B2C REST API and IDP

Hands-on Lab

Released:

Terms of Use

Microsoft Confidential - For Internal Use Only ***-*** Do Not Distribute Outside of Microsoft

© 2016 Microsoft Corporation. All rights reserved.

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

For more information, see **Microsoft Copyright Permissions** at [**http://www.microsoft.com/permission**](http://www.microsoft.com/permission)

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The Microsoft company name and Microsoft products mentioned herein may be either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

**This document reflects current views and assumptions as of the date of development and is subject to change.  Actual and future results and trends may differ materially from any forward-looking statements.  Microsoft assumes no responsibility for errors or omissions in the materials.**

**THIS DOCUMENT IS FOR INFORMATIONAL AND TRAINING PURPOSES ONLY AND IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, WHETHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT.**

|  |  |
| --- | --- |
| About the Author | |
| **Author**: | **Ronny Bjones** |
| **Bio**: | Ronny Bjones is Director of Cloud Identity & Privacy Services for Microsoft Engineering (Cloud & Enterprise). Ronny kicked of the design and development of [Azure Active Directory B2C](https://azure.microsoft.com/en-us/documentation/services/active-directory-b2c/). Ronny is responsible for developing the concepts, prototyping, incubation and bringing the service into production. Ronny holds several patents in the field of identity and privacy. |

“About the Authors” is an important item as it establishes the credibility of the text by explaining how much experience the author team has in the field. Add as many “About the Authors” as needed from the Quick Parts Gallery. Change “Author” to a different title, such as “Subject Matter Expert” if that is more appropriate. Include SMEs who assisted with the development of the course. Add this to every Module.

Table of Contents

[Lab Overview 1](#_Toc451337794)

[Exercise 0: Setup 2](#_Toc451337795)

[Exercise 1: Add Wingtip REST API Claims Provider 4](#_Toc451337796)

[Exercise 2: Add Wingtip Corp Claims Provider 7](#_Toc451337797)

[Appendix 9](#_Toc451337798)

# Lab Overview

Several paragraphs – or longer – describing an overview of the lab including a description of the lab and why certain topics are covered. This is also called the ‘LAB ABSTRACT’ that will be used for hand-off to conferences as part of the content hand-off process

###### Abstract

During this lab, you will run several exercises that will help you achieve a better understanding on how to interface external identity providers and rest API’s

###### Learning Objectives

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

1. Add a REST API to your trust framework policy
2. Add the necessary keys to authenticate to the REST API
3. Learn how to use the recorder
4. Add input claims to the user journey

**Estimated time to complete this lab: *70* minutes**

# Exercise 0: Setup

Each exercise consists of a scenario and learning objectives, the scenario describes the purpose of the exercices, while the objectives are listed and have bullet points.

#### Scenario

In this exercise, we will create an advanced policy

As part of this setup, we will:

* Download the reference repo from github.com.
* Install the cmdlet tools needed to create the necessary keys.

|  |  |
| --- | --- |
| Task | Detailed Steps |
| *Download the reference repo* | Steps need to have BOLD when you indicate a certain path or a step to click and execute, always use numbering for each of the steps that need to be executed. .   1. Download the github repo https://github.com/beejones/B2CDemoTools as zip file. 2. Extract the zip file to your local disk. |
| *Setup Powershell cmdlets (windows exclusive)* | 1. Goto <your disk>\B2CDemoTools\ExploreAdmin   These files are marked unsecure because they are downloaded from the internet. Unblock each file by right-click, properties and mark Unblock. |

# Exercise 1: Add Wingtip REST API Claims Provider

Each exercise consists of a scenario and learning objectives, the scenario describes the purpose of the exercices, while the objectives are listed and have bullet points.

#### Scenario

We will add the REST API claims provider to the extensions policy.

After completing this exercise, you will understand:

* How to specify a REST API in your policy?
* Use a REST API in the user journey.
* Using the user journey recorder.

The REST API is an attribute provider set up by Wingtip toys. It keeps track of all the loyalty numbers of their customers. Using a loyalty number will give customers a price reduction when renting video games.

