# Lab Answer Key: Module 9: Implementing Azure Active Directory

# Lab: Implementing Azure AD

## Exercise 1: Administering Active AD

#### Task 1: Create directories

1. Ensure that the MSL-TMG1 and 20533C-MIA-CL1 virtual machines are both running, and then sign in to 20533C-MIA-CL1 as **Student** with the password **Pa$$w0rd**.
2. Start Internet Explorer, browse to **http://manage.windowsazure.com**, and then sign in by using the Microsoft account that is associated with your Azure subscription.
3. In the navigation panel on the left, click **ACTIVE DIRECTORY**.
4. Click **New**, click **DIRECTORY**, and then click **CUSTOM CREATE**.
5. In the **Add directory** dialog box, enter the following settings, and then click **Complete** (check mark):

* **DIRECTORY**: Create new directory
* **NAME**: Adatum
* **DOMAIN NAME**: *Use your initials* + *the directory name* + *random numbers* (for example, abcadatum123456). If you get the **The domain is not unique** message, change the numbers until you get a green check mark.
* **COUNTRY OR REGION**: United States

#### Task 2: Activate Azure AD Premium trial

1. In the navigation panel on the left, click **ACTIVE DIRECTORY**.
2. Click the **Adatum** directory.
3. Click **Licenses**.
4. Click **Try Azure Active Directory premium now**.
5. In the Activate Azure AD Premium trial pop-up window, click the check mark to confirm the selection.
6. Click the **Click** **here** **to refresh** link, and then verify that Azure AD Premium is activated.

#### Task 3: Manage users by using the Azure portal

1. On the **active** **directory** page, click **Adatum**.
2. On the **Adatum** page, click **USERS**.
3. Click the **ADD USER** button at the bottom of the page.
4. In the **Tell us about this user** dialog box, enter the following settings, and then click **Next**:

* **TYPE OF USER**: New user in your organization
* **USER NAME**: rdesforges

1. In the **user profile** dialog box, enter the following settings, and then click **Next**:

* **FIRST NAME**: Remi
* **LAST NAME**: Desforges
* **DISPLAY NAME**: Remi Desforges
* **ROLE**: User
* **Enable Multi-Factor Authentication**: Do not select

1. Click **Create**.
2. On the **Get temporary password** page, note the new password.
3. Click **Complete** (check mark).
4. Click **ADD USER**.
5. In the **Tell us about this user** dialog box, enter the following settings, and then click **Next**:

* **TYPE** **OF USER**: New user in your organization
* **USER NAME**: kgruber

1. In the **user** **profile** dialog box, enter the following settings, and then click **Next**:

* **FIRST NAME**: Karen
* **LAST NAME**: Gruber
* **DISPLAY NAME**: Karen Gruber
* **ROLE**: Global Admin
* **ALTERNATE EMAIL ADDRESS**: Type the email address of the Microsoft account that is the Service Administrator or a Co-Administrator of your Azure subscription.
* **Enable Multi-Factor Authentication**: Do not select

1. Click **Create**.
2. On the **Get temporary password** page, note the new password.
3. Click **Complete** (check mark).
4. At the top-right corner of the page, click your Azure subscription name, and then click **Sign** **Out**.
5. On the **You have been signed out** page, click **SIGN IN**.
6. On the **Microsoft** **Azure** page, click **Use another account**, and then sign in to Azure by using the following credentials (where *XXXadatumXXX* is your unique Adatum number):

* **Username**: kgruber@XXXadatumXXX.onmicrosoft.com
* **Password**: Enter the temporary password you noted above.

1. On the **Update your password** page, in the **Current password** box, type the temporary password. In the **New password** and **Confirm password** boxes, type **Pa$$w0rd123**, and click **Update password and sign in**. > **Note:** Although kgruber is a Global Administrator, the attempt to sign in to the portal fails and the following message appears: We were unable to find any Azure subscriptions where you are a service administrator or co-administrator. This is because this account is not the Service Administrator or a Co-Administrator of the Azure subscription. This is by design.
2. Close Internet Explorer.

