Implement Directory Synchronization

Lab scenario

You have been asked to create a proof of concept demonstrating how to integrate on-premises Microsoft Entra Domain Services environment with an Microsoft Entra tenant. Specifically, you want to:

- Implement a single-domain Microsoft Entra Domain Services forest by deploying an Azure VM hosting an Microsoft Entra Domain Services domain controller
- Create and configure an Microsoft Entra tenant
- Synchronize the Microsoft Entra Domain Services forest with the Microsoft Entra tenant

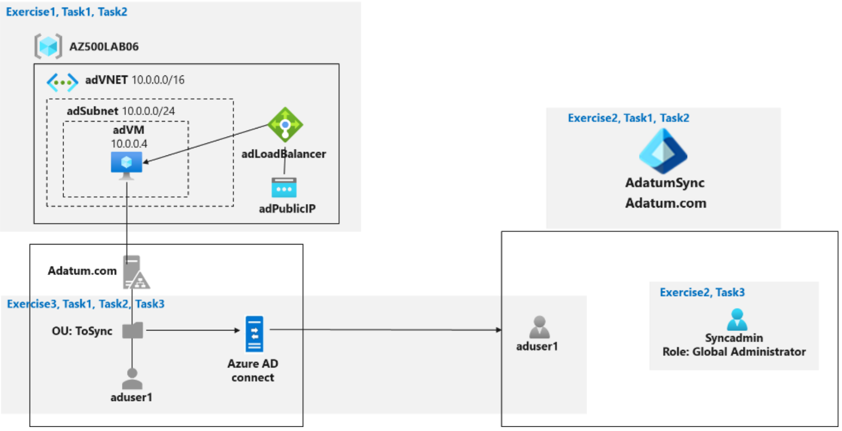
For all the resources in this lab, we are using the **East US** region. Verify with your instructor this is the region to use for class.

Lab objectives

In this lab, you will complete the following exercises:

- Exercise 1: Deploy an Azure VM hosting an Microsoft Entra ID domain controller
- Exercise 2: Create and configure an Microsoft Entra tenant
- Exercise 3: Synchronize Microsoft Entra ID forest with a Microsoft Entra tenant

Implement Directory Synchronization



Instructions

Exercise 1: Deploy an Azure VM hosting an Microsoft Entra ID domain controller

In this exercise, you will complete the following tasks:

- Task 1: Identify an available DNS name for an Azure VM deployment
- Task 2: Use an ARM template to deploy an Azure VM hosting an Microsoft Entra ID domain controller

Task 1: Identify an available DNS name for an Azure VM deployment

In this task, you will identify a DNS name for your Azure VM deployment.

1. Sign-in to the Azure portal `https://portal.azure.com/`.
   Note: Sign in to the Azure portal using an account that has the Owner or Contributor role in the Azure subscription you are using for this lab.

2. Open the Cloud Shell by clicking the first icon in the top right of the Azure Portal. If prompted, click **PowerShell** and **Create storage**.

3. Ensure **PowerShell** is selected in the drop-down menu in the upper-left corner of the Cloud Shell pane.

4. In the PowerShell session within the Cloud Shell pane, run the following to identify an available DNS name you can use for an Azure VM deployment in the next task of this exercise:

   ```
   Test-AzDnsAvailability -DomainNameLabel <custom-label> -Location '<location>'
   ```

   Note: Replace the `<custom-label>` placeholder with a valid DNS name that is likely to be globally unique. Replace the `<location>` placeholder with the name of the region into which you want to deploy the Azure VM that will host the Active Directory domain controller you will use in this lab.

   Note: To identify Azure regions where you can provision Azure VMs, refer to **https://azure.microsoft.com/en-us/regions/offers/**

5. Verify that the command returned **True**. If not, rerun the same command with a different value of the `<custom-label>` until the command returns **True**.

6. Record the value of the `<custom-label>` that resulted in the successful outcome. You will need it in the next task.

7. Close the Cloud Shell.

Task 2: Use an ARM template to deploy an Azure VM hosting an Microsoft Entra ID domain controller

In this task, you will deploy an Azure VM that will host an Microsoft Entra ID domain controller

1. Open another browser tab in the same browser window and navigate to the **https://github.com/Azure/azure-quickstart-templates/tree/master/application-workloads/active-directory/active-directory-new-domain**.

2. On the **Create an Azure VM with a new AD Forest** page, click **Deploy to Azure**. This will automatically redirect the browser to the **Create an Azure VM with a new AD Forest** blade in the Azure portal.

