# ComponentSpace SAML for ASP.NET Entra ID (Azure AD) Integration Guide


www.componentspace.com

# Contents

# Introduction

This document describes integration with Microsoft Entra ID (previously known as Azure Active Directory) as the identity provider.

For information on configuring Microsoft Entra ID 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

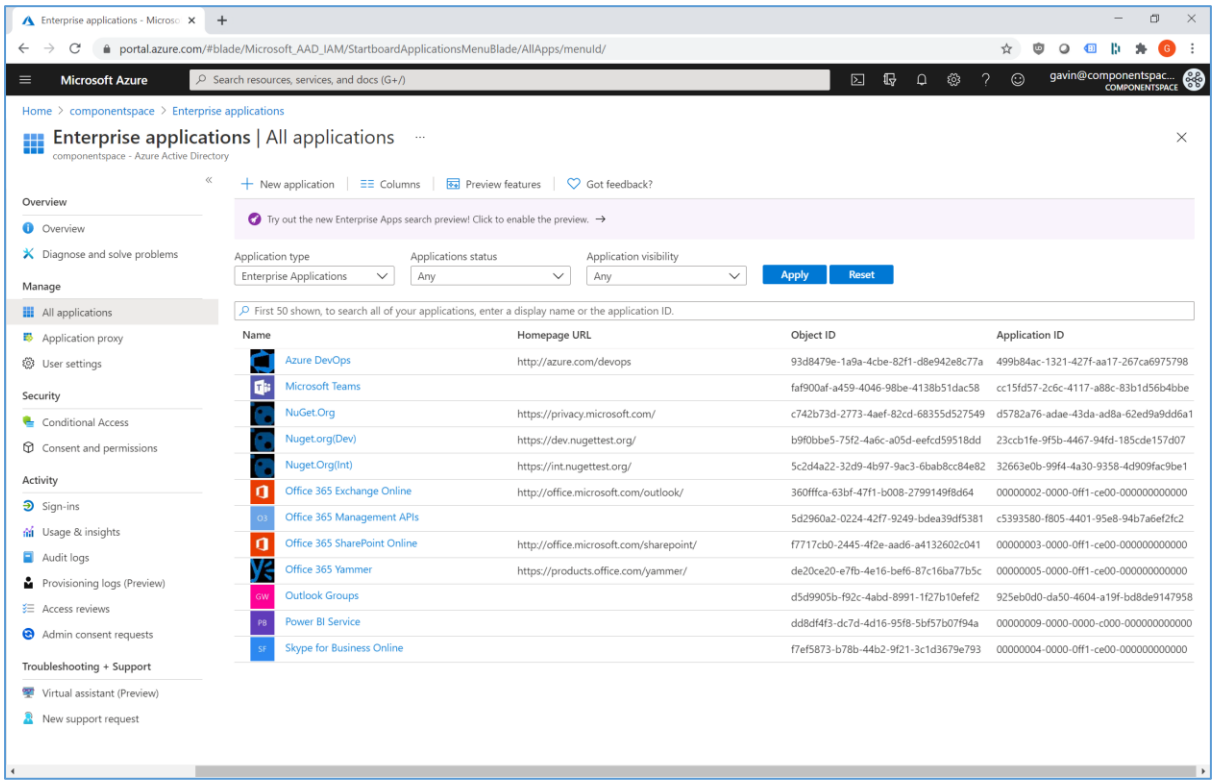
Login to Microsoft Entra as an administrator.

https://entra.microsoft.com

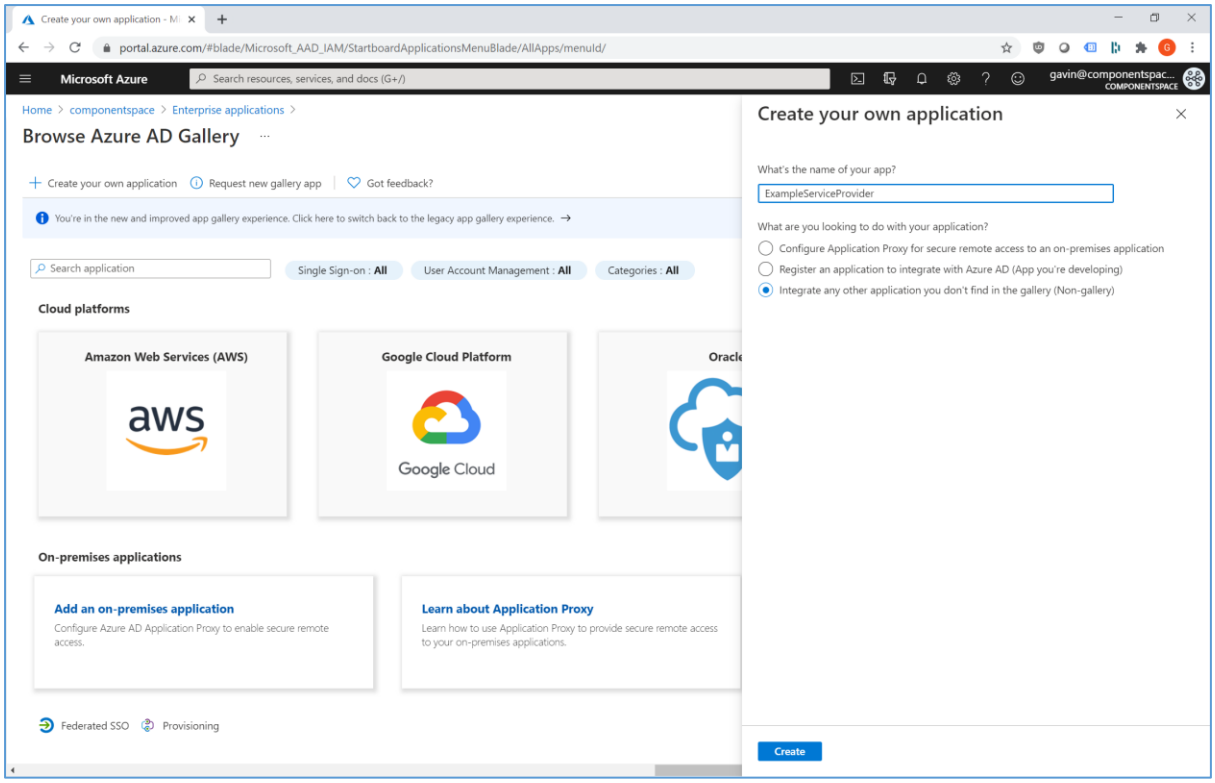
It's also possible to access the configuration through Azure.

