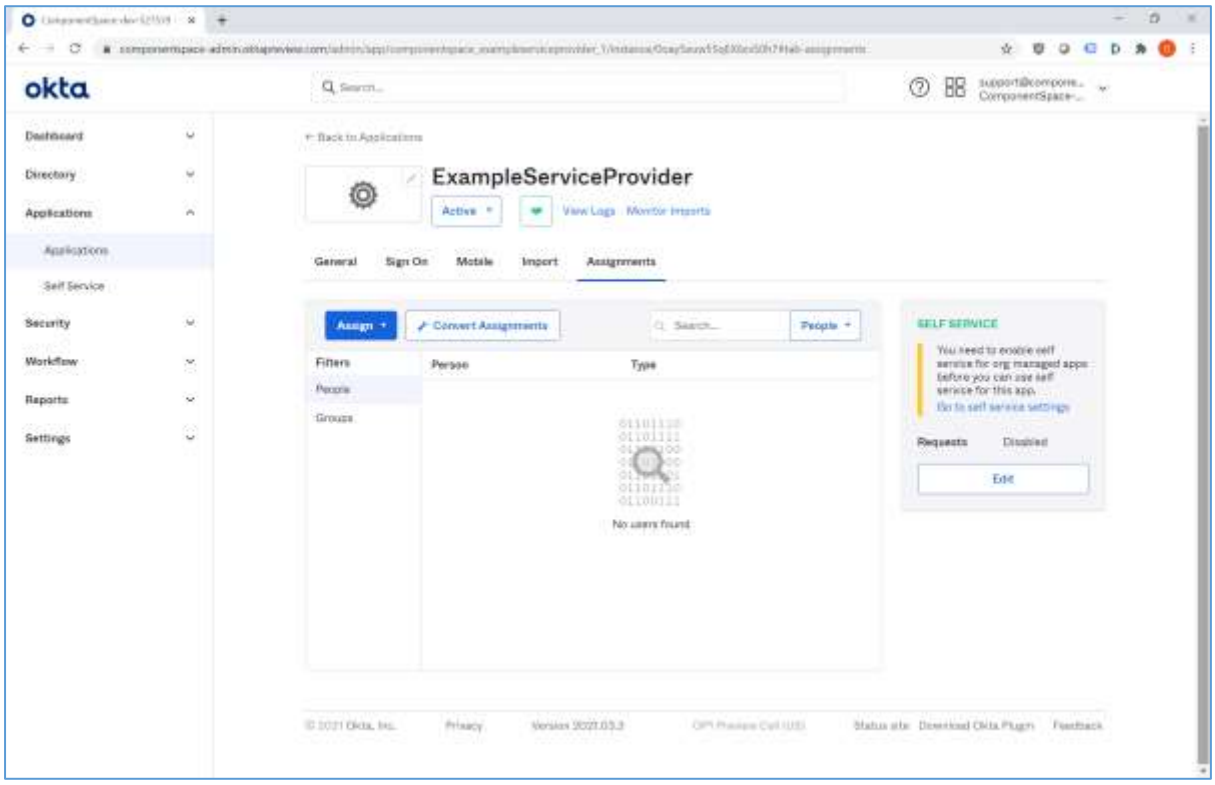
Click the Next button, indicate this is an internal app, and click the Finish button.



