



ComponentSpace SAML for ASP.NET Microsoft 365 Integration Guide

Contents

Introduction	1
Configuring a Domain for SAML SSO	1
Confirming a Domain's SSO Settings.....	2
Updating a Domain's SSO Settings.....	3
Adding a User	3
Immutable Identifier	3
Confirming a User's Settings	4
Updating a User	4
Deleting a User.....	4
Microsoft 365 SAML Metadata	4
Identity Provider Configuration	5
SP-Initiated SSO.....	5
SP-Initiated SLO.....	8
IdP-Initiated SSO	9
IdP-Initiated SLO	12


```
Set-MsolDomainAuthentication -FederationBrandName $domain -DomainName $domain -  
Authentication federated -PreferredAuthenticationProtocol SAML -IssuerUri $issuer -  
SigningCertificate $cert -PassiveLogOnUri $ssoUrl -LogOffUri $logoffUrl -Verbose
```

The Set-MsolDomainAuthentication cmdlet configures authentication for the domain.

The “-Authentication federated” parameter specifies to use single sign on.

The “-PreferredAuthenticationProtocol SAML” parameter specifies to use the SAML protocol rather than WS-Federation.

\$domain

The \$domain is a domain name configured in Microsoft 365.

\$issuer

The \$issuer is the identity provider’s name. This name must match with the local identity provider name. For example, if the LocalIdentityProviderConfiguration Name is https://ExampleIdentityProvider, then the \$issuer must be set to the same value.

Microsoft 365 restricts the issuer to a single domain. If the issuer is already defined for a domain, an “Unable to convert the domain. The settings you selected are already in use.” error occurs.

\$ssoUrl

The \$ssoUrl is the identity provider’s SSO service URL. In browser-based SP-initiated SSO, Microsoft 365 will send an authentication request to this endpoint.

\$logoffUrl

The \$logoffUrl is the identity provider’s SLO service URL.

\$cert

The \$cert is the identity provider’s base-64 encoded certificate. Microsoft 365 will use this certificate to verify signed SAML assertions from the identity provider.

Confirming a Domain’s SSO Settings

Run the Get-MsolDomainFederationSettings cmdlet to confirm a domain’s SSO settings.

```
$domain = "componentspace.com"  
Get-MsolDomainFederationSettings -DomainName $domain
```

Run the Get-MsolDomain cmdlet to list the domains and their authentication methods.

```
Get-MsolDomain
```

Updating a Domain's SSO Settings

If the federation settings are to be updated, the authentication method must first be reset to managed.

The following example cmdlet resets the domain to managed.

```
$domain = "componentspace.com"  
Set-MsolDomainAuthentication -DomainName $domain -Authentication Managed
```

Once reset, run the Set-MsolDomainAuthentication cmdlet to configure single sign on for the domain.

Adding a User

Run the New-MsolUser cmdlet to add a user to the domain.

Refer to the Microsoft document for instructions on bulk provisioning.

```
New-MsolUser -UserPrincipalName test@componentspace.com -ImmutableId 12345678 -  
FirstName Test -LastName User -DisplayName "Test User" -LicenseAssignment  
"componentspaceau:ENTERPRISEPACK" -usageLocation US
```

UserPrincipalName

The UserPrincipalName is the primary user identity.

ImmutableId

The ImmutableId is uniquely identifies the user.

LicenseAgreement

The LicenseAssignment assigns licenses to the user. Use the Get-MsolAccountSku cmdlet to select a value for the license assignment.

Immutable Identifier

The immutable identifier uniquely and permanently identifies a user.

The SAML response sent by the identity provider includes the immutable identifier as the subject name identifier in the SAML assertion. The user principal name is included as the IDPEmail SAML attribute. Both these values must match with the Microsoft 365 configuration for single sign on to be successful.

For user information stored in Active Directory, the user's object GUID (objectGUID attribute) may be used as the immutable identifier.

For user information stored in a database or some other user registry, a unique identifier must be assigned as the immutable identifier.

In the example identity provider, a fixed immutable identifier is used.

Confirming a User's Settings

Run the Get-MsolUser to confirm a user's settings.

```
Get-MsolUser -UserPrincipalName test@componentspace.com
```

Additional details, including the immutable identifier, may be retrieved using a PowerShell select.

```
Get-MsolUser -UserPrincipalName test@componentspace.com | select UserPrincipalName, ImmutableId, FirstName, LastName
```

Updating a User

Users may be updated by using the PowerShell Set-MsolUser cmdlet.

```
Set-MsolUser -UserPrincipalName test@componentspace.com -ImmutableId 12345678
```

Deleting a User

During testing, it may be necessary to delete and reconfigure users in Microsoft 365.

