Implementing and Managing Hybrid Identities

The following topics will be covered in this document:

- Azure AD Connect
- Azure AD Connect installation
- Manage Azure AD Connect
- Password writeback
- Password sync

We will discuss Azure AD Connect and see how to configure and sync the on-premises identity to Azure AD. We will explain the password writeback and password sync that will help to sync the password Azure to onpremises.

1- Azure AD Connect

The Azure AD Connect service can be used to synchronize your on-premises active directory identities to Azure AD. It helps to connect your on-premises users to Azure and other applications to get authentication with Azure AD. It is called hybrid connectivity.

Integrating the on-premises identity with Azure AD provides the common identity for accessing cloud and on-premises resources. We can use the single identity to access the on-premises and cloud-based applications like Office 365, SharePoint Online, and so on.

It provides the following features:

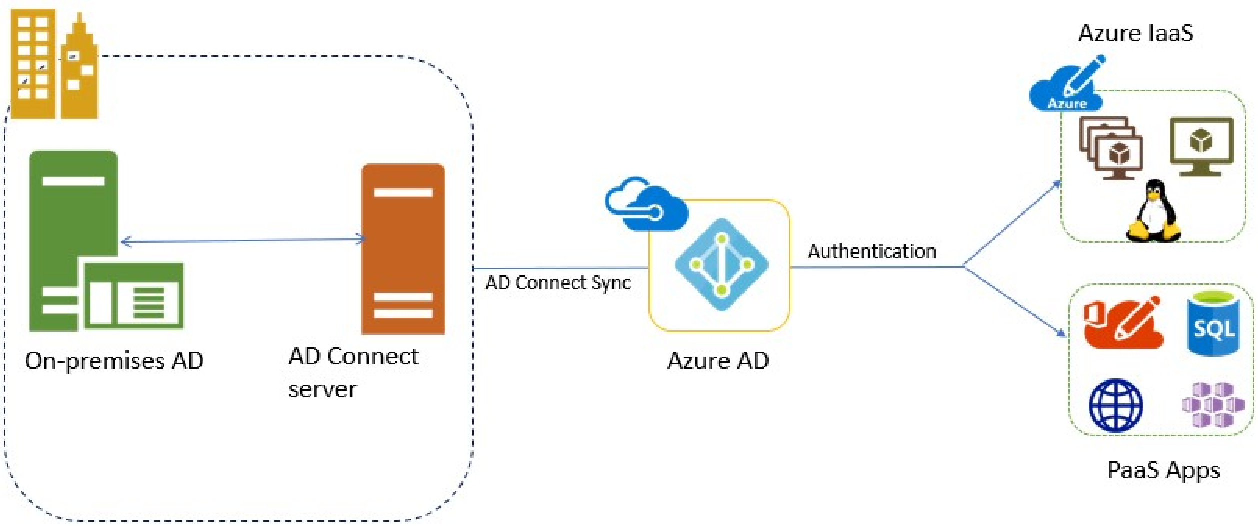
Password hash synchronization	It provides the single sign-on (SSO) method to synchronize the password of users by synchronizing the password of on-premises users

	to Azure AD in the hash format.
Pass-through authentication	It allows users to use the same password of on-premises and cloud for signing in to applications. Only the pass-through agent gets installed, and as per the number of authentications per second, we may need more than one agent.
Federation integration	Federation services can be used to configure the setup of the hybrid environment and SSO while configuring on-premises Active Directory Federation Services (ADFS) which require an additional server.
Synchronization	It helps to create users, groups, and other objects. It verifies if the identity information of on-premises users and groups match with the cloud identity. It synchronizes password hashes as well.
Health monitoring	Azure AD Connect Health provides monitoring for Azure AD Connect, and we can see Azure AD Connect health-related information/errors on the Azure portal.

Azure AD Connect services can be installed in a separate server in the onpremises AD and can be tightly integrated with Azure AD after installation and configuration. Azure sync services will sync the on-premise AD component to Azure AD.

On-premises and Azure users can use the same credentials to log in to Azure and on-premises. For more details, you can refer to Azure AD Connect, which helps you to understand the components.

Please take a look the following diagram:



1.1- Azure AD Connect installation

Before you install the Azure AD Connect, you need to have the following prerequisites, without which, you will not be able to configure the Azure AD. The following requirements are mandatory. We can see these properties been asked during configuration:

- You should have an Azure AD services/user account which has global admin rights to configure the Azure AD Connect to Azure AD.
- You should have an on-premises services/user account which has enterprise admin rights to configure the Azure AD Connect to Azure AD.
- Please download the Azure AD Connect from

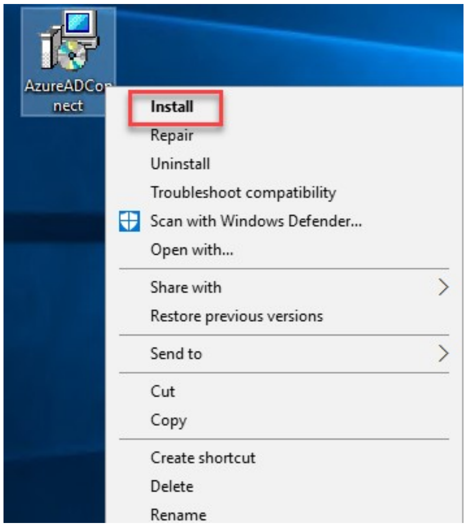
https://www.microsoft.com/en-us/download/details.aspx?id=47594 .

- Whenever you configure the AD Connect, the domain name should match with a public domain name, or else you will get a warning message.

