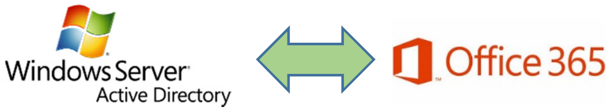
infostream, inc.

Installing Azure Active Directory Sync (AADSync, informally known as DirSync)

What you need to know about DirSync - our experiences with DirSync and Office 365, by David Parizek and Henry Verlander.



DirSync can help simplify Active Directory users' experiences with Office 365, and eliminate the need for multiple passwords without adding major infrastructure. However, we found that the setup process was somewhat difficult to navigate that there was much more to the program than first met the eye. In this article, we are attempting to provide a brief and concise step-by-step guide for using AADSync with Office 365 for email purposes.

Introduction

InfoStream does a lot of Office 365 email migrations, so when we heard about Microsoft's Azure Active Directory Connection tool previously known as DirSync, it definitely sounded like something we'd want to use. After migrating a client to Office 365, end users would often have problems with usernames and passwords in the two environments. It was relatively easy for users to get confused. The number one feature that drew Infostream to DirSync is "Password Synchronization". That feature can definitely simplify the experience for end users. We dove into the deep end of the pool and are now using DirSync and AADSync at a number of our clients. Our usage of DirSync has been confined exclusively to syncing between local Active Directory environments and Office 365.

As with all Microsoft products there is more than one version. It gets confusing with this product, because Microsoft changed names the second time around. Directory Sync (DirSync) was released and tied to Office 365, becoming the default name everybody uses. Azure Active Directory Sync (AADSync) was rolled out with the Azure Cloud platform, and has several additional capabilities as well as the password sync. As a newer version that still does what we want, AADSync is the version this paper will focus on. If you are working with DirSync, the theory and the steps will be similar, but some of the command line syntax may change.

Locations of critical files

Microsoft Azure Active Directory Sync Services can be downloaded from the following location:
https://www.microsoft.com/en-us/download/details.aspx?id=44225
MIIS Client for Azure Active Directory (for configuration) is at
"C:\Program Files\Microsoft Azure AD Sync\UIShell\miisclient.exe"
Microsoft Azure Directory Sync Client Command
"C:\Program Files\Microsoft Azure AD Sync\Bin\DirectorySyncClientCmd.exe"

Scenarios

When your organization decides to implement DirSync, it is critical to know where you are in the following scenarios. We have grouped our own experiences into three distinct scenarios. Each scenario is designed to be a complete series of steps to implement AADSync. The scenarios vary, depending on the status of in-house Exchange and Office 365 at the time you start implementation. We suggest that you read the headings of each of the following scenarios carefully and decide which one applies to your organization. Then, follow the steps that apply to you in that section.

SCENARIO 1- In-house exchange is active with a planned migration to Office 365 not yet underway

One of the hardest parts of using DirSync is matching of local users to cloud users. In this scenario, it is easy. The Office365 environment is empty, so when DirSync doesn't find a matching user to sync with, it creates a new user and automatically links them together.

The sequence of steps is as follows:

1) In local ADUC, move all local users, groups and contacts to a new OU named Office365.
    a. You can have sub-OU's, but there should be a parent OU which defines the objects which will be syncing to Office 365.
2) Change all users' UPN to match their email address.
    a. Example: contoso.com, NOT contoso.local in ADUC properties.
    b. Here's how to do that https://technet.microsoft.com/en-us/library/cc772007.aspx
    c. After creating the new Suffix, you must apply it to all users in ADUC.
3) Make sure that each user has their default email address filled in under the GENERAL PROPERTIES tab in ADUC.
4) Install DirSync, but do not SYNC. Configure OU FILTERING and MAILBOX GUID exclusion first.
    a. OU filtering
        i. http://msexchangeguru.com/2012/08/10/office-365-2/
    b. Excluding mailbox GUID.
        i. http://www.cheddon.co.uk/msexchmailboxguid-office-365/
        ii. If you don't exclude the mailbox GUID, Office 365 will not allow you to assign licenses to the cloud mailboxes.
5) Perform Sync. Upon initial Sync, if Office 365 is empty, DirSync will create all the new users and link them to their counterpart in local Active Directory.
    a. There are several syncs that are required to update both Office 365 and Active Directory. Microsoft Recommends that for future manual DirSync's, you use the Directory Sync Client Command. This performs all of the Full and Delta sync's for both connectors that would occur during a scheduled, automated sync.
    b. The Recommended Sync tool is NOT listed in the Start menu. It's located at:
        i. "C:\Program Files\Microsoft Azure AD Sync\Bin\DirectorySyncClientCmd.exe"
    c. Adding a shortcut to the desktop for this command is also recommended. If you do, fill in the "Start In" field with:

        i. "C:\Program Files\Microsoft Azure AD Sync\Bin"

