



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

Contents

Introduction	1
Configuring an Enterprise Application for SAML SSO	1
Service Provider Configuration	8
SP-Initiated SSO	8
IdP-Initiated SSO	10
SAML Logout	11
Multitenant Support	12
Troubleshooting	13

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-ss0>

Configuring an Enterprise Application for SAML SSO

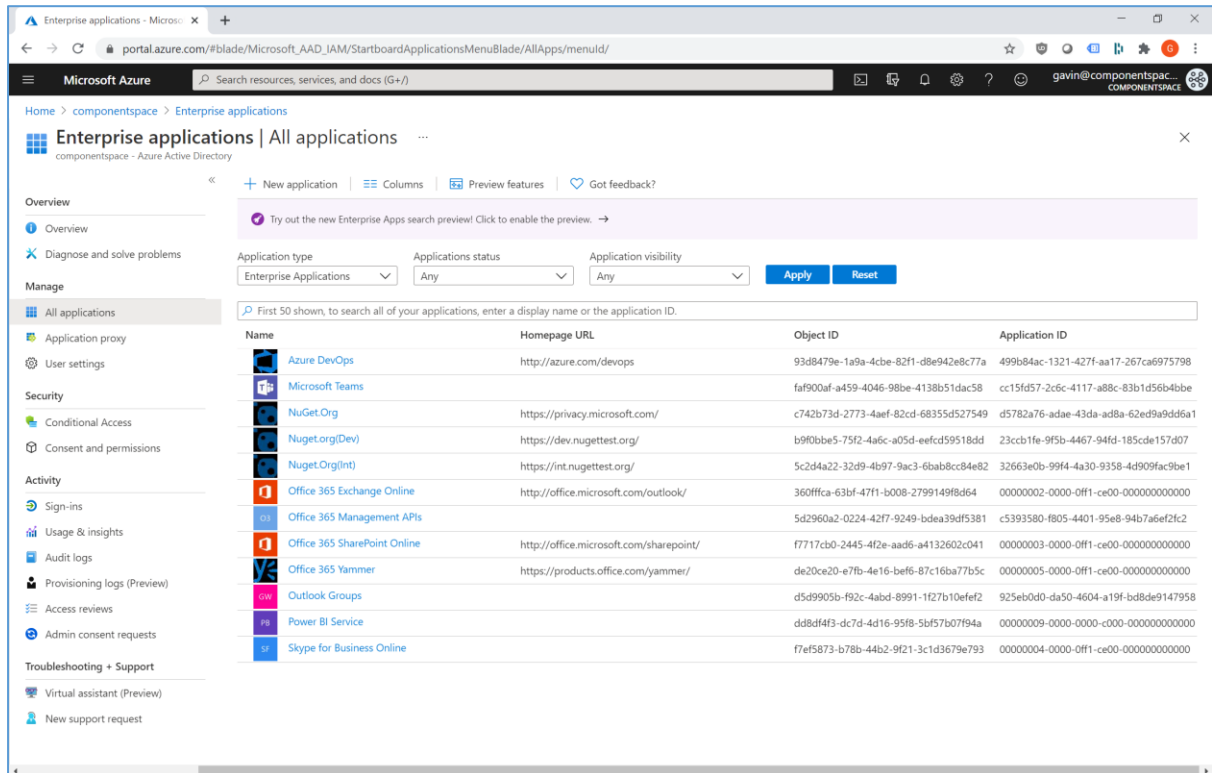
Login to Microsoft Entra as an administrator.

<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.

