|  |  |
| --- | --- |
|  | Azure Active Directory B2C  Module 5 Lab – Set Up Policies |
|  |  |
|  |  |

Contents

[Overview 3](#_Toc458772403)

[Learning Objectives 3](#_Toc458772404)

[1. Setup the Trust Framework policy and Relying Party policies 3](#_Toc458772405)

[2. Setup cryptographic keys 4](#_Toc458772406)

[3. Upload policies and run user journeys 4](#_Toc458772407)

[4. Create a new User Journey to sign in a user without MFA 5](#_Toc458772408)

# Overview

During this lab, you will set up the Trust Framework policy and relying party policies, then create the new user sign-in journey.

**Estimated time to complete this lab: 45 minutes**.

# Learning Objectives

After completing the exercises in this lab, you will be able to:

* Set up the Trust Framework policy
* Set up the relying party policies
* Create a new user journey to create a different user experience

## Setup the Trust Framework policy and Relying Party policies

|  |  |
| --- | --- |
| Task | Detailed Steps |
| Download tools | 1. Go to **https://github.com/beejones/B2CDemoTools** 2. Click **Clone or download**, click **Download ZIP** and extract it to c:\B2c\ 3. The DLLs (in the ExploreAdmin folder) may need to be unblocked: right-click each of the individual DLLs in turn, click **Properties**, **Unblock** and **OK**   **Note:** We will assume this download is in the **c:\b2c\B2CDemoTools-master** folder in the rest of the labs. All the policies in this exercise are located in the **c:\b2c\B2CDemoTools-master\B2CPolicies\Advanced Policies Starter Pack** folder and we will refer to all these policies as the **Advanced Policies Starter Pack** in the rest of the document. All the policies conform to the TrustFrameworkPolicy\_0.3.0.0.xsd schema.   1. Navigate to **the c:\b2c\B2CDemoTools-master\Labs\TrustFramework** folder and open the **Course\_TrustFramework.docx** – you can use this for copy/paste of some code snippets |
| Setup Notepad++ (if you have not already got it) | 1. Go to **https://notepad-plus-plus.org/download** and install the latest version. 2. Open **Notepad++** 3. Click **Plugins**, **Plugin Manager**, **Show Plugin Manager** 4. From the list, select **XML Tools** and click **Install** 5. After the installation completes, you should be able to click the **Plugins** menu option in **Notepad++** and the new option **XML Tools** |
| Validate a policy using the provided XSD | 1. Click **File**, **Open** and open **lamnahealth.onmicrosoft.com\_base.xml** policy from the **c:\b2c\B2CDemoTools\B2CPolicies\Advanced Policies Starter Pack** folder 2. Click **Plugins**, **XML Tools**, **Validate Now** 3. Put the path to the **TrustFrameworkPolicy\_0.3.0.0.xsd** in the text box and click **OK** 4. A message box should show stating “XML is valid.” 5. To show what happens with invalid XML, add the following line at line 10 (right after that **TrustFrameworkPolicy** node:   <Foo></Foo>   1. Validate XML again by clicking **Plugins**, **XML Tools**, **Validate Now**   **Note:** An error message similar to the following should show:  ERROR: Element '{http://schemas.microsoft.com/online/cpim/schemas/2013/06}**Foo**': This element is not expected. Expected is one of ( {http://schemas.microsoft.com/online/cpim/schemas/2013/06}**BasePolicy**, {http://schemas.microsoft.com/online/cpim/schemas/2013/06}**Contacts**, {http://schemas.microsoft.com/online/cpim/schemas/2013/06}**DocumentReferences**, {http://schemas.microsoft.com/online/cpim/schemas/2013/06}**BuildingBlocks**, {http://schemas.microsoft.com/online/cpim/schemas/2013/06}**ClaimsProviders**, {http://schemas.microsoft.com/online/cpim/schemas/2013/06}**UserJourneys**, {http://schemas.microsoft.com/online/cpim/schemas/2013/06}**RelyingParty** ). |
|  | 1. Delete the foo line |

## Setup cryptographic keys

|  |  |
| --- | --- |
| Task | Detailed Steps |
| Create required keys for the policies | 1. Open **PowerShell** as an administrator and go to the folder ExploreAdmin in B2CDemoTools folder 2. Import the ExploreAdmin.dll using the following command:   import-module .\ExploreAdmin.dll  **Note:** If this causes an error, check your dlls are unblocked and that you are running PowerShell as an administrator.   1. Enter the following commands to create the keys (this may pop up an interactive login window, in which you should enter your tenant admin user credentials):   New-CpimKeyContainer *<*B2CDirName*>*.onmicrosoft.com TokenSigningKeyContainer key0 rsa 2048 0 0  New-CpimKeyContainer *<*B2CDirName*>*.onmicrosoft.com TokenEncryptionKeyContainer key0 rsa 2048 0 0  **Note:** These keys will be used in a later lab.There are two different key containers: the first is TokenSigningKeyContainer and the second one is TokenEncryptionKeyContainer. The key0 in both the commands is the identifier of the key. For all practical purposes, it is not used by AAD B2C directly, but used by admins for operations such as deleting a key if necessary. The last two parameters in each case are timestamps indicating when the key can become active and when it will expire. For this exercise, we will create keys without any time limits. In general, for key roll over, an admin can create new keys and AAD B2C will typically use the appropriate keys. |

