

ComponentSpace

SAML for ASP.NET Core

Salesforce

Identity Provider

Integration Guide

Contents

Introduction.....	1
Enabling the Identity Provider	1
Creating a Connected App	3
Service Provider Configuration	7
SP-Initiated SSO	8
IdP-Initiated SSO	10
SAML Logout.....	12

Introduction

This document describes integration with Salesforce as the identity provider.

For information on configuring Salesforce for SAML SSO, refer to the following articles.

https://help.salesforce.com/articleView?id=identity_provider_enable.htm&type=0

https://developer.salesforce.com/page/Salesforce_IdP_Setup

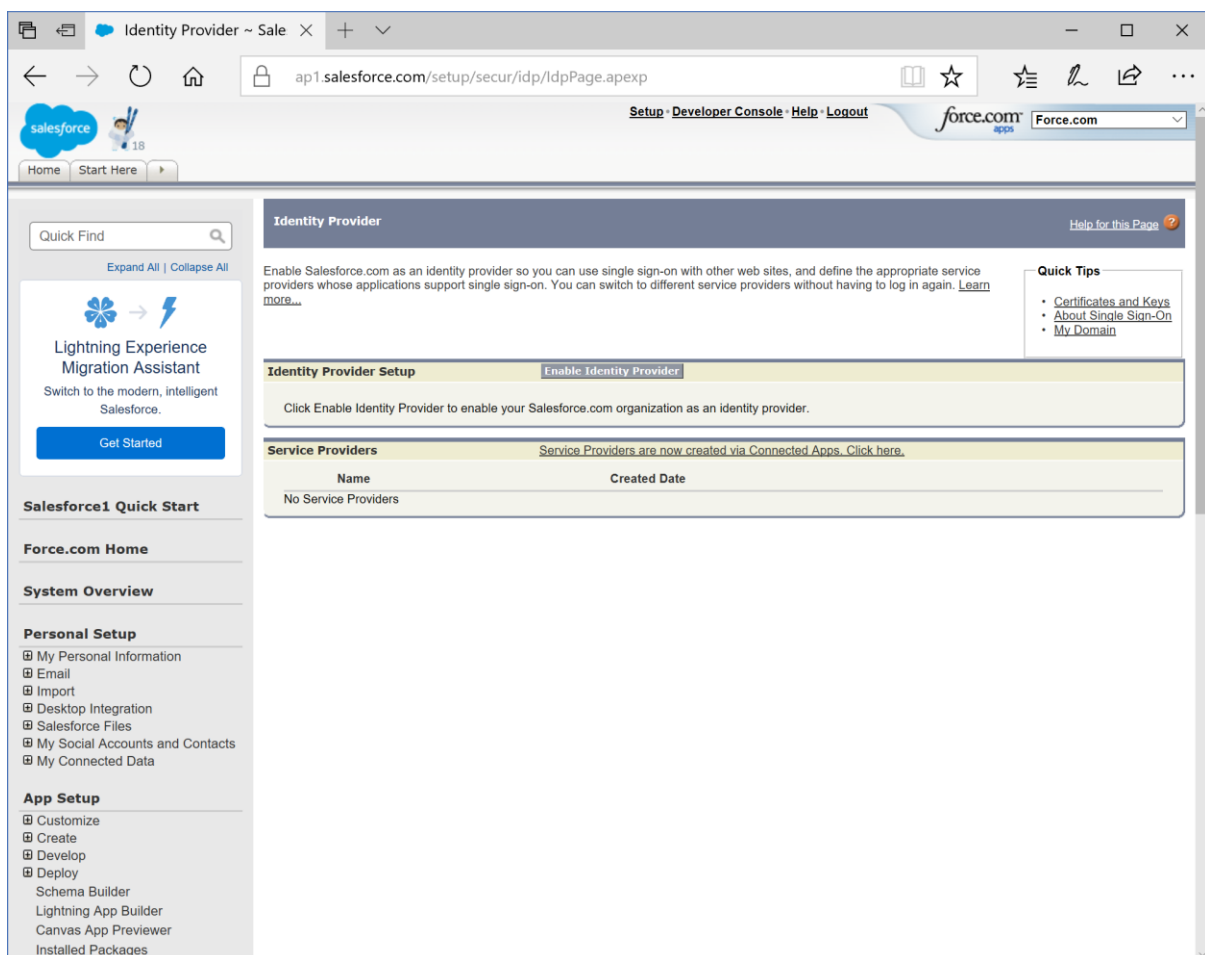
Enabling the Identity Provider

Log into Salesforce as an administrator.