Users may be deleted using the Microsoft 365 administration portal or by using the PowerShell Remove-MsolUser cmdlet.

```
Remove-MsolUser -UserPrincipalName test@componentspace.com
```

Deleting a user moves the user to the Microsoft 365 recycle bin. To create a user with the same name, the user first must be removed from the recycle bin. This requires the object identifier associated with the user.

The Get-MsolUser cmdlet is used to retrieve the object identifier.

```
Get-MsolUser -ReturnDeletedUsers -SearchString test@componentspace.com | select UserPrincipalName, ObjectId
```

The Remove-MsolUser cmdlet is used to delete the user from the recycle bin.

```
Remove-MsolUser -RemoveFromRecycleBin -ObjectId 67d6bdaa-b312-41b9-b8d0-8311dabc07ed
```

Microsoft 365 SAML Metadata

Metadata may be downloaded from:

<https://nexus.microsoftonline-p.com/federationmetadata/saml20/federationmetadata.xml>

Identity Provider Configuration

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

```
<PartnerServiceProvider
  Name="urn:federation:MicrosoftOnline"
  Description=" Microsoft 365"
  SignAssertion="true"
  NameIDFormat="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"
  AuthnContext="urn:oasis:names:tc:SAML:2.0:ac:classes>PasswordProtectedTransport"
  AssertionConsumerServiceUrl="https://login.microsoftonline.com/login.srf"
  SingleLogoutServiceUrl="https://login.microsoftonline.com/login.srf">
  <PartnerCertificates>
    <Certificate FileName="Certificates\microsoft365.cer"/>
  </PartnerCertificates>
</PartnerServiceProvider>
```

Some of this information was extracted from the Microsoft 365 SAML metadata.

The two partner certificate files correspond to the two signing certificates included in the metadata.

Ensure the PartnerName specifies the correct partner identity provider.

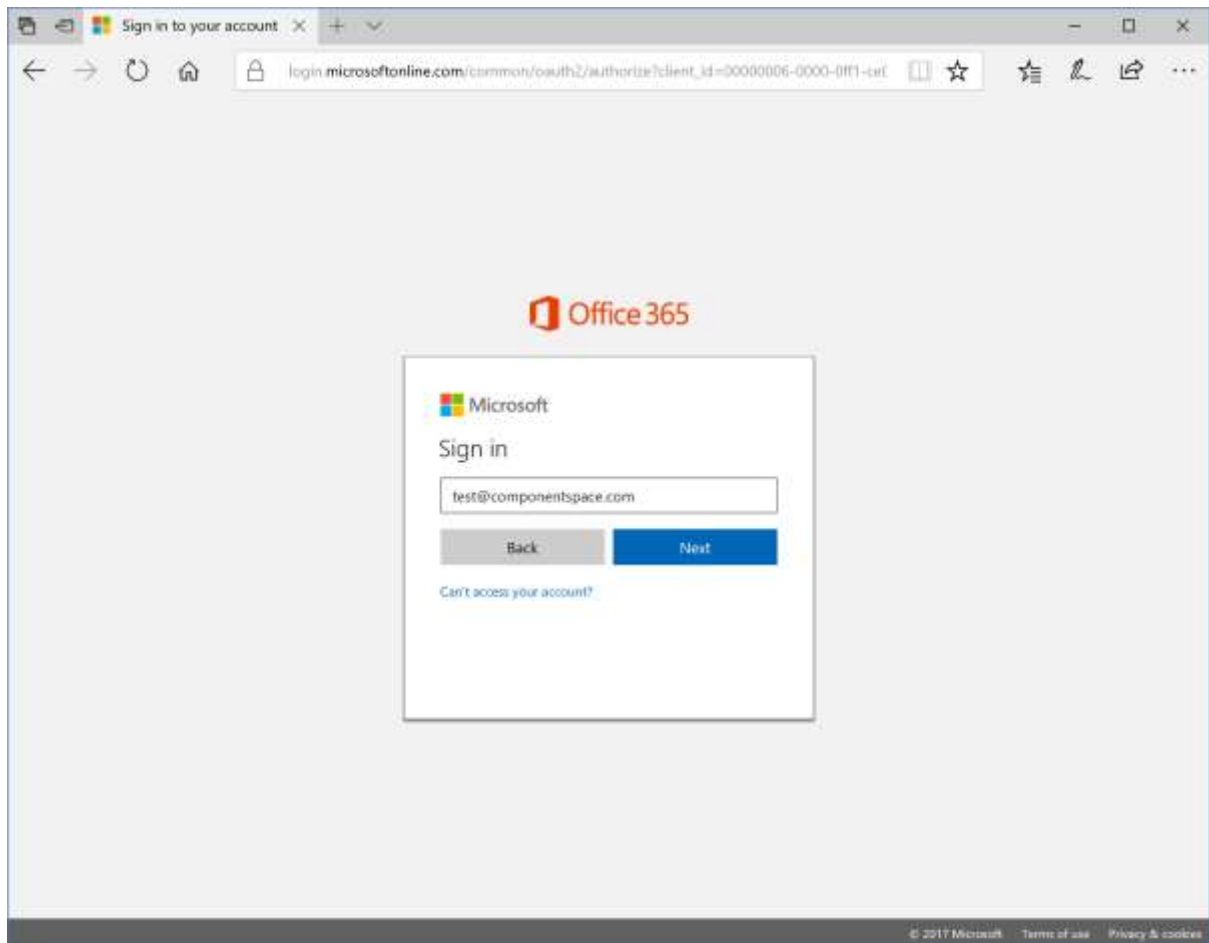
```
<add key="PartnerName" value="urn:federation:MicrosoftOnline"/>
```

