ComponentSpace
SAML for ASP.NET Core
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

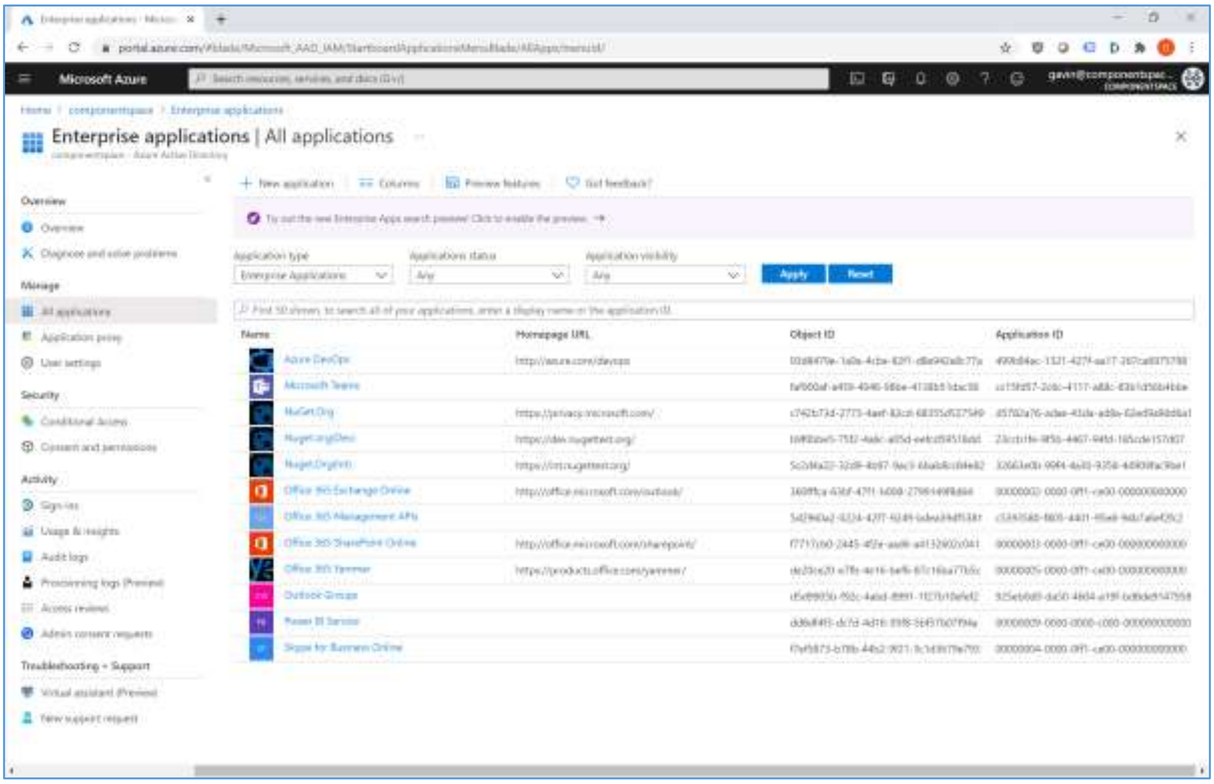
Login to Microsoft Entra as an administrator.

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.



Try out the new Enterprise Apps search preview! Click to enable the preview. →

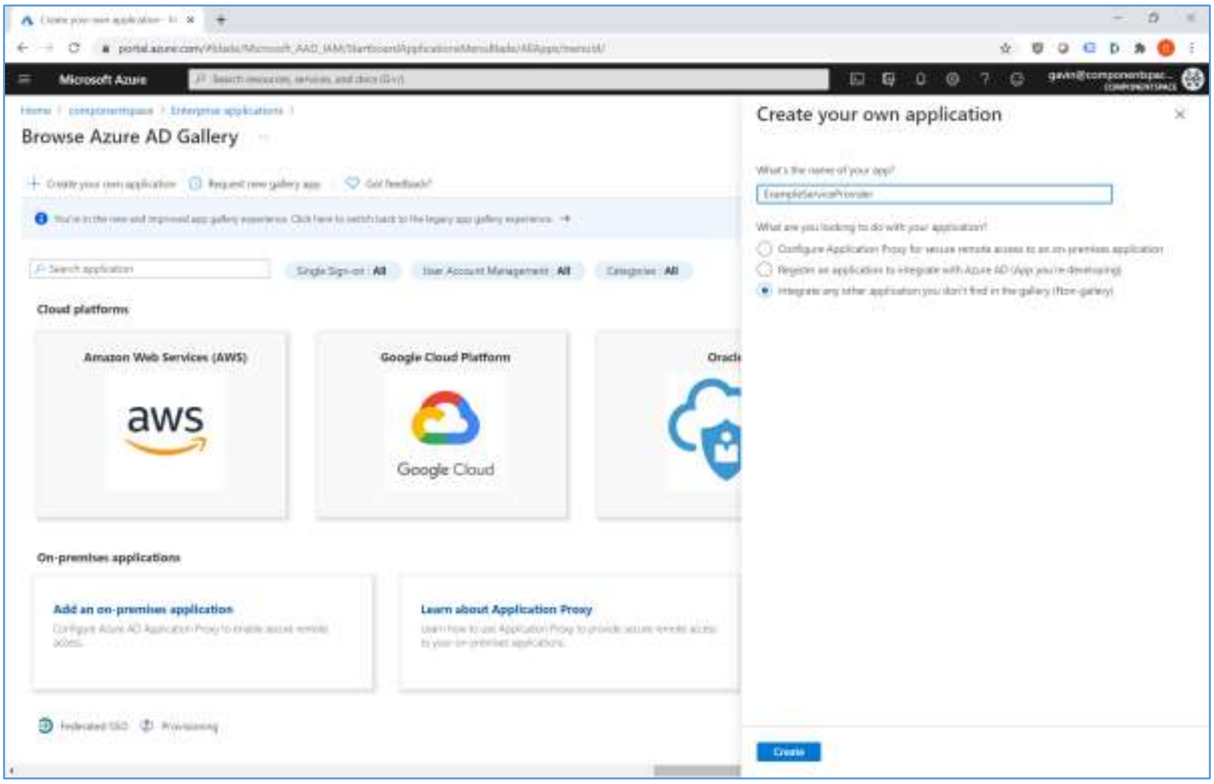
Application type: Enterprise Applications

Applications status: Any

Application visibility: Any

Name	Homepage URL	Object ID	Application ID
Azure DevOps	http://azure.com/devops	[illegible]	[illegible]
Microsoft Teams		[illegible]	[illegible]
NuGet.Org	https://privacy.microsoft.com/	[illegible]	[illegible]
NugetOrgDev	https://dev.nugettest.org/	[illegible]	[illegible]
NugetOrgInt	https://int.nugettest.org/	[illegible]	[illegible]
Office 365 Exchange Online	http://office.microsoft.com/outlook/	[illegible]	[illegible]
Office 365 Management APIs		[illegible]	[illegible]
Office 365 SharePoint Online	http://office.microsoft.com/sharepoint/	[illegible]	[illegible]
Office 365 Yammer	https://products.office.com/yammer/	[illegible]	[illegible]
Outlook Groups		[illegible]	[illegible]
Power BI Service		[illegible]	[illegible]
Skype for Business Online		[illegible]	[illegible]

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



Create your own application

What's the name of your app?