<https://login.salesforce.com>

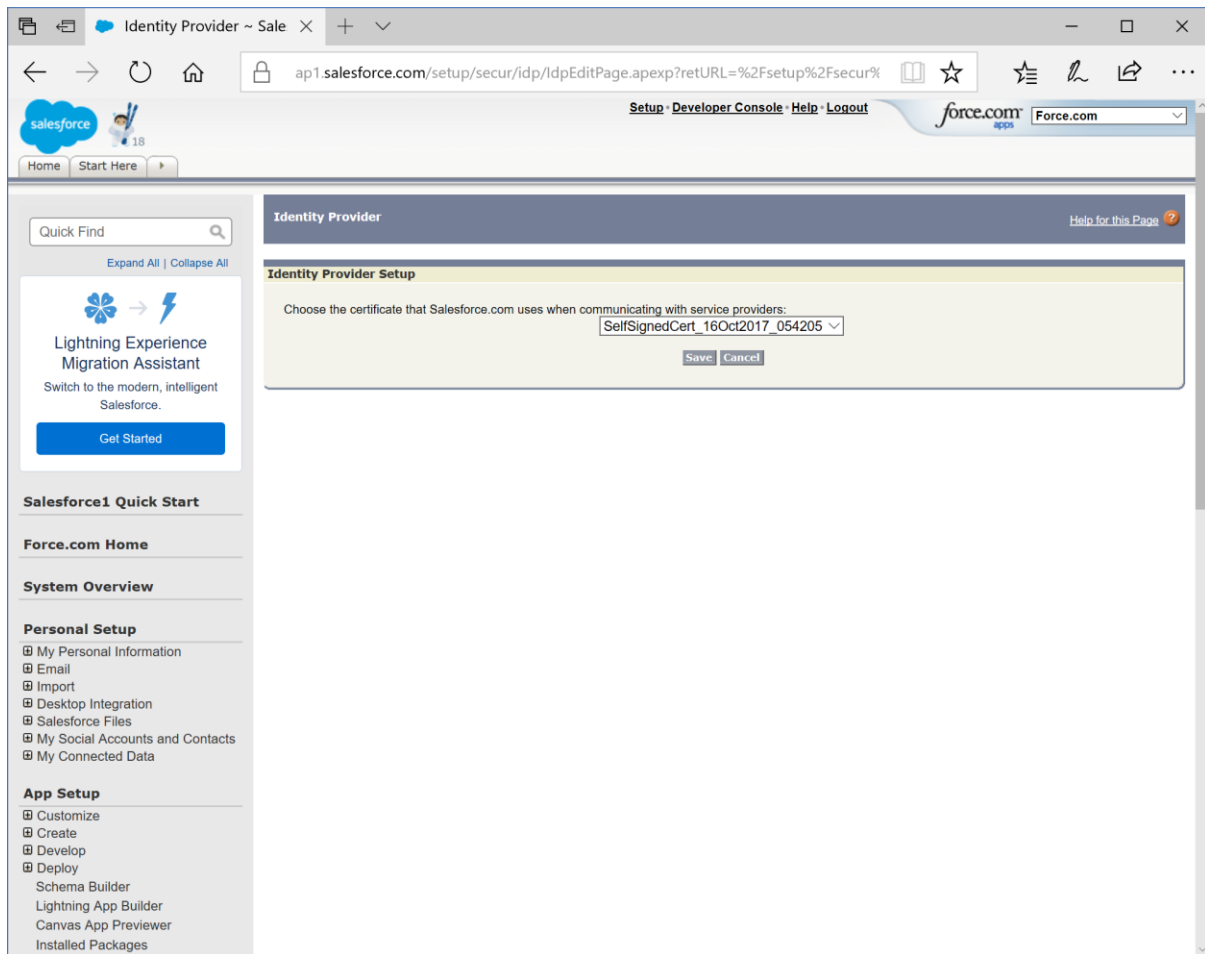
Select Setup > Administration Setup > Security Controls > Identity Provider.

Enable the identity provider.



Select a Salesforce certificate to use.

ComponentSpace SAML for ASP.NET Core Salesforce Identity Provider Integration Guide



Download the metadata. This is used to configure the service provider.

ComponentSpace SAML for ASP.NET Core Salesforce Identity Provider Integration Guide

The screenshot shows the Salesforce Identity Provider Setup page in a web browser. The browser's address bar displays the URL `ap1.salesforce.com/setup/secur/ldp/ldpPage.apexp`. The page header includes the Salesforce logo, a user profile icon, and navigation links for Setup, Developer Console, Help, and Logout. The main content area is titled "Identity Provider" and contains a brief explanation of the setup process. Below this, the "Identity Provider Setup" section is expanded, showing details for the current setup, including the issuer, certificate details, and SAML metadata discovery endpoints. The "Service Providers" section is also visible, showing a table with columns for Name and Created Date, and a message indicating that service providers are now created via Connected Apps.

Identity Provider

Enable Salesforce.com as an identity provider so you can use single sign-on with other web sites, and define the appropriate service providers whose applications support single sign-on. You can switch to different service providers without having to log in again. [Learn more...](#)

Quick Tips

- [Certificates and Keys](#)
- [About Single Sign-On](#)
- [My Domain](#)

Identity Provider Setup [Edit](#) [Disable](#) [Download Certificate](#) [Download Metadata](#)

Details

Issuer `https://componentspace-dev-ed.my.salesforce.com`

Currently chosen certificate details

Label	Unique Name
<code>SelfSignedCert_16Oct2017_054205</code>	<code>SelfSignedCert_16Oct2017_054205</code>
Created Date	Expiration Date
16/10/2017 4:42 PM	16/10/2019 11:00 AM
Key Size	
4096	

SAML Metadata Discovery Endpoints

Service Provider	Endpoint
Salesforce Identity	<code>https://componentspace-dev-ed.my.salesforce.com/.well-known/samlidp.xml</code>

Service Providers [Service Providers are now created via Connected Apps. Click here.](#)

Name	Created Date
No Service Providers	

Creating a Connected App

Select Setup > App Setup > Create > Apps.

