# Lab Answer Key: Module 4: Planning and configuring directory synchronization

# Lab: Configuring directory synchronization

## Exercise 1: Preparing for directory synchronization

#### Task 1: Configure UPN

1. Sign in to the LON-DC1 virtual machine as **ADATUM\Administrator** with a password of **Pa55w.rd**.
2. On the Start screen, click **Administrative Tools**, and then double-click **Active Directory Domains and Trusts**.
3. In the Active Directory Domains and Trusts window, right-click **Active Directory Domains and Trusts**, and then click **Properties**.
4. Select the **UPN Suffixes** tab, in the **Alternative UPN suffixes:** box, type **gsp.Adatumvsxxxxx.virsoftlabs.com**, replacing *xxxx* with your unique Adatum number and then click **Add**.
5. Click **OK**.
6. On the Start screen, right-click **Windows PowerShell**, and then click **Run as administrator**.
7. At the Windows PowerShell prompt, type the following command, replacing *xxxx* with your unique Adatum number and then press Enter:

Get-ADUser -Filter \* -Properties SamAccountName | foreach { Set-ADUser $\_ -UserPrincipalName ($\_.SamAccountName + "@gsp.Adatumvsxxxxx.virsoftlabs.com" )}

#### Task 2: Prepare problem user accounts

1. On the LON-DC1, in the Windows PowerShell prompt, type the following command, and then press Enter:

CD C:\labfiles\

1. At the Windows PowerShell prompt, type the following command, and then press Enter:

Set-ExecutionPolicy Unrestricted

1. To confirm the execution policy change, press **Enter**.
2. At the Windows PowerShell prompt, type the following command, and then press Enter:

.\CreateProblemUsers.ps1

**Note:** Wait until the script has completed before proceeding to the next step.

1. This Windows PowerShell script will make the following changes in AD DS:

* Klemen Sic. Add the "@" character to the beginning of "adatum" for the **UserPrincipalName** attribute.
* Lara Raisic. Replace the existing string with "lara@adatum.com" for the **EmailAddress** attribute.
* Logan Boyle. Replace the existing string with "lara@adatum.com" for the **EmailAddress** attribute.
* Lara Raisic. Replace the existing string with "lara@adatum.com" for the **emailAddress** attribute.
* Logan Boyle. Replace the existing string with "lara@adatum.com" for the **emailAddress** attribute.
* Holly Spencer. Replace the existing string with "holly @adatum.com" for the **EmailAddress** attribute.
* Maj Hojski. Replace the existing string with " " for the **emailAddress** attribute.

#### Task 3: Run the IdFix tool and fix identified issues

1. On LON-CL1, open Microsoft Edge, and then connect to [**https://www.microsoft.com/en-us/download/details.aspx?id=36832**](https://www.microsoft.com/en-us/download/details.aspx?id=36832)
2. On the IdFix DirSync Error Remediation Tool page, click **Download**.
3. Wait for the download to complete, and then click **Open**.
4. In the File Explorer windows, browse to the **Downloads** folder, right-click **IdFix.zip**, and then click **Extract All...**
5. In the **Extract Compressed (Zipped) Folders** dialog box, in the destination box, type **C:\Deployment Tools\IdFix**, and then click **Extract**.
6. In File Explorer, in the **C:\Deployment Tools\IdFix** folder, right-click **IdFix**, and then click **Run as administrator**.
7. In the User Account Control dialog box, click **Yes**.
8. In the **IdFix Privacy Statement** message box, click **OK**.
9. Click **Query**. You should see several errors.
10. Click the **ERROR** column to sort the character errors to the top of the list.