ExampleServiceProvider

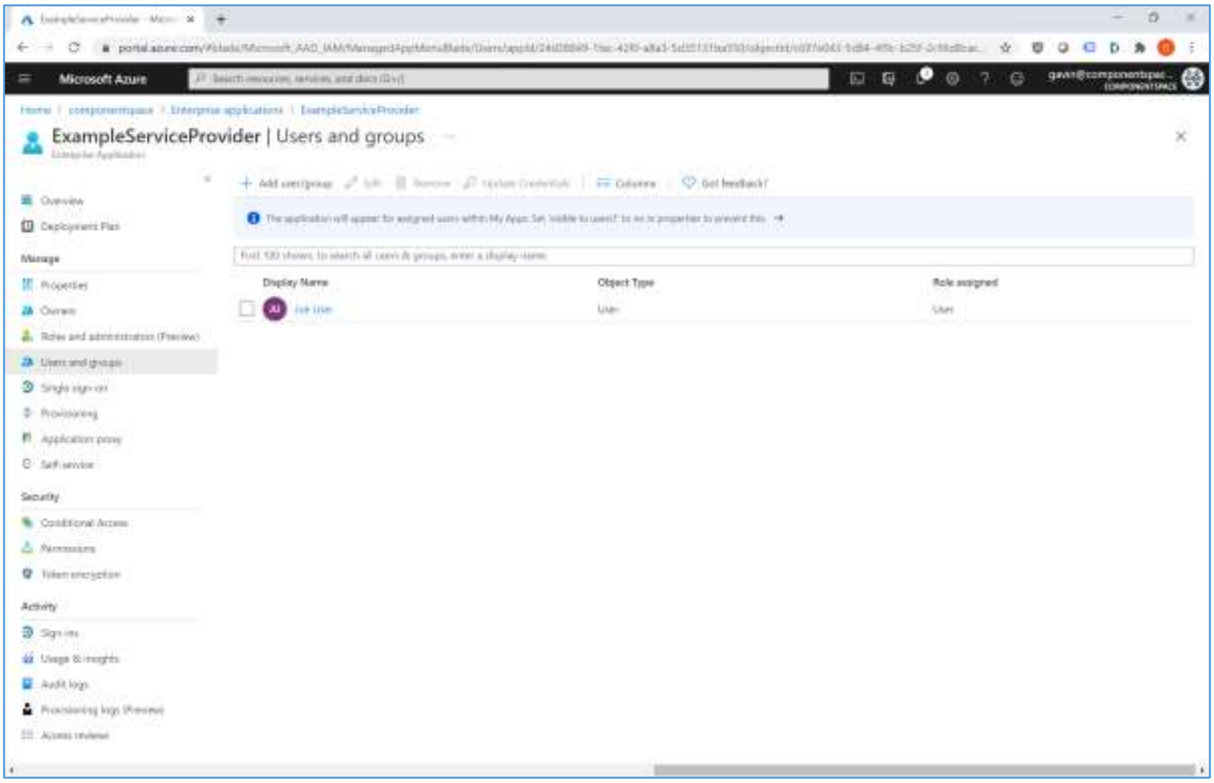
What are you looking to do with your application?

○ Configure Application Proxy for secure remote access to an on-premises application

○ Register an application to integrate with Azure AD (App you're developing)

● Integrate any other application you don't find in the gallery (Non-gallery)

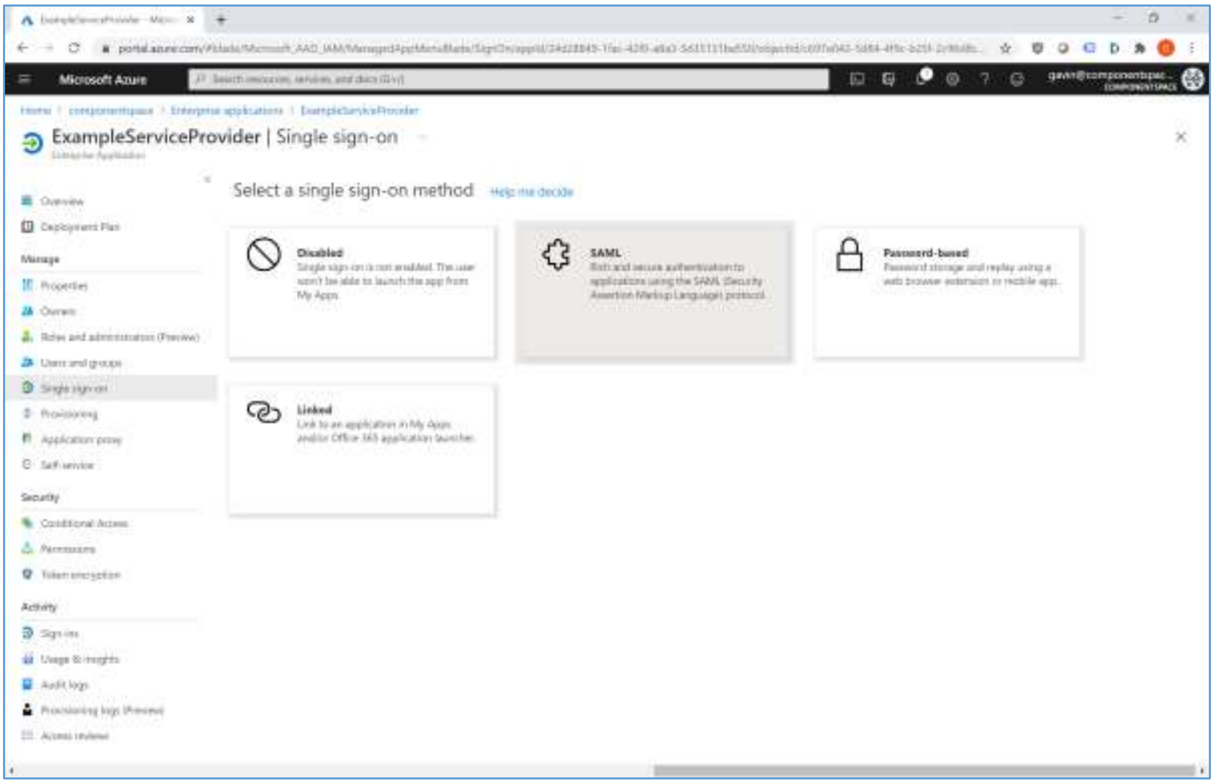
Assign users access to the application.