We will change the default user journey to authenticate the customer and use the userid to collect the loyalty number from the REST API. The loyalty number will be returned to the application.

|  |  |
| --- | --- |
| Task | Detailed Steps |
| Check if you have your keys for the tenant | 1. Make sure to have the crypto keys. You can generate them by opening Windows Powershell   Run New-CpimKeyContainer <tenant> TokenSigningKeyContainer TokenSigningKeyContainer rsa 2048 0 0  New-CpimKeyContainer <tenant> TokenEncryptionKeyContainer TokenEncryptionKeyContainer rsa 2048 0 0 |
| Upload crypto keys to the tenant | 1. Run Windows Powershell. Change to the directory where ExploreAdmin is stored. 2. Run the following powershell commands:   Cd <your location>\ExploreAdmin  Import-Module .\ ExploreAdmin.dll  Set-CpimKeyContainer -Tenant <tenant> -StorageReferenceId  B2cRestClientId -UnencodedAsciiKey 12345678  Set-CpimKeyContainer -Tenant <tenant> -StorageReferenceId  B2cRestClientSecret -UnencodedAsciiKey abcdef  The clientId 12345678, clientSecret abcdef are preset in the REST API as basic authentication credentials. |
| Create your tenant’s base policies | 1. Copy <your disk>\B2CDemoTools\B2CPolicies\Lab Templates\[Reference\_B2C\_1A\_base.xml](https://github.com/beejones/B2CDemoTools/blob/master/B2CPolicies/Lab%20Templates/Reference_B2C_1A_base_Extensions.xml) to your location.   Rename the file as <tenant>\_B2C\_1A\_Base.xml (example B2CAuth .onmicorosft.com\_B2C\_1A\_Base.xml).   1. Edit <tenant>\_B2C\_1A\_Base\_Extensions.xml. Edit the file and replace all b2ccharm to the name of your tenant (e.g. B2CAuth). 2. Copy <your disk>\B2CDemoTools\B2CPolicies\Lab Templates\[Reference\_B2C\_1A\_base\_Extensions.xml](https://github.com/beejones/B2CDemoTools/blob/master/B2CPolicies/Lab%20Templates/Reference_B2C_1A_base_Extensions.xml) to your location.   Rename the file as <tenant>\_B2C\_1A\_Base\_Extensions.xml (example B2CAuth .onmicorosft.com\_B2C\_1A\_Base\_Extensions.xml).   1. Edit <tenant>\_B2C\_1A\_Base\_Extensions.xml. Replace all b2ccharm to the name of your tenant (e.g. B2CAuth). |
| Add claim type used by the REST API | 1. Edit <tenant>\_B2C\_1A\_Base\_Extensions.xml. 2. Open <your disk>\B2CDemoTools\ B2CPolicies\Final\b2ccharm.onmicrosoft.com\_B2C\_1A\_base\_Extensions.xml. Copy the section ClaimsSchema under BuildingsBlocks. This defines the Loyalty claims used by the REST API. Copy the ClaimsSchema under BuildingsBlocks in <Tenant>\_B2C\_1A\_Base\_Extensions.xml |
| Add the REST API claims provider to <tenant>\_B2C\_1A\_Base\_Extensions.xml. | 1. Edit <Tenant>\_B2C\_1A\_Base\_Extensions.xml. 2. Add the following under </BuildingBlocks>   <ClaimsProviders>  </ClaimsProviders>  Open <your disk>\B2CDemoTools\B2CPolicies\ Final\b2ccharm.onmicrosoft.com\_B2C\_1A\_base\_Extensions.xml.  Search for Loyalty Rest Api. Copy from the line above <ClaimsProvider> until </ClaimsProvider>. Paste the copied text in your <tenant>\_B2C\_1A\_Base\_Extensions.xml policy in-between <ClaimProviders> </ClaimsProviders>  We now have added a reference to the REST API to our policies. |
