WorkshopPLUS – Modern Authentication and Authorization

Azure AD

Labs prerequisites –

Web browser

Ability to install applications (PowerShell module)

Student Lab Manual

Instructor Edition (Book Title Hidden Style)

Version 2.0

**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: 1](#_Toc106186845)

[Exercise 1: Access an Azure AD tenant 1](#_Toc106186846)

[Task 1 – verify your directory status 1](#_Toc106186847)

[Task 2 – Create a new Azure AD tenant 1](#_Toc106186848)

[Exercise 2 – Populate AAD tenant 1](#_Toc106186849)

[Task 1 – Create users 1](#_Toc106186850)

[Task 2 – Create Groups 1](#_Toc106186851)

[Task 3 – Add with lower privilege account 1](#_Toc106186852)

[Exercise 3 – Manage an application 1](#_Toc106186853)

[Task 1 – Register a user-facing application 1](#_Toc106186854)

[Task 2 – Register an API application 1](#_Toc106186855)

[Task 3 – Restrict access to the application 1](#_Toc106186856)

[Task 4 – Test access 1](#_Toc106186857)

[Exercise 4: Microsoft Graph 1](#_Toc106186858)

[Task 1 – use the Graph Sandbox 1](#_Toc106186859)

[Exercise 5: Microsoft Graph PowerShell 1](#_Toc106186860)

[Task 1 – Start PowerShell ISE and install Graph SDK module 1](#_Toc106186861)

[Task 2 – connect to your Azure AD tenant 1](#_Toc106186862)

[Task 3 – work with objects in your tenant 1](#_Toc106186863)

# Labs prerequisites:

#### Introduction

This lab guides you through some common Azure AD tasks.

#### Objectives

Manage application related content of an Azure AD tenant.

#### Prerequisites (if applicable)

Edge or Chrome Web browser

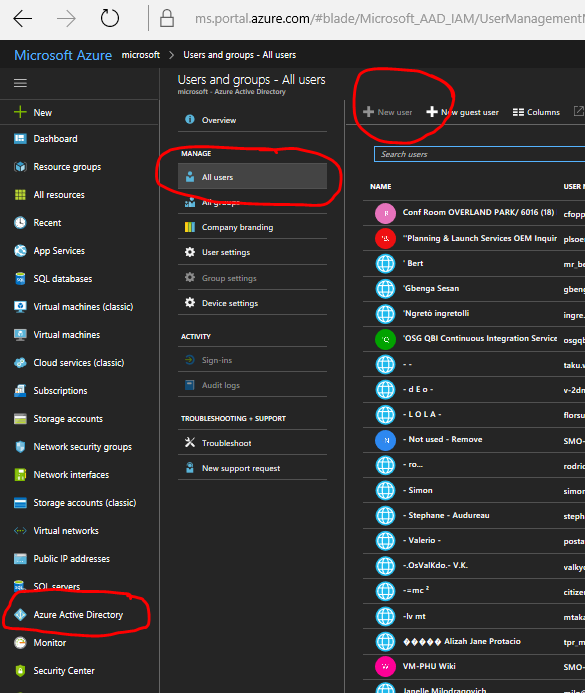
#### Estimated time to complete this lab

30 mins

# Exercise 1: Access an Azure AD tenant

### Task 1 – verify your directory status

If you think you already have an Azure AD tenant, access it through the <https://aad.portal.azure.com> and verify your status. If you are NOT a global admin in the tenant you have access to, you will need to create a new tenant. To verify your access level, select the *Azure Active Directory* option from the TOC (left) pane, *Users and Groups* option and then *All Users*. If the *‘+ New user’* option is greyed out, you are not a global admin.



### Task 2 – Create a new Azure AD tenant

If based on the above test, you do not have an Azure AD tenant that you can control, please create one using instructions in: <https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-howto-tenant>

# Exercise 2 – Populate AAD tenant

### Task 1 – Create users

Use instructions in <https://docs.microsoft.com/en-us/azure/active-directory/add-users-azure-active-directory> to create three users in your tenant: [manager@yourtenantname.onmicrosoft.com](mailto:manager@yourtenantname.onmicrosoft.com), [user1@yourtenantname.onmicrosoft.com](mailto:user1@yourtenantname.onmicrosoft.com) and [user2@yourtenantname.onmicrosoft.com](mailto:user2@yourtenantname.onmicrosoft.com). Make sure that your record their initial passwords somewhere for future use. Give the *manager* user a User Administrator AzureAD role.

To test logins with these users, open <https://portal.office.com> in a different browser or in-private/confidential instance of the same browser. This way you will avoid the site re-using your current authentication cookies. Login with each of the three credentials. If you are getting past the login and to an Office error page, your login is working.

### Task 2 – Create Groups

Use instructions in <https://docs.microsoft.com/en-us/azure/active-directory/active-directory-groups-create-azure-portal> to create two security groups: *managers* and *users*. Assign the *manager* user created above to the *managers* group and the *user1* to as Owner (not Member) of the *users* group (do not add user2 yet!).

### Task 3 – Add with lower privilege account

Login to <https://aad.portal.azure.com> as user1. Using the same instructions as above, add user2 to the users group. This features enables non-admin users to manage groups they own.