ExampleServiceProvider | Users and groups

Display Name	Object Type	Role assigned
Joe User	User	User

Select SAML as the single sign-on method.



Disabled
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

SAML
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

Password-based
Password storage and replay using a web browser extension or mobile app.

Linked
Link to an application in My Apps and/or Office 365 application launcher.

Configure single sign-on.

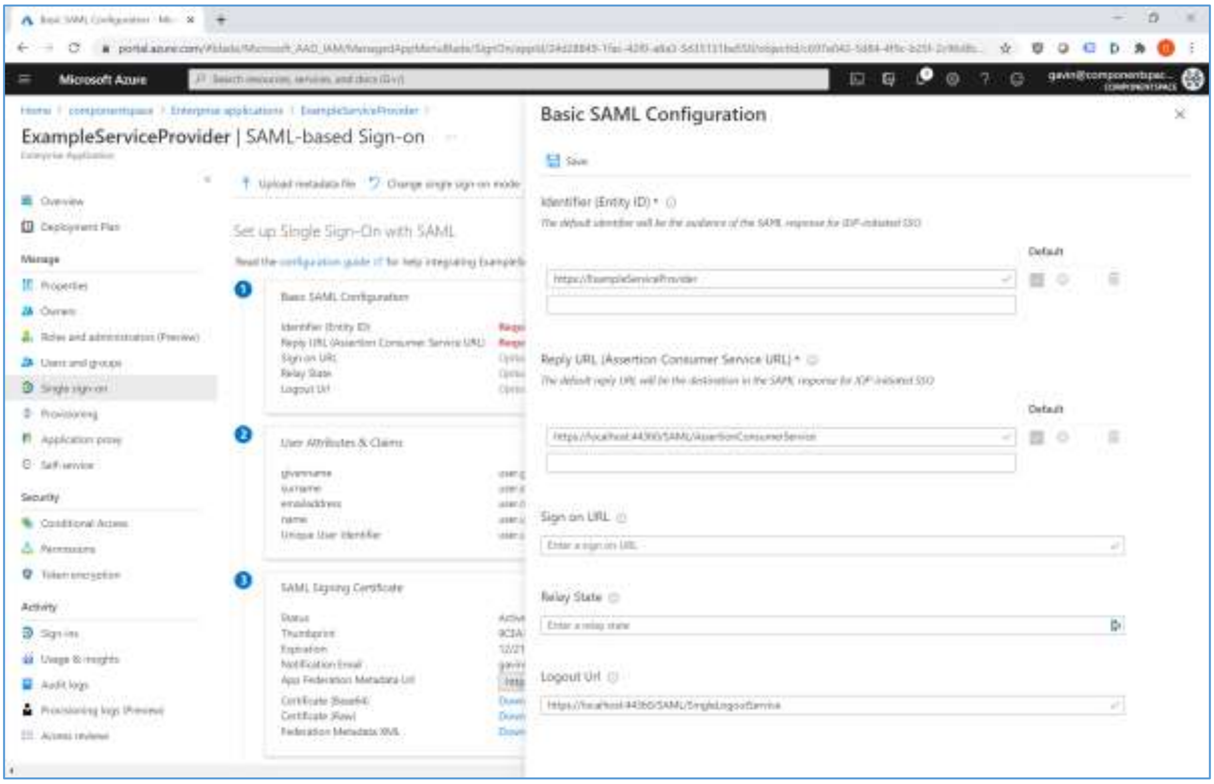
The identifier is the SAML entity ID. This name must match with the local service provider name. For example, if the LocalServiceProviderConfiguration's Name is https://ExampleServiceProvider, then the identifier must be set to the same value.

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.



Basic SAML Configuration

Save

Identifier (Entity ID) *

The default identifier will be the audience of the SAML response for IDP-initiated SSO

Default

https://ExampleServiceProvider

Reply URL (Assertion Consumer Service URL) *

The default reply URL will be the destination in the SAML response for IDP-initiated SSO