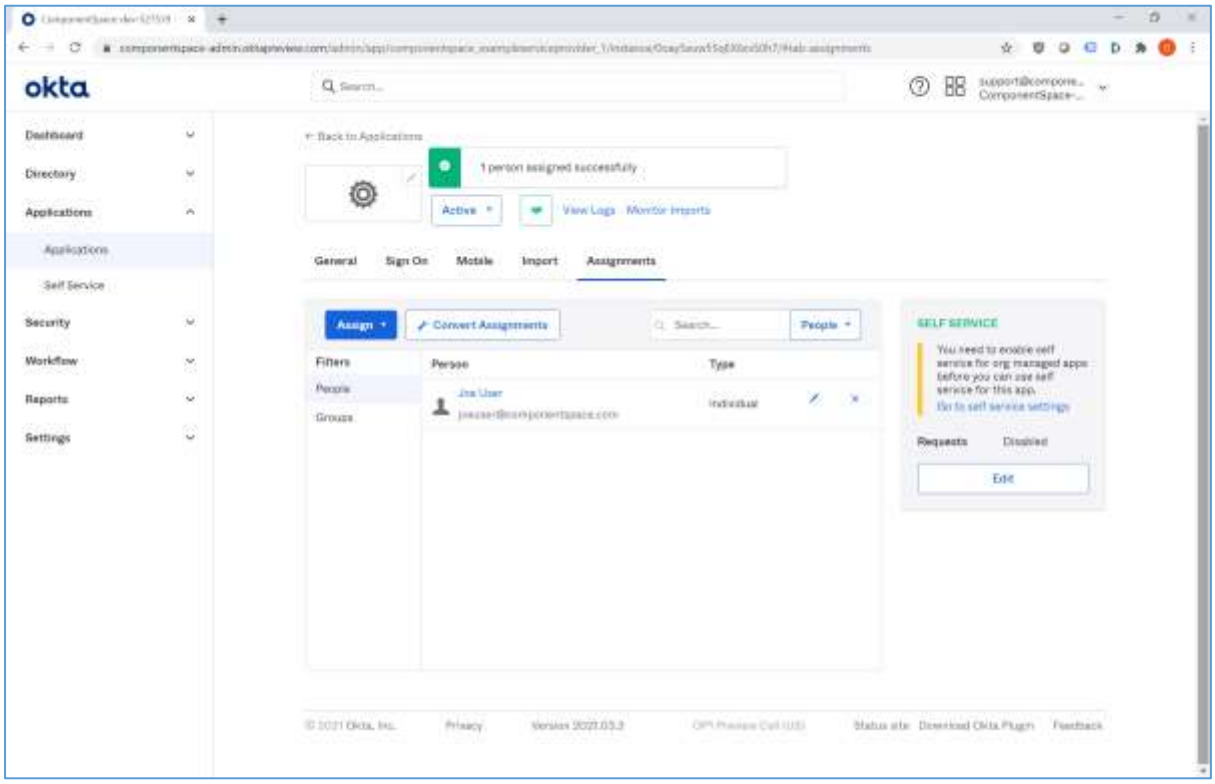
View the setup instructions or download the identity provider metadata. This information will be required when configuring the service provider.



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.

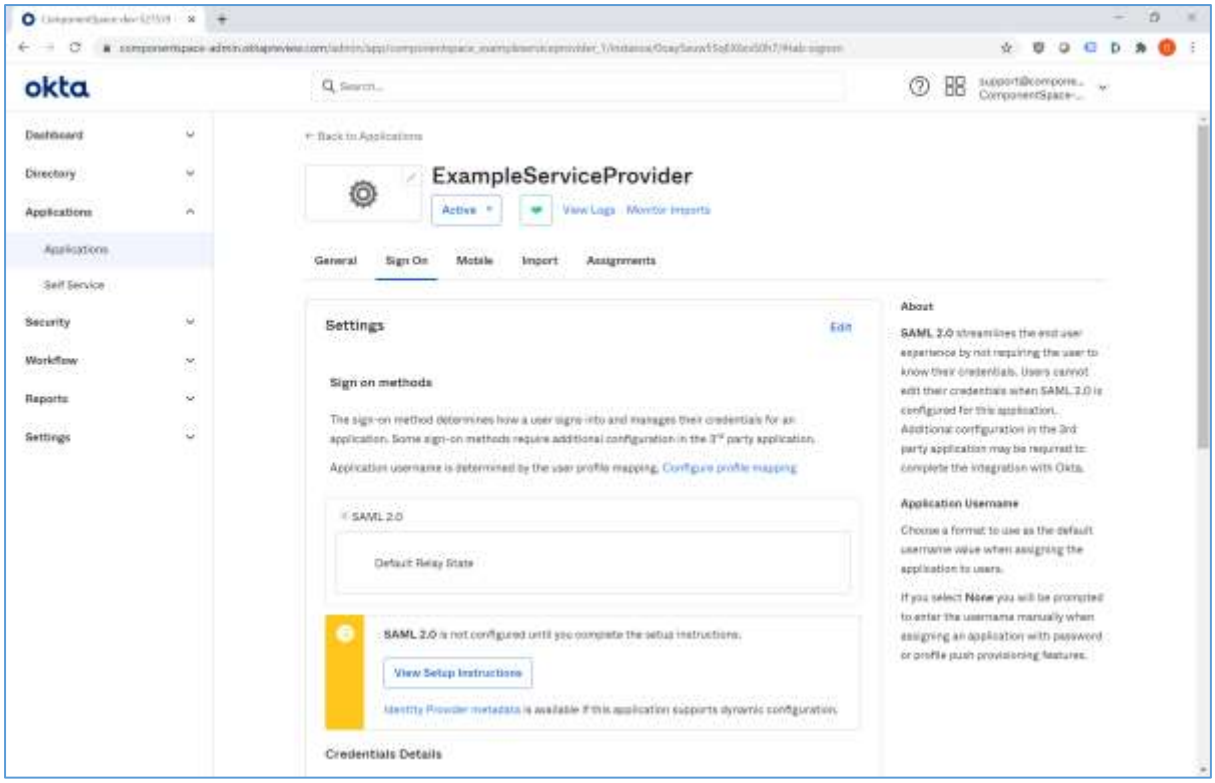


The application is now configured in Okta for SAML SSO.

