

ComponentSpace SAML for ASP.NET Core IdentityServer Integration Guide

Contents

Introduction.....	1
Adding SAML Support.....	1
Service Provider Configuration	2
Application Startup	2
Identity Provider Configuration	3
SP-Initiated SSO	3
IdP-Initiated SSO	7
SAML Logout.....	7

Introduction

IdentityServer doesn't natively support SAML SSO but it is extensible.

This document describes how to add SAML support to IdentityServer acting as a service provider.

The reader is assumed to have an existing IdentityServer project.

For information on IdentityServer, refer to the following documentation.

<https://identityserver4.readthedocs.io/en/latest/>

For information on building, configuring and running IdentityServer, refer to the following documentation.

http://docs.identityserver.io/en/latest/quickstarts/0_overview.html

IdentityServer supports users signing in using external identity providers.

IdentityServer is the SAML service provider and the external providers are the SAML identity providers. The application authenticating to IdentityServer may use any available protocol (e.g. OpenID Connect).

The following sections described how to enable sign-on using external SAML identity providers.

Adding SAML Support

Add the ComponentSpace.Saml2 NuGet package to the IdentityServer project.

**ComponentSpace.Saml2** by ComponentSpace
Enable SAML v2.0 identity provider (IdP) and service provider (SP) single sign-on (SSO) in ASP.NET...

**IdentityServer4** by Brock Allen,Dominick Baier
OpenID Connect and OAuth 2.0 Framework for ASP.NET Core

**Microsoft.AspNetCore.Authentication.Google** by Microsoft
ASP.NET Core contains middleware to support Google's OpenId and OAuth 2.0 authentication wor...

**Serilog.AspNetCore** by Microsoft,Serilog Contributors
Serilog support for ASP.NET Core logging

Add the Certificates folder to the IdentityServer project. The following certificate files may be copied from the ExampleServiceProvider project.

- sp.pfx

- idp.cer

Service Provider Configuration

In IdentityServer's appsettings.json, include the SAML configuration.

```
"SAML": {
  "$schema": "https://www.componentspace.com/schemas/saml-config-schema-v1.0.json",
  "Configurations": [
    {
      "LocalServiceProviderConfiguration": {
        "Name": "https://IdentityServer",
        "Description": "Identity Server",
        "AssertionConsumerServiceUrl": "https://localhost:5001/SAML/AssertionConsumerService",
        "SingleLogoutServiceUrl": "https://localhost:5001/SAML/SingleLogoutService",
        "LocalCertificates": [
          {
            "FileName": "certificates/sp.pfx",
            "Password": "password"
          }
        ]
      },
      "PartnerIdentityProviderConfigurations": [
        {
          "Name": "https://ExampleIdentityProvider",
          "Description": "Example Identity Provider",
          "SignAuthnRequest": true,
          "SignLogoutRequest": true,
          "SignLogoutResponse": true,
          "SingleSignOnServiceUrl": "https://localhost:44313/SAML/SingleSignOnService",
          "SingleLogoutServiceUrl": "https://localhost:44313/SAML/SingleLogoutService",
          "PartnerCertificates": [
            {
              "FileName": "certificates/idp.cer"
            }
          ]
        }
      ]
    }
  ]
}
```

For information on SAML configuration, refer to the SAML for ASP.NET Core Configuration Guide.

Application Startup

In the ConfigureServices method in IdentityServer's Startup class, add the following.

```
services.Configure<CookiePolicyOptions>(options =>
{
  // SameSiteMode.None is required to support SAML SSO.
```

```
options.MinimumSameSitePolicy = SameSiteMode.None;
});

// Add SAML SSO services.
services.AddSaml(Configuration.GetSection("SAML"));

// Add SAML authentication services.
services.AddAuthentication().AddSaml(options =>
{
    options.SignInScheme = IdentityServerConstants.ExternalCookieAuthenticationScheme;
});
```

For more information, refer to the SAML for ASP.NET Core Developer Guide.

