Dependencies

This middleware has the following dependencies, which can be installed through NuGet:
1. IdentityModel
2. Microsoft.AspNetCore.Authentication.OpenIdConnect
3. System.IdentityModel.Tokens.Jwt

Template Project

The solution provided shows how to use this middleware to add authentication to a Blazor web project. Note that the settings needed to configure the middleware should not be hard-coded into an application for production purposes and the configuration should instead be read from a more suitable place matching the way other application configuration is read. The hard-coded parameters are used to simplify the example project.

Application Configuration

As shown in the template Blazor project, in order to use the middleware, you need to supply a few settings:

1. AppDomain: Set this to the Base URI for your site.
2. Authority: This is the SAP tenant (in the form "https://xxxxxxxxxx.accounts.ondemand.com"), and will be the base of the URI used for administration of the identity platform.
3. ClientId: This is the Client ID as generated below.
4. ClientSecret: This is the Client Secret as generated below.
5. License: This is the license key for the middleware. Note that the "localhost" application domain does not require a license key.
6. Expiry: The expiry date for the license.
7. AuthsPerDay: Number of authentication redirections per day allowed by the license.

SAP Identity Authentication Tenant Settings

1. Create a new Custom Application (Applications->Add)
2. Update Trust Settings
2.1. Set Type to OpenID Connect

2.2. Update OpenID Connect Configuration

2.2.1. Enter a name for the settings

2.2.2. Set the Redirect URI to your site
This will need to be the base URI of your website followed by "/signin-oidc"

2.2.3. Set the Post Logout Redirect URI to your site
This will need to be the base URI of your websire followed by "/signout-callback-oidc"

2.3. Update Assertion Attributes
Add a user attribute for "Groups", with the assertion attribute left as the default ("groups").

3. Update API Authentication

3.1. Create a Client ID and Client Secret pair for the API.
Under "Configure Secrets", Add a new secret, noting down both the Client ID and the Client Secret. Enter these into their corresponding Application Configuration settings.

4. Add groups
Navigate to Users & Authorizations -> User Groups. Here you will be able to create groups.

5. Add users
Navigate to Users & Authorizations -> User Management. Here, you can add users that should be able to log in to your application, and assign the users to groups.