ComponentSpace SAML for ASP.NET Core Salesforce Identity Provider Integration Guide

The screenshot shows the Salesforce App Manager interface. The browser address bar displays a URL from ap1.salesforce.com. The page header includes navigation links like 'Setup', 'Developer Console', 'Help', and 'Logout', along with the 'force.com' logo and a user profile dropdown. The left sidebar contains a 'Quick Find' search bar and a list of navigation items: 'Salesforce1 Quick Start', 'Force.com Home', 'System Overview', 'Personal Setup' (with sub-items like 'My Personal Information', 'Email', 'Import', 'Desktop Integration', 'Salesforce Files', 'My Social Accounts and Contacts', 'My Connected Data'), and 'App Setup' (with sub-items like 'Customize', 'Create', 'Apps', 'Custom Labels', 'Interaction Log Layouts', 'Objects', 'Big Objects', 'Picklist Value Sets').

The main content area is titled 'Apps' and includes a 'Help for this Page' link. It contains an introductory paragraph about apps, a yellow informational banner about User Profile Tab Visibility settings, and a table of existing apps. Below the table is a 'Connected Apps' section showing 'No Apps found.' and a 'New' button to create a connected app.

Action	App Label	Console	Custom	Description
Edit Del	Force.com	☐	☒	Start Here
Edit	Ideas	☐	☐	Salesforce CRM Ideas
Edit	Marketing	☐	☐	Best-in-class on-demand marketing automation
Edit	Platform	☐	☐	The fundamental Force.com platform
Edit	Sales	☐	☐	The world's most popular sales force automation (SFA) solution
Edit	Service	☐	☐	Manage customer service with accounts, contacts, cases, and more
Edit	Site.com	☐	☐	Build pixel-perfect, data-rich websites using the drag-and-drop Site.com application, and manage content and published sites.

Click new to create a connected app.

Connected App ~ Sales

ap1.salesforce.com/app/mgmt/forceconnectedapps/forceAppEdit.apexp

Quick Find

Expand All | Collapse All

Lightning Experience Migration Assistant

Switch to the modern, intelligent Salesforce.

Get Started

Salesforce1 Quick Start

Force.com Home

System Overview

Personal Setup

- My Personal Information
- Email
- Import
- Desktop Integration
- Salesforce Files
- My Social Accounts and Contacts
- My Connected Data

App Setup

- Customize
- Create
 - Apps
 - Custom Labels
 - Interaction Log Layouts
 - Objects
 - Big Objects
 - Picklist Value Sets
 - Packages
 - Report Types
 - Tags
 - Service Cloud Launch Pad
 - Action Link Templates

New Connected App

Save Cancel

Basic Information

Connected App Name ExampleServiceProvider

API Name ExampleServiceProvider

Contact Email support@componentspace.com

Contact Phone

Logo Image URL

Icon URL

Info URL

Description

API (Enable OAuth Settings)

Enable OAuth Settings

Web App Settings

Start URL

Enable SAML

Entity ID https://ExampleServiceProvider

ACS URL https://localhost:44360/SAML/AssertionConsumerService

Enable Single Logout

Single Logout URL https://localhost:44360/SAML/SingleLogoutService

Single Logout Binding

Subject Type Username

Name ID Format urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified

Issuer https://componentspace-dev-ed.my.salesforce.com

IdP Certificate Default IdP Certificate

Verify Request Signatures

Encrypt SAML Response

Upload a certificate: C:\ComponentSpace\Pro Browse...

The connect app name and app name are for display purposes only.

The entity ID is the service provider's name.

For example:

<https://ExampleServiceProvider>

The assertion consumer service URL is the endpoint to receive SAML responses.

For example:

<https://localhost:44360/SAML/AssertionConsumerService>

The single logout service URL is the endpoint to receive SAML logout messages.

For example:

<https://localhost:44360/SAML/SingleLogoutService>

SAML authn request are signed so the service provider's certificate is uploaded.

