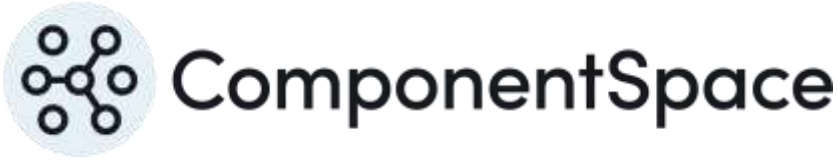


ComponentSpace
SAML for ASP.NET
Azure AD
Integration Guide

www.componentspace.com

Contents

Introduction

This document describes integration with Azure Active Directory as the identity provider.

For information on configuring Azure Active Directory for SAML SSO, refer to the following article.

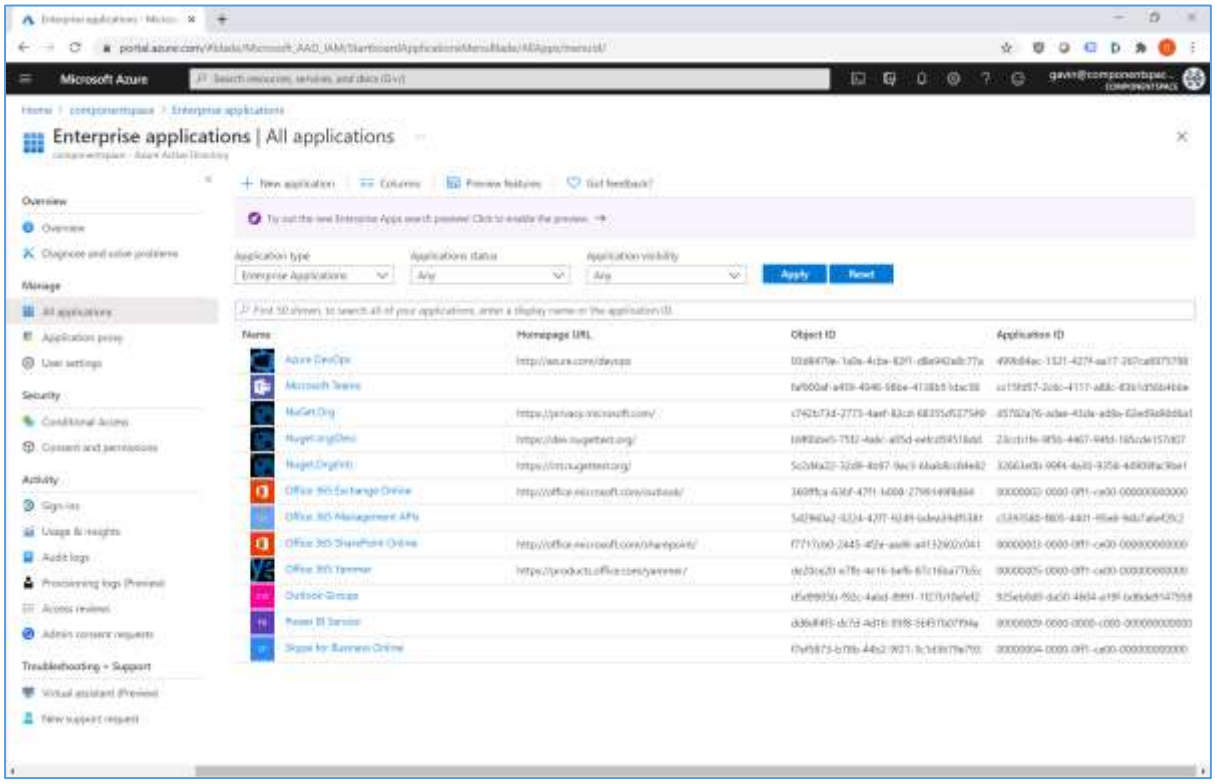
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/add-application-portal-setup-sso

Configuring an Enterprise Application for SAML SSO

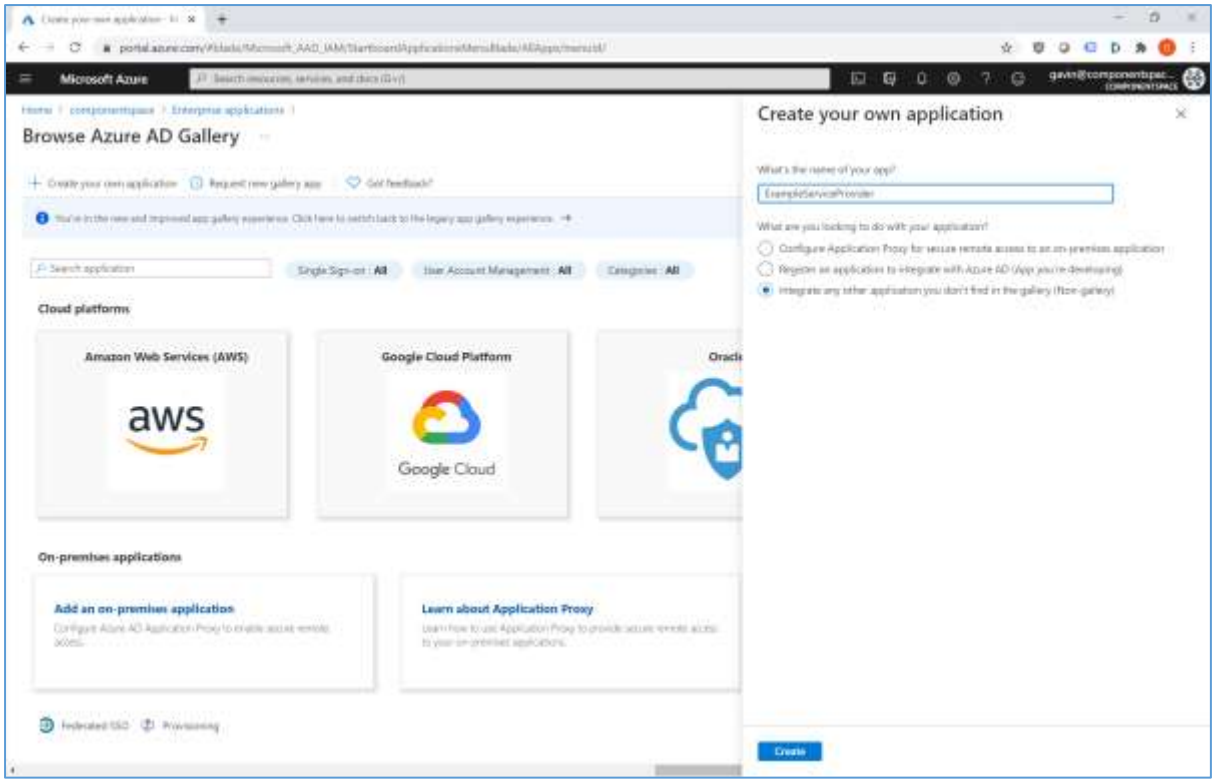
Login to Azure as an administrator.

