Integration of Windows IIS Authentication with SAML2

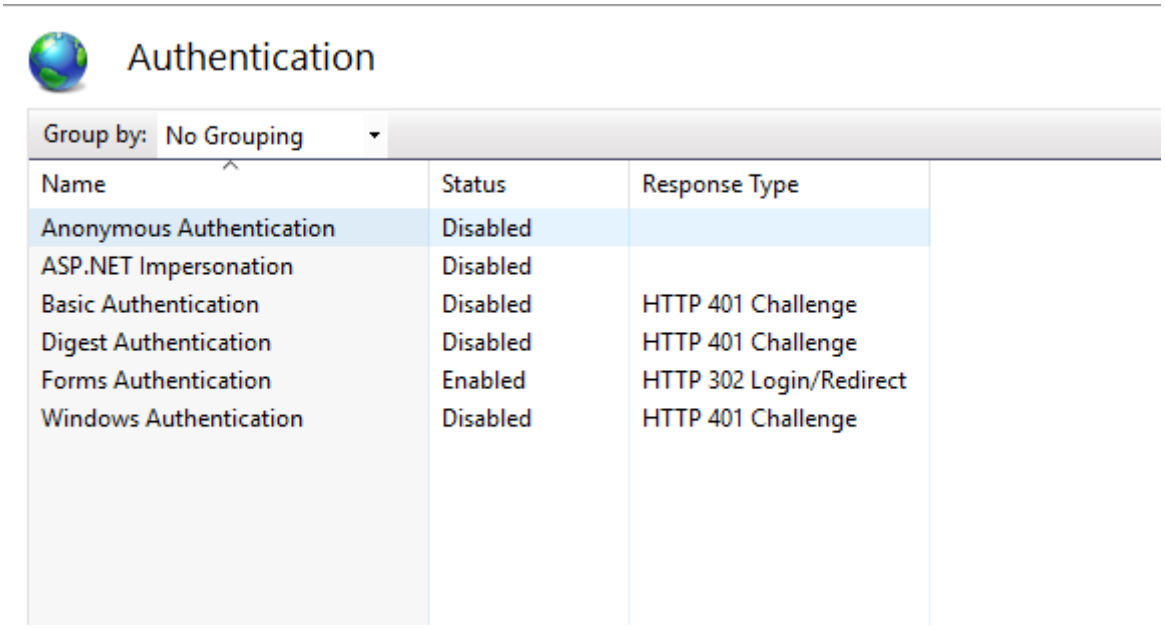
Content

1. Introduction

This guide is intended for administrators who want to secure their users' access to websites and applications hosted with Windows Internet Information Services (IIS) with DoubleClue Multi-Factor-Authentication (MFA). This can be achieved by using SustainSys module to add the SAML2 standard to the ASP.net Framework of IIS and set up DoubleClue as a SAML Identity Provider (IdP). SustainSys is a free open source software that is published under the MIT license.

2. Enabling Forms Authentication in IIS

1. Go to the IIS Manager and here to the side section
2. Search for the application that you want to secure with DoubleClue MFA and select it
3. Select the authentication tool
4. Enable Forms Authentication



3. Add the SustainSys Package Files to the Project

To connect your Windows IIS via SAML, you need to add the files of the SustainSys Modules to the project. Different components of IIS need different packages, which can be downloaded at https://www.nuget.org/packages. We provide more information and direct links to the packages needed for different IIS components in chapter 5. Configuring the Application's web.config.

Alternatively, you can contact us at support@doubleclue.com and we will send you the requested files.