Default

https://localhost:44360/SAML/AssertionConsumerService

Sign on URL

Enter a sign on URL

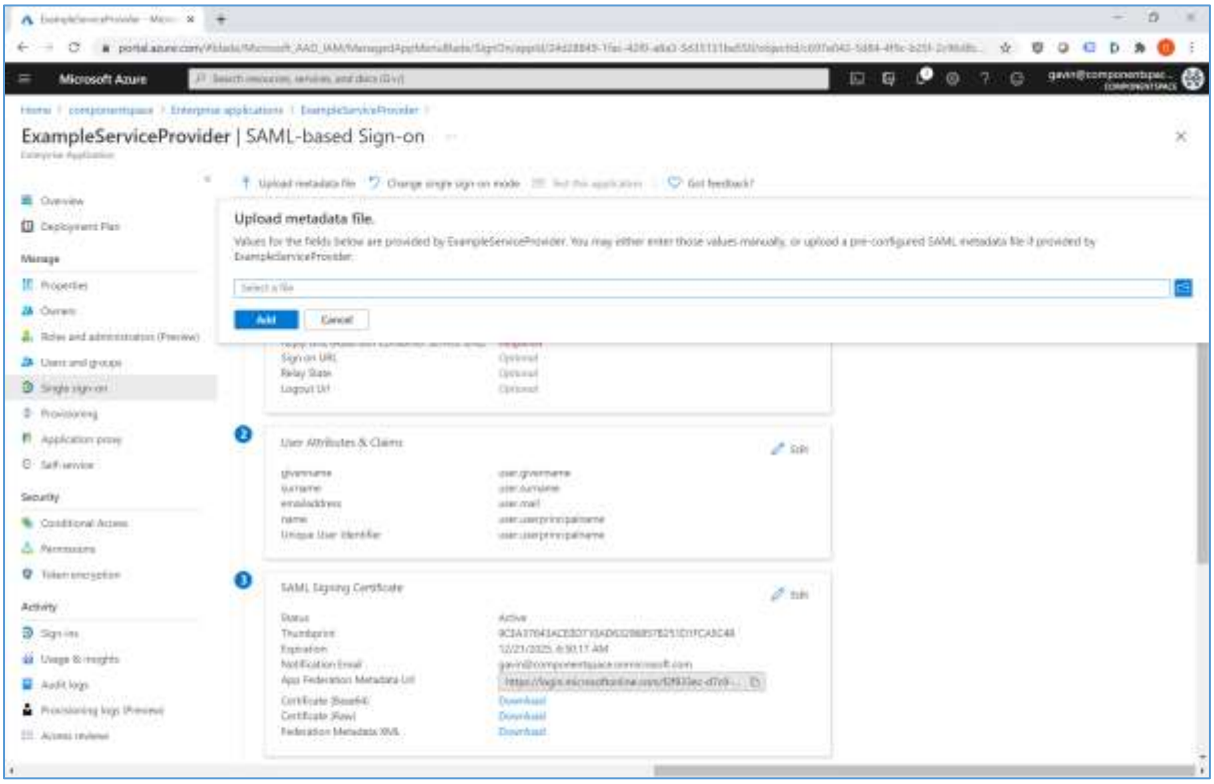
Relay State

Enter a relay state

Logout Url

https://localhost:44360/SAML/SingleLogoutService

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



ExampleServiceProvider | SAML-based Sign-on

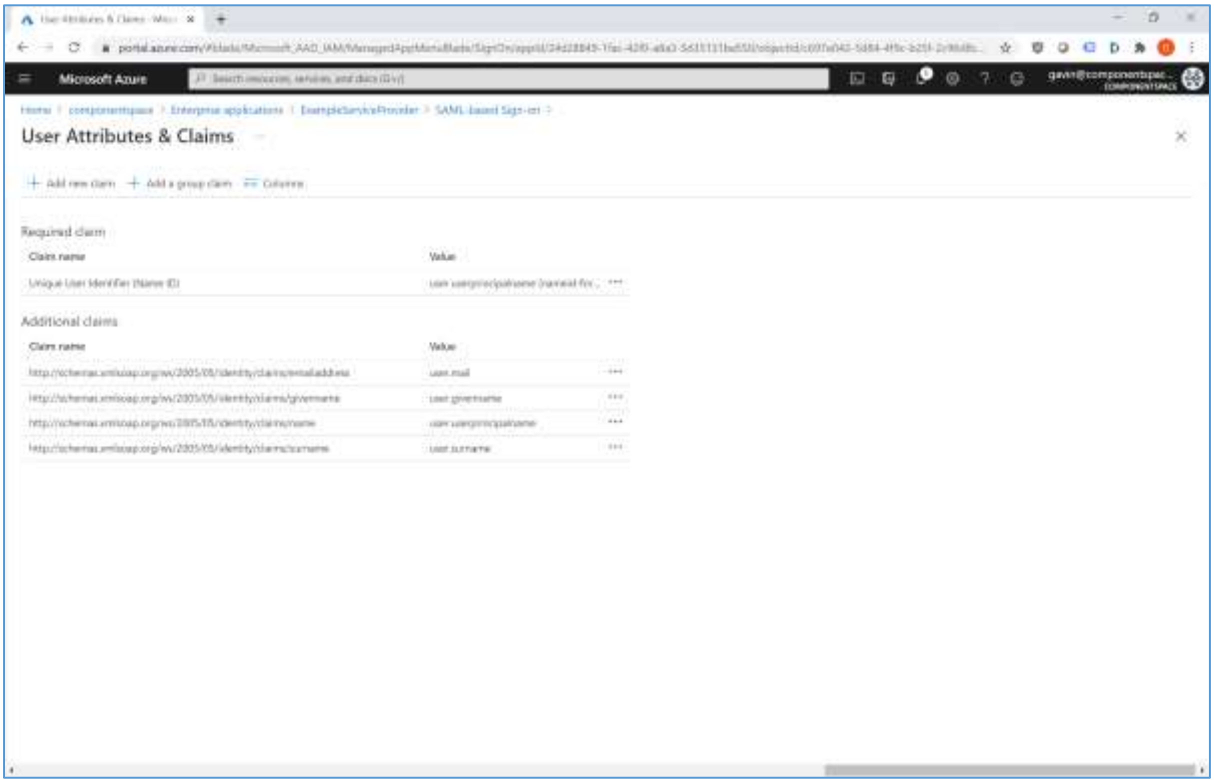
Upload metadata file

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.

Select a file

Add Cancel

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.


Microsoft Azure
Search resources, services, and docs (G+/)
Home > componentspace > Enterprise applications > ExampleServiceProvider > SAML-based Sign-on >

User Attributes & Claims

+ Add new claim
+ Add a group claim
Columns

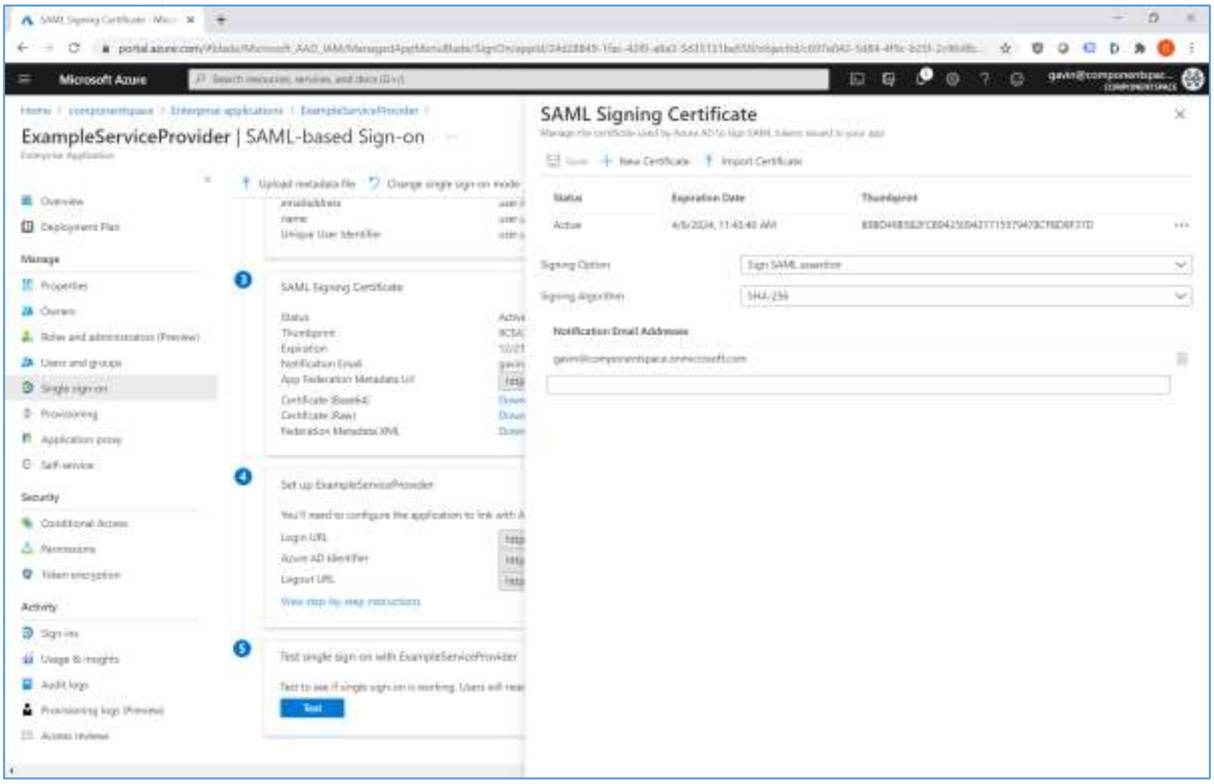
Required claim

Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname [nameid-for...

