

# Azure Cloud Sync

Originally AD Connect was the way that we synced Active Directory (AD) to Azure/365 (AAD). That had an agent on-premise that synced with Azure. The configuration of the agent was on-premise. Eventually Microsoft has reviewed this and is in process of replacing AD Connect with Azure Cloud Sync. There is still the need for an agent on-premise, but the configuration is handled in Azure. This allows more on-premise flexibility and you can add multiple agents for resiliency.

Download the agent:

[https://portal.azure.com/#view/Microsoft\\_AAD\\_Connect\\_Provisioning/CloudSyncMenuBlade/~/\\_Agents](https://portal.azure.com/#view/Microsoft_AAD_Connect_Provisioning/CloudSyncMenuBlade/~/_Agents)

Check to see if GPO has any "LOG ON AS A SERVICE" GPO that will prohibit the installation. The installation creates a new domain user service account. If there are restrictions to the service account the installation will fail. Short period of time add the "EVERYONE" group to the policy and then install. Once installed add the newly created domain user account into the policy and remove "EVERYONE".

Server must be running at least .NET 4.7.1

<https://dotnet.microsoft.com/en-us/download/dotnet-framework/net471>

Installation will require a restart to apply.

Install the agent. This does not configure or apply any changes. The agent must be in place before you can create the configurations in Azure. It is recommended to install 2 agents for resiliency. They MUST have direct access to the domain controllers and open ports to communicate with Azure. Preference would be to have it installed on DC when available.

Machine generated alternative text: Microsoft Azure Active Directory Connect Provisioning Agent Cor

Launch AD Connect. Export the configuration for review. You will want to duplicate the configuration between AD Connect and Azure Cloud Sync. Therefore you need to know from the source, what is the current configuration. Personally, I like to print it out and use a highlighter to identify the key settings.

Once the agent is installed you will see it on the agents page. You then will have the option to create the configuration.

[https://portal.azure.com/#view/Microsoft\\_AAD\\_Connect\\_Provisioning/CloudSyncMenuBlade/~/\\_/CloudSyncConfigurations](https://portal.azure.com/#view/Microsoft_AAD_Connect_Provisioning/CloudSyncMenuBlade/~/_/CloudSyncConfigurations)

If the "New Configuration" option is not available, something is wrong with the agents. To date, known problems. Agent installation used wrong settings, ports were not open to Azure, agent was not installed.

Create NEW Cloud Sync Configuration:

Click the "New Configuration" and create. At this point it is not active and not configured.

You will be placed into configuring the new sync configuration.

1. Add scoping filters (optional)
  1. Historically this is the most used. Depending on setup this varies a lot and this needs special note. The configuration from AD Connect really comes into play on this. Some configuration simply synced all user accounts. Others configurations limited by either a security group (my preference when I setup), or by one or multiple OU. This is the spot where you have to duplicate those setting properly.
  2. Easiest method of adding scopes will be to copy/paste the Distinguished Name from AD.
2. Attribute mapping
  1. To date, I have not had to make any changes here. Again, refer to the original configuration from AD Connect.
3. Test (recommended)
  1. This is important!!! ALWAYS test. Test users that are and are not supposed to be synced (if any). This is the way to verify that the settings you put into place are working or not.
  2. Add the DN for the user account and then click PROVISION. This does not change anything, simply test if it will sync.
4. View default properties (optional)
  1. There are some options here, I normally keep them default.
5. Enable your configuration (required)
  1. NOPE, not yet.

Swap Sync Management:

AD Connect and Azure Cloud Sync CANNOT be running at the same time. That is why we did not enable the Azure Cloud Sync yet. At this point either method is setup and can do the sync, but you cannot have both. Make sure you have made the required adjustments beforehand. My biggest

fear is that

---

Revision #1

Created 23 December 2023 04:49:18 by ColtM

Updated 13 June 2024 01:28:01 by ColtM