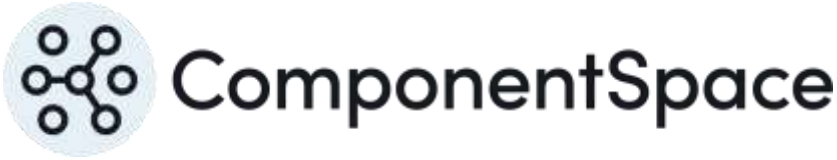


ComponentSpace
SAML for ASP.NET Core
Salesforce
Identity Provider
Integration Guide

www.componentspace.com

Contents

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

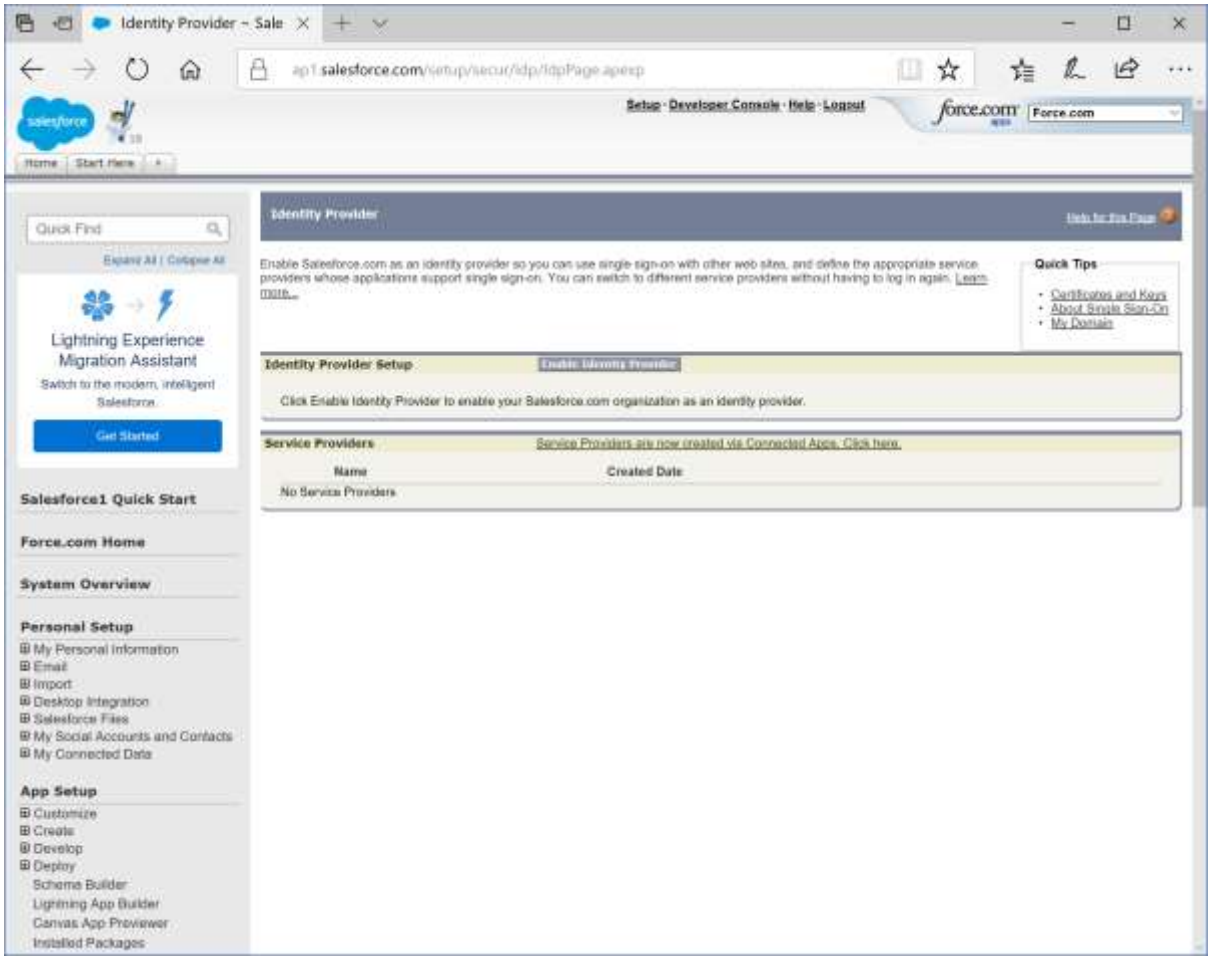
Enabling the Identity Provider

Log into Salesforce as an administrator.