https://portal.azure.com

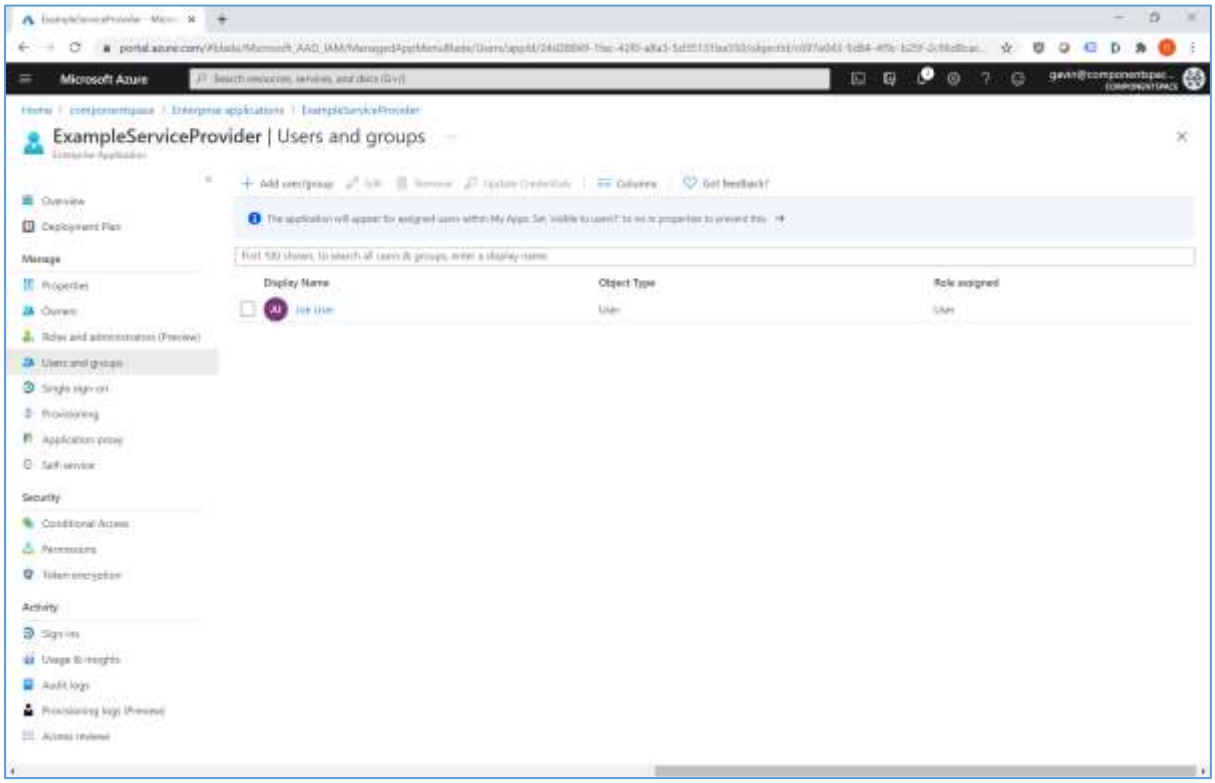
Navigate to enterprise applications for Azure Active Directory.



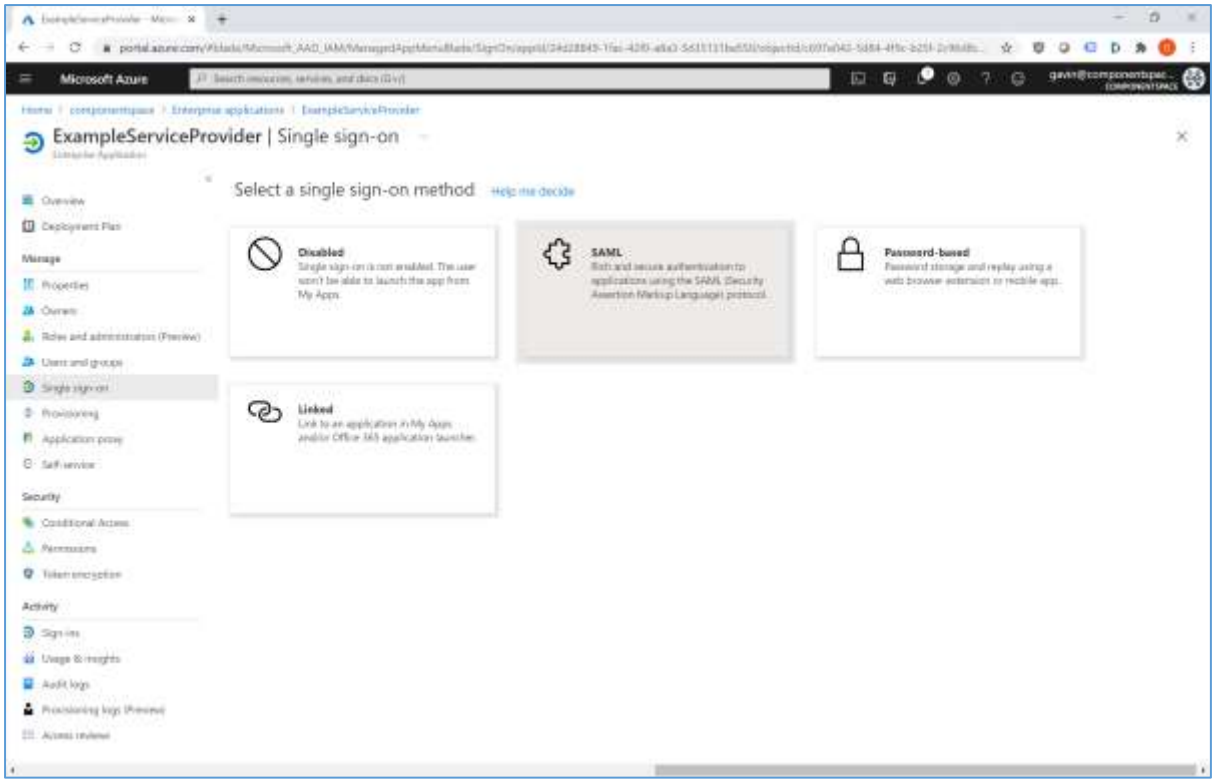
Add a non-gallery application. The application name is for display purposes only.