https://portal.azure.com

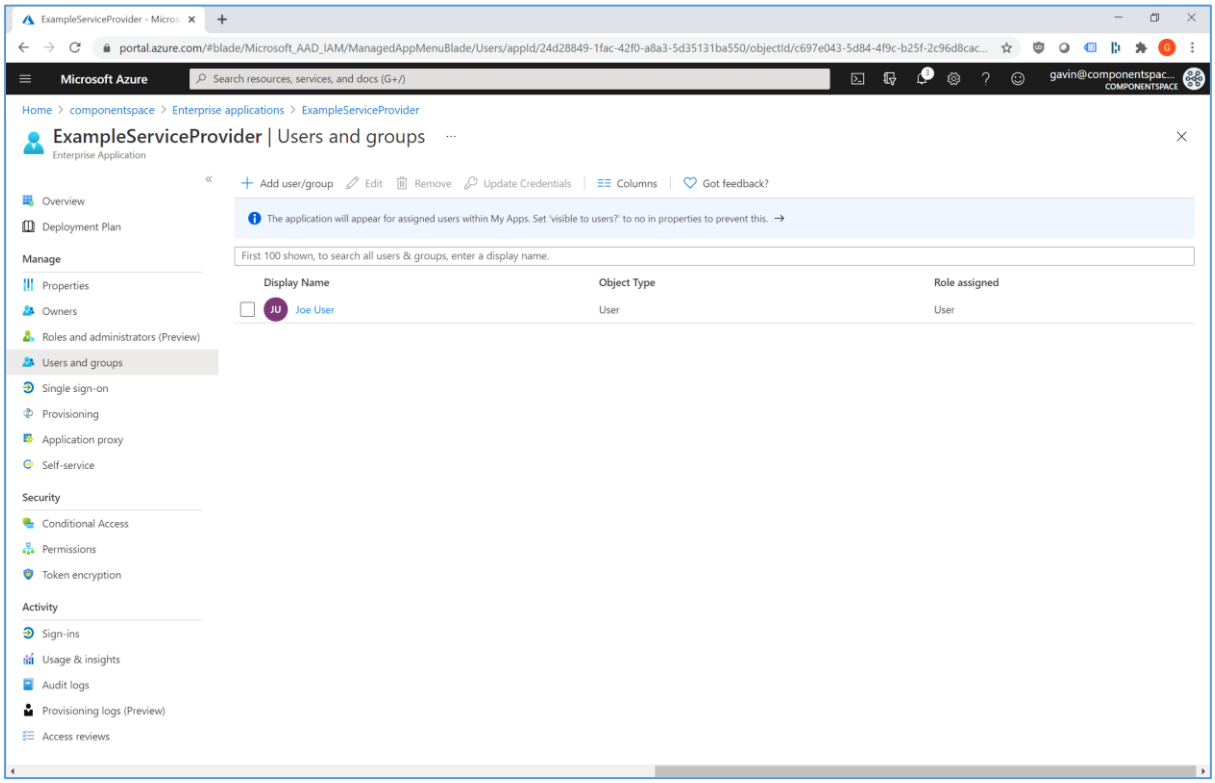
Navigate to enterprise applications for Microsoft Entra.



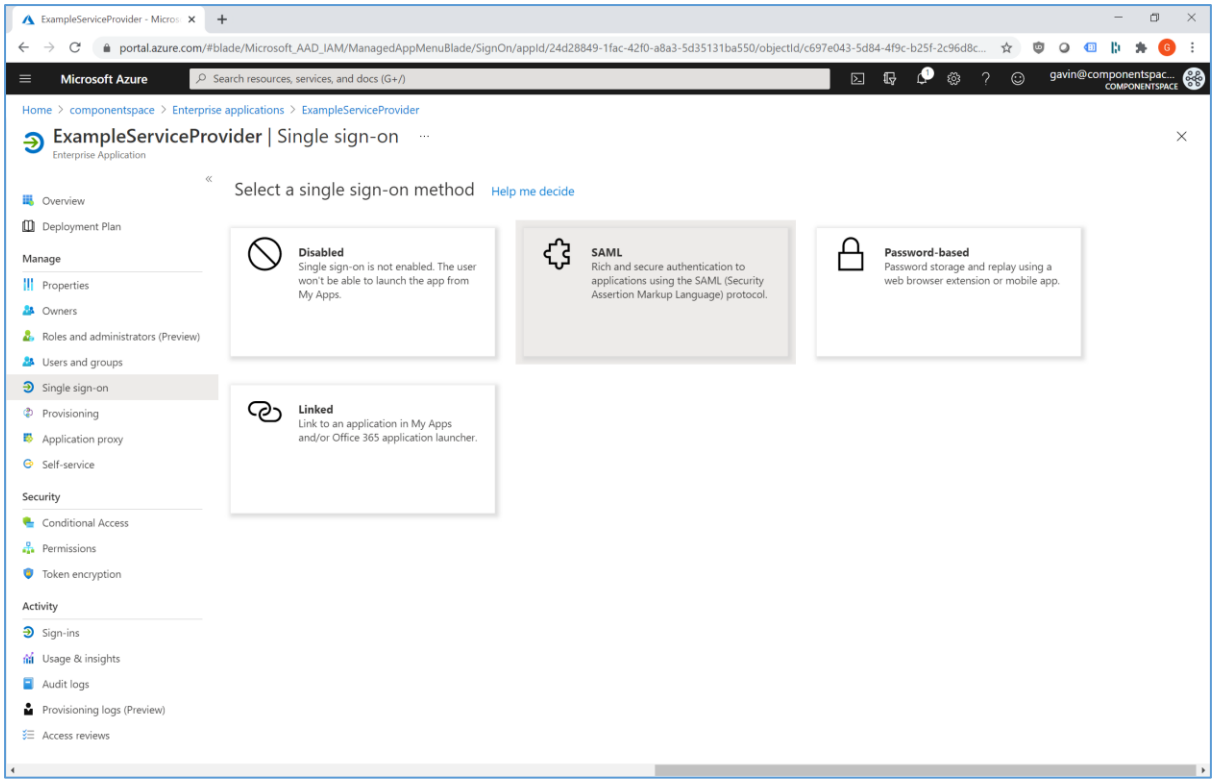

Add a non-gallery application. The application name is for display purposes only.