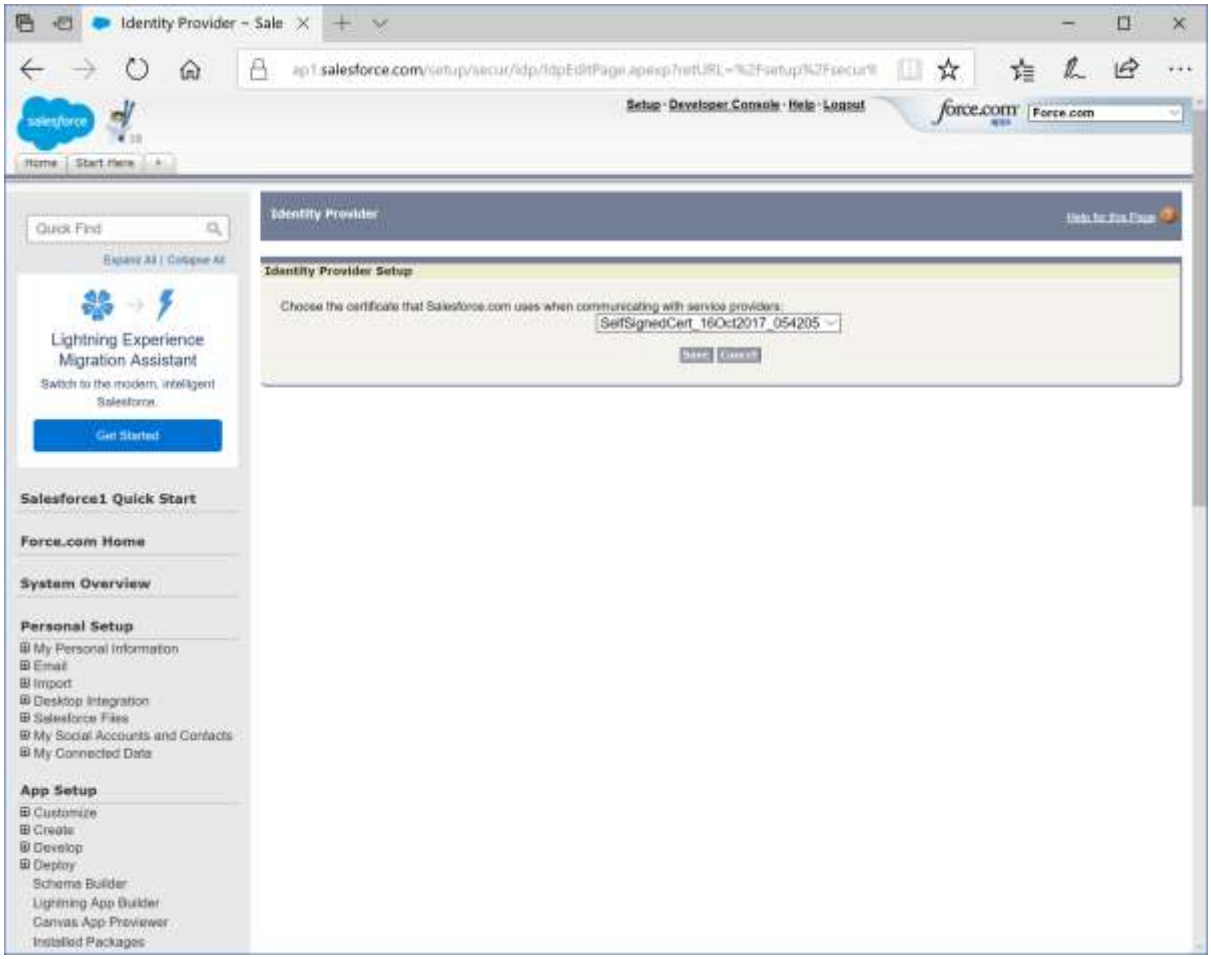
https://login.salesforce.com

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

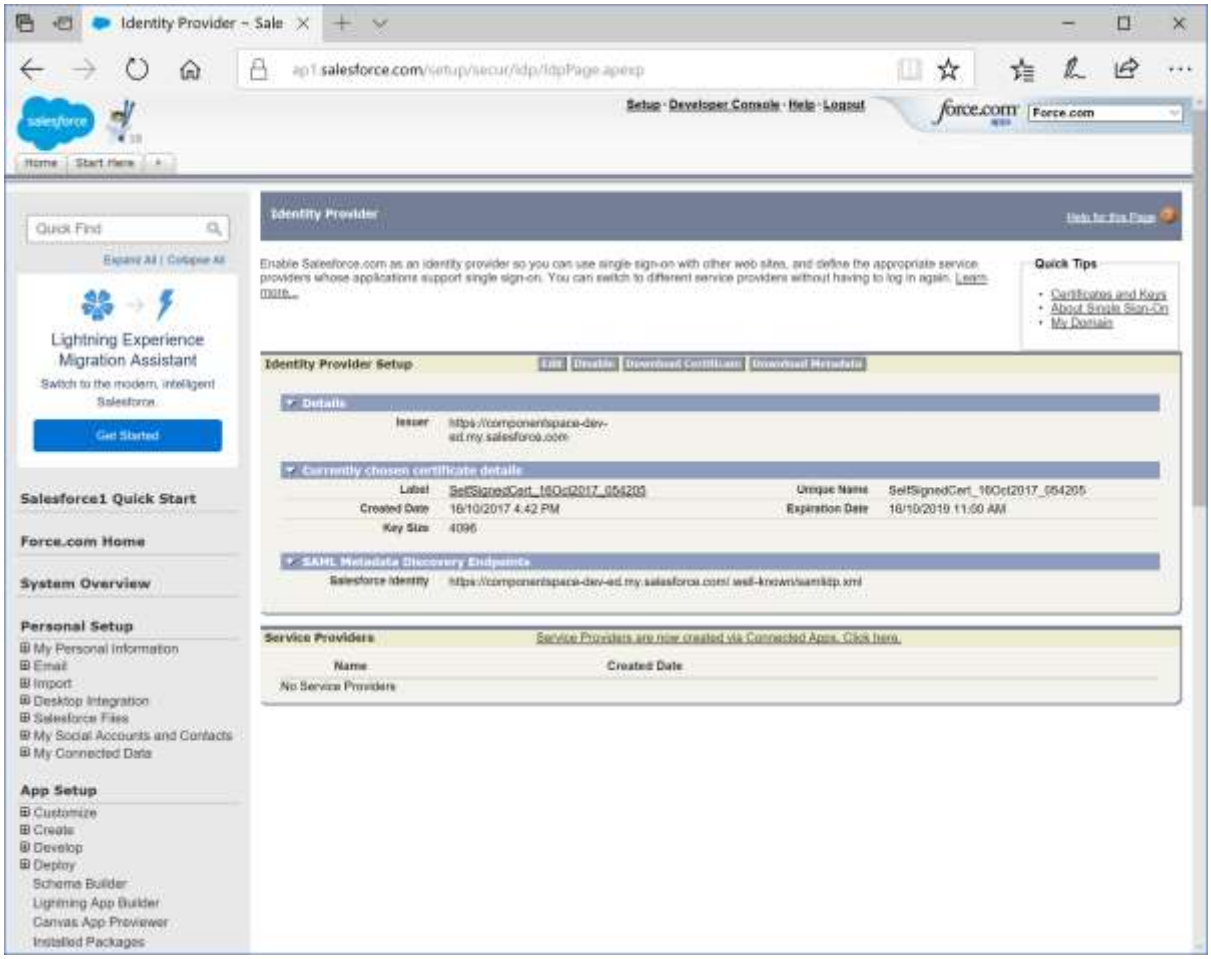
Enable the identity provider.