SP-Initiated SSO

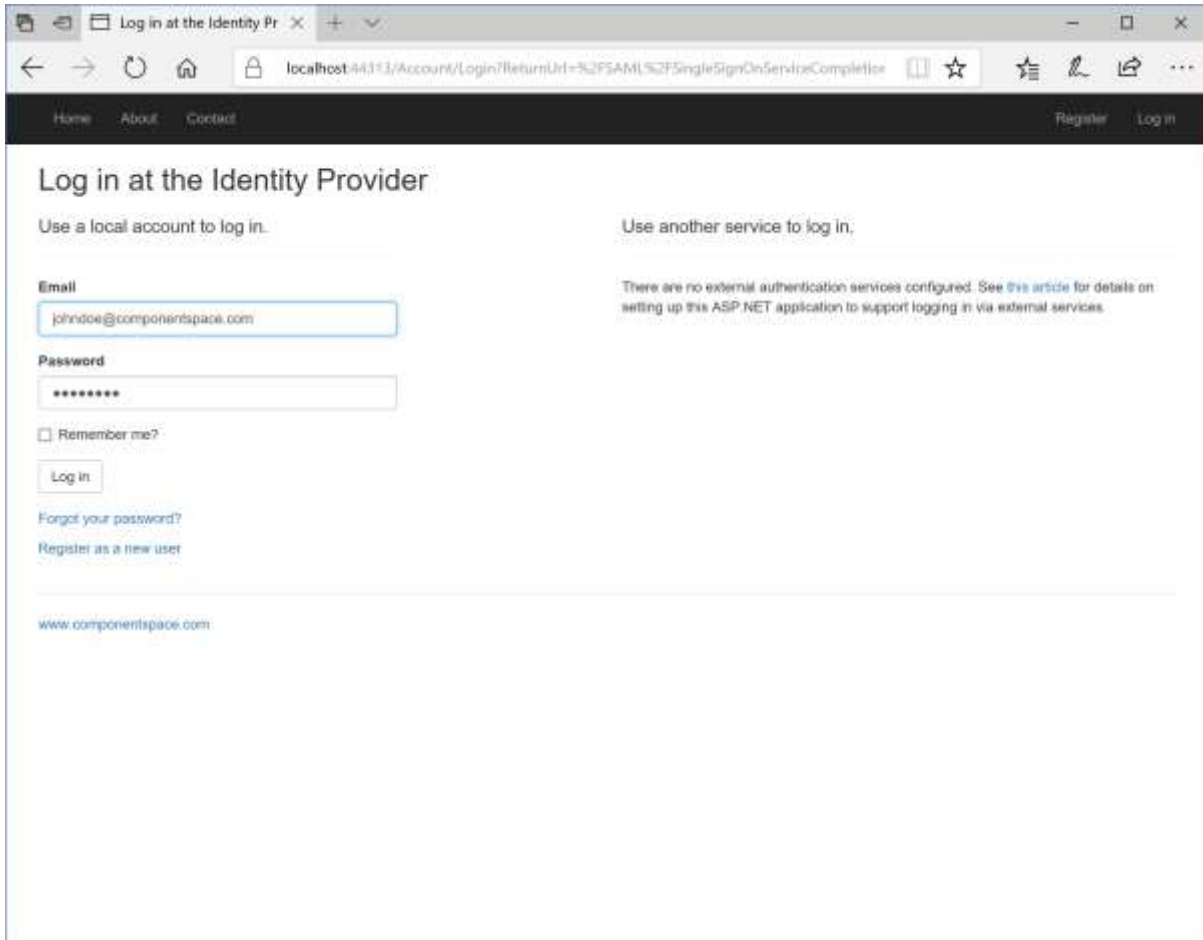
Browse to <https://portal.microsoftonline.com>.