Assign users access to the application.



Select SAML as the single sign-on method.



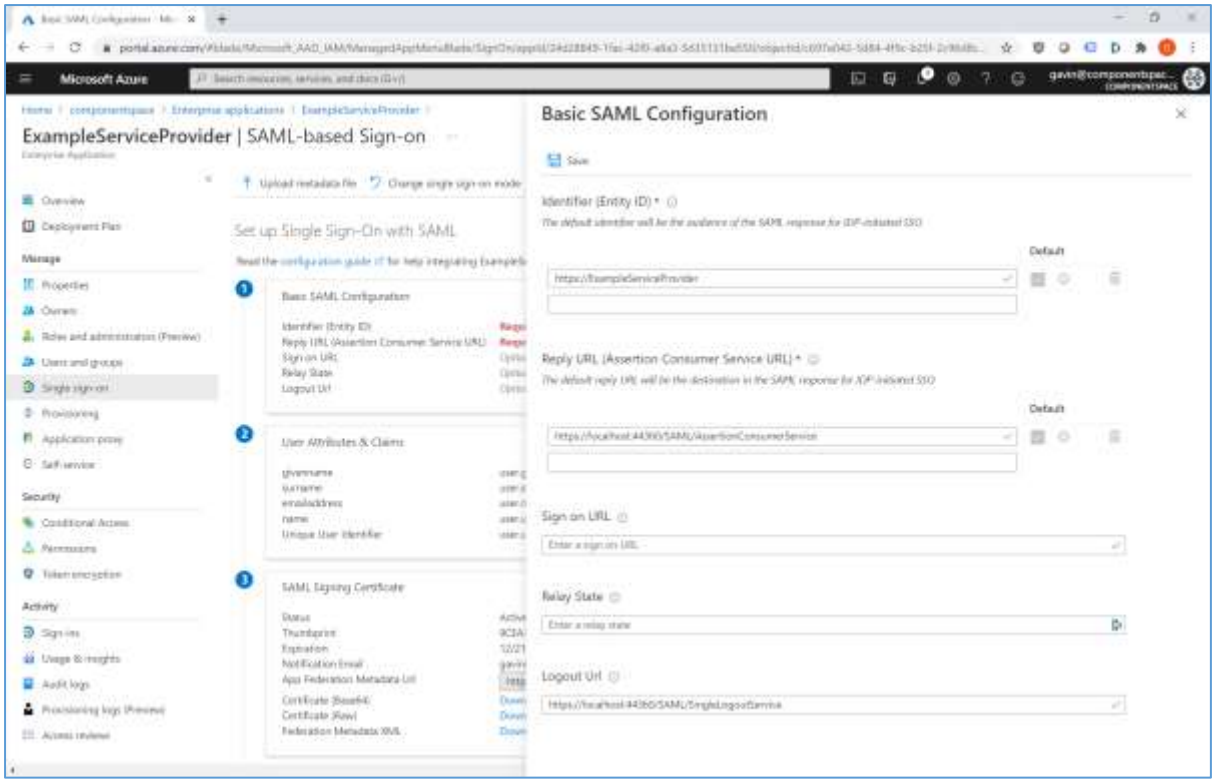
Configure single sign-on.

The identifier is the SAML entity ID. This name must match with the local service provider name. For example, if the LocalServiceProviderConfiguration's Name is https://ExampleServiceProvider, then the identifier must be set to the same value.

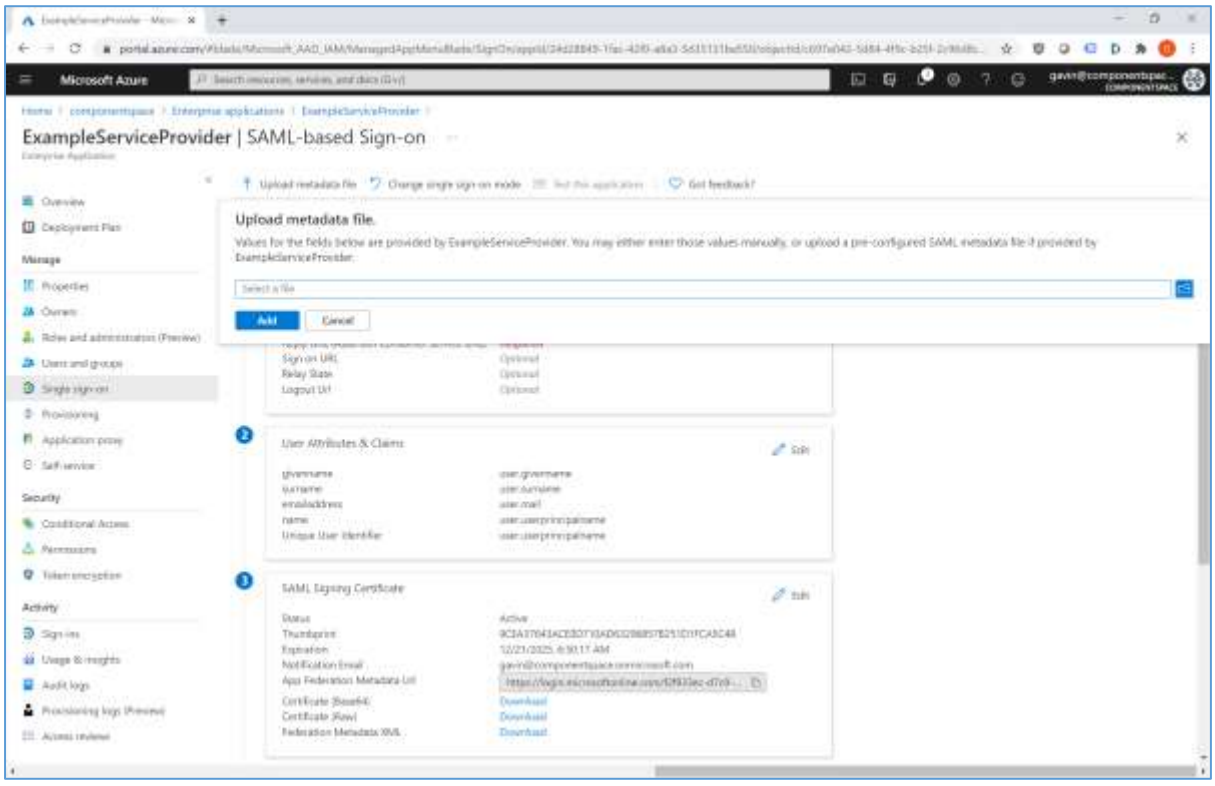
The reply URL is the assertion consumer service URL (e.g. https://localhost:44360/SAML/AssertionConsumerService).

