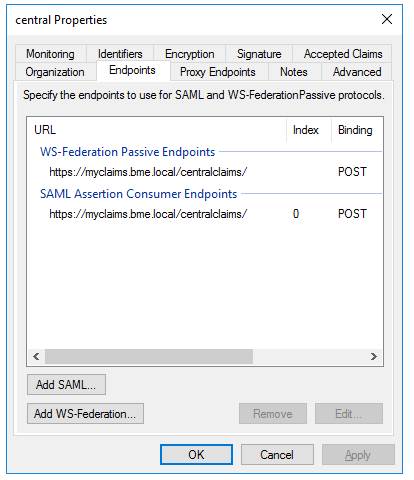
How to Utilize a Single Claims Relying Party Trust for Multiple Claims Web Applications

1. Create a central claims aware App for example - [https://myclaims.bme.local/centralclaims/](https://nam06.safelinks.protection.outlook.com/?url=https%3A%2F%2Fmyclaims.bme.local%2Fcentralclaims%2F&data=02%7C01%7Ctapand%40microsoft.com%7Cad40ea0f11d049d0ba4b08d7eb89f65f%7C72f988bf86f141af91ab2d7cd011db47%7C1%7C0%7C637236850085912598&sdata=CTsTC8gLPAgjjsNVCpKB9G2KQZyekFjxoVlKQuPFils%3D&reserved=0) . This App will sit between other claims aware Apps  and ADFS and handle the redirects. Its also claims aware.
2. Add the [https://myclaims.bme.local/centralclaims/](https://nam06.safelinks.protection.outlook.com/?url=https%3A%2F%2Fmyclaims.bme.local%2Fcentralclaims%2F&data=02%7C01%7Ctapand%40microsoft.com%7Cad40ea0f11d049d0ba4b08d7eb89f65f%7C72f988bf86f141af91ab2d7cd011db47%7C1%7C0%7C637236850085922592&sdata=xqOaQazdin6muhXQqDQAbaJGfcHIR8L%2BDu6XsEOoLgs%3D&reserved=0) App as an RP to ADFS and populate WS-Fed and SAML POST endpoints pointing to the Identifier of the App. i.e. [https://myclaims.bme.local/centralclaims/](https://nam06.safelinks.protection.outlook.com/?url=https%3A%2F%2Fmyclaims.bme.local%2Fcentralclaims%2F&data=02%7C01%7Ctapand%40microsoft.com%7Cad40ea0f11d049d0ba4b08d7eb89f65f%7C72f988bf86f141af91ab2d7cd011db47%7C1%7C0%7C637236850085922592&sdata=xqOaQazdin6muhXQqDQAbaJGfcHIR8L%2BDu6XsEOoLgs%3D&reserved=0)



1. Decorate the Default.aspx.cs file with the following –

//-----------------------------------------------------------------------------

//

// THIS CODE AND INFORMATION IS PROVIDED "AS IS" WITHOUT WARRANTY OF

// ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO

// THE IMPLIED WARRANTIES OF MERCHANTABILITY AND/OR FITNESS FOR A

// PARTICULAR PURPOSE.

//

// Copyright (c) Microsoft Corporation. All rights reserved.

//

//

//-----------------------------------------------------------------------------

using System;

using System.Web.UI;

using System.Web.UI.WebControls;

using Microsoft.IdentityModel.Claims;

public partial class \_Default : System.Web.UI.Page

{

    protected void Page\_Load(object sender, EventArgs e)

    {

        string RelyingParty;

        string Endpoint;

        RelyingParty = Request.QueryString["RelyingParty"];

        if (Request.HttpMethod == "GET")

        {

            if (RelyingParty == "prod")

            {

                Endpoint = "<https://myclaims.bme.local/capass/>";

            }

            else if (RelyingParty == "stage")

            {

                Endpoint = "<https://myclaims.bme.local/claimsApp2/>";

