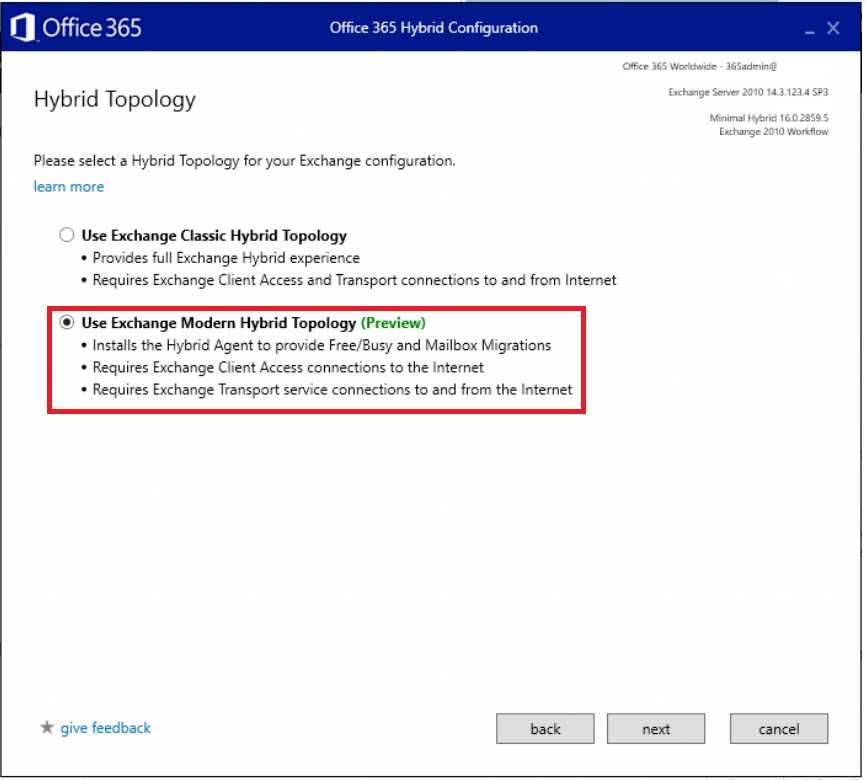
How to migrate email to Office 365 Exchange Online with zero downtime (the easy way)



Some people will tell you that Hybrid is not a good idea for small business networks, since it is “too complex” or “too messy.” Don’t listen to the naysayers. They are just not aware yet of how stupidly simple it has become, with options like [minimal hybrid](https://docs.microsoft.com/en-us/exchange/mailbox-migration/use-minimal-hybrid-to-quickly-migrate) and the brand new  
[Hybrid Agent.](https://docs.microsoft.com/en-us/exchange/hybrid-deployment/hybrid-agent)

Recently(ish) Microsoft improved the Hybrid Configuration Wizard, and made migrations even more simple than they were before, even for small and mid-sized businesses. So this post will stand as an update to all previous posts I’ve had about migration to Exchange Online using other methods like Cutover, Staged or “Classic Hybrid.” In our demonstration here, will be using the so-called “Modern Hybrid” method, which relies on that new Hybrid Agent.

There are still a lot of legacy environments out there, and it is not even a debate anymore as to which migration method provides the smoothest experience to end users (while also being the easiest for admins to complete, end-to-end). So I encourage you to try this out if you’re looking to do a migration sometime soon.

Without further ado, let’s jump in and cover, step-by-step, the migration of mailboxes from Exchange Server 2010, 2013 or 2016 to Microsoft Office 365 Exchange Online.

Setup your subscription (if you haven’t yet)

I assume most of my readers will be looking to migrate into Microsoft 365 Business subscriptions, but any subscription that includes Exchange Online will do for now (and this guide works for any 365 plan/flavor).

You can setup your domain right away and add users when you sign-up, or if you prefer (as I do), then you can skip past these sections to get going without making too many changes.

Graphical user interface, text, application, chat or text message

Description automatically generated

Depending on which subscription you ordered, you might notice that the initial setup wizard asks for all kinds of stuff (e.g. device management settings)–but as I mentioned, you don’t have to configure them right now. In general I don’t use the wizard, and I don’t recommend that you do, either. This can all be customized later.

For example, once you are into your admin portal, you can still add your domain name(s): go to **Setup > Domains**. Click **Add domain**.

Graphical user interface, application

Description automatically generated

I recommend the option to manage your own DNS records–just take the TXT record they give to you, and input that into your DNS provider (GoDaddy, Network Solutions, or whomever you use to manage your domain name). This step will prove to Microsoft that you own the domain name(s) that you are adding. Note it can take some time to verify after you make the changes.

