# Module 9: Implementing Azure Active Directory

# Lab: Implementing Azure AD

### Scenario

The IT department at A. Datum Corporation currently uses AD DS, and a range of Active Directory-aware applications. While preparing for synchronizing its AD DS to Azure AD, A. Datum wants you to test some of the features of Azure AD. The company wants you to control access to third-party SaaS apps by using Azure AD users and groups. A. Datum also wants you to configure SSO to these apps and protect them by using Multi-Factor Authentication.

In addition to these tasks, A. Datum wants you to evaluate some of the advanced features Azure AD Premium offers. It also wants you join a Windows 10-based computer to an Azure AD tenant to prepare for implementing this configuration on all the Windows 10-based computers in the Research department.

### Objectives

After completing this lab, you will be able to:

* Administer Azure AD.
* Configure SSO for Azure AD gallery applications.
* Configure multi-factor authentication for administrators.
* Use the advanced features offered by Azure AD Premium.
* Configure SSO from a Windows 10-based computer that is joined to Azure AD.

### Lab Setup

Estimated Time: 60 minutes

Virtual Machine: **20533E-MIA-CL1**

Username: **Student**

Password: **Pa55w.rd**

Before you start this lab, ensure that you complete the tasks in the Preparing the environment demonstration, which is in the first lesson of this module. Also ensure that the setup script is complete.

## Exercise 1: Administering Active AD

### Scenario

You want to test the functionality of Azure AD by first creating a new Azure AD tenant and enabling the Premium functionality. You then want to create some pilot users and groups in Azure AD. You plan to use the Azure portal interface and Microsoft Azure Active Directory Module for Windows PowerShell.

The main tasks for this exercise are as follows:

1. Create directories
2. Activate Azure AD Premium trial
3. Manage users by using the Azure portal
4. Manage groups by using the Azure portal
5. Manage users and groups by using Azure PowerShell

#### Task 1: Create directories

1. Ensure that you are signed in to MIA-CL1 as **Student** with the password **Pa55w.rd**.
2. Start Microsoft Edge, browse to the Azure portal at [**http://portal.azure.com**](http://portal.azure.com) and then, when prompted, and then sign in using the Microsoft account that is the Service Administrator of your subscription.
3. Add a directory by using the following settings:

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

1. Leave Microsoft 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. In the Azure portal, navigate to the **Adatum** directory.
2. Activate the Azure AD Premium trial.

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

1. Create a user in the Adatum directory with the following settings:

* Name: **Remi Desforges**
* User name: **rdesforges@*domain-name*.onmicrosoft.com** where ***domain-name*** is the name you assigned to the Azure Active Directory tenant in the first task of this exercise
* First Name: **Remi**
* Last Name: **Desforges**

1. Note the new password.
2. Create another user in the Adatum directory with the following settings:

* Name: **Karen Gruber**
* User name: **kgruber@*domain-name*.onmicrosoft.com** where ***domain-name*** is the name you assigned to the Azure Active Directory tenant in the first task of this exercise
* First Name: **Karen**
* Last Name: **Gruber**
* Directory role: **Global administrator**

1. Note the new password.
2. Open an InPrivate Microsoft Edge window, navigate to the Azure portal, sign in as **Remi Desforges**, when prompted, change the password to a new value and then sign-out and close the InPrivate Microsoft Edge window. Take a note of the new password.
3. Open an InPrivate Microsoft Edge window, navigate to the Azure portal, sign in as **Karen Gruber**, when prompted, change the password to a new value and then sign-out and close the InPrivate Microsoft Edge window. Take a note of the new password.
4. Click **Sign out** and close the in-private session of Microsoft Edge.

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

1. From the Azure portal, assign an Azure Active Directory Premium P2 license to your user account in the **Adatum** Azure AD.
2. From the Azure portal, enable **self-service group management** and allow users to create security groups.
3. Create the following group in the Adatum directory:

* Name: **Sales**
* Description: **Sales employees**
* Membership type: **Assigned**
* Enable Office features?: **No**

1. Add **Remi Desforges** to the **Sales** group.
2. Create the following group in the Adatum directory:

* Name: **Marketing**
* Description: **Marketing employees**
* Membership type: **Assigned**
* Enable Office features?: **No**

1. Add **Karen Gruber** to the **Marketing** group.
2. Create the following group in the Adatum directory:

* Name: **Sales and Marketing**
* Description: **Sales and Marketing employees**
* Membership type: **Assigned**
* Enable Office features?: **No**

1. Add the **Sales** and **Marketing** groups to the **Sales and Marketing** group.

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

1. Start **Windows PowerShell ISE** as an administrator.
2. Open **F:\Labfiles\Lab09\Starter\Set-20553D0901Lab.ps1**.
3. In the PowerShell ISE, in the command prompt pane, enter the following command, and then press Enter:

Connect-MsolService

1. When prompted, sign in as Karen Gruber.
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.rd123' -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 Windows PowerShell ISE, in the script pane, select the code that you just edited. 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, run the following command to list all the users:

Get-MsolUser

1. Create a new group by running the following command:

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

1. In the PowerShell ISE, in the command prompt pane, enter the following command, and then press Enter to list all the groups:

Get-MsolGroup

1. In the PowerShell ISE, in the script pane, locate the following code, and then 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 Microsoft Edge displaying the Azure portal.
3. From the **adatum** blade, verify that **Mario Ledford** appears in the list of users.
4. From the **adatum** blade, 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 Application SSO

### Scenario

Because A. Datum is planning to deploy cloud-based applications, and requires users to use SSO for these applications, you now want to install and configure a test application, and then validate the SSO experience.

