Exchange on premise - Interactive poll joining details

- **QR code**

Alternatively

- Slido.com
- Code - 426378

Exchange server on premise - removing after a hybrid migration

14 May 2021

V1.0

LOCAL DIGITAL Cyber

Our purpose

- We are delivering cyber expertise, support and guidance - identifying opportunities for enhancement in the local authority cyber security posture.
- We are working with a selection of councils who completed the Mitigating Malware and Ransomware survey (February 2020).
- We deliver cyber tools, with support, and together with the local authority execute a roadmap for cyber enhancement. This is increasing councils' resilience against ransomware attacks.
- The roadmap (aka Cyber Treatment Plan) is also being used as a communication vehicle within local authorities to drive the cyber agenda and prioritise on budget allocation from senior leaders.
- Promoting interactive and open collaboration is allowing local authority cyber security professionals to '***raise the cyber voice***' within Senior Leadership teams

Who we are

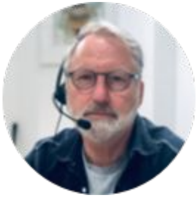
We are the cyber security team of the Local Digital Collaboration Unit at MHCLG

Brad

Cyber product owner

Greg

Agile delivery lead



Jay

Technical lead

Ian

LA engagement lead

Dev

Communication

Chris

Cyber lead

+ **Technical support specialists**

LOCAL DIGITAL Cyber

Cyber clinics

Clinics so far…...

- 12th March - AD toolkit
- 19th March - OpenVAS
- 26th March - LME
- 9th April - Conditional Access Policy
- 16th April - M365 Backups - Why bother ?
- 23rd April - Offline Backups
- 30th April - MFA for on premise accounts
- 7th May - Password & identity protection

- Any suggested topics you would like to us cover in future clinics?

  cybersupport@localdigital.gov.uk

- Rerun any of the above?

Agenda

Hybrid Exchange - on premise server - removing after a hybrid migration

- Overview
- Why would I keep it ?
- Can I remove it ?
- Scenarios
- The future
- Summary

Overview

- Previously, Microsoft Hybrid migrations to Exchange Online required you to keep an Exchange server on premise.

- Removing it would leave you with an unsupported system.

- However, the stance on this is altering as Microsoft are now moving away from on premise email systems. For most configurations Microsoft are still recommending that you keep at least one Exchange Server on premise if you require synchronisation services.

slido

What version of MS Exchange Server are you running on premise ?

ⓘ Start presenting to display the poll results on this slide.

Reasons to keep an Exchange server on premise:

1. Directory synchronisation required after a hybrid email migration between on premise AD and Azure AD
2. Management requirements (of email and user accounts)
3. Internal relaying of email to internal and external mailboxes
4. Older email clients in use in client compute base
5. Local mailboxes that are not worth a monthly fee for being online
6. Legacy systems that won’t work with Exchange Online

Other than Microsoft Requirements, what are you using your on premise Exchange Server for ?

ⓘ Start presenting to display the poll results on this slide.

How to secure your on premise Exchange

1. Ensure it is running the latest version of Exchange Server 2016 (highest CU etc)*
2. A free hybrid only license for Exchange 2016 is available as part of Exchange Online services if you are running earlier versions so no license cost is involved.
3. Regularly patch the host server OS and Exchange software
4. Secure the transit between the Exchange Server and Microsoft Servers (e.g only allowing traffic to/from approved sources through perimeter firewalls)
5. Lock traffic to/from Exchange server to only go to approved Microsoft Servers
6. Tidy up publicly published DNS records that are no longer required

* Exchange Server 2019 can also be used but requires a full license

How often do you check for updates and patch your Exchange Server Application ?

ⓘ Start presenting to display the poll results on this slide.

Microsoft scenarios

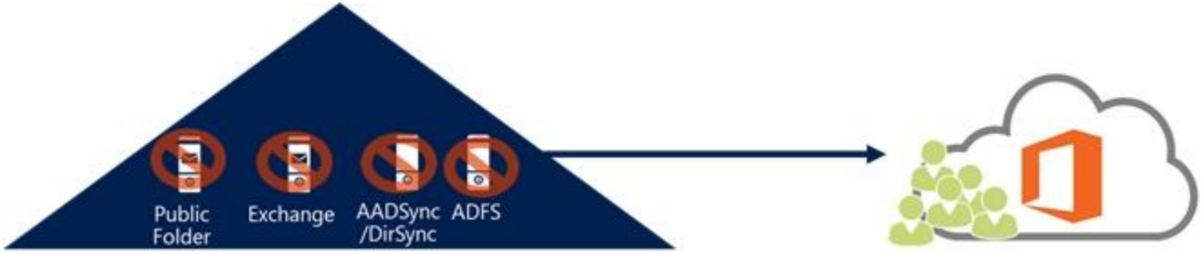
Microsoft scenario 1

Issue:

My organization has been running in a hybrid configuration and I have all of my mailboxes in Exchange Online. I do not need to manage my users from on-premises and no longer have a need for directory synchronization or password synchronization.