Graphical user interface, application

Description automatically generated

Important: At this point you don’t want to add any users or assign any licensing yet. If you already have assigned licenses, go remove the licensing, at least for the Exchange Online plan. This will remove any mailboxes that were provisioned in the cloud (you don’t want them to be “in the way” when you go to migrate).

Prepare for Azure AD Connect

Let’s say your on-premises domain name is **companyname.local**—that means users probably sign in with something like *username@companyname.local*, or *companydomain\username*. Unfortunately, these identities are meaningless in Azure AD and Microsoft 365 won’t understand them.

In the cloud, we have to ensure that your users can sign-in using their email address as the username, e.g. **username@companyname.com**. To get these matching one another on-prem, we might have some adjustments to make. Don’t worry—most of the time they are painless.

To add UPN suffixes on-premises, open the **Active Directory Domains and Trusts** MMC, and then right-click **Active Directory Domains and Trusts** at the root of the tree, and select **Properties**. If it isn’t already listed in here, then enter your external email domain name(s) and click **Add**. Click **OK**.

Graphical user interface, text, application, email

Description automatically generated

The reason you do this is so that you can go assign users the UPN suffix that matches their primary email domain name. In **Active Directory Users and Computers**, check the **Properties/Account**tab on your user objects. Note: It is also possible to bulk-select users and edit the suffix field en masse.

Graphical user interface, text, application, email

Description automatically generated

Performing the UPN suffix switch will have no impact on end-user sign-in, except that they could (if they wanted) start signing in with [username@emaildomainname.com](mailto:username@emaildomainname.com) instead of domain\username (though both will continue to work).

However, if your on-premises users have a sign-in name like: BobSmith, but their email address looks more like: [BSmith@domain.com](mailto:BSmith@domain.com), then you should change the UPN *prefix*attribute on-premises to match the email address also. E.g. *BobSmith* should become *BSmith*.

If the prefix values already match, then you should be good to go without making any further changes. But if they don’t match, then this change is going to impact on-premises sign-in experiences, obviously. Therefore, you will need to communicate this change in advance, so that users are aware of when they need to start signing in to the domain using their email address instead of the legacy format.

Install Azure AD Connect

You can [download](https://go.microsoft.com/fwlink/?LinkId=615771) and install Azure AD Connect on either a Domain Controller, or a Member server (at least 2012 R2 recommended) within your on-premises environment. Note that Windows Small Business Server (SBS) and Windows Server Essentials (WSE) are not officially supported. Therefore, use a separate member server in these environments.

Graphical user interface, text, application

Description automatically generated

You can use the [express settings](https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-express) for the fastest configuration. This will copy all your identities into the cloud, and that might include some extras (e.g. legacy service accounts) that you have to subsequently go remove from the cloud, after migration is done and the tool has been removed. That’s okay. Optionally, you can also do a [Custom installation](https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-custom), which I describe in my [Microsoft 365 Business Admin Guide](https://www.itpromentor.com/m365b-ebook/).

Once this is completed, all of your user identities should be active in the cloud. Test it out by signing into [https://portal.office.com](https://portal.office.com/) with an email and password from the on-premises environment.

Run the Hybrid Configuration Wizard

Now, it is a known fact that hybrid migrations will give you the best user experience, bar none. Those with Outlook will simply get prompted to close and reopen. They will sign into Office 365 using their email and password, and all of their mail items show up like normal. IT doesn’t have to do a damn thing for them (well, some people will still be confused and panic, and not know what to do when it tells them exactly what they should do, but you get my point–it’s still easier this way).

Graphical user interface, text, application

Description automatically generated

You are ready to initiate hybrid. To start, just [download](https://aka.ms/HybridWizard) and run the Hybrid Configuration Wizard on your Azure AD Connect server.

Graphical user interface, text, application, email

Description automatically generated

You can just allow the wizard to find the optimal server and proceed **Next**.

Graphical user interface, application

Description automatically generated

You will need to specify administrative user credentials both on-prem and in the cloud, so that the hybrid wizard can connect to both ends and configure things appropriately.

Graphical user interface, application

Description automatically generated

Once it has made a connection, the next step is to choose **Minimal Hybrid**. You would only use Full Hybrid if you had like hundreds of mailboxes to move over a set of staged out migration waves. Small and Mid-sized orgs can usually accomplish their migration all at once, with *Minimal* Hybrid. **Next**.