6) Optional: Uninstall Exchange (See Wrap up)
    a. Uninstalling Exchange will remove all users' email addresses from Active Directory and you must be prepared for that before allowing synchronization to occur.

After the migration is completed, and Exchange is disabled, most of the management of users and groups is done locally. For example, Distribution Group memberships are managed locally, with the changes syncing to Office365.

SCENARIO 2 – The Organization has already migrated to Office 365, and Exchange is still installed

In this scenario, the Office 365 mailboxes were created manually with no SYNC to local Active Directory.   Exchange has been disabled but not uninstalled from Active Directory. All mailbox management is being performed in the Office 365 portal.   Users are forced to manage 2 usernames and 2 passwords.

Here are the steps if you are a scenario 2 organization.

1) Move all local users, groups and contacts to a new ADUC OU structure named Office365.
    a. You can have sub-OU's, but there should be a parent OU which defines the objects which will be syncing to Office 365.
    b. Do not change the users' UPN.   Leave all users with the existing .local suffix.
2) Install DirSync and configure the OU filter before performing a Sync.
    a. If the filter is not set, then DIRSYNC will find all the users in the entire Active Directory and try to sync them. Here is a good step by step for configuring "Organizational Units Based Filtering".
    b. http://msexchangeguru.com/2012/08/10/office-365-2/
3) Configure Mailbox GUID filtering, before performing the first Sync.
    a. http://www.cheddon.co.uk/msexchmailboxguid-office-365/
4) Perform the procedures in "SMTP MATCHING" from the article below
    a. https://support.microsoft.com/en-us/kb/2641663/en-us
5) Perform initial sync.
    a. Run DIRSYNC wizard
    b. There are several syncs that are required to update both Office 365 and Active Directory. Microsoft Recommends that for future manual DirSync's, you use the Directory Sync Client Command. This performs all of the Full and Delta sync's for both connectors that would occur during a scheduled, automated sync.
    c. The Recommended Sync tool is NOT listed in the Start menu. It's located at:
        i. "C:\Program Files\Microsoft Azure AD Sync\Bin\DirectorySyncClientCmd.exe"
    d. Adding a shortcut to the desktop for this command is also recommended. If you do, fill in the "Start In" field with:

        i. "C:\Program Files\Microsoft Azure AD Sync\Bin"

6) Optional: Uninstall Exchange (See Wrap up)
    a. Uninstalling Exchange will remove all users' email addresses from local Active Directory. You must be prepared for that before allowing synchronization to occur.

With a little luck at this step, users will be matched via default SMTP address and then linked with their "immutable ID". If things go wrong, you might see duplicate users appear in Office 365. In that case, use PowerShell to permanently delete the duplicates from Office 365 and try again. From this point forward, you must manage many of the users' Office 365 attributes from local Active Directory.

SCENARIO 3 – The Organization has already migrated to Office 365 and Exchange never was installed locally

When EXCHANGE does not exist in the local Active Directory, the users do not have email addresses included in their ADUC properties. In this scenario, Technicians must use the ADUC Advanced Attribute "PROXY ADDRESSES" field to manage the data that is synced to Office 365. The most critical part of implementing Dirsync in Scenario 3 is to perform the steps in the proper sequence. Here is our advice.

1) Move all local users, groups and contacts to a new OU named Office365.
    a. You can have sub-OU's, but there should be a parent OU which defines the objects which will be syncing to Office 365.
2) Edit Users' Proxy Addresses:
    a. Manually, open each user and group in ADUC Advanced Properties,
    b. go to the Attribute Editor tab,
    c. Scroll down to PROXY ADDRESSES.
    d. Enter all of the email addresses for that user or group.
        i. The default address must be formatted as SMTP:JSmith@contoso.com
        ii. Alternate addresses must be added with the "smtp" in lower case.
        iii. Do the same for users and groups.
        iv. Enter the default email address in the "GENERAL" properties tab for each user or group in ADUC.

