The following Windows Server releases support Azure AD Connect v2:

* Windows Server 2016
* Windows Server 2019
* Windows Server 2022

Note: Azure AD Connect v2 requires Windows Server 2016 or higher. You must migrate Azure AD Connect to a new server if running an older Windows Server version.

Do you already have Azure AD Connect v1 installed on Windows Server 2016 or higher and want to upgrade? Or do you already have Azure AD Connect v2 running and want to upgrade to the latest version for new features and bug fixes? If so, this is a different process.

Azure AD Connect v2.0 major changes

These are the new significant changes in Azure AD Connect v2:

* SQL Server 2019 LocalDB
* MSAL authentication library
* Visual C++ Redist 14
* TLS 1.2
* All binaries signed with SHA2
* Windows Server 2012 and Windows Server 2012 R2 are no longer supported
* PowerShell 5.0

**Steps**

1. Check source server’s Azure AD Connect version
   1. Start Azure Active Directory Synchronization Service from the program’s menu. Click in the menu bar on **Help > About**. Azure AD Connect version 1.6.16.0 (aka a release of v1) shows up.
2. Export source server’s Azure AD Connect configuration

Before you migrate, Azure AD Connect to another server, you must create an Azure AD Connect export configuration.

* 1. Start Microsoft Azure Active Directory Connect from the program’s menu. Click on **Configure**.
  2. Click **View or export current configuration**. Click **Next**.
  3. Click **Export Settings**.
  4. Save the .json file on the new Windows Server that you will install Azure AD Connect on.

1. Check Azure AD Connect user sign-in settings
   1. Go back to the Additional tasks. Click on **Change user sign-in**. Click **Next**.
   2. Write down or take a screenshot of the User sign-in settings. You will need to provide these settings in the Azure AD Connect setup wizard on the new Windows Server.

**Ex.** [**user@domain.local**](mailto:user@domain.local) **admin.jason@co-alliance.com**

* 1. The Azure AD export configuration will not export the User sign-in settings. Write the settings down.

**Ex. Password Hash Synch only, pw write-back-groupwrite back**

* 1. If Device Writeback is enabled, will have to document settings.
  2. Run the following from Admin – Powershell and save info to text file:

**(Get-ADSyncGlobalSettings).Parameters | select Name,Value**

**Get-ADSyncScheduler**

1. On the new target server, confirm or enable TLS 1.2 on Azure AD Connect server
   1. Run PowerShell ISE as administrator on the new server. Copy the below PowerShell script and run.

New-Item 'HKLM:\SOFTWARE\WOW6432Node\Microsoft\.NETFramework\v4.0.30319' -Force | Out-Null

New-ItemProperty -path 'HKLM:\SOFTWARE\WOW6432Node\Microsoft\.NETFramework\v4.0.30319' -name 'SystemDefaultTlsVersions' -value '1' -PropertyType 'DWord' -Force | Out-Null

New-ItemProperty -path 'HKLM:\SOFTWARE\WOW6432Node\Microsoft\.NETFramework\v4.0.30319' -name 'SchUseStrongCrypto' -value '1' -PropertyType 'DWord' -Force | Out-Null

New-Item 'HKLM:\SOFTWARE\Microsoft\.NETFramework\v4.0.30319' -Force | Out-Null

New-ItemProperty -path 'HKLM:\SOFTWARE\Microsoft\.NETFramework\v4.0.30319' -name 'SystemDefaultTlsVersions' -value '1' -PropertyType 'DWord' -Force | Out-Null

New-ItemProperty -path 'HKLM:\SOFTWARE\Microsoft\.NETFramework\v4.0.30319' -name 'SchUseStrongCrypto' -value '1' -PropertyType 'DWord' -Force | Out-Null

New-Item 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server' -Force | Out-Null

New-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server' -name 'Enabled' -value '1' -PropertyType 'DWord' -Force | Out-Null

New-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server' -name 'DisabledByDefault' -value 0 -PropertyType 'DWord' -Force | Out-Null

New-Item 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client' -Force | Out-Null

New-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client' -name 'Enabled' -value '1' -PropertyType 'DWord' -Force | Out-Null

New-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client' -name 'DisabledByDefault' -value 0 -PropertyType 'DWord' -Force | Out-Null

Write-Host 'TLS 1.2 has been enabled.'

* 1. After running the script, you must restart the Windows Server for the changes to take effect.

1. Download Azure AD Connect v2
   1. Download the latest Azure AD Connect version by going to the Microsoft Download Center. ***At the moment, the newest version is Azure AD Connect 2.1.20.0.***
2. Install Azure AD Connect v2
   1. Double-click the AzureADConnect.msi file, and let the setup extract the files. Agree to the license terms and click **Continue**.
   2. Click on **Customize** for a custom install.
   3. Check the checkbox **Import synchronization settings**. Browse to the exported Azure AD Connect .json file. Click **Install.**
   4. Select the same **User sign-in settings** configured on the old Azure AD Connect server. In a previous step, you should of made note these settings. Click **Next**.
   5. With Azure AD Connect v1, we enter our Azure AD global administrator account. In Azure AD Connect v2, we can use a user account with the Hybrid Identity Administrator user role. We no longer need the Global Administrator role for this.