Select a Salesforce certificate to use.

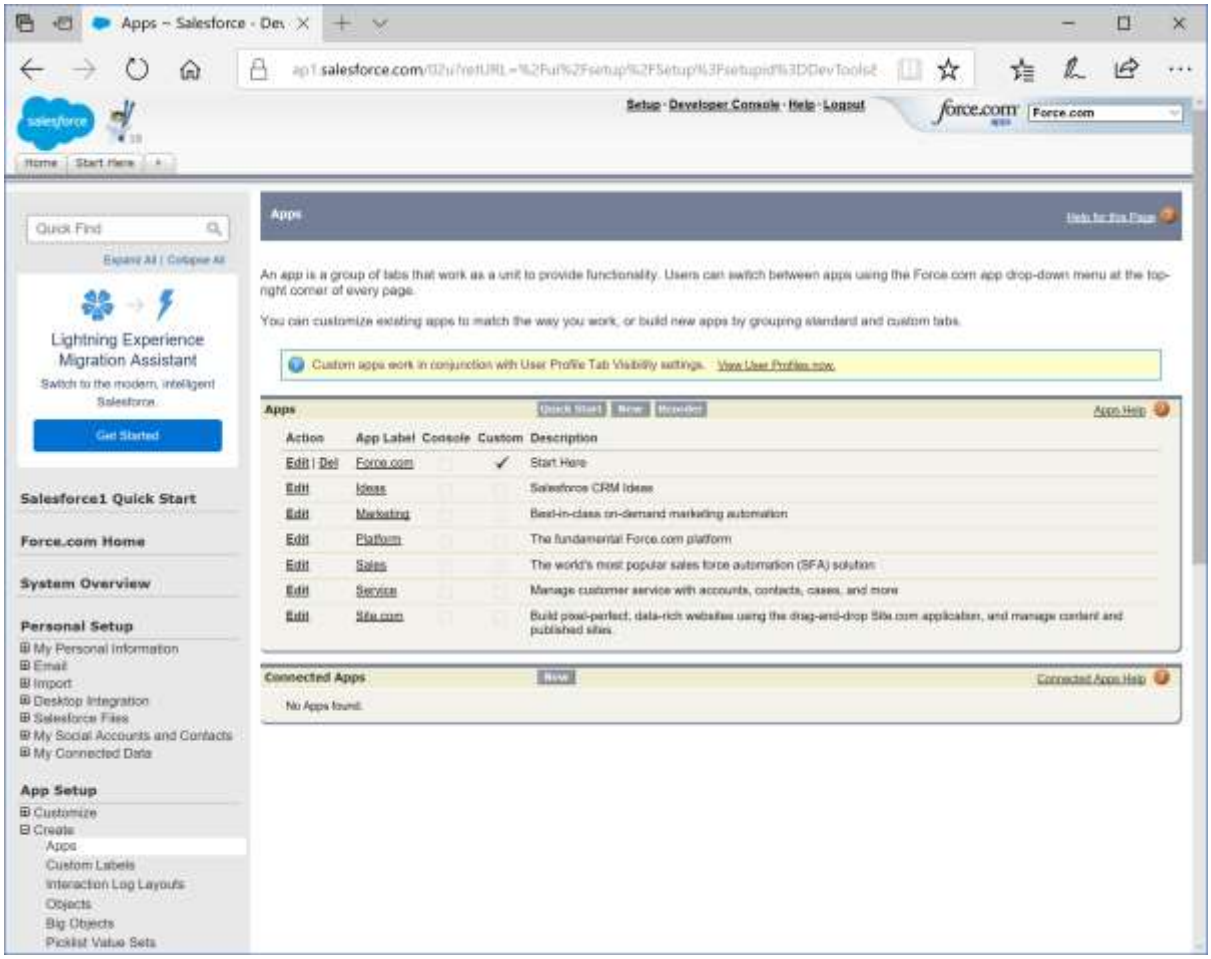


Download the metadata. This is used to configure the service provider.