#### Task 4: Manage groups by using the Azure portal

1. Start Internet Explorer, browse to **https://manage.windowsazure.com**, and sign in by using the Microsoft account that is associated with your Azure subscription.
2. In the navigation panel on the left, click **ACTIVE DIRECTORY**.
3. Click **Adatum**.
4. Click **Configure**.
5. Scroll down and in the group management, enable **Delegated Group Management Enabled** by selecting **Yes.**
6. Click **Save**.
7. Click **GROUPS**.
8. Click **ADD A GROUP**.
9. In the **Add Group** dialog box, enter the following settings, and then click **Complete**:

* **NAME**: Sales
* **DESCRIPTION**: Sales team

1. Click **Sales**.
2. Click **ADD MEMBERS**.
3. In the **Add members** dialog box, click **Remi Desforges**, and click **Complete**.
4. Click the **Back** button.
5. Click **ADD GROUP**.
6. In the **Add Group** dialog box, enter the following settings, and then click **Complete**:

* **NAME**: Marketing
* **DESCRIPTION**: Marketing employees

1. Click **Marketing**.
2. CLICK **ADD** **Members**.
3. In the **Add members** dialog box, click **Remi Desforges**, and click **Complete** (check mark).
4. Click the **Back** button.
5. Click **ADD GROUP**.
6. In the **Add Group** dialog box, enter the following settings, and then click **Complete**:

* **NAME**: Sales and Marketing
* **DESCRIPTION**: Sales and Marketing employees

1. Click **Sales and Marketing**.
2. Click **ADD MEMBERS**.
3. In the **Add members** dialog box, click the **SHOW** drop-down box, select **Groups**, and click the **Confirm** button to the right of the **SHOW** drop-down box.
4. Click **Marketing**.
5. Click **Sales**.
6. Click **Complete** (check mark).
7. Click the **Back** button.

#### Task 5: Manage users and groups by using Azure PowerShell

1. On the taskbar, right-click **Windows PowerShell**, and then click **Run ISE as Administrator**.
2. If a **User Account Control** dialog box appears, click **Yes**.
3. In the PowerShell ISE, click **File**, and then click **Open**.
4. In the **Open** dialog box, browse to \*\*D:09\*\*.
5. Click **ExampleCommands.ps1**, and then click **Open**.
6. If the script pane is not visible, on the **View** menu, click **Show Script Pane**.
7. In the PowerShell ISE, in the command prompt pane, enter the following command and press Enter:

Connect-MsolService

1. In the **Enter Credentials** dialog box, sign in as **kgruber@XXXadatumXXX.onmicrosoft.com** (where *XXXadatumXXX* is your unique Adatum domain name) with a password of **Pa$$w0rd123**, and then click **OK**.
2. In the PowerShell ISE, in the script pane, locate the following code:

New-MsolUser -UserPrincipalName mledford@<#Copy your Azure Directory name here#>.onmicrosoft.com -DisplayName "Mario Ledford" -FirstName "Mario" -LastName "Ledford" -Password 'Pa$$w0rd123' -ForceChangePassword $false -UsageLocation "US"

1. Replace **<#Copy your Azure Directory name here#>** with your Azure AD directory name.
2. In the PowerShell ISE, in the script pane, select the code that you just edited.
3. On the toolbar, click the **Run Selection** button and wait for the script to complete.
4. In the PowerShell ISE, in the command prompt pane, enter the following command, and then press Enter:

Get-MsolUser

1. In the PowerShell ISE, in the script pane, locate the following code and select it:

New-MsolGroup -DisplayName "Azure team" -Description "Adatum Azure team users"

1. On the toolbar, click the **Run Selection** button and wait for the script to complete.
2. In the PowerShell ISE, in the command prompt pane, enter the following command, and press Enter:

Get-MsolGroup

1. In the PowerShell ISE, in the script pane, locate the following code and select it:

$group = Get-MsolGroup | Where-Object {$\_.DisplayName -eq "Azure team"}

1. On the toolbar, click the **Run Selection** button, and wait for the script to complete.
2. In the PowerShell ISE, in the script pane, locate the following code and select it:

$user = Get-MsolUser | Where-Object {$\_.DisplayName -eq "Mario Ledford"}

1. On the toolbar, click the **Run Selection** button, and wait for the script to complete.
2. In the PowerShell ISE, in the script pane, locate the following code and select it:

Add-MsolGroupMember -GroupObjectId $group.ObjectId -GroupMemberType "User" -GroupMemberObjectId $user.ObjectId

1. On the toolbar, click the **Run Selection** button, and wait for the script to complete.
2. In the PowerShell ISE, in the script pane, locate the following code and select it:

Get-MsolGroupMember -GroupObjectId $group.ObjectId

1. On the toolbar, click the **Run Selection** button, and wait for the script to complete.
2. Switch to Internet Explorer.
3. Click **USERS**, and verify that **Mario Ledford** appears in the list of users.
4. Click **GROUPS**, and verify that **Azure team** appears in the list of groups.

**Result**: After completing this exercise, you should have created some pilot users and groups in Azure AD by using the Azure portal and Microsoft Azure Active Directory Module for Windows PowerShell. You will also enable the Azure AD Premium functionality.

## Exercise 2: Configuring SSO

#### Task 1: Add directory applications and configure SSO

1. On the **Adatum** directory page, click **APPLICATIONS**.
2. Click **ADD**.
3. In the **What do you want to do?** dialog box, click **Add an application from the gallery**.
4. In the **Add an application for my organization to use** dialog box, in the search box, type **Microsoft**, and then press Enter.
5. Click **Microsoft Account (Windows Live)**, in the **Display** Name text box, type **Microsoft Account**, and then click the check mark.
6. Verify that **Configure single sign-on** is enabled by default.
7. Click **Assign** **accounts**.
8. From the **Show** drop-down menu, select **AllUsers**, and then click the check mark. In the user list, click **Mario Ledford**.
9. At the bottom of the screen, click **ASSIGN**.
10. In the **Assign Users** dialog box, select **I want to enter Microsoft Account credentials on behalf of the user**.
11. In the **Email Address** box, type the email address of the Microsoft account associated with your Azure subscription. In the **Password** box, type the corresponding password, and then click the check mark.
12. Above Microsoft account, click the **Back** arrow.
13. At the bottom of the screen, click **ADD**.
14. In the **What do you want to do?** dialog box, click **Add an application from the gallery**.
15. In the **Add an application for my organization to use** dialog box, in the search box, type **Skype**, and then press Enter.
16. Click **Skype**, in the **Display** **Name** text box, type **Skype**, and then click the check mark.
17. Verify that **Configure single sign-on** is enabled by default.
18. Click **Assign** **accounts**.
19. From the **Show** drop-down menu, select **All** **Users**, and then click the check mark.
20. In the user list, click **Mario Ledford**.
21. At the bottom of the screen, click **ASSIGN**.
22. In the **Assign Users** dialog box, clear **I want to enter Skype credentials on behalf of the user**, and then click the check mark.
23. In the **Email Address** box, type the email address of the Microsoft account associated with your Azure subscription. In the **Password** box, type the corresponding password, and then click the check mark.
24. On the top right side of the page, click your Azure account name, and then click **Sign out**.

#### Task 2: Test SSO

1. Close and restart Internet Explorer. In the address box, type **https://account.activedirectory.windowsazure.com/applications**, and then press Enter.
2. On the **Microsoft** **Azure** page, click **Use another account**.
3. On the **Microsoft Azure** page, enter the following credentials (where *XXXadatumXXX* is your unique Adatum domain name), and then click **Continue**:

* Username: **mledford@XXXadatumXXX.onmicrosoft.com**
* Password: **Pa$$w0rd123**