Additional claims

Claim name	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname

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



ExampleServiceProvider | SAML-based Sign-on

Enterprise Application

emailaddress

name

Unique User Identifier

3 SAML Signing Certificate

Status

Thumbprint

Expiration

Notification Email

App Federation Metadata Url

Certificate (Base64)

Certificate (Raw)

Federation Metadata XML

4 Set up ExampleServiceProvider

You'll need to configure the application to link with A

Login URL

Azure AD Identifier

Logout URL

View step-by-step instructions

5 Test single sign-on with ExampleServiceProvider

Test to see if single sign-on is working. Users will nee

SAML Signing Certificate

Manage the certificate used by Azure AD to sign SAML tokens issued to your app

Status	Expiration Date	Thumbprint
Active	4/5/2024, 11:43:40 AM	83BD44B5B2FC8042500421715579478CFBD8F31D

Signing Option: Sign SAML assertion

Signing Algorithm: SHA-256

Notification Email Addresses

gavin@componentspace.onmicrosoft.com

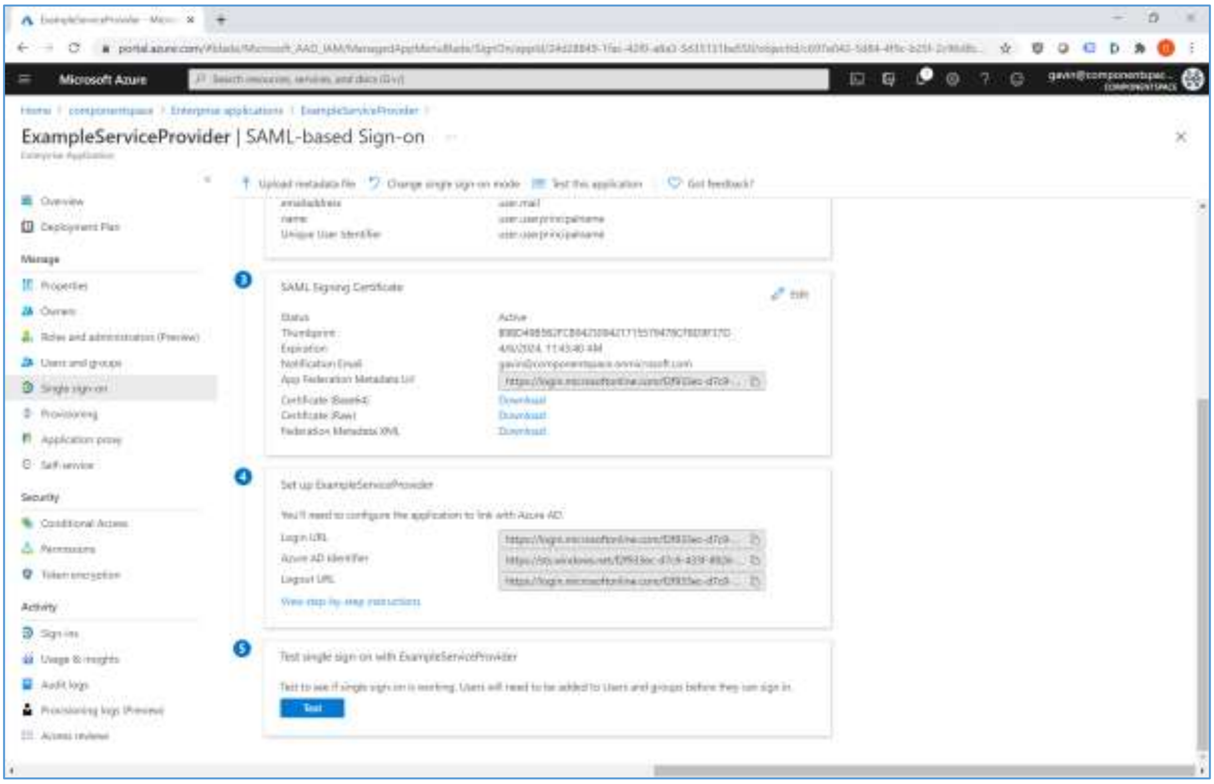
Information is displayed that’s required for configuring the service provider application.

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.



ExampleServiceProvider | SAML-based Sign-on

emailaddress user.mail
name user.userprincipalname
Unique User Identifier user.userprincipalname

3 SAML Signing Certificate

Status: Active
Thumbprint: [illegible]
Expiration: 4/6/2024, 11:43:40 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

4 Set up ExampleServiceProvider

You'll need to configure the application to link with Azure AD.

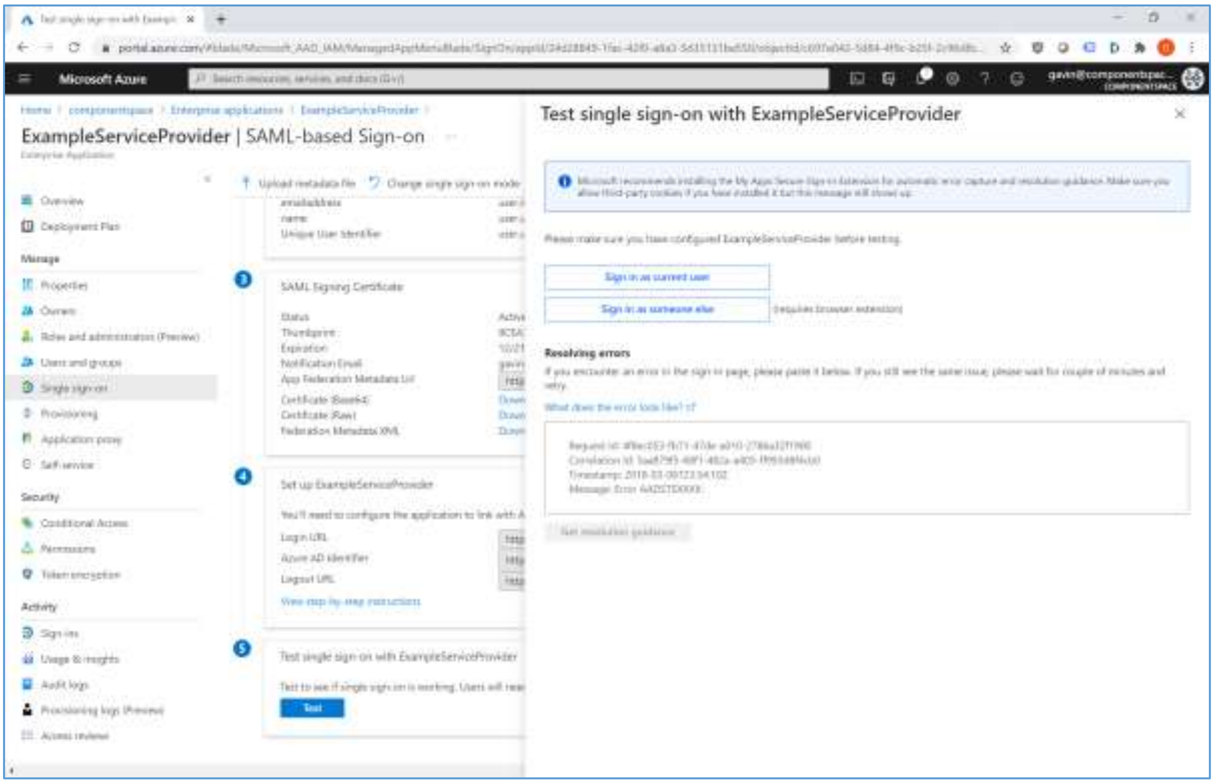
Login URL: https://login.microsoftonline.com/f2f933ec-d7c9-...
Azure AD Identifier: https://sts.windows.net/f2f933ec-d7c9-433f-892e-...
Logout URL: https://login.microsoftonline.com/f2f933ec-d7c9-...