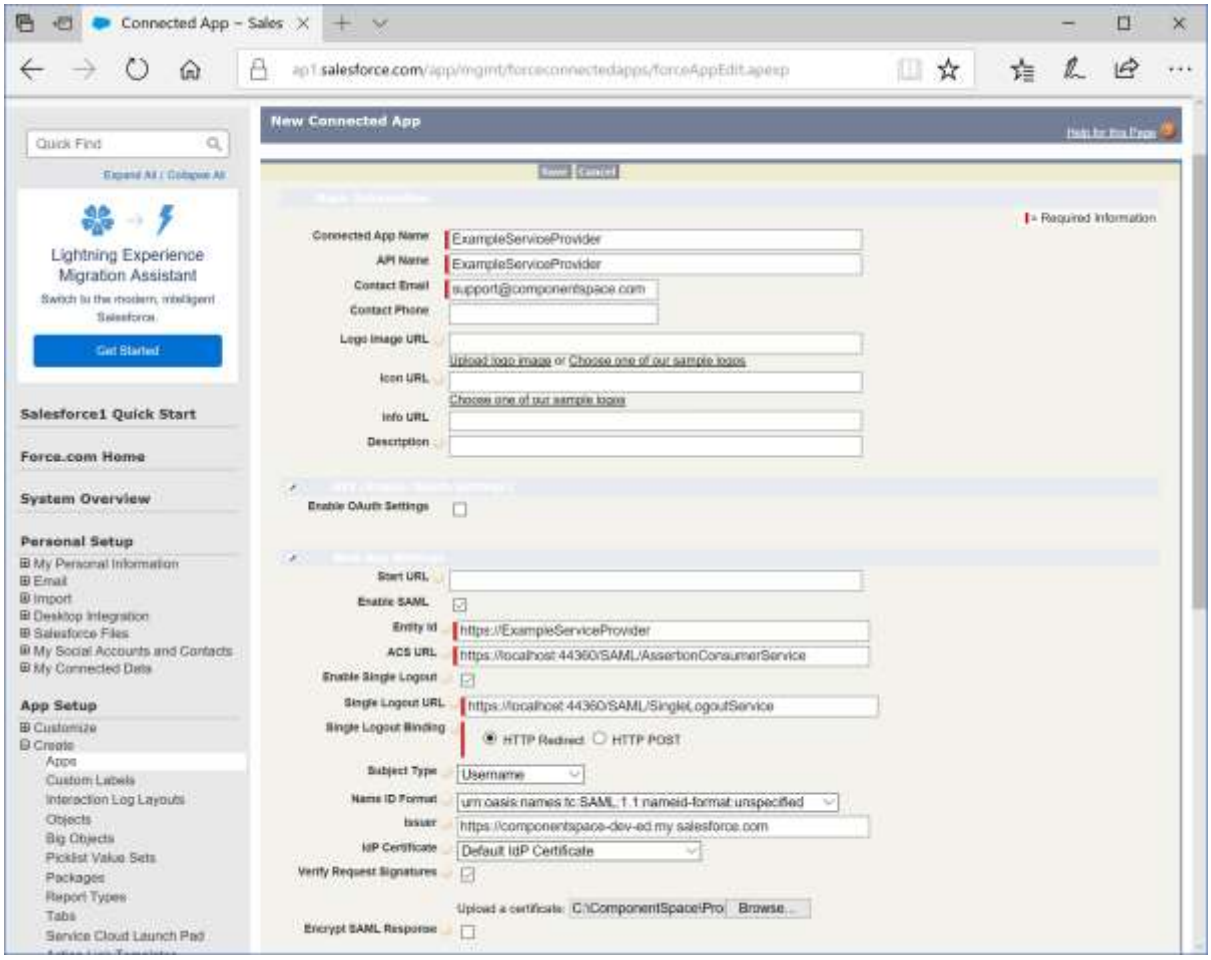


Creating a Connected App

Select Setup > App Setup > Create > Apps.



Click new to create a connected app.



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

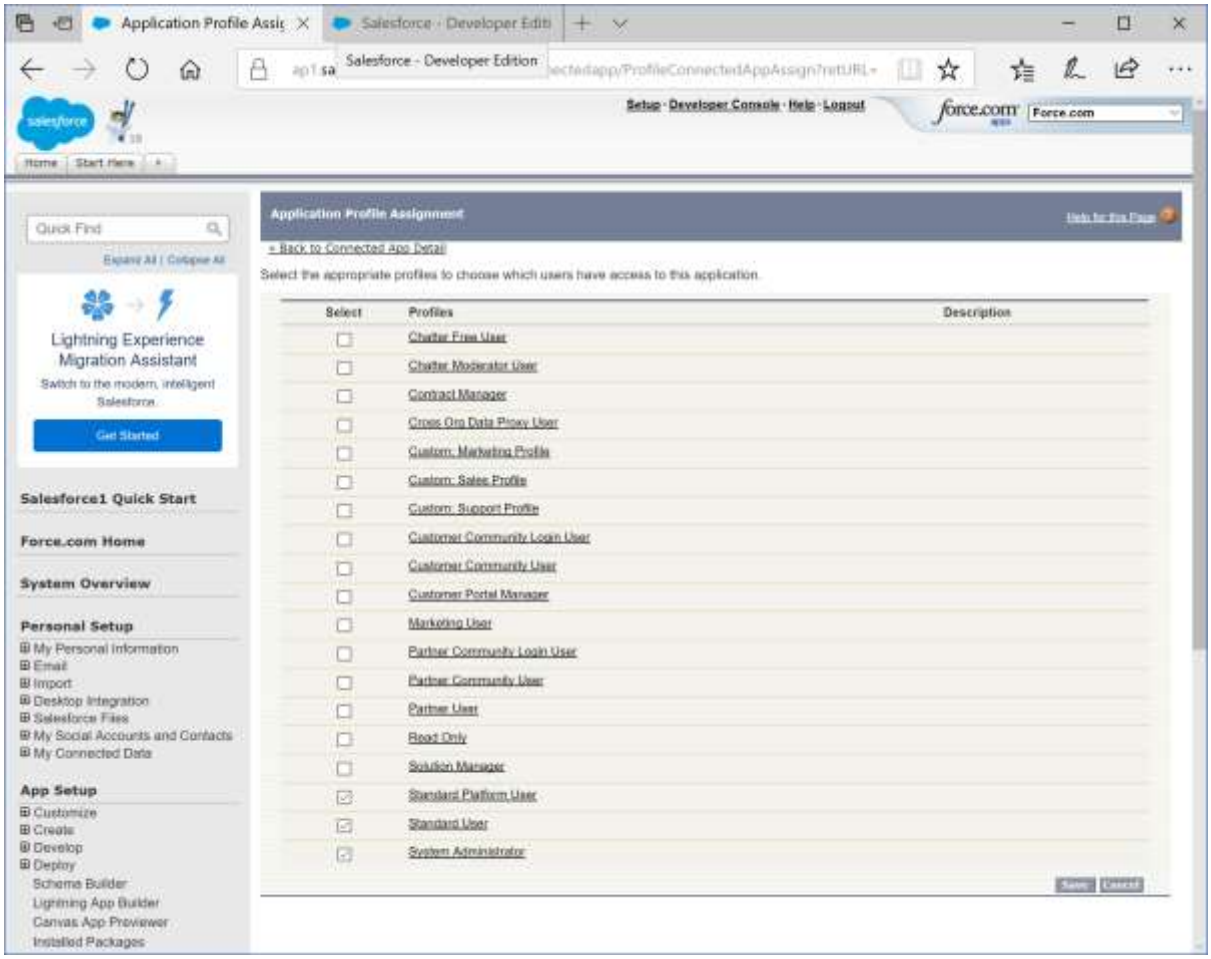
SAML authn request are signed so the service provider's certificate is uploaded.