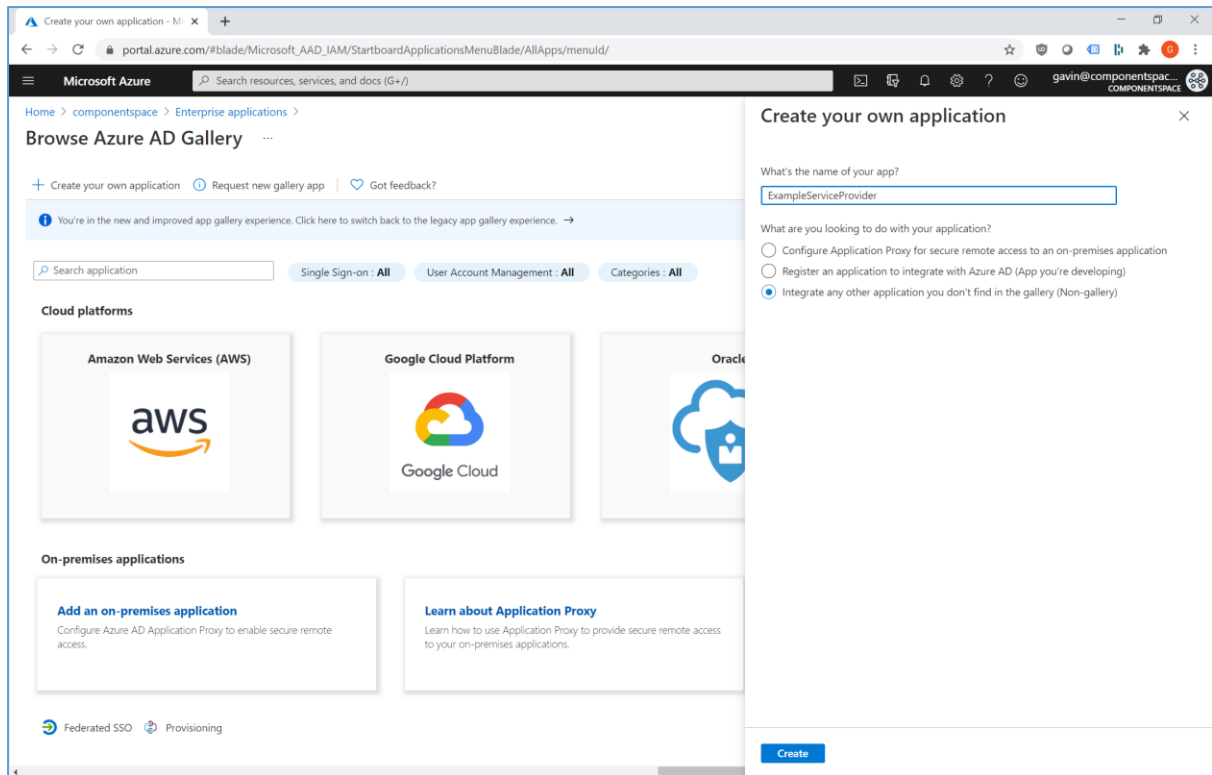


The screenshot shows the 'Enterprise applications' page in the Microsoft Entra portal. The page title is 'Enterprise applications | All applications'. The left sidebar contains navigation links: Overview, Diagnose and solve problems, Manage (All applications, Application proxy, User settings), Security (Conditional Access, Consent and permissions), Activity (Sign-ins, Usage & insights, Audit logs, Provisioning logs (Preview), Access reviews, Admin consent requests), and Troubleshooting + Support (Virtual assistant (Preview), New support request). The main content area has a search bar and filters for Application type (Enterprise Applications), Applications status (Any), and Application visibility (Any). Below the filters is a table listing applications:

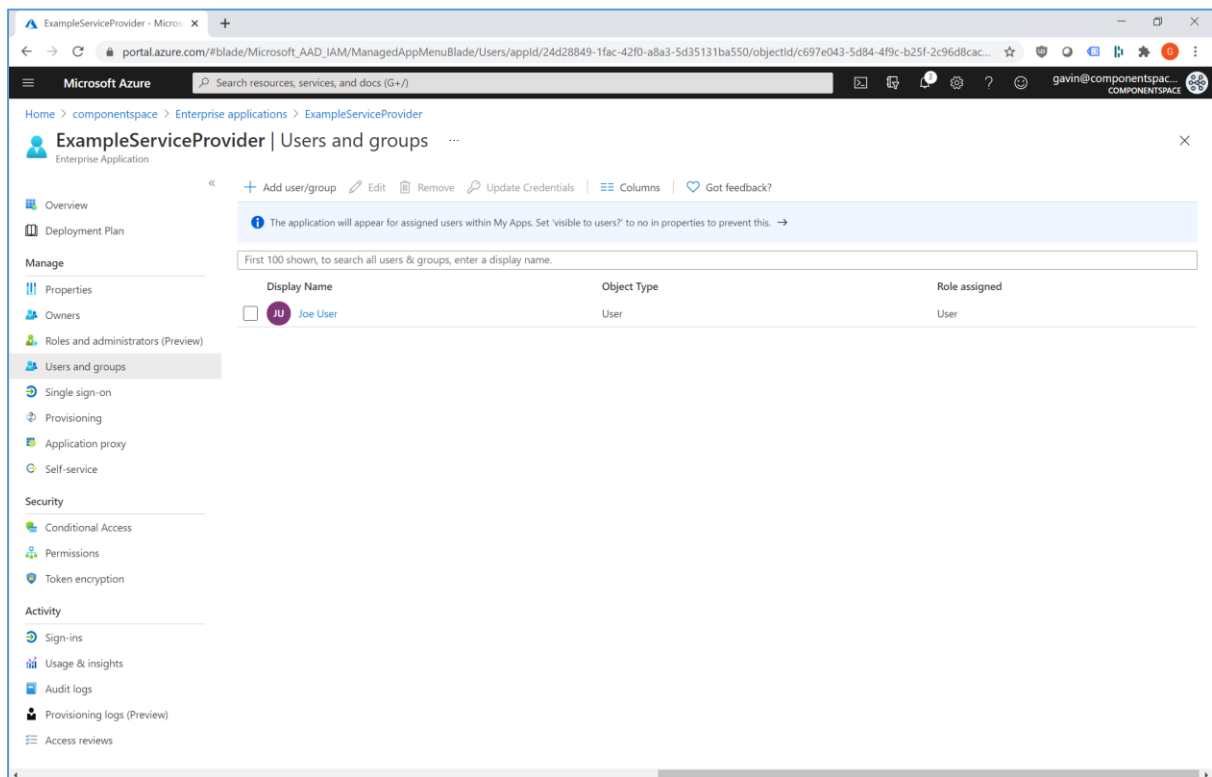
Name	Homepage URL	Object ID	Application ID
Azure DevOps	http://azure.com/devops	93d8479e-1a9a-4cbe-82f1-d8e942e8c77a	499b84ac-1321-427f-aa17-267ca6975798
Microsoft Teams		faf900af-a459-4046-98be-4138b51dac58	cc15fd57-2c6c-4117-a88c-83b1d56b4bbe
NuGet.Org	https://privacy.microsoft.com/	c742b73d-2773-4aef-82cd-68355d527549	d5782a76-adae-43da-ad8a-62ed9a9dd6a1
NuGet.org(Dev)	https://dev.nugettest.org/	b9f0bbe5-75f2-4a6c-a05d-eefcd59518dd	23ccb1fe-9f5b-4467-94fd-185cde157d07
NuGet.Org(Int)	https://int.nugettest.org/	5c2d4a22-32d9-4b97-9ac3-6bab8cc84e82	32663e0b-99f4-4a30-9358-4d909fac9be1
Office 365 Exchange Online	http://office.microsoft.com/outlook/	360ffca-63bf-47f1-b008-2799149f8d64	00000002-0000-0ff1-ce00-000000000000
Office 365 Management APIs		5d2960a2-0224-42f7-9249-bdea39df5381	c5393580-f805-4401-95e8-94b7a6ef2fc2
Office 365 SharePoint Online	http://office.microsoft.com/sharepoint/	f7717cb0-2445-4f2e-aad6-a4132602c041	00000003-0000-0ff1-ce00-000000000000
Office 365 Yammer	https://products.office.com/yammer/	de20ce20-e7fb-4e16-bef6-87c16ba77b5c	00000005-0000-0ff1-ce00-000000000000
Outlook Groups		d5d9905b-f92c-4abd-8991-1f27b10efef2	925eb0d0-da50-4604-a19f-bd8de9147958
Power BI Service		dd8df4f3-dc7d-4d16-95f8-5b57b07f94a	00000009-0000-0000-c000-000000000000
Skype for Business Online		f7ef5873-b78b-44b2-9f21-3c1d3679e793	00000004-0000-0ff1-ce00-000000000000