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.

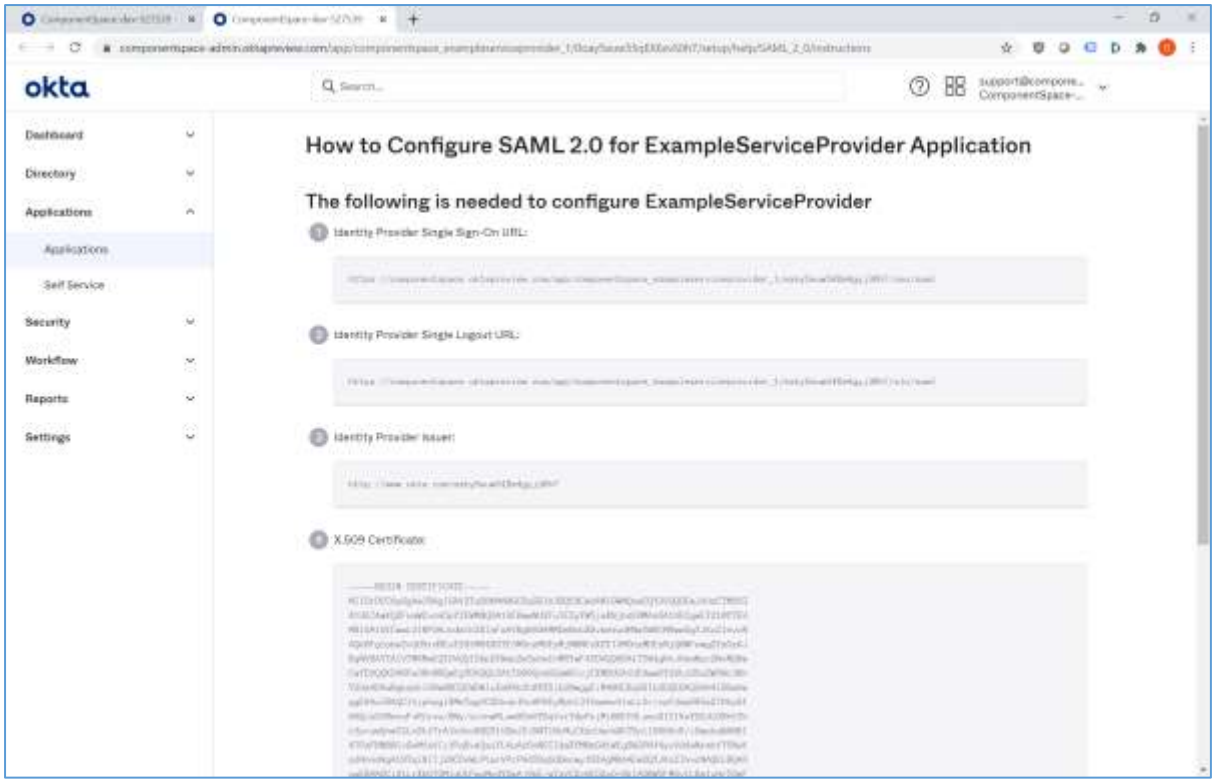


There are two options for setting up the partner identity provider configuration in the example service provider's SAML configuration.

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.