Solution:

Since all of the users will be managed in Microsoft 365 or Office 365, and there are no additional directory synchronization requirements, **you can** safely disable directory synchronization and remove Exchange from the on-premises environment.



Microsoft scenario 2

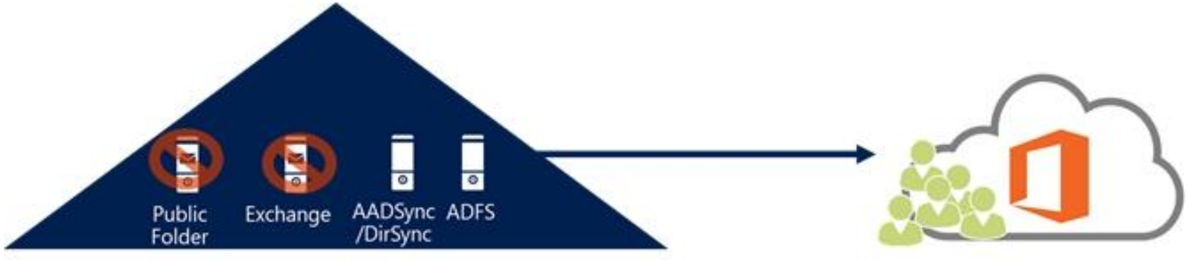
Issue:

My organization has been running in a hybrid configuration for about a year now and have finally moved my last mailbox to the cloud.

I plan to keep Active Directory Federation Services (AD FS) for user authentication of my Exchange Online mailboxes. (This scenario would apply to any customer that is planning on keeping directory synchronisation).

Reasons to keep directory synchronisation in place are manyfold. The primary reason would be SSO with Azure Services.

Desired State:

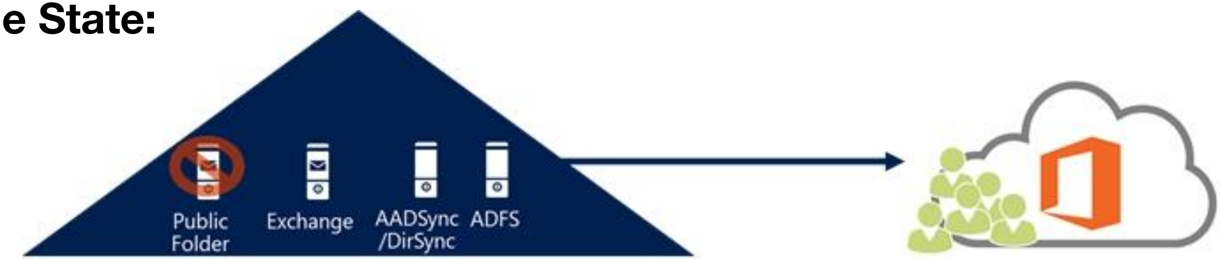


Microsoft scenario 2 (cont.)

Solution:

Since it is planned to keep AD FS, they will also have to keep directory synchronisation since it is a prerequisite. **Because of that, they cannot fully remove the Exchange servers from the on-premises environment. However, they can decommission most of the Exchange servers, but leave at least one of servers behind for user management.** Keep in mind that the servers that are left running can be run on virtual machines since the workload is almost completely shifted to Exchange Online.

Achievable State:



Microsoft scenario 2 (cont.)

- If you choose to remove ADFS from your infrastructure, Azure AD Connect will synchronize your on-premises credentials with the cloud. Each service will authenticate users independently:
- Microsoft 365 identity services will manage online requests.
  Active directory will manage the internal authentication.
- If you don't have any on-premises mailbox(es), you can safely decommission **most** of your exchange server(s), leaving one or more for user management purposes - **because the source of authority is still defined as on-premises.**

Microsoft scenario 3

Issue:

- I want to remove my Exchange servers on-premises after moving all of my mailboxes to Exchange Online.
- However, we discovered that we are using Exchange for other purposes, such as for a Simple Mail Transfer Protocol (SMTP) relay for an application or for access to public folders.
- If you have a need for Exchange servers on-premises