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

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

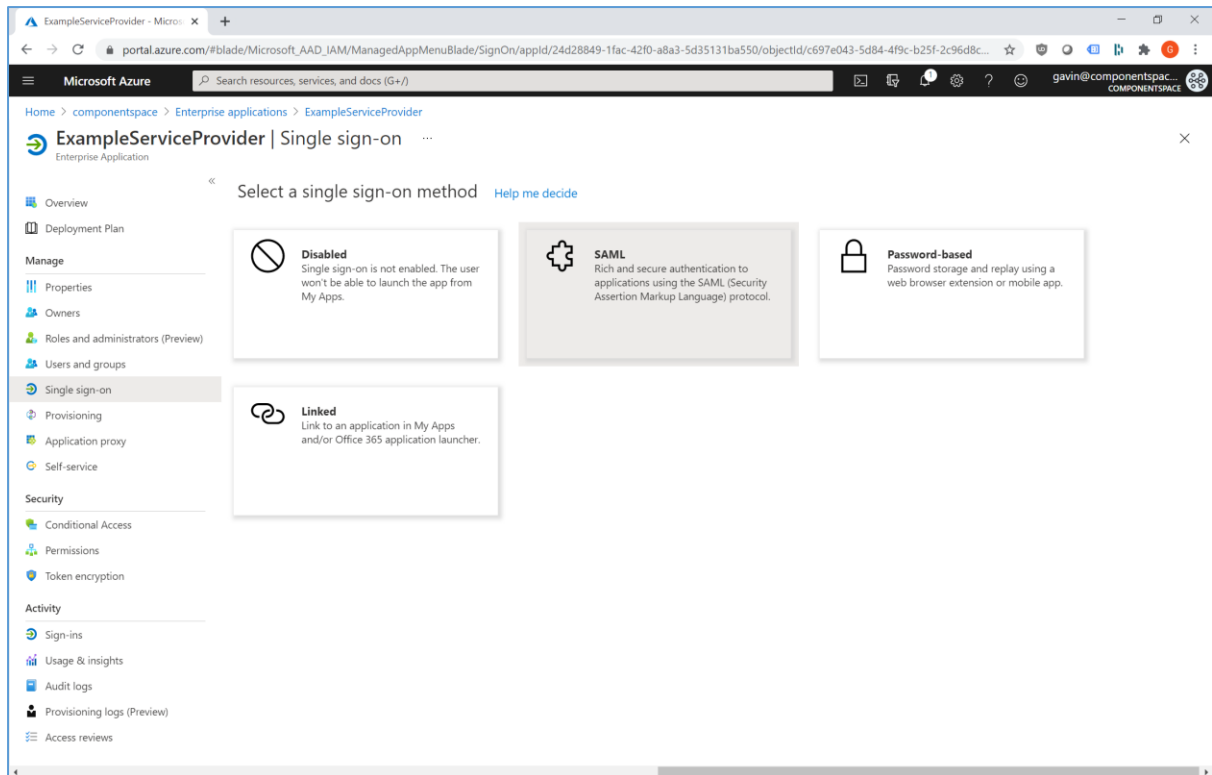


Assign users access to the application.



Select SAML as the single sign-on method.

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



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.

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

The screenshot shows the 'Basic SAML Configuration' dialog in the Microsoft Azure portal. The dialog is titled 'Basic SAML Configuration' and has a 'Save' button at the top left. It contains the following fields:

- Identifier (Entity ID):** The default identifier will be the audience of the SAML response for IDP-initiated SSO. The value entered is `https://ExampleServiceProvider`.
- Reply URL (Assertion Consumer Service URL):** The default reply URL will be the destination in the SAML response for IDP-initiated SSO. The value entered is `https://localhost:44360/SAML/AssertionConsumerService`.
- Sign on URL:** The value entered is `Enter a sign on URL`.
- Relay State:** The value entered is `Enter a relay state`.
- Logout Url:** The value entered is `https://localhost:44360/SAML/SingleLogoutService`.

On the left side of the dialog, there is a list of configuration steps:

1. Basic SAML Configuration
2. User Attributes & Claims
3. SAML Signing Certificate

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

The screenshot shows the 'Upload metadata file' dialog in the Microsoft Azure portal. The dialog is titled 'Upload metadata file.' and contains the following text:

Values for the fields below are provided by ExampleServiceProvider. You may either enter those values manually, or upload a pre-configured SAML metadata file if provided by ExampleServiceProvider.