Please follow the given steps to configure the Azure AD Connect:

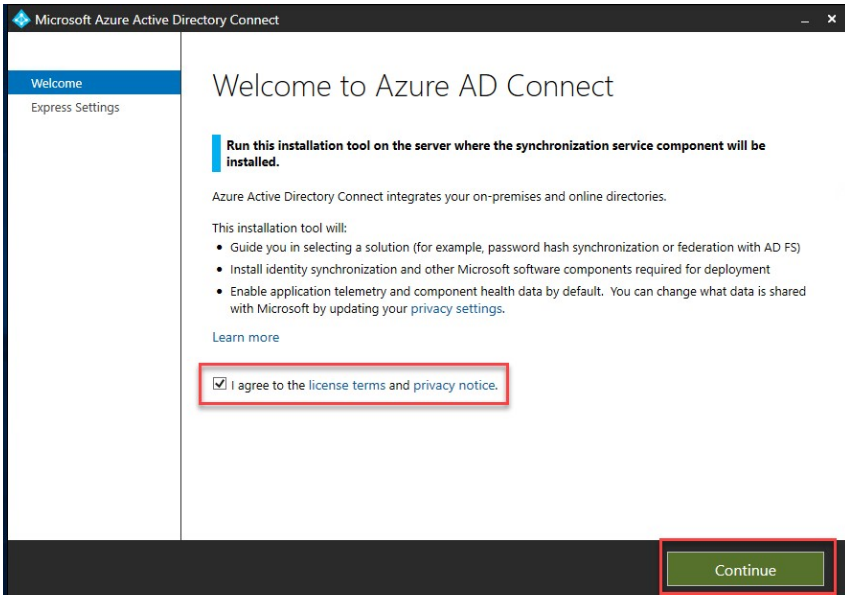
1. Download the Azure AD Connect (https://www.microsoft.com/enus/download/details.aspx?id=47594), or you can download it from the Azure portal.

2. Click on the AD Connect MSI setup and then click on **Install**. Please take a look at the following screenshot:



3. Once you click on the **Install** option, the installation wizard will open.

4. Please agree to the license terms and policy and click on the **Continue** button as shown in the following screenshot:



Welcome to Azure AD Connect

Run this installation tool on the server where the synchronization service component will be installed.

Azure Active Directory Connect integrates your on-premises and online directories.

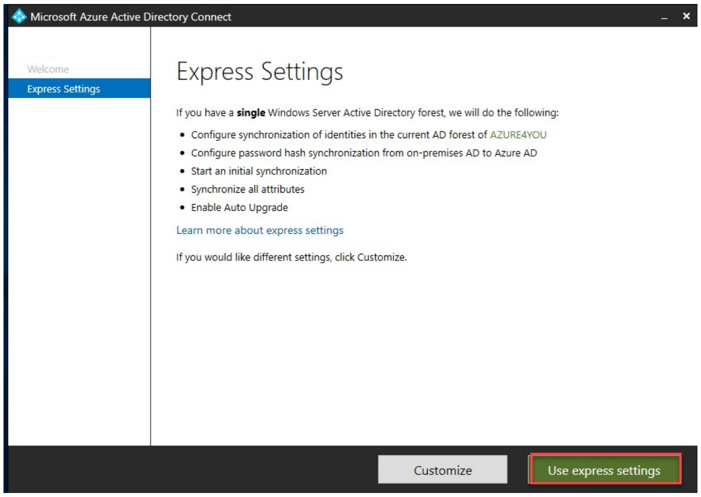
This installation tool will:

- Guide you in selecting a solution (for example, password hash synchronization or federation with AD FS)
- Install identity synchronization and other Microsoft software components required for deployment
- Enable application telemetry and component health data by default. You can change what data is shared with Microsoft by updating your privacy settings.

Learn more

☑ I agree to the license terms and privacy notice.

5. Once done, select the **Express Settings** to configure the Azure AD Connect as shown in the following screenshot:



Express Settings

If you have a **single** Windows Server Active Directory forest, we will do the following:

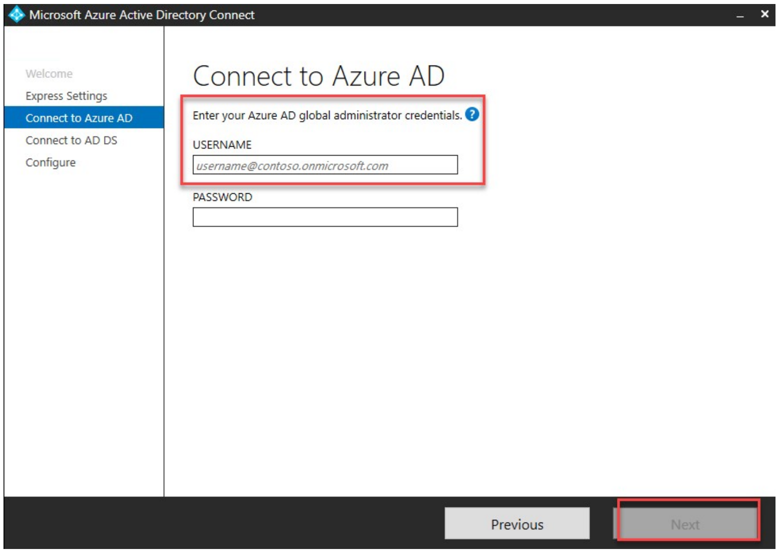
- Configure synchronization of identities in the current AD forest of AZURE4YOU
- Configure password hash synchronization from on-premises AD to Azure AD
- Start an initial synchronization
- Synchronize all attributes
- Enable Auto Upgrade

Learn more about express settings

If you would like different settings, click Customize.

6. When you click on the use express settings, it will ask you to provide the global administrator credentials which have *.onmicrosoft.com* in the user ID as shown in the following screenshot.

It will connect to the Azure AD and verify the credentials before we proceed to the next step as shown in the following screenshot:



Connect to Azure AD

Enter your Azure AD global administrator credentials.