The logout URL is the logout service URL (e.g. https://localhost:44360/SAML/SingleLogoutService).

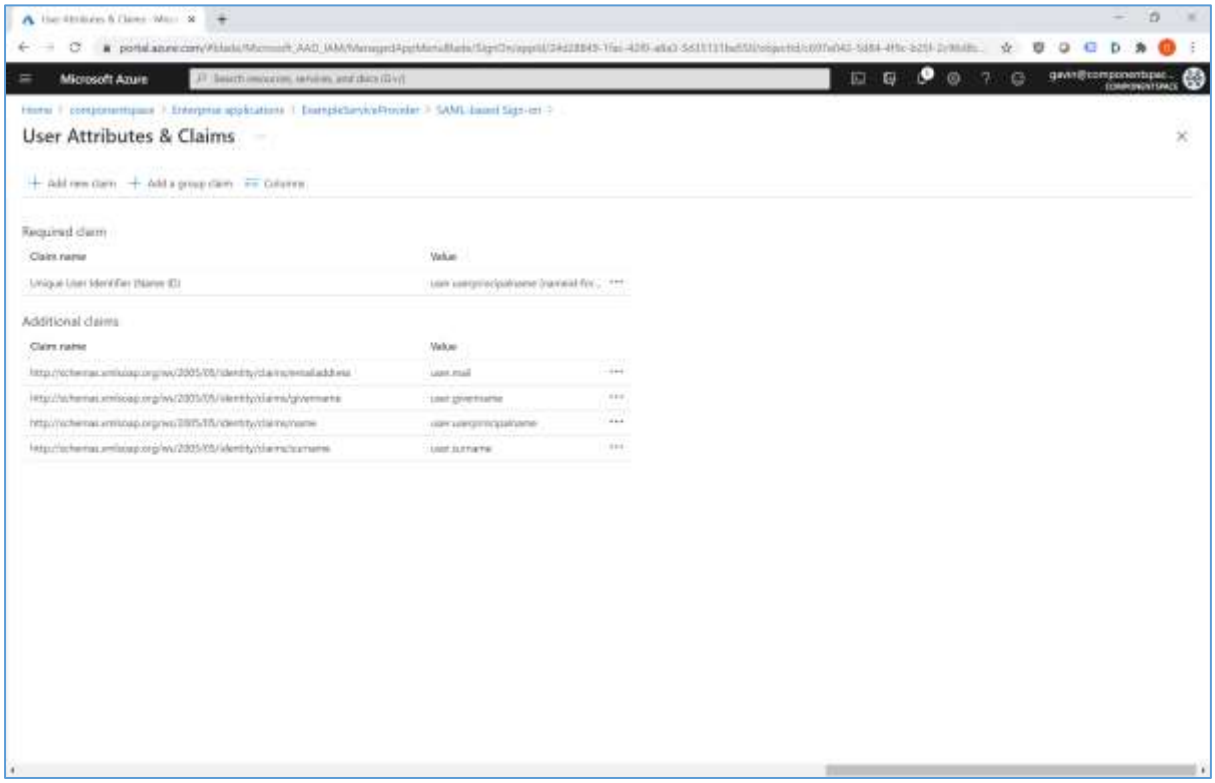
The optional sign on URL and relay state aren't used.



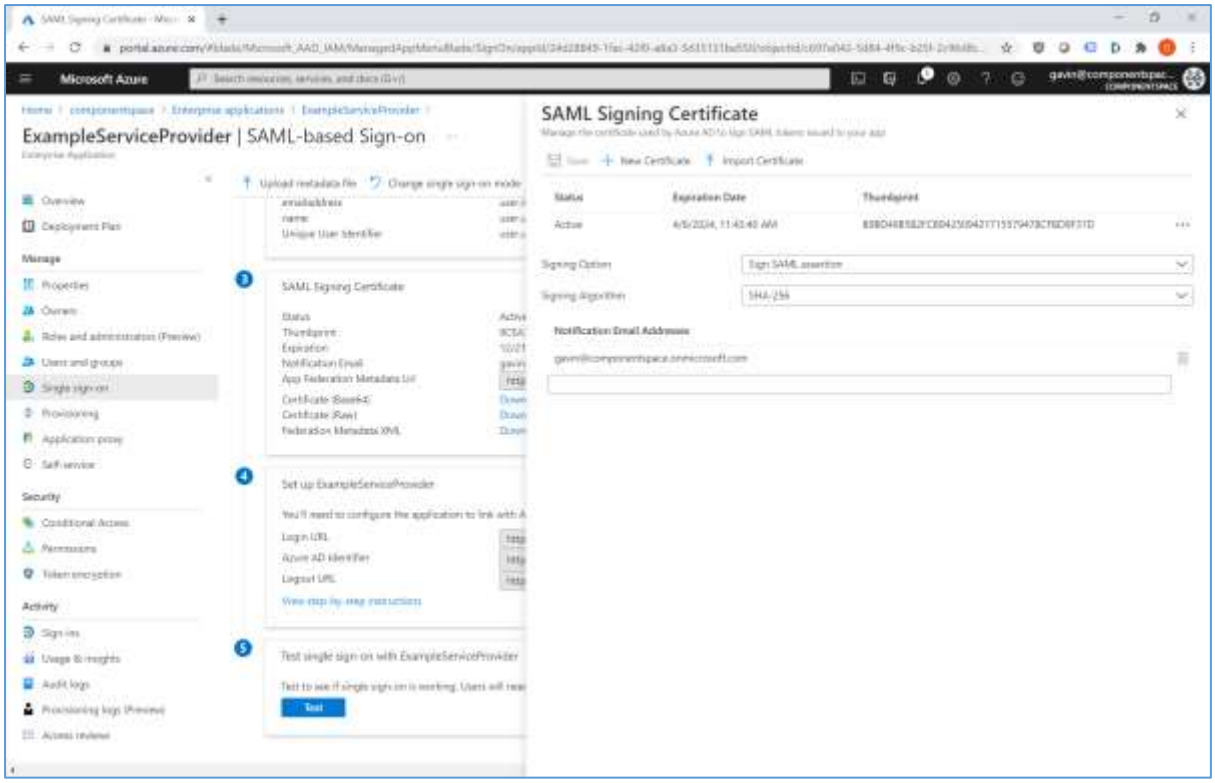
Alternatively, rather than entering these values manually, the service provider SAML metadata file may be uploaded.