Below the text, there is a 'Select a file' button and an 'Add' button. The dialog also shows the 'Basic SAML Configuration' dialog in the background, with the following fields visible:

- Sign on URL:** Optional
- Relay State:** Optional
- Logout Url:** Optional

Below the 'Basic SAML Configuration' dialog, there is a section for 'User Attributes & Claims' with the following attributes:

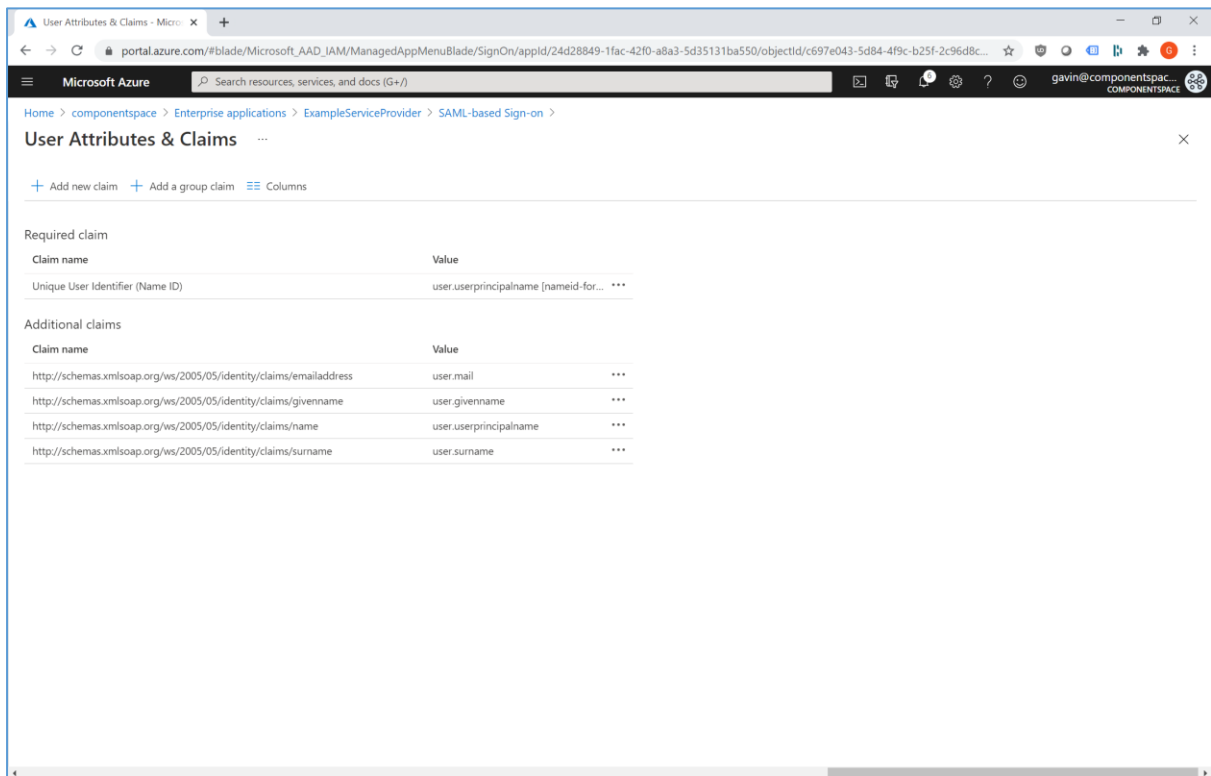
- givenname: user.givenname
- surname: user.surname
- emailaddress: user.mail
- name: user.userprincipalname
- Unique User Identifier: user.userprincipalname

Below the 'User Attributes & Claims' section, there is a section for 'SAML Signing Certificate' with the following attributes:

- Status: Active
- Thumbprint: 9CEA37643ACE0D710AD63296857B251D1FCAS48
- Expiration: 12/21/2025, 6:50:17 AM
- Notification Email: gavin@componentspace.onmicrosoft.com
- App Federation Metadata Url: https://login.microsoftonline.com/f2f933ec-d7c9-...
- Certificate (Base64): Download
- Certificate (Raw): Download
- Federation Metadata XML: Download

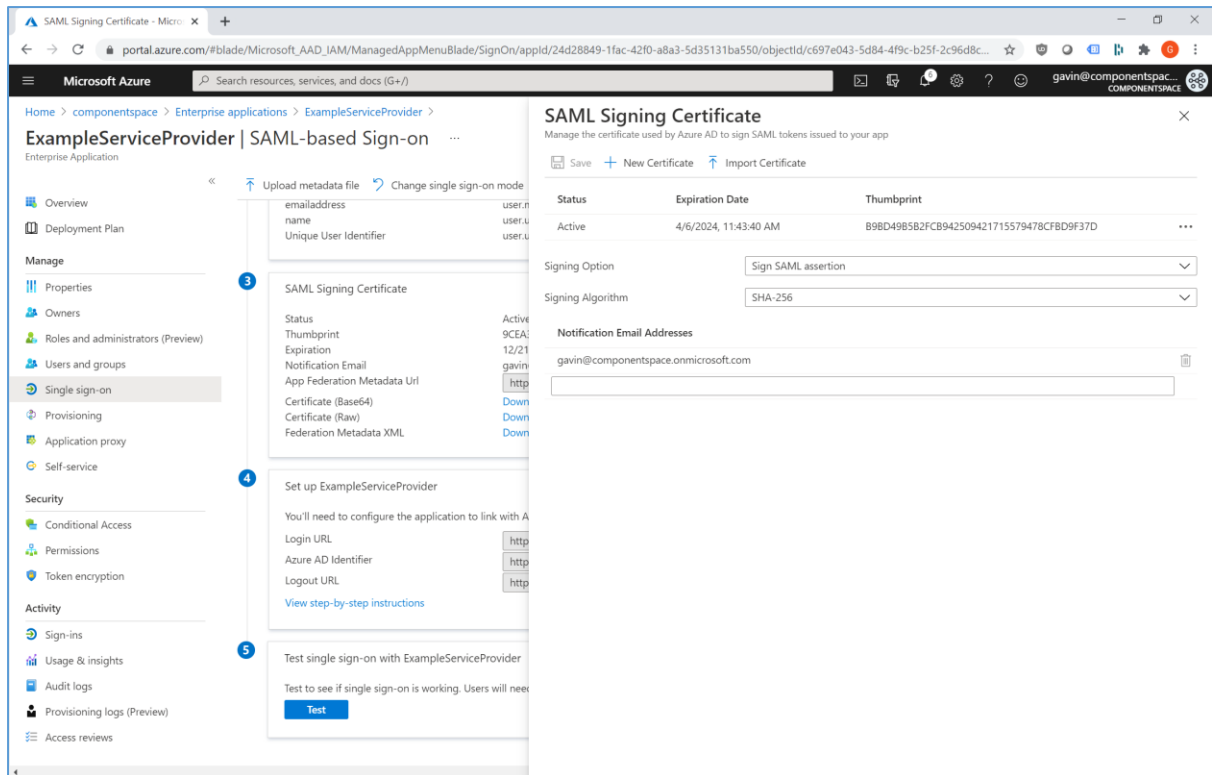
ComponentSpace SAML for ASP.NET Entra ID (Azure AD) Integration Guide