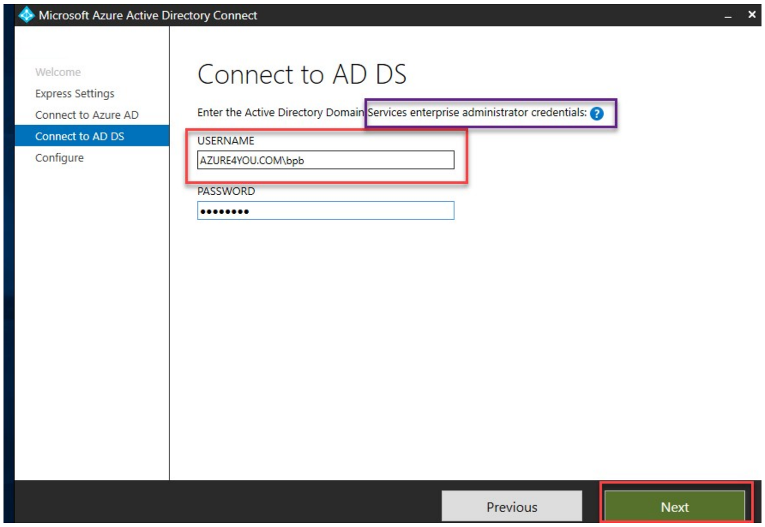
USERNAME: username@contoso.onmicrosoft.com

PASSWORD:

7. Provide the services admin credentials which have enterprise admin rights.

8. While providing the credentials, please follow domainname.com\userid.

9. Once you provide the credentials, click on the **Next** button as shown in the following screenshot:



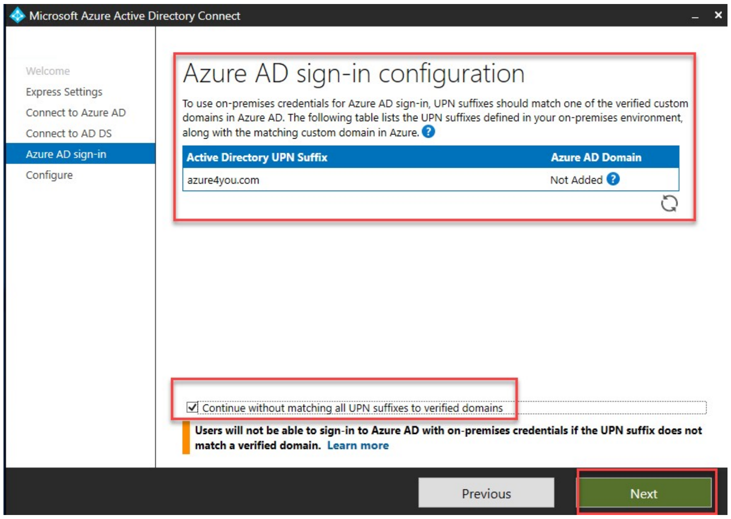
Connect to AD DS

Enter the Active Directory Domain Services enterprise administrator credentials:

USERNAME: AZURE4YOU.COM\bpb

PASSWORD: ••••••••

10. Then, it will ask you to verify the UPN suffix, but if you are doing this installation in production, then please match the UPN suffix and move forward. Please take a look at the following screenshot:



Azure AD sign-in configuration

To use on-premises credentials for Azure AD sign-in, UPN suffixes should match one of the verified custom domains in Azure AD. The following table lists the UPN suffixes defined in your on-premises environment, along with the matching custom domain in Azure.

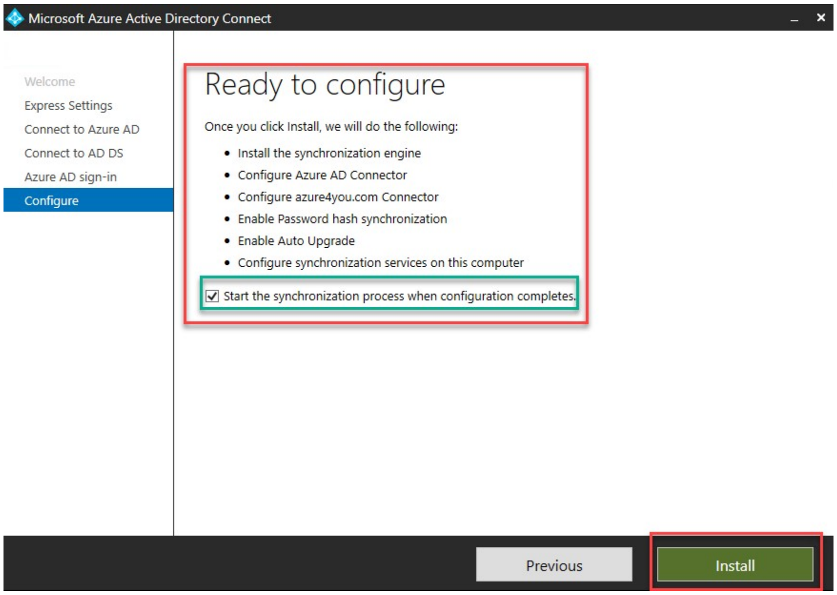
Active Directory UPN Suffix	Azure AD Domain
azure4you.com	Not Added

☑ Continue without matching all UPN suffixes to verified domains

Users will not be able to sign-in to Azure AD with on-premises credentials if the UPN suffix does not match a verified domain. Learn more

11. Once you click on **Next**, you are ready for configuration.

12. Start the synchronization process when the configuration is completed. But in production, it’s recommended that you start the synchronization process only after the AD Connect installation. Please take a look at the following screenshot:



Ready to configure

Once you click Install, we will do the following:

- Install the synchronization engine
- Configure Azure AD Connector
- Configure azure4you.com Connector
- Enable Password hash synchronization
- Enable Auto Upgrade
- Configure synchronization services on this computer

☑ Start the synchronization process when configuration completes.

13. When you click on next, first it will verify the connectivity between Azure AD and on-premise. Then, it will configure the connection between Azure AD and on-premises AD.