Once you have downloaded the files, add them to the project directory. You can normally find this in the "bin" folder of the web application or website you want to connect with your DoubleClue

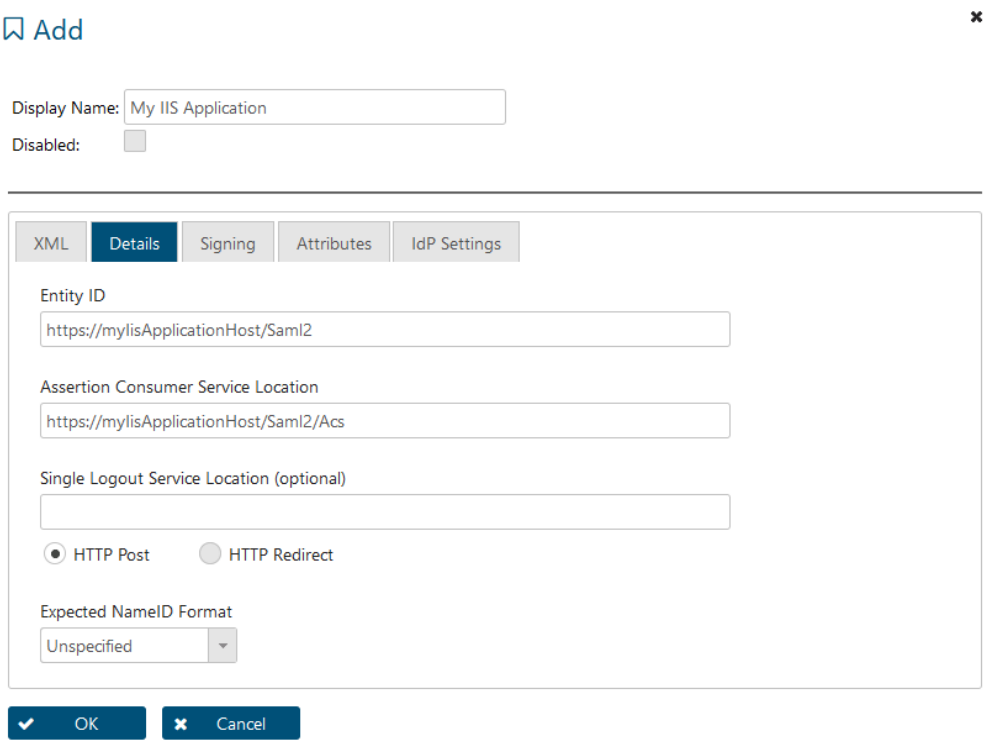
Enterprise Management (DCEM). It is the same folder in which the ***web.config*** is located. If the “bin” folder does not exist in the directory, you need to create a folder and call it “bin.

For the authentication to work properly, it is important that the whole directory of the web application or website are accessible for users when they log in. Therefore, it is advised to allow full access to the folder for authenticated users. This can be done in the preferences under the security tab of the parent folder.

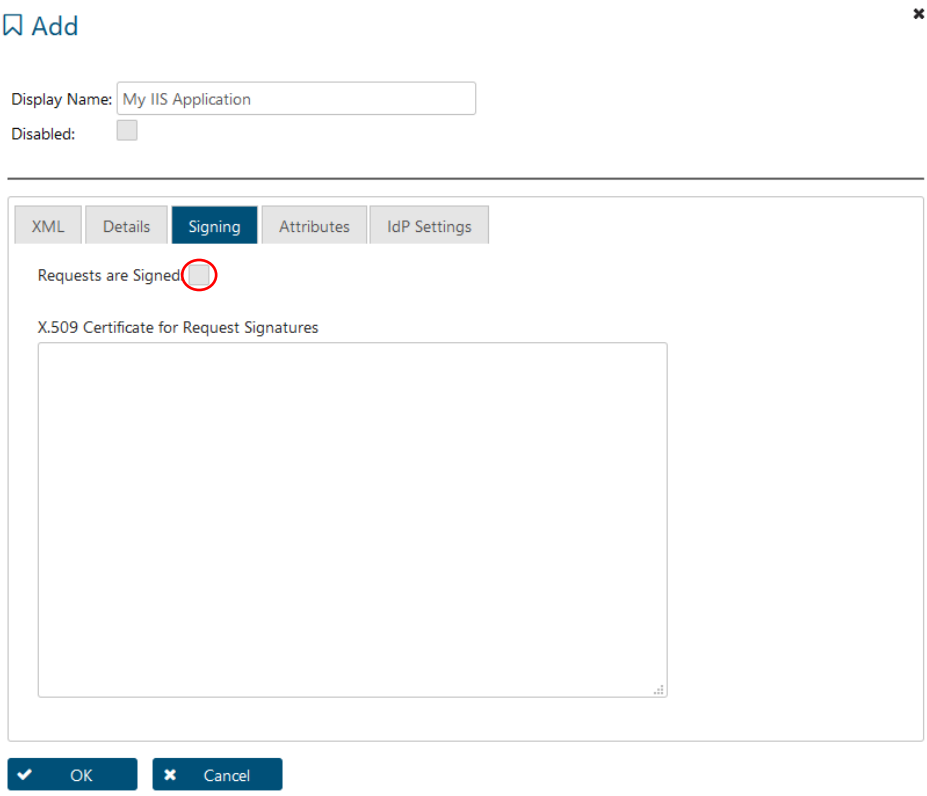
4. Preparing DCEM to be an Identity Provider