# Exercise 3 – Manage an application

### Task 1 – Register a user-facing application

1. Install App Launcher Chrome extension in your edge or Chrome browser:

|  |
| --- |
| https://chrome.google.com/webstore/detail/azure-ad-app-launcher/dgfmoiiecjedmgimnhcchpcgbopppeil |

1. Use Azure Portal (https://portal.azure.com) to register an application:
   1. Name the app ‘*WebApp1’* and give it a Web reply url with value ‘https://oidcdebugger.com/debug’
   2. In the Authentication tab and turn both checkboxes on, Save it
   3. Use the App Launcher to request an id token for the applications.

### Task 2 – Register an API application

1. Use Azure Portal (https://portal.azure.com) to register an application:
   1. Name the app ‘*WebAPI1’*. It does not need a redirect uri – it will not use passive authentication to get tokens
   2. Select *Expose an API* option
   3. Select + Add scope
   4. Replace the Guid in the Application ID with a friendly name for your API, e.g.: *api://myapi.* Select *Save and continue*
   5. Give the scope a name and description of your choice, e.g. *Order.Create* for value.
   6. You may want to create one or more other scope definitions
2. Go to the main menu for your AAD and select App Registration then your user-facing app (WebApp1).
3. Use App Launcher to request tokens for this app: select id\_token token; in the scope enter the names of scopes you defined for your API
4. Are you getting both id and access tokens? Does the access token have the right scope(s)?

### Task 3 – Restrict access to the application

Sign in as tenant admin to <https://aad.portal.azure.com> and select the **Enterprise applications** tab. Then select **All applications** and find the application you have just added (e.g. enter *WebApplication1* in the search field). Select the **Properties** tab and switch *‘Requires user assignment’* to Yes. Select the **Users and groups** tab and click on the **Add user** option. Select either the admin user or the admin group and add it as permitted to access this application.

### Task 4 – Test access

Use the App Launcher from the browser to run your ‘application’ and try signing in as either admin or user1 to test whether AAD is correctly applying your restrictions (*admin* user should be able to sign in, *user1* should not). Note: you should both logout and close the browser window to clear all authn cookies.

# Exercise 4: Microsoft Graph

### Task 1 – use the Graph Sandbox

Navigate to <https://developer.microsoft.com/en-us/graph/graph-explorer> and sign in using the admin user created in Exercise 1. Press Run Query to execute the pre-entered <https://graph.microsoft.com/v1.0/me/> query. You should see the admin user’s attributes.

Experiment with some additional queries using the Sample Queries in the left tab. Also:

<https://graph.microsoft.com/v1.0/users?$filter=startswith(mail,'admin')>

<https://graph.microsoft.com/v1.0/groups?$select=mailNickName>

# Exercise 5: Microsoft Graph PowerShell

### Task 1 – Start PowerShell ISE and install Graph SDK module

From the Start menu find PowerShell ISE application and start it in admin mode (unless you know you have the SDK module already installed).

Enter command

|  |
| --- |
| *Install-Module Microsoft.Graph -Scope CurrentUser* |

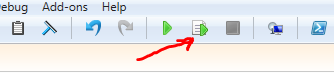
in the command window (usually bottom left corner, blue-background pane). Accept the message box permission to complete the install.

Before using the above command you may (depending on your company policy) change the PowerShell execution policy as follows:

|  |
| --- |
| Set-ExecutionPolicy -Scope Process -ExecutionPolicy Bypass |

### Task 2 – connect to your Azure AD tenant

.Enter the following command into the top-left (Script) pane, then select it and press the Run Selection (F8) button (marked below).



|  |
| --- |
| *Connect-MgGraph -TenantId "xxxxxxxx" -Scopes “User.Read.All”* |

You will be prompted for your credentials. Use the admin user created in Exercise 1 to sign in. On successful completion you should see:

|  |
| --- |
| Welcome To Microsoft Graph! |

### Task 3 – work with objects in your tenant

Experiment with some of the commands using the following mapping of Http verbs to PowerShell command prefixes:

| **HTTP method** | **Command verb** | **Example** |
| --- | --- | --- |
| GET | Get | Get-MgUser [API reference](https://docs.microsoft.com/en-us/graph/api/user-get?view=graph-rest-1.0&preserve-view=true) |
| POST | New | New-MgUserMessage [API reference](https://docs.microsoft.com/en-us/graph/api/user-post-messages?view=graph-rest-1.0&preserve-view=true) |
| PUT | New | New-MgTeam [API reference](https://docs.microsoft.com/en-us/graph/api/team-put-teams?view=graph-rest-1.0&preserve-view=true) |
| PATCH | Update | Update-MgUserEvent [API reference](https://docs.microsoft.com/en-us/graph/api/event-update?view=graph-rest-1.0&preserve-view=true) |
| DELETE | Remove | Remove-MgDriveItem [API reference](https://docs.microsoft.com/en-us/graph/api/driveitem-delete?view=graph-rest-1.0&preserve-view=true) |

*Get-MgUser*

*Get-MgApplication*

[Use Postman with the Microsoft Graph API - Microsoft Graph | Microsoft Learn](https://learn.microsoft.com/en-us/graph/use-postman)