MICROSOFT ACTIVE DIRECTORY SYNCHRONIZATION, ADFS, AND EXCHANGE HYBRID
TABLE OF CONTENTS:

How to Use Microsoft Active Directory Synchronization for Office 365 More Effectively .................................. 3

Exchange Hybrid/Coexistence Migrations to Office 365 ................................................................. 8

ADFS and its Integration with O365 ........... 11
CHAPTER 1: How to Use Microsoft Active Directory Synchronization for O365 More Effectively

In this chapter, we are going to focus on how to use Microsoft Active Directory Synchronization (“MS DirSync”) for Office 365 more effectively. For those of you who are unaware of what MS DirSync is, here is a quick summary:

MS DirSync is a useful feature/aspect of Office 365 that allows an organization to synchronize their local Active Directory forest up to Office 365.

Follow along for a lesson on MS DirSync!
Benefits for using MS DirSync are:

- A useful way to bulk populate the Office 365 tenant with an organizations users and distribution groups.

- Allow for management of the user accounts, mailboxes, and distribution lists from a company’s local Active Directory as they are used to with an on-premises MS Exchange environment.

- In this tech tip, We will discuss how to manually force a DirSync operation to commence and I’ll outline the Synchronization Service Manager which can be used to manage and obtain granular information with regard to DirSync and any issues/errors that may arise.
How to Manually Force a DirSync

After you setup and establish MS DirSync with Office 365, by default the service will automatically synchronize with Office 365 every 3 hours. This is not always acceptable especially if you have made some adds/moves/changes in your local Active Directory and you need to get those changes synched up to Office 365 ASAP.

Some examples of where waiting for the 3 hour interval isn’t sufficient are:

• A new hire has just started and needs to get their email/mailbox established ASAP
• A user needs to be added/removed from an important distribution list.
• An employee has been terminated and the disabling/removal of the account/mailbox needs to be synchronized.
So, to manually force the DirSync operation, perform the following:

- Log onto your MS Directory Synchronization Server.
- Browse to the following location: \Program Files\Microsoft Online Directory Sync
- Locate the DirSyncConfigShell.psc1 file and Double-click
- When the Powershell module opens, input the following command: Start-OnlineCoexistenceSync and press “Enter”.
- This will start a DirSync operation immediately, thus not having to wait for the 3-hour interval.

Synchronization Service Manager

- This “Synchronization Service Manager” is a nice little gem that can help you with managing MS DirSync especially if errors arise. This tool is also installed when you first install MS DirSync, and you can locate it by browsing to the following location on the DirSync server:
  \Program Files\Microsoft Online Directory Sync\SYNCBUS\Synchronization Service\UIShell\n
- Once there, look for a green icon with 2 white arrows within named “miisclient” and double-click to execute. (NOTE: You should create a shortcut and place it on your Desktop and/or within the Start Menu so you don’t always have to browse here to run this program.)

- Now, the Synchronizaton Service Manager opens. For now, we are only going to discuss the “Operations” tab, which is where you will spend 90% of your time within this tool. Within this Operations tab, you will see a log of all of the DirSync operations that have run since the product’s initial install date. You will see the automatic synch jobs and their status that run every 3 hours, and you can also see any and all of the manual jobs that you have run as well.
If you highlight one of the entries in the log (either SourceAD or TargetWebService), below you will see details associated with that particular job.

You can see the statistics that show all of the adds/updates/renames/deletes that occurred with that synchronization, and on the right you can identify the Synchronization errors that occurred, if any.

You can even get further granular by selecting one of the items that errored (usually denoted by a CN= at the start of the entry) and get information on the object/group that encountered the problems. In the main log, the “Status” column will depict an overview if issues were found or not.

If you see “Success”, everything was fine. The bottom line, is that this Synchronization Service Manager allows for a nice alternative then just the email notifications that get received from Microsoft to the one, main user/email account on the tenant for investigating and troubleshooting issues.

Clearing the Runs No, it’s not what you are thinking! (Get your minds out of the gutter!).

However it is an important operation to perform if your Directory Synchronization stops running or updating. All of the logs and line items that are displayed within the Synchronization Service Manager are stored within a local SQL Express 2008 database, and if this gets full, then DirSync will stop updating to Office 365 until this is resolved.

To do so, Log into the Synchronization Service Manager Click on the “Actions” menu at the top of the screen. Highlight and select “Clear Runs”. This will clear the listed runs and essentially purge these excess logs from the database, allowing MS DirSync to run properly once again; thus synchronizing with Office 365 as normal.
This tip focuses on Exchange Hybrid/Coexistence migrations to Office 365 with the new Wave 15 (Exchange 2013) backend. If you are not aware, Microsoft released the new version of Office 365 (branded as “Wave 15”) on Feb. 27, 2013 and there are some new wrinkles and challenges to be encountered as a result.