User attributes and claims may be edited. These map user properties in Azure Active Directory to the SAML subject name identifier (Name ID) and SAML attributes sent in the SAML assertion as required by the service provider.



The SAML signing certificate is used by Azure AD to sign SAML messages. If required, this certificate and the signature options may be changed.



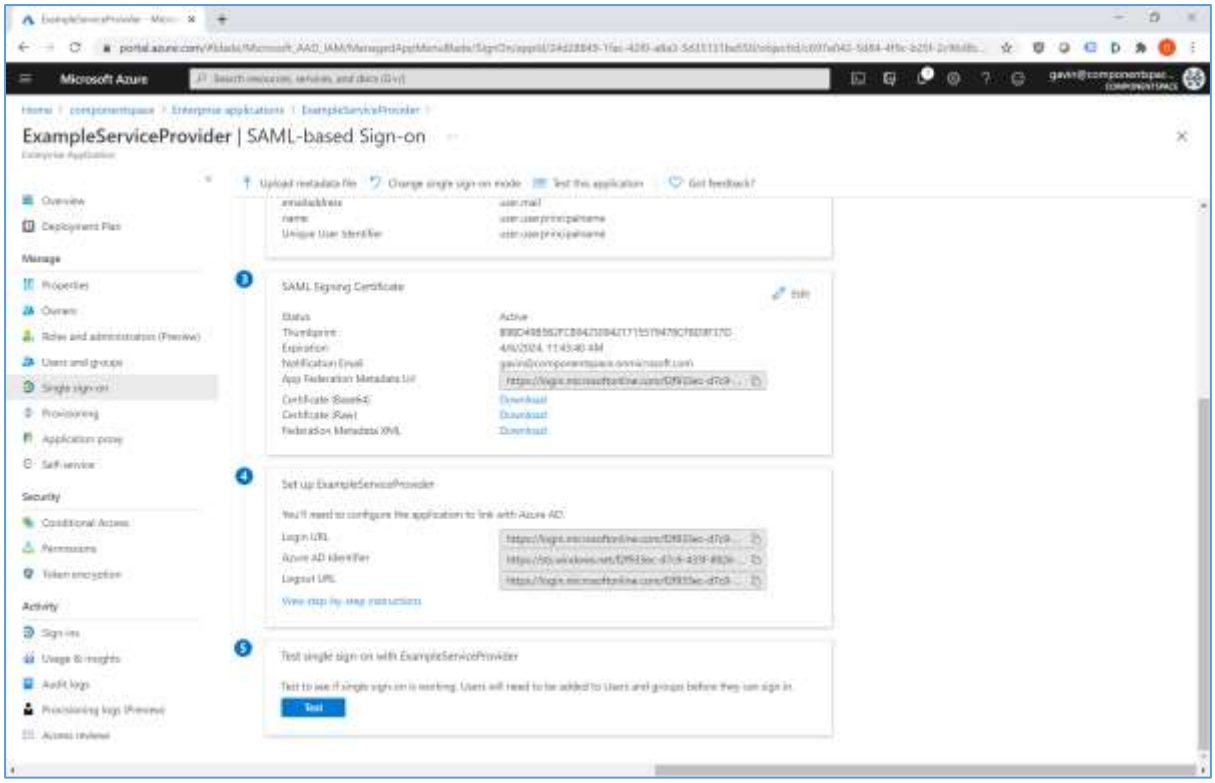
Information is displayed that's required for configuring the service provider application.

The login URL is the PartnerIdentityProviderConfiguration's SingleSignOnServiceUrl.

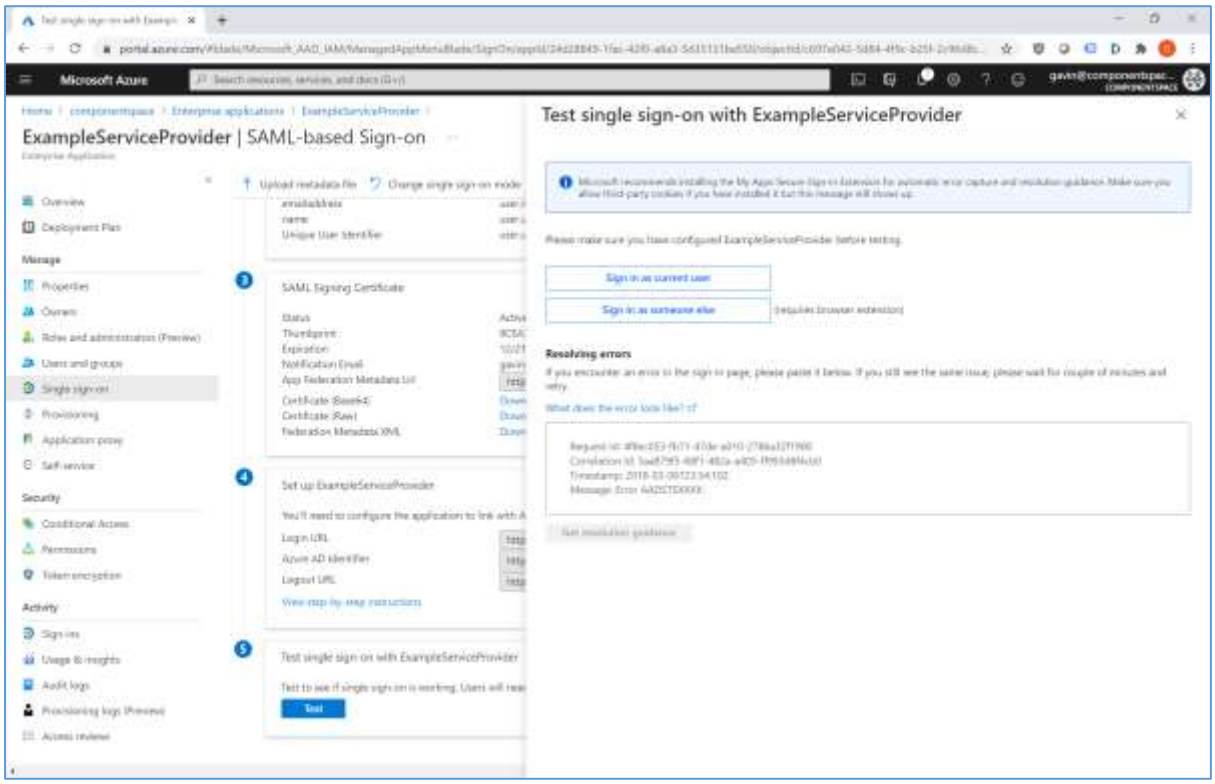
The Azure AD identifier is the PartnerIdentityProviderConfiguration's Name.