For example:

sp.cer

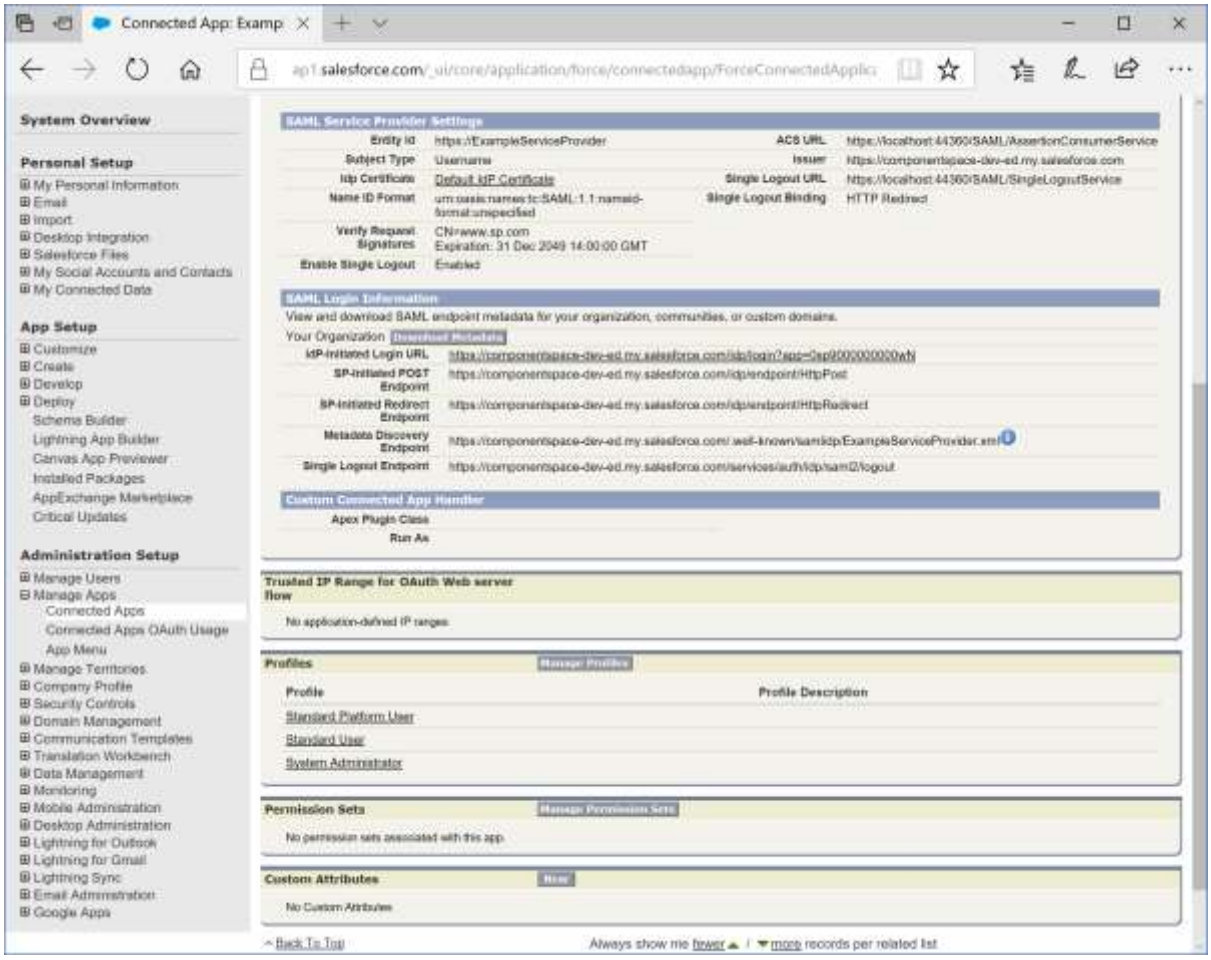
Click Manage > Manage Profiles.

Permit users to access the connected app by assigning profiles.



Review the connected app's configuration.

Note the URL for IdP-initiated SSO.