Specify a user with a federated domain name (e.g. test@componentspace.com).

ComponentSpace SAML for ASP.NET Microsoft 365 Integration Guide

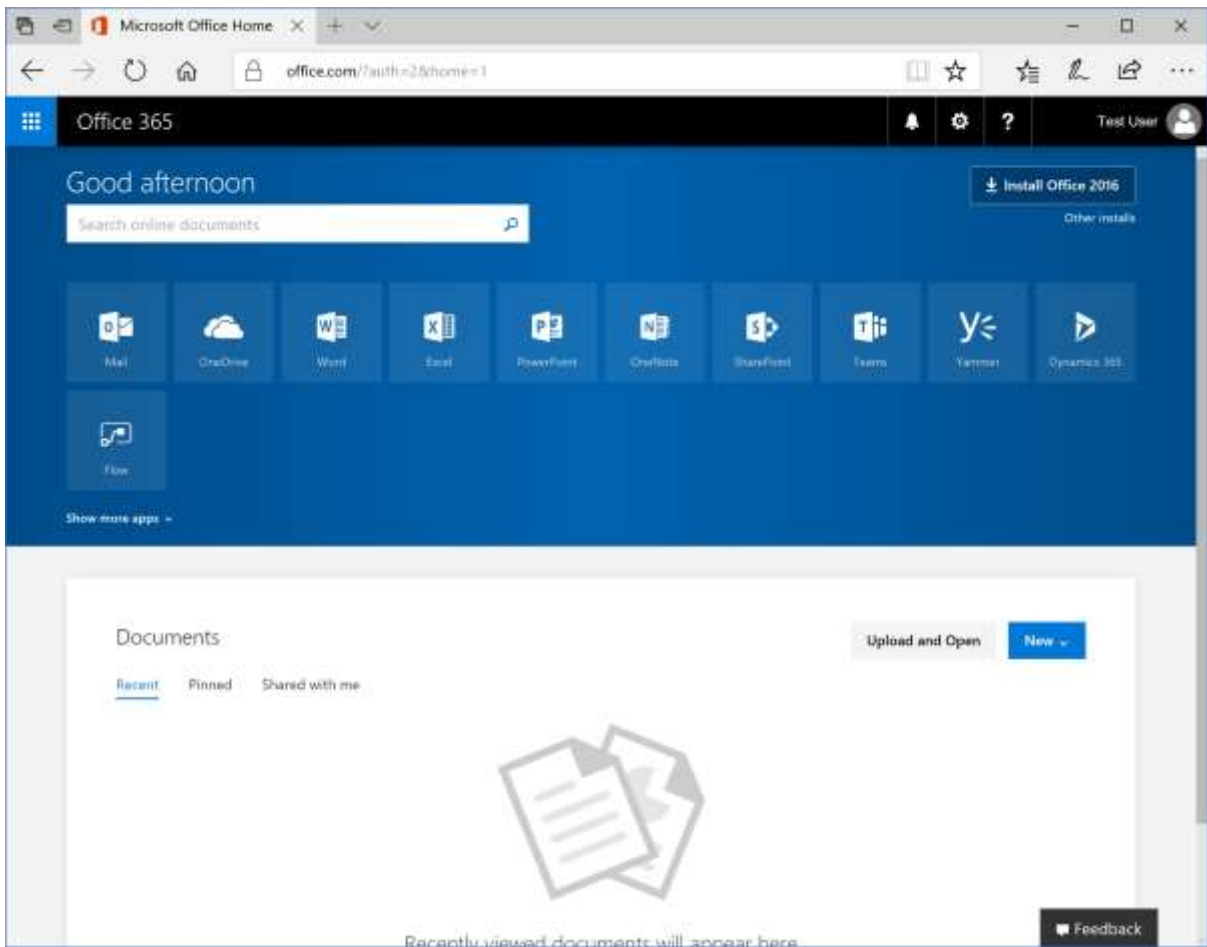


Microsoft 365 passes control to the identity provider.