Graphical user interface, text, application

Description automatically generated

The other choice to make here is between a Classic and Modern hybrid topology. At the time of this writing, the “modern” is still in preview. I won’t go into the technical details too much, except to say that modern is even easier to use than the classic option, and will probably be the preferred mechanism going forward. **Use Exchange Modern Hybrid Topology**.

Graphical user interface, text, application

Description automatically generated

What this does, is installs a “Hybrid Agent” on the server that you’re running this wizard from (you’ll have to accept some EULA terms). The agent will configure and publish an Azure Application proxy–this in turn allows your Exchange migration to be routed via an Azure web service front-end, so Office 365 talks through that proxy, rather than directly with your local server, for its migration endpoint.

Graphical user interface, application

Description automatically generated

Go ahead and finish the wizard. Click **Update**.

Graphical user interface, text, application

Description automatically generated

And that should be the end.

Graphical user interface, text, application, Teams

Description automatically generated

Configure migration batches

Now navigate to the [Exchange admin center](https://outlook.office365.com/ecp/), find **recipients > migration**. Click the **ellipses**and go to **Migration endpoints**.

Graphical user interface, text, application

Description automatically generated

You can see in the details here that the hybrid wizard has linked the application proxy to Exchange Online–this is how the migration jobs will be carried out.

Graphical user interface, text, application, email

Description automatically generated

Now you can create a new migration batch for your users. Again from the **recipients > migration** tab, pick the plus sign, a select **Migrate to Exchange Online**.

Graphical user interface, text, application

Description automatically generated

Choose the first option for **Remote move migration** and **Next**.

Graphical user interface, text, application

Description automatically generated

It is possible to just browse your address book and select the users individually using that plus sign there under **Select the users that you want to move**, or you can use a [csv file](https://docs.microsoft.com/en-us/exchange/mailbox-migration/csv-files-for-migration) with all of the email addresses in it.

Graphical user interface, text, application, email

Description automatically generated

After you confirm your selection, the wizard will show you the URL of the migration endpoint. In a classic hybrid scenario, this would need to be configured to point to your mail server’s public address such as *mail.companyname.com*, and you would have had to prove ownership of the domain(s) again–ick! But in this case we’re using a modern hybrid, so it will be the Azure proxy address that was setup by the hybrid agent.

Even though this looks complex, it is not (it’s easier than it was in the past actually) because you didn’t really need to “do” anything except run that wizard. **Next**.

Graphical user interface, application, Word

Description automatically generated

Name your batch and complete the wizard. I recommend that you choose the option to automatically start but manually complete the batch. That way, you can come back to the portal when you are ready, select the migration batch, and move the status to **Complete** on the right.

Table

Description automatically generated

As mentioned, PC users will need to close and reopen Outlook to sign back in to Office 365 (they will be prompted to do so). Mobile users must delete their email accounts from their mobile devices, and then add them back (preferably using the Outlook app). Microsoft provides some [end-user instruction](https://support.office.com/en-us/article/Office-365-mobile-setup-7dabb6cb-0046-40b6-81fe-767e0b1f014f?ui=en-US&rs=en-US&ad=US) that you can use.

Congrats, you’re in the cloud now. Easiest. Email. Migration. Ever.

Be sure to complete your cutover by configuring your DNS records to point at Exchange, and other follow-up items I will mention below.

Configure DNS records

**WARNING**: DO NOT PROCEED TO THIS STEP UNTIL YOU HAVE ALREADY COMPLETED YOUR MIGRATION JOBS AND MAILBOXES HAVE BEEN MOVED TO THE CLOUD.

To find the appropriate DNS records, navigate to the [365 admin portal](https://admin.microsoft.com/), and return to **Setup > Domains**.

Graphical user interface, application

Description automatically generated

Pick your domain to continue the setup process and fetch the new MX, autodiscover, etc. records, and get them all configured in your portal for GoDaddy, Network Solutions, or whomever hosts your public DNS for you.

On-premises if you have a DNS zone for the external domain(s) you will also want to update your CNAME for autodiscover so that it points to autodiscover.outlook.com. If you do not have a DNS zone for the external domain on-premises, then you are good to go, as the on-premises clients should already be looking to external DNS for the external domain lookups.

And last but not least, on the on-premises Exchange server, change the SCP to a null value:

Get-ClientAccessServer | Set-ClientAccessServer -AutoDiscoverServiceInternalUri $null

Assign licenses if you haven’t already!