Service Provider Configuration

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

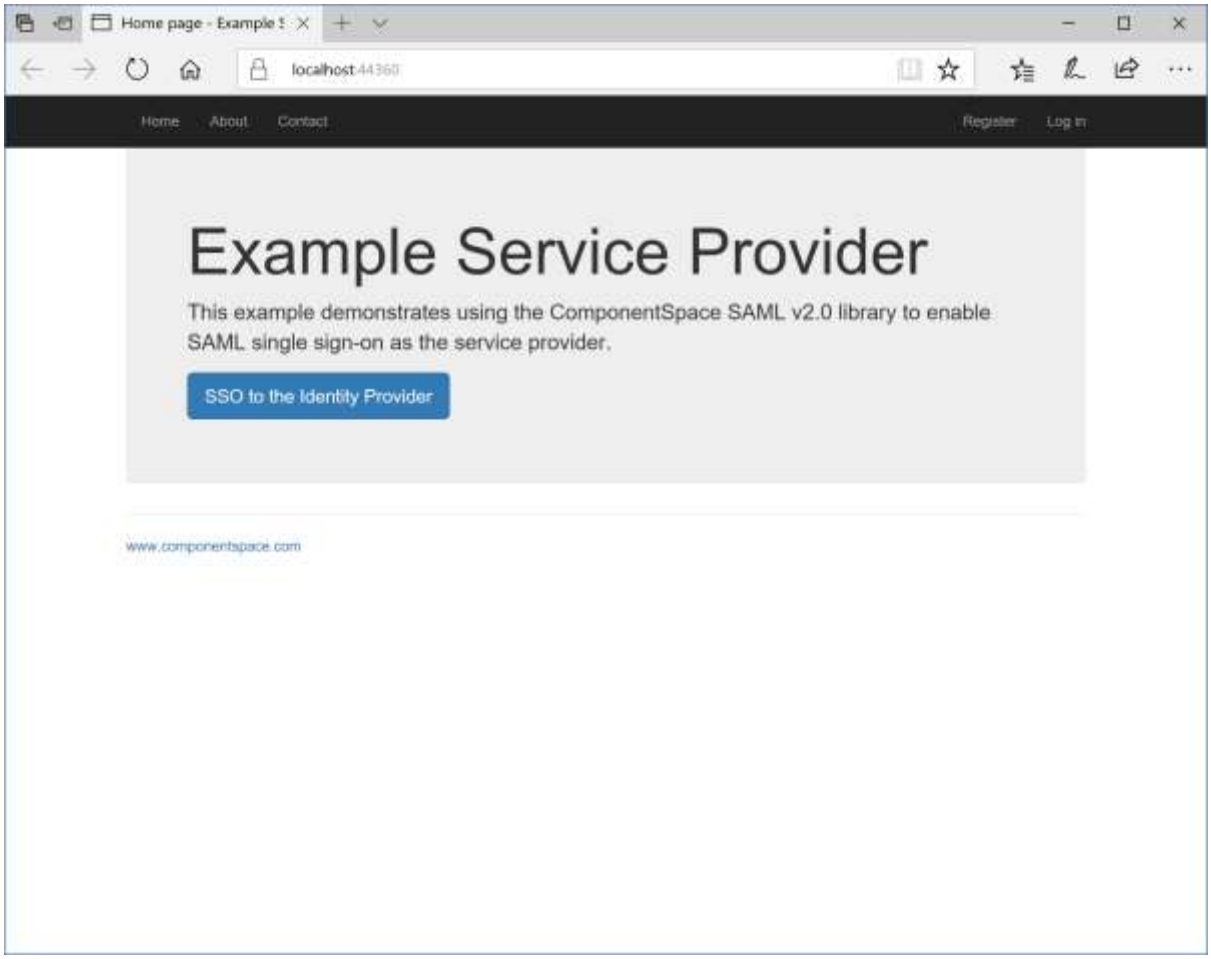
```
{
 "Name": "https://componentspace-dev-ed.my.salesforce.com",
 "Description": "Salesforce",
 "SignAuthnRequest": true,
 "SingleSignOnServiceUrl": "https://componentspace-dev-
ed.my.salesforce.com/idp/endpoint/HttpRedirect",
 "SingleLogoutServiceUrl": "https://componentspace-dev-