3. On the **Create an Azure VM with a new AD Forest** blade, click **Edit parameters**.

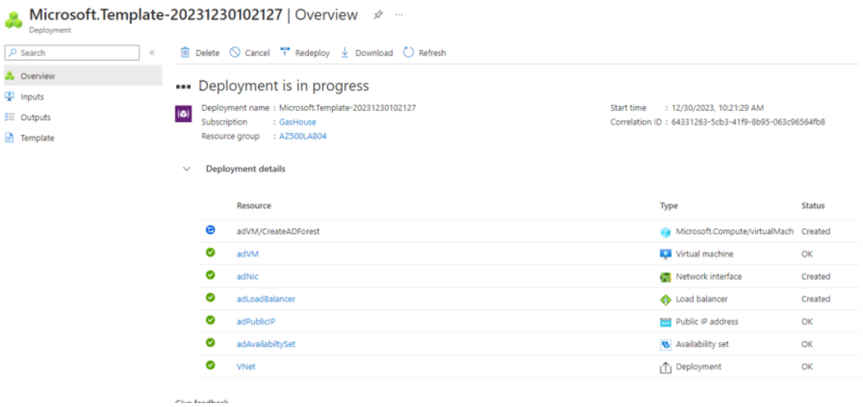
4. On the **Edit parameters** blade, click **Load file**, in the **Open** dialog box, navigate to the folder **\\AllFiles\Labs\06\active-directory-new-domain\azuredeploy.parameters.json**, click **Open**, and then click **Save**.

5. On the **Create an Azure VM with a new AD Forest** blade, specify the following settings (leave others with their existing values):

Setting	Value
Subscription	the name of you Azure subscription
Resource group	click **Create new** and type the name **AZ500LAB04**
Region	the Azure region you identified in the previous task
Admin Username	**Student**
Admin Password	**Please use your personal password created in Lab 02 > Exercise 1 > Task 1 > Step 9.**

Setting	Value
Domain Name	**adatum.com**
Dns Prefix	the DNS hostname you identified in the previous task
VM Size	**Standard_D2s_v3**

6. On the **Create an Azure VM with a new AD Forest** blade, click **Review + create**, and then click **Create**.



Deployment is in progress

Deployment name : Microsoft.Template-20231230102127
Subscription : GasHouse
Resource group : AZ500LAB04

Start time : 12/30/2023, 10:21:29 AM
Correlation ID : 64331263-5cb3-41f9-8b95-063c96564fb8

Deployment details

Resource	Type	Status
adVM/CreateADForest	Microsoft.Compute/virtualMach	Created
adVM	Virtual machine	OK
adNic	Network interface	Created
adLoadBalancer	Load balancer	Created
adPublicIP	Public IP address	OK
adAvailabiltySet	Availability set	OK
VNet	Deployment	OK

Note: Do not wait for the deployment to complete but instead proceed to the next exercise. The deployment might take about 15 minutes. You will use the virtual machine deployed in this task in the third exercise of this lab.

Result: After you completed this exercise, you have initiated deployment of an Azure VM that will host a Microsoft Entra ID domain controller by using an Azure Resource Manager template

Exercise 2: Create and configure an Microsoft Entra tenant

In this exercise, you will complete the following tasks:

- Task 1: Create a Microsoft Entra tenant
- Task 2: Add a custom DNS name to the new Microsoft Entra tenant
- Task 3: Create a Microsoft Entra ID user with the Global Administrator role

Task 1: Create a Microsoft Entra tenant

In this task, you will create a new Microsoft Entra tenant to use in this lab.

1. In the Azure portal, in the **Search resources, services, and docs** text box at the top of the Azure portal page, type **Microsoft Entra ID** and press the **Enter** key.

2. On the blade displaying **Overview** of your current Microsoft Entra tenant, click **Manage tenants**, and then on the next screen, click **+ Create**.

3. On the **Basics** tab of the **Create a tenant** blade, ensure that the option **Microsoft Entra ID** is selected and click **Next: Configuration >**.

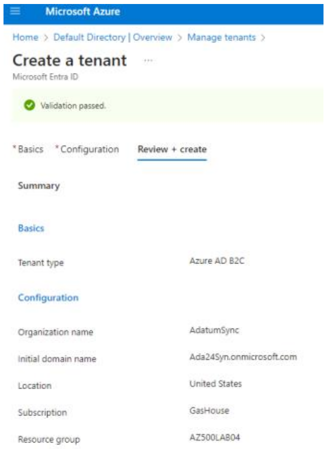
4. On the **Configuration** tab of the **Create a directory** blade, specify the following settings:

Setting	Value
Organization name	**AdatumSync**
Initial domain name	a unique name consisting of a combination of letters and digits
Country or region	**United States**

5. **Note**: Record the initial domain name. You will need it later in this lab.

6. **Note**: The green check mark in the **Initial domain name** text box will indicate whether the domain name you typed in is valid and unique. (Record your initial domain name for later use).