You can find general information on how to prepare DCEM to be an Identity Provider in chapter 12 of the “DCEM_Manual_EN.pdf”.

1. Add a new Service Provider to DCEM and choose the custom template.
2. Choose a globally unique Entity ID
3. Setup the “Assertion Consumer Service Location” myIisHost/Saml2/Acs. Ideally, the URL uses an SSL encryption, as Personally Identifiable Information (PII) will be exchanged with the service provider.



4. It is not necessary to sign SAML requests in this scenario. We therefore advice to go to the Signing and uncheck the “Requests are Signed” checkbox here. If you want to sign requests, see DCEM_Manual_EN.pdf chapter 12.



5. Modify the Application's Configuration Files

For the installed modules to be functional, you need to configure the respective configurations files of the IIS hosted applications.

In this chapter, you will find the code parts that need to be modified, depending on the used IIS components.

5.1 ASP.net Webforms and ASP.net MVC

For ASP.net Webforms:

Nuget packages: Sustainsys.Saml2.HttpModule
URL: https://www.nuget.org/packages/Sustainsys.Saml2.HttpModule

For ASP.net MVC:

Nuget package: Sustainsys.Saml2.Mvc
https://www.nuget.org/packages/Sustainsys.Saml2.Mvc/

Implement the following changes into the **web.config**:

1. Define sections and integrate the dll-files added in step 3.

Code Sample:

```
<section name="system.identityModel"
type="System.IdentityModel.Configuration.SystemIdentityModelSection,
System.IdentityModel, Version=4.0.0.0, Culture=neutral,
PublicKeyToken=B77A5C561934E089" />
    <section name="system.identityModel.services"
type="System.IdentityModel.Services.Configuration.SystemIdentityModelServicesSect
ion, System.IdentityModel.Services, Version=4.0.0.0, Culture=neutral,
PublicKeyToken=B77A5C561934E089" />
    <section name="sustainsys.saml2"
type="Sustainsys.Saml2.Configuration.SustainsysSaml2Section, Sustainsys.Saml2" />
```

2. Add the forms authentication.

   Code Sample:

```
<system.web>
    <authentication mode="Forms">
      <forms loginUrl="~/Saml2/SignIn" />
    </authentication>
</system.web>
```

3. Add the session authentication module. The public keys are part of the downloaded dll-modules.

   Code Sample:

```
<system.webServer>
    <modules>
      <add name="SessionAuthenticationModule"
type="System.IdentityModel.Services.SessionAuthenticationModule,
System.IdentityModel.Services, Version=4.0.0.0, Culture=neutral,
PublicKeyToken=b77a5c561934e089" preCondition="managedHandler" />
   </modules>
  </system.webServer>
```

4. Add the Saml2 configuration to the file. You have to modify some of the content in this section according to the settings in your DCEM. Enter the entityID , which you can find in your DCEM under SAML -> Settings. If your DCEM doesn't have an Entity ID yet, you can give it one. You can freely choose the Entity ID as long as it is globally unique. It is recommended to use your URL as the Entity ID. Also provide a return URL to which the user will be redirected after the successful authentication and add a link to import the meta data of your DCEM.