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.

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



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

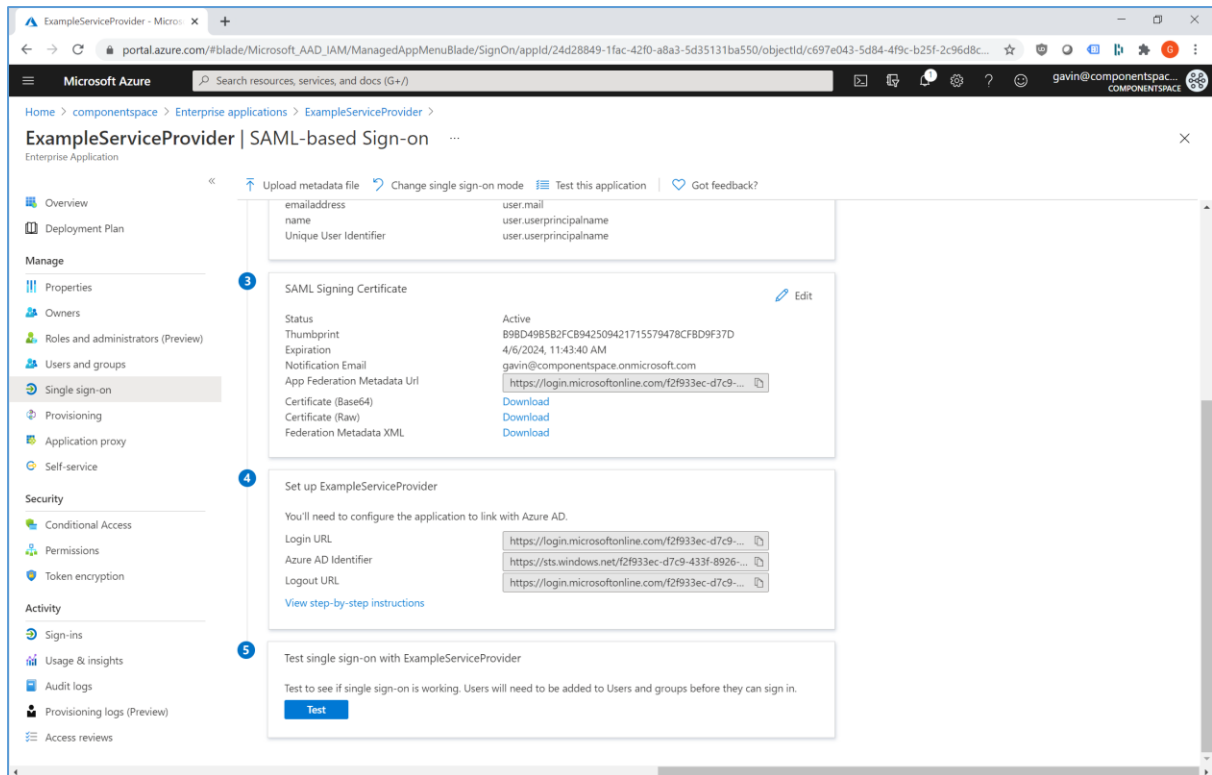
The login URL is the PartnerIdentityProviderConfiguration's SingleSignOnServiceUrl.

The Microsoft Entra identifier is the PartnerIdentityProviderConfiguration's Name.