Assign users access to the application.




Select SAML as the single sign-on method.




Configure single sign-on.

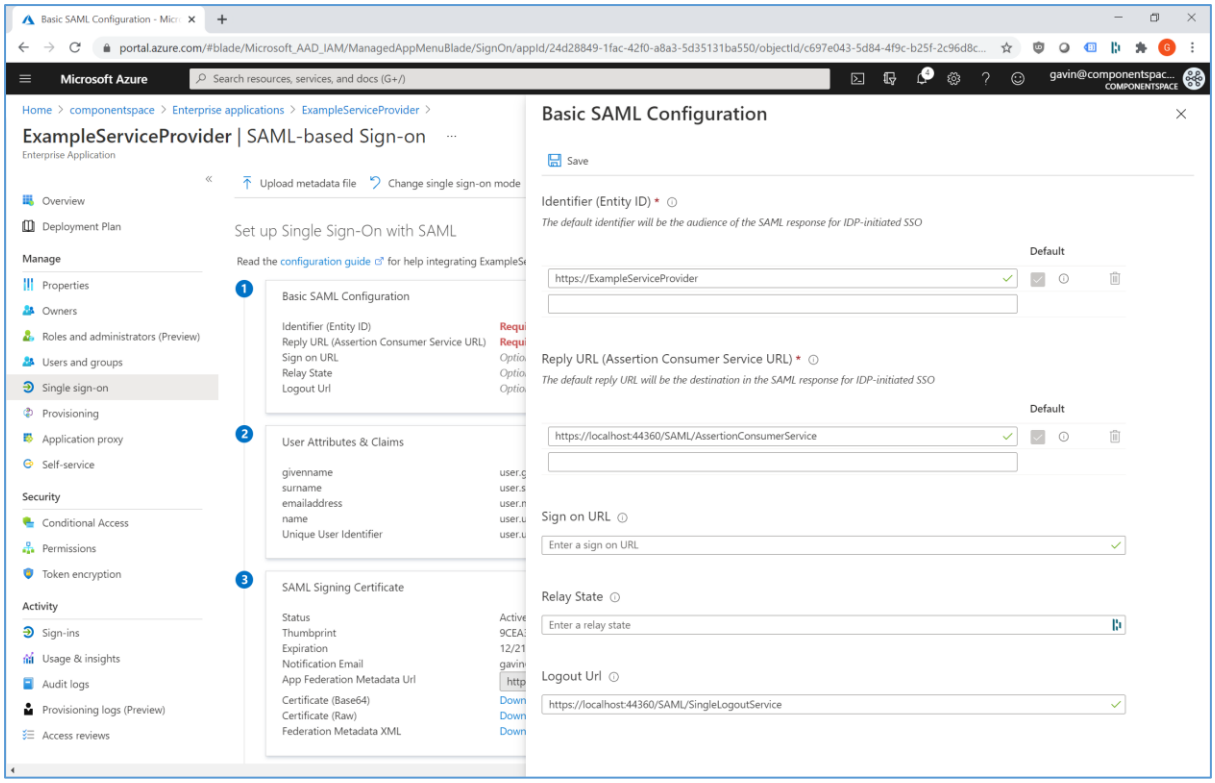
The identifier is the SAML entity ID. This name must match with the local service provider name. For example, if the LocalServiceProviderConfiguration's Name is https://ExampleServiceProvider, then the identifier must be set to the same value.

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

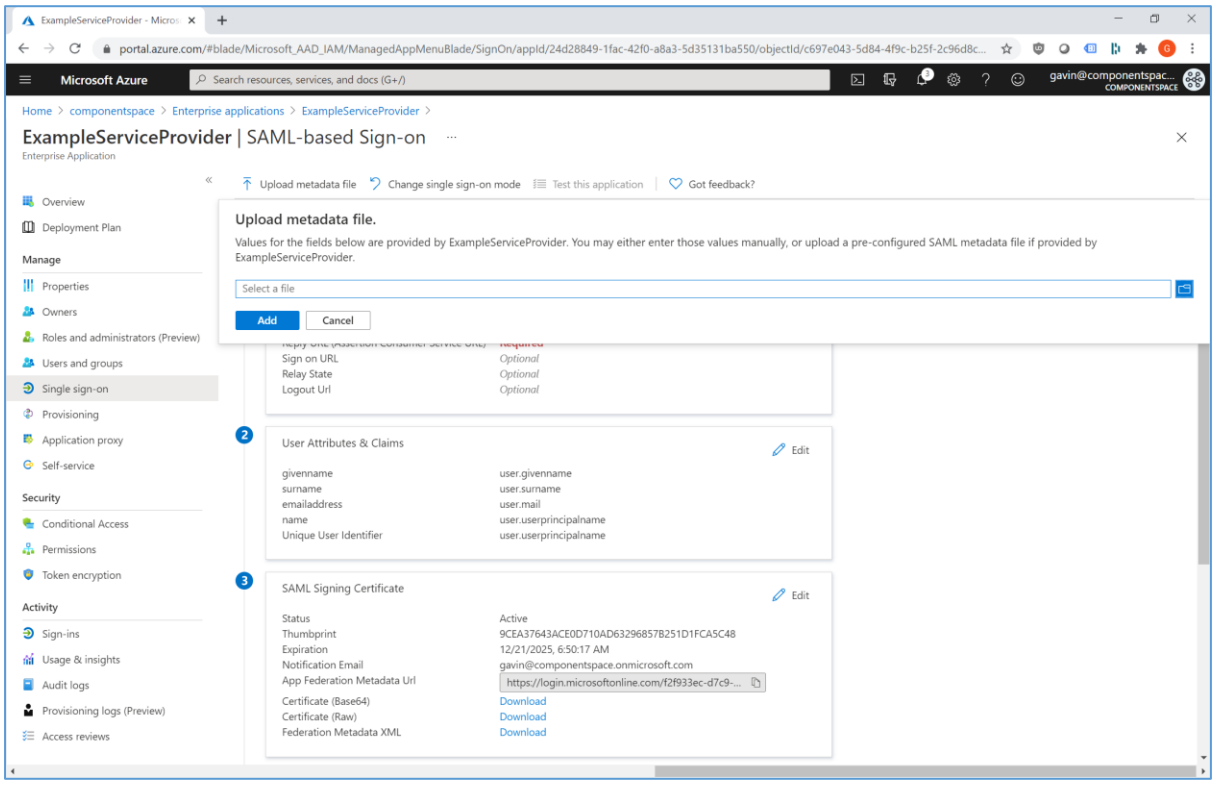
The logout URL is the logout service URL (e.g. https://localhost:44360/SAML/SingleLogoutService).