Code Sample:

```
<sustainsys.saml2 entityId="YourDoubleClueSamlEntityId"
returnUrl="http://YourWebApplicationStartPage"
authenticateRequestSigningBehavior="Never">
    <identityProviders>
      <add entityId="YourDoubleClue.com" wantAuthnRequestsSigned="false"
loadMetadata="true"
metadataLocation="YourDoubleClue.com/dcem/saml/idp_metadata.xml"
allowUnsolicitedAuthnResponse="true" binding="HttpRedirect" />
    </identityProviders>
    <serviceCertificates>
      <!--<add fileName="~/App_Data/Sustainsys.Saml2.Tests.pfx"/>-->
    </serviceCertificates>
  </sustainsys.saml2>
```

5. It isn't necessary to sign requests. We therefore advice to set wantAuthnRequestsSigned="false" (see Code Sample above) and to uncheck the box saying "Requests are Signed" under "Signing" in the Service Provider entry in DCEM.
   If you want to sign requests, see DCEM_Manual_EN.pdf chapter 12 and https://readthedocs.org/projects/saml2/downloads/pdf/latest/ chapter 3.16.

You can find a full code sample for the web.config of the Sustainsys.Saml2.HttpModule and Sustainsys.Saml2.Mvc in chapter 6.2 Full Code Sample for Sustainsys.Saml2.HttpModule and Sustainsys.Saml2.Mvc Configuration.

5.2 ASP.net Core MVC

Nuget package: Sustainsys.Saml2.AspNetCore2
https://www.nuget.org/packages/Sustainsys.Saml2.AspNetCore2/

1. Add a new file for the Account Controller class.

Code Sample:

```
[Route("account")]
public class AccountController : Controller
{
        [HttpGet("Login")]
         [AllowAnonymous]
         public IActionResult Login()
         {
                if (User.Identity.IsAuthenticated)
                    {
                      return RedirectToAction("Index", "Home");
                    }


              var result = new ChallengeResult(
                  Saml2Defaults.Scheme,
                  new AuthenticationProperties
                  {
                      RedirectUri = Url.Action("index", "Home"),
                  });
              return result;
         }

}
```

2. Implement the App Configuration into the **Appsettings.json.**

Code Sample:

```
"AppConfiguration": {
    "ServiceProvider": {
      //"Certificate": "OMVAdmin-DevTest-public_privatekey.pfx",
      "EntityId": "YourDoubleClueSamlEntityId ",
      "ReturnUrl": "http://YourWebApplicationStartPage",
      "AuthenticateRequestSigningBehavior": "Never"
    },
    "IdentityProvider": {
      "EntityId": "YourDoubleClue.com",
      "MetadataLocation": "YourDoubleClue.com/dcem/saml/idp_metadata.xml",
      "WantAuthRequestsSigned": "false",
      "LoadMetadata": "true"
    }
  }
```

3. Add the start up code for the initialization in ASP.NET Core to the S**tartup.cs**:

Code Sample:

```
services.AddIdentity<IdentityUser, IdentityRole>()
                .AddDefaultTokenProviders();

            services.AddAuthentication()
                .AddSaml2(options =>
                {
                    options.SPOptions.EntityId = new
EntityId(Configuration["AppConfiguration:ServiceProvider:EntityId"]);
                    options.SPOptions.ReturnUrl = new
Uri(Configuration["AppConfiguration:ServiceProvider:ReturnUrl"]);
                    SigningBehavior authenticateRequestSigningBehavior =
SigningBehavior.Never;

SigningBehavior.TryParse(Configuration["AppConfiguration:ServiceProvider:Authenti
cateRequestSigningBehavior"],
                        out authenticateRequestSigningBehavior);
                    options.SPOptions.AuthenticateRequestSigningBehavior =
authenticateRequestSigningBehavior;
                    options.IdentityProviders.Add(
                        new IdentityProvider(
                            new
EntityId(Configuration["AppConfiguration:IdentityProvider:EntityId"]),
options.SPOptions)
                        {
                            LoadMetadata = bool.Parse(
Configuration["AppConfiguration:IdentityProvider:LoadMetadata"]),
                            MetadataLocation =
Configuration["AppConfiguration:IdentityProvider:MetadataLocation"],
                            WantAuthnRequestsSigned =
bool.Parse(Configuration["AppConfiguration:IdentityProvider:WantAuthRequestsSigne
d"])
                        });
                });
```