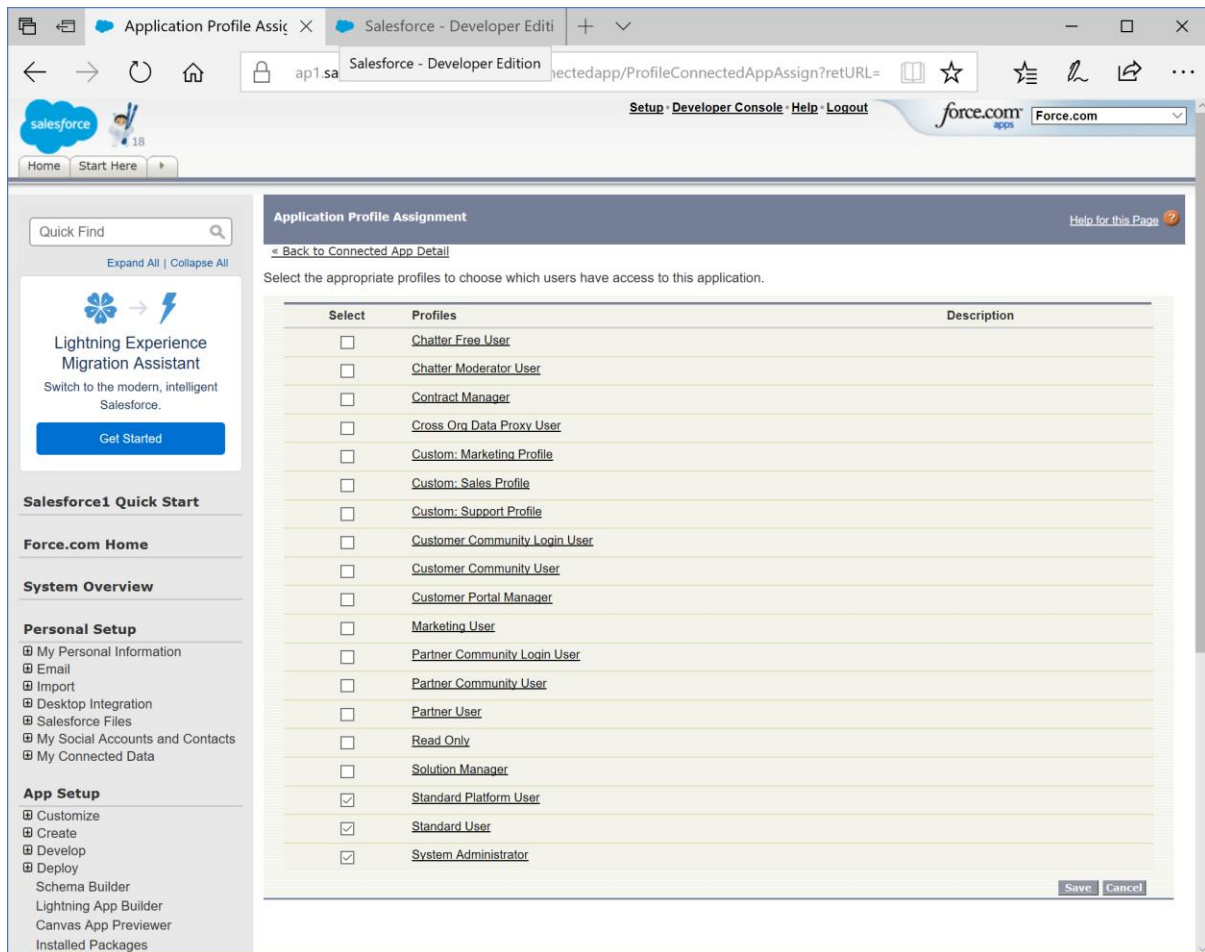
For example:

sp.cer

Click Manage > Manage Profiles.

Permit users to access the connected app by assigning profiles.

ComponentSpace SAML for ASP.NET Core Salesforce Identity Provider Integration Guide



The screenshot shows the Salesforce 'Application Profile Assignment' page. The browser address bar indicates the URL is `ap1.salesforce.com/connectedapp/ProfileConnectedAppAssign?retURL=`. The page title is 'Application Profile Assignment'. Below the title, there is a link to 'Back to Connected App Detail'. The main instruction is 'Select the appropriate profiles to choose which users have access to this application.' Below this is a table with columns 'Select', 'Profiles', and 'Description'. The table lists various profiles, and the 'Standard Platform User', 'Standard User', and 'System Administrator' profiles are selected with checkboxes. At the bottom right of the table, there are 'Save' and 'Cancel' buttons.

Select	Profiles	Description
☐	Chatter Free User	
☐	Chatter Moderator User	
☐	Contract Manager	
☐	Cross Org Data Proxy User	
☐	Custom: Marketing Profile	
☐	Custom: Sales Profile	
☐	Custom: Support Profile	
☐	Customer Community Login User	
☐	Customer Community User	
☐	Customer Portal Manager	
☐	Marketing User	
☐	Partner Community Login User	
☐	Partner Community User	
☐	Partner User	
☐	Read Only	
☐	Solution Manager	
☒	Standard Platform User	
☒	Standard User	
☒	System Administrator	

Review the connected app's configuration.

Note the URL for IdP-initiated SSO.

The screenshot shows the Salesforce 'Connected App: Example' configuration page. The left sidebar contains navigation links for System Overview, Personal Setup, App Setup, and Administration Setup. The main content area is divided into several sections:

- SAML Service Provider Settings:** A table with fields for Entity ID, Subject Type, IdP Certificate, Name ID Format, Verify Request, Signatures, and Enable Single Logout.
- SAML Login Information:** A section for viewing and downloading SAML endpoint metadata, including fields for IdP-Initiated Login URL, SP-Initiated POST Endpoint, SP-Initiated Redirect Endpoint, Metadata Discovery Endpoint, and Single Logout Endpoint.
- Custom Connected App Handler:** A section for defining the Apex Plugin Class and Run As user.
- Trusted IP Range for OAuth Web server flow:** A section for defining IP ranges.
- Profiles:** A table listing profiles such as Standard Platform User, Standard User, and System Administrator.
- Permission Sets:** A section for managing permission sets.
- Custom Attributes:** A section for managing custom attributes.