ed.my.salesforce.com/services/auth/idp/saml2/logout",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

Ensure the PartnerName specifies the correct partner identity provider.

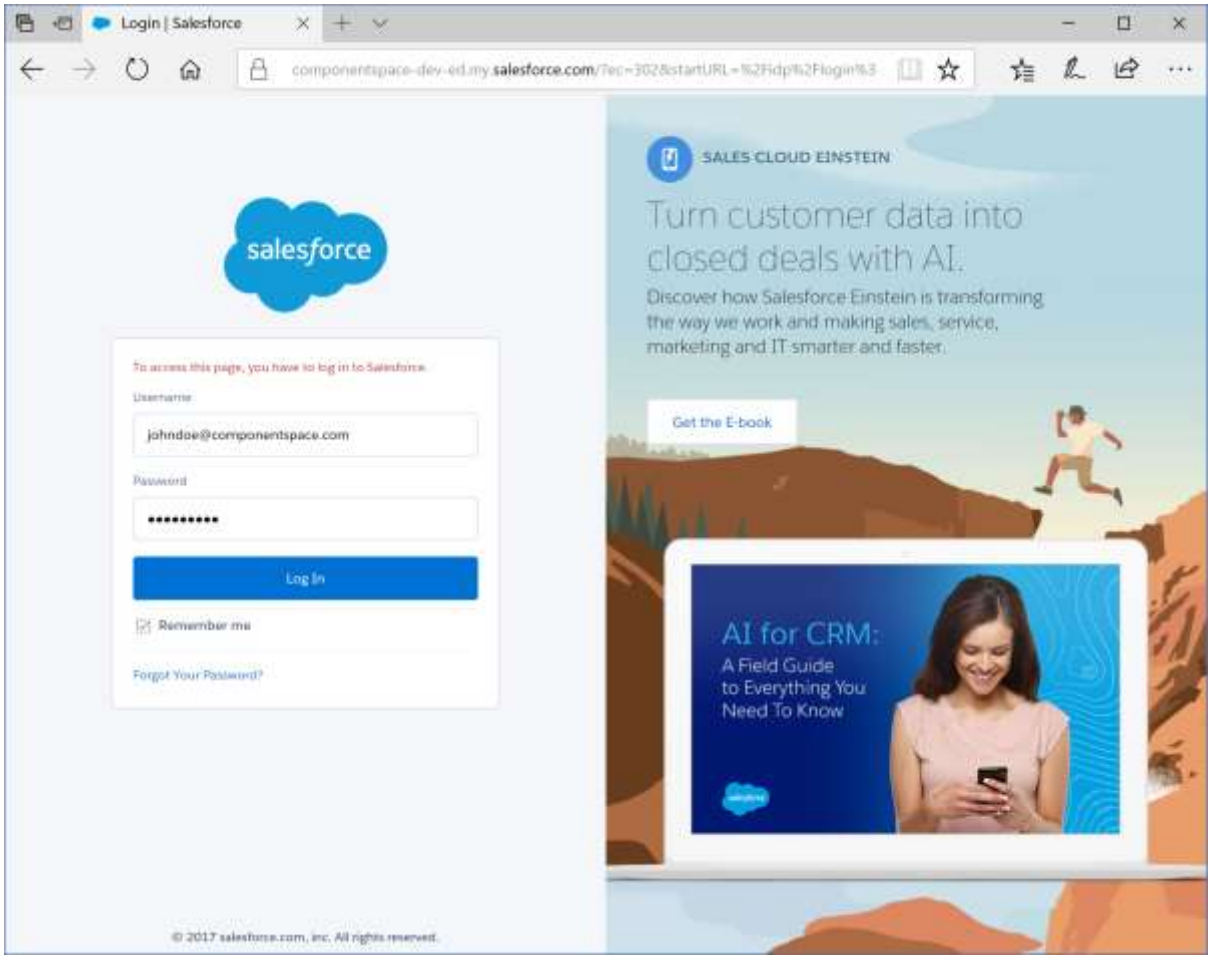
```
"PartnerName": "https://componentspace-dev-ed.my.salesforce.com"
```

SP-Initiated SSO

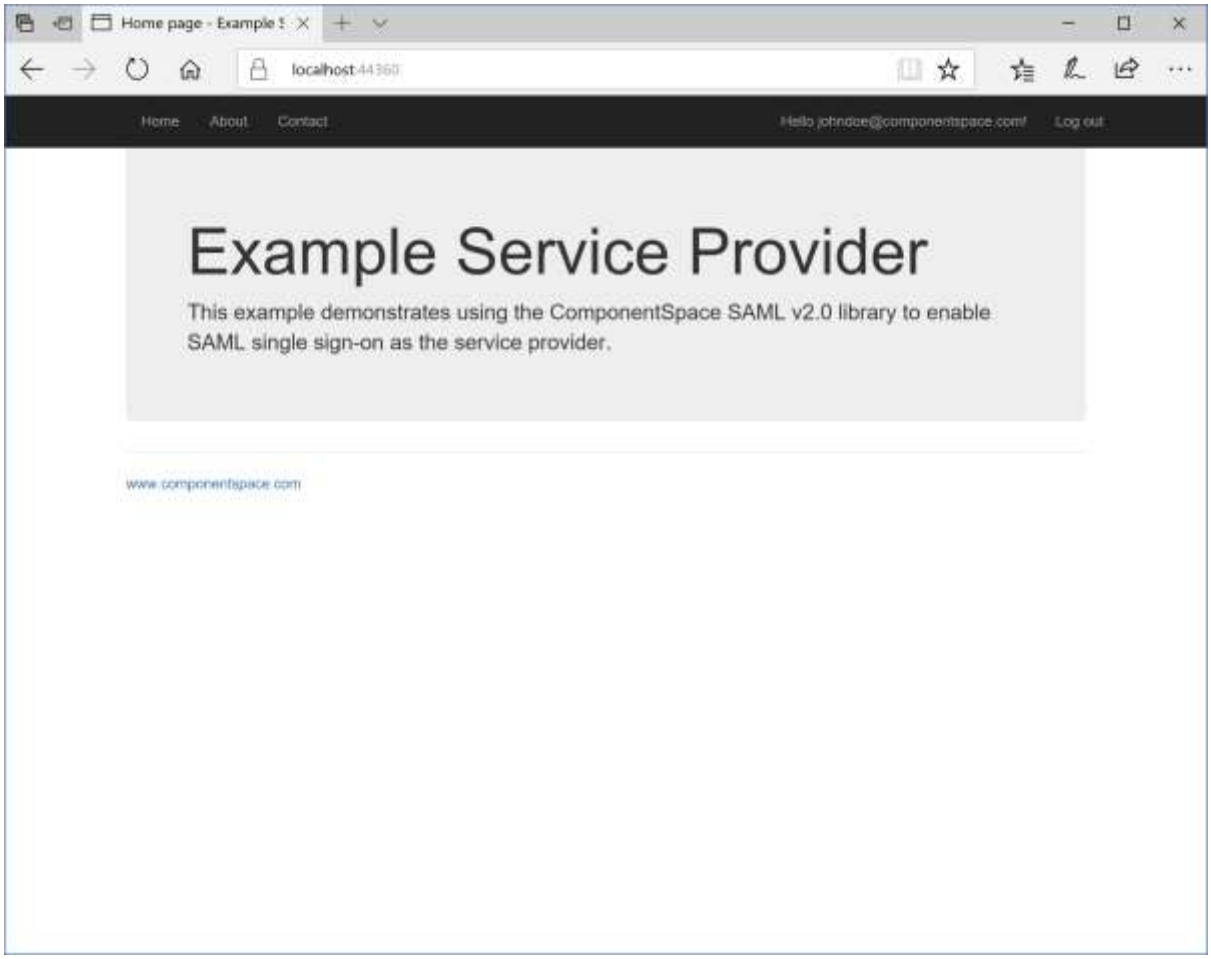
Browse to the example service provider and click the button to SSO to the identity provider.



Log into Salesforce.