6. Appendix

6.1 Further Information

https://readthedocs.org/projects/saml2/downloads/pdf/latest/
https://resources.infosecinstitute.com/form-authentication-asp-net-security-part-3/#gref

6.2 Full Code Sample for Sustainsys.Saml2.HttpModule and Sustainsys.Saml2.Mvc Configuration

```
<?xml version="1.0" encoding="UTF-8"?>

<configuration>

  <configSections>
```

```
    <!-- Add these sections below any existing. -->

    <section name="system.identityModel"
type="System.IdentityModel.Configuration.SystemIdentityModelSection,
System.IdentityModel, Version=4.0.0.0, Culture=neutral,
PublicKeyToken=B77A5C561934E089" />

    <section name="system.identityModel.services"
type="System.IdentityModel.Services.Configuration.SystemIdentityMode
lServicesSection, System.IdentityModel.Services, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=B77A5C561934E089" />

    <section name="sustainsys.saml2"
type="Sustainsys.Saml2.Configuration.SustainsysSaml2Section,
Sustainsys.Saml2" />

  </configSections>

  <appSettings>

    <add key="webpages:Version" value="3.0.0.0" />

    <add key="webpages:Enabled" value="false" />

    <add key="ClientValidationEnabled" value="true" />

    <add key="UnobtrusiveJavaScriptEnabled" value="true" />

  </appSettings>

  <system.web>

    <authentication mode="Forms">

      <forms loginUrl="~/Saml2/SignIn" />

    </authentication>

    <compilation targetFramework="4.7.2" />

    <httpRuntime targetFramework="4.7.2" />

  </system.web>

  <system.webServer>

    <modules>

      <!-- Add the SessionAuthenticatioModule -->

      <add name="SessionAuthenticationModule"
type="System.IdentityModel.Services.SessionAuthenticationModule,
System.IdentityModel.Services, Version=4.0.0.0, Culture=neutral,
PublicKeyToken=b77a5c561934e089" />

       <add name="Saml2AuthenticationModule"
type="Sustainsys.Saml2.HttpModule.Saml2AuthenticationModule,
Sustainsys.Saml2.HttpModule" />

     </modules>
```

```
  </system.webServer>

  <sustainsys.saml2 entityId="yourDoubleClue"
returnUrl="https://yourIisApplication/welcome"
authenticateRequestSigningBehavior="Always"
outboundSigningAlgorithm="SHA512">

    <nameIdPolicy allowCreate="true" format="Unspecified" />

    <identityProviders>

      <add entityId="yourDoubleClue"
metadataLocation="https://yourDoubleClue.com/dcem/saml/idp_metadata.
xml" allowUnsolicitedAuthnResponse="true"
wantAuthnRequestsSigned="true" loadMetadata="false">

          <!--<signingCertificate storeName="TrustedPublisher"
storeLocation="LocalMachine"

                x509FindType="FindBySubjectName"
findValue="company.com"/>-->

      </add>

    </identityProviders>

     <serviceCertificates>

       <add use="Signing"
findValue="fce56b9cc41a0933d630ac228265425f90748217" storeName="My"
storeLocation="LocalMachine" x509FindType="FindByThumbprint" />

    </serviceCertificates>

  </sustainsys.saml2>

  <system.identityModel.services>

    <federationConfiguration>

      <cookieHandler requireSsl="false" />

    </federationConfiguration>

  </system.identityModel.services>

  <system.identityModel>

    <identityConfiguration>

      <securityTokenHandlers>

        <add
type="System.IdentityModel.Services.Tokens.MachineKeySessionSecurity
TokenHandler, System.IdentityModel.Services, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b77a5c561934e089" />

        <remove
type="System.IdentityModel.Tokens.SessionSecurityTokenHandler,
```

```
System.IdentityModel, Version=4.0.0.0, Culture=neutral,
PublicKeyToken=b77a5c561934e089" />

      </securityTokenHandlers>

    </identityConfiguration>

  </system.identityModel>

</configuration>
```