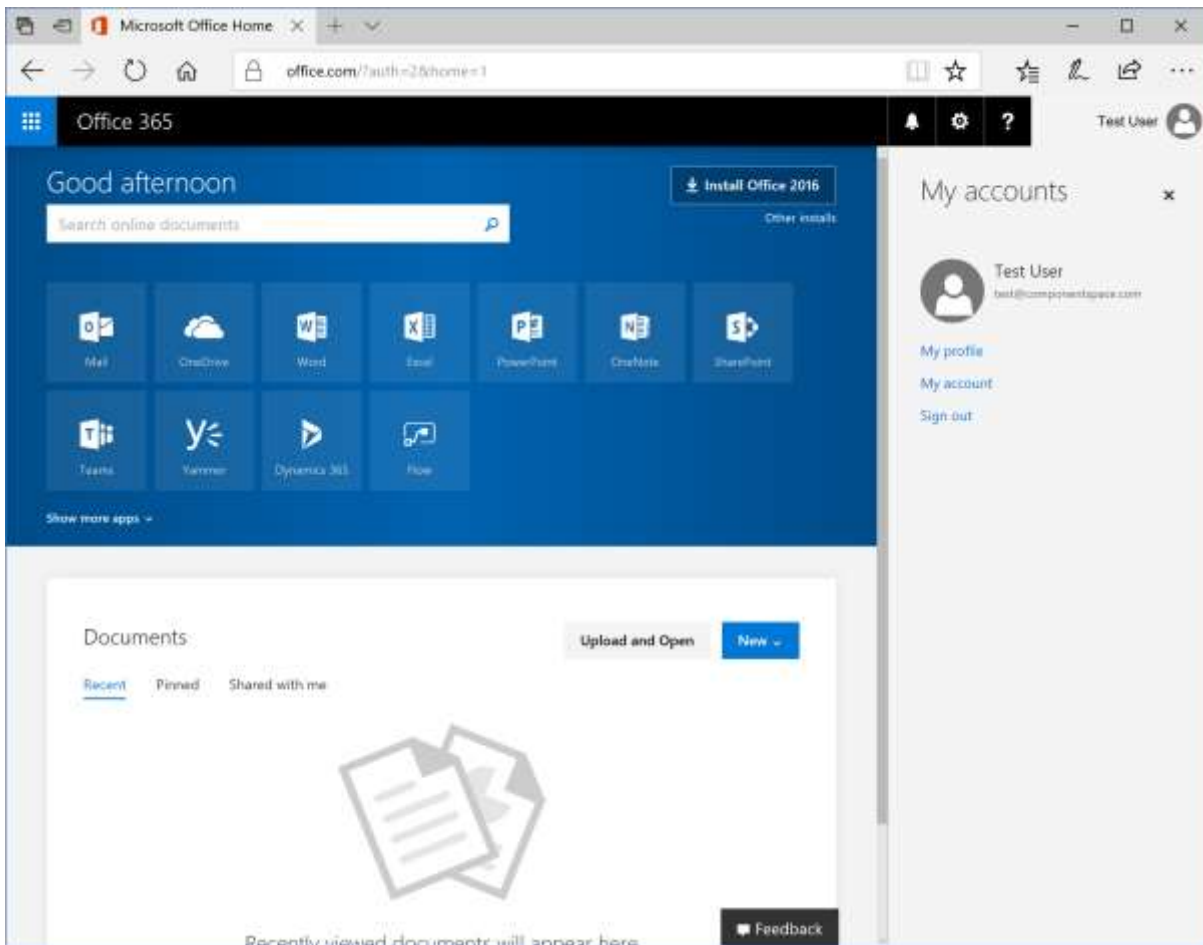
Login at the identity provider.

The identity provider returns control to Microsoft 365 where the user is automatically logged in.



