Do I need an on-premise Exchange using Exchange online

[A picture containing text, light

Description automatically generated](https://msb365.abstergo.ch/wp-content/uploads/2018/10/emily-morter-188019-unsplash.jpg)

The story is often the same one: I get invited for a workshop from a customer about projects for messaging and/or Office 365 topics and one of the main questions is about on-premises Exchange, Hybrid Exchange and/or Exchange online.

However, there is a confusion in the IT world out there about these topics. The question I mostly get asked is: “do we still need an on-premises Exchange when we move to Exchange Online? Why do we do that? We don’t have any more mailboxes on-premises.”

Well the answer is, yes – there is still at least one Exchange server on-premises needed even when we migrate to Exchange online, even worst, for redundancy reasons there are theoretically even two of them needed … BUT this applies to 85% of the cases in the field! There are still some 15% with a scenario where we don’t need an on-premises Exchange server anymore.

In this article I will describe why in 85% of the scenarios an on-premises Exchange is needed and why in 15% not.

**What is Identity Hybrid?**

To start with the explanation, we need to begin with this chapter. The most of us are familiar with the idea of Exchange hybrid. In a hybrid environment we have Exchange mailboxes from our organization in Exchange online and Exchange on-premises server with a shared namespace, shared address book and free-busy coexistence etc.

We also know that our on-premises Exchange server stores object attributes in the Active Directory, whcih we need to sync to Azure AD to support the Exchange online hybrid. However, even if we have moved all of our organization mailboxes to Exchange online, we still have a directory sync requirement. Therefore we have an “Identity Hybrid”.

What happens if we uninstall our last Exchange Server?

We still have the Identity Hybrid – that is unrelated to our last Exchange server on-premises. However, with directory sync in place (AADConnect) the majority of Azure AD attributes are read-only in Azure AD. That means that all of the changes have to be done in the local Active Directory and then synced to the Azure AD.

If we uninstall our last on-premises Exchange server, we do not have a supported way to change these attributes anymore, if we even know what these attributes for Exchange are.

To make changes we would need to resort ADSIEdit etc. and we don’t even have a good script engine to help with consistency and bulk edits.

**Attributes? Which ones?**

Well, the important attributes are:

* msExchMailboxGUID
* msDsConsistencyGUID
* proxyAddresses
* E-mail address policies (Yes, this is not an attribute, but Exchange ensures uniqueness and the consistency of proxyAddresses)
* legacyExchangeDN (and X500 addresses in the proxyAddresses as well)

There is no rule without at least one exception! The UPN (User Principal Name) and the Mobile Number are not a part of it.

**Okay so far, but what do we really need?**

I think the reasons why we still need Exchange on-premises even if we have moved all mailboxes to the cloud is now clear. However, if we think about the requirements of an Exchange Server the next question is, what do we really need?

A must have to manage the mailboxes in Exchange online is the Exchange Management Shell and the Exchange Control Panel. This is the reason why there is still an Exchange on-premises required. However, the good news are, we do not need the same amount of disks and RAM for this Exchange server. That’s why we can easily virtualize the management server.

Another point we really need to be ready for Exchange with all mailboxes in Exchange online is, that all Exchange tools in AD are updated in a supported way.

Last but not least there are nine attributes that write all the way back from Exchange directory (EXODS) to AD, that means AADConnect needs to be configured for that.

However, if I really want to remove the very last Exchange Server even by knowing the facts we just learned, there is one way. If we remove the directory synchronization first – this makes all the objects editable in the cloud and unrelated to Active Directory.

However, we also need to remember that an on-premises Exchange server can also act as a mail relay for all of our on-premises applications and devices which need to send e-mails.

Further information about how and when to decommission on-premises Exchange server in a hybrid deployment you can find at Microsoft by following this Link: <https://docs.microsoft.com/en-us/exchange/decommission-on-premises-exchange>

**Ok, good, this was about the 85% of the marked, how about the other 15%?**

In the past, I wrote an article about [migrating on-premises mailboxes to Office 365 by using Quest tools](https://msb365.abstergo.ch/?p=2352).

The scenario in that article was that I had an old site (Forest old) with on-premises Exchange and a green field site (Forest new) without anything. Before we migrate the Active Directory users from the old to the new forest, we need to install the Exchange schema extension to the new forest. After that we can migrate the users to the new forest.

Graphical user interface

Description automatically generated

When the users are migrated, we need to sync them to our new Office 365 tenant by using AADConnect. After the users are synced to Azure AD, we create new mailboxes in the Office 365 tenant (on Exchange online).

Graphical user interface, application

Description automatically generated

Now, we can use a third party tool like Quest, BitTitan etc. to migrate the mailbox content from the old on-premises site to the new Office 365 Tenant.

Diagram

Description automatically generated

How this kind of migration works in detail, I have written down in another article here at my blog. If you are interested in it, feel free to follow this link [HERE](https://msb365.abstergo.ch/?p=2352).

However, if we  are using this scenario, we don’t have a directory synchronization for Exchange between the local Active Directory and the Azure AD. That means we can run the Exchange online remote PowerShell cmdlet and manage our Exchange online environment in this way or using the Office 365 online portal.