**B2C Multiple Application Consent Sample Code Prerequisites**

The B2C Multiple Application Consent sample application has several prerequisites that must be configured prior to its use including:

1. Follow the steps in this tutorial <https://docs.microsoft.com/en-us/azure/active-directory-b2c/custom-policy-get-started> to prepare your B2C tenant to support the creation of custom policies using the Identity Experience Framework.
2. Create an Azure Storage Account. Within that storage account create a container named azureblue with public blob access. Upload the unified.cshtml file in the SAMLSPProvider folder to that container. Create a table within that storage account named B2CConsent to store user consent results.
3. Create an Azure App Service (Windows, .Net Core 3.1). Build and deploy the REST API in the Visual Studio solution to that app service. Create an application setting in the Configuration of the app service named TableStorageConnectionString and set its value to the connection string of the storage account created in step 2.
4. Update the sample TrustFrameworkExtensions.xml file in the SAMLSPProvider folder replacing the markers for B2C tenant name, storage account name, REST API URL, Identity Server URL, etc. with appropriate values for your environment.
5. Update the sample SignUpOrSignIn.xml file in the SAMLSPProvider folder replacing the markers for B2C tenant name.
6. Upload the custom policy files to the Identity Experience Framework in the B2C blade.