1. On the applications page, click the ellipsis (...) next to **Microsoft Account**. Note the options to update the credentials and report a problem about the Microsoft account.
2. On the applications page, click **Microsoft Account**.
3. In the **Microsoft Account** dialog box, click **Install Now**.
4. On the Internet Explorer bar, click **Run**.
5. In the **Access Panel Extension** dialog box, on the **Welcome to the Access Panel Extension Setup Wizard** page, click **Next**.
6. On the **Install Access Panel Extension** page, click **Install**.
7. In the **User Account Control** dialog box, click **Yes**.
8. In the **Access Panel Extension** dialog box, on the **Completed the Access Panel Extension Setup Wizard** page, click **Finish**.
9. On the Internet Explorer bar, click **Enable**.
10. Close Internet Explorer.
11. On the taskbar, click **Internet Explorer**.
12. In Internet Explorer, in the address box, type **https://account.activedirectory.windowsazure.com/applications**, and then press Enter.
13. On the **Microsoft** **Azure** page, enter the following credentials (where *XXXadatumXXX* is your unique Adatum domain name), and click **Continue**.

* Username: **mledford@XXXadatumXXX.onmicrosoft.com**
* Password: **Pa$$w0rd123**

1. On the **applications** page, click **Microsoft** **Account**, and then in the Microsoft account, enter your subscription credentials. > **Note:** If you are prompted to sign in again, use the credentials for your subscription account.
2. Verify that you signed in to your Microsoft account based on the credentials that have been entered on behalf of the user.
3. Switch to the **Access Panel Applications** tab.
4. On the **applications** page, click **Skype**; note that you are now prompted for credentials, because you did not enter any credentials on behalf of the user when configuring SSO.
5. Close the **Skype** dialog box.
6. Close Internet Explorer.

**Result**: After completing this exercise, you should have installed and configured a test application and validated the SSO experience.

## Exercise 3: Configuring Multi-Factor Authentication

#### Task 1: Configure Multi-Factor Authentication

1. On the taskbar, click **Internet Explorer**.
2. In Internet Explorer, in the address box, type **https://manage.windowsazure.com**, and then press Enter.
3. On the **Microsoft Azure** page, click your Azure subscription name; if your Azure subscription is not shown, click **Use another account**.
4. On the **Sign in** page, enter the credentials for the Microsoft account associated with your Azure subscription, and then click **Sign in**.
5. In the navigation pane, scroll down, and click **ACTIVE DIRECTORY**.
6. Click the right arrow next to the **Adatum** directory.
7. Click **CONFIGURE**.
8. Under **multi-factor authentication**, click **Manage service settings**.
9. If you get a **Sign in** page, enter the Microsoft account associated with your Azure subscription, and then click **Sign in**.
10. On the **multi-factor** **authentication** page, click **users**.
11. In the **users** list, select the check box for **Karen Gruber**, and in the **quick steps** section, click **Enable**.
12. On the **About enabling multi-factor auth** page, click **enable** **multi-factor** **auth**.
13. On the **Updates successful** page, click **close**.
14. In Internet Explorer, close the **Multi-factor** **Authentication** tab.
15. Close Internet Explorer.

#### Task 2: Test Multi-Factor Authentication

1. On the taskbar, click **Internet Explorer**.
2. In Internet Explorer, in the address box, type **https://account.activedirectory.windowsazure.com/applications**, and then press Enter.
3. On the **Microsoft** **Azure** page, click **Use another account**.
4. On the **Sign in** page, enter the following credentials (where *XXXadatumXXX* is your unique Adatum domain name), and then click **Sign in**:

* Username: **kgruber@XXXadatumXXX.onmicrosoft.com**
* Password: **Pa$$w0rd123**

**Note:** Note the following message: Your admin has required that you set up this account for additional security verification.

1. Click **Set it up now**.
2. On the **additional security verification** page, click in the first box, and note the contact method options.
3. Optional step: If you have access to a mobile phone in the classroom, and have a signal or data connection, you can complete the additional security verification steps on the **additional** **security** **verification** page.