**Note:** Ignore topleveldomain errors, which cannot be fixed by the IdFix tool.

1. In the Klemen Sic row, in the **ACTION** column, select **EDIT**.
2. In the Holly Spencer row, in the **ACTION** column, select **EDIT.**
3. In the Maj Hojski row, in the **ACTION** column, select **EDIT**
4. On the toolbar, click **Apply**.
5. In the **Apply Pending** dialog box, click **Yes**; note the **COMPLETE** status in the **ACTION** column indicating successful writes.
6. Switch to **File Explorer**, and in the **C:\Deployment Tools\IdFix** folder, double-click **Verbose <date> <time>.txt** to view the updated transactions in the transaction log.
7. Switch back to the IdFix tool.
8. On the toolbar, click **Query**.
9. Click in the **UPDATE** column to locate the Logan Boyle error, and replace the string with **logan@adatum.com**, and then in the **ACTION** column, select **EDIT**.
10. Click in the **UPDATE** column to locate the Maj Hojski error, and replace the string with **maj@adatum.com**, and then in the **ACTION** column, select **EDIT**.
11. On the toolbar, click **Apply**.
12. In the **Apply Pending** box, click **Yes**.
13. On the toolbar, click **Query** and verify that errors are corrected.

**Note:** Where there are format and duplicate errors for distinguished names, the UPDATE column either contains the same string as the VALUE column, or the UPDATE column entry is blank; in either case, this means that IdFix cannot suggest a remediation for the error. You can either fix these errors outside IdFix, or manually remediate them within IdFix. You can also export the results and use Windows PowerShell to remediate a large number of errors.

#### Task 4: Configure the Office 365 tenant for directory synchronization

1. On LON-CL1, on the desktop, double-click Windows Azure Active Directory Module for Windows PowerShell.
2. At the **Windows PowerShell** prompt, type the following command, and press Enter after each:

$msolcred = Get-Credential

1. In the **Windows PowerShell Credential** dialog box, enter **Holly@gspAdatumvsxxxxx.onmicrosoft.com** in the **User name** box, enter the password ‘Pa55w.rd’ in the **Password** box, and then click **OK**.
2. At the **Windows PowerShell** prompt, type the following command, and then press Enter:

Connect-MsolService -Credential $msolcred

1. At the **Windows PowerShell** prompt, type the following command, and then press Enter:

Set-MsolDirSyncEnabled -EnableDirSync $true -Force

**Note:** The **-Force** switch disables the confirmation dialog box.

1. Although you might have to wait up to 24 hours for activation to complete, you should be able to continue.
2. At the **Windows PowerShell** prompt, type the following command, and then press Enter:

(Get-MsolCompanyInformation).DirectorySynchronizationEnabled

1. The output returns "**True**" if sync is enabled.

**Note:** It might take a few minutes to return "True." Rerun the command until you see "True" showing.

1. Switch to Microsoft Edge, and in the address box, type **https://portal.office.com,** and then press Enter.
2. On the **Sign-in** page, in the **Name** box, select **holly@gspAdatumvsxxxxx.onmicrosoft.com**. In the **Password** box, type the password ‘Pa55w.rd’, and then click **Sign in**.
3. Navigate to the **Office 365 Admin center**.
4. In the Office365 admin center, in the left side menu, click **Health**, and then click **Directory Sync Status**.

If you do not see "Directory Sync Status", activation was not yet completed.

1. Verify that the text **True** appears to the right of **Active Directory synchronization enabled**.

**Result**: After completing this exercise, you will have resolved issues in AD DS identified by the IdFix tool and you will have enabled Active Directory synchronization in Office 365.

## Exercise 2: Configuring directory synchronization

#### Task 1: Download and install Azure AD Connect

1. Sign in to the **LON-DC1** as **ADATUM\Administrator** with a password of **Pa55w.rd**. If the Networks pane appears, click **Yes**.
2. In Server Manager, click **Local Server**.
3. Beside the text **IE Enhanced Security Configuration**, click on the Hyperlink **On**.
4. In **Internet Explorer Enhanced Security Configuration**, below **Administrators**, click **Off and click** OK\*\*.
5. Start **Internet Explorer** from the taskbar.
6. If a **Windows Internet Explorer 10** dialog box appears, select **Use recommended security and compatibility settings**, and then click **OK**.
7. In the **Address** box, type **https://portal.office.com**, and then press Enter.
8. On the **Sign in** page, in the **Name** box, type **holly@gspAdatumvsxxxxx.onmicrosoft.com**.
9. In the **Password** box, type the password ‘Pa55w.rd’, and then click **Sign in**.
10. Navigate to the Office 365 admin center.
11. In the left side menu, click **Users**, and then click **Active users**.