The optional Sign On URL isn't used. It's for those scenarios where the service provider doesn't support IdP-initiated SSO.  Microsoft Entra will redirect to this URL and then expect the SP to initiate SSO back to Microsoft Entra (i.e. SP-initiated SSO). It's not part of the actual SSO flow or SAML specification but rather a workaround for when IdP-initiated SSO isn't supported.

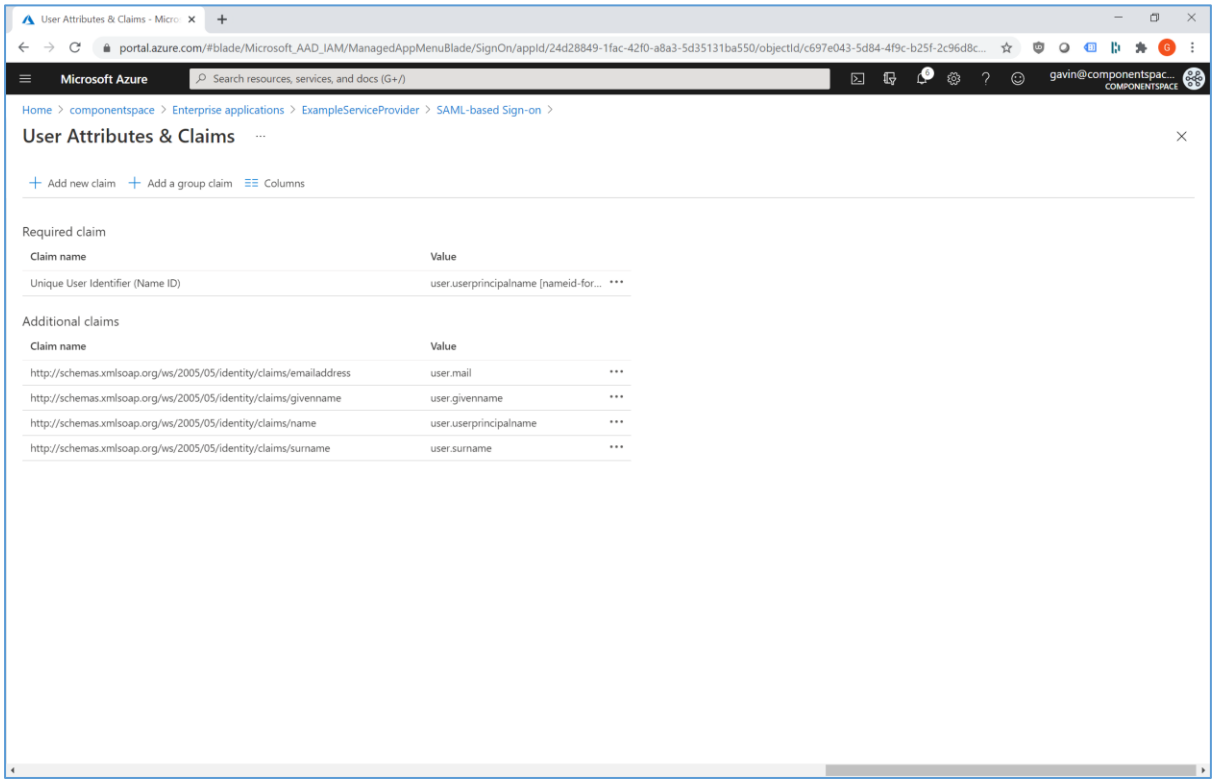
The optional relay state isn't used.



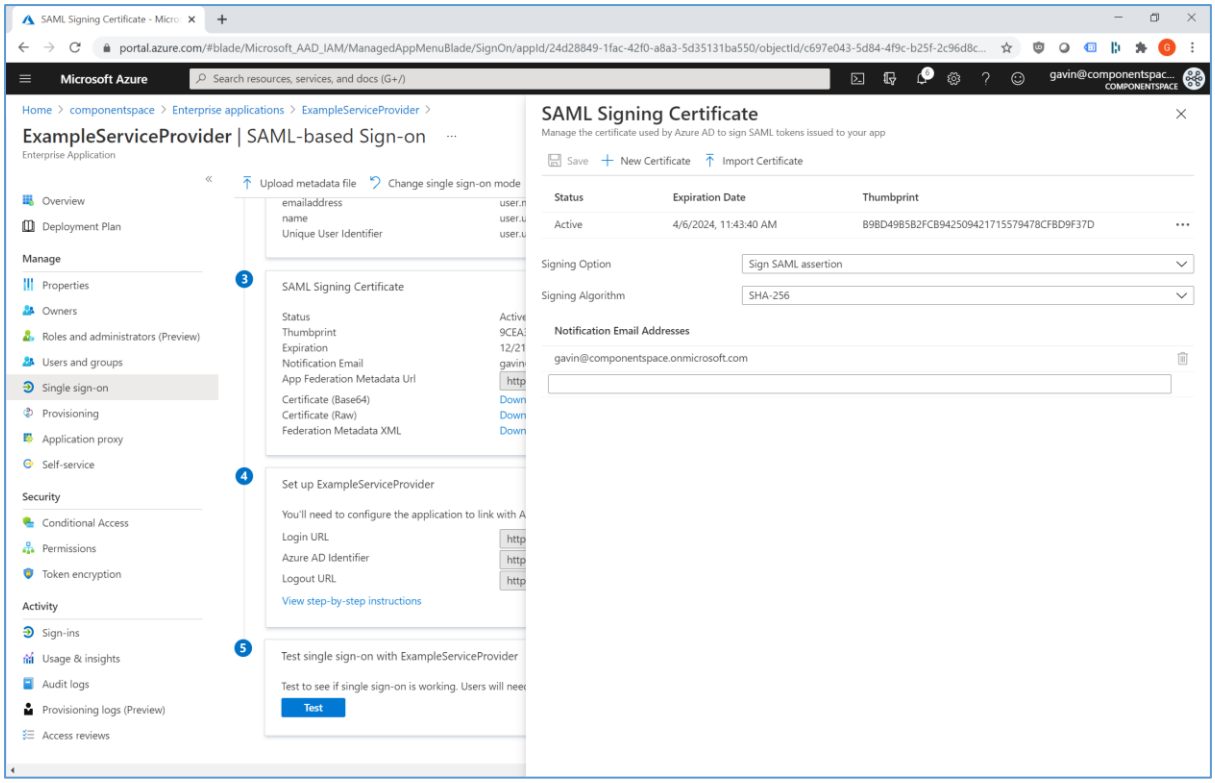

Alternatively, rather than entering these values manually, the service provider SAML metadata file may be uploaded.



