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

# Lab: Implementing Azure Active Directory

## Exercise 1: Administering Azure AD

#### Task 1: Create an Azure Active Directory tenant

1. Ensure that you are signed in to MIA-CL1 as **Student** with the password **Pa55w.rd**.
2. Start Mirosoft Edge, browse to the Azure portal at [**https://portal.azure.com**](https://portal.azure.com), and then sign in using the Microsoft account that is the Service Administrator of your subscription.
3. In the Azure portal, in the hub menu, click **+ Create a resource**, click **Identity** and then, click **Azure Active Directory**.
4. On the **Create directory** blade, specify the following and click **Create**:

* Organization name: **Adatum**
* Initial domain name: *a unique, valid name*
* Country or region: **United States**

1. Leave Mirosoft Edge open and wait until the Azure Active Directory tentant is provisioned. Note the unique name you specified, since you will need it later in this task.

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

1. Refresh the Mirosoft Edge window displaying the Azure portal. Next, click the **Directory + subscription** filter icon appearing directly to the left of your name in the upper right corner of the Azure portal and, in the **Directory + Subscription** pane, click the name of the Azure Active Directory tenant you created in the previous task.
2. In the hub menu of the Azure portal, click **Azure Active Directory**. This will display the **adatum** Azure Active Directory tenant blade.
3. Click **Start a free trial**.
4. In the **Azure AD and Office 365** section, click **Get a free trial for Azure AD Premium**.
5. On the **Activate** blade, in the **AZURE AD PREMIUM P2** section, click **Free trial**.
6. On the **Activate Azure AD Premium P2 trial**, click **Activate**.
7. Wait until the Azure AD Premium trial is successfully activated.

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

1. Navigate back to the **adatum** Azure Active Directory tenant blade.
2. On the adatum blade, click **Users**.
3. Click **+ New user**
4. On the **User** blade, specify the following settings (where ***domain-name*** is the name you assigned to the Azure Active Directory tenant in the first task of this exercise):

* Name: **Remi Desforges**
* User name: **rdesforges@*domain-name*.onmicrosoft.com**

1. Click **Profile** and, on the **Profile** blade, specify the following settings and click **OK**:

* First Name: **Remi**
* Last Name: **Desforges**

1. Accept the default **Properties**, **Groups** and **Directory role** settings, click the **Show Password** checkbox and note the temporary password.
2. Click **Create**.
3. Click **+ New user**
4. On the **User** blade, specify the following settings (where ***domain-name*** is the name you assigned to the Azure Active Directory tenant in the first task of this exercise):

* Name: **Karen Gruber**
* User name: **kgruber@*domain-name*.onmicrosoft.com**

1. Click **Profile** and, on the **Profile** blade, specify the following settings and click **OK**:

* First Name: **Karen**
* Last Name: **Gruber**

1. Accept the default **Properties** and **Groups** settings and click **Directory role**.
2. On the **Directory role** blade, click **Global administrator** and click **OK**.
3. Click the **Show Password** checkbox and note the temporary password.
4. Click **Create**.
5. Start an InPrivate Mirosoft Edge session and browse to the Azure portal at [**https://portal.azure.com**](https://portal.azure.com).
6. When prompted to sign in, specify the full user name (including the @\*domain-name\*.onmicrosoft.com suffix) of Remi Desforges' account and the corresponding temporary password.
7. On the **Update your password** page, in the **Current password** box, type again the temporary password. In the **New password** and **Confirm password** text boxes, type a new password, and click **Update password and sign in**. Take a note of the new password.

**Note:** If you receive the message **We've seen that password too many times before. Choose something harder to guess**, you'll need to modify the password until it is unique enough to be accepted.