**Note:** If you see the Active Directory synchronization is being activated warning, you can ignore it at this time, but you will not be able to run directory synchronization later in this exercise. You must wait until directory synchronization is activated. However, you can complete the following steps, even if you do see the warning message.

1. Click **Holly Spencer**.
2. On the Holly Spencer page, click **Edit** in the **User name / Email** section.
3. In the Aliases section, type **Holly** in the **Alias** textbox and ensure that **gsp.Adatumvsxxxxx.virsoftlabs.com** domain is selected. Click **Add**.
4. Click **Set as primary** and then read the warning and click **Save**.
5. Click **Sign Out**.
6. Close Internet Explorer.
7. Open **Internet Explorer**.
8. If a **Windows Internet Explorer 10** dialog box appears, select **Use recommended security and compatibility settings**, and then click **OK**.
9. In the **Address** box, type **https://portal.office.com**, and then press Enter.
10. Sign in as **holly@gsp.Adatumvsxxxxx.virsoftlabs.com**, using the password the password ‘Pa55w.rd’.
11. In the left side menu, click **Users**, and then click **Active users**.
12. Select **More** and then select **Directory synchronization**.
13. On the **Directory Synchronization** pane, select **Go to the DirSync management**.
14. Next to **Directory sync client version**, click \*\* Upgrade to the latest version of Azure AD Connect\*\*.

**Note:** You will automatically be redirected to the Microsoft Azure Active Directory Connect download page. Alternatively you can also search for Microsoft Azure Active Directory Connect in the Microsoft Download Center.

1. On the **Microsoft Azure Active** **Directory Connect** download page in Internet Explorer, click **Download**.
2. In the Internet Explorer notification bar, click **Save as**, browse to **C:\Labfiles**, and then click **Save**. If the LabFiles folder does not exist, create it.
3. When the download has completed, in the Internet Explorer notification bar, click **Open folder**.
4. In **File Explorer**, right-click **AzureADConnect.msi**, and then click **Install**.
5. In the **Microsoft Azure Active Directory Connect** wizard, on the **Welcome** page, click **I agree to the license terms and privacy notice**, and then click **Continue**.
6. On the **Express Settings** page, click **Customize**.
7. Leave the Microsoft Azure Active Directory Connect wizard open for the next task.

#### Task 2: Run the Azure AD Connect tool with custom settings

1. On the **Install required components** page, leave all the checkboxes unchecked and click **Install**.
2. On the **User Sign-in** page, click **Password Synchronization**, and then click **Next**.
3. On the **Connect to Azure AD** page, enter the following credentials, and then click **Next**:

* User name: **holly@gsp.Adatumvsxxxxx.virsoftlabs.com**.
* Password: Pa55w.rd

1. On the **Connect your directories** page, click **Add Directory**.
2. In the **AD Forest account** dialog, select **Create new account**, enter the following credentials, and then click **OK**:

* User name: **ADATUM\Administrator**
* Password: **Pa55w.rd**

1. Click **Next**.
2. On the **Azure AD sign-in configuration** page click **Next**.
3. On the **Domain and OU filtering** page, click **Sync selected domains and OUs**, expand **Adatum.com**, clear all check boxes for the child containers except for the **IT** checkbox, and then click **Next.**
4. On the **Uniquely identifying your users** page, click **Next**.
5. On the **Filter users and devices** page, verify that **Synchronize all users and devices** is selected, and then click **Next**.
6. On the **Optional Features** page, leave the default options, and then click **Next**.
7. On the **Ready to configure** page, review the features that will be installed. Ensure that **Start the synchronization process when configuration completes** is selected, and then click **Install.**