SP-Initiated SLO

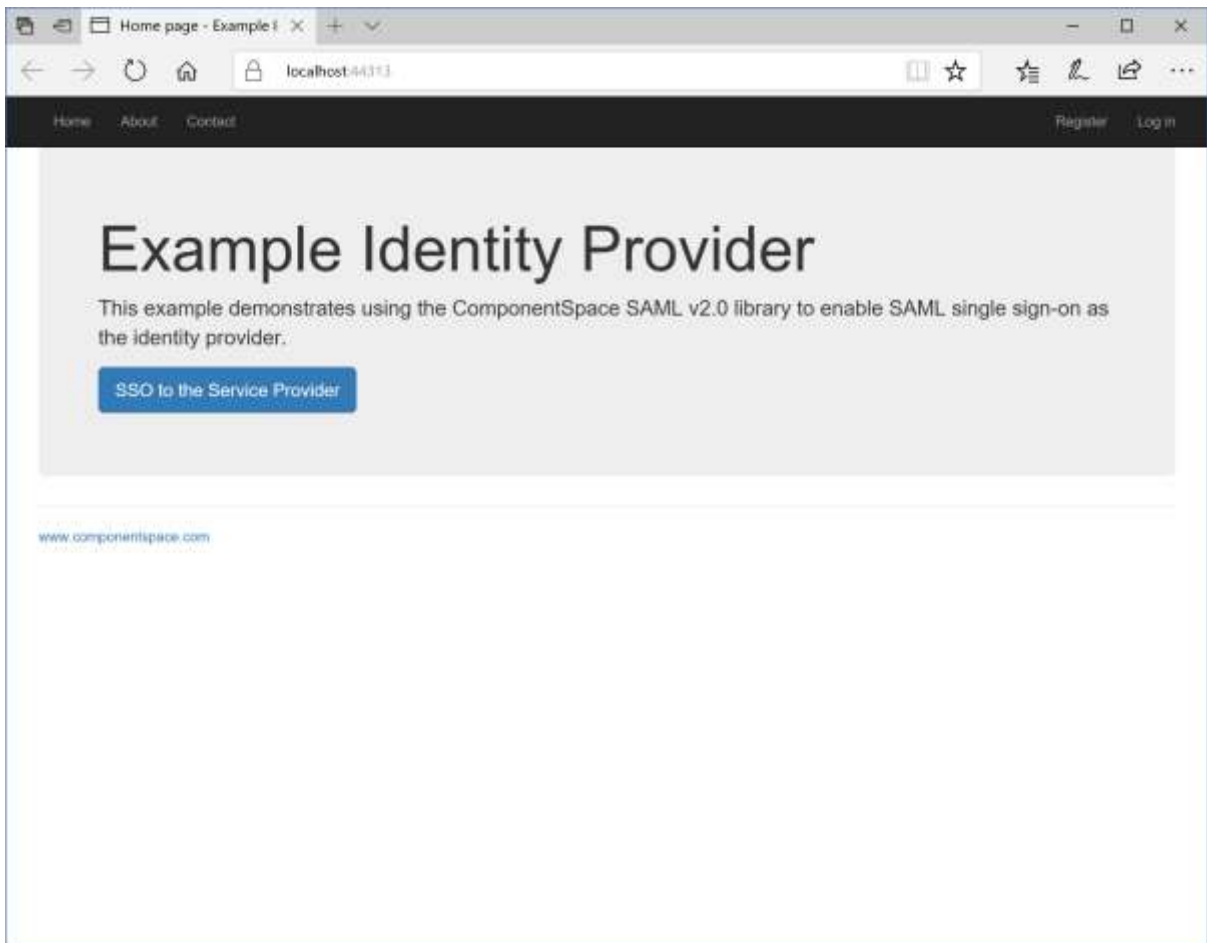
Logout from Microsoft 365.



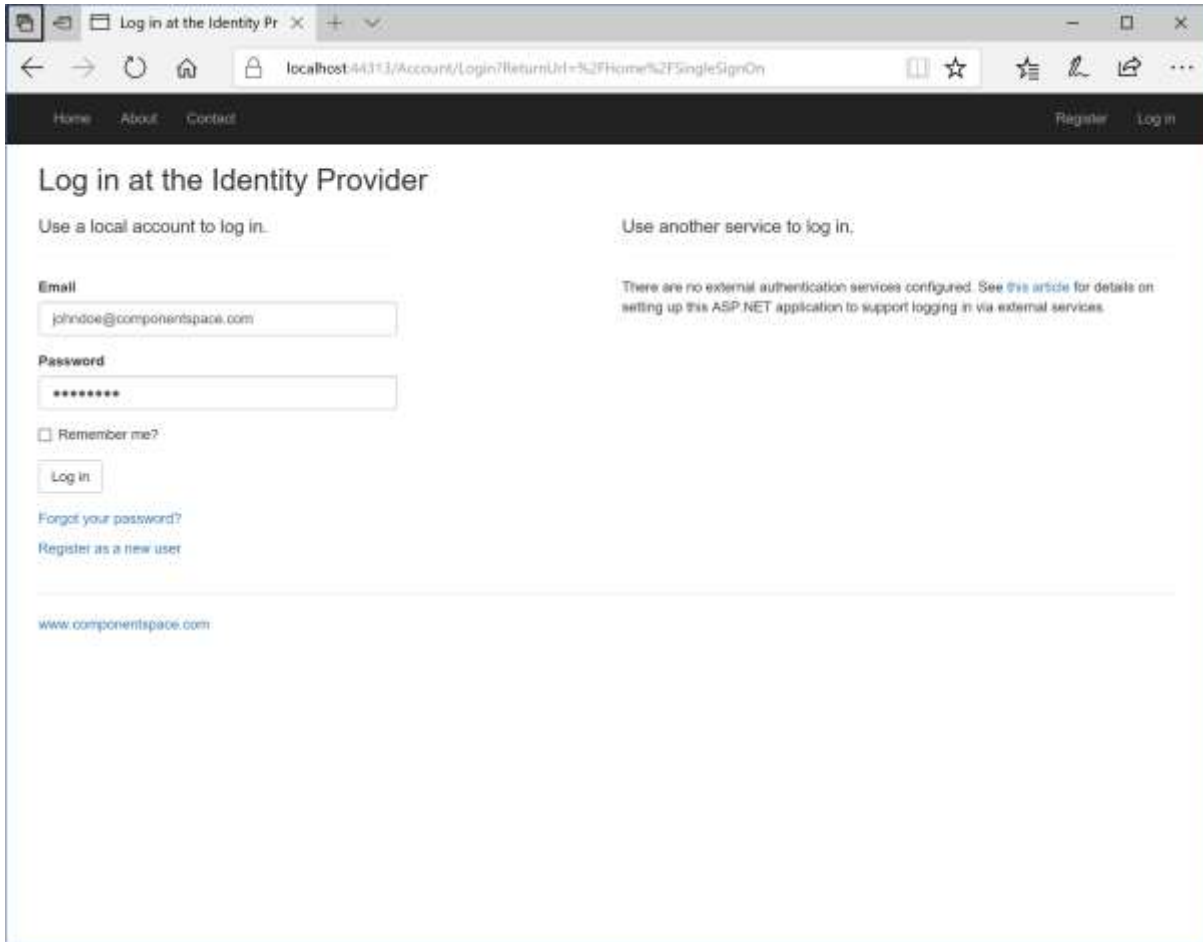
The user is also logged out from the identity provider.

