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 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](#_Toc51156964)

[Exercise 1: Access an Azure AD tenant 7](#_Toc51156965)

[Task 1 – verify your directory status 7](#_Toc51156966)

[Task 2 – Create a new Azure AD tenant 7](#_Toc51156967)

[Exercise 2 – Populate AAD tenant 8](#_Toc51156968)

[Task 1 – Create users 8](#_Toc51156969)

[Task 2 – Create Groups 8](#_Toc51156970)

[Task 3 – Add with lower privilege account 8](#_Toc51156971)

[Task 4 – Add an application 8](#_Toc51156972)

[Task 5 – Restrict access to the application 8](#_Toc51156973)

[Task 5 – Test access 9](#_Toc51156974)

[Exercise 3: Azure AD PowerShell 10](#_Toc51156975)

[Task 1 – Start PowerShell ISE and install AzureAD module 10](#_Toc51156976)

[Task 2 – connect to your Azure AD tenant 10](#_Toc51156977)

[Task 3 – work with objects in your tenant 10](#_Toc51156978)

[Exercise 4: Microsoft Graph 11](#_Toc51156979)

[Task 1 – use the Graph Sandbox 11](#_Toc51156980)

# 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)

Web browser

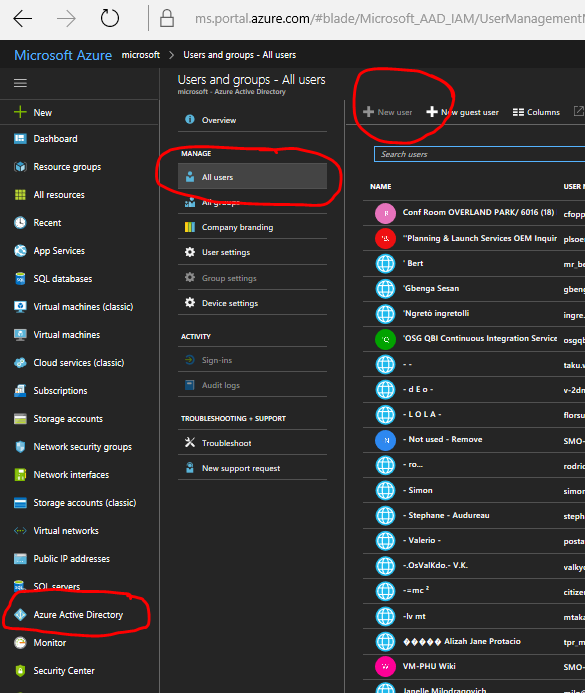
#### Estimated time to complete this lab

45mins

# 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.

### Task 4 – Add an application

Follow instructions in <https://blogs.msdn.microsoft.com/azuredev/2017/03/29/4-ways-of-adding-your-application-to-azure-active-directory/> to create a new web application and add it to your tenant. Use the first method using Visuals Studio.

### Task 5 – 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 5 – Test access

From Visual Studio 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 3: Azure AD PowerShell

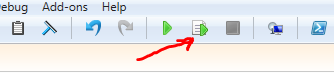
### Task 1 – Start PowerShell ISE and install AzureAD module

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

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

### 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-AzureAD

You will be prompted for your credentials. Use the admin user created in Exercise 1 to sign in. If the login was successful, you should see output like this:

Account Environment TenantId TenantDomain AccountType

------- ----------- -------- ------------ -----------

mrochon@mr.com AzureCloud cf6c572c-…23d040495 mr.onmicrosoft.com User

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

Experiement with some of the commands listed in the online reference: https://docs.microsoft.com/en-us/powershell/azure/active-directory/install-adv2?view=azureadps-2.0, e.g:

Get-AzureADUser

Get-AzureADApplication

Create new user: <https://docs.microsoft.com/en-us/powershell/azure/active-directory/new-user-sample?view=azureadps-2.0>

# 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>