**Note:** The installation process will take approximately 10 minutes to complete.

1. Once the installation completes, on the **Configuration complete** page, click **Exit**.
2. On the Start screen, sign out of LON-DC1, and then sign back in as **Adatum\Administrator** with password **Pa55w.rd.**

**Note:** Because Adatum\administrator was used to install Azure AD Connect, it will be automatically added to the ADSyncAdmins group, and you need to sign out for the Kerberos token to be updated. Otherwise, if you use a different user account to install Azure AD Connect, you will need to manually add the Azure AD Connect admin to the local ADSyncAdmins group on LON-DC1.

#### Task 3: Configure synchronization service filtering for organizational units

1. On LON-DC1, click **Start**, open **Azure AD Connect** folder, and then click on **Synchronization Service.**
2. In **Synchronization Service Manager**, click the **Connectors** tab.
3. In the **Connectors** tab, double-click **Adatum.com**.
4. In the **Properties** dialog box, click **Configure Directory Partitions**.
5. Click **Containers**.
6. In the **Credentials** dialog box, enter the following credentials, and then click **OK**:

* User name: **Administrator**
* Password: **Pa55w.rd**
* Domain: **Adatum.com**

**Note:** While this account is not the one used for directory synchronization, you use the account credentials temporarily to access AD DS for configuring filtering.

1. In the **Select Containers** dialog box, select the **Research** checkbox, verify that **IT** is selected, and then click **OK**.
2. Click **OK** to close the Properties dialog window.

#### Task 4: Configure synchronization service filtering for object attribute

1. On LON-DC1, open the Start screen, open **Azure AD Connect** folder, and then click **Synchronization Rules Editor**.
2. In **Synchronization Rules Editor**, click **Add new rule**.
3. On the **Create inbound synchronization rule** dialog window, in the **Name** box, type **In from AD - User DoNotSyncFilter**
4. For **Connected System**, select **Adatum.com**.
5. For **Connected System Object Type**, select **user**.
6. For **Metaverse Object Type**, select **person**.
7. For **Link Type**, select **Join**.
8. For **Precedence**, type **50**.
9. Click **Next**.
10. In the **Create inbound synchronization rule** dialog box, on the **Scoping filter** tab, click **Add group**, and then click **Add clause**.
11. In **Add scoping filters**:

* For **Attribute**, select **msDS-cloudExtensionAttribute15**.
* For **Operator**, select **EQUAL**.
* For **Value**, type **NoSync**,

1. Click **Next**.
2. On the **Add join rules**, click **Next**.
3. On the **Add transformations** page, click **Add transformation**.

* For **FlowType**, select **Constant**.
* For **Target Attribute**, select **cloudFiltered**.
* In the **Source** text box, type **True**.

1. To save the rule, click **Add**, and then close Synchronization Rules Editor window.
2. Open Windows PowerShell from the Start menu. In Windows PowerShell, type the following command, and then press Enter. The initial synchronization can take several minutes to complete. Leave the Windows PowerShell window open.

Start-ADSyncSyncCycle -PolicyType Initial

#### Task 5: Verify that synchronization was successful

1. Ensure that you are signed in to the LON-DC1 as **ADATUM\Administrator** with a password of **Pa55w.rd**.
2. Open Internet Explorer, and then browse to <http://aka.ms/siqtee>
3. After **AdministrationConfig-en.msi** finishes downloading, click **Run**.
4. In the Microsoft Azure Active Directory Module for Windows PowerShell Setup Wizard, on the **Welcome** page, click **Next**.
5. On the **License Terms** page, click **I accept the terms in the License Terms**, and then click **Next**.
6. On the **Install Location** page, click **Next**.
7. On the **Ready to Install** page, click **Install**.
8. On the **Completing the Microsoft Azure Active Directory Module for Windows PowerShell Setup** page, click **Finish**.
9. On the Start screen, open Azure AD Connect folder, and then click **Synchronization Service**.
10. In **Synchronization Service Manager on LON-DC1**, click **Operations**.
11. In the **Connector Operations** list, click the line at the top of the list, and then review the **Start Time**, **End Time**, and the **Status**.
12. Verify the connector has a **Start Time** and **End Time** that aligns with the last time synchronization was initiated in the previous task.
13. On the taskbar, right-click **Windows PowerShell**, and then select **Run as Administrator**.
14. At the Windows PowerShell prompt, type the following commands, and then press Enter after each one:

Import-Module MSOnline

Connect-MsolService

1. In the **Enter Credentials** dialog box, enter the following credentials, and then click **OK**:

* User name: **holly@gsp.Adatumvsxxxxx.virsoftlabs.com**
* Password: The password ‘Pa55w.rd’

1. At the Windows PowerShell prompt, type the following command, and then press Enter:

Get-MsolCompanyInformation | fl LastDirSyncTime

1. Verify the **LastDirSyncTime** aligns with the last time synchronization was initiated in the previous task.
2. On the Start screen, open **Internet Explorer**, and then type https://portal.office.com/admin/default.aspx in the address bar.
3. On the **Sign-in** page, sign in by using the following credentials:

* User name: **holly@gsp.Adatumvsxxxxx.virsoftlabs.com**
* Password: Pa55w.rd

1. In the admin center, click **DirSync Status**.
2. Verify that the **Last synced less than an hour ago** message appears.
3. In the Active users list, note that your on-premises accounts from the selected OUs now have a status of Synced with Active Directory.

**Result**: After completing this exercise, you will have installed Azure AD Connect with customized settings. Upon completion of the installation, you will start directory synchronization to Office 365 and have verified that synchronization was successful.

## Exercise 3: Managing Active Directory users and groups

#### Task 1: Create a new user and group account

1. On **LON-DC1**, in **Server Manager**, click **Tools**, and then click **Active Directory Users and Computers**.
2. In the console tree, expand **Adatum.com**, right-click **Research**, click **New**, and then click **User**.
3. In the **First name** box, type **Perry**.
4. In the **Lastname** box, type **Brill**.
5. In the **User logon name** box, type **Perry**, select your lab domain **UPN** (not **Adatum.com**), and then click **Next**.
6. In the **Password** and **Confirm password** boxes, type **Pa55w.rd**, clear the **User must change password at next logon** checkbox, click **Next**, and then click **Finish**.
7. In the **Research** OU user list, double-click the **Perry Brill** user.
8. In the **Properties** dialog box, in the **E-mail** box, type **Perry@gsp.Adatumvsxxxxx.virsoftlabs.com**, and then click **OK**.
9. In the console tree, right-click the **Research** OU, click **New**, and then click **Group**.
10. In the New Object - Group window, in the **Group name:** box, type **Project Team**, click **Universal**, click **Distribution**, and then click **OK**.
11. In the **Research** OU, double-click the **Project Team** group.
12. In the **Properties** dialog window, in the **E-mail** box, type **projectteam@Gsp.Adatumvsxxxxx.virsoftlabs.com**.
13. On the **Members** tab, click **Add**.
14. In the **Select Users, Contacts, Computers, Service Accounts, or Groups** dialog box, in the **Enter the object names to select**, type the following names, and then click **Check Names**:

* Arturs Priede
* August Towle
* Cai Chu

1. Click **OK** twice.

#### Task 2: Move a user out of the scope of synchronization

1. On LON-DC1, at the **Windows PowerShell** prompt, type the following command, and then press Enter:

Get-MsolUser -Search Vera

1. Verify that the user Vera Pace is listed in Office 365.
2. On LON-DC1, in Active Directory Users and Computers, move Vera Pace from the Research OU to the Sales OU, by right-clicking **Vera Pace** in the Research OU user list, and then clicking **Move** and selecting **Sales** OU. Click **OK**.