            }

            else

            {

                Endpoint = "<https://3rd-Application-endpoint/>";

            }

            Response.Cookies["Endpoint"].Value = Endpoint;

            Response.Redirect("<https://azr.sts.msidentity.com/adfs/ls/IdpInitiatedSignOn.aspx?LoginToRP=https://myclaims.bme.local/centralclaims>");

        }

        else if (Request.HttpMethod == "POST")

        {

            if (Request.Cookies["Endpoint"].Value is object)

            {

                Endpoint = Request.Cookies["Endpoint"].Value;

                Response.ClearContent();

                Response.StatusCode = 307;

                Response.StatusDescription = "Temporary Redirect";

                Response.RedirectLocation = ResolveClientUrl(Endpoint);

                Response.Flush();

            }

        }

        else

        {

            Response.Write("The requested HTTP method (" + Request.HttpMethod + ") is not supported by this redirector page. This page supports HTTP GET and POST. Please contact your administrator.");

        }

    }

}

//-------------------------------------------------------------------------------------------------------------------------------------------------

1. On the new claims aware app make the following changes in web.config. i.e. replace the default audienceUris And realm to point to the central app , rather than their own.

<audienceUris>

        <!--<add value="<https://myclaims.bme.local/CAPASS/>" />--> ---- > remove the default.

          <!--Updated to pint to centralclaims RP identifier-->

          <add value="<https://myclaims.bme.local/centralclaims/>" /> ---- > add the Identifier of the central claims App as the Audience URI of other Apps.

       </audienceUris>

<federatedAuthentication>

          <!--Updated to point to centralclaims RP identifier-->

          <wsFederation passiveRedirectEnabled="true" issuer="<https://azr.sts.msidentity.com/adfs/ls/>" realm="<https://myclaims.bme.local/centralclaims/>" requireHttps="true" />

          <cookieHandler requireSsl="true" />

      </federatedAuthentication>

1. Now browse to central App with query param like this  -

"<https://myclaims.bme.local/centralclaims/?RelyingParty=prod>" --- > this will be validated against Request.QueryString["RelyingParty"]; In the Default.aspx.cs of the central App and then Authenticated to appropriate RP. [https://myclaims.bme.local/capass/](https://nam06.safelinks.protection.outlook.com/?url=https%3A%2F%2Fmyclaims.bme.local%2Fcapass%2F&data=02%7C01%7Ctapand%40microsoft.com%7Cad40ea0f11d049d0ba4b08d7eb89f65f%7C72f988bf86f141af91ab2d7cd011db47%7C1%7C0%7C637236850085932589&sdata=g4%2Fsd8ekMPlfEaZ7YJxvtk5h7w7hGVfGwSkZB4gx38U%3D&reserved=0) in this case.

"<https://myclaims.bme.local/centralclaims/?RelyingParty=stage>" --- > this will be validated against Request.QueryString["RelyingParty"]; In the Default.aspx.cs of the central App and then Authenticated to appropriate RP.

[https://myclaims.bme.local/claimsApp2/](https://nam06.safelinks.protection.outlook.com/?url=https%3A%2F%2Fmyclaims.bme.local%2FclaimsApp2%2F&data=02%7C01%7Ctapand%40microsoft.com%7Cad40ea0f11d049d0ba4b08d7eb89f65f%7C72f988bf86f141af91ab2d7cd011db47%7C1%7C0%7C637236850085932589&sdata=hCjNSvDv1y3Q%2Buk%2FYA%2FIPSA7eC1UzXkXYjqIoCPbQkk%3D&reserved=0) in this case.



Taparshi Pandit

Service Engineer II

ID Operations & Service Eng

+91+91-9874778677 | +91-9000959847

[tapand@microsoft.com](mailto:tapand@microsoft.com) | CEDIS– ADFS Support [CEDISADFSSUP@microsoft.com](mailto:CEDISADFSSUP@microsoft.com)