Service Provider Configuration

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

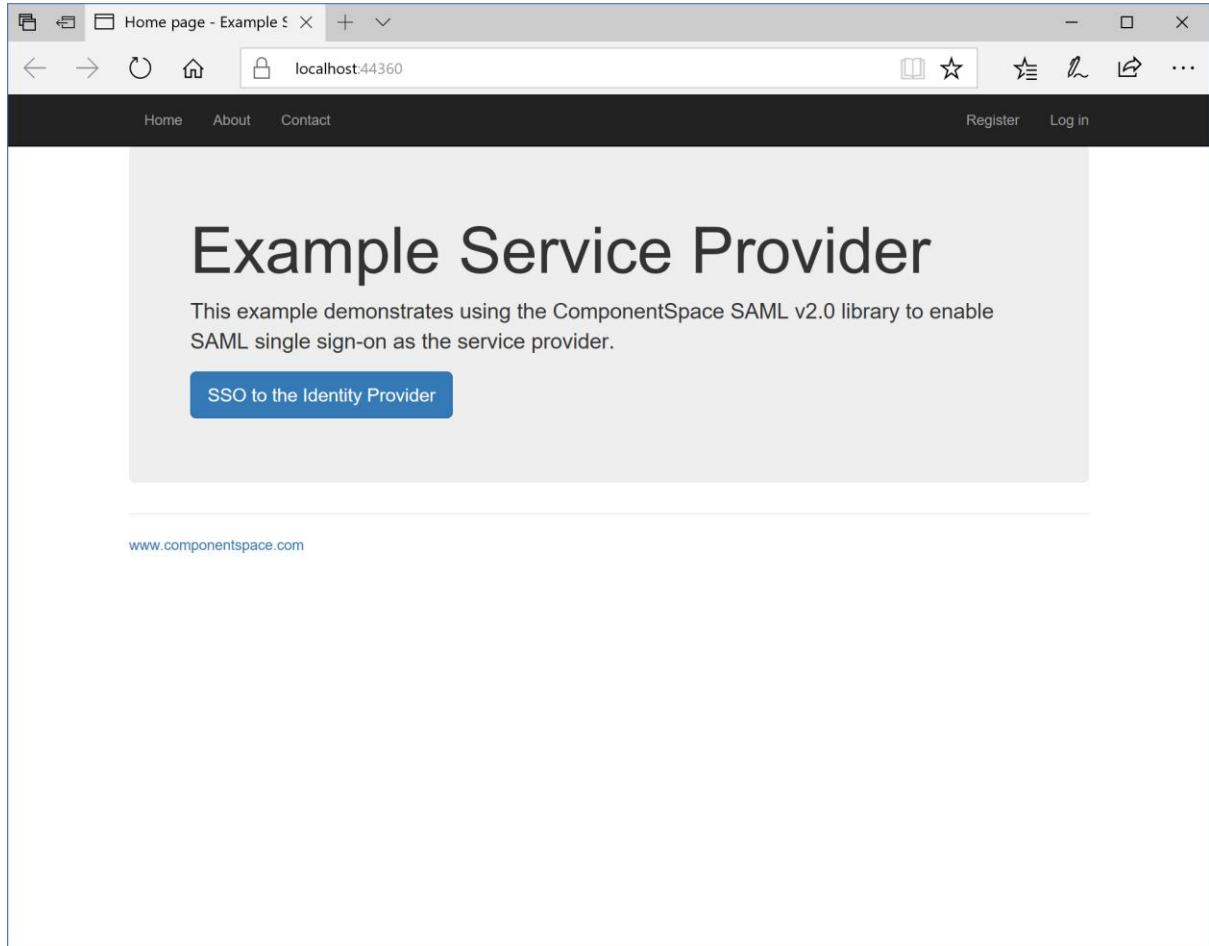
```
{
  "Name": "https://componentspace-dev-ed.my.salesforce.com",
  "Description": "Salesforce",
  "SignAuthnRequest": true,
  "SingleSignOnServiceUrl": "https://componentspace-dev-ed.my.salesforce.com/idp/endpoint/HttpRedirect",
  "SingleLogoutServiceUrl": "https://componentspace-dev-ed.my.salesforce.com/services/auth/idp/saml2/logout",
  "PartnerCertificates": [
    {
      "FileName": "certificates/salesforce.cer"
    }
  ]
}
```

Ensure the PartnerName specifies the correct partner identity provider.

```
"PartnerName": "https://componentspace-dev-ed.my.salesforce.com"
```