7. Click **Review + create** and then click **Create**.



Validation passed.

Summary

Basics

Tenant type	Azure AD B2C

Configuration

Organization name	AdatumSync
Initial domain name	Ada24Syn.onmicrosoft.com
Location	United States
Subscription	GasHouse
Resource group	AZ500LAB04

Note: Wait for the new tenant to be created. Use the **Notification** icon to monitor the deployment status.

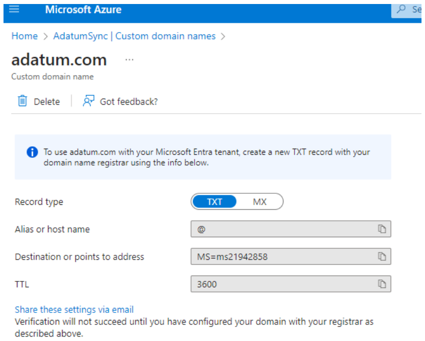
Task 2: Add a custom DNS name to the new Azure AD tenant

In this task, you will add your custom DNS name to the new Azure AD tenant.

1. In the Azure portal, in the toolbar, click the **Directory + subscription** icon, located to the right of the Cloud Shell icon.
2. In the **Directory + subscription** blade, select the newly created tenant **AdatumSync** line and click the **Switch** button.

   Note: You may need to refresh the browser window if the **AdatumSync** entry does not appear in the **Directory + subscription** filter list.

3. On the **AdatumSync | Microsoft Entra ID** blade, in the **Manage** section, click **Custom domain names**.
4. On the **AdatumSync | Custom domain names** blade, click **+ Add custom domain**.
5. On the **Custom domain name** blade, in the **Custom domain name** text box, type **adatum.com** and click **Add Domain**.
6. On the **adatum.com** blade, review the information necessary to perform verification of the Microsoft Entra domain name and then select **Delete** twice.



adatum.com
Custom domain name

To use adatum.com with your Microsoft Entra tenant, create a new TXT record with your domain name registrar using the info below.

Record type: TXT

Alias or host name: @

Destination or points to address: MS=ms21942858

TTL: 3600

Share these settings via email

Verification will not succeed until you have configured your domain with your registrar as described above.

   Note: You will not be able to complete the validation process because you do not own the **adatum.com** DNS domain name. This will not prevent you from synchronizing the **adatum.com** Microsoft Entra Domain Services domain with the Microsoft Entra tenant. You will use for this purpose the initial DNS name of the Microsoft Entra tenant (the name ending with the **onmicrosoft.com** suffix), which you identified in the previous task. However, keep in mind that, as a result, the DNS domain name of the Microsoft Entra Domain Services domain and the DNS name of the Microsoft Entra tenant will differ. This means that Adatum users will need to use different names when signing in to the Microsoft Entra Domain Services domain and when signing in to Microsoft Entra tenant.

Task 3: Create an Microsoft Entra ID user with the Global Administrator role

In this task, you will add a new Microsoft Entra ID user and assign them to the Global Administrator role.

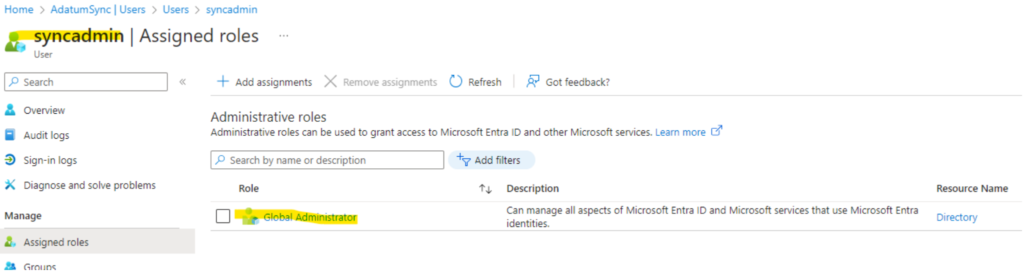
1. On the **AdatumSync** Microsoft Entra tenant blade, in the **Manage** section, click **Users**.
2. On the **Users | All users** blade, click **+ New User** and then **Create new user**.
3. On the **New user** blade, ensure that the **Create user** option is selected, specify the following settings on the Basics tab (leave all others with their default values) and click **Next: Properties >**:

Setting	Value
User name	**syncadmin**
Name	**syncadmin**
Password	ensure that the option **Auto-generate password** is selected and click **Show Password**

4. **Note**: Record the full user name. You can copy its value by clicking the **Copy to clipboard** button on the right-hand side of the drop-down list displaying the domain name and pasting it into a notepad document. You will need this later in this lab.
5. **Note**: Record the user's password by clicking the **Copy to clipboard** button on the right-hand side of the Password text box and pasting it into a notepad document. You will need this later in this lab.
6. On the **Properties** tab, scroll to the bottom and specify the Usage Location: **United States** (leave all others with their default values) and click **Next: Assignments >**.