The main tasks for this exercise are as follows:

1. Add directory applications and configure SSO
2. Test SSO

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

1. In the **Adatum** directory, add the **Microsoft Account (Windows Live)** application from the gallery:
2. Configure single sign-on for the application with the **Pasword-based Sign-on** setting.
3. Assign the application to **Mario Ledford**.
4. Select the option that allows you to enter the Microsoft account credentials on behalf of the user.
5. In the **Email Address** box, type the name of your Microsoft account you are using for this lab. In the **Password** box, type the corresponding password, and then click the check mark.
6. In the **Adatum** directory, add the **Skype** application from the gallery:
7. Configure single sign-on for the application with the **Pasword-based Sign-on** setting.
8. Assign the application to **Mario Ledford**
9. Sign out from the Azure portal.

#### Task 2: Test SSO

1. Open an Microsoft Edge window and browse to [**https://myapps.microsoft.com**](https://myapps.microsoft.com). When prompted, sign in by using specify the full user name (including the @\*domain name\*.onmicrosoft.com suffix) of **Mario Ledford's account** and the corresponding password **Pa55w.rd**.
2. On the applications page, click the ellipsis next to **Skype**. Note the option to update the credentials.
3. On the applications page, click the ellipsis next to **Microsoft Account**. Note that there is no option to update the credentials.
4. Switch to the Windows PowerShell ISE window and use the Windows PowerShell **Set-Service** cmdlet to set the startup of the Windows Update service to manual.
5. Switch back to the Microsoft Edge window, click **Skype** and, when prompted, install the My Apps Secure Sign-in Extension Microsoft Store app with the default settings and enable the extension once the installation completes.
6. Restart Microsoft Edge and browse to [**https://myapps.microsoft.com**](https://myapps.microsoft.com). When prompted, sign in as **Mario Ledford**.
7. From the Application Access Panel, start **Skype**. Note that you are now prompted for credentials, because you did not enter any credentials on behalf of the user when configuring SSO.
8. Click **Cancel** in the **Skype** dialog box.
9. Sign out from the Application Access Panel and close Microsoft Edge.
10. Switch to the Windows PowerShell ISE window and use the Windows PowerShell **Set-Service** cmdlet to disable the Windows Update service.

**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

### Scenario

Because A. Datum requires applications to use Multi-Factor Authentication, you now want to configure and test Multi-Factor Authentication for Global Administrators.

The main tasks for this exercise are as follows:

1. Configure Multi-Factor Authentication
2. Test Multi-Factor Authentication

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

1. Start Internet Explorer and sign in to the Azure portal by using the Microsoft account that is the Service Administrator of your subscription.
2. Enable Multi-Factor Authentication for the Adatum Azure AD user account of **Karen Gruber**.
3. Close Microsoft Edge.

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

1. Open Microsoft Edge, browse to [**https://myapps.microsoft.com**](https://myapps.microsoft.com), and sign in as **Karen Gruber**. You will be presented with the message stating ***Your admin has required that you set up this account for additional security verification***.
2. Click **Set it up now**.
3. On the **Additional security verification** page, in the first drop-down list, select **Authentication phone**. Enter your phone number and select the option **Call me**.
4. 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

### Scenario

A. Datum has an increasing demand to provide its remote and mobile users, who are using Windows 10-based devices, with secure access to the cloud resources. The company wants to join Windows 10 devices to Azure AD and simplify access to cloud resources by enabling SSO. Before they can implement this, you want to test this functionality by joining a WindowsÂ 10-based computer to Azure AD.

The main tasks for this exercise are as follows:

1. Join a Windows 10-based computer to Azure AD
2. Authenticate to Azure from a Windows 10 Azure-joined computer
3. Remove the lab environment

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

1. Start Microsoft Edge and sign in to the Azure portal by using your Azure subscription.
2. Verify that the **Adatum** directory allows all users to join their devices to Azure AD.
3. On MIA-CL1, click **Settings**, click **Accounts**, and then join MIA-CL1 into Azure AD by using the Adatum Azure AD credentials of Karen Gruber.
4. In the Azure portal, verify that **MIA-CL1** is shown on the Devices blade of the **Karen Gruber** user account.
5. Restart **MIA-CL1**.

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

1. Sign in to MIA-CL1 by using the Karen Gruber's Adatum Azure AD account and the password you set for this account in exercise 1.
2. Start Microsoft Edge and browse to the Azure portal.
3. Verify that you are automatically signed in as Karen Gruber by using SSO.
4. Sign out from MIA-CL1

#### Task 3: Remove the lab environment

1. On MIA-CL1, close all open windows without saving any files.
2. Start **Windows PowerShell** as Administrator and, from the **Administrator: Windows PowerShell** window, run **Remove-20533EEnvironment**.
3. When prompted, sign in by using the Microsoft account that is the Service Administrator of your Azure subscription.
4. If you have multiple Azure subscriptions, select the one you want the script to target.
5. If prompted, specify the current lab number.
6. When prompted for confirmation, type **y**.
7. Start Microsoft Edge, browse to the Azure portal, and sign in by using the Microsoft account that is the Service Administrator of your Azure subscription.
8. In the Azure portal, reset the dashboard to the default state.
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.

**Question** What is the major benefit of joining Windows 10-based devices to Azure AD?

**Question** What is the requirement for Delegated Group Management in Azure AD?

©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.