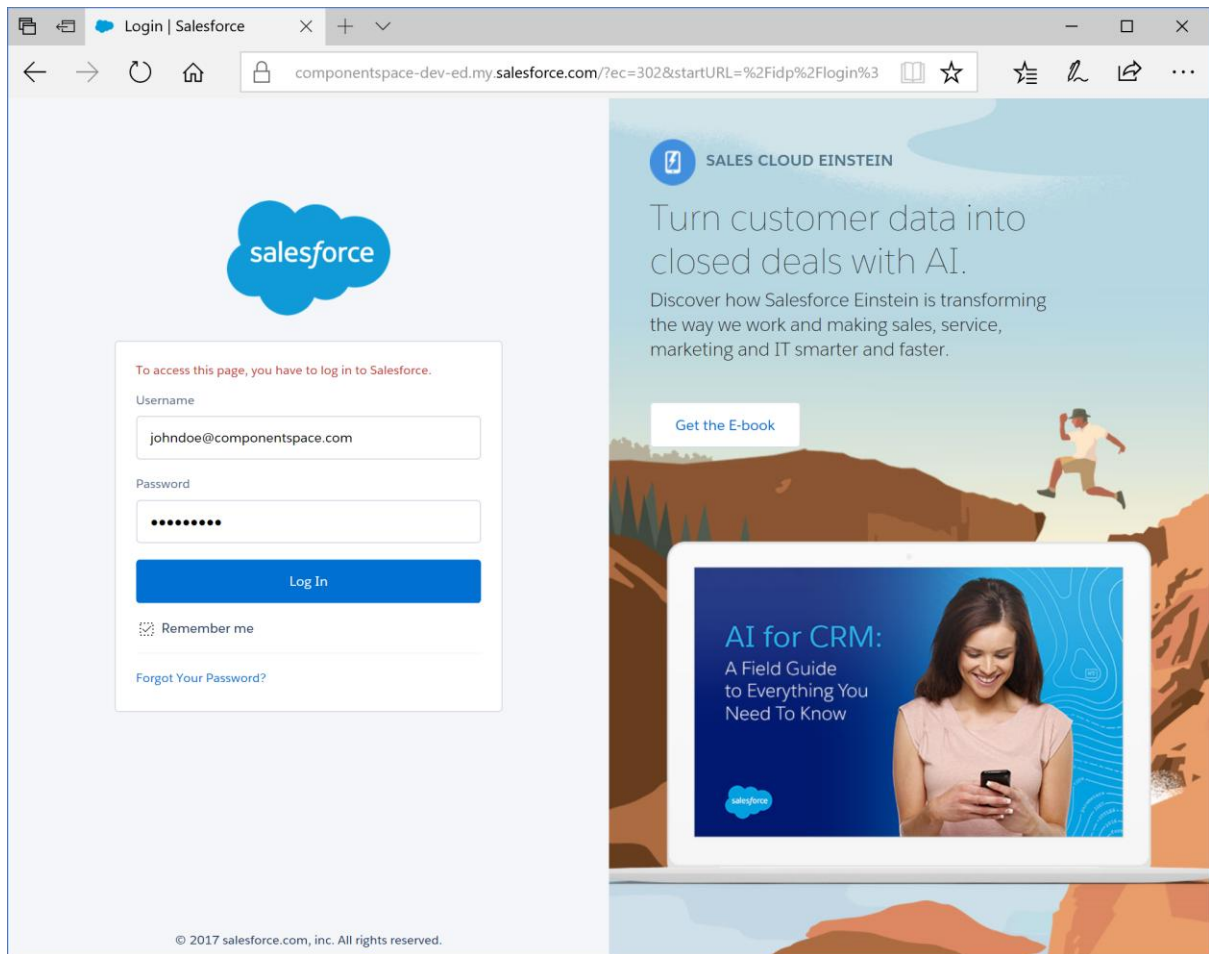
SP-Initiated SSO

Browse to the example service provider and click the button to SSO to the identity provider.