The logout URL is the PartnerIdentityProviderConfiguration's SingleLogoutServiceUrl.

Alternatively, the Azure AD federation metadata XML may be downloaded and imported into the service provider's SAML configuration.



Once the Azure AD configuration and the service provider's SAML configuration are complete, SSO may be tested.



Service Provider Configuration

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

```
<PartnerIdentityProvider
  Name="https://sts.windows.net/f2f933ec-d7c9-433f-8926-d3a0732a7dcf/"
  Description="Azure AD"
  SignLogoutRequest="true"
  SignLogoutResponse="true"
  SingleSignOnServiceUrl="https://login.microsoftonline.com/f2f933ec-d7c9-433f-8926-
d3a0732a7dcf/saml2"
  SingleLogoutServiceUrl="https://login.microsoftonline.com/f2f933ec-d7c9-433f-8926-
d3a0732a7dcf/saml2">
  <PartnerCertificates>
    <Certificate FileName="Certificates\azure.cer"/>
  </PartnerCertificates>
</PartnerIdentityProvider>
```

This information is available as part of the enterprise application single sign-on configuration in Azure AD.

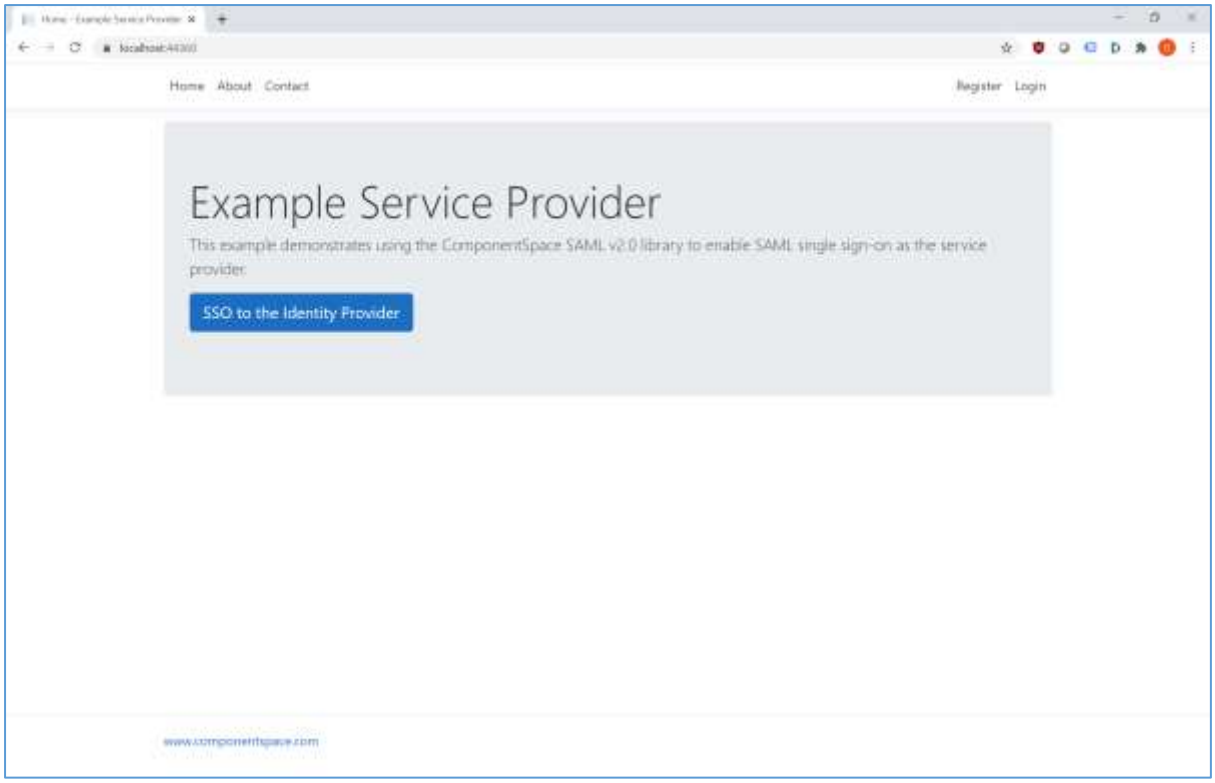
The partner certificate is the SAML signing certificate downloaded from Azure AD. We recommend downloading the base-64 encoded certificate.