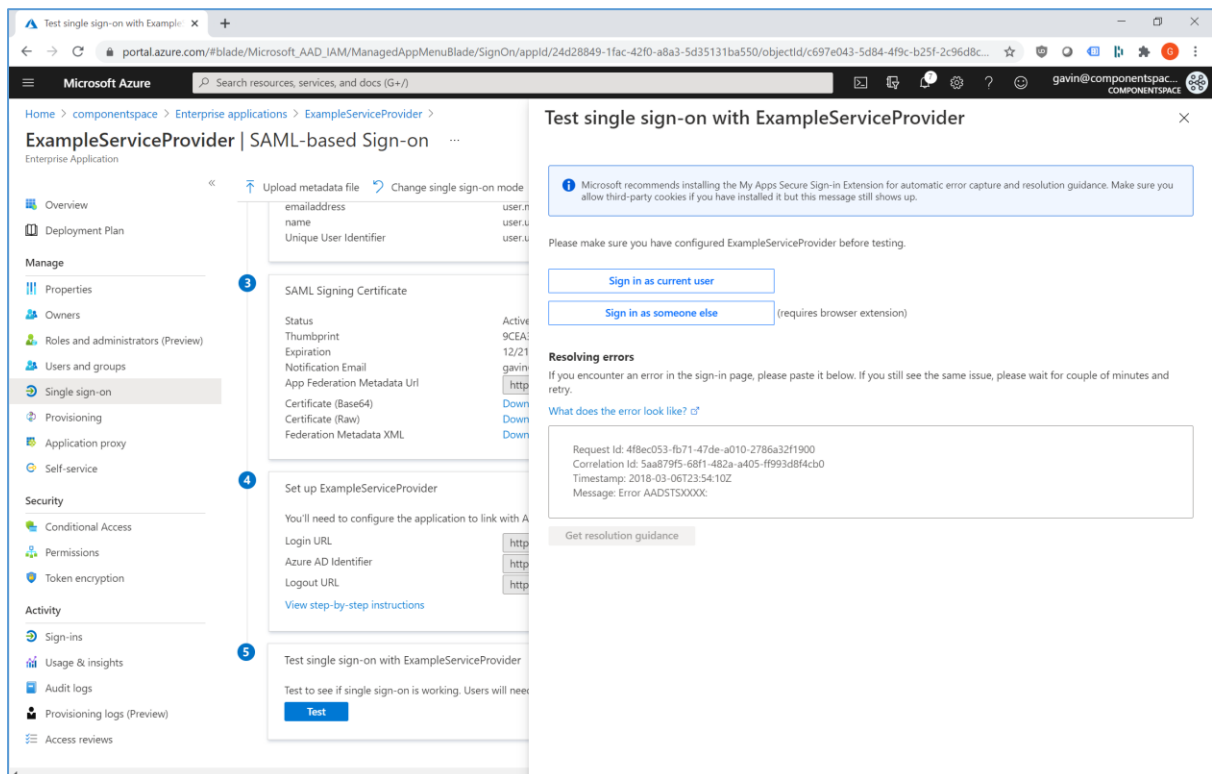
The logout URL is the PartnerIdentityProviderConfiguration's SingleLogoutServiceUrl.

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

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



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.

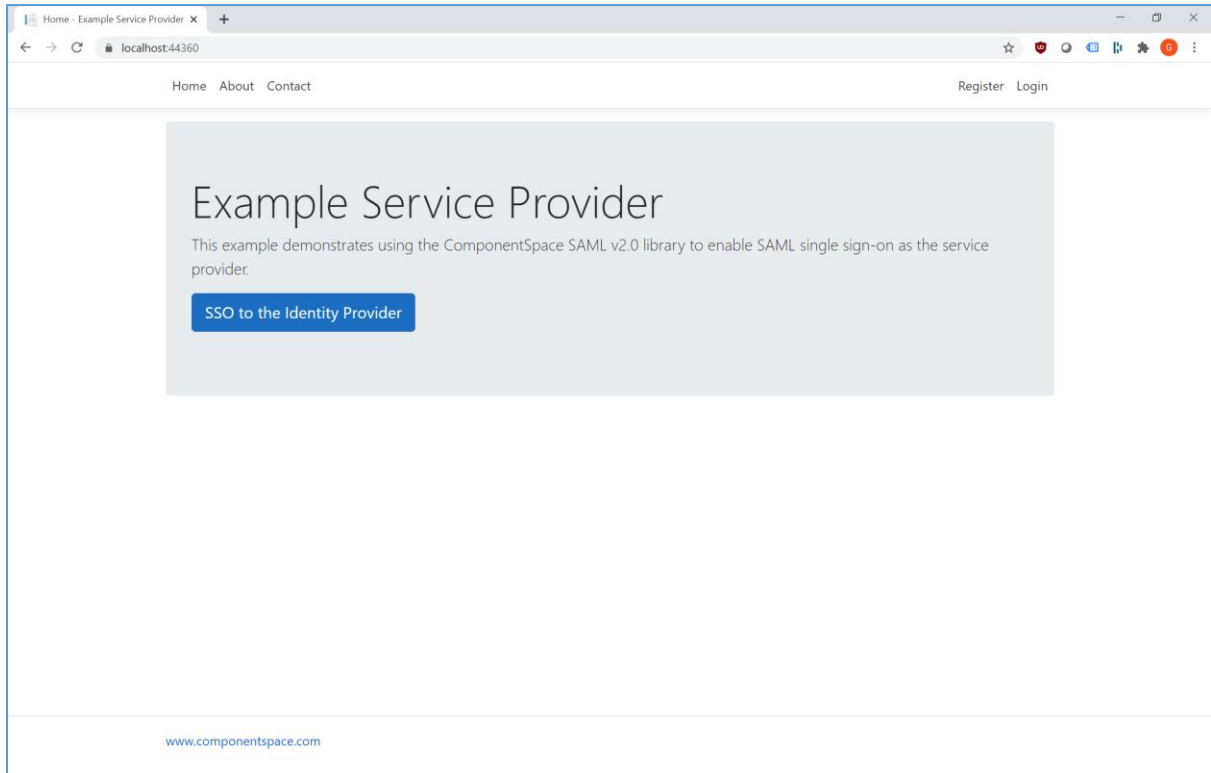
Ensure the PartnerName specifies the correct partner identity provider.