7. On the **Assignments** tab, click **+ Add role**, search for and select **Global Administrator**, and then click **Select**. Click **Review + create** and then click **Create**.

   Note: An Azure AD user with the Global Administrator role is required in order to implement Microsoft Entra Connect.

   syncadmin | Assigned roles

   User

   Administrative roles

   Administrative roles can be used to grant access to Microsoft Entra ID and other Microsoft services. Learn more

	Role	Description	Resource Name
□	Global Administrator	Can manage all aspects of Microsoft Entra ID and Microsoft services that use Microsoft Entra identities.	Directory

8. Open an InPrivate browser window.

9. Navigate to the Azure portal at `https://portal.azure.com/` and sign in using the **syncadmin** user account. When prompted, change the password you recorded earlier in this task to your own password that meets the complexity requirements and record it for future reference. You will be prompted for this password in later tasks.
   Note: To sign in you will need to provide a fully qualified name of the **syncadmin** user account, including the Microsoft Entra tenant DNS domain name, which you recorded earlier in this task. This user name is in the format syncadmin@`<your_tenant_name>`.onmicrosoft.com, where `<your_tenant_name>` is the placeholder representing your unique Microsoft Entra tenant name.

10. Sign out as **syncadmin** and close the InPrivate browser window.

Result: After you completed this exercise, you have created an AMicrosoft Entra tenant, seen how to add a custom DNS name to the new Microsoft Entra tenant, and created an Azure AD user with the Global Administrator role.

Exercise 3: Synchronize Microsoft Entra ID forest with a Microsoft Entra tenant

In this exercise, you will complete the following tasks:

- Task 1: Prepare Microsoft Entra Domain Services for directory synchronization
- Task 2: Install Microsoft Entra Connect
- Task 3: Verify directory synchronization

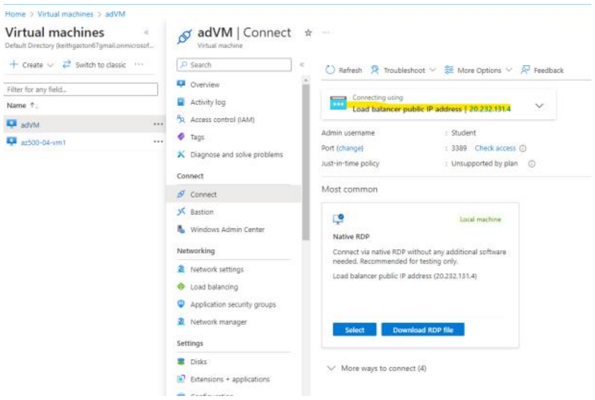
Task 1: Prepare Microsoft Entra Domain Services for directory synchronization

In this task, you will connect to the Azure VM running Microsoft Entra Domain Services domain controller and create a directory synchronization account.

Before you start this task, ensure that the template deployment you started in the first exercise of this lab has completed.

1. In the Azure portal, set the **Directory + subscription** filter to the the Microsoft Entra tenant associated with the Azure subscription into which you deployed the Azure VM in the first exercise of this lab.
2. In the Azure portal, in the **Search resources, services, and docs** text box at the top of the Azure portal page, type **Virtual machines** and press the **Enter** key.
3. On the **Virtual machines** blade, click the **adVM** entry.
4. On the **adVM** blade, click **Connect** and, in the drop down menu, click **RDP**.
5. In the **IP address** drop-down, select **Load balancer public IP address**, then click **Download RDP File** and use it to connect to the **adVM** Azure VM via Remote Desktop. When prompted to authenticate, provide the following credntials:

Setting	Value
User name	**Student**
Password	**Please use your personal password created in Lab 02 > Exercise 1 > Task 1 > Step 9.**



Connecting using
Load balancer public IP address | 20.232.131.4

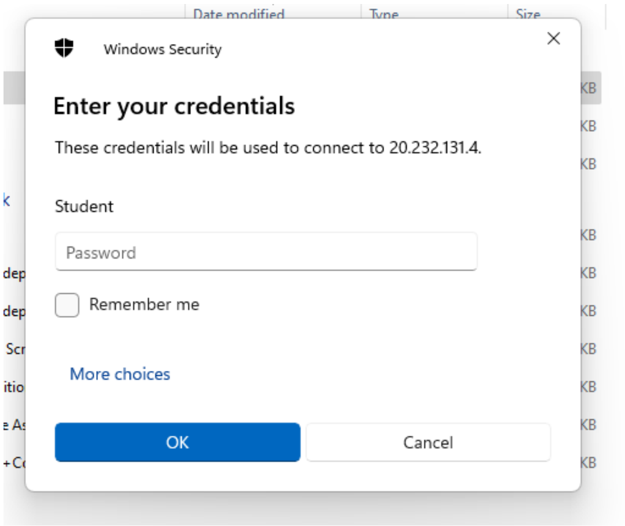
Admin username : Student
Port (change) : 3389 Check access
Just-in-time policy : Unsupported by plan