Ensure the PartnerName specifies the correct partner identity provider.

```
<add key="PartnerName" value="https://sts.windows.net/f2f933ec-d7c9-433f-8926-
d3a0732a7dcf/"/>
```

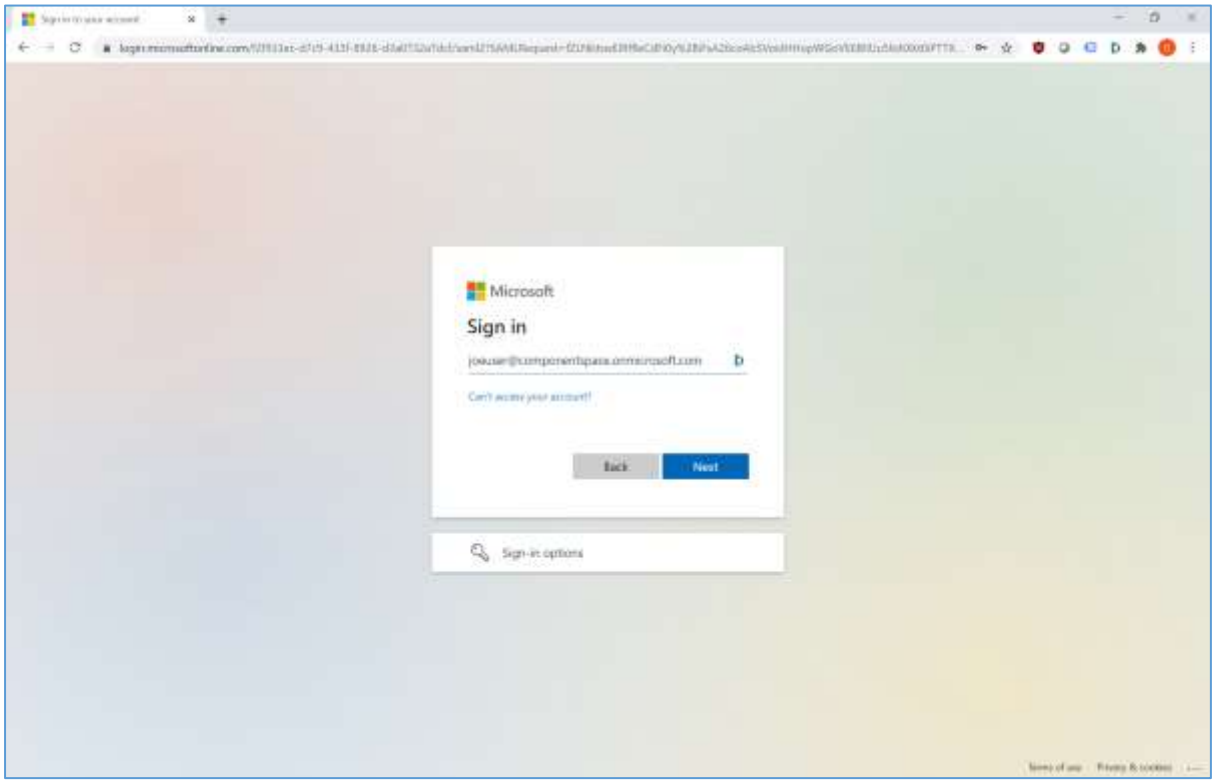
SP-Initiated SSO

Browse to the example service provider.

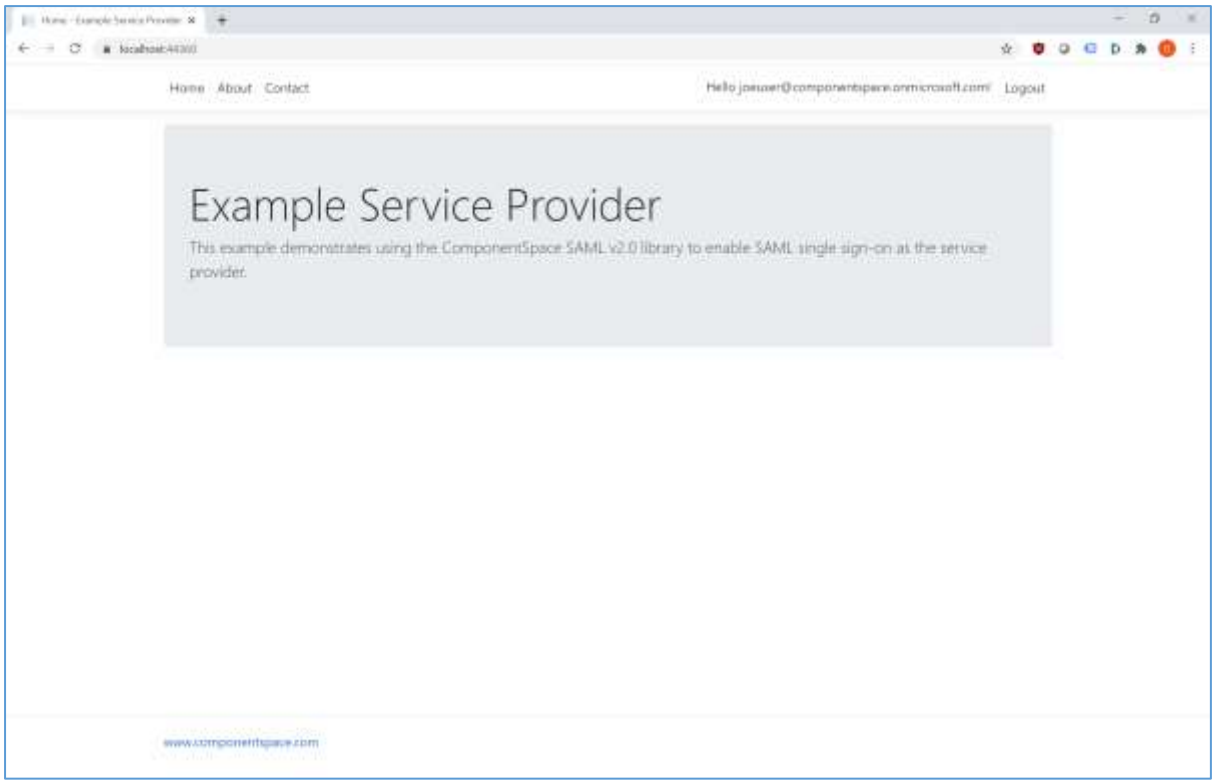


Click the button to SSO to the identity provider.

Login to Azure as a user assigned to the application.



The user is automatically logged in at the service provider.