Note: We recommend using an account with the least privileges. So, we will create a service account for the Hybrid Identity Administrator and use that from now on.

* Sign into the Azure AD portal.
* Create a new user that is cloud only
* Navigate to Azure Active Directory > Roles and administrators. Search for the role Hybrid identity administrator. Assign the service account to the role.

**Ex. svc-adconnect@domain.onmicrosoft.com**

* 1. You can get an error that it can’t connect to Active Directory. Click on **Change Credentials**.

You can select account option:

* **Create new AD account:** Azure AD Connect will create an AD DS Connector account (MSOL\_xxxxxxxxxx) in AD with all the necessary permissions.
* **Use existing AD account:** Provide an existing account with the required permissions. Read more on [how to create an AD DS Connector account](https://www.alitajran.com/create-ad-ds-connector-account/).

NOTE: The best option is to select **Create new AD account**. If a new AD account is created, once removing staging mode, AD Connect synchronization breaking after implementing Azure AD MFA is to exclude the Azure AD Connect Sync Account from Azure AD MFA.

Service accounts, such as the Azure AD Connect Sync Account, are non-interactive accounts that are not tied to any particular user. They are usually used by back-end services allowing programmatic access to applications, but are also used to sign in to systems for administrative purposes. Service accounts like these should be excluded since MFA can’t be completed programmatically.

* 1. Fill in the credentials. Click on **OK**.
  2. Ensure that both checkboxes (Start sync & Enable staging mode) are checked and click **Install**.
  3. Wait for the Azure AD Connect upgrade to finish.
  4. Configuration complete. Azure AD Connect configuration succeeded, and the synchronization process has been initiated. Click **Exit**.
  5. Verify that Azure AD Connect V2 is successfully installed.
  6. Start **Azure Active Directory Synchronization Service** from the program’s menu. Click in the menu bar on **Help > About**. In our example, Azure AD Connect version **2.1.x.x** shows up.
  7. Compare Exported and Applied JSON files via Notepad to confirm they are the same.
  8. Verify that the synchronization status shows the status **success**. **It should not show any errors or permissions issues**.

1. Enable staging mode on old server
2. On the old server, start **Microsoft Azure Active Directory Connect**. Click on **Configure** and select **Configure staging mode**. Click **Next**.
3. Fill in the Azure AD global administrator or hybrid identity administrator credentials. Click **Next**.
4. Make sure the checkbox **Start the synchronization process when configuration completes is checked**. Click **configure**.
5. Staging mode is successfully enabled on the old Azure AD Connect server. Click **Exit**.
6. Disable staging mode on new server
7. On the new server, start Microsoft Azure Active Directory Connect. Click on **Configure** and select **Configure staging mode**. Click **Next**.
8. Fill in the Azure AD global administrator or hybrid identity administrator credentials. Click **Next**.
9. Uncheck the checkbox **Enable staging mode**. Click **Next**.
10. Make sure the checkbox **Start the synchronization process when configuration completes is checked.** Click **configure**.
11. Staging mode is successfully disabled on the new Azure AD Connect server. Click **Exit**.
12. Check Azure AD Connect synchronization
    1. Start **Azure Active Directory Synchronization Service**. Verify that the synchronization status shows as **success**.

NOTE: There may be permission issues on specific users (e.g., all Domain Admin members, and others). You will need to enable inheritance on each user using ADUC (in advanced mode) under Security tab of each user with issue.

* 1. Sign in to the [Microsoft 365 admin center](https://admin.microsoft.com/). Click on the **sync status** in the **Azure AD Connect tile**.

Note: The **directory sync status** shows the Directory sync client version and Directory sync service account. If you don’t have the **Azure AD Connect tile**, you can navigate to **Health > Directory sync status**.

1. Uninstall Azure AD Connect.
   1. The last steps that you want to take care of on the old Azure AD Connect server are:

Shutdown the old Azure AD Connect server for a couple of days just in case or disable the Azure AD Connect services. Then, after everything works as you expect continue with remaining items below:

* Uninstall Azure AD Connect (this will also uninstall some other AD Connect components)
* Remove old on premise AD DS Connector account
* Remove old Azure AD Connector account

1. Confirm new AAD Connect server registered and remove old one from the Azure AD Connect Health portal.

NOTE: This is only required if Azure P1 or better licensed, otherwise, Azure AD Connect Health under Heath and Analytics, is not available and there will be a error when steps a or b is done.

1. Go to Azure portal at <https://portal.azure.com/> and to Azure AD Connect. In right windowpane, click on Azure AD Connect Health under Heath and Analytics.
2. Click on **Sync services** and in right windows pane, click on the service name.
3. Confirm new AAD Connect server listed and shows healthy (If not listed, stop and follow note below. If it is listed, then continue with step d. below).

Note: If the new AAD Connect server is not listed, go to the new server running AAD Connect and go to the Control Panel | Programs and Features. Select the Microsoft Azure AD Connect Health agent for sync and click **Change**.

It will open an administrative Windows PowerShell window and will ask for global admin credentials. Once that is provided, it will run through a series of steps and should provide a “Agent registration completed successfully” message. You can then go back to the Azure portal and refresh browser and should see that AAD Connect server listed and as healthy.

1. Click on the old AAD Connect server and click Delete. Enter server name and click Remove.