Connect via native RDP without any additional software needed. Recommended for testing only.
Load balancer public IP address (20.232.131.4)

6. **Note**: Wait for the Remote Desktop session and **Server Manager** to load.

7. **Note**: The following steps are performed in the Remote Desktop session to the **adVM** Azure VM.

8. **Note**: If the **Load balancer public IP address** is not available in the **IP address** drop-down of the RDP blade, in the Azure Portal search for **Public IP addresses**, select **adPublicIP** and note its IP address. Click the Start button, type **MSTSC** and hit **Enter** to launch the remote desktop client. Type the load balancer's public IP address in the **Computer:** text box and click **Connect**.



Windows Security

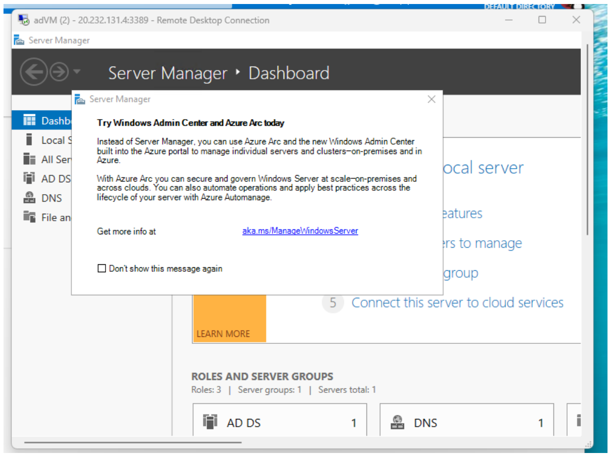
Enter your credentials

These credentials will be used to connect to 20.232.131.4.

Student

Password

□ Remember me



adVM (2) - 20.232.131.4:3389 - Remote Desktop Connection

Server Manager

Server Manager ‣ Dashboard

Server Manager

Try Windows Admin Center and Azure Arc today

Instead of Server Manager, you can use Azure Arc and the new Windows Admin Center built into the Azure portal to manage individual servers and clusters—on-premises and in Azure.

With Azure Arc you can secure and govern Windows Server at scale—on-premises and across clouds. You can also automate operations and apply best practices across the lifecycle of your server with Azure Automanage.

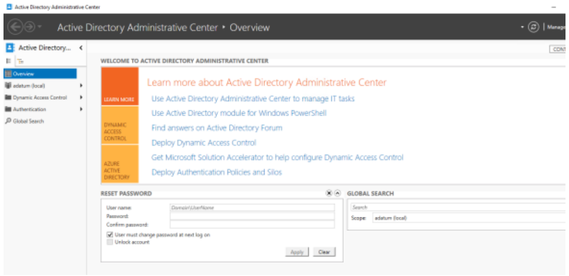
Get more info at aka.ms/ManageWindowsServer

□ Don't show this message again

ROLES AND SERVER GROUPS

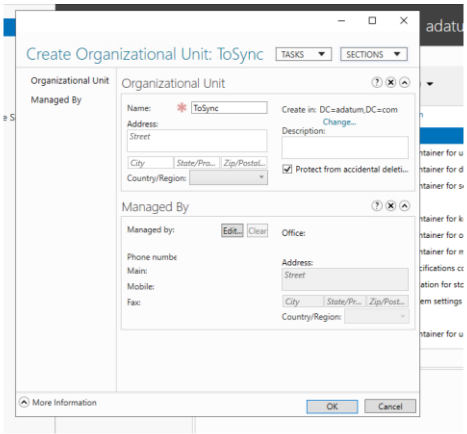
Roles: 3 | Server groups: 1 | Servers total: 1

9. In **Server Manager**, click **Tools** and, in the drop-down menu, click **Microsoft Entra ID Administrative Center**.