The user is automatically logged in at the service provider.



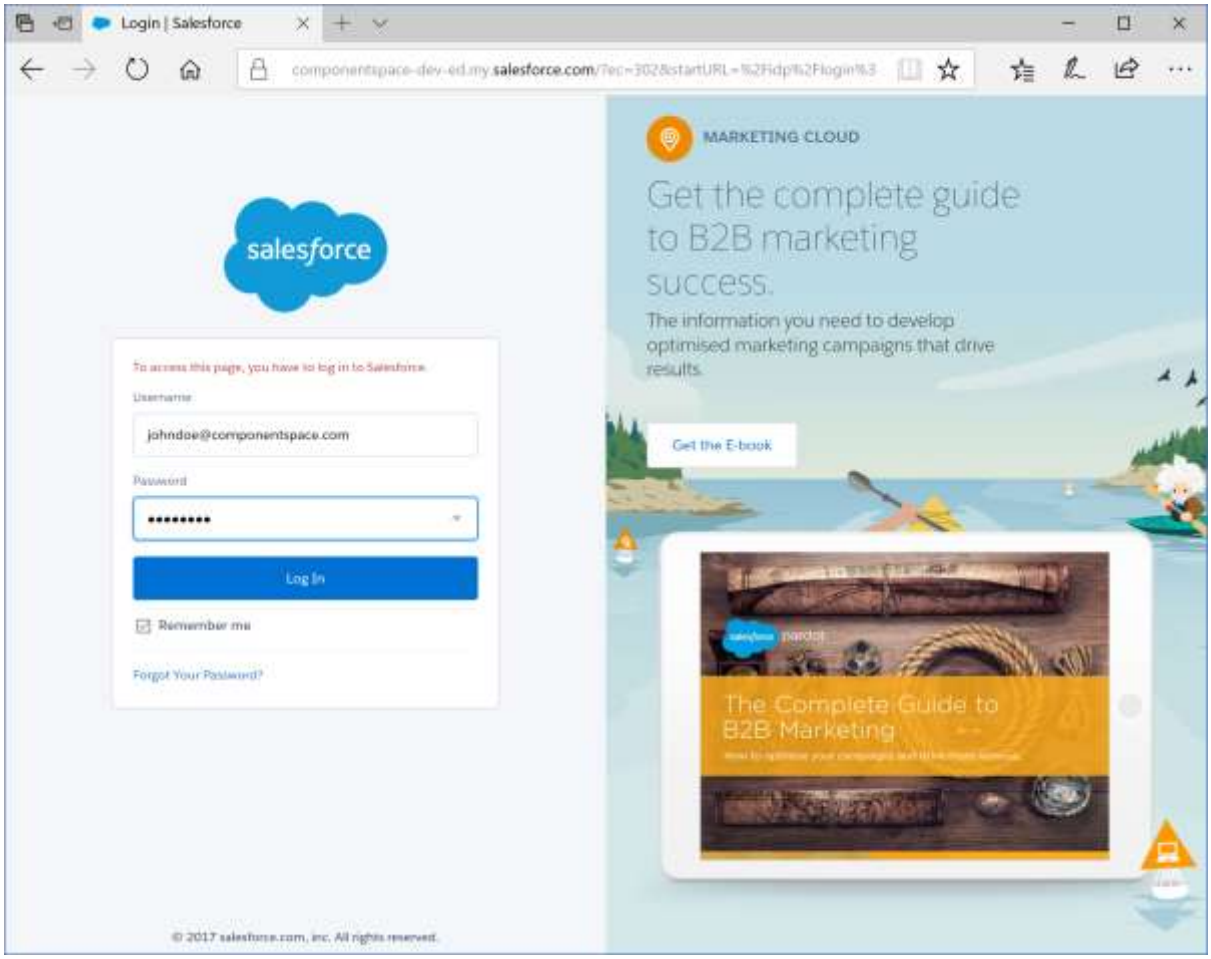
IdP-Initiated SSO

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

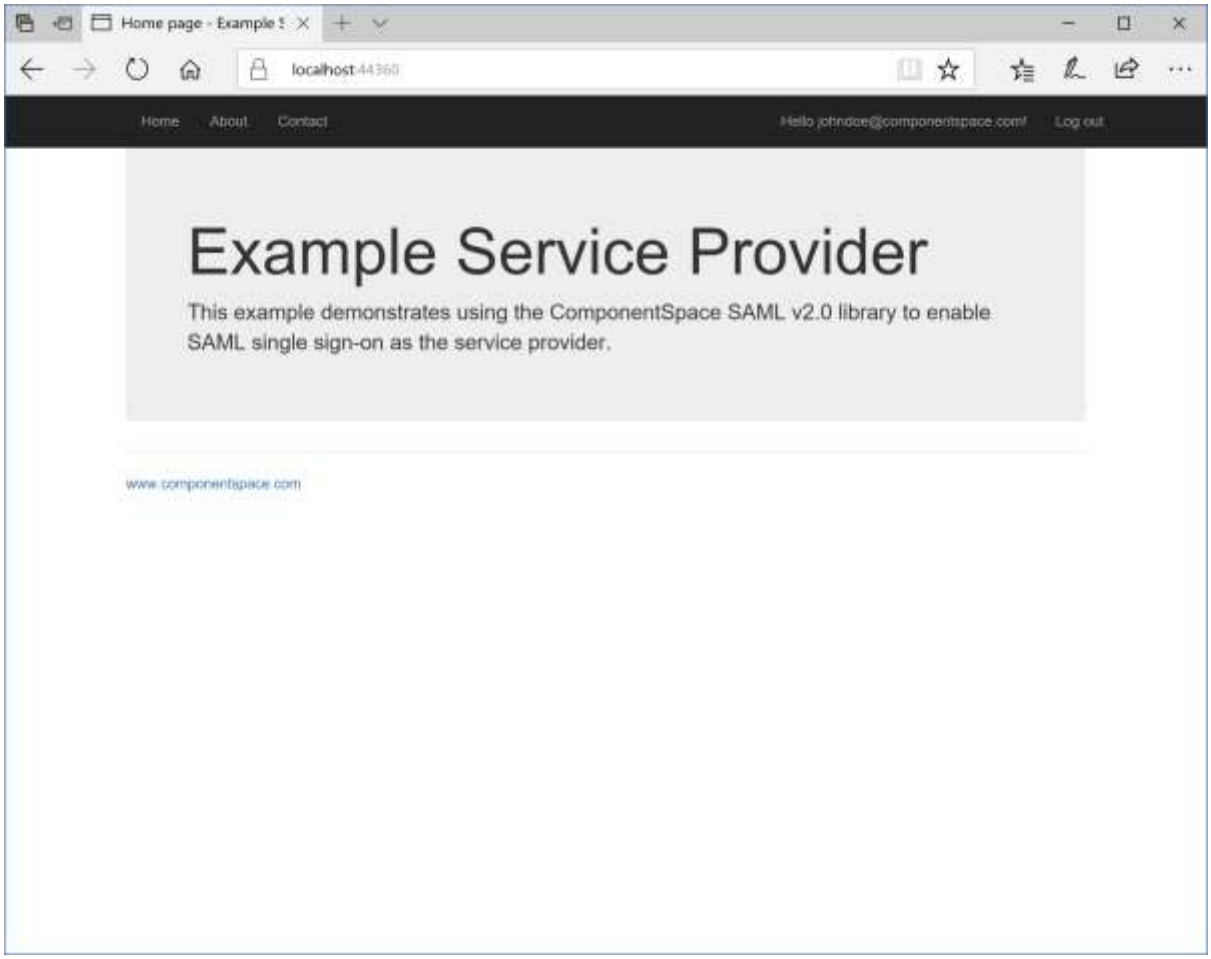
For example:

https://componentspace-dev-ed.my.salesforce.com/idp/login?app=0sp9000000000wN

Alternatively, select the connect app from the app launcher.



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.