B2C Claim Customization Mini-Lab

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**: | **John Araya** |
| **Bio**: | Senior Software Engineer, Azure AAD B2C |

“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](#_Toc451297828)

[Exercise 1: Adding a custom user attribute to a policy 2](#_Toc451297829)

[Exercise 2: Authenticate and examine a B2C user token 4](#_Toc451297830)

[Appendix 6](#_Toc451297831)

# 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 of the capabilities in Azure AAD B2C that allow you to gather custom claims from your end users.

###### Learning Objectives

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

* Create custom user attributes and configure your applications to gather them
* Understand the differences between how custom attributes are stored in Azure AD, gathered from the end user in the UI, and appear in the user’s B2C token
* View the claims that appear in a B2C user token after authentication

**Estimated time to complete this lab: *10* minutes**

# Exercise 1: Adding a custom user attribute to a policy

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 use the Azure AAD B2C portal to create two custom attributes. We will then configure a policy to gather these attributes, as well as several pre-built attributes, from the user when the policy is invoked.

After completing this exercise, you will understand:

* How to create a custom attribute in the B2C portal
* How to specify which attributes should appear in the directory versus the B2C user token

|  |  |
| --- | --- |
| Task | Detailed Steps |
| Navigate to the Azure B2C portal | 1. Navigate to <https://portal.azure.com> 2. Log in with the tenant administrator account you created as part of the pre-work for this lab 3. Navigate to the Azure AAD B2C portal by selecting “Browse” in the far-left panel, then selecting “Azure AD B2C” |
| Add a custom user attribute  *The B2C admin portal supports adding string-type custom user attributes to your tenant and policies. Advanced policies may be configured with different types of attributes.Product information or explanation about a certain feature goes here.* | 1. In the Settings blade, select “User attributes”. Note that several pre-configured user attributes are available 2. In the “User attributes” blade, click the “Add” button 3. In the “Add an attribute” blade, enter “Gamertag” in the “Name” field 4. Select “String” as the “Data Type”, and enter any string in the “Description” field. The “Description” field is seen only by administrators 5. Repeat this process by adding an additional claim named “VictoryTaunt”. This lab and follow-up labs will assume attributes with these names are available |
| Configure a policy to use several attributes  *Product information or explanation about a certain feature goes here.* | 1. Close the “User attributes” blade. In the main “Settings” blade, select “Sign-up or sign-in policies” 2. Select the policy you created as part of the pre-work for this lab 3. On the top panel of your policy blade, select “Edit” 4. Select the “Sign-up attributes” blade. On the following blade, select the claims below, then click “OK”:    1. City    2. Display Name    3. Email Address    4. Gamertag    5. VictoryTaunt 5. Select the “Application claims” blade. On the following blade, select the claims below, then click “OK”:    1. Display Name    2. Email Addresses    3. Gamertag    4. Identity Provider    5. User is new    6. User’s Object ID 6. Note the differences between the two lists you have selected. There is a difference between the claims that will be queried from the user and stored in the directory versus the claims that will be sent directly to the application as part of the user’s token.    1. In the B2C portal, all “sign-up attributes” queried from the user are always stored in the directory. In advanced policies, you can configure these differently as well. |

# Exercise 2: Authenticate and examine a B2C user token

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, you will execute the policy we have just modified, and examine both the sign-up attributes requested of the user, and the claims that appear in the token after authentication

After completing this exercise, you will understand:

* How custom attributes are gathered from the user
* How different OpenID Connect standard claims and custom claims appear in the B2C user token

|  |  |
| --- | --- |
| Task | Detailed Steps |
| Execute the “sign-up or sign-in” policy  *Note that the fields shown to the user to input their attributes are all input boxes expecting strings. In advanced policies, this can be changed to use other types of input controls.* | 1. Close the policy editing blade. In the main policy blade for your “sign-up or sign-in policy”, ensure that your test application is selected, and the redirect URI is set to <https://aadb2cplayground.azurewebsites.net> 2. Click the “Run Now” button to execute your policy in a new tab 3. On the first screen, you will be asked which type of account you would like to sign up. Assuming you have completed the pre-work for this lab, select the “Facebook” option. 4. Authenticate with Facebook with a user that does not yet exist in your tenant. If you would like to delete an existing user from your tenant, you may do so via the classic Azure portal at <https://manage.windowsazure.com> (Active Directory->Your tenant->Users->Select and delete). You may also do this via AD Graph commands. 5. If this is the first time this user is signing in to this tenant, you will be presented with a profile creation page based on what you have previously configured as “Sign-up attributes” for this policy. Note the following:    1. Several claims have been pre-filled based on the information received for this user from Facebook. The user may choose to modify these claims before signing up to your tenant    2. Changing the email address requires verifying ownership of the new email address    3. The custom user attributes are requested from the user via text input boxes 6. Click “Create” to finish setting up the account. We will use this newly created user in later labs. |
| Examine the token that has been sent to your application  *The token contains claims, including custom claims, based on the configuration you have entered in the B2C portal Product information or explanation about a certain feature goes here.* | 1. You should now be directed to the landing page at <https://aadb2cplayground.azurewebsites.net>. This page will verify the signature on the ID token it receives from B2C, and displays the claims that we held within the token 2. Note that the claims that appear here include standard OpenID Connect claims, such as the “iss” (issuer) claim, as well as additional custom claims based on your configuration. For example:    1. The “Gamertag” claim appears as “extension\_Gamertag”    2. The “idp” claim identifies that the user logged in via Facebook    3. The “User is new” claim is true (this will not be the case for subsequent logins for this user in this tenant) |

# 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 |
|  |  |