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

SP-Initiated SSO

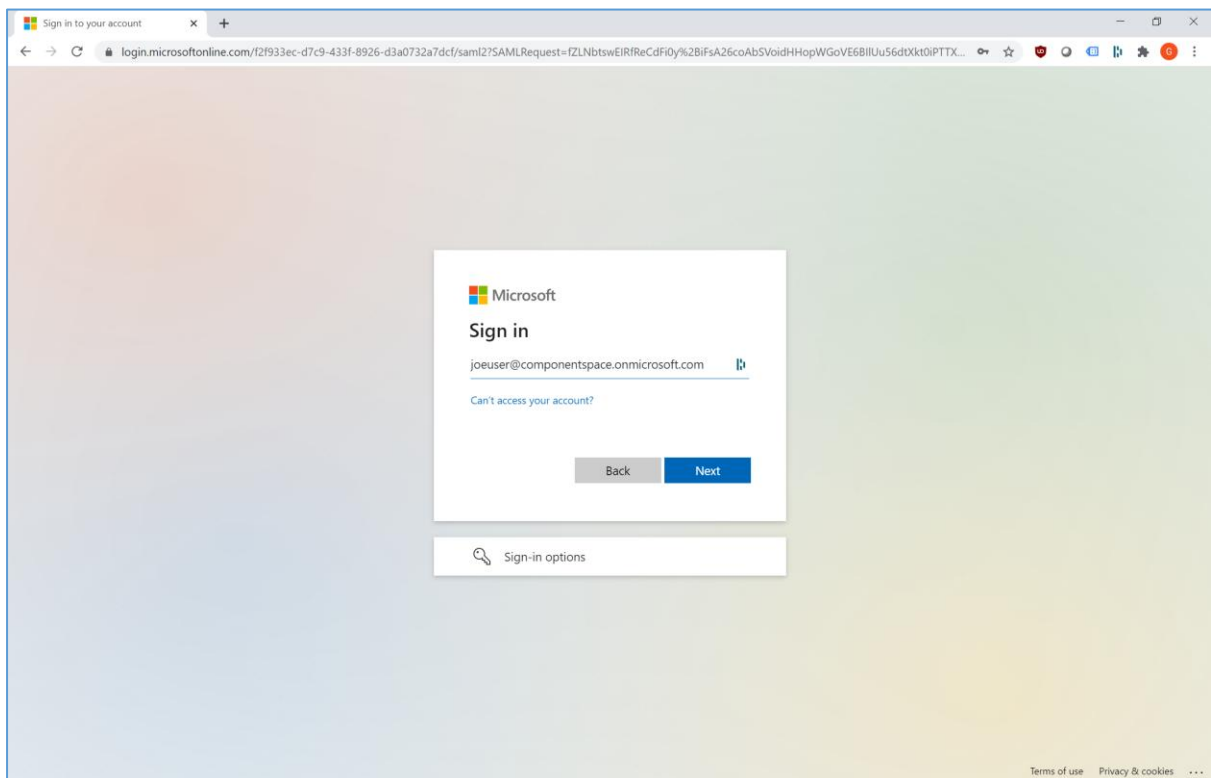
Browse to the example service provider.

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

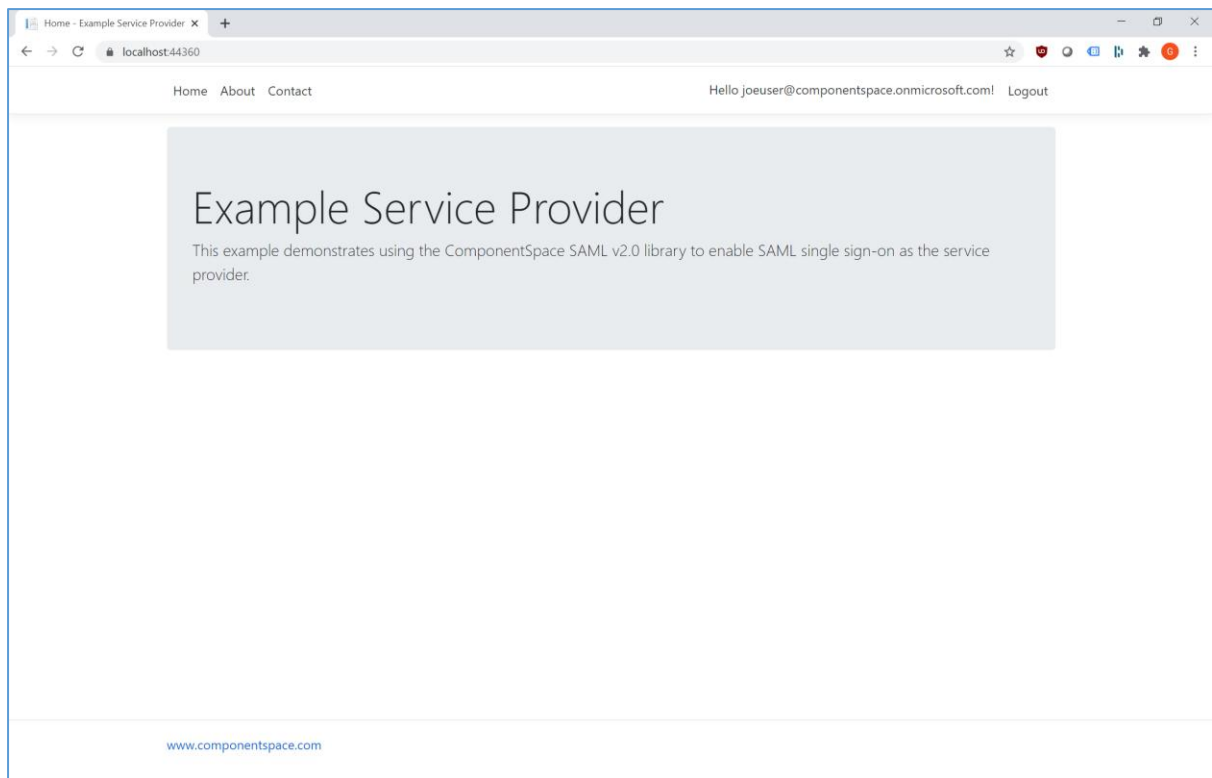


Click the button to SSO to the identity provider.

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



The user is automatically logged in at the service provider.



