Limiting Your Organization's Exposure to Azure AD Using Domain, OU, App, and Attribute Filtering

WHITE PAPER

SEMPERIS

Synchronizing objects and their attributes from an on-premises Active Directory environment to Azure AD is a common process in many organizations. Azure AD domain, OU, app, and attribute filtering allow organizations to synchronize only a handful of attributes to minimize the exposure of personally identifiable information in this setup. So, why do so few organizations use it?

In Europe, the dust is settling around the General Data Protection Regulation (GDPR). As an industry, we've made some great improvements into protecting the privacy of people using technology. Microsoft also made big strides and adjustments to their products, including the tool almost every organization uses to synchronize objects from on-premises directories to Azure Active Directory: Azure AD Connect.

Besides the **Privacy** page in Azure AD Connect since version 1.1.749.0 and a page where organizations can find out which attributes for their Azure AD objects leave Europe, Microsoft offers another feature, which I don't see a lot of organizations implement: **Azure AD app and attribute filtering**.

GDPR and the privacy of your colleagues

Whatever warm and fuzzy feeling Azure AD might give you, with GDPR goggles on, it should be seen as another identity store. Just like Active Directory Domain Services on-premises, it holds personally identifiable information (PII) on the people inside your organization (and in some scenarios also on people outside your organization), labeled in GDPR terms as data subjects.

I find it surprising that so few organizations use this feature because in this day and age of GDPR, organizations need to think hard about the data for their people and customers, where this information is stored, and how the data is protected in terms of confidentiality, integrity, and availability.

A privacy impact analysis (PIA) should be a part of each implementation containing personally identifiable information (PII). So, when introducing Azure AD, but also when extending the on-premises Active Directory to Azure AD in a Hybrid Identity setup, a PIA should be created.

The PIA for Hybrid Identity implementations should include the work relationship between the data subjects and the organization and automatic deletions in Azure AD when a user object is disabled and/or deleted in Active Directory, after spending some time in the Azure AD Recycle Bin and purge space.

There are many additional measures organizations can take, depending on the risks in their Hybrid Identity environment, consisting of Active Directory on-premises and Azure AD. Measures like using ExpressRoute to exchange data, regular penetration tests and evaluations, disaster recovery preparation, encryption using arguably safe encryption methods (TLS 1.2), and disabling any writeback functionality are commonplace in the environments I encounter.

However, limiting the exposure of the organization by limiting the attributes and objects synchronized to Azure AD is not always part of these countermeasures.

Get it right, the first time

The first thing to notice is that the **Azure AD app and attribute filtering** page in the Azure AD Connect Configuration wizard is only visible when an admin chooses to **Customize** the Azure AD Connect implementation, instead of using the "4-click" **Express Settings** flow.

Microsoft's easy approach might backfire here, especially since synchronized attributes don't magically disappear from Azure AD, even after you go back into the Azure AD Connect wizard to **Change synchronization settings** or adjust the built-in synchronization rules to no longer synchronize privacy-sensitive attributes…

It's best to get this right, the first time.

Admins can worry less about the objects, though. **Domain/OU filtering** can be configured as part of **Change synchronization settings** and together with the Azure AD Recycle Bin, this makes for a straightforward way to clean Azure AD from any objects your organization doesn't want to live there. The only thing to keep in mind is Azure AD Connect's default export deletion threshold of 500 objects.

151 attributes, by default

When an admin performs Microsoft's "4-click" **Express Settings** installation of Azure AD Connect, up to 151 attributes are synchronized from an on-premises Active Directory Domain Services environment to Azure AD. These attributes provide the foundation for the whole range of scenarios including implementing an Exchange Hybrid environment and working in third-party cloud applications through Azure AD Single Sign-on.

> **Note:** Of course, if a certain attribute has no value (null) for an object in Active Directory, then that attribute is not synchronized for that object. If an object doesn't have an attribute (e.g., user objects don't have members, where groups typically do), then that attribute is also not synchronized.

There is a list of attributes available online, but you can also export files from Azure AD Connect that specify the attributes per Azure AD app. Using this method, Azure AD Connect will disclose which attributes are truly necessary and not just (for Microsoft) nice to have.

> **Note:** In past versions of Azure AD Connect, when you used **Customize**, the Azure AD Connect installation would not automatically upgrade. In recent versions, the Automatic Upgrades feature has been improved to include almost all configuration scenarios. Admins don't need to worry about losing automatic upgrades to Azure AD Connect when they use either **Domain/OU filtering** or **Azure AD app and attribute filtering**.

While tempting, we won't touch the built-in synchronization rules to minimize the synchronization of objects and attributes, in this paper.