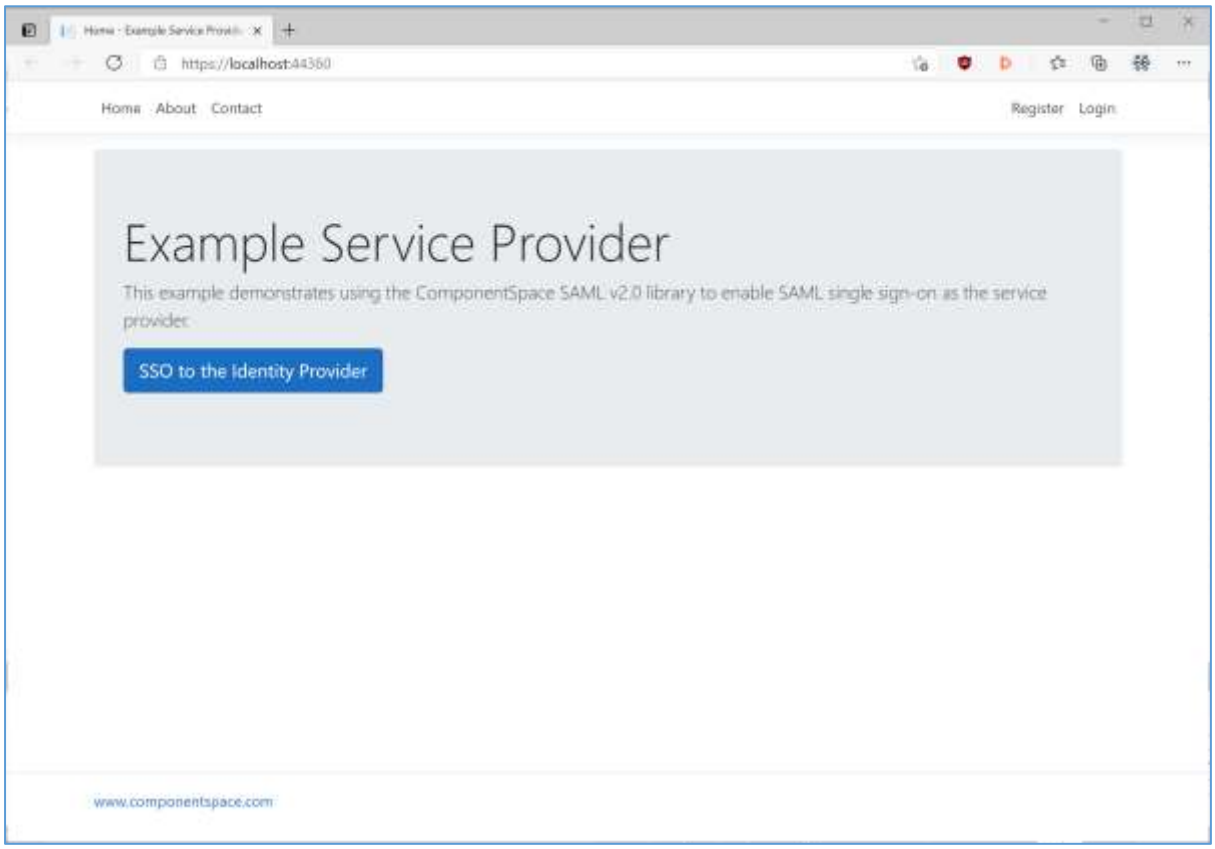
```
{
  "Name": "http://www.okta.com/exky5euw54Xm4gyj30h7",
  "Description": "Okta",
  "SignAuthnRequest": true,
  "SignLogoutRequest": true,
  "SignLogoutResponse": true,
  "SingleSignOnServiceUrl":
"https://componentspace.oktapreview.com/app/componentspace_exampleserviceprovider
_1/exky5euw54Xm4gyj30h7/sso/saml",
  "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.