View step-by-step instructions

5 Test single sign-on with ExampleServiceProvider

Test to see if single sign-on is working. Users will need to be added to Users and groups before they can sign in.

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



Test single sign-on with ExampleServiceProvider

Microsoft recommends installing the My Apps Secure Sign-in Extension for automatic error capture and resolution guidance. Make sure you allow third-party cookies. If you have installed it but this message still shows up.

Please make sure you have configured ExampleServiceProvider before testing.

Sign in as current user

Sign in as someone else (requires browser extension)

Resolving errors

If you encounter an error in the sign in page, please paste it below. If you still see the same issue, please wait for couple of minutes and retry.

What does the error look like?

```
Request Id: [illegible]
Correlation Id: [illegible]
Timestamp: 2018-03-09T22:34:10Z
Message: Error AADSTSXXXX:
```

Get resolution guidance

Microsoft Azure
Search resources, services, and docs (G+/)
Home > componentspace > Enterprise applications > ExampleServiceProvider >
ExampleServiceProvider | SAML-based Sign-on
Enterprise Application
Upload metadata file
Change single sign-on mode
Overview
Deployment Plan
Manage
Properties
Owners
Roles and administrators (Preview)
Users and groups
Single sign-on
Provisioning
Application proxy
Self-service
Security
Conditional Access
Permissions
Token encryption
Activity
Sign-ins
Usage & insights
Audit logs
Provisioning logs (Preview)
Access reviews
SAML Signing Certificate
Set up ExampleServiceProvider
Test single sign-on with ExampleServiceProvider
Test

Service Provider Configuration

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

```
{
  "Name": "https://sts.windows.net/f2f933ec-d7c9-433f-8926-d3a0732a7dcf/",
  "Description": "Entra ID (Azure AD)",
  "SingleSignOnServiceUrl": "https://login.microsoftonline.com/f2f933ec-d7c9-433f-8926-d3a0732a7dcf/saml2",
  "SingleLogoutServiceUrl": "https://login.microsoftonline.com/f2f933ec-d7c9-433f-8926-d3a0732a7dcf/saml2",
  "PartnerCertificates": [
    {
      "FileName": "certificates/azure.cer"
    }
  ]
}
```

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

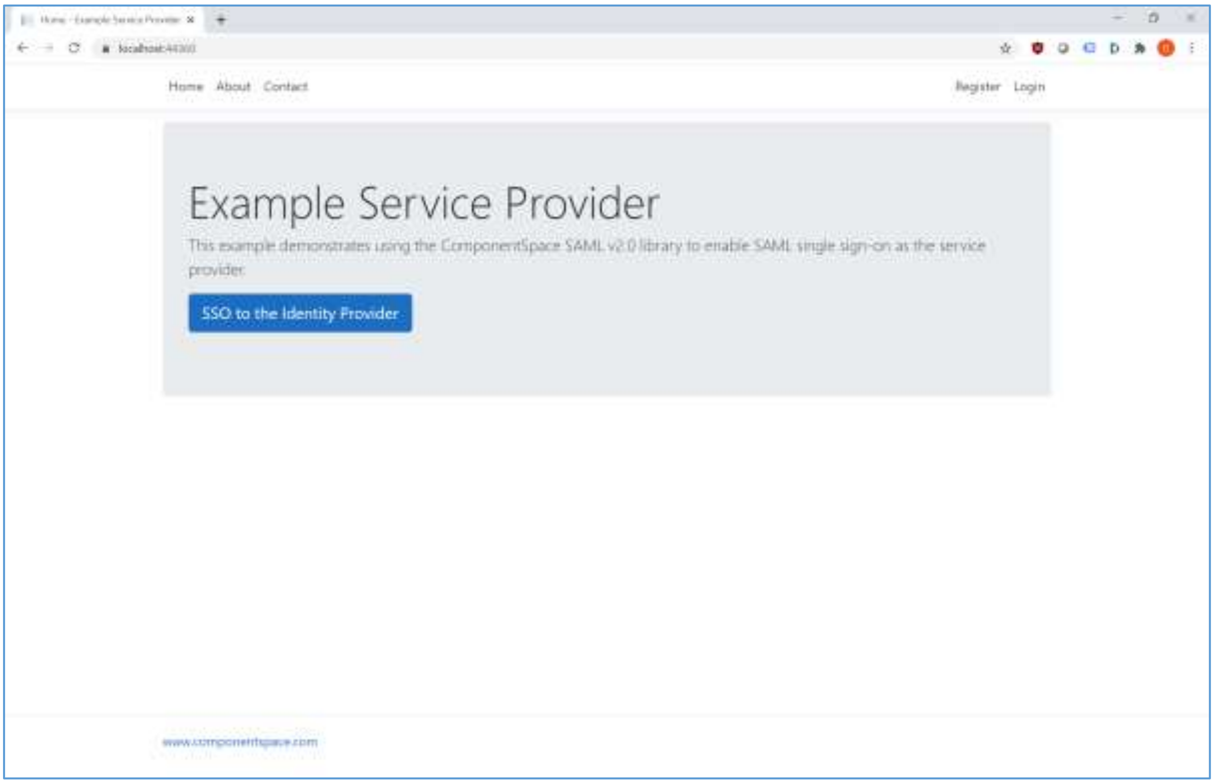
The partner certificate is the SAML signing certificate downloaded from Microsoft Entra. We recommend downloading the base-64 encoded certificate.

Ensure the PartnerName specifies the correct partner identity provider.

```
"PartnerName": "https://sts.windows.net/f2f933ec-d7c9-433f-8926-d3a0732a7dcf/"
```

SP-Initiated SSO

Browse to the example service provider.