Get it right, the first time

Customize settings in Azure AD Connect

The best way to get it right the first time is by clicking **Customize** in the **Express Settings** screen when an admin sets up the (first) Azure AD Connect installation for a (new) Azure AD tenant. The customized flow presents additional pages when compared to the Express Settings flow and requires more thought. The number of pages depends on the choices you make during the flow. For instance, when you specify federation with AD FS as the sign-in method, several AD FS-related pages are added to the flow.

In the **Customized** flow, both **Domain/OU filtering** and **Azure AD app and attribute filtering** (as part of the **Optional features**) can be configured. The **Optional features** page is shown in figure 1.

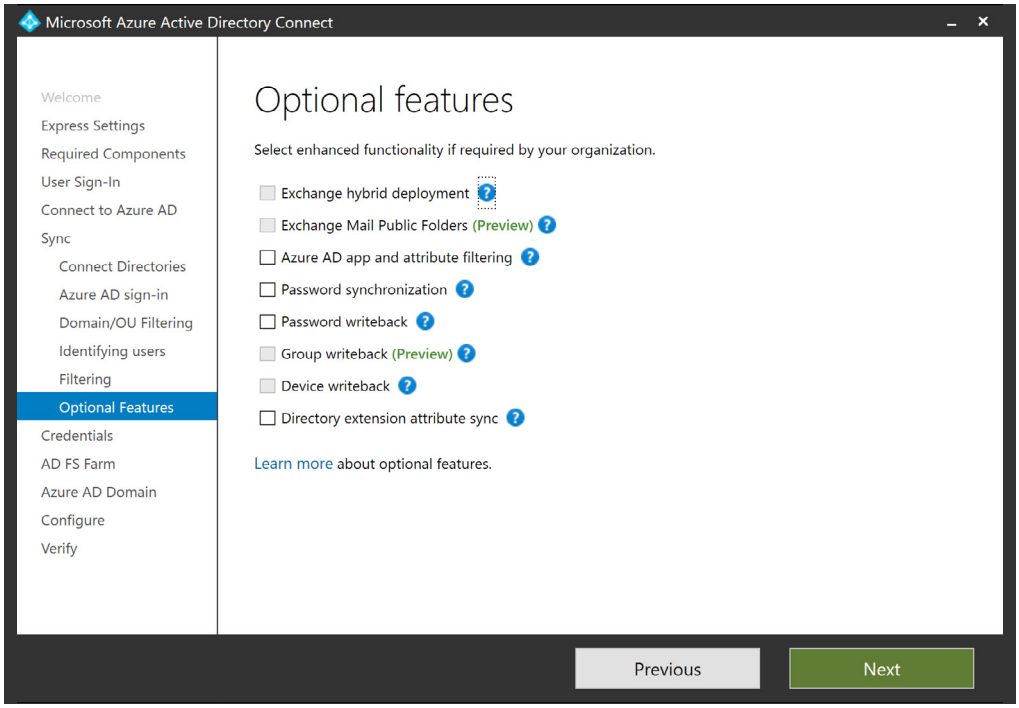

Figure 1. The Optional features page as part of the customized Azure AD Connect configuration wizard

> **Tip!**
> When the option **Start the synchronization process when configuration completes** is disabled on the **Ready to configure** screen at the last step of the initial Azure AD Connect configuration workflow, by default, Azure AD Connect will not start synchronizing until the process is started at a later point in time. This allows for a review of the configuration before any harm is done.

Customize synchronization options

In many situations, **Domain/OU filtering** and **Azure AD app and attribute filtering** will be configured after the initial Azure AD Connect configuration workflow.

> **Warning!**
> While this will remove out-of-scope objects from Azure AD after 30 days, attributes for previously synchronized objects will remain in Azure AD and will no longer be kept up to date. As out-of-date, incorrect, and missing attributes are the three possible outcomes of the steps below, assess the impact these scenarios might have per synchronized object type (user, group, contact, inetorgperson) on your organization's processes like reporting, before proceeding.

Below are the steps to limit your organization's exposure to Azure AD:

1. First, log on to the Windows Server installation that hosts your Azure AD Connect installation.
2. Click on the **Azure AD Connect** shortcut on the **Desktop** or the **Start Menu**, or launch C:\Program Files\Microsoft Azure Active Directory Connect\AzureADConnect.exe.
3. On the **Welcome to Azure AD Connect** page, click **Continue**.
   The remark about the synchronization service scheduler being suspended while the configuration wizard is open can be safely ignored, as long as we don't keep the wizard open for too long.