User attributes and claims may be edited. These map user properties in Microsoft Entra 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 Microsoft Entra to sign SAML messages. If required, this certificate and the signature options may be changed.



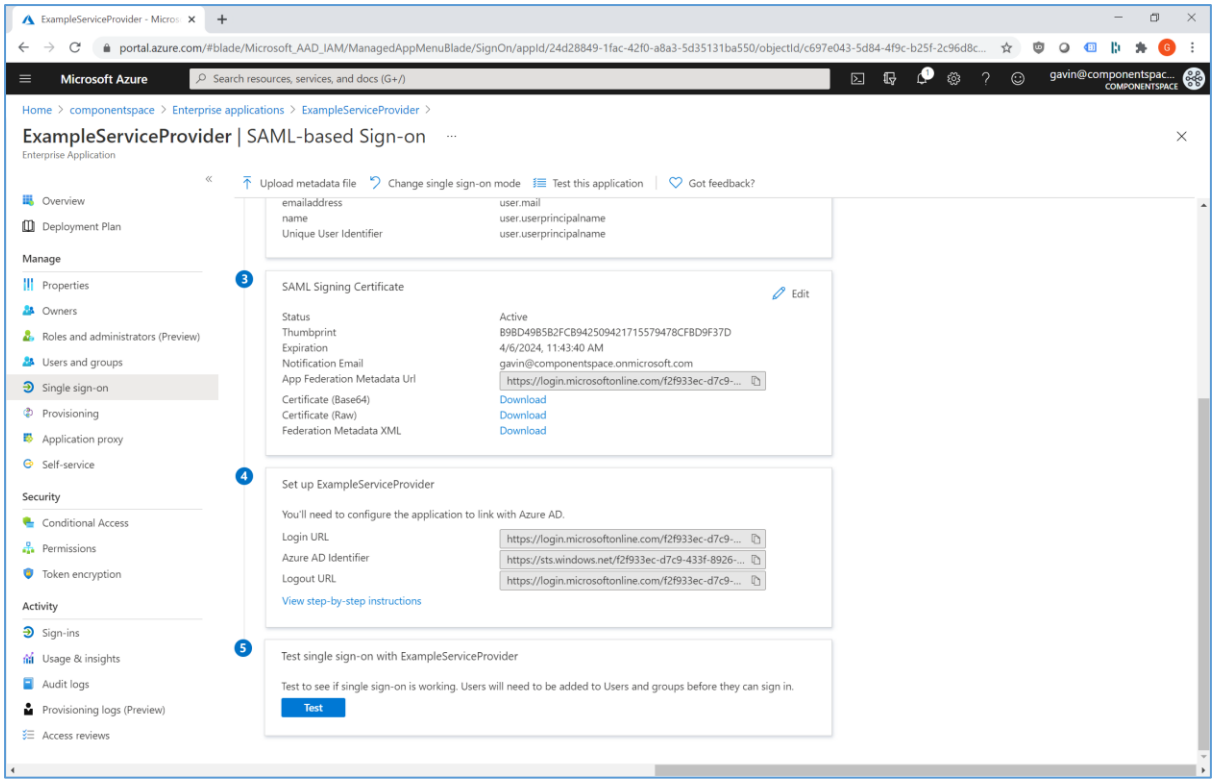

Information is displayed that's required for configuring the service provider application.

The login URL is the PartnerIdentityProviderConfiguration's SingleSignOnServiceUrl.

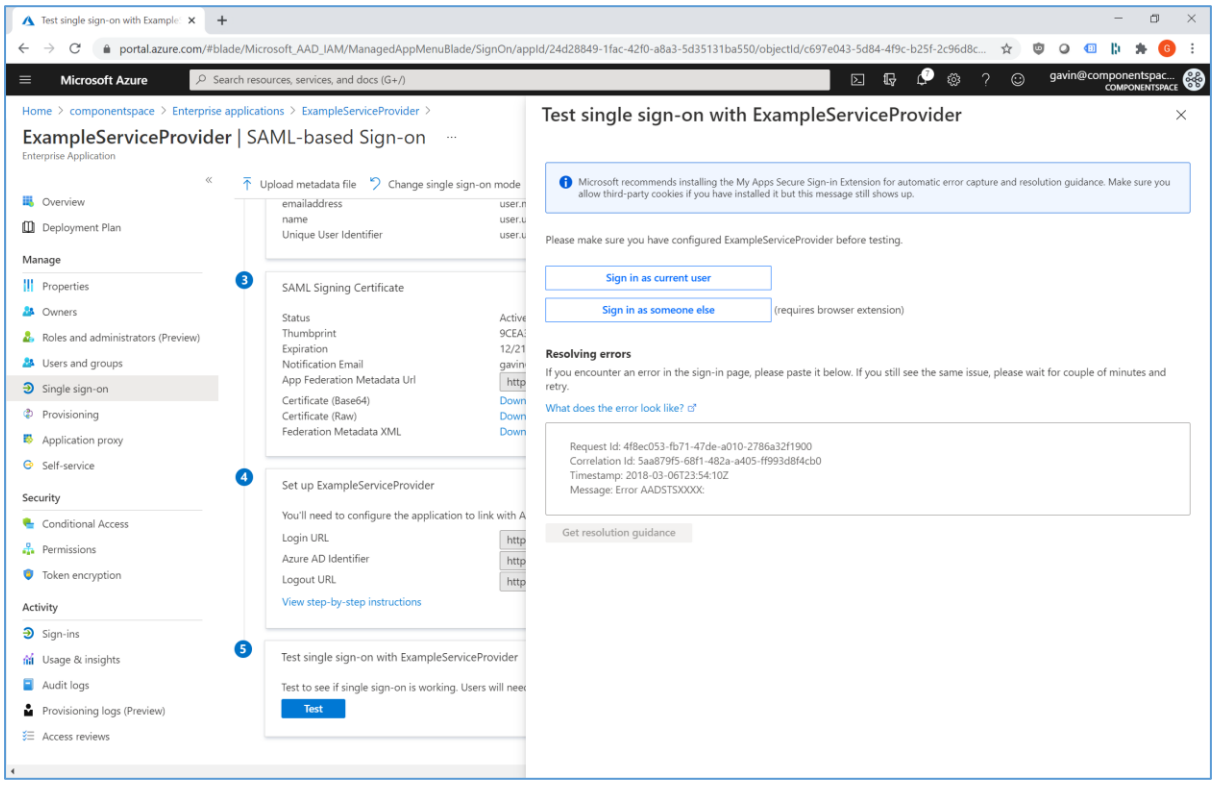
The Microsoft Entra identifier is the PartnerIdentityProviderConfiguration's Name.