IdP-Initiated SSO

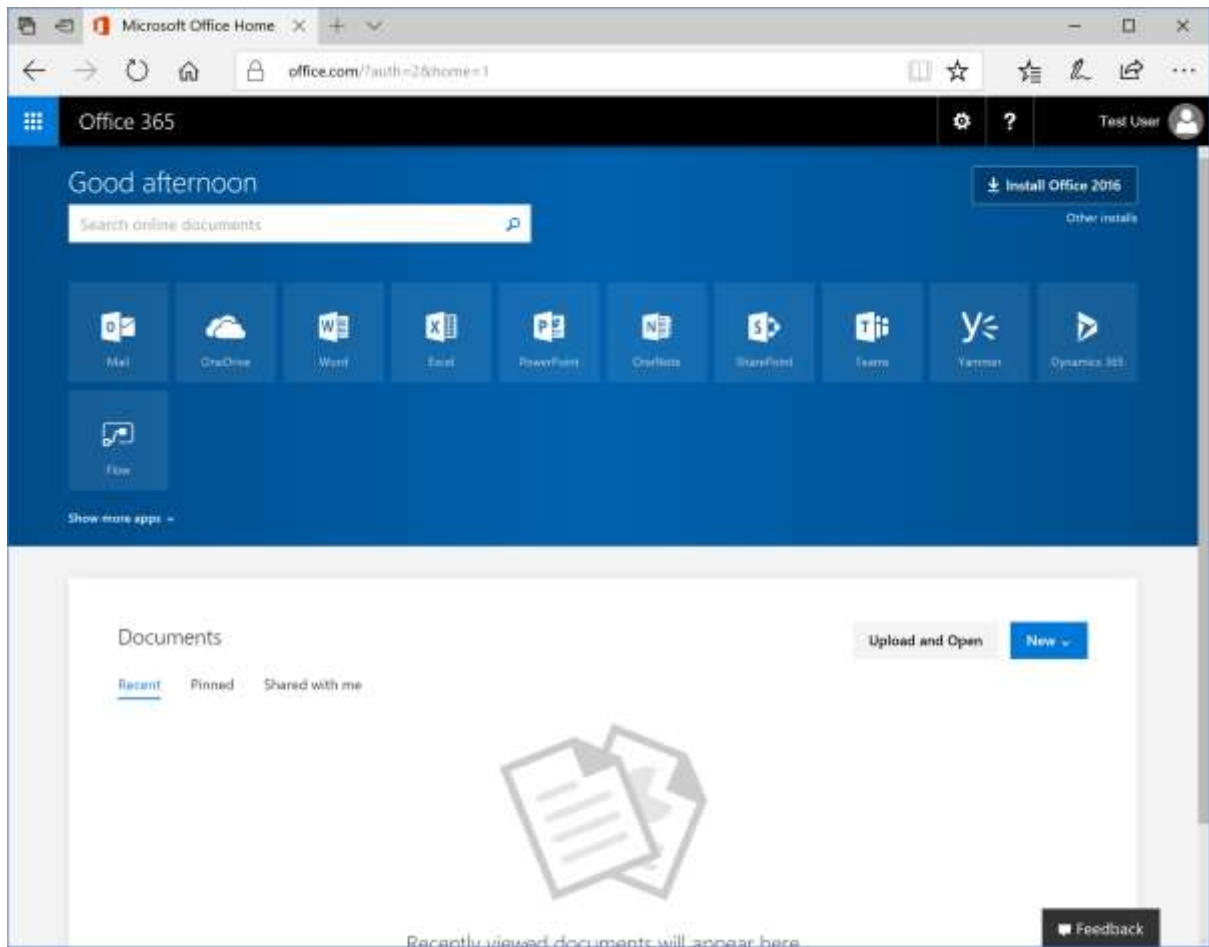
Browse to the identity provider.



