# Connecting Office 365 to Active Directory with Single Sign On

## Custom Install of Azure AD Connect

* To install Azure AD connect, navigate to <https://www.microsoft.com/en-ca/download/details.aspx?id=47594> to **download the installer**.
* The first menu will be the **Express Settings** menu. Click **Customize** to start a customized install.
* On the **Install required components** page, leave all the options **unchecked**.
* On the **User sign-in** page, select **Password Hash Sync or Pass-through Authentication** to connect to local AD.
* On the **Connect to Azure AD** page, do **NOT** use a global admin account from the local AD, use one with the default onmicrosoft.com domain that comes with the Azure AD tenant. It will not be used after the wizard is complete.
* Under **Connect your directories**, leave the directory type as **Active Directory**, and add the forest(s).
* An **AD forest account** window will come up. It states an AD account with sufficient permissions is required for periodic synchronization. You can either **let Azure AD create one for you** **or use an existing account.**
* On the **Azure AD sign-in configuration** page, verify your domain is **verified**. If it is not, it will be given the chance later on in the wizard to be verified.
* Under **Domain and OU filtering**, you can unselect domains and OUs you do not want synchronized to Azure AD
* Under **Uniquely identifying your users**, there are multiple options in the event of one user having many accounts and other outlying factors. Azure may state at the bottom how it is done on your on-premises directory.
* Leave the **Filter users and devices** page as is
* On the **Optional features** page, select **Password writeba**ck so that if a password is changed using Office 365 that it syncs with the local AD.
* On the **Enable single sign-on** page, log in with a **Domain Admin** account to enable single sign-on. These credentials are only used to create the account and are not stored.
* Next, you should be able to start the synchronization process and **install**. Once that is done, it will allow you to **verify** one more time.
* After the install has completed, **sign out and sign in** again to Windows.

## Configuring the Intranet Zone for client machines

* Open **Group Policy Management**
* **Right click to Edit** the desired group policy
* Navigate to **User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page** and select **Site to Zone** assignment list.
* **Enable** the **Site to Zone Assignment List policy** and put the following in the dialog box:

**Value: `https://autologon.microsoftazuread-sso.com`**

**Data: 1**

## Note

* The difference between Password Hash Synch and Pass-Through Authentication is that with Password Hash Synch Azure AD performs the login authentication itself, and with Pass-Through authentication Azure AD has your local AD do the login authentication.