The logout URL is the PartnerIdentityProviderConfiguration's SingleLogoutServiceUrl.

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




Once the Microsoft Entra 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="Microsoft Entra ID"
 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 Microsoft Entra.

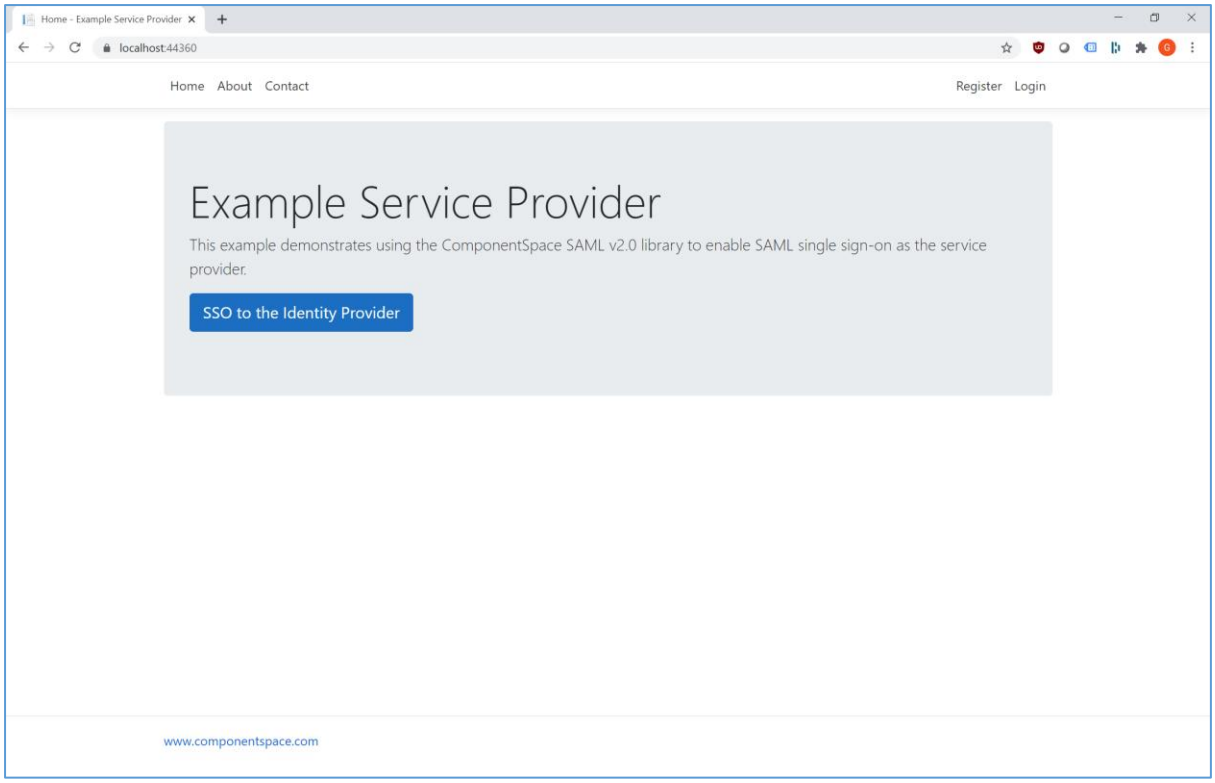
The partner certificate is the SAML signing certificate downloaded from Microsoft Entra. We recommend downloading the base-64 encoded certificate.

Ensure the PartnerName specifies the correct partner identity provider.