1. If prompted to stay signed in, click **No**. Next, if prompted to start Microsoft Azure tour, click **Maybe later**. Next, click the user name in the upper-right corner and, in the drop-down menu, click **Sign out**
2. Close the InPrivate Mirosoft Edge session.
3. Start an InPrivate Mirosoft Edge window and browse to the Azure portal at [**https://portal.azure.com**](https://portal.azure.com).
4. When prompted to sign in, specify the full user name (including the @\*domain name\*.onmicrosoft.com suffix) of Karen Gruber's account and the corresponding temporary password.
5. On the **Update your password** page, in the **Current password** box, type the temporary password. In the **New password** and **Confirm password** boxes, type a new password, and click **Update password and sign in**. Take a note of the new password.

**Note:** If you receive the message **We've seen that password too many times before. Choose something harder to guess**, you'll need to modify the password until it is unique enough to be accepted.

1. If prompted to stay signed in, click **No**. Next, if prompted to start Microsoft Azure tour, click **Maybe later**. Next, click the user name in the upper-right corner and, in the drop-down menu, click **Sign out**

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

1. Switch to the Microsoft Edge window displaying the Azure portal and ensure that you are viewing the **Users - All users** page of the **adatum** Azure Active Directory tenant blade.
2. Click your user account that is the Service Administrator of your subscription.
3. Click **Profile**.
4. In the **Usage location** drop down list, select your country and click **Save**.
5. Click **Licenses**.
6. Click **+ Assign**.
7. On the **Assign license** blade, click **Products**.
8. On the **Products** blade, select the checkbox next to the **Azure Active Directory Premium P2** entry and click **Select**.
9. Click **Assignment options**.
10. On the **License options** blade, verify that **Azure Active Directory Premium P2**, **Azure Active Directory Premium Plan 1**, **Azure Multi-Factor Authentication**, and **Cloud App Security Discovery** are set to **On** and click **OK**.
11. Click **Assign**.
12. Verify that the assignment completed successfully.
13. Navigate back to the **adatum** blade and click **Groups**.
14. Click **General** (Note: if the options listed below are grayed out, refresh the Edge browser window).
15. On the **General** blade, specify the following settings and click **Save**:

* Owners can manage group membership requests in the Access Panel: **Yes**.
* Users can create security groups in Azure portals: **Yes**

1. Click **All groups**.
2. Click **+ New group**.
3. On the **Group** blade, specify the following settings:

* Group Type: **Security**
* Group name: **Sales**
* Group description: **Sales employees**
* Membership type: **Assigned**

1. Click **Members**.
2. On the **Members** blade, select the checkbox next to the entry **Remi Desforges** and click **Select**.
3. Click **Create** and close the **Group** blade.
4. Switch back to the **Groups - All groups** blade and click **+ New group**.
5. On the **Group** blade, specify the following settings:

* Group Type: **Security**
* Group name: **Marketing**
* Group description: **Marketing employees**
* Membership type: **Assigned**

1. Click **Members**.
2. On the **Members** blade, select the checkbox next to the entry **Karen Gruber** and click **Select**.
3. Click **Create** and close the **Group** blade.
4. Switch back to the **Groups - All groups** blade and click **+ New group**.
5. On the **Group** blade, specify the following settings:

* Group type: **Security**
* Group name: **Sales and Marketing**
* Group description: **Sales and Marketing employees**
* Membership type: **Assigned**

1. Click **Members**.
2. On the **Members** blade, select the checkbox next to the **Sales** and **Marketing** entries and click **Select**.
3. Click **Create** and close the **Group** blade.

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

1. On MIA-CL1, click **Start**, in the Start menu, expand the **Windows PowerShell** folder, right-click **Windows PowerShell ISE**, click **More**, and then click **Run as administrator**. When prompted by User Account Control for confirmation, click **Yes**.
2. In the PowerShell ISE, click **File**, and then click **Open**.
3. In the **Open** dialog box, browse to **F:\Labfiles\Lab09\Starter\**.
4. Click **Set-20553D0901Lab.ps1**, and then click **Open**.
5. In the PowerShell ISE window, in the console pane, enter the following command and press Enter:

Connect-MsolService

1. In the **Enter Credentials** dialog box, enter the full name (including the @\*domain name\*.onmicrosoft.com suffix) of Karen Gruber's user account and its password, 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 domain name here#>.onmicrosoft.com -DisplayName 'Mario Ledford' -FirstName 'Mario' -LastName 'Ledford' -Password 'Pa55w.rd' -ForceChangePassword $false -UsageLocation 'US'

1. Replace ***<#Copy your Azure Directory domain name here#>*** with the unique name you used to specify the DNS domain name of the Adatum Azure AD tenant in the first exercise of this lab.
2. In the PowerShell ISE window, 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 window, in the console pane, enter the following command, press Enter, and verify that the new user appears in the list of users:

Get-MsolUser

1. In the PowerShell ISE window, 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 window, in the console pane, enter the following command, press Enter, and verify that the new group appears in the list of groups:

Get-MsolGroup

1. In the PowerShell ISE window, 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 window, 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 window, 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 window, 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 the **adatum** blade of the Azure portal in Mirosoft Edge.
3. Click **Users**, **All users**, and verify that **Mario Ledford** appears in the list of users.
4. Switch back to the **adatum** blade of the Azure portal in Mirosoft Edge.
5. Click **Groups**, **All groups**, and verify that **Azure team** appears in the list of groups.

**Result**: After completing this exercise, you should have created Azure AD users and groups by using the Azure portal and Microsoft Azure Active Directory Module for Windows PowerShell. You also should have enabled the delegated group management Azure AD Premium functionality.

## Exercise 2: Configuring Application SSO

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

1. Navigate to the **adatum** Azure Active Directory tenant blade in the Azure portal and click **Enterprise applications**.
2. Click **+ New application**.
3. On the **Add an application** blade, in the **Enter a name** text box above the **Add from the gallery** section, type **Microsoft Account (Windows Live)**
4. In the list of results, click **Microsoft Account (Windows Live)**
5. On the **Microsoft Account (Windows Live)** blade, click **Add**. Wait till the application gets added.
6. On the **Microsoft Account (Windows Live) - Getting started** blade, click **Configure single sign-on (required)**.
7. On the **Single sign-on** blade, in the **Single Sign-on Mode** drop-down list, select **Pasword-based Sign-on** and click **Save**.
8. Close the **Single sign-on** blade and, on the **Microsoft Account (Windows Live) - Getting started** blade, click **Assign a user for testing (required)**.
9. On the **Users and groups** blade, click **+ Add user**.
10. On the **Add assignment** blade, click **Users and groups**.
11. On the **Users and groups** blade, in the **Select** text box, type **Mario Ledford**.
12. Select the entry representing the Mario Ledford user account and click **Select**.
13. Click **Assign Credentials**.
14. On the **Assign Credentials** blade, next to the **Assign credentials on behalf of the user?** label, click **Yes**.
15. On the **Assign Credentials** blade, in the **Email Address** text box, type the email address of your Microsoft Account that is the Service Administrator of the Azure subscription you are using for this lab, in the **Password** text box, type the passwod of that account, and click **OK**.
16. Click **Assign**.
17. Navigate back to the **Add an application** blade, in the search box, type **Skype**.
18. In the list of search results, click **Skype** and, then on the **Skype** blade, click **Add**. Wait till the application gets added.
19. On the **Skype - Getting started** blade, click **Configure single sign-on (required)**.
20. On the **Single sign-on** blade, in the **Single Sign-on Mode** drop-down list, select **Pasword-based Sign-on** and click **Save**.
21. Close the **Single sign-on** blade and, back on the **Skype - Getting started** blade, click **Assign a user for testing (required)**.
22. On the **Users and groups** blade, click **+ Add user**.
23. On the **Add assignment** blade, click **Users and groups**.
24. On the **Users and groups** blade, in the **Select** text box, type **Mario Ledford**.
25. Select the entry representing the Mario Ledford user account and click **Select**.
26. Click **Assign**.
27. On the top right side of the page, click your Azure account name, and then click **Sign out**.