14. It will install the sync services and verify the Azure AD.

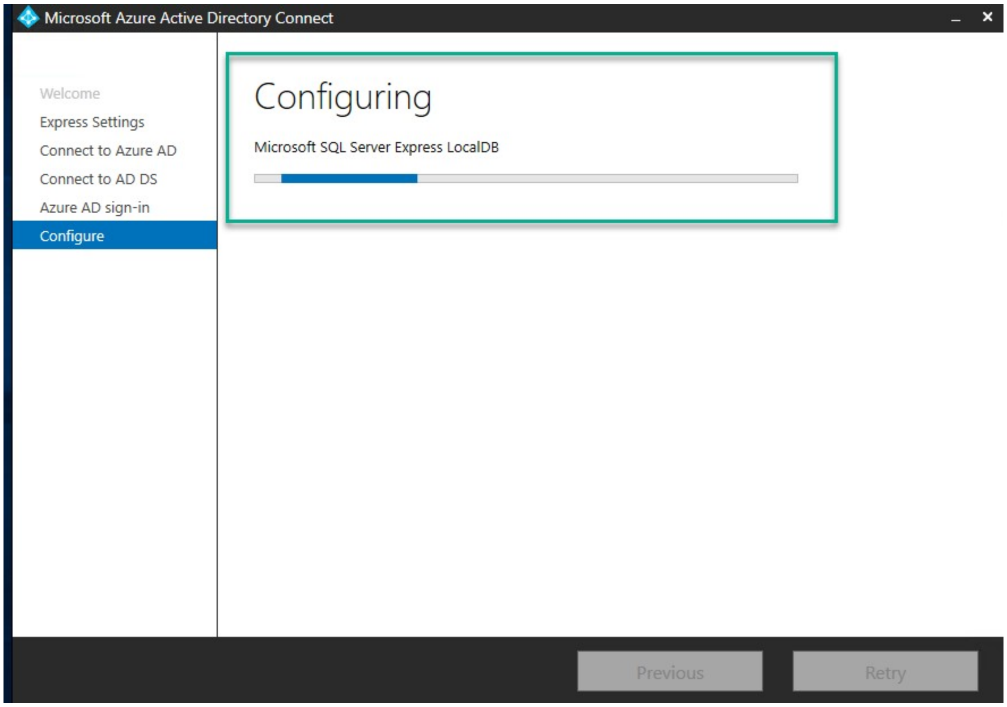
15. Now, it will configure the Azure AD and update the sync.

16. After that, it will configure the setup to the on-premise domain.

17. After that, it will enable the password hash sync.

18. Now, it will save the sync settings.

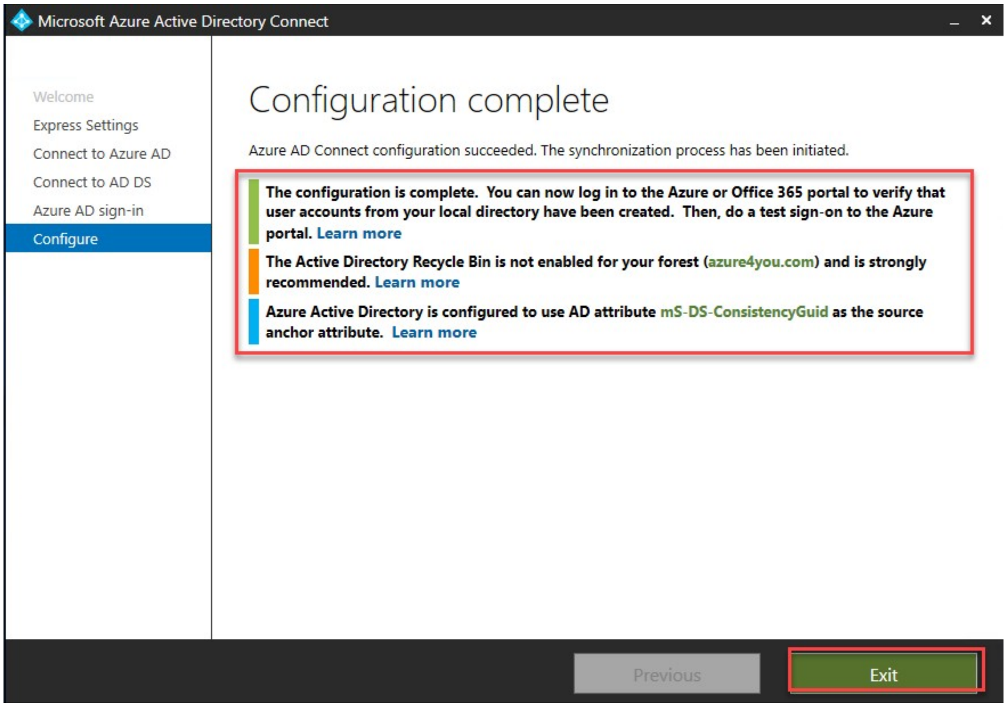
19. After that, the final steps will be performed by the AD Connect setup to install and configure the AD Connect Health agent for sync services as shown in the following screenshot:



Configuring

Microsoft SQL Server Express LocalDB

20. Now, the setup has been completed. So, exit from the setup as shown in the following screenshot:



Configuration complete

Azure AD Connect configuration succeeded. The synchronization process has been initiated.

The configuration is complete. You can now log in to the Azure or Office 365 portal to verify that user accounts from your local directory have been created. Then, do a test sign-on to the Azure portal. Learn more

The Active Directory Recycle Bin is not enabled for your forest (azure4you.com) and is strongly recommended. Learn more

Azure Active Directory is configured to use AD attribute mS-DS-ConsistencyGuid as the source anchor attribute. Learn more