Identity Provider Configuration

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

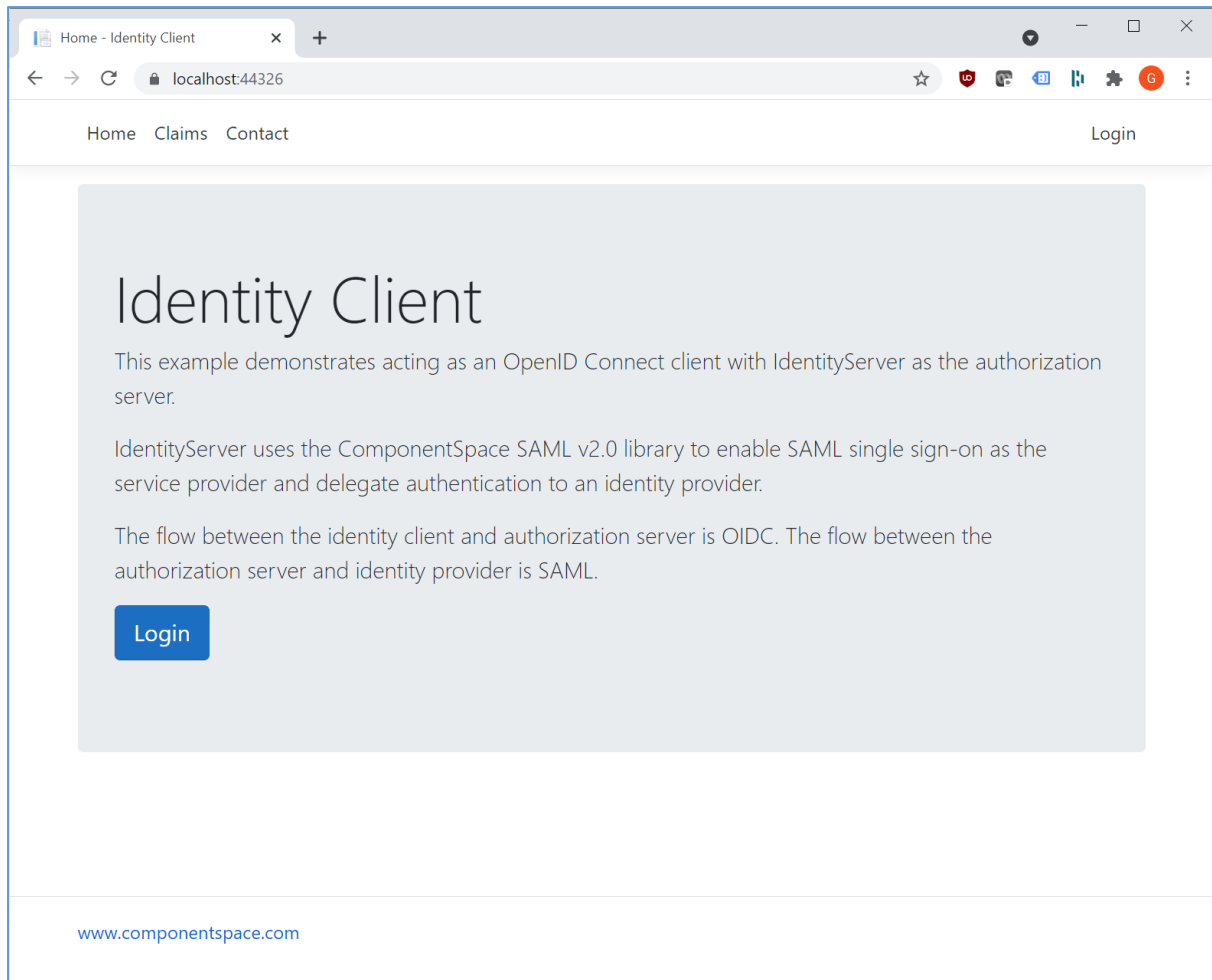
```
{
  "Name": "https://IdentityServer",
  "Description": "Identity Server",
  "WantAuthnRequestSigned": true,
  "SignSamlResponse": true,
  "SignLogoutRequest": true,
  "SignLogoutResponse": true,
  "AssertionConsumerServiceUrl": "https://localhost:5001/SAML/AssertionConsumerService",
  "SingleLogoutServiceUrl": "https://localhost:5001/SAML/SingleLogoutService",
  "PartnerCertificates": [
    {
      "FileName": "certificates/sp.cer"
    }
  ]
}
```