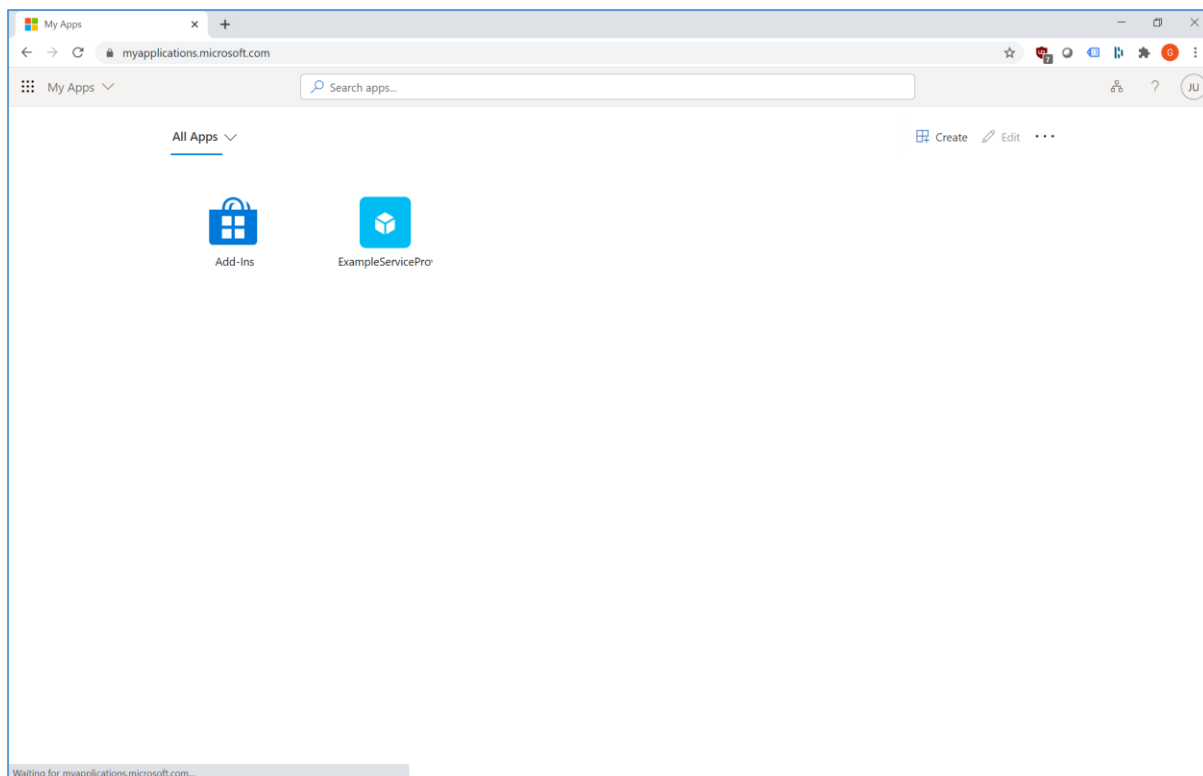
IdP-Initiated SSO

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

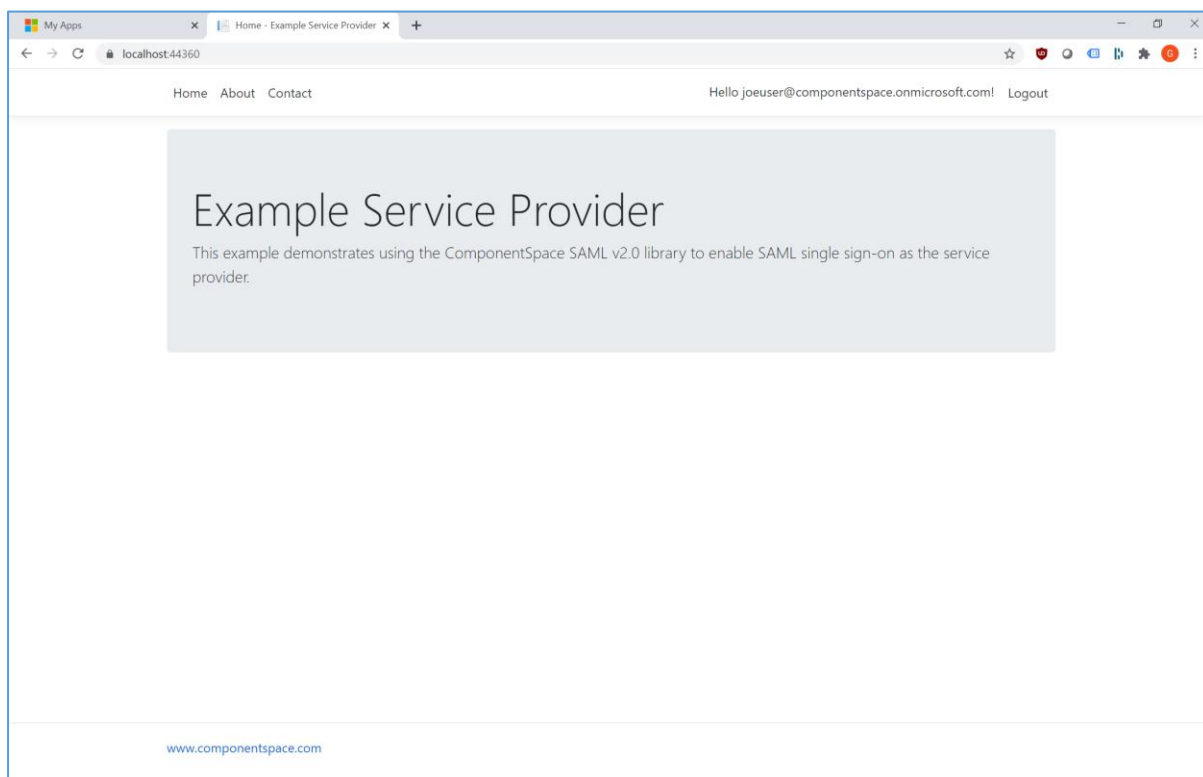
Alternatively, browse to the URL specified in the application properties for direct access to the application.

Select the ExampleServiceProvider application.

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



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.