# 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. Additionally, it wants you join a Windows 10-based computer to an Azure AD tenant to test the Azure AD functionality and 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: **20533C-MIA-CL1**

Username: **Student**

Password: **Pa$$w0rd**

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 directory and enabling the Premium functionality. You then want to create some pilot users and groups in Azure AD. You plan to use both the portal 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 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. In Internet Explorer, browse to **http://manage.windowsazure.com,** and then sign in to the portal by using the Microsoft account that is associated with your Azure subscription.
3. Add a directory by using the following settings:

* **DIRECTORY**: Create new directory
* **NAME**: Adatum
* **DOMAIN NAME**: *Use your initials + the* *directory name + random numbers (e.g. abcadatum123456)*
* **COUNTRY** **OR REGION**: United States

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

1. In the navigation pane, select the **Adatum** directory.
2. In the **Licenses** tab, enable **Azure AD Premium trial** feature.

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

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

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

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

* **USER NAME**: kgruber
* **FIRST NAME**: Karen
* **LAST NAME**: Gruber
* **DISPLAY NAME**: Karen Gruber
* **ROLE**: Global Admin
* In the **ALTERNATE EMAIL ADDRESS** box, 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. Note the new password **.**
2. Sign out of the portal.
3. Sign in as **Karen Gruber**, and then change the temporary password to **Pa$$w0rd123**.

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

1. Browse to **https://manage.windowsazure.com**, and sign in by using the Microsoft account that is associated with your Azure subscription.
2. Select the **Adatum** directory, and then click **Configure**.
3. Enable **Delegated Group Management Enabled**.
4. Create the following group in the Adatum directory:

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

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

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

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

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

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 **D:09.ps1**.
3. In the PowerShell ISE, in the command prompt pane, enter the following command, and then press Enter:

Connect-MsolService

1. 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 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. 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, enter the following command, and then press Enter 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 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

### 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, create the following application from the gallery:

* **Microsoft Account (Windows Live)**

1. Verify that **Configure single sign-on** is enabled by default.
2. Assign the application to the following user:

* **Mario Ledford**

1. Select the option that allows you to enter the Microsoft account credentials on behalf of the user.
2. 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.
3. In the **Adatum** directory, create the following application from the gallery:

* **Skype**

1. Verify that **Configure single sign-on** is enabled by default.
2. Assign the application to the following user:

* **Mario Ledford**

1. In the **Assign User** dialog box, do not enter the Microsoft Account credentials on behalf of the user.

#### Task 2: Test SSO

1. Go to **https://account.activedirectory.windowsazure.com/applications**, and sign in by using the following credentials (where ***XXXadatumXXX*** is your unique Adatum domain name):

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

1. On the applications page, note the options to update the credentials and report a problem about the Microsoft account.
2. Run the Microsoft Account application, and complete the Access Panel Extension Setup Wizard.
3. Go to **https://account.activedirectory.windowsazure.com/applications**, and sign in by using the following credentials (where ***XXXadatumXXX*** is your unique Adatum domain name):

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

1. Click **Microsoft Account**, enter the credentials for your subscription account, and verify that your sign-in to the Access Panel has automatically signed you in to your Microsoft account. > **Note:** If you are prompted to sign in again, use the credentials for your subscription account.
2. Click **Skype**, and then verify that you are prompted for credentials. This happens because you did not enter any credentials on behalf of the user when you configured SSO.

**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. Sign in to the Azure portal by using your Azure subscription.
2. Configure the **Adatum** directory to enable Multi-Factor Authentication for **Karen Gruber**.

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

1. Go to **https://account.activedirectory.windowsazure.com/applications**, and sign in by using the following credentials (where ***XXXadatumXXX*** is your unique Adatum domain name):

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

1. Note the following message: **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, note the contact method options.
4. 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

### 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. Reset the environment

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

1. Sign in to the Azure portal by using your Azure subscription.
2. On MIA-CL1, click **Settings**, click **Accounts**, and then join MIA-CL1 into Azure AD by using the following credentials:

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

1. Verify that **MIA-CL1** is shown in the **Device** tab of the **Karen Gruber** user account.

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

1. Sign in to MIA-CL1 with Karen Gruber's credentials:

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

1. Provide a verification method.
2. Create a PIN.
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.

#### Task 3: Reset the environment

1. Close all open applications without saving any files.
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. You will be prompted to sign in 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.

**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.