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

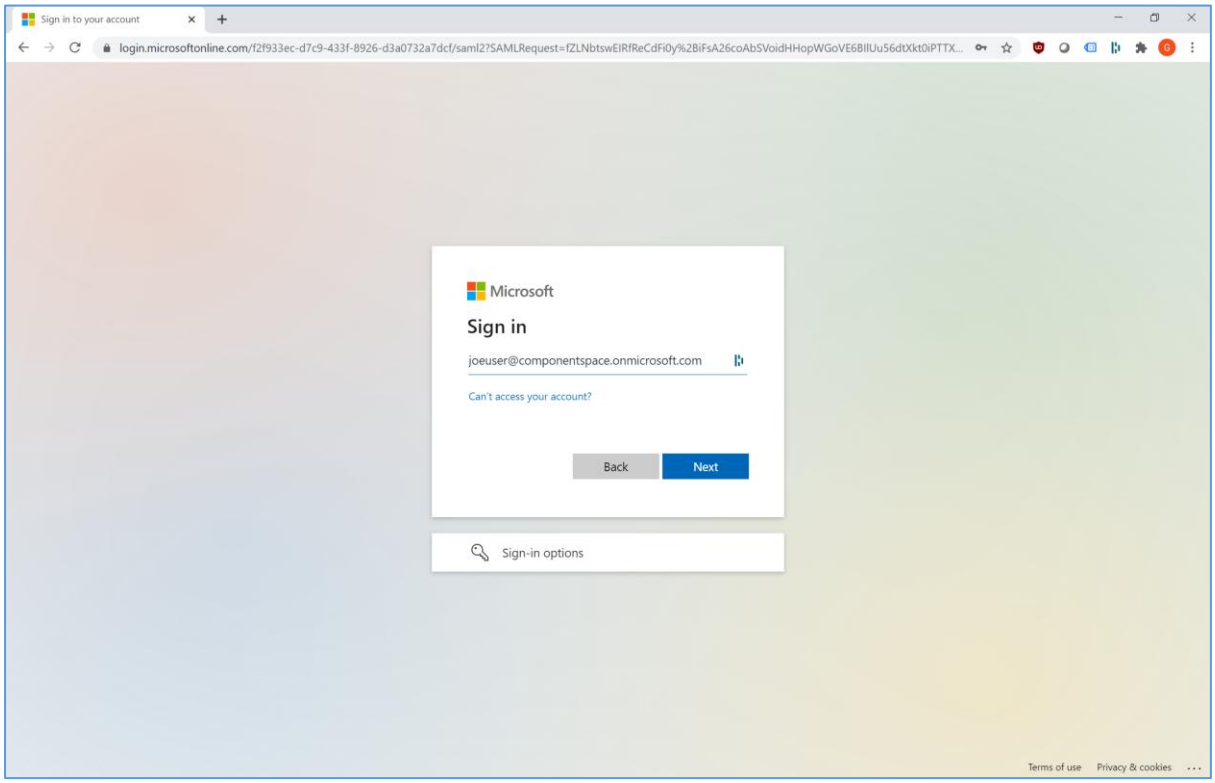
## SP-Initiated SSO

Browse to the example service provider.

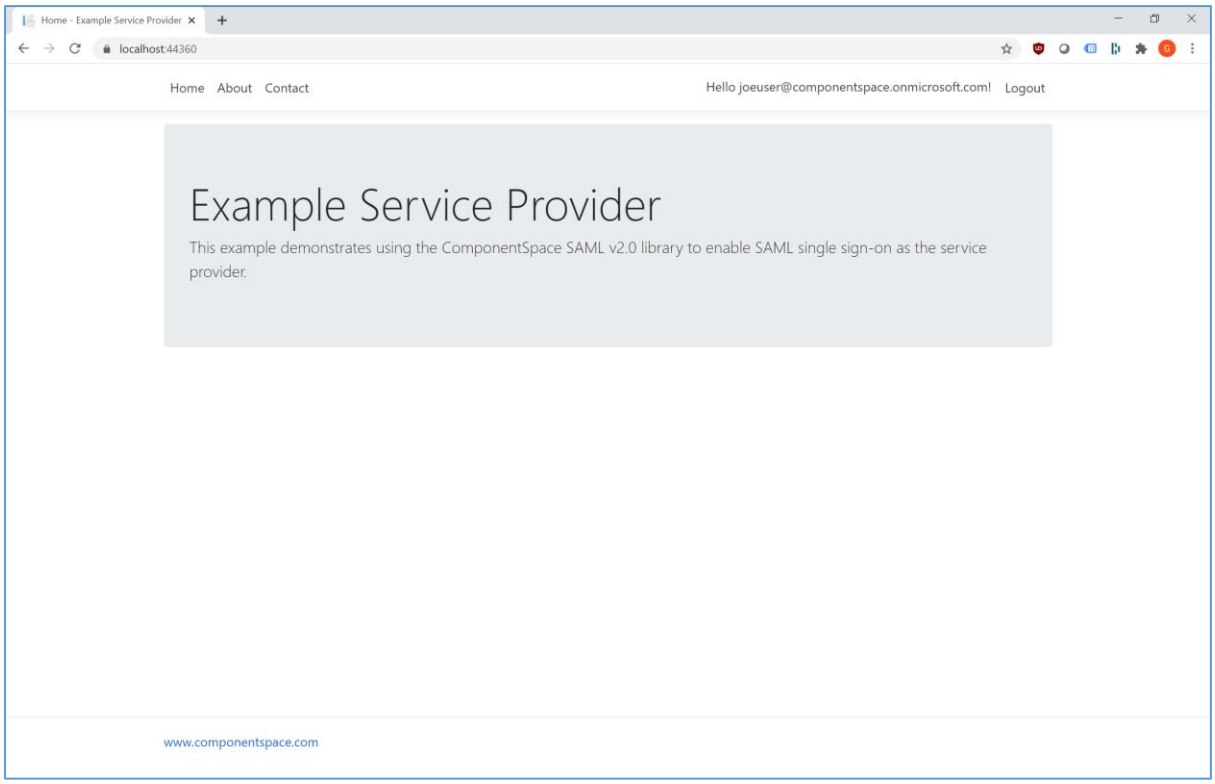



Click the button to SSO to the identity provider.

Login to Microsoft Entra as a user assigned to the application.



The user is automatically logged in at the service provider.