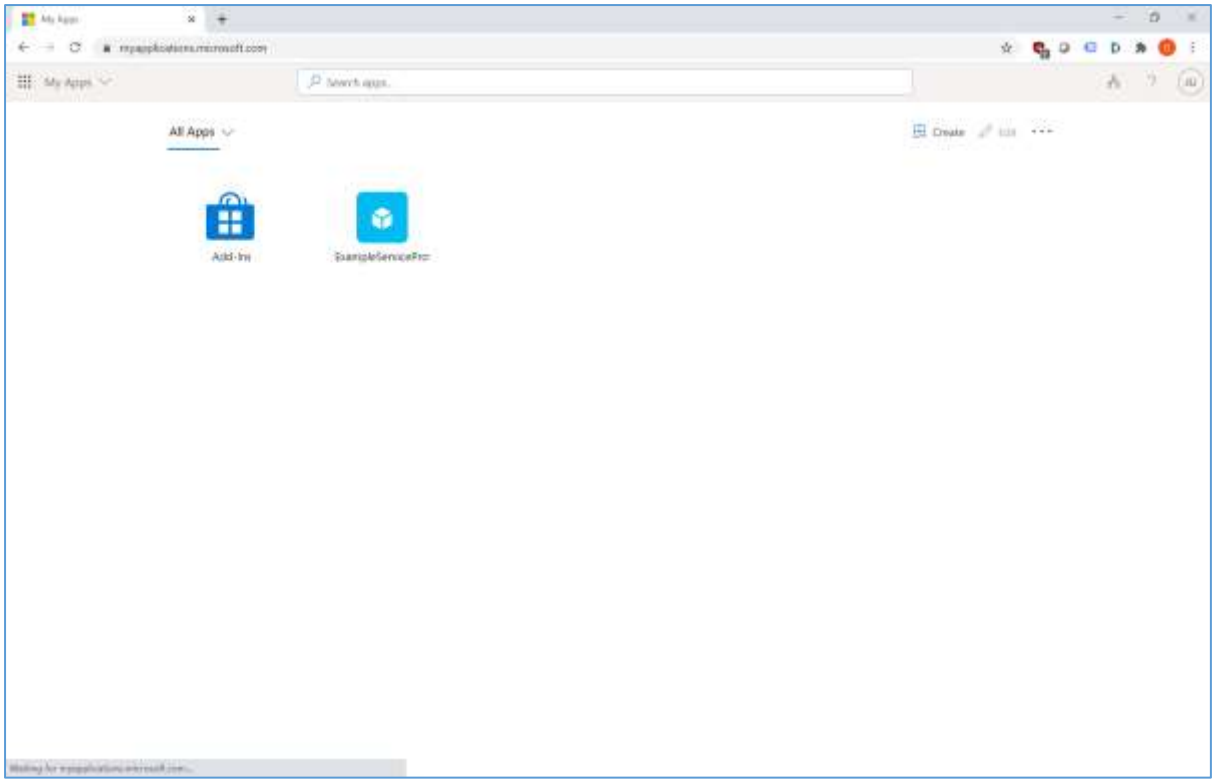


IdP-Initiated SSO

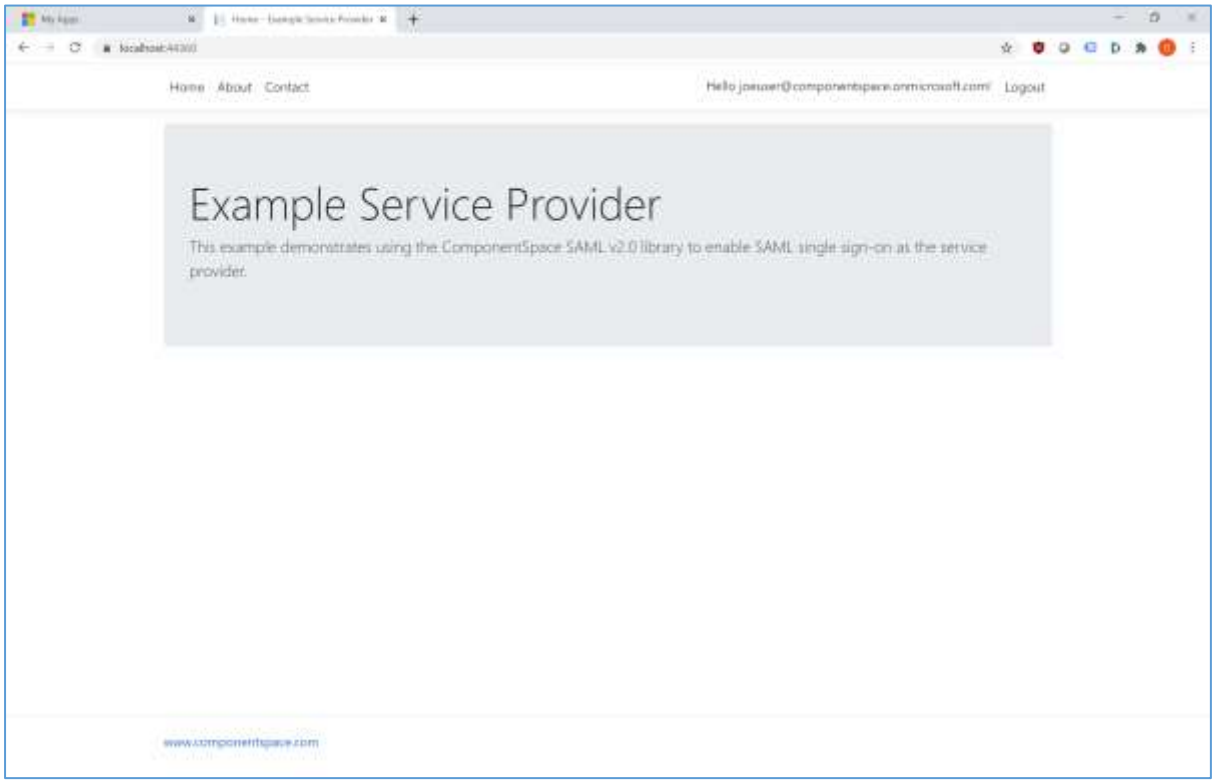
Browse to https://myapps.microsoft.com and login.

Alternatively, browse to the Azure user access URL specified in the application properties for direct access to the application.

Select the ExampleServiceProvider application.



The user is automatically logged in at the service provider.



SAML Logout

Azure Active Directory supports both SP-initiated and IdP-initiated SAML logout.

Troubleshooting

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