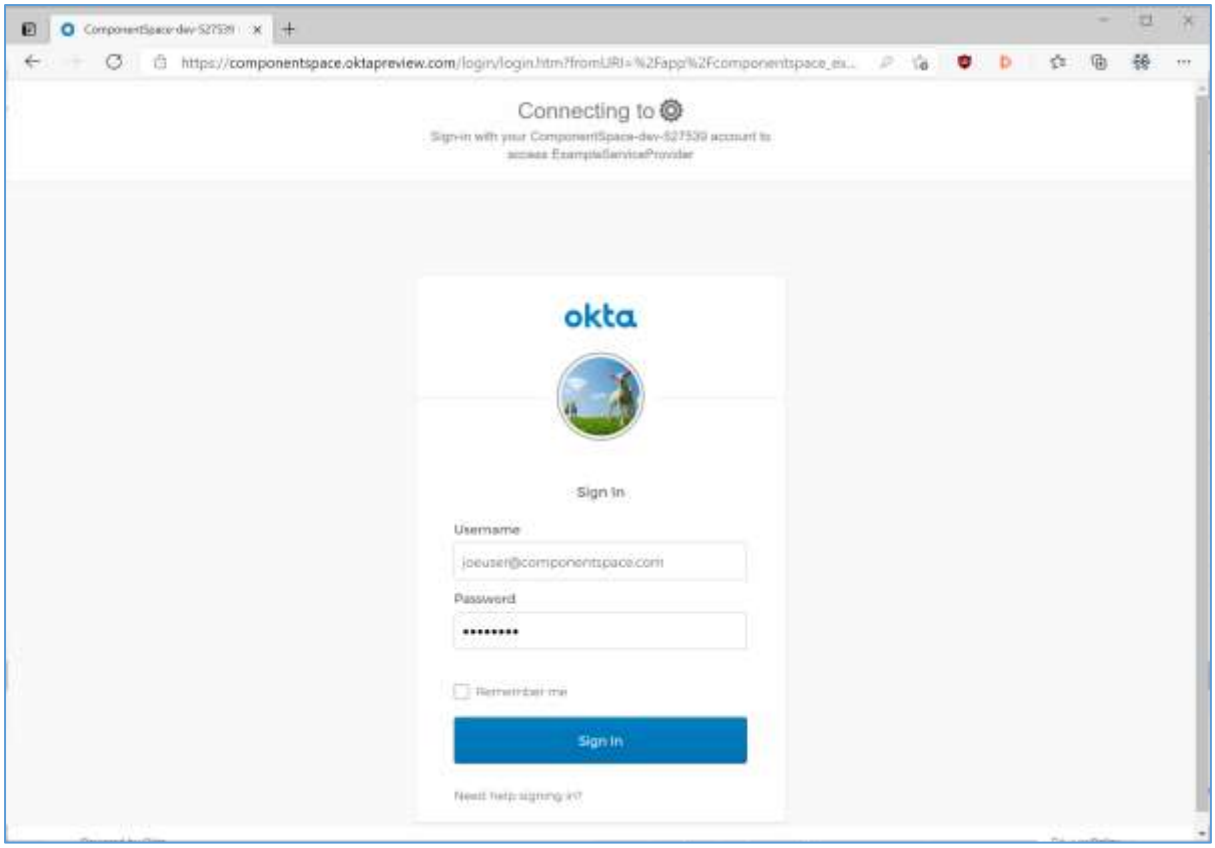
```
"PartnerName": "http://www.okta.com/exky5euw54Xm4gyj30h7"
```

SP-Initiated SSO

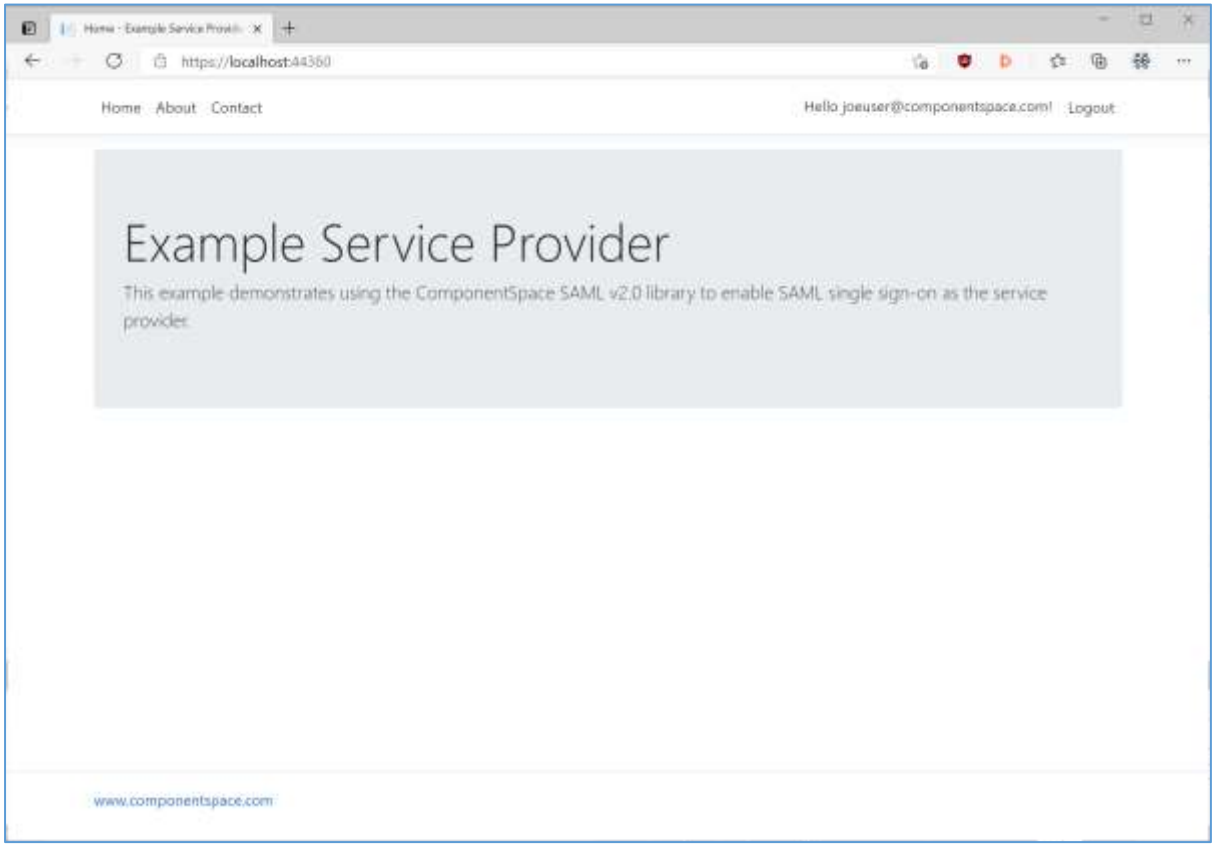