Active Directory Administrative Center
Active Directory Administrative Center • Overview
Active Directory...
Overview
adatum (local)
Dynamic Access Control
Authentication
Global Search
WELCOME TO ACTIVE DIRECTORY ADMINISTRATIVE CENTER
LEARN MORE
DYNAMIC ACCESS CONTROL
AZURE ACTIVE DIRECTORY
Learn more about Active Directory Administrative Center
Use Active Directory Administrative Center to manage IT tasks
Use Active Directory module for Windows PowerShell
Find answers on Active Directory Forum
Deploy Dynamic Access Control
Get Microsoft Solution Accelerator to help configure Dynamic Access Control
Deploy Authentication Policies and Silos
RESET PASSWORD
User name:
Password:
Confirm password:
☑ User must change password at next log on
□ Unlock account
Apply
Clear
GLOBAL SEARCH
Search
Scope: adatum (local)

10. In **Microsoft Entra admin center**, click **adatum (local)**, in the **Tasks** pane, under the domain name **adatum (local)** click **New**, and, in the cascading menu, click **Organizational Unit**.

11. In the **Create Organizational Unit** window, in the **Name** text box, type **ToSync** and click **OK**.


Create Organizational Unit: ToSync

Name: ToSync

Create in: DC=adatum,DC=com

☑ Protect from accidental deleti...

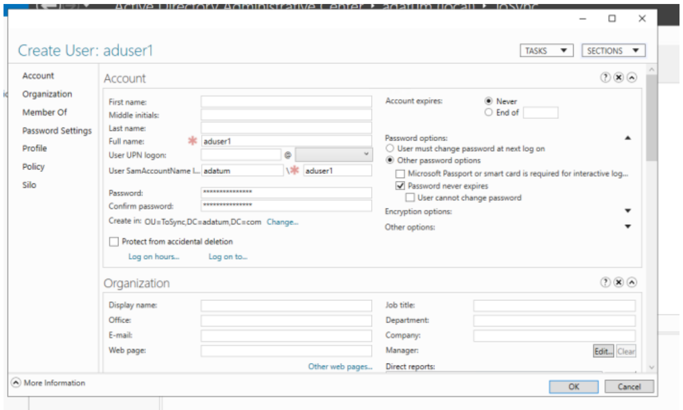
12. Double-click the newly created **ToSync** organizational unit such that its content appears in the details pane of the Microsoft Entra ID Administrative Center console.

13. In the **Tasks** pane, within the **ToSync** section, click **New**, and, in the cascading menu, click **User**.

14. In the **Create User** window, create a new user account with the following settings (leave others with their existing values) and click **OK**:

Setting	Value
Full Name	**aduser1**
User UPN logon	**aduser1**

Setting	Value
User SamAccountName logon	**aduser1**
Password and Confirm Password	**Please use your personal password created in Lab 02 > Exercise 1 > Task 1 > Step 9.**
Other password options	**Password never expires**


Create User: aduser1

Account

First name:
Middle initials:
Last name:
Full name: aduser1
User UPN logon: @
User SamAccountName l... adatum \ aduser1
Password: ***************
Confirm password: ***************
Create in: OU=ToSync,DC=adatum,DC=com Change...
□ Protect from accidental deletion

Account expires: ● Never ○ End of
Password options:
○ User must change password at next log on
● Other password options
□ Microsoft Passport or smart card is required for interactive log...
☑ Password never expires
□ User cannot change password
Encryption options:
Other options:

Organization

Display name:
Office:
E-mail:
Web page:
Job title:
Department:
Company:
Manager:
Direct reports:

Task 2: Install Microsoft Entra Connect

In this task, you will install Microsoft Entra Connect on the virtual machine.

1. Within the Remote Desktop session to **adVM**, use Microsoft Edge to navigate to the Azure portal at **https://portal.azure.com**, and sign in by using the **syncadmin** user account you created the previous exercise. When prompted, specify the full User principal name and password that you recorded in the previous exercise.

2. In the Azure portal, in the **Search resources, services, and docs** text box at the top of the Azure portal page, type **Microsoft Entra ID** and press the **Enter** key.

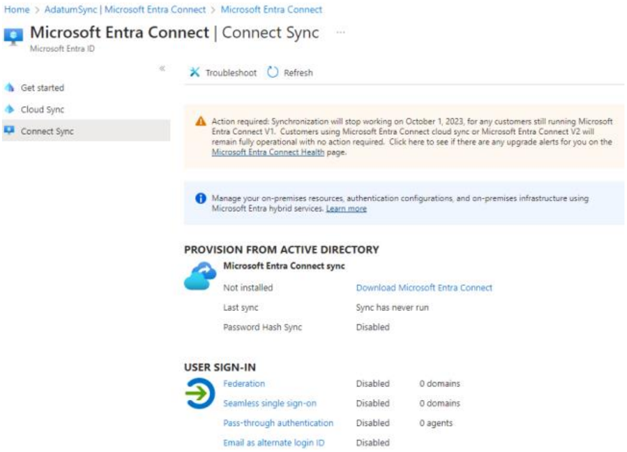
3. In the Azure portal, on the **AdatumSync | Overview** blade, in the left navigation panel under **Manage**, click **Microsoft Entra Connect**.