One in particular deals with Exchange Hybrid/Coexistence with this new Office 365 Wave 15.

This week’s tech tip will be short and sweet; however it will save you time when trying to decide how to architect the solution.
1.) If you are dealing with any customers who have the new Wave 15 Office 365 tenants and want Exchange Hybrid, here are some things to consider when planning the architecture.

- If the customer has an Exchange 2007 or Exchange 2010 on-premises environment, then you can install/setup/configure an Exchange 2013 Hybrid/Coexistence server in order to facilitate the migration and establish the coexistence.

- If the customer has Exchange 2003, then you CANNOT use an Exchange 2013 Hybrid server. This is because Exchange 2013 is incompatible and simply cannot coexist with Exchange 2003. In this case, you MUST use an Exchange 2010 Hybrid/Coexistence server in order to facilitate this migration.

2.) If you are indeed migrating a customer with an existing Exchange 2003 or SBS 2003 environment, then you must also perform a double-migration. This means that you must first migrate the mailboxes to the Exchange 2010 Hybrid server, and THEN you can migrate the mailbox up to Office 365 Wave 15.

- If you attempt to do a straight “New Remote Move Request” from a mailbox living on an Exchange 2003 server directly to Office 365 Wave 15, you WILL get errors and the mailbox migration will fail.
Most of the errors will cite corruption on most if not all of the items, and occasionally you will see different errors, but basically they occur because the Exchange 2013 servers within Office 365 Wave 15 simply cannot communicate properly with the Exchange 2003 servers/mailboxes.

So, if you have a customer with this scenario, make sure you plan the deployment of your Exchange 2010 Hybrid server accordingly. Meaning, make sure you install the mailbox server role upon installing Exchange 2010 and make sure that you have allocated enough disk space to the Exchange 2010 server to temporarily accommodate the mailboxes that will be living upon it during this double migration.

You may also need to add some extra RAM/CPU to it so it can temporarily handle serving these mailboxes while its performing its typical hybrid tasks.
CHAPTER 3: ADFS and its Integration with Office 365

ADFS? Not so fast!

Active Directory Federation Services (ADFS) was introduced by Microsoft as a part of Windows 2003 R2 as a method to “link” two unlike Active Directory domains as a means to simplify access to systems and applications (for example, within a partner’s network/organization) through web-based services using Single-Sign On (SSO) technology.

Microsoft now offers it up as a means to accomplish the same SSO capabilities with Office 365.
We have been a part of many ADFS deployments with respect to Office 365, and we can say that it works quite well once it is up and running. However, we feel that there are a lot more negatives or “cons” with an ADFS deployment, especially in comparison to other tools that are now available to similarly accomplish SSO, namely our Password Synchronization tool from MessageOps.

If a component of your ADFS environment is down/offline, your users WILL NOT be able to access their mailboxes (email/calendars/contacts, etc.)

What this means, is that if the ADFS Proxy server is down or unavailable, then user authentication requests will not get passed down to the back-end ADFS server and subsequently not to the domain controllers, thus users’ can’t log in. Obviously, if the main back-end ADFS server (which houses the database) is down/offline, then users can’t log into the Office 365 environment (MS Outlook and OWA) as well.

Isn’t one of the main reasons to move an email/messaging environment to the cloud is to avoid or remove these on-premises dependencies? When you deploy ADFS, you are essentially shifting the on-premises dependency from your on-premises Exchange/GroupWise/Lotus Notes servers to these ADFS servers?
We have also worked first-hand with customers that have experienced problems/issues with their ADFS servers, and they are “dead in the water” with regard to email until these servers get fixed/back online.

Now, keep in mind that even when ADFS is down, email is still being delivered to your user’s Inboxes as they don’t affect mail flow, which would obviously be affected in the case of an on-premises email server crash; however, your phone and the phones of your IT staff colleagues will still be getting blown-up by users who can’t get to their email.

**Password Synchronization Tool:**

So, if you are wondering how you can still achieve SSO without all of the CONs listed above and having a dependency on your on-premises environment, we at Champion/MessageOps have the solution for you. Use this link that explains the Password Sync tool in more detail and all of the specs/requirements for it.

The most important thing about this tool, is that if the Password Sync server encounters an issue, it **DOES NOT** affect users’ abilities to access their Office 365 mailboxes.
Conclusion:

The bottom line is that you should seriously weigh all of your options before investing in ADFS to be a part of your Office 365 solution. Especially for small and medium-sized organizations, the better option may be to either utilize a tool like Password Synchronization or perhaps not even go with an SSO solution at all.