SP-Initiated SSO

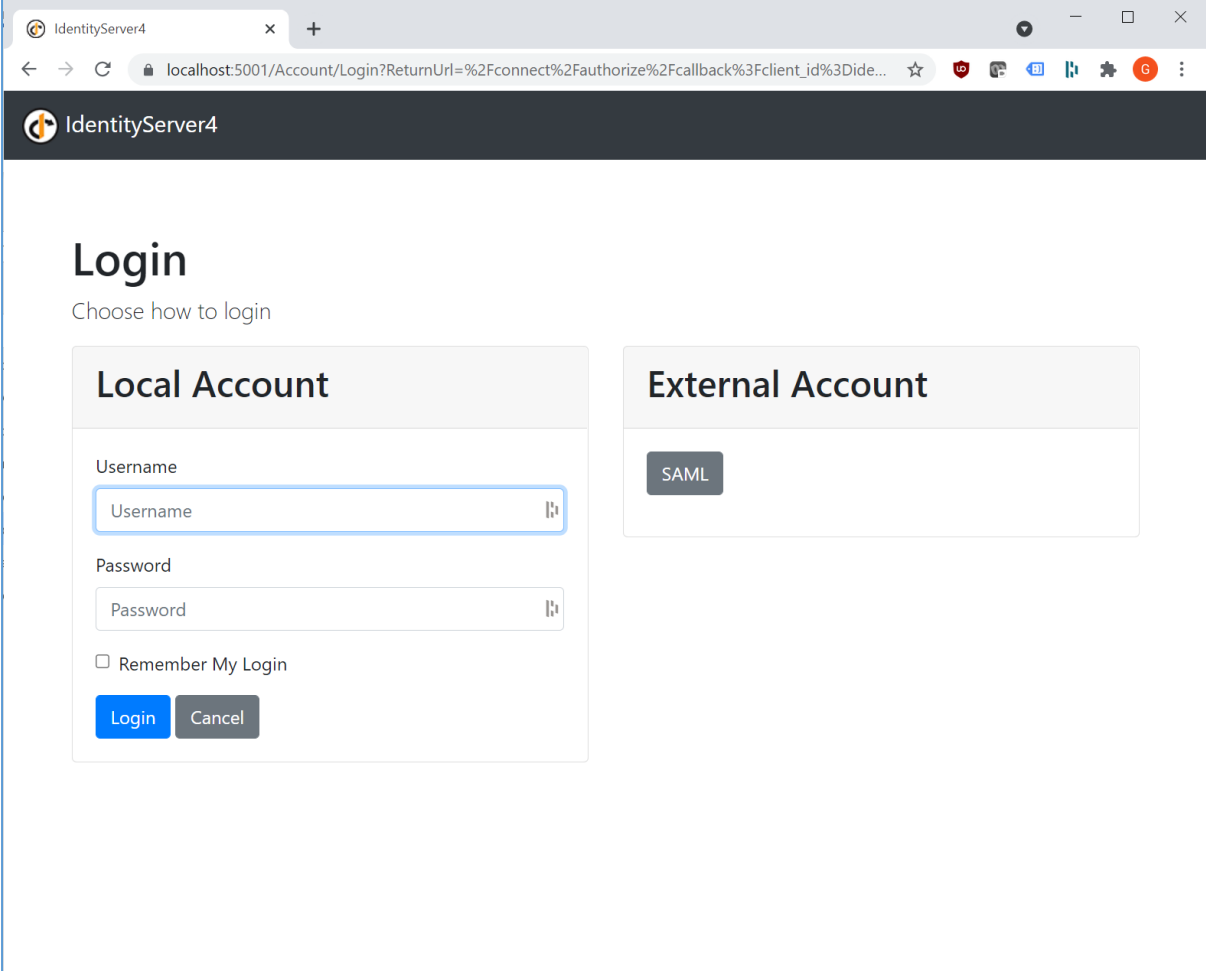
The reader is assumed to have an application that authenticates to IdentityServer using OpenID Connect or some other protocol.

For more information, refer to the IdentityServer documentation.

Browse to the application and initiate login.



At the IdentityServer login page, click the SAML external login button.



The screenshot shows a web browser window with the title 'IdentityServer4'. The address bar displays 'localhost:5001/Account/Login?ReturnUrl=%2Fconnect%2Fauthorize%2Fcallback%3Fclient_id%3Dide...'. The page header features the IdentityServer4 logo and name. The main content area is titled 'Login' with the subtitle 'Choose how to login'. There are two primary login options: 'Local Account' and 'External Account'. The 'Local Account' section includes input fields for 'Username' and 'Password', a 'Remember My Login' checkbox, and 'Login' and 'Cancel' buttons. The 'External Account' section contains a single 'SAML' button.

IdentityServer4

Login

Choose how to login

Local Account

Username

Password

☐ Remember My Login

Login Cancel

External Account

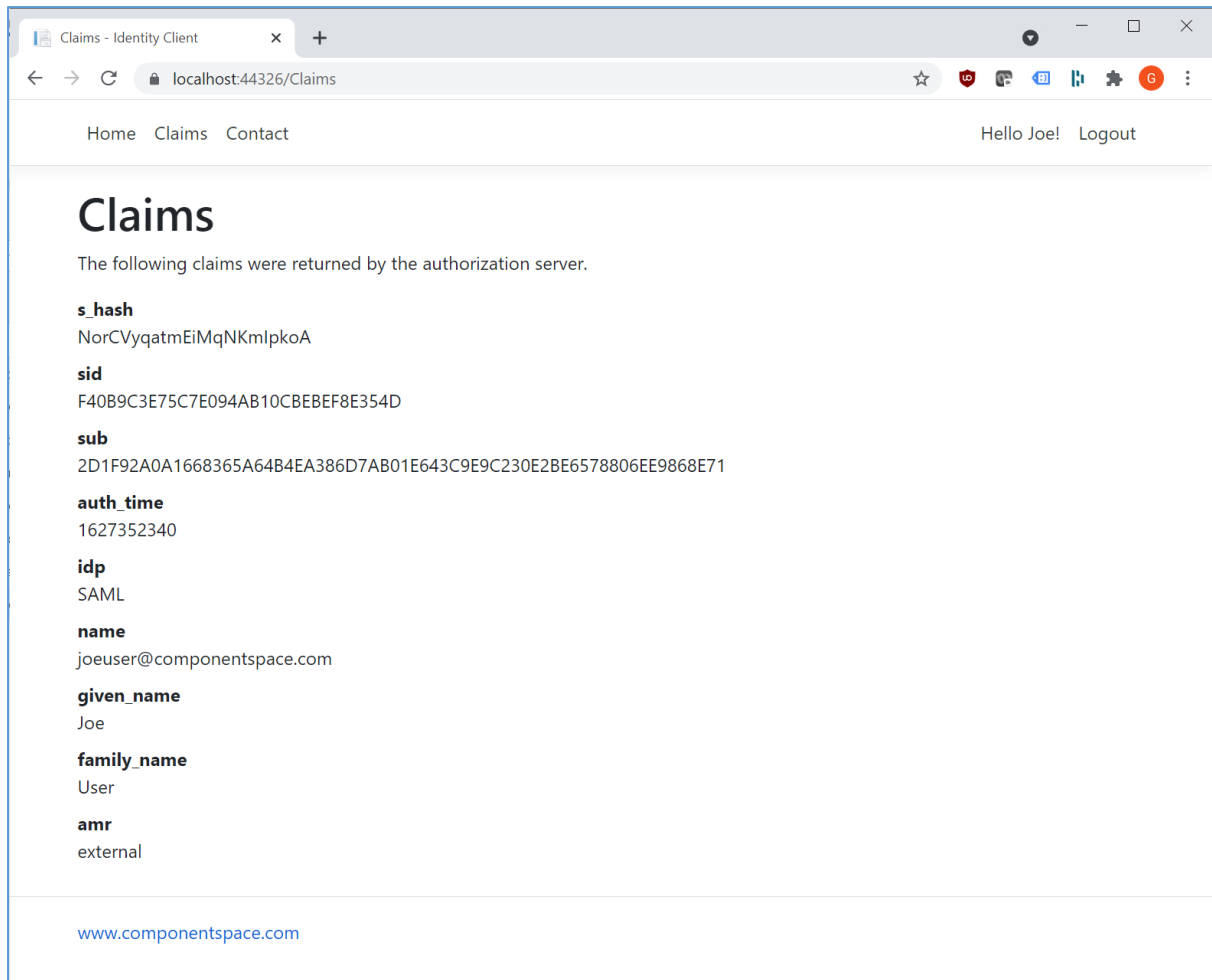
SAML

Login at the SAML identity provider.

The screenshot shows a web browser window with the address bar displaying `localhost:44313/Identity/Account/Login?ReturnUrl=%2FSaml%2FSingleSignOnServiceCompletion`. The page title is "Log in - Example Identity Provider". The navigation bar includes links for Home, About, Contact, Register, and Login. The main heading is "Log in at the Identity Provider". Below this, there are two columns: "Use a local account to log in." and "Use another service to log in." The local account section contains fields for Email (joeuser@componentspace.com) and Password (masked with dots), a "Remember me?" checkbox, a "Log in" button, and links for "Forgot your password?" and "Register as a new user". The external services section states: "There are no external authentication services configured. See [this article](#) for details on setting up this ASP.NET application to support logging in via external services." The footer displays the website URL `www.componentspace.com`.

Depending on how IdentityServer is configured, you may be prompted whether to allow the requested permissions.

The user is automatically logged in at the service provider.



IdP-Initiated SSO

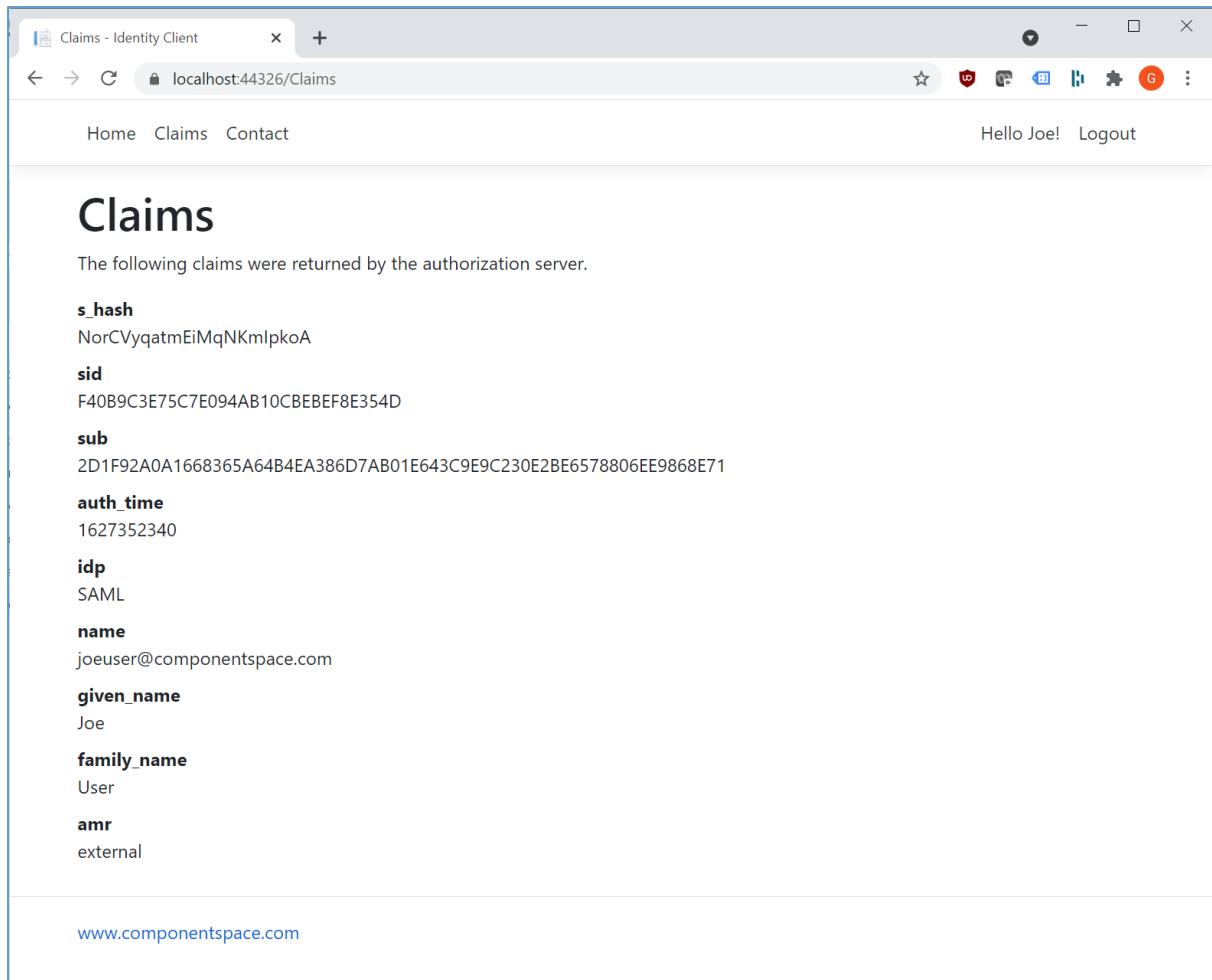
IdP-initiated SSO is not supported by IdentityServer.

SAML Logout

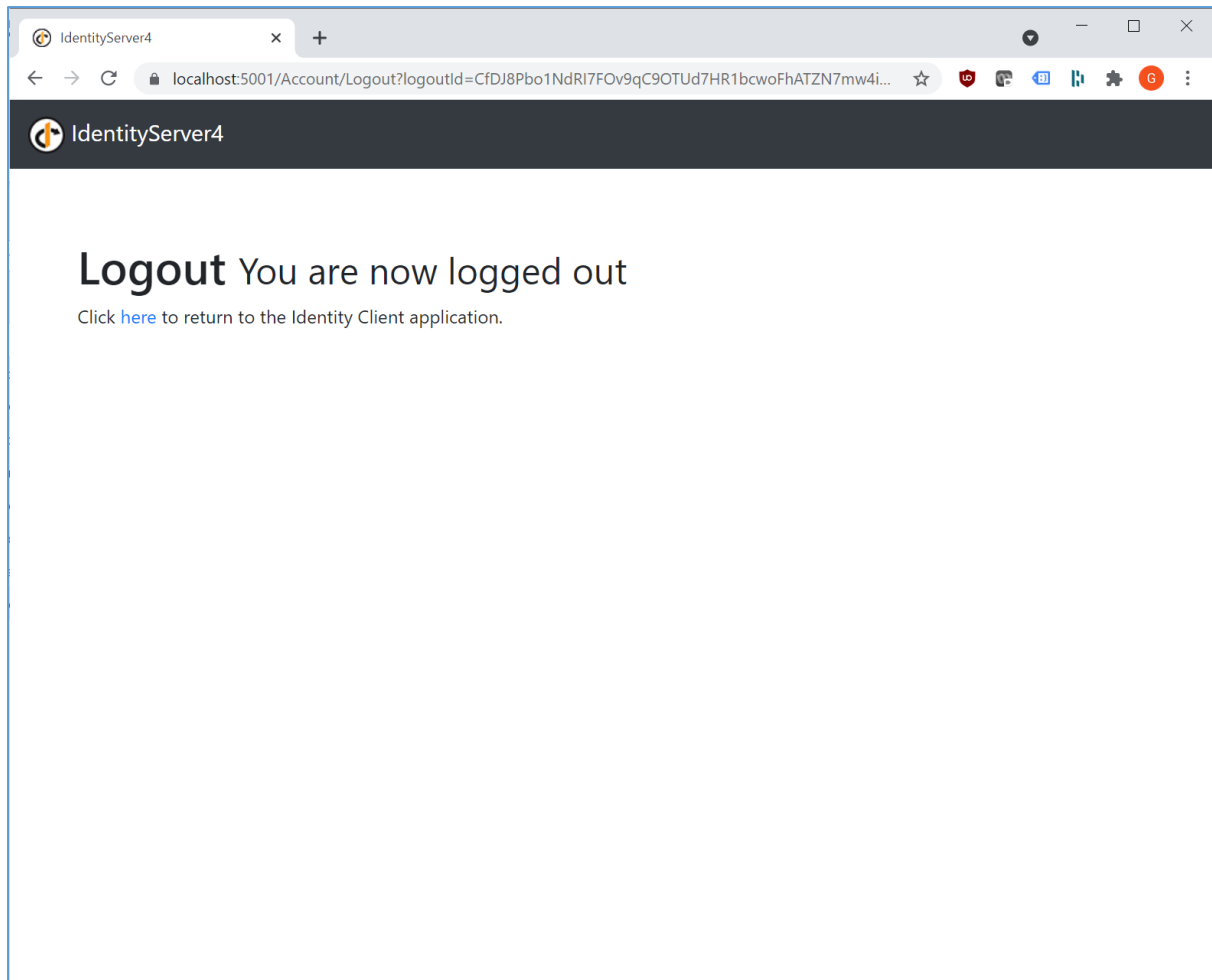
IdP-initiated SAML logout is not supported by IdentityServer.

SP-initiated SAML logout is supported.

Initiate logout at the application.



You are logged out at IdentityServer and the SAML identity provider.



Click the link to return to the application.

