# Lab Answer Key: Module 10: Managing an Active Directory infrastructure in a hybrid environment

# Lab: Implementing and managing Azure AD synchronization

## Exercise 1: Configuring directory synchronization

#### Task 1: Sign in to the Azure VM hosting an Active Directory domain controller.

1. Sign in to MIA-CL1 as **Student** with the password **Pa$$w0rd**.
2. Open Internet Explorer and browse to the Azure portal at https://portal.azure.com.
3. When prompted, sign in by using the Microsoft account that is the Service Administrator or a co-admin of your Azure subscription.
4. In the hub menu of the Azure portal, click **Virtual machines (classic)**.
5. In the Virtual machines (classic) blade, click **AdatumDC1**.
6. In the AdatumDC1 blade, click **Connect**.
7. When prompted whether to open or save the .rdp flie, click **Open**.
8. In the **Remote Desktop Connection** dialog box, click **Connect**.
9. If a Remote Desktop Connection warning message displays, select **Don't ask me again for connections to this computer**, and then click **Connect**.
10. In the **Windows Security** dialog box, enter a user name of **ADATUM\* with the password** Pa$$w0rd123\*\*.
11. If another Remote Desktop Message displays, select **Don't ask me again for connections to this computer**, and then click **Yes**.

#### Task 2: Create a new Azure AD tenant and a Global Admin account

1. After the sign-in is complete, click the Windows logo in the lower left corner, and then on the **Start** screen, click **Internet Explorer**.
2. If a **Set up Internet Explorer 11** dialog box opens, click **Use recommended security, privacy, and compatibility settings**, and then click **OK**.
3. In Internet Explorer, navigate to the Azure classic portal at **https://manage.windowsazure.com**.
4. When prompted, sign in to the Azure classic portal by using an account that is the Service Administrator or a co-admin of your Azure subscription.
5. In the Azure classic portal, click **ACTIVE DIRECTORY** in the navigation bar.
6. Click **New**, click **DIRECTORY**, and then click **CUSTOM CREATE**.
7. In the **Add directory** dialog box, provide the following settings, and then click **Complete** (check mark):

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

1. On the **adatumsync** page, click the **USERS** tab.
2. Click **ADD USER** on the command bar.
3. 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: **SyncAdmin**

1. In the **USER** **PROFILE** dialog box, provide the following settings, and then click **Next**:

* FIRST NAME: **Sync**
* LAST NAME: **Admin**
* DISPLAY NAME: **Sync Admin**
* ROLE: Global **Admin**
* ALTERNATE EMAIL ADDRESS: *Type the email address of your Microsoft account*
* Enable Multi-Factor Authentication: *Do not select*

1. Click **Create**.
2. On the **Get temporary password** page, note the full user name and the temporary password, and then copy them to Notepad.
3. Click **Complete** (check mark).
4. Click the cogwheel icon in the upper right corner of the Internet Explorer window, click **Safety** in the drop-down menu, and then click **inPrivate Browsing.**
5. In the InPrivate Browsing session, navigate to the Azure classic portal at **https://manage.windowsazure.com**.
6. When prompted, type the full name of the newly created SyncAdmin account, and then click **Continue**.
7. When prompted for the password, type the temporary password which you copied to Notepad, and then click **Sign in**.
8. On the **Update your password** page, in the **Current password** text box, type the temporary password, in the **New password** and **Confirm password** text boxes, type **Pa$$w0rd**, and then click **Update password and sign in**.
9. On the **No subscriptions found** page, click **SIGN OUT**.
10. Close the InPrivate Internet Explorer session.

#### Task 3: Install Azure AD Connect with custom settings

1. Open an Internet Explorer session and browse to https://www.microsoft.com/en-us/download/details.aspx?id=47594
2. On the **Microsoft Azure Active Directory Connect** page, click the cogwheel in the upper right corner of the Internet Explorer window and select **Internet options** from the drop down menu.
3. In the **Internet Options** dialog box, click the **Security** tab.
4. Click **Trusted sites**, and then click **Sites**.
5. In the **Add this website to the zone** text box, replace the current entry with \*\*https://\*.microsoft.com**, and then click** Add\*\*.
6. Click **Close**, and then click **OK**.
7. Back on the **Microsoft Azure Active Directory Connect** page, click **Download**. Note - if this fails, close your IE browser, reopen, and browse again to https://www.microsoft.com/en-us/download/details.aspx?id=47594.
8. In the pop-up window, click **Save**.
9. After the download is complete, click **Open Folder**.
10. In the File Explorer window, double-click **AzureADConnect.msi** to start the installation.
11. On the **Welcome** page, select **I agree to the license terms and privacy notice**, and then click **Continue**.
12. On the **Express Settings** page, click **Customize**.
13. On the **Required Component** page, review the options, and then click **Install**.
14. On the **User sign-in** page, verify that **Password Synchronization** is selected, and then click **Next**.
15. On the **Connect to Azure AD** page, provide the credentials of the newly created SyncAdmin Azure AD Global Admin, and then click **Next**:

* User name: **SyncAdmin@ *yourdomainname*.onmicrosoft.com**
* Password: **Pa$$w0rd**

1. On the **Connect your directories** page, verify that the **adatum.com** forest is selected, under user name, type **ADATUM\* with the password** Pa$$w0rd123**, and then click** Add Directory\*\*.
2. Verify that under Configured Directories, adatum.com is listed, and then click **Next**.
3. On the **Azure AD sign-in configuration** page, note the message **Users will not be able to sign-in Azure AD using their on-premises credentials**, select **Continue without any verified domains**, and then click **Next**.
4. On the **Domain and OUfiltering** page, select the **Sync selected domains and OUs** check box, expand the **adatum.com** entry, clear all checkboxes with exception of the one next to the **Accounts** organization unit, and then click **Next**.
5. On the **Uniquely identifying your users** page, verify that **Users are represented only once across all directories** is selected, and then click **Next**.
6. On the **Filtering** page, verify that **Synchronize all users and devices** is selected, and then click **Next**.
7. On the **Optional feature** page, verify that **Password synchronization** is selected, and then click **Next**.
8. On the **Ready to configure** page, verify that **Start the synchronization process when configuration completes** is selected, and then click **Install**. > **Note:** Installation might take 5-10 minutes.
9. On the **Configuration complete** page, click **Exit** to close Azure AD Connect. > **Note:** You might need to wait a few minutes for the initial synchronization to complete.
10. Switch back to the Azure classic portal in the Internet Explorer window.
11. In the Azure classic portal, navigate to the **adatumsync** Active Directory page, click **USERS**, and then confirm that the list of users includes all the names from the Accounts organizational unit (OU).

**Result**: After completing this exercise, you should have installed and configured Azure AD Connect, and you should have it ready for test synchronization.

## Exercise 2: Synchronizing directories

#### Task 1: Modify attributes of an Active Directory user and Initiate manual synchronization

1. On AdatumDC1, switch to the Server Manager window, and from the **Tools** menu, open the **Active Directory** **Administrative** **Center**.
2. Click **adatum (local)**, and then double-click **Accounts**.
3. After the Accounts OU content is displays, double-click the **Beverly Beach (bbeach)** account.
4. In the **Beverly Beach (bbeach)** window, make changes to the following fields, and then click **OK**:

* **Job Title**: **VP**
* **Department**: **Marketing**

1. On AdatumDC1, on the taskbar, right-click the **Windows PowerShell** shortcut, right-click **Windows PowerShell** on the menu and then click **Run as administrator**.
2. At the command prompt in the Windows PowerShell command-line interface, type the following command, and then press Enter: Get-ADSyncScheduler > **Note:** **Get-ADSyncScheduler** displays the current configuration settings for synchronization with Azure AD.
3. At the Windows PowerShell command prompt, type the following command, and then press Enter: Start-ADSyncSyncCycle -PolicyType Delta
4. Wait until synchronization completes before proceeding to the next step.
5. Switch back to the Azure classic portal in the Internet Explorer window.
6. Click the USERS tab on the **adatumsync** page.
7. Click the **Beverly Beach** entry.
8. On the **Beverly beach** page, click **WORK INFO**.
9. Verify that the **JOB TITLE** and the **DEPARTMENT** entries match the ones you configured for the Active Directory account. If you do not see any changes, wait for a few minutes, and then refresh the page.
10. Close the AdatumDC1 remote desktop session, and then click **OK** when prompted.

#### Task 2: Reset the environment

1. On MIA-CL1, 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. Type 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 might remove Azure services in your subscription. We therefore recommend that you use an Azure trial pass that was provisioned specifically for this course, and not your own Azure account. The script will take 5-10 minutes to reset your Azure environment and make it ready for the next module. The script removes all storage, virtual machines, virtual networks, cloud services, and resource groups. **Important:** The script might not be able to get exclusive access to a storage account to delete it; if this occurs, you will see an error. If you find objects remaining after the reset script is complete, you can rerun the **Reset-Azure** script, or you can use the Azure classic portal to delete all the objects in your Azure subscription manually, with the exception of the default directory.

**Result**: After completing this exercise, you should have changed attributes on a user account, and then forced synchronization.

©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.