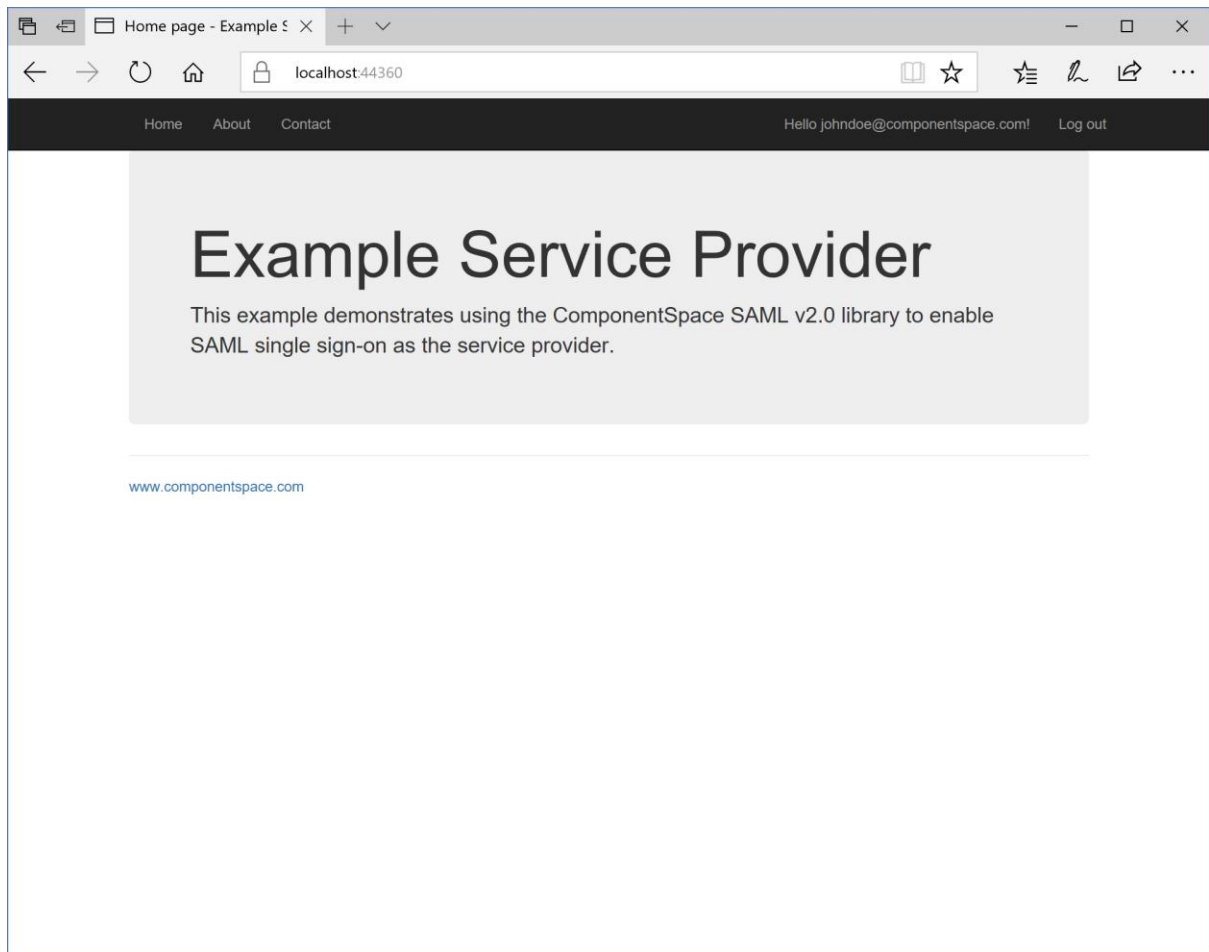


Log into Salesforce.

ComponentSpace SAML for ASP.NET Core Salesforce Identity Provider Integration Guide



The user is automatically logged in at the service provider.



IdP-Initiated SSO

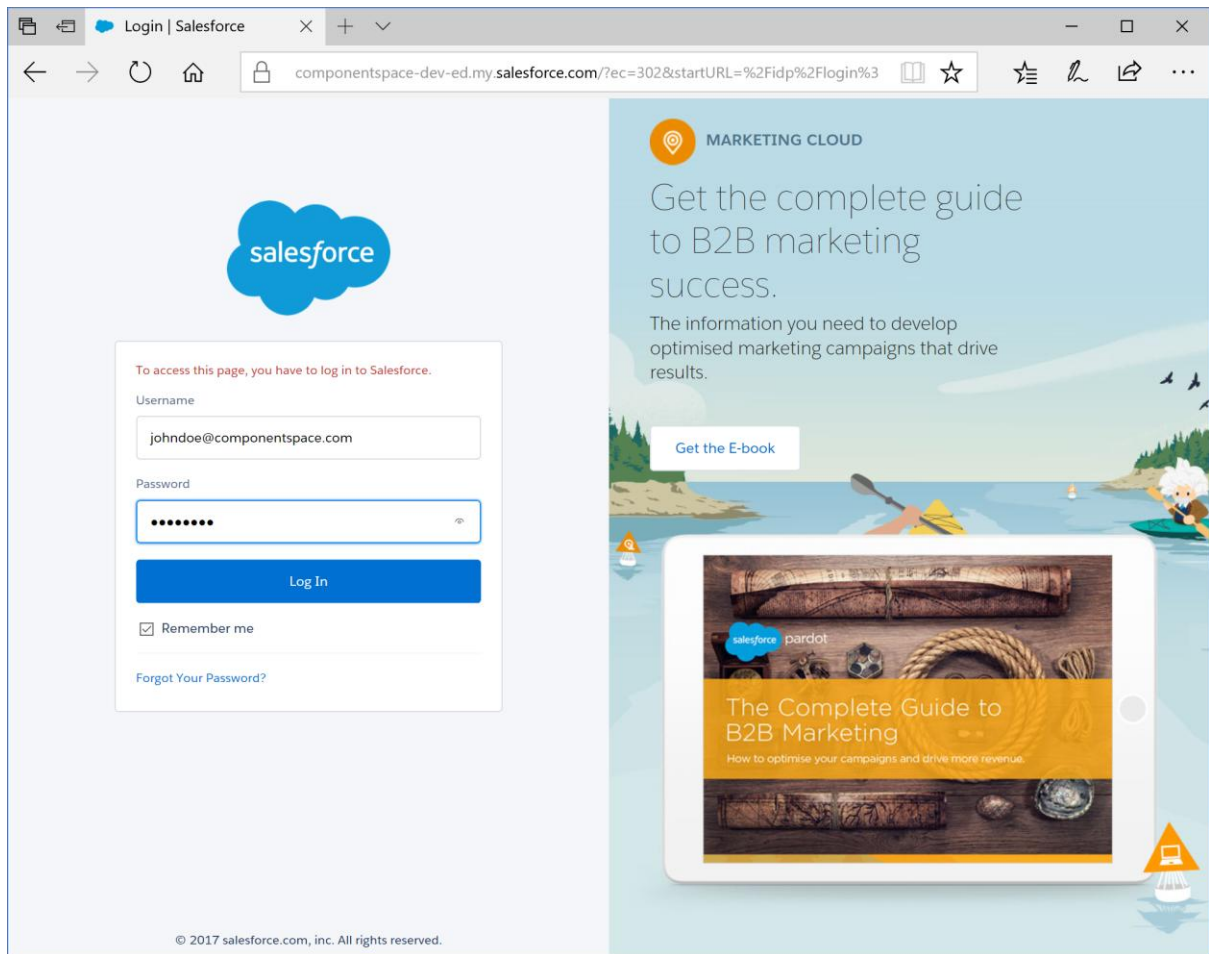
Browse to the URL for IdP-initiated SSO and login.