4. On the **Microsoft Entra Connect | Get started** blade, click **Connect Sync** in the left navigation panel and then click the **Download Microsoft Entra Connect** link. You will be redirected to the **Microsoft Entra Connect** download page.

5. On the **Microsoft Entra Connect** download page, click **Download**.

6. When prompted, click **Run** to start the **Microsoft Entra Connect** wizard.

7. On the **Welcome to Microsoft Entra Connect** page of the **Microsoft Entra Connect** wizard, click the checkbox **I agree to the license terms and privacy notice** and click **Continue**.


Home > AdatumSync | Microsoft Entra Connect > Microsoft Entra Connect
Microsoft Entra Connect | Connect Sync
Microsoft Entra ID
Get started
Cloud Sync
Connect Sync
Troubleshoot
Refresh

Action required: Synchronization will stop working on October 1, 2023, for any customers still running Microsoft Entra Connect V1. Customers using Microsoft Entra Connect cloud sync or Microsoft Entra Connect V2 will remain fully operational with no action required. Click here to see if there are any upgrade alerts for you on the Microsoft Entra Connect Health page.

Manage your on-premises resources, authentication configurations, and on-premises infrastructure using Microsoft Entra hybrid services. Learn more

PROVISION FROM ACTIVE DIRECTORY

Microsoft Entra Connect sync

Not installed	Download Microsoft Entra Connect
Last sync	Sync has never run
Password Hash Sync	Disabled

USER SIGN-IN

Federation	Disabled	0 domains
Seamless single sign-on	Disabled	0 domains
Pass-through authentication	Disabled	0 agents
Email as alternate login ID	Disabled	

8. On the **Express Settings** page of the **Microsoft Entra Connect** wizard, click the **Customize** option.

9. On the **Install required components** page, leave all optional configuration options deselected and click **Install**.

10. On the **User sign-in** page, ensure that only the **Password Hash Synchronization** is enabled and click **Next**.

11. On the **Connect to Microsoft Entra ID** page, authenticate by using the credentials of the **syncadmin** user account you created in the previous exercise and click **Next**.

12. On the **Connect your directories** page, click the **Add Directory** button to the right of the **adatum.com** forest entry.

13. In the **AD forest account** window, ensure that the option to **Create new Microsoft Entra ID account** is selected, specify the following credentials, and click **OK**:

Setting	Value
User Name	**ADATUM\Student**
Password	**Please use your personal password created in Lab 04 > Exercise 1 > Task 2**

14. Back on the **Connect your directories** page, ensure that the **adatum.com** entry appears as a configured directory and click **Next**

15. On the **Microsoft Entra ID sign-in configuration** page, note the warning stating **Users will not be able to sign-in to Microsoft Entra ID with on-premises credentials if the UPN suffix does not match a verified domain name**, enable the checkbox **Continue without matching all UPN suffixes to verified domain**, and click **Next**.

    Note: As explained earlier, this is expected, since you could not verify the custom Microsoft Entra ID DNS domain **adatum.com**.

16. On the **Domain and OU filtering** page, click the option **Sync selected domains and OUs** and clear the checkbox next to the domain name **adatum.com**. Click to expand **adatum.com**, select only the checkbox next to the **ToSync** OU, and then click **Next**.

17. On the **Uniquely identifying your users** page, accept the default settings, and click **Next**.

18. On the **Filter users and devices** page, accept the default settings, and click **Next**.

19. On the **Optional features** page, accept the default settings, and click **Next**.

20. On the **Ready to configure** page, ensure that the **Start the synchronization process when configuration completes** checkbox is selected and click **Install**.

    Note: Installation should take about 2 minutes.

21. Review the information on the **Configuration complete** page and click **Exit** to close the **Microsoft Entra Connect** window.

Task 3: Verify directory synchronization

In this task, you will verify that directory synchronization is working.

1. Within the Remote Desktop session to **adVM**, in the Microsoft Edge window displaying the Azure portal, navigate to the **Users - All users (Preview)** blade of the Adatum Lab AMicrosoft Entra ID tenant.

2. On the **Users | All users** blade, note that the list of user objects includes the **aduser1** account.

   Note: You might have to wait a few minutes and select **Refresh** for the **aduser1** user account to appear.

3. Click the **aduser1** account and select the **Properties** tab. Scroll down to the **On-premises** section, note that the **On-premises sync enabled** attribute is set to **Yes**.

