WorkshopPLUS – Modern Authentication and Authorization

OAuth2 and OpenIDConnect

Labs prerequisites –

Web browser

Http client, e.g. Fiddler (Composer) or Postman

Student Lab Manual

Instructor Edition (Book Title Hidden Style)

Version 1.0

**Conditions and Terms of Use**

**Microsoft Confidential - For Internal Use Only**

This training package is proprietary and confidential, and is intended only for uses described in the training materials. Content and software is provided to you under a Non-Disclosure Agreement and cannot be distributed. Copying or disclosing all or any portion of the content and/or software included in such packages is strictly prohibited.

The contents of this package are for informational and training purposes only and are 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.

Training package content, including URLs and other Internet Web site references, is subject to change without notice. Because Microsoft must respond to changing market conditions, the content should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication. 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.

© 2016 Microsoft Corporation. All rights reserved.

**Copyright and Trademarks**

© 2016 Microsoft Corporation. All rights reserved.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in 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.

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 Use of Microsoft Copyrighted Content at  
[*http*://www.microsoft.com/about/legal/permissions/](http://www.microsoft.com/about/legal/permissions/)

Microsoft®, Internet Explorer®, and Windows® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Other Microsoft products mentioned herein may be either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. All other trademarks are property of their respective owners.

Contents

[Labs prerequisites: 6](#_Toc492644805)

[Exercise 1: Get access token for an application 7](#_Toc492644806)

[Answers 8](#_Toc492644807)

[Task 1 8](#_Toc492644808)

[Task 2 8](#_Toc492644809)

[Task 3 9](#_Toc492644810)

# Labs prerequisites:

#### Introduction

This lab allows you to try out the various OAuth2 flows and use OpenIDConnect.

#### Objectives

Obtain id token and/or access token for various application topologies.

#### Prerequisites (if applicable)

Web browser

Web client, e.g. Fiddler or Postman

Each task will require some of the following properties:

|  |  |
| --- | --- |
| **Property** | **Value** |
| *URL of authz server* | https://login.microsoftonline.com/ModernAuthn.onmicrosoft.com/ |
| *Tenant id* | c29c8631-b372-4cf1-91f5-76180b30594b |
| *Confidential (web) client id* | 1c635c96-739f-4a45-8020-0ee6ba133681 |
| *Confidential client URI* | https://modernauthn.com/ |
| *Confidential client secret* | foWz-8aGxcD0qGC@Z5qkdx-?ipLoKFF5 |
| *Redirect uri* | https://jwt.ms/ |
| *User id* | [user1@modernauthn.onmicrosoft.com](mailto:user1@modernauthn.onmicrosoft.com) |
| *User password* | M0dern@uth |
| *User id* | user4@modernauthn.onmicrosoft.com |
| *User password* | Phoenix04 |
| *ResourceId* | https://graph.windows.net |

OAuth2 specification: <https://tools.ietf.org/html/rfc6749>

#### Estimated time to complete this lab

30min

#### Scenario

## Exercise 1: Get access token for an application

Use the OAuth2 specification to request an access token to the <https://graph.windows.net> (Azure AD Graph) resource (answers to all tasks are contained at the end of this document) for the following scenarios. Verify token contents using <http://jwt.io> or http://jwt.ms.

For each task, first determine which OAuth2 flow is appropriate. Once you know that, look it up in the spec or open its demo in the demos folder. If you do the latter, replace the parameters with appropriate values. Note that if a redirection is required as part of the flow, you may need to use the browser rather than Fiddler to initiate the request. You will still use Fiddler to see the responses. Flows which do not require redirection and flows using verbs other than GET can be initiated from the Fiddler Composer tab.

Task 1: An unattended batch service

Task 2: Web application (not SPA) user

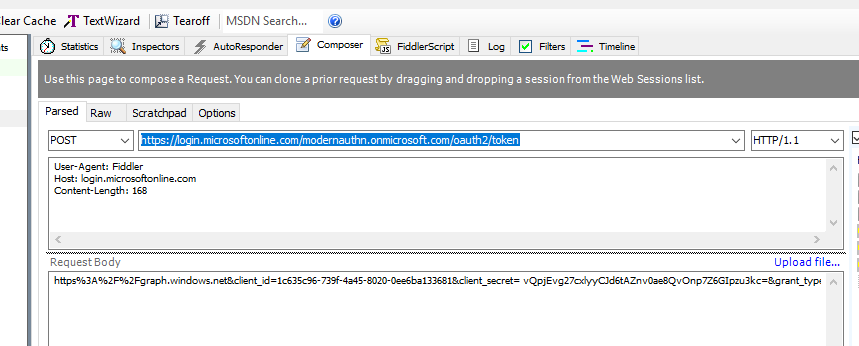
## Answers

### Task 1

Use an http client to send the following **POST** request:

URL: <https://login.microsoftonline.com/modernauthn.onmicrosoft.com/oauth2/token>

Body: https%3A%2F%2Fgraph.windows.net&client\_id=1c635c96-739f-4a45-8020-0ee6ba133681&client\_secret= vQpjEvg27cxlyyCJd6tAZnv0ae8QvOnp7Z6GIpzu3kc=&grant\_type=client\_credentials



### Task 2

Use a web browser to send the following GET request. Keep Fiddler open so that you can intercept the code response for use later on.

URL: https://login.microsoftonline.com/modernauthn.onmicrosoft.com/oauth2/authorize?client\_id=1c635c96-739f-4a45-8020-0ee6ba133681&redirect\_uri= https%3A%2F%2Fjwt.ms%2F&resource=https://graph.windows.net&response\_type=code%20id\_token&scope=openid%20profile&response\_mode=form\_post&nonce=1234567890

Use Fiddler to intercept the OAuth2 code sent to the jwt.ms web site (here used just as a valid http return address). Use Fiddler Composer to exchange the code for an access token:

URL: (POST) https://login.microsoftonline.com/modernauthn.onmicrosoft.com/oauth2/token

Body: client\_id=1c635c96-739f-4a45-8020-0ee6ba133681&client\_secret=vQpjEvg27cxlyyCJd6tAZnv0ae8QvOnp7Z6GIpzu3kc%3D&code***=<<replace with code value from previous request>>****&*grant\_type=authorization\_code&redirect\_uri=https%3A%2F%2Fjwt.ms%2F

### Task 3

Use a web browser to send the following GET request. Keep Fiddler open so that you can intercept the token response.

URL: GET [https://login.microsoftonline.com/modernauthn.onmicrosoft.com/oauth2/authorize?response\_type=id\_token&client\_id=1c635c96-739f-4a45-8020-0ee6ba133681&redirect\_uri=https%3A%2F%2Fjwt.ms%2F&resource=https%3A%2F%2Fgraph.windows.net&state=](https://login.microsoftonline.com/modernauthn.onmicrosoft.com/oauth2/authorize?response_type=id_token&client_id=1c635c96-739f-4a45-8020-0ee6ba133681&redirect_uri=https%3A%2F%2Fmicrosoft.com%2F&resource=https%3A%2F%2Fgraph.windows.net&state=)XYZ&nonce=123

(Please remove any extra spaces that may be included in a copy/paste using the above url). Use Fiddler to intercept the OIDC token sent to the microsoft.com web site.