| Upload <tenant>\_B2C\_1A\_Base\_Extensions.xml.<Tenant>\_B2C\_1A\_Base\_Extensions.xml <Tenant>\_B2C\_1A\_Base\_Extensions.xml | 1. Go to the portal. In settings select “All Policies” 2. Upload base Policy. Check “ Overwrite the policy if it exists”. Click on “Select a file”. Browse and select <Tenant>\_B2C\_1A\_Base.xml. 3. Upload Policy. Check “ Overwrite the policy if it exists”. Click on “Select a file”. Browse and select <Tenant>\_B2C\_1A\_Base\_Extensions.xml. |
| Add REST API to the user journey | 1. Open <Tenant>\_B2C\_1A\_Base.xml.  Search for <UserJourney Id="SignUpOrSignIn">. Copy the full user journey. 2. Open <Tenant>\_B2C\_1A\_Base\_Extensions.xml and paste beyond </ClaimsProviders>. Enclose the UserJourney by <UserJourneys></UserJourneys>. Rename the id Add REST API to the user journey SignUpOrSignIn to SignUpOrSignInWithRestAndIdp. |
| Change the SignUpOrSignInWithRestAndIdp user journey to include the REST API | 1. In <Tenant>\_B2C\_1A\_Base\_Extensions.xml find <OrchestrationStep Order="10" Type="SendClaims" in the SignUpOrSignInWithRestAndIdp user journey. Change this step’s Order to 11 because we will add an additional step in between step 9 and step 11 which will do the REST call.   Add the following lines as the new orchestration step order 10. <OrchestrationStep Order="10" Type="ClaimsExchange">  <ClaimsExchanges> <ClaimsExchange Id="LoyaltyRestExchange" TechnicalProfileReferenceId="LoyaltyRest" />  </ClaimsExchanges>  </OrchestrationStep>   1. Upload your policy to the portal. |
| Create your application policy B2C\_1A\_SignupWithRestAndIdp B2C\_1A\_SignupWithRestAndIdp B2C\_1A\_SignupWithRestAndIdp B2C\_1A\_SignupWithRestAndIdp **B2C\_1A\_SignupWithRestAndIdp** | 1. Copy <your disk>\B2CDemoTools\B2CPolicies\Lab Templates\ Reference\_B2C\_1A\_SignupWithRestAndIdp.xml to your location. 2. Rename Reference\_B2C\_1A\_SignupWithRestAndIdp.xml to <Tenant>\_B2C\_1A\_SignupWithRestAndIdp. 3. Open <Tenant>\_B2C\_1A\_SignupWithRestAndIdp.xml and replace all b2ccharm to the name of your tenant. |
| Add the recorder to the policy | 1. Add two attributes to the root TrustFrameworkPolicy element in the <Tenant>\_B2C\_1A\_SignupWithRestAndIdp policy.  DeploymentMode="Development" UserJourneyRecorderEndpoint="[https://b2crecorder.azurewebsites.net/stream?id](https://na01.safelinks.protection.outlook.com/?url=https%3a%2f%2fb2crecorder.azurewebsites.net%2fstream%3fid&data=01%7c01%7cRonny.Bjones%40microsoft.com%7c8b6721f3c2e24b9a335c08d37ea82324%7c72f988bf86f141af91ab2d7cd011db47%7c1&sdata=iKOYf0GjkzrL93WfJxTMS5d%2buzym1y8i%2fg%2bYH1FzLNA%3d)=<your unique GUID for this policy> |
| Upload the policy | 1. Upload your new policy <Tenant>\_B2C\_1A\_SignupWithRestAndIdp to the portal and check whether it is uploaded without validation errors. Notice that under <RelyingParty> there is a definition for the DefaultUserJourney which is pointing to the user journey SignUpOrSignInWithRestAndIdp you just created. |
| Test the policy in the portal | 1. Goto the B2C portal. In settings select “All Policies”. Now select your policy. In the “run policies” blade press button “Run now”. This will execute your new user journey. |
| View your user journey in the recorder | 1. Goto https://b2crecorder.azurewebsites.net/trace\_102.html?id=<your unique GUID for this policy>   Press Refresh now and the details of the user journey will show up. |