4. On the **aduser1** blade, in the **Job Information** section, note that the **Department** attribute is not set.

5. Within the Remote Desktop session to **adVM**, switch to the **Microsoft Entra admin center**, select the **aduser1** entry in the list of objects in the **ToSync** OU, and, in the **Tasks** pane, in the **aduser1** section, select **Properties**.

6. In the **aduser1** window, in the **Organization** section, in the **Department** text box, type **Sales**, and select **OK**.

7. Within the Remote Desktop session to **adVM**, start **Windows PowerShell**.

8. From the **Administrator: Windows PowerShell** console, run the following to start Microsoft Entra Connect delta synchronization:

```
9.  Import-Module -Name 'C:\Program Files\Microsoft Azure AD
    Sync\Bin\ADSync\ADSync.psd1'
10.
    Start-ADSyncSyncCycle -PolicyType Delta
```

11. Switch to the Microsoft Edge window displaying the **aduser1** blade, refresh the page and note that the Department property is set to Sales.

    Note: You might need to wait for up to three minutes and refresh the page again if the **Department** attribute remains not set.

Result: After you completed this exercise, you have prepared Microsoft Entra Domain Services for directory synchronization, installed Microsoft Entra Connect, and verified directory synchronization.

Clean up resources

Note: Start by disabling Microsoft Entra ID synchronization

1. Within the Remote Desktop session to **adVM**, start Windows PowerShell as Administrator.

2. From the Windows PowerShell console, install the MsOnline PowerShell module by running the following (when prompted, in the NuGet provider is required to continue dialog box, type **Yes** and hit Enter.):

```
3. [Net.ServicePointManager]::SecurityProtocol =
   [Net.SecurityProtocolType]::Tls12
4. Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force
   Install-Module MsOnline -Force
```

5. From the Windows PowerShell console, connect to the AdatumSync Microsoft Entra tenant by running the following (when prompted, sign in with the **syncadmin** credentials):

   ```
   Connect-MsolService
   ```

6. From the Windows PowerShell console, disable the Microsoft Entra Connect synchronization by running the following:

   ```
   Set-MsolDirSyncEnabled -EnableDirSync $false -Force
   ```

7. From the Windows PowerShell console, verify that the operation was successful by running the following:

   ```
   (Get-MSOLCompanyInformation).DirectorySynchronizationEnabled
   ```

   Note: The result should be `False`. If that is not the case, wait a minute and re-run the command.

   Note: Next, remove the Azure resources

8. Close the Remote desktop session.

9. In the Azure portal, set the **Directory + subscription** filter to the Microsoft Entra tenant associated with the Azure subscription into which you deployed the **adVM** Azure VM.

10. In the Azure portal, open the Cloud Shell by clicking the first icon in the top right of the Azure Portal.

11. In the drop-down menu in the upper-left corner of the Cloud Shell pane, select **PowerShell**, and, when prompted, click **Confirm**.

12. In the PowerShell session within the Cloud Shell pane, run the following to remove the resource group you created in this lab:

    ```
    Remove-AzResourceGroup -Name "AZ500LAB06" -Force -AsJob
    ```

13. Close the **Cloud Shell** pane.

    Note: Finally, remove the Microsoft Entra tenant

    Note 2: Deleting a tenant is meant to be a very hard process, so it can never accidentally or maliciously be done. That means that removing the tenant as part of this lab often does not work. While we have the steps here to delete the tenant, it is not required to consider yourself as completing this lab. If you ever have a need to remove a tenant in the real world, there are articles on DOCS.Microsoft.com to help you.

14. Back in the Azure portal, use the **Directory + subscription** filter to switch to the **AdatumSync** Microsoft Entra tenant.

15. In the Azure portal, navigate to the **Users - All users** blade, click the entry representing the **syncadmin** user account, on the **syncadmin - Profile** blade click **Delete**, and, when prompted to confirm, click **Yes**.

16. Repeat the same sequence of steps to delete the **aduser1** user account and the **On-Premises Directory Synchronization Service Account**.

17. Navigate to the **AdatumSync - Overview** blade of the Microsoft Entra tenant, click **Manage tenants** and select the check box of the **AdatumSync** directory, click **Delete**, on the **Delete tenant 'AdatumSync'** blade, click the **Get permission to delete Azure resources** link, on the **Properties** blade of AMicrosoft Entra, set **Access management for Azure resources** to **Yes** and click **Save**.

    Note: While deleting if you receive any warning sign like **Delete all users** then proceed to delete the users that you have created or if the warning sign says **Delete LinkedIn applications** click on the warning message and confirm the deletion of the LinkedIn application, all the warning need to be addressed to pass the deletion of the tenant.

18. Sign out from the Azure portal and sign in back.

19. Navigate back to the **Delete tenant 'AdatumSync'** blade and click **Delete**.