Browse to the example service provider and click the button to SSO to the identity provider.



Login to Okta.



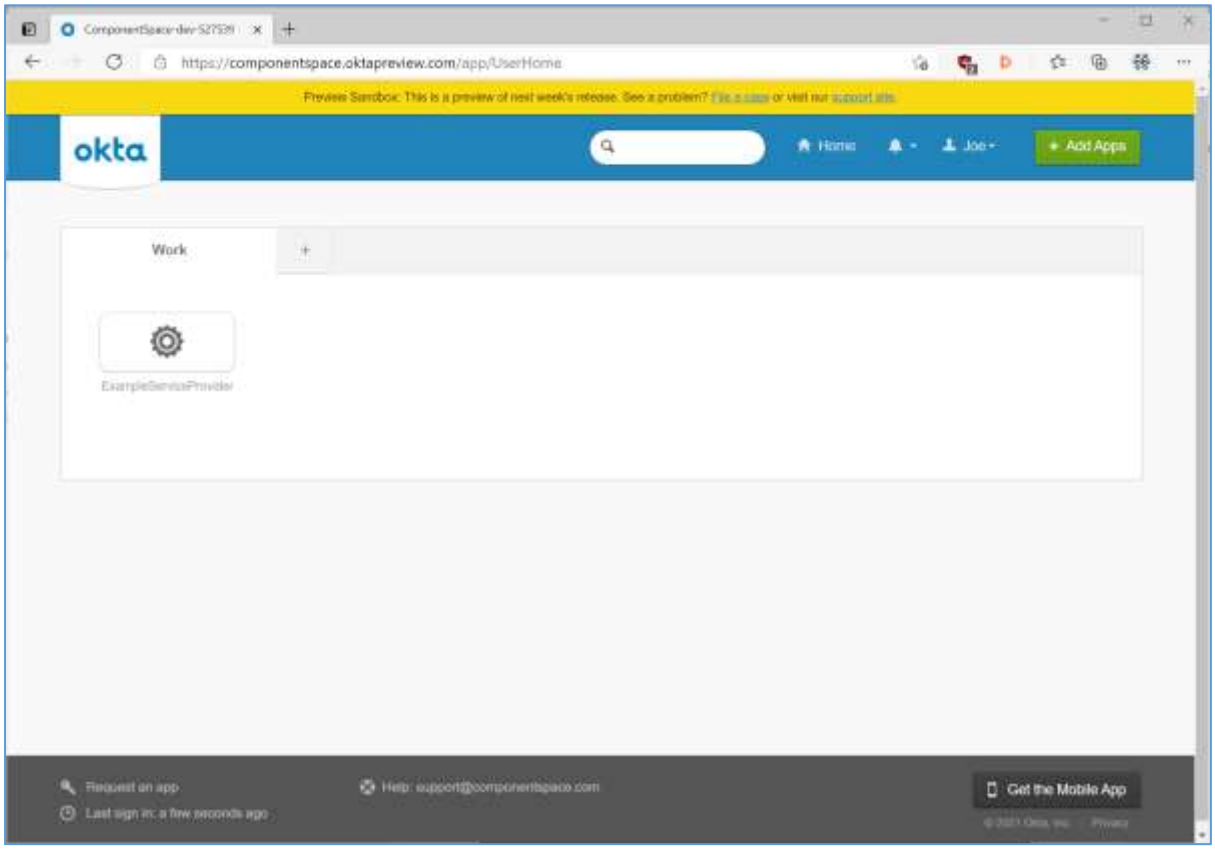