# Exercise 2: Add Wingtip Corp Claims Provider

Each exercise consists of a scenario and learning objectives, the scenario describes the purpose of the exercices, while the objectives are listed and have bullet points.

#### Scenario

We will add the Wingtip corporate claims provider to the extensions policy.

After completing this exercise, you will understand:

* How to specify an Openid Connect provider in your policy?
* Use the new provider into the user journey

The Wingtip Cork identity provider is an Openid Connect provider used by the employees of Wingtip toys to rent games.

We will change our user journey to authenticate the employees and use the userid to collect the loyalty number from the rest api. The claims collected are identical whether Facebook or Wingtip Corp was selected.

|  |  |
| --- | --- |
| Task | Detailed Steps |
| Add the Wingtip Corp claims provider to <tenant>\_B2C\_1A\_Base\_Extensions.xml. | 1. Edit <tenant>\_B2C\_1A\_Base\_Extensions.xml 2. We are going to add a new claims provider into the section:   <ClaimsProviders>  </ClaimsProviders>   1. Open <your disk>\B2CDemoTools\ B2CPolicies\Final\b2ccharm.onmicrosoft.com\_B2C\_1A\_base\_Extensions.xml.  Search for IdentityServer on the page. Copy from the line above <ClaimsProvider> until </ClaimsProvider>. Paste the copied text in your <tenant>\_B2C\_1A\_Base\_Extensions.xml policy in-between <ClaimProviders> </ClaimsProviders>   We now have added a reference to the Wingtip Corp to our policies. |
| Upload crypto keys to the tenant *Product information or explanation about a certain feature goes here.* | 1. We need a client secret to authenticate to the identity server. 2. Run Windows Powershell. Change to the directory where ExploreAdmin is stored. 3. Run the following powershell commands:   Cd <your location>\ExploreAdmin  Import-Module .\ ExploreAdmin.dll  Set-CpimKeyContainer -Tenant b2ccharm.onmicrosoft.com -StorageReferenceId  B2CAuthClientSecret -UnencodedAsciiKey abcdef |
| Change the clientid for your tenant | 1. The clientId [https://login.microsoftonline.com/te/<tenant](https://login.microsoftonline.com/te/%3ctenant)> e.g. https://login.microsoftonline.com/te/b2ccharm.onmicrosoft.com are preset in the identity server as client so replace b2ccharm with the name of your tenant. 2. Also change the IdTokenAudience to the same value as the clientId. The identity server will use the client id to scope the JSON Web Token to the client id. |
| Upload the policy | 1. Upload your policy <Tenant>\_B2C\_1A\_SignupWithRestAndIdp to the portal and check whether it is uploaded without validation errors. |
| Change your application policy B2C\_1A\_SignupWithRestAndIdp B2C\_1A\_SignupWithRestAndIdp to support the Wingtip corp identity provider | 1. We need to extend the identity selection screen to add our new Wingtip Corp identity provider.   In the B2C\_1A\_SignupWithRestAndIdp user journey, goto Orchestration Step order=1. We need to add our provider in the selection screen.  Add <ClaimsProviderSelection TargetClaimsExchangeId="IdentifyServerExchange" />   1. Now we need to map IdentifyServerExchange to the right technical profile of the Wingtip corp identity provider. When you inspect the <ClaimsProvider> definition of identity server you will notice we have a technical profile called ‘IdentityServer’. In Orchestration Step order=2 we will add this mapping by the following line:   <ClaimsExchange Id="IdentifyServerExchange" TechnicalProfileReferenceId="IdentityServer" />  You are now ready to test the Wingtip Corp identity server. |
| Upload the policy | 1. Upload your new policy <Tenant>\_B2C\_1A\_SignupWithRestAndIdp to the portal and check whether it is uploaded without validation errors. |
| Test the policy in the portal | 1. Goto the B2C portal. In settings select “All Policies”. Now select your policy. In the “run policies” blade press button “Run now”. This will execute your new user journey. |
| View your user journey in the recorder | 1. Goto https://b2crecorder.azurewebsites.net/trace\_102.html?id=<your unique GUID for this policy>.   Press Refresh now and the details of the user journey will show up. |

# Appendix

This Appendix provides information about the actual lab manual and labcode, as well as the virtual machine requirements needed for this lab. Use this page to keep information about lab updates / modifications and corrections to the manual, as well as the uniquely defined labcode.

|  |  |  |
| --- | --- | --- |
| Labcode | Manual Version | Last Update |
|  | Version 7 | 12/8/2010 6:38:00 PM |

**Lab Notes**

|  |  |
| --- | --- |
| Description | Details |
|  |  |

**Virtual Machine Requirements**

|  |  |
| --- | --- |
| Virtual Machine Name | Details |
|  |  |