#### Task 3: Move a user into the scope of synchronization

1. On LON-DC1, ensure that the **Active Directory Users and Computers** is opened.
2. In the console tree, if needed expand **Adatum.com**, and then click **Marketing**.
3. Right-click **Ada Russell**, and click **Move**.
4. In the **Move** dialog box, expand **Adatum.com**, click **Research**, and then click **OK**.

#### Task 4: Change group membership

1. In the console tree of **Active Directory Users and Computers**, click **Research**.
2. In the right pane, double-click **Research**.
3. In the **Research Properties** dialog box, click the **Members** tab.
4. Select the following three users, and then click **Remove**. In the confirmation dialog box, click **Yes**.

* Claire Roberson
* Connie Vaughn
* Esther Wiggins

1. Click **OK**.

#### Task 5: Force synchronization

1. On LON-DC1, from the taskbar, right-click the **Windows PowerShell** shortcut, and then click **Run as administrator**.

**Note:** If a **User Account Control** dialog box appears, click **Yes**.

1. At the Windows PowerShell prompt, type the following, and then press Enter:

Start-ADSyncSyncCycle -PolicyType Delta

**Note:** The **Delta** switch is used here so that only the updates are synchronized.

1. Wait until synchronization has completed before proceeding to the next task.

#### Task 6: Validate the results of directory synchronization

1. To verify the new user you created, on LON-CL1, open the Office 365 Admin Center in Microsoft Edge by typing **https://portal.office.com/adminportal/home** in the address bar.
2. Sign in using the following credentials:

* User name: **holly@gsp.Adatumvsxxxxx.virsoftlabs.com**
* Password: Pa55w.rd

1. In the **Office 365 Admin Center**, in the left navigation, click **Users**, and then click **Active Users**.
2. In the Active Users list, verify that **Perry** **Brill** has a value of **Synced with Active Directory** in the Sync Type column.

**Note:** You might need to wait up to 10 minutes before the account appears. Refresh the list until you see Perry Brill's account.

1. In the **Active Users** list, click **Perry** **Brill**.
2. Under Product licenses section, click **Edit**.
3. On the **Product licenses** page, in the **Location** drop-down menu, select **United** **Kingdom**, and then click on the icon next to **Office 365 Enterprise E5**.
4. Click **Save**, and then click **Close** twice.
5. Repeat the steps 8-11 to assign Office 365 license for user Ada Russell.
6. To verify that you have created the new group, in **Office 365 admin center**, in the left navigation, click **Groups**, and then click **Groups**.
7. In the **Groups** list, verify that the **Project Team** appears.

**Note:** You might need to wait up to 10 minutes before the group appears. Refresh the list until you see the object.

1. In the **Groups** list, select the Project Team group.

**Note:** In the right pane, notice that **Edit Members** is unavailable. This is because group membership is maintained by Active Directory. To view the membership, you need to use Windows PowerShell.

1. On LON-DC1, in Windows PowerShell, type the following command, and then press Enter:

Get-MsolGroup

1. Verify that you see Research and Project Team groups. Copy the ObjectID value for these two groups.
2. To verify that you updated the group membership in AD DS, type the following command at the Windows PowerShell prompt, and then press Enter:

Get-MsolGroupMember -GroupObjectId <ObjectID for Research group>

1. Verify the membership of the group does not contain the users removed in AD DS. The users who were removed from the group are:

* Claire Roberson
* Connie Vaughn
* Esther Wiggins

1. To verify that you have moved the user, Vera Pace, out of the scope of synchronization, type the following command at the Windows PowerShell prompt, and then press Enter:

Get-MsolUser -Search Vera

1. At the Windows PowerShell prompt, type the following command, and then press Enter:

Get-MsolAccountSku

**Note:** The number of **ConsumedUnits** is now less than before.

1. Leave the virtual machines running for the next lab.

**Result**: After completing this exercise, you will have identified how managing user and group accounts has changed with directory 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.