For example:

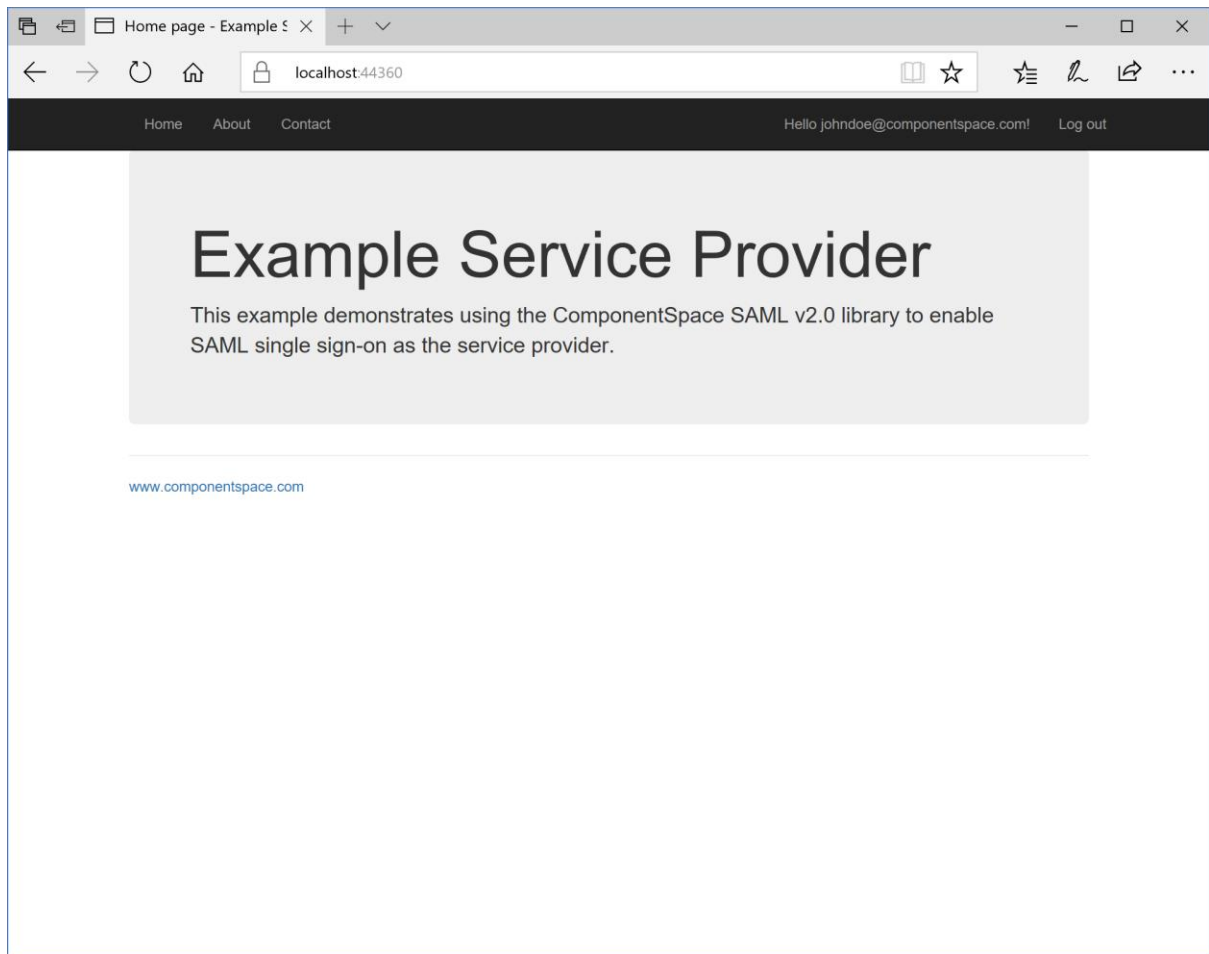
<https://componentspace-dev-ed.my.salesforce.com/idp/login?app=0sp90000000000wN>

Alternatively, select the connect app from the app launcher.

ComponentSpace SAML for ASP.NET Core Salesforce Identity Provider Integration Guide



The user is automatically logged in at the service provider.



SAML Logout

SP-initiated logout returns the user to the Salesforce login page and no logout response is returned to the service provider.

Logging out at Salesforce (i.e. IdP-initiated logout) does not send a logout request to the service provider.

These are limitations in Salesforce and the user should close the browser to complete logout.