The user is automatically logged in at the service provider.



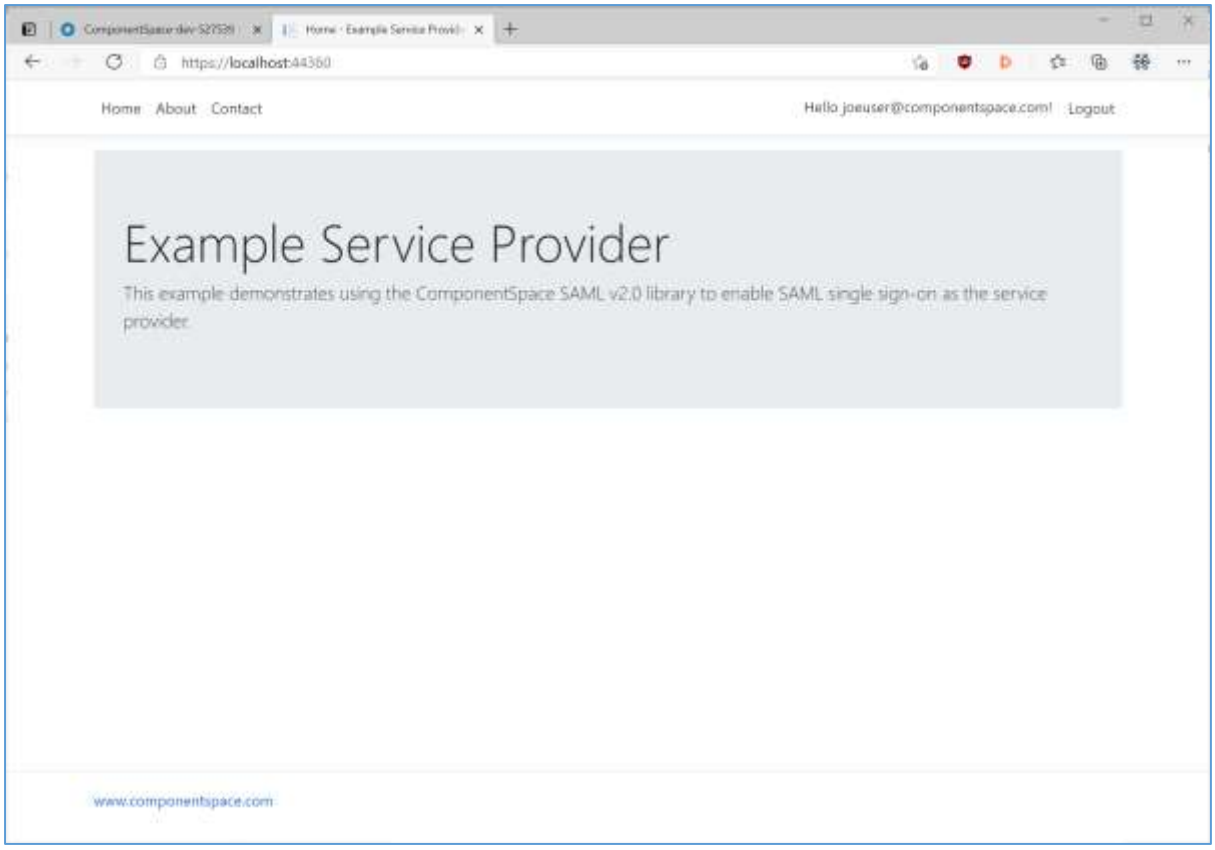
IdP-Initiated SSO

Login to Okta.