If a user is matched and synced to Office 365 when they do not have a local email address, then DirSync will REMOVE ALL EXISTING EMAIL ADDRESSES and replace them with JSmith@contoso.onmicrosoft.com

3) Install DirSync and configure the OU filter before performing a Sync.
    a. If the filter is not set, then DIRSYNC will find all the users in the entire Active Directory and try to sync them.
  b. Article for configuring "Organizational Units Based Filtering".
        i. http://msexchangeguru.com/2012/08/10/office-365-2/

4) Perform the procedures in “SMTP MATCHING” from the article below
    a. https://support.microsoft.com/en-us/kb/2641663/en-us
5) Perform SYNC. Run the AADSYNC wizard.
    a. There are several syncs that are required to update both Office 365 and Active Directory. Microsoft Recommends that for future manual DirSync’s, you use the Directory Sync Client Command. This performs all of the Full and Delta sync’s for both connectors that would occur during a scheduled, automated sync.
    b. The Recommended Sync tool is NOT listed in the Start menu. It’s located at:
        i. “C:\Program Files\Microsoft Azure AD Sync\Bin\DirectorySyncClientCmd.exe"
    c. Adding a shortcut to the desktop for this command is also recommended. If you do, fill in the “Start In” field with:
        i. "C:\Program Files\Microsoft Azure AD Sync\Bin"

With a little luck here, users will be matched via initial SMTP address, then permanently linked with their “immutable ID”, and there will be no duplicates created. From this point forward, you must manage many of the users’ Office 365 attributes from local Active Directory.

Optional Wrap up (Uninstall Exchange)

1. Temporarily stop the Synchronization schedule from running while completing the remaining steps.
        i. To stop DirSync, go to the C:\Program Files\Windows Azure Active Directory Sync folder.
        ii. Open the Microsoft.Online.DirSync.Scheduler.exe.Config file with the Notepad. Edit the “SyncTimeInterval” value to a higher number of hours.
        iii. For AADSync, go to “TASK SCHEDULER” in administrative tools and edit the timing of the task there.
2. Manually add Email addresses to active directory objects (users and groups)
    a. open each user or group in ADUC Advanced Properties View
    b. go to the Attribute Editor tab,
    c. Scroll down to PROXY ADDRESSES.
    d. Enter all of the email addresses for the user.
        i. The default address must be formatted as SMTP:JSmith@contoso.com
        ii. Alternate addresses must be added with the “smtp” in lower case.
        iii. Do the same for users and groups.
        iv. Additionally, enter the default email address under the “GENERAL” properties tab for each user or group in ADUC.
3. Uninstall Exchange
   http://www.infostream.cc/2011/10/04/removing-exchange-2007-from-small-business-server-2008

4. Reinitiate normal Dirsync synchronization interval by reversing step 1

GENERAL TIPS:

1) There are several different versions of ADDSYNC and DirSync. Make sure you get the latest version. The official name of the new version is Azure Active Directory Sync. Here is a good Microsoft article about the differences in the versions. https://msdn.microsoft.com/en-us/library/azure/dn757582.aspx

2) AADSYNC will attempt to Sync every user in the entire ADUC if you don't stop it. Make sure users are organized into OU's and configure OU FILTERING immediately after installing DirSync. We suggest starting with a "TEST OU" with only 1 or 2 test users in it. When you have gotten a feel for it, then change the OU Filter or add more users. Synchronization mistakes and errors can be very difficult to fix.

3) If local users have User Logon Names which differ from their email addresses, it can be confusing for them. If the user logs on to their computer as JSmith, but their email address starts with JohnS, you will need to be careful when setting up User Logon Name in ADUC. Make sure the local AD User Logon Name field matches the default email address.

CONCLUSION

DirSync is a great tool for connecting two powerful systems, Active Directory and Office 365. In a world where everything needs a password and every password should be changed regularly, limiting the number of those passwords is a great benefit for end users. After being configured, DirSync does not require a lot of changes or maintenance, so after the initial setup, its simplifying features become more and more valuable as time goes on.