#### Task 2: Configure SSO on a client computer

1. From Microsoft Edge, browse to [**https://myapps.microsoft.com**](https://myapps.microsoft.com).
2. On the **Microsoft Azure** page, click **Use another account**.
3. When prompted to sign in, specify the full user name (including the @\*domain name\*.onmicrosoft.com suffix) of the Mario Ledford's account you created in the previous exercise and **Pa55w.rd** as the corresponding password.
4. On the Apps page, click the ellipsis next to the **Skype** icon. Note the option to update the credentials.
5. On the Apps page, click the ellipsis next to the **Microsoft Account (Windows Live)** icon. Note that there is no option to update the credentials.
6. Switch to the PowerShell ISE window, the console pane, enter the following command, and press Enter:

Set-Service -Name 'wuauserv' -StartupType Manual

1. Switch to the Microsoft Edge window and, on the Apps page, click **Skype**.
2. In the **Skype** dialog box, click **Install Now**.
3. In the **Store** window, under the **My Apps Secure Sign-in Extension** header, click **Get**.
4. Wait for the extension to be downloaded and then switch back to the Microsoft Edge window.
5. When prompted, in the **You have a new extension** dialog box in the Microsoft Edge window, click **Turn it on**.
6. In the upper right corner of the Microsoft Edge window, click the ellipsis and, in the drop-down menu, click **Extensions**.
7. Verify that My Apps Secure Sign-in Extension is turned on. If not, click **My Apps Secure Sign-in Extension** and move the slider to the **On** position.
8. Restart Microsoft Edge and browse back to [**https://myapps.microsoft.com**](https://myapps.microsoft.com). If prompted to sign in, specify the full user name (including the @\*domain name\*.onmicrosoft.com suffix) of the Mario Ledford's account you created in the previous exercise and **Pa55w.rd** as the corresponding password.
9. On the Apps page, click **Skype**. Note that you are prompted for credentials, because you did not enter any credentials on behalf of the user when configuring the application single sign-on settings.
10. Click **Cancel** in the **Skype** dialog box.
11. Click the user name in the upper right corner of the Microsoft Edge page and click **Sign out**.
12. Close Microsoft Edge.
13. Switch to the PowerShell ISE window,the console pane, enter the following command, and press Enter:

Set-Service -Name 'wuauserv' -StartupType Disabled

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

## Exercise 3: Configuring Multi-Factor Authentication

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

1. Start Microsoft Edge, browse to the Azure portal at [**https://portal.azure.com**](https://portal.azure.com), and then sign in using the Microsoft account that is the Service Administrator of your subscription.
2. In the hub menu, click **All services** and then, in the service menu, click **Azure Active Directory**.
3. On the **adatum** blade, click **Users**.
4. Click **All users**.
5. In the toolbar of the **Users and groups - All users** blade, click **Multi-Factor Authentication**. This will open another Microsoft Edge tab. If prompted, sign in using the Microsoft account that is the Service Administrator of your subscription.
6. On the **multi-factor authentication** page, ensure that the **users** tab is displayed. In the **users** list, select the check box next to **Karen Gruber** and, in the **quick steps** section, click **Enable**.
7. On the **About enabling multi-factor auth** page, click **enable multi-factor auth**.
8. On the **Updates successful** page, click **close**.
9. Click the user name entry in the upper right corner of the Microsoft Edge window and, in the drop down menu, click **Sign out**.
10. Close the Microsoft Edge window, including both tabs.