**Result**: After completing this exercise, you should have configured Multi-Factor Authentication for administrators.

## Exercise 4: Configuring SSO from a Windows 10-based computer that is joined to Azure AD

#### Task 1: Join a Windows 10-based computer to Azure AD

1. On the taskbar, click **Internet Explorer**.
2. In Internet Explorer, in the address box, type **https://manage.windowsazure.com**, and then press Enter. If required, sign in by using the Microsoft account that is associated with your Azure subscription.
3. On MIA-CL1, click the Start button, and then click **Settings**.
4. In **Settings**, click **Accounts**, and then click **Work Access**.
5. On the **Connect to work or school** page, click **Join or leave** **an** **organization**. This will redirect you to the About section of the **SYSTEM Settings**.
6. Click **Join Azure AD**.
7. On the **What** **happens** **next** page, click **Next**.
8. On the **Let's get you signed in** page, type the following credentials, and then click **Sign in**:

* Username: **kgruber@XXXadatumXXX.onmicrosoft.com**
* Password: **Pa$$w0rd123**

1. On the **Help us protect your account** page, click **Set it up now**.
2. On the **Verify your identity** page, from drop-down menu, select **Phone call**.
3. In the **Select your country or region** drop-down list, select the country or region where your phone is registered. In the **Phone number** text box, type your phone number. Click **Next**.
4. Press the # key on your phone to complete verification.
5. On the **Keep your existing apps working** page, click **Next**.
6. On the **Make sure this is your organization** page, click **Join**.
7. On the **All finished** page, click **Finish**.
8. Switch back to Internet Explorer.
9. In the navigation panel on the left, click **ACTIVE DIRECTORY**.
10. Select the **Adatum** directory.
11. Click **Users**, and then select the **Karen Gruber** account.
12. Click the **Devices** tab.
13. On the **You are about to view private user data** page, select **it is acceptable for admins in my organization to view this data**, and then click **OK** (confirm selection).
14. From the **View** drop-down menu, select **Devices**.
15. Verify that **MIA-CL1** is listed.
16. Sign out of **MIA-CL1**.

#### Task 2: Authenticate to Azure from a Windows 10 Azure-joined computer

1. Sign in to MIA-CL1 by using the following credentials:

* Username: **kgruber@XXXadatumXXX.onmicrosoft.com**
* Password: **Pa$$w0rd123**

1. On the **Set up a PIN** page, click **Setup** **PIN**.
2. On the **Set up a PIN** page, type and retype a four-digit PIN, and then click **OK**. Note that you cannot use a common number pattern (such as four identical digits).
3. Start Internet Explorer, and then go to **https://portal.office.com**.
4. Verify that you are automatically signed in as Karen Gruber by using SSO.
5. Close all open applications and sign out from 20533C-Mia-CL1.

#### Task 3: Reset the environment

1. Sign in to 20533C-Mia-CL1 as **Student** with the password **Pa$$w0rd**.
2. On the taskbar, right-click **Windows** **PowerShell**, and then click **Run as administrator**.
3. In the **User Account Control** dialog box, click **Yes**.
4. In the PowerShell ISE, in the command prompt pane, enter the following command, and then press Enter:

Reset-Azure

1. When prompted (twice), sign in by using the Microsoft account associated with your Azure subscription.
2. If you have multiple Azure subscriptions, select the one you want the script to target.
3. When prompted for confirmation, type **y.**

**Note:** This script removes Azure services in your subscription. Therefore, we recommend that you use an Azure trial pass that was provisioned specifically for this course and not your own Azure account. The script resets your Azure environment so that it is ready for the next lab. The script removes all storage accounts, virtual machines, virtual networks, cloud services, and resource groups containing these resources.

**Result**: After completing this exercise, you should have joined the Mia-CL1 computer to Azure AD and tested the SSO access to the resources in the cloud.

©2016 Microsoft Corporation. All rights reserved.

The text in this document is available under the [Creative Commons Attribution 3.0 License](https://creativecommons.org/licenses/by/3.0/legalcode), additional terms may apply. All other content contained in this document (including, without limitation, trademarks, logos, images, etc.) are **not** included within the Creative Commons license grant. This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it. Some examples are for illustration only and are fictitious. No real association is intended or inferred. Microsoft makes no warranties, express or implied, with respect to the information provided here.