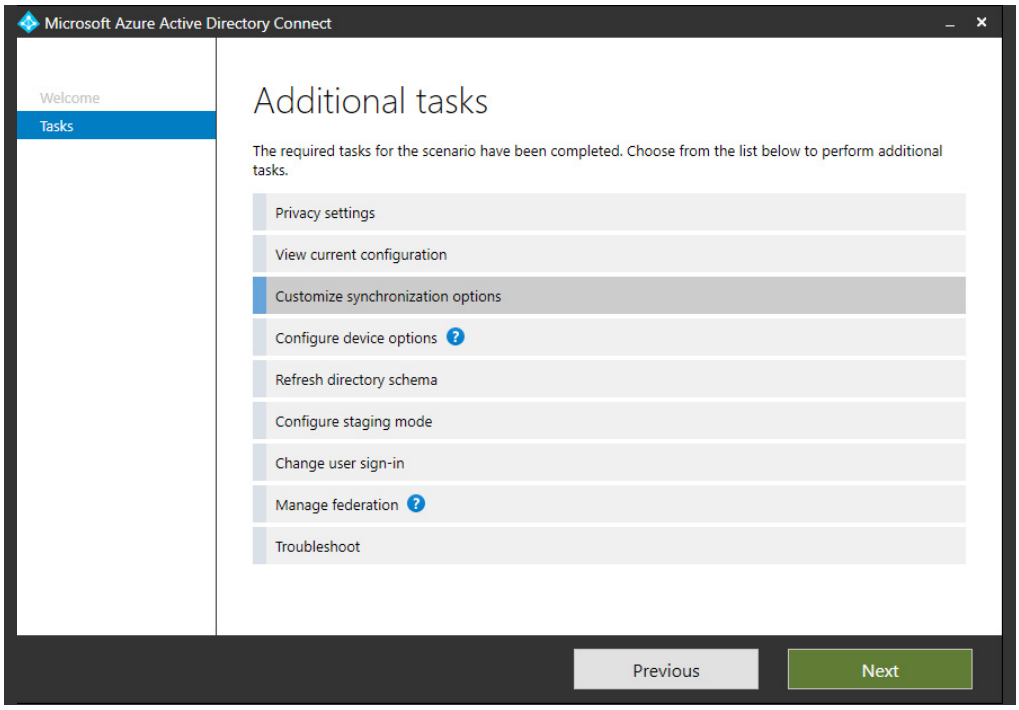

Figure 2. Additional tasks for Azure AD Connect

4. On the **Additional tasks** page, click on **Customize synchronization options**.
   Your tasks might include less tasks than shown in figure 2 or other tasks, depending on the configuration and version of Azure AD Connect. Click **Next**.

5. On the **Connect to Azure AD** page, sign in with an Azure AD-based account with **Global Administrator** or **Company Administrator** privileges. Perform multi-factor authentication and/or privileged identity management to connect.

6. When you want to remove entire Active Directory forests from the scope of Azure AD Connect, remove them on the **Connect your directories** page. Make sure to also remove or reconfigure any service account used by Azure AD Connect in that forest. Click **Next** when done.