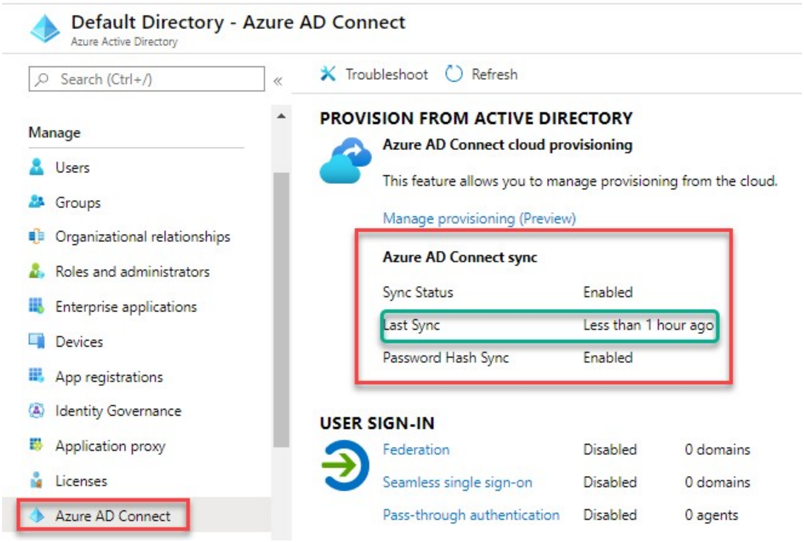
2- Manage Azure AD Connect

We can manage the Azure AD Connect from the portal after installation, and we can see the configuration details of the on-premises AD. Please follow the given steps:

1. Please log in to the Azure portal.

2. Go to **Azure AD Connect** under the **Manage** tab and click on the Azure AD Connect.

You will be able to see the last sync is **Less than 1 hour ago** and the sync status has been enabled as shown in the following screenshot:



PROVISION FROM ACTIVE DIRECTORY

Azure AD Connect cloud provisioning

This feature allows you to manage provisioning from the cloud.

Manage provisioning (Preview)

Azure AD Connect sync

Sync Status	Enabled
Last Sync	Less than 1 hour ago
Password Hash Sync	Enabled

USER SIGN-IN

Federation	Disabled	0 domains
Seamless single sign-on	Disabled	0 domains
Pass-through authentication	Disabled	0 agents

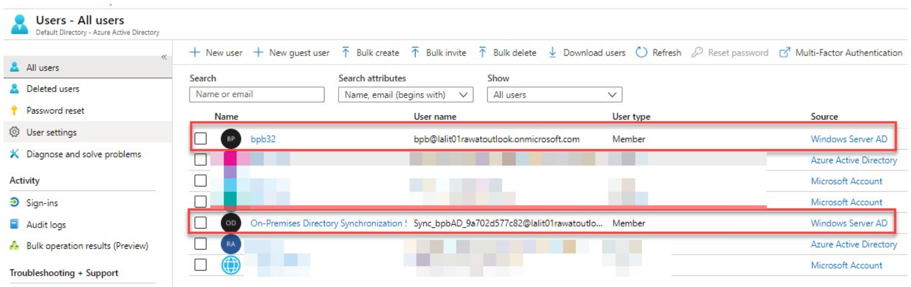
3. We can also set up the **Federation**, **Seamless single sign-on**, and **Pass-through authentication** services.

4. Azure AD health services can be managed from the same portal.

5. Let us check whether the users have been synced to Azure AD or not.

6. We will go to the **Users** tab and check the on-premise users which are synced from your on-premises AD.

7. Now, in the following screenshot, you can see the user bpb32 source is **Windows Server AD**, and if you can see Azure AD users, the sources are Azure AD:



Search: Name or email

Search attributes: Name, email (begins with)

Show: All users

	Name	User name	User type	Source
□	bpb32	bpb@lalit01rawatoutlook.onmicrosoft.com	Member	Windows Server AD
□	[redacted]	[redacted]	[redacted]	Azure Active Directory
□	[redacted]	[redacted]	[redacted]	Microsoft Account
□	[redacted]	[redacted]	[redacted]	Microsoft Account
□	On-Premises Directory Synchronization !	Sync_bpbAD_9a702d577c82@lalit01rawatoutlo...	Member	Windows Server AD
□	[redacted]	[redacted]	[redacted]	Azure Active Directory
□	[redacted]	[redacted]	[redacted]	Microsoft Account

3- Password writeback

Password writeback will help you to synchronize the password which has been changed in Azure AD to on-premises AD. This feature needs to be enabled from the Azure AD Connect and provides the security mechanism to send the password from Azure AD to the on-premises AD. It provides the following features:

Enforcement of on-premises AD password policies	If users reset their passwords, then it is ensured to meet your on-premises AD policy before committing it to the directory. This review process includes history, complexity, age, password filters, and other password restrictions which have been defined in your on-premises AD.
Zero-delay feedback	Password writeback syncs the operations and users are notified immediately if their password doesn't meet the password policy or can't be changed for any reason.
Supports password changes from the access panel and Office 365	When federated or password hash synchronized users need to change their expired or non-expired passwords, those passwords are written back to your local AD environment.
Supports password writeback when an admin resets them from the Azure portal	When an admin resets a user's password in the Azure portal, if that user is federated or password hash synchronized, the password is written back to on-premises AD, but this functionality is not supported from the office admin portal

Doesn't require any inbound firewall rules	Password writeback uses an Azure service relay as an underlying communication channel and all commutation is outbound over port 443

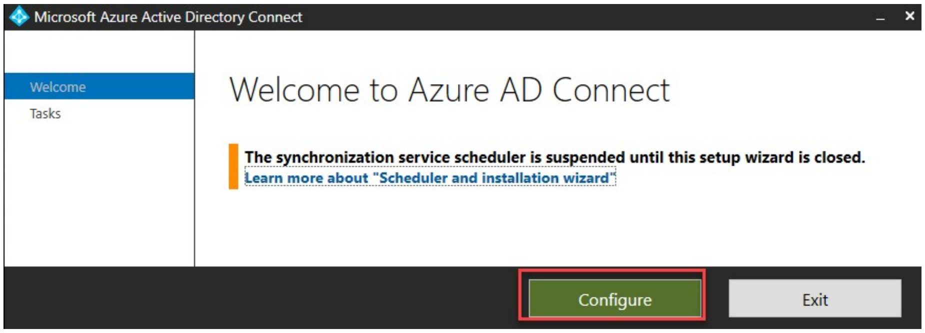
3.1- Enabling the password writeback from the Azure AD