Click the button to SSO.

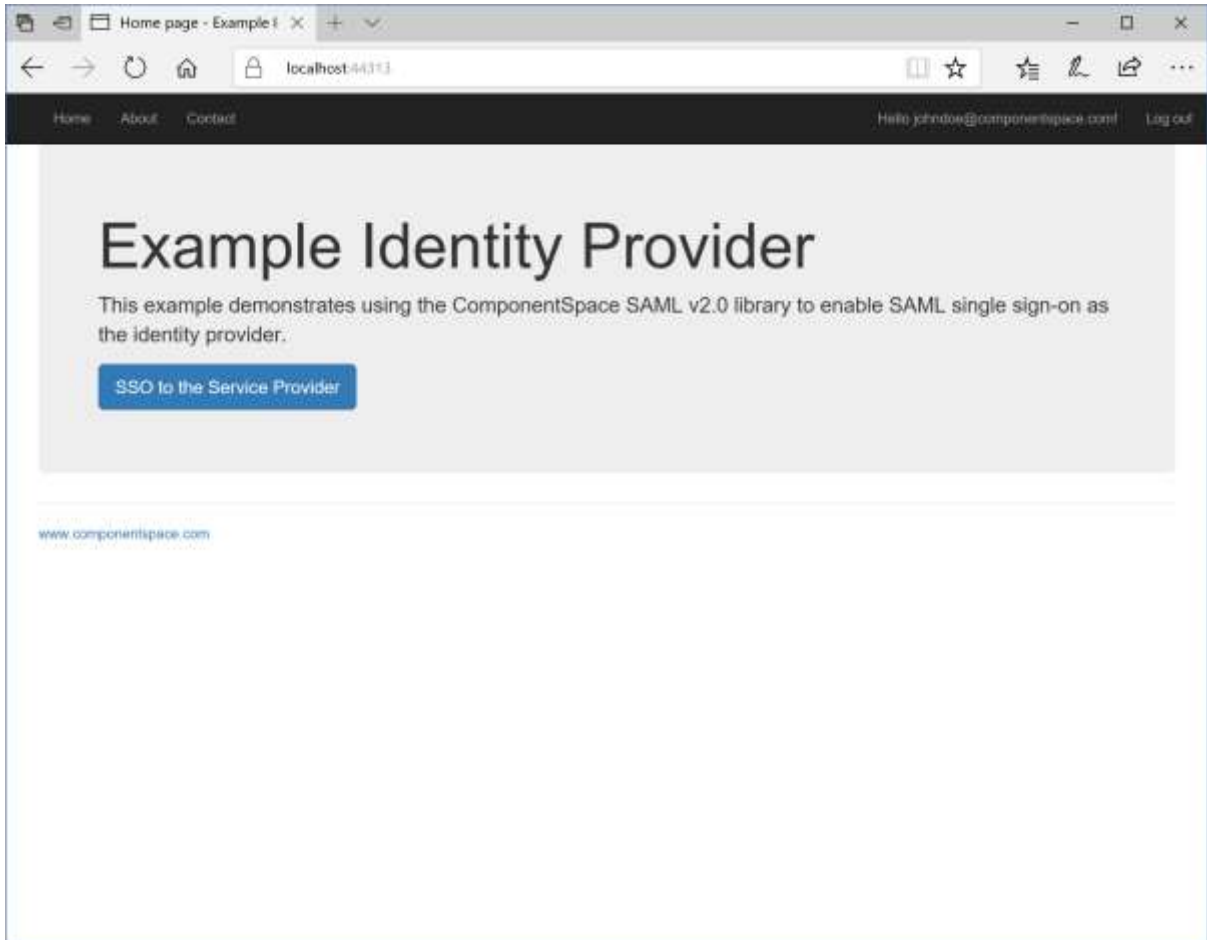


Login and control passes to Microsoft 365 where the user is automatically logged in.



IdP-Initiated SLO

Browse to the identity provider and logout.



Control passes to Microsoft 365 but the user is not logged out.

This is a limitation in Microsoft 365 of a less frequently used scenario.

The user should close the browser to ensure successful logout.