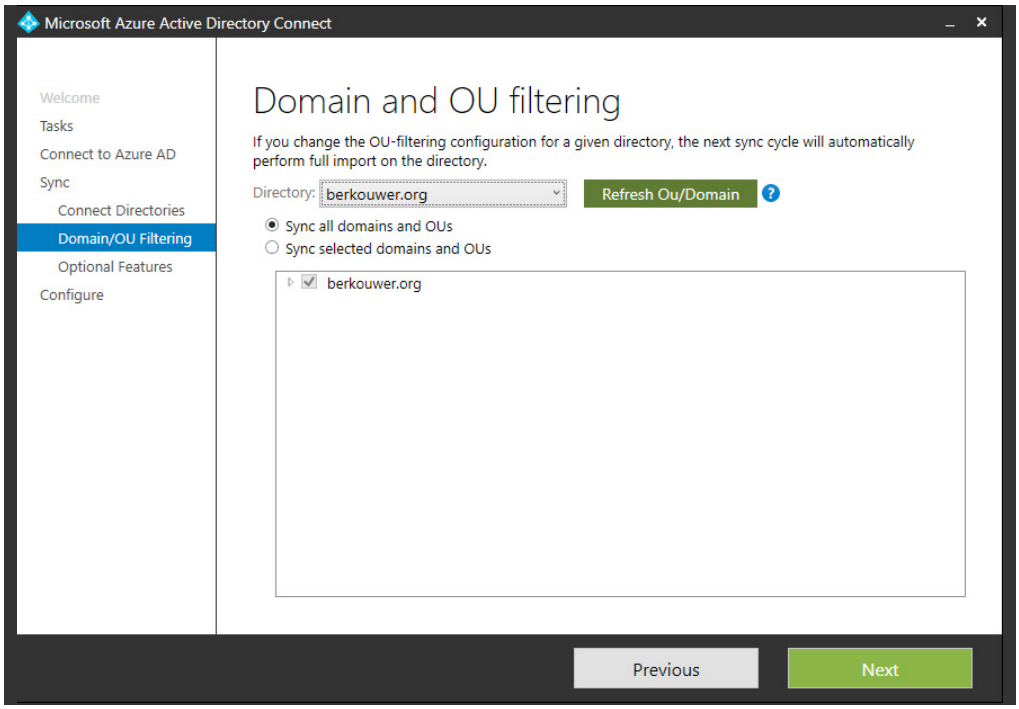

Figure 3. Domain and OU filtering in the Azure AD Connect configuration wizard

7. On the **Domain and OU filtering** page, shown in figure 3, select the directory you want to configure filtering for, and select **Sync selected domains and OUs**. Then, in the field below, tick any domain and/or Organizational Unit (OU) you want to include in the scope of Azure AD Connect.

> **Tip!**
> When your organization utilizes an Active Directory domain or OU structure where computer objects are stored separately, you can choose to exclude these domains and/or OUs to prevent the Hybrid AD Join process from synchronizing information on all Windows 10-based domain-joined devices to Azure AD for Single Sign-on purposes, like the Operating System version, its SID, information on the registered owner, and its issued public key certificate.

8. On the **Optional features** page, select the **Azure AD app and attribute filtering** option. By enabling Azure AD app and attribute filtering, the set of synchronized attributes can be tailored to a specific set. Click **Next**.

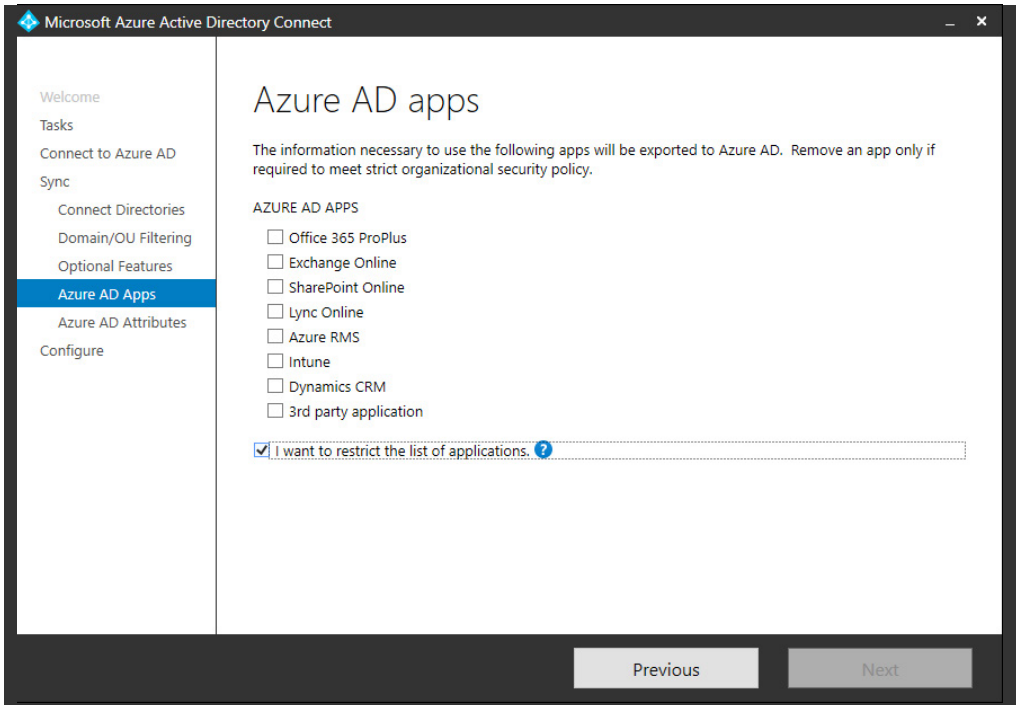

Figure 4. Azure AD apps in the Azure AD Connect configuration wizard

9. On the subsequent **Azure AD apps** page, as shown in figure 4, select the option **I want to restrict the list of applications**. This will remove the greyed-out selections for **Office 365 ProPlus, Exchange Online, SharePoint Online, Lync Online, Azure RMS, Intune, Dynamics CRM,** and **3rd party application**. Alas, the **Next** button is greyed out with no app selected, so we need to select at least one app. Select the scenario(s) that best align with your organization's use of Microsoft cloud functionality, or select Office 365 ProPlus, when you want to truly minimize the number of attributes synchronized; from an admin administrative effort point of view, this would only require you to unselect 15 attributes on the next screen. Click **Next**.