Click the ExampleServiceProvider button.



The user is automatically logged in at the service provider.



SAML Logout

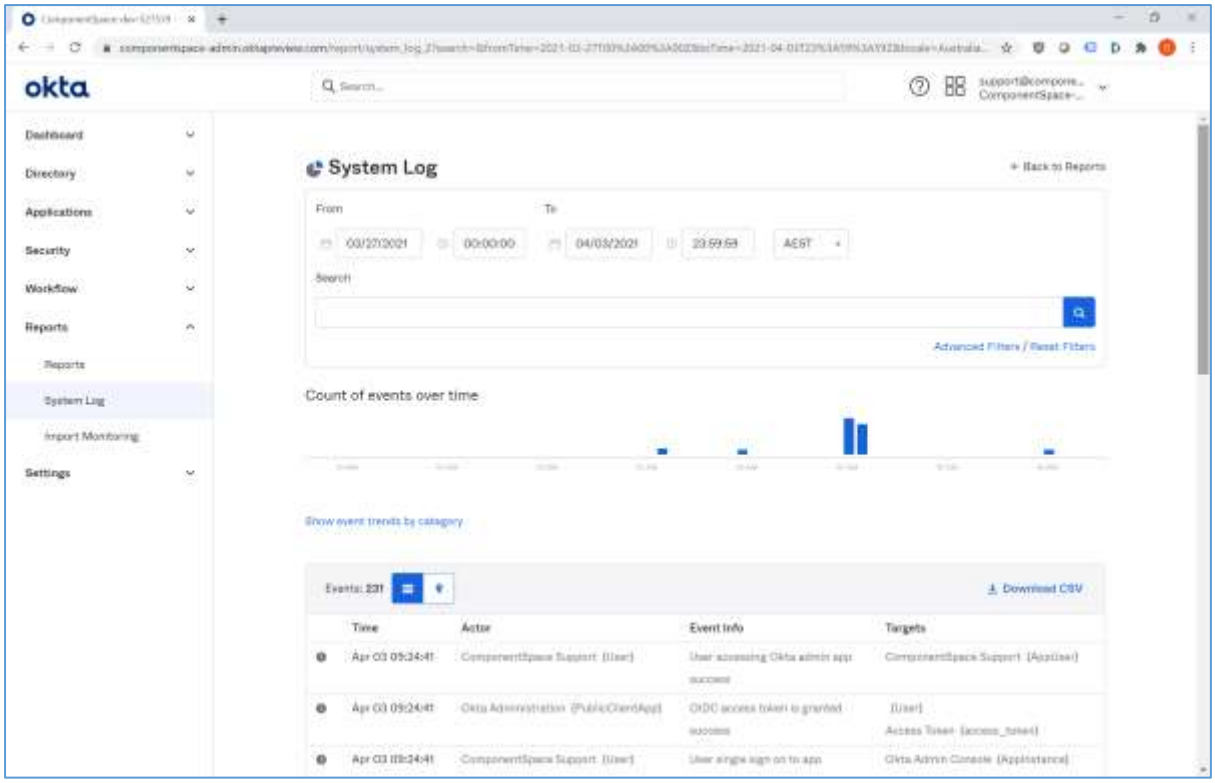
Okta supports SP-initiated SAML logout only.

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.


okta
Dashboard
Directory
Applications
Security
Workflow
Reports
Reports
System Log
Import Monitoring
Settings
System Log
Back to Reports
From
To
Search
Advanced Filters / Reset Filters
Count of events over time
Show event trends by category
Events: 231
Download CSV
Time
Actor
Event Info
Targets