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

1. Start Microsoft Edge and browse to [**https://myapps.microsoft.com**](https://myapps.microsoft.com).
2. On the **Microsoft Azure** page, click **Use another account**.
3. When prompted to sign in, specify the full user name (including the @\*domain name*.onmicrosoft.com suffix) of the Karen Gruber's account and the corresponding password. You will be presented with the message stating* **Your admin has required that you set up this account for additional security verification**\*.
4. Click **Set it up now**.
5. On the **Additional security verification** page, in the first drop-down list, select **Authentication phone**.
6. In the **Select your country or region** drop down list, click the entry representing your country or region.
7. In the adjacent text box, type your mobile phone number, under **Method** select **Send me a code by text message**, and click **Next**.
8. Retrieve the message on your mobile phone, type it in the text box on the page, and click **Verify**.
9. On the page **Step 3: Keep using your existing applications**, note the **Get started with this app password** entry, and click **Done**.
10. Click the user name in the upper right corner of the **Apps** page and, in the drop-down menu, click **Sign out**.
11. Close Microsoft Edge.

**Result**: After completing this exercise, you should have configured Multi-Factor Authentication for a Global Admin account.

## 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. Start Microsoft Edge, browse to the Azure portal at [**https://portal.azure.com**](https://portal.azure.com), and then sign in using the Microsoft account that is the Service Administrator of your subscription.
2. In the hub menu, click **All services** and then, in the service menu, click **Azure Active Directory**.
3. On the **adatum** blade, click **Devices**.
4. On the **Devices - All devices** blade, click **Device settings**.
5. Verify that the **Users may join devices to Azure AD** setting is set to **All**.
6. On MIA-CL1, click Start and then click **Settings**.
7. In the Settings app, click **Accounts**, and then click **Access work or school**.
8. On the **Access work or school** page, click **Connect**. This will open the **Set up a work or school account** window.
9. Click **Join this device to Azure Active Directory**.
10. On the **Let's get you signed in** page, in the **Work or school account** text box, type the full user name (including the @\*domain name\*.onmicrosoft.com suffix) of the Karen Gruber's account and click **Next**.
11. On the **Enter password** page, type the password you assigned to the Karen Gruber's account in exercise 1 of this lab and click **Sign in**.
12. Since you set up Karen Gruber's account with MFA in the previous exercise, you should receive at this point a text message conatining a verification code. Retrieve the verification code from your mobile phone, type it in the text box on the **Help us protect your account** page, and click **Next**.
13. On the **Make sure this is your organization** page, click **Join**.
14. On the **You're all set** page, click **Done**.
15. Switch back to Microsoft Edge.
16. Navigate back to the **adatum** page, click **Users and Groups**, click **All Users**, and then click **Karen Gruber**
17. On the **Karen Gruber** blade, click **Devices**.
18. Verify that **MIA-CL1** appears in the list of devices.
19. Restart **MIA-CL1**.

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

1. Sign in to MIA-CL1 by using the full user name (including the @\*domain name\*.onmicrosoft.com suffix) of the Karen Gruber's Adatum Azure AD account and its password.
2. Start Microsoft Edge, and then go to [**https://portal.azure.com**](https://portal.azure.com).
3. Verify that you are automatically signed in as Karen Gruber by using single sign-on.
4. Close all open applications sign out from MIA-CL1.

#### Task 3: Remove the lab environment

1. On MIA-CL1, close all open windows without saving any files.
2. On the taskbar, right-click the **Windows PowerShell** icon, and then click **Run as Administrator**. In the User Account Control dialog box, click **Yes**.
3. Type the following command, and then press **Enter**:

Remove-20533EEnvironment

1. When prompted, sign in by using the Microsoft account that is the Service Administrator of your Azure subscription.
2. If you have multiple Azure subscriptions, select the one you want the script to target.
3. If prompted, specify the current lab number.
4. When prompted for confirmation, type **y**.
5. Start Microsoft Edge, browse to the Azure portal at [**https://portal.azure.com**](https://portal.azure.com), and sign in by using the Microsoft account that is the Service Administrator of your Azure subscription.
6. In the Azure portal, on Dashboard, click **Edit**.
7. Right-click unoccupied area of the dashboard and, in the right-click menu, click **Reset to default state**. When prompted to confirm, click **Yes**.
8. Click **Done customizing**.
9. Close all open windows.

**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.