Perform the following steps:

1. Log in to on-premises machines where you have installed the Azure AD.

2. Open the Azure AD Connect, and you will see the welcome wizard.

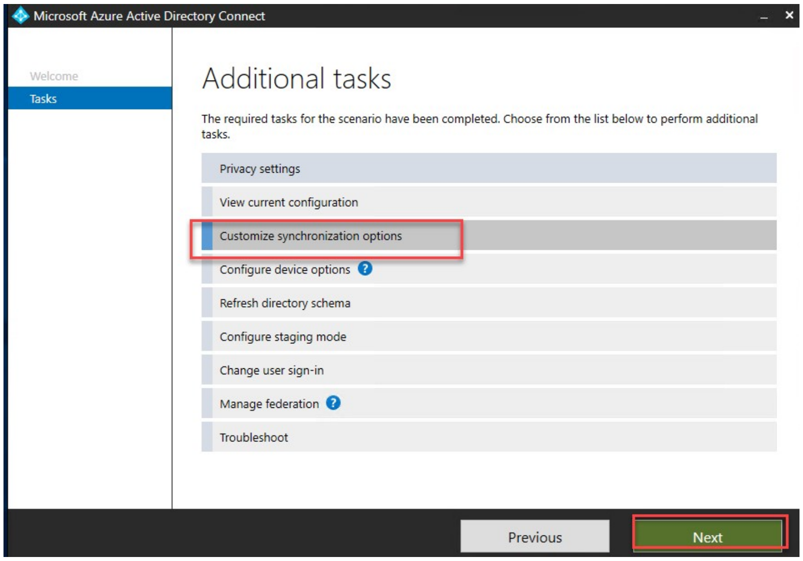
3. Click on **Configure** as shown in the following screenshot:



Welcome to Azure AD Connect

The synchronization service scheduler is suspended until this setup wizard is closed.
Learn more about "Scheduler and installation wizard"

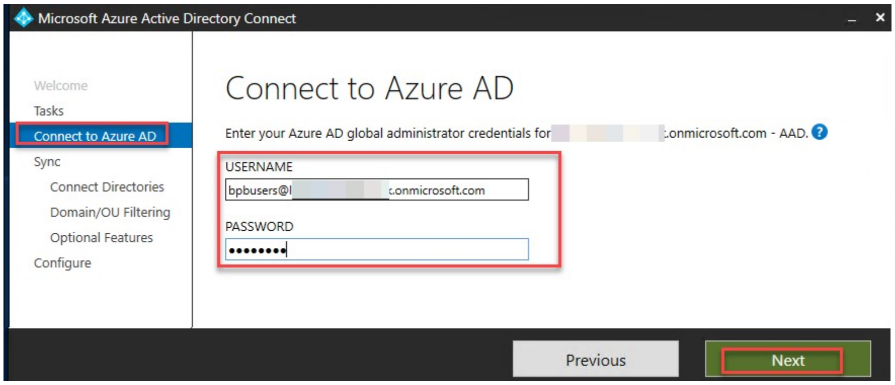
4. Click on **Customize synchronization options** to configure the password writeback. Please take a look at the following screenshot:



Additional tasks

The required tasks for the scenario have been completed. Choose from the list below to perform additional tasks.

It will ask you to connect to the Azure AD and provide the credentials to configure it as shown in the following screenshot:



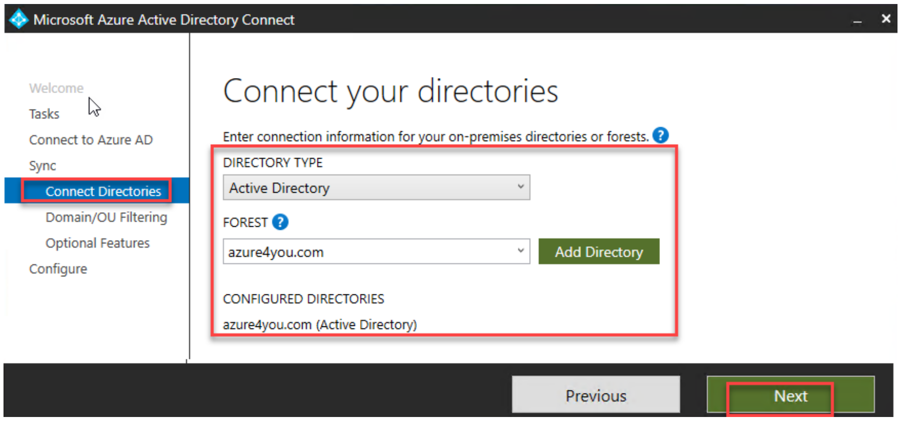
Connect to Azure AD

Enter your Azure AD global administrator credentials for [redacted].onmicrosoft.com - AAD.

USERNAME: bpbusers@[redacted].onmicrosoft.com

PASSWORD: ••••••••

Now, please select the type of the directory and forest. Click on the **Next** button as shown in the following screenshot



Connect your directories

Enter connection information for your on-premises directories or forests.

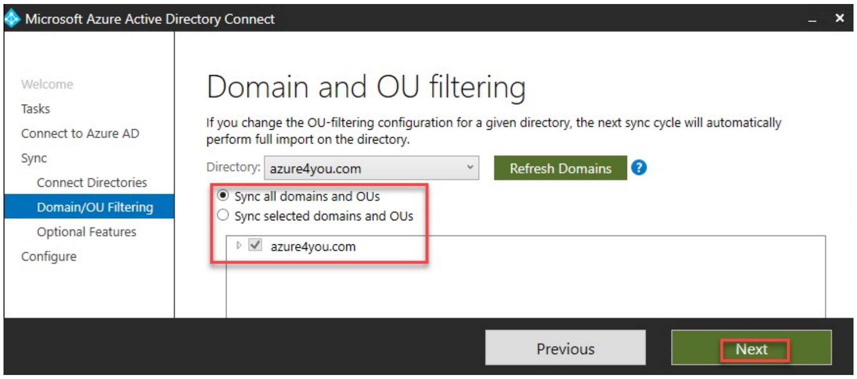
DIRECTORY TYPE: Active Directory

FOREST: azure4you.com

CONFIGURED DIRECTORIES

azure4you.com (Active Directory)

Now, you can select **Sync all domains and OUs** and your domain as well as shown in the following screenshot:



Domain and OU filtering

If you change the OU-filtering configuration for a given directory, the next sync cycle will automatically perform full import on the directory.