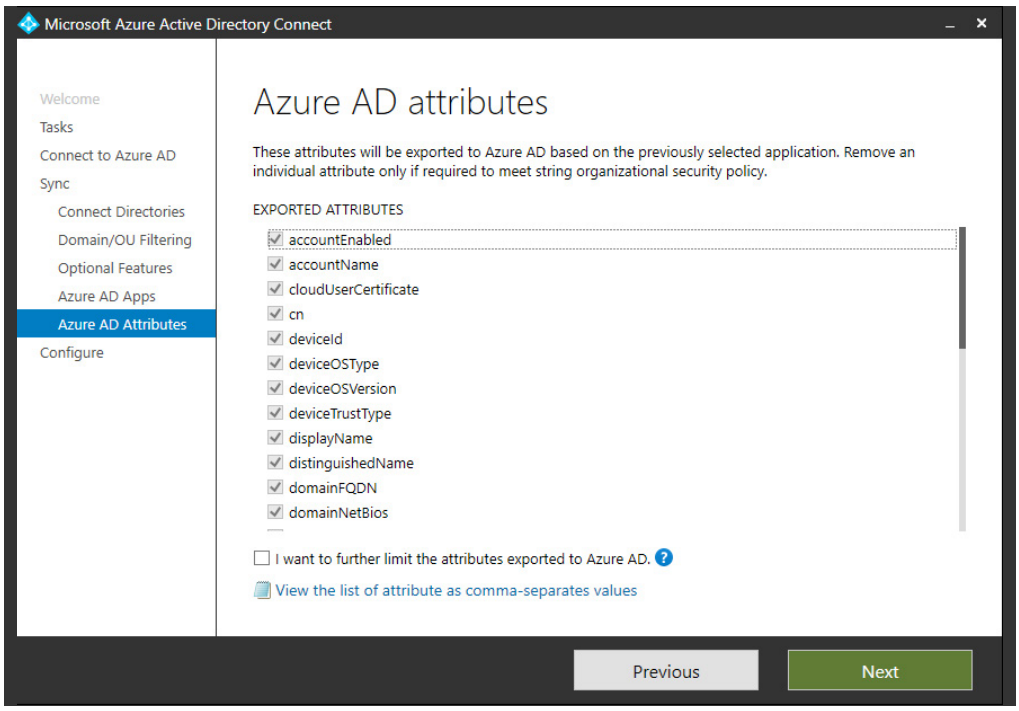

Figure 5. Azure AD attributes in the Azure AD Connect configuration wizard

10. On the **Azure AD attributes** page, click **Next** or continue on the journey to Minimal Sync (MinSync), by selecting **I want to further limit the attributes exported to Azure AD**. The **View the list of attribute as comma-separates values** link can be used to gain a list of attributes, which ones are exported, and which ones are mandatory. The **IsMandatory** flag is enforced on the **Azure AD attributes** page in the **Azure AD Connect** configuration wizard because even when you further limit the attributes, some attributes are still greyed out and will need to be synchronized no matter what. Unselecting every other attribute, except for these attributes (**accountEnabled, sourceAnchor,** and **userPrincipalName**) constitutes MinSync. However, when you also have groups in scope for Azure AD Connect, the **cn, securityEnabled,** and **member** attributes also become essential and should be selected. The Azure AD Connect configuration wizard does not distinguish attributes per object type.

    Click **Next** when done.

11. On the **Ready to configure** page, click **Configure**.

12. On the **Configuration complete** page, click **Exit** to exit the Azure AD Connect configuration wizard and have the synchronization schedule resume.

Perform the same steps on any Staging Mode Azure AD Connect installation your organization might have deployed.

Concluding

Only a limited set of attributes is mandatory for synchronization between Active Directory on-premises and Azure AD. As an admin, make sure you know what attributes are synchronized by default and how to limit the attributes that are actually synchronized in terms of GDPR. Preferably, get this right the first time.

About Semperis

Semperis is an enterprise identity protection company that helps organizations recover from cyber breaches and identity system failures, on-premises and in the cloud. The company's patented technology for Active Directory is used by customers in the Fortune 500, government, financial, healthcare, and other industries worldwide. Semperis solutions are accredited by Microsoft and recognized by Gartner.
For more information, please visit www.semperis.com.