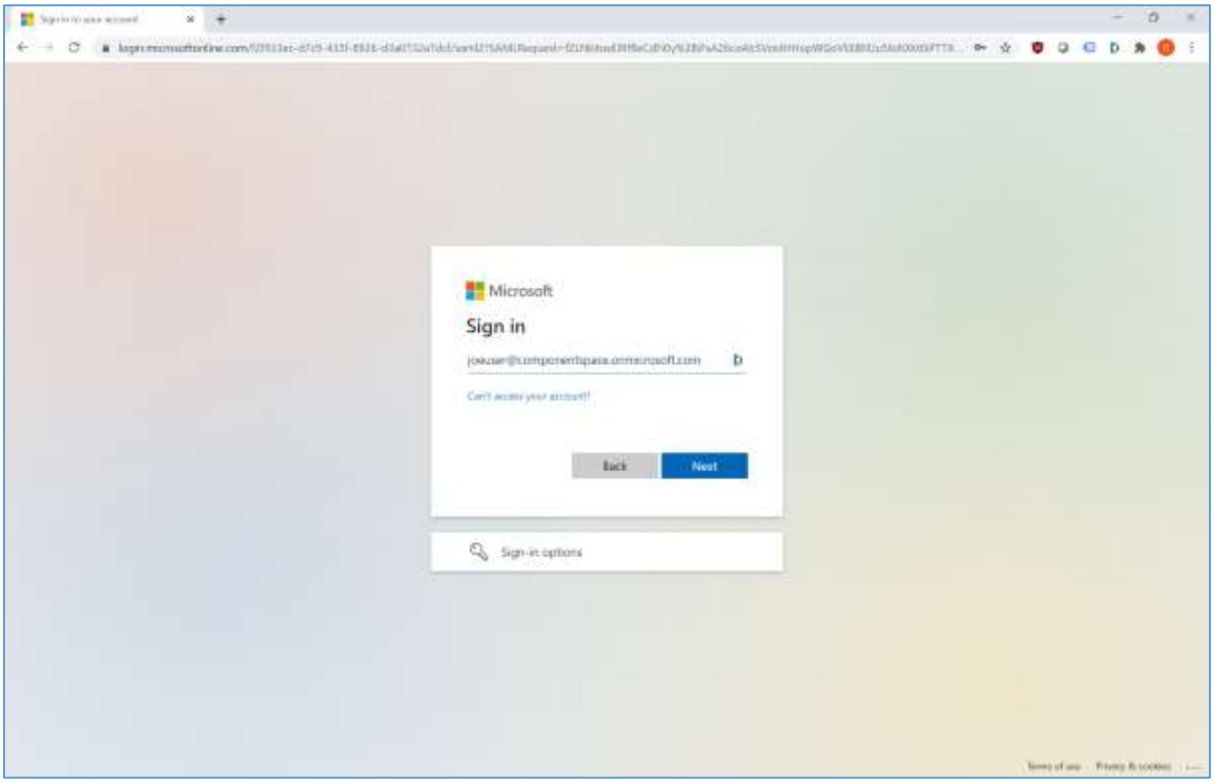


Example Service Provider

This example demonstrates using the ComponentSpace SAML v2.0 library to enable SAML single sign-on as the service provider.

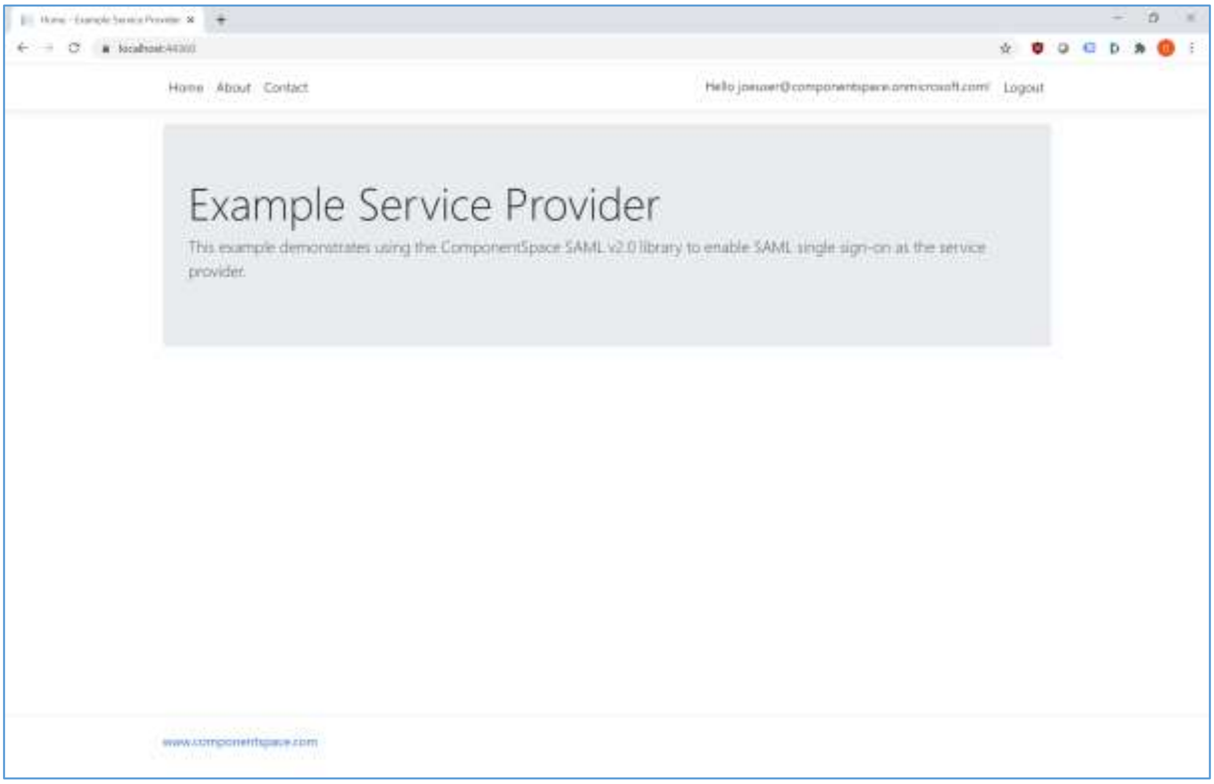
Click the button to SSO to the identity provider.

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



joeuser@componentspace.onmicrosoft.com

The user is automatically logged in at the service provider.