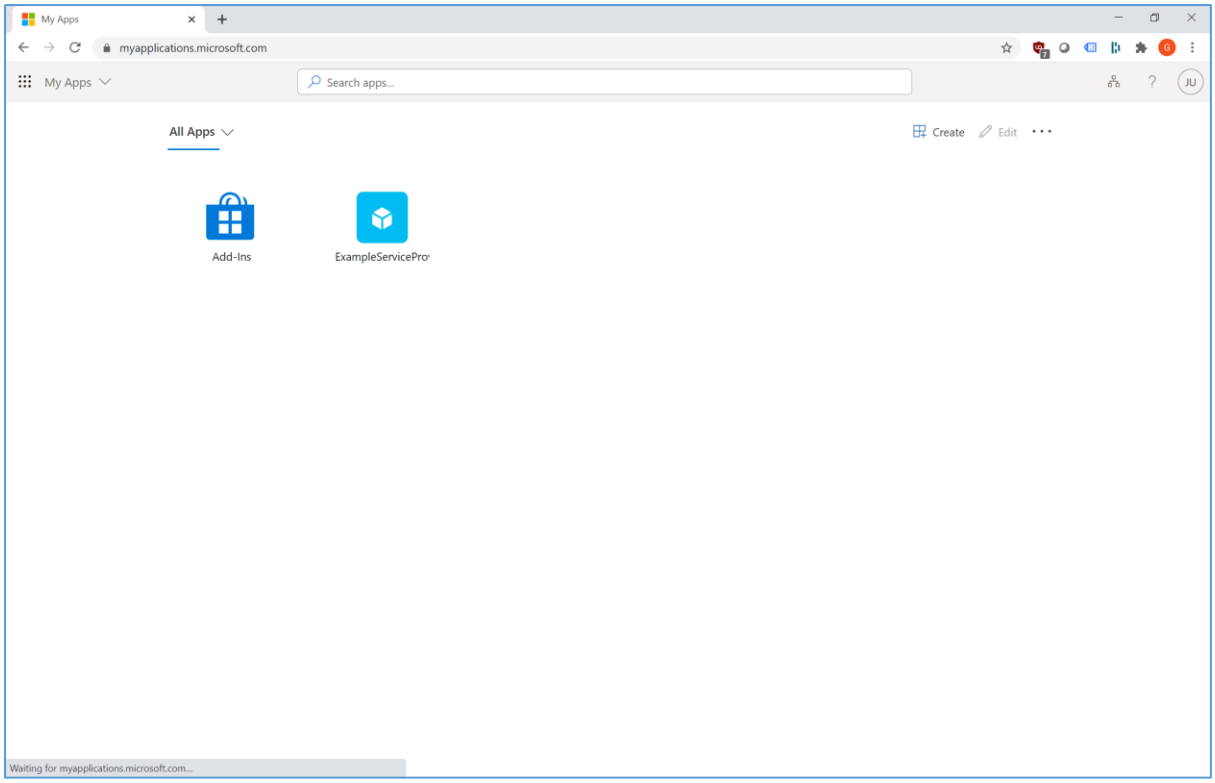



## IdP-Initiated SSO

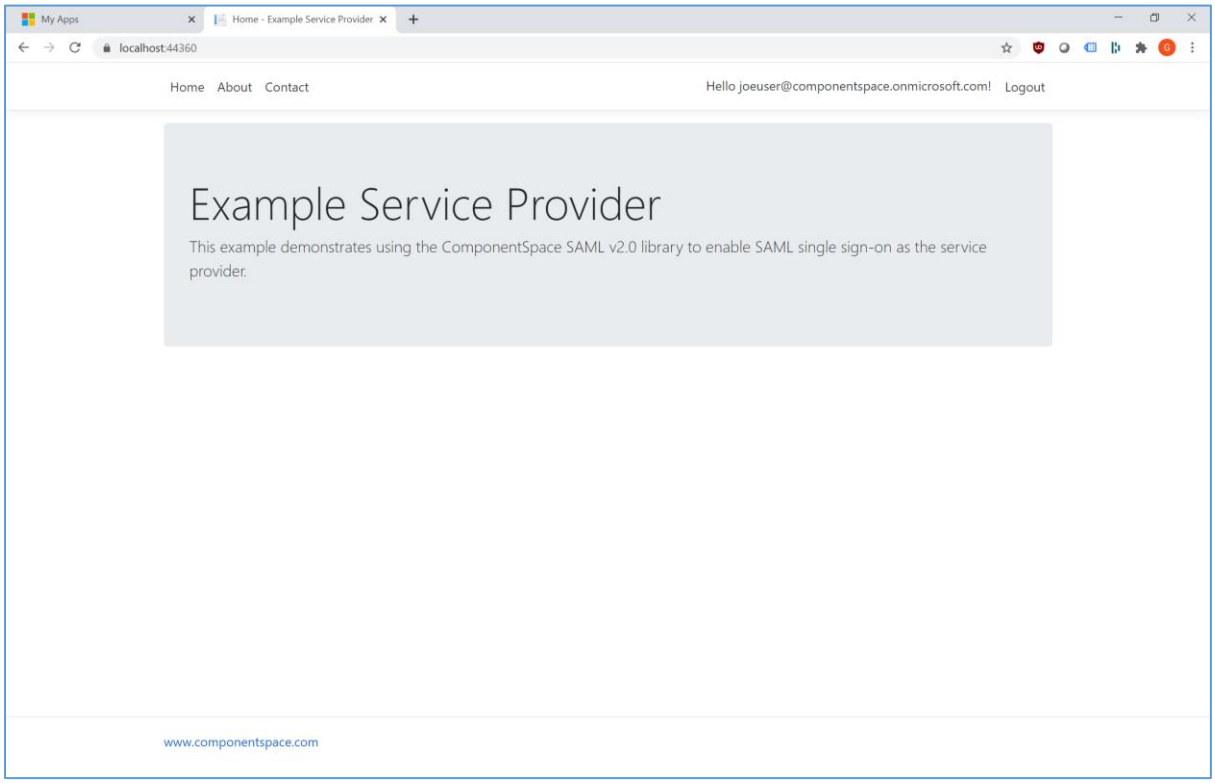
Browse to https://myapps.microsoft.com and login.

Alternatively, browse to the 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

Microsoft Entra supports both SP-initiated and IdP-initiated SAML logout.

## Multitenant Support

The previous sections describe SAML SSO to Entra ID in a single tenant deployment.

Entra ID also supports SSO from any Microsoft Entra tenant by converting a single tenant application to multitenant. For more information, refer to:

https://learn.microsoft.com/en-us/entra/identity-platform/howto-convert-app-to-be-multi-tenant

Entra ID publishes both tenant specific and tenant independent SAML metadata.

https://learn.microsoft.com/en-us/entra/identity-platform/federation-metadata

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

The name is a regular expression that matches any Entra tenant. This is required as Entra ID sets the issuer field to that of the tenant where the user is authenticated and this isn't necessarily known at configuration time.

The first certificate is from the single tenant's SAML metadata. The other certificates are from the tenant independent SAML metadata. SAML messages originating from the tenant where the application is deployed will be signed with a tenant specific certificate. SAML messages from any other tenant will be signed with a tenant independent certificate.

```
<PartnerIdentityProvider
 Name="https://sts.windows.net/"
 Description="Microsoft Entra ID multitenant"
 SingleSignOnServiceUrl="https://login.microsoftonline.com/common/saml2"
 SingleLogoutServiceUrl="https://login.microsoftonline.com/common/saml2">
 <PartnerCertificates>
  <Certificate FileName="Certificates\azure.cer"/>
  <Certificate FileName="Certificates\azure-common-1.cer"/>
  <Certificate FileName="Certificates\azure-common-2.cer"/>
  <Certificate FileName="Certificates\azure-common-3.cer"/>
  <Certificate FileName="Certificates\azure-common-4.cer"/>
 </PartnerCertificates>
</PartnerIdentityProvider>
```

To support matching SAML message issuer fields against the <PartnerIdentityProvider> Name pattern, regular expression support must be enabled. This should be done at application start-up.

```
using ComponentSpace.SAML2.Configuration.Resolver;

// Support matching SAML message issuer fields against regular expression patterns.
SAMLController.ConfigurationNameResolver =
new RegexSAMLConfigurationNameResolver();
```

## Troubleshooting

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