|  |  |
| --- | --- |
|  | Azure Active Directory B2C  Module 8 Lab – Add an Identity Server |
|  |  |
|  |  |

Contents

[Overview 3](#_Toc458770332)

[Learning Objectives 3](#_Toc458770333)

[1. Add Wingtip Corp Claims Provider 3](#_Toc458770334)

# Overview

During this lab, you will add a corporate, Openid Connect claims provider to the extensions policy created in the previous lab.

**Estimated time to complete this lab: 30 minutes**.

# Learning Objectives

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

* Specify an Openid Connect provider in your policy
* Use the provider in the user journey

## Add Wingtip Corp Claims Provider

|  |  |
| --- | --- |
| Task | Detailed Steps |
| Add the Wingtip Corp claims provider | 1. Edit the **<tenant>\_Base\_Extensions** policy 2. Navigate to the **c:\B2C\B2CDemoTools-master\B2CPolicies\Final** folder (or wherever you have saved it) and edit **b2ccharm.onmicrosoft.com\_B2C\_1A\_base\_Extensions.xml** 3. Search for **IdentityServer**, and copy the **ClaimsProvider** node (from the line above <ClaimsProvider> until </ClaimsProvider>) 4. Back in the **<tenant>\_Base**\_**Extensions** policy, paste the copied text within the ClaimProviders node   **Note:** You have just added a reference to the Wingtip Corp in your policies. |
| Upload crypto keys to the tenant | 1. Run the **Windows Azure Active Directory PowerShell** Module as Administrator 2. Switch to the directory where ExploreAdmin is stored and enter the command:   Import-Module .\ExploreAdmin.dll   1. Run the following powershell command:   Set-CpimKeyContainer -Tenant <tenant> -StorageReferenceId  B2CAuthClientSecret -UnencodedAsciiKey abcdef  **Note:** We have created a client secret which we will use to authenticate to the identity server. |
| Change the clientid for your tenant | 1. Back in the **<tenant>\_Base**\_**Extensions** policy within the ClaimsProvider node you just pasted, locate the **client\_id** and replace b2ccharm with your **tenantId** as follows:   <Item Key="client\_id">https://login.microsoftonline.com/te/<tenantId></Item>   1. Similarly, locate the **IdTokenAudience** and replace b2ccharm with your **tenantId** as follows:   <Item Key="IdTokenAudience">https://login.microsoftonline.com/te/<tenantId></Item>  **Note:** The identity server uses the client id to scope the JSON Web Token to the client id. |
| Change the SignupOrSigninWithRestAndIdp user journey to support the Wingtip corp identity provider | 1. Still in **<tenant>\_Base\_Extensions.xml**, search for **Orchestration Step order=”1”** 2. Within the <ClaimsProviderSelections> node add the following line:   <ClaimsProviderSelection  TargetClaimsExchangeId="IdentifyServerExchange" />  **Note:** This adds our provider to the selection screen.   1. Locate the **Orchestration Step order=”2”** and within the <ClaimsExchanges> node the add the following line:   <ClaimsExchange Id="IdentifyServerExchange"  TechnicalProfileReferenceId="IdentityServer" />  **Note:** This maps the IdentifyServerExchange to the technical profile of the Wingtip corp identity provider. If you inspect the <ClaimsProvider> definition of identity server, you will see that you already have a technical profile called ‘IdentityServer’.   1. **Save** and **upload** the policy |
| Test the policy | 1. Select the **SignupOrSigninWithRestAndIdp** policy and click **Run Now**, and notice that you can now sign in using the Wingtip Corp identity server – it won’t work because the IdP (Wingtip Corp) doesn’t recognise you |