Also, make sure you have assigned the purchased licenses to your user accounts via **Users > Active users** in the [365 admin center](https://admin.microsoft.com/).

Graphical user interface, application

Description automatically generated

A note about SMTP relay (if applicable)

The preferred method for relaying mail from an on-premises scan to email device or third-party application, is to use SMTP submission. See [this article](https://docs.microsoft.com/en-us/exchange/mail-flow-best-practices/how-to-set-up-a-multifunction-device-or-application-to-send-email-using-office-3) for this and the other two options. For example, Office 365 can provide a [relay connector](https://technet.microsoft.com/en-us/library/dn554323%28v=exchg.150%29.aspx#option3) to replace the same functionality you used to have with your local Exchange server (but it is not the preferred option).

A note about licensing options

If a user interacts with Office 365 software using Windows 10 and the full installed Office client apps, then you would assign them Microsoft 365 Business licenses. These licenses also include ATP (for extra anti-malware and anti-phishing protection).

If you have users who do not use Windows 10 or the client applications, you do not have to assign them Microsoft 365 Business. If all they need is email and other online apps like OneDrive, then consider Business Essentials for them (or even Exchange Online Plan 1 for email only users). However, be sure to add anything else they use or benefit from, for example:

* Exchange Online Archiving (archive mailbox, legal holds, etc.)
* Data Loss Prevention (DLP)
* Azure Information Protection (email encryption)
* Advanced Threat Protection (ATP) plan 1
* Intune (Device management)

The funny thing is, when you consider everything you might have to add for an “email only” user (e.g. to properly manage and secure them), it can end up being almost as much as just licensing them for the full Microsoft 365 Business anyway.

Shared mailboxes are not real people, and so are generally considered free (you don’t need licenses assigned to them). But, there is a catch–if you do need to protect them for interactive access, then you would treat them like any other mailbox, give them a mailbox license with whatever additional protections you need. For instance, you could purchase Exchange plan 2 if you needed to enable legal hold on that shared mailbox. Add ATP if they also need to receive that protection. Etc.

A note about public folders

If you still have public folders out there that are actually being used, consider migrating to something more contemporary like [Outlook groups](https://docs.microsoft.com/en-us/exchange/collaboration/public-folders/migrate-to-office-365-groups?view=exchserver-2019) (or, see if that workflow could live in Teams even).

Otherwise, if you insist on remaining in the stone age, the easiest way to accomplish a migration of some old PF data in the SMB is to just export to PST from the on-premises server, and then re-import them to a new public folder mailbox that you setup in Exchange online from **public folders > public folder mailboxes**. You may need to reset permissions.

Graphical user interface, application

Description automatically generated

Remove Azure AD Connect and the on-premises Exchange Server

Once you are all done with migration, your choice whether you keep passwords syncing or not. If you do, then that means you always have to create your accounts on-prem, and make certain other changes on-prem. I describe this split-management experience [here](https://www.itpromentor.com/hybrid-cheat-sheet/).

But, if your intention is to migrate all other network components to Microsoft 365, including shared files, etc., then there is probably no reason to keep that relic around any longer. Just find the Azure AD Connect tool under Add/remove and uninstall it. Then you can disable synchronization online also, using [this method](https://docs.microsoft.com/en-us/office365/enterprise/turn-off-directory-synchronization).

You can also [remove your Exchange server](https://docs.microsoft.com/en-us/exchange/decommission-on-premises-exchange) at this point, provided that you have moved all mailboxes and removed any other dependencies such as local SMTP relay. Do NOT remove the Exchange server until you have completely uninstalled Azure AD Connect and disabled directory synchronization.

Oh, and once you have removed the Azure AD Connect tool, you can also go into your 365 admin portal, and clean up the active users–delete anything that doesn’t need to be there.

A note about everything else

Congratulations, you are basically done. However, there is still a lot to do, like configure [email authentication](https://www.itpromentor.com/email-auth/), setup [Mobile device management or Mobile application management](https://www.itpromentor.com/mdm-showdown/), configure your [antispam and antimalware settings](https://www.itpromentor.com/anti-spam/), including ATP [anti-phishing](https://www.itpromentor.com/atp-1/), [safelinks](https://www.itpromentor.com/atp-3/" \t "_blank)and [safe attachments](https://www.itpromentor.com/atp-2/), enable [multi-factor](https://www.itpromentor.com/mfa-refresh/), and a whole bunch of [other things](https://www.itpromentor.com/12-steps-scc/). So don’t stop learning in this environment–there is so much out there to explore. I hope this site has been a good resource for you in doing just that.