## Upload policies and run user journeys

|  |  |
| --- | --- |
| Task | Detailed Steps |
| Modify the tenantId in the policies | 1. Open **lamnahealth.onmicrosoft.com\_B2C\_1A\_base.xml** policy from the Advanced Policies Starter Pack in a text editor 2. In the root **TrustFrameworkPolicy** element, update the **TenantId** attribute to reflect your tenant   **Note:** At this point, you may also want to rename the file to reflect the tenant, but the file name is not used by the B2C system when the policies are uploaded.   1. Find the **TechnicalProfile** element with **Id="Facebook-OAUTH"**, and then locate Metadata element with **Key="client\_id"**   **Note:** This is the application identifier that AAD B2C will use to authenticate the user with Facebook.   1. Back in the Azure Portal, on the **Settings** blade, click **Identity providers** and then click **Facebook** 2. Copy the **Client ID** (this is the one you pasted, having copied it from Facebook, in a much earlier lab) 3. Paste this into the **client\_id** element (in the text editor)   **Note:** When you originally copied the Client ID, you also copied the Facebook client secret. This policy is setup to use the same secret, specified using CryptographicKey in the policy – so no change is needed for this.   1. Update all the other policies (e.g. lamnahealth.onmicrosoft.com\_signup.xml) with the correct **tenantId**, found both in the TrustFrameWorkPolicy element and the BasePolicy element, and save them |
| Upload the policies | 1. In the Azure Portal, logged in as the tenant admin, on the **Settings** blade, click **All Policies** 2. Click **Upload Policy**, and then browse to **<TenantName>.onmicrospoft.com\_base.xml** policy, and follow the instructions to upload it   **Note:** The base policy must be uploaded first, then the base\_extensions policy (as it depends on the base one), and then the other policies in any order (as they all depend on the base\_extensions policy. When the policy is uploaded, the name is prepended with B2C\_1A\_. This is done to differentiate between policies created by the portal, and handcrafted ones.   1. Upload the **base\_extensions** xml file, and then the remaining ones |
| Run a policy (to test) | **Note:** Here, and for all of these policies as you try them out, make sure that the Run Policy is referring to your test app, and the aadb2cplayground website.   1. In the **All Policies** blade, click the **signin** policy 2. Click **Run now** signing in with an existing account (noting that MFA is active – you don’t have to complete the MFA)   **Note:** Whenever you run one of these policies, just ensure that on the Run Policy section, the correct application is selected (B2CTestApp), and the correct redirect URI is selected (the “playground” address). |

## Create a new User Journey to sign in a user without MFA

|  |  |
| --- | --- |
| Task | Detailed Steps |
| Copy an existing user journey to create a new one | 1. Open **<TenantName>.onmicrosoft.com\_base.xml** from the Advanced Policies Starter Pack and locate the **UserJourneys** node, and within that the **UserJourney Id=”SignIn”** node 2. Copy the **whole node** (from <UserJourney> and </UserJourney>), and paste it as an independent user journey (within the UserJourneys node) 3. Rename the **Id** attribute on the copied UserJourney element to **SignIn\_NoMFA** (or something similar) 4. The OrchestrationStep elements with Order = 5 to 7 perform phone authentication - **remove steps 5 to 7** 5. Change the **Order** of the last OrchestrationStep from **8** to **5** (if you do not do this, and you then attempt to use the policy, B2C will complain about inconsistent order numbers) 6. **Save** your changes |
| Create a new policy to execute the new user journey | 1. Open the **signin** xml policy in NotePad++ (if necessary) and save it as **<TenantName>.onmicrosft.com\_signin\_nomfa.xml** or something similar 2. Change the **PolicyId** attribute of **TrustFrameworkPolicy** element to **signin\_nomfa** (when a policy is uploaded, the PolicyId attribute is used to determine its name in the system) 3. Change the **ReferenceId** attribute of the **DefaultUserJourney** element to SignIn\_NoMFA   **Note:** This indicates which UserJourney will be executed when a request comes in with a signin\_nomfa policy id.   1. **Save** this policy and (in the Azure Portal) **upload** both the policies (base and signin\_nomfa) – in the case of the base one, select **Overwrite the policy if it exists** 2. Click **<TenantName.onmicrosft.com>\_signin\_nomfa.xml** (or whatever) on the **AllPolicies** blade and click **Run Now** (showing that MFA is not active) |