Home - Example Service Provider
localhost:44360
Home
About
Contact
Hello joeuser@componentspace.onmicrosoft.com!
Logout

Example Service Provider

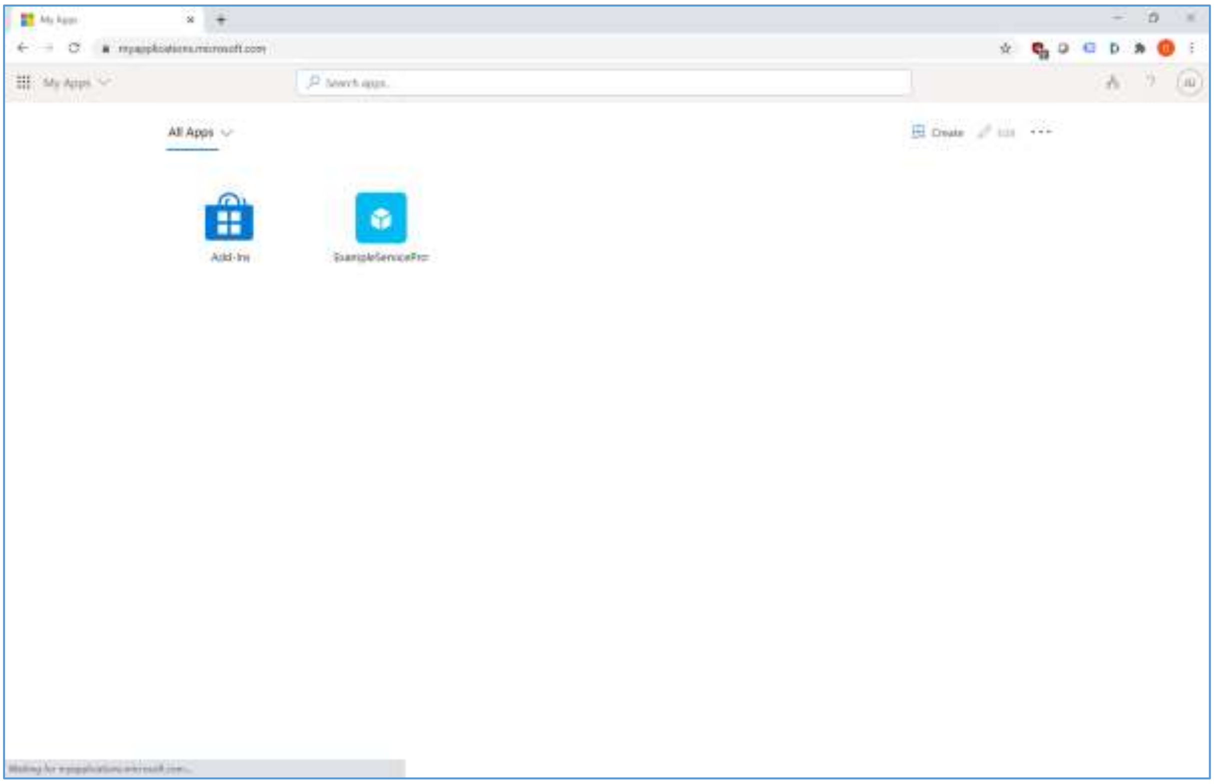
This example demonstrates using the ComponentSpace SAML v2.0 library to enable SAML single sign-on as the service provider.

IdP-Initiated SSO

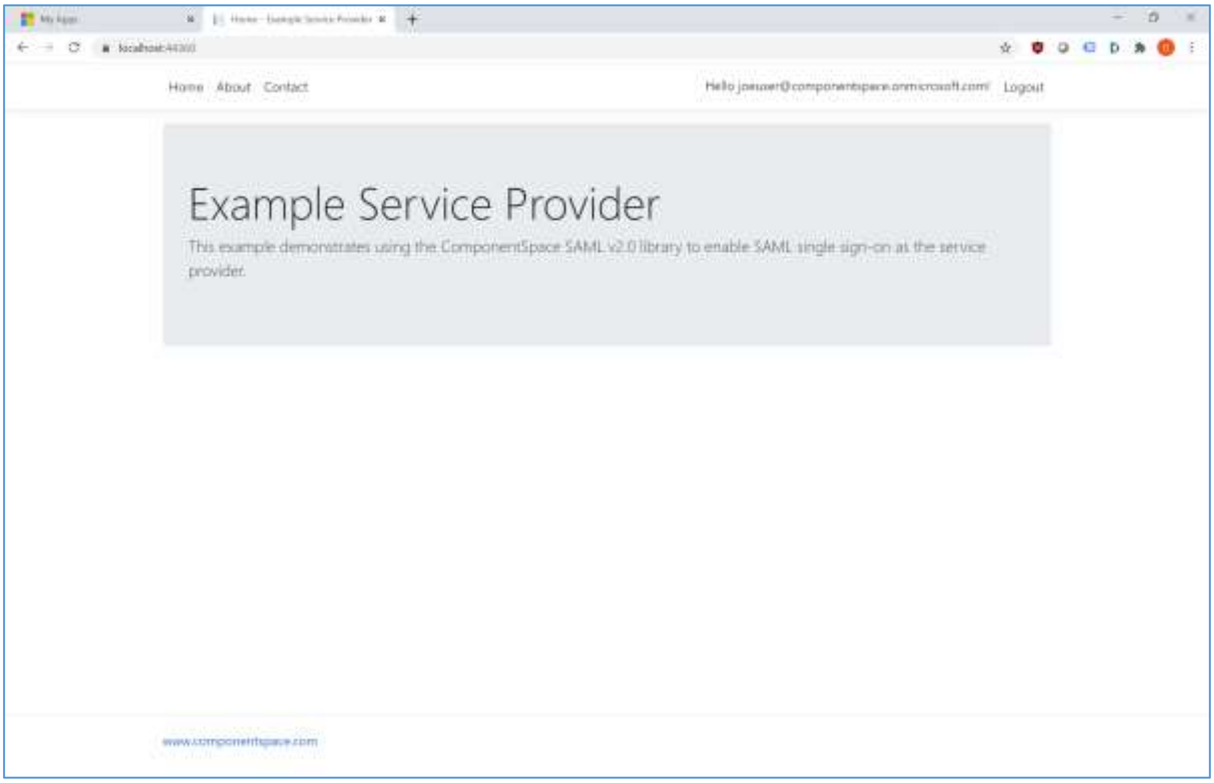
Browse to https://myapps.microsoft.com and login.

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

Select the ExampleServiceProvider application.


My Apps
myapplications.microsoft.com
My Apps
Search apps
All Apps
Create
Edit
Add-Ins
ExampleServicePro
Waiting for myapplications.microsoft.com...

The user is automatically logged in at the service provider.



This example demonstrates using the ComponentSpace SAML v2.0 library to enable SAML single sign-on as 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.

```
{
  "Name": "https://sts.windows.net/",
  "Description": "Entra ID (Azure AD) multitenant",
  "SingleSignOnServiceUrl": "https://login.microsoftonline.com/common/saml2",
  "SingleLogoutServiceUrl": "https://login.microsoftonline.com/common/saml2",
  "PartnerCertificates": [
    {
      "FileName": "certificates/azure.cer"
    },
    {
      "FileName": "certificates/azure-common-1.cer"
    },
    {
      "FileName": "certificates/azure-common-2.cer"
    },
    {
      "FileName": "certificates/azure-common-3.cer"
    },
    {
      "FileName": "certificates/azure-common-4.cer"
    }
  ]
}
```

To support matching SAML message issuer fields against the PartnerIdentityProviderConfiguration.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.
builder.Services.AddTransient<ISamlConfigurationNameResolver,
RegexSamlConfigurationNameResolver>();
```

Troubleshooting

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