ComponentSpace

SAML for ASP.NET Core

IdentityServer

Integration Guide
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Adding SAML Support</td>
<td>1</td>
</tr>
<tr>
<td>Service Provider Configuration</td>
<td>2</td>
</tr>
<tr>
<td>Application Startup</td>
<td>2</td>
</tr>
<tr>
<td>Identity Provider Configuration</td>
<td>3</td>
</tr>
<tr>
<td>SP-Initiated SSO</td>
<td>3</td>
</tr>
<tr>
<td>IdP-Initiated SSO</td>
<td>7</td>
</tr>
<tr>
<td>SAML Logout</td>
<td>7</td>
</tr>
</tbody>
</table>
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.


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.

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",
         "LocalCertificates": [
            {
               "FileName": "certificates/sp.pfx",
               "Password": "password"
            }
         ]
      },
   },
   "PartnerIdentityProviderConfigurations": [
   {
      "Name": "https://ExampleIdentityProvider",
      "Description": "Example Identity Provider",
      "SignAuthnRequest": true,
      "SignLogoutRequest": true,
      "SignLogoutResponse": true,
      "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.

```csharp
services.Configure<CookiePolicyOptions>(options =>
{
   // SameSiteMode.None is required to support SAML SSO.
   options.MinimumSameSitePolicy = SameSiteMode.None;
});
```
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,
  "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.
Login at the SAML identity provider.
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.
Logout You are now logged out
Click [here](#) to return to the Identity Client application.

Click the link to return to the application.
Identity Client

This example demonstrates acting as an OpenID Connect client with IdentityServer as the authorization server.

IdentityServer uses the ComponentSpace SAML v2.0 library to enable SAML single sign-on as the service provider and delegate authentication to an identity provider.

The flow between the identity client and authorization server is OAuth. The flow between the authorization server and identity provider is SAML.

Login