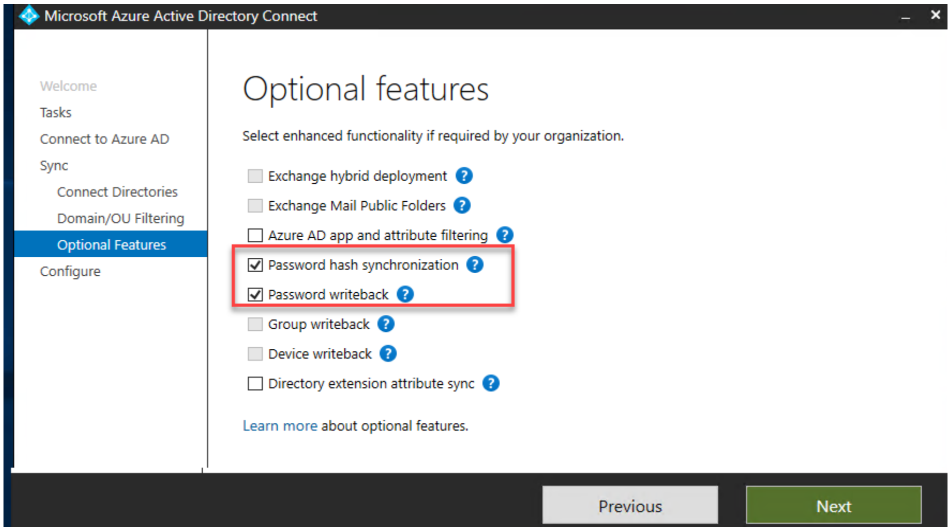
Directory: azure4you.com

● Sync all domains and OUs

○ Sync selected domains and OUs

☑ azure4you.com

Please select the password writeback and click on the **Next** button as shown in the following screenshot:



Optional features

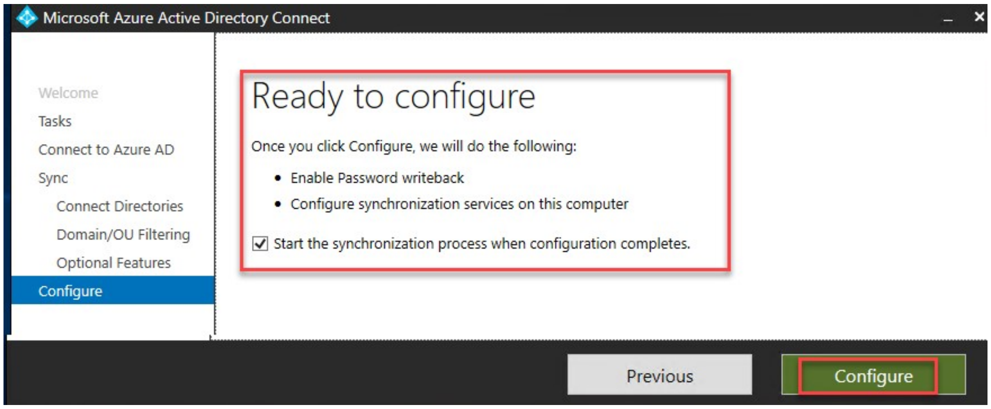
Select enhanced functionality if required by your organization.

- □ Exchange hybrid deployment
- □ Exchange Mail Public Folders
- □ Azure AD app and attribute filtering
- ☑ Password hash synchronization
- ☑ Password writeback
- □ Group writeback
- □ Device writeback
- □ Directory extension attribute sync

Learn more about optional features.

5. Once you are done with **Next**, it will verify all the settings and be ready for configuration.

6. Click on the **Configure** button. It will take a few minutes to complete the sync process and enable the password writeback. Please take a look at the following screenshot:



Ready to configure

Once you click Configure, we will do the following:

- Enable Password writeback
- Configure synchronization services on this computer

☑ Start the synchronization process when configuration completes.

In this section, we explained and demonstrated how to configure the password writeback. In the next section, we will demonstrate enabling the password writeback from the portal.

3.2- Enabling password writeback from the portal

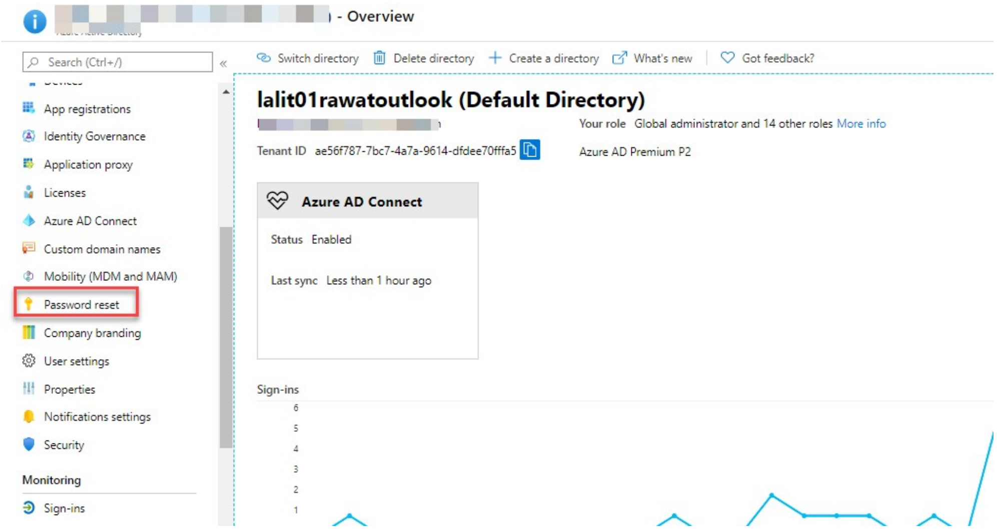
Perform the following steps:

1. For password writeback, we need the Azure AD P1 or P2 license.

2. Go to the portal.

3. Go to Azure AD.

Under the **Manage** tab, select **Password reset** as shown in the following screenshot:



[redacted] - Overview

lalit01rawatoutlook (Default Directory)

[redacted]

Your role Global administrator and 14 other roles More info

Tenant ID ae56f787-7bc7-4a7a-9614-dfdee70fffa5

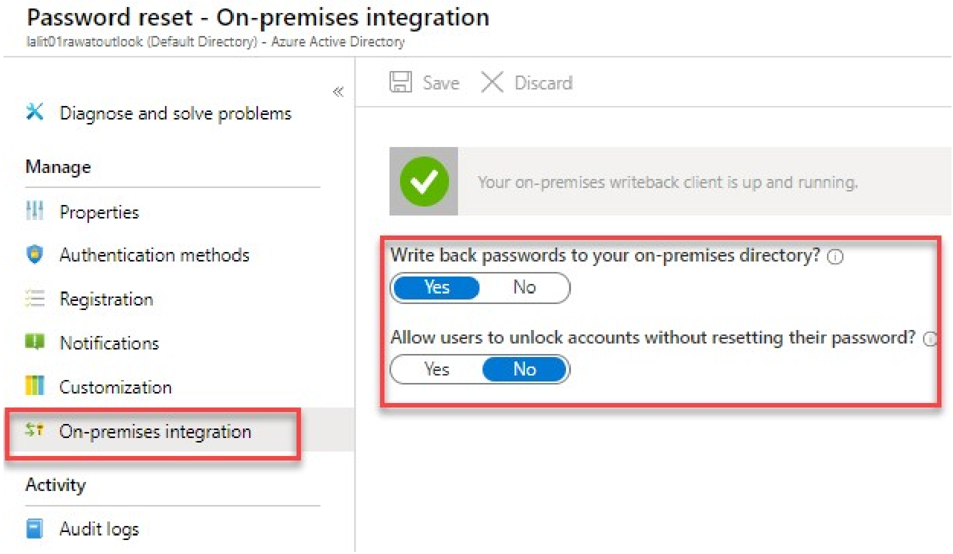
Azure AD Premium P2

Azure AD Connect

Status Enabled

Last sync Less than 1 hour ago

4. In the password reset, under the **Manage** tab, please select the on-premises integration and enable the writeback password to your on-premises directory. Please take a look at the following screenshot:



Password reset - On-premises integration

lalit01rawatoutlook (Default Directory) - Azure Active Directory

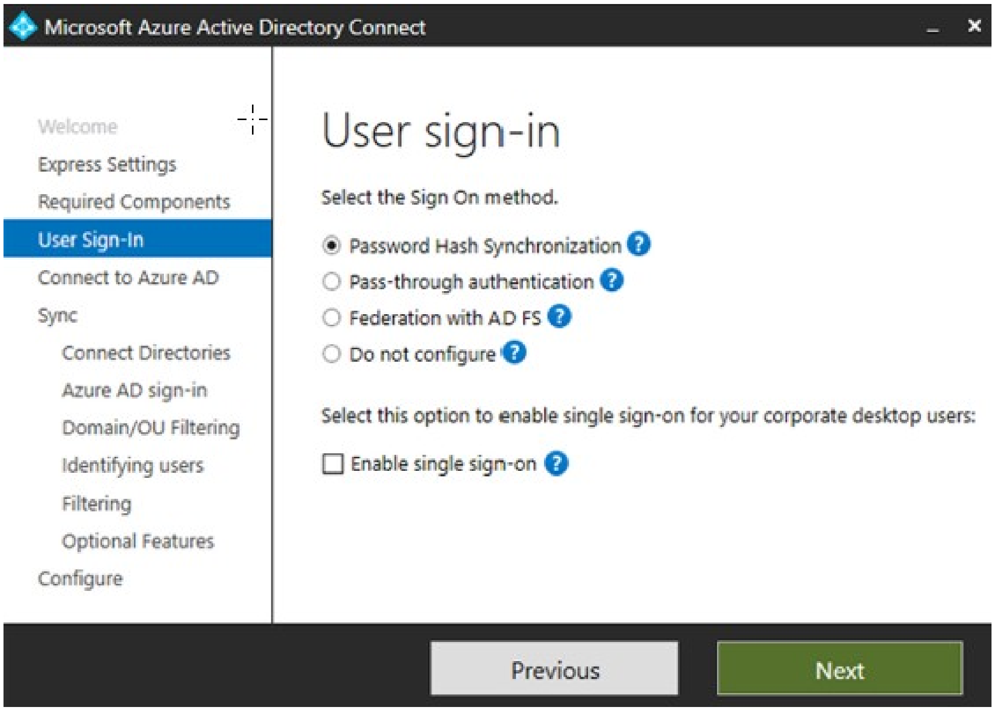
Your on-premises writeback client is up and running.

Write back passwords to your on-premises directory? [✓ Yes] No

Allow users to unlock accounts without resetting their password? Yes [✓ No]

4- Password sync

Password sync will be enabled automatically if we select the Azure AD Connect express setting installation. If you choose the custom setting, you can select the password hash sync on the user sign-in page. You can enable it.



User sign-in

Select the Sign On method.

● Password Hash Synchronization

○ Pass-through authentication

○ Federation with AD FS

○ Do not configure

Select this option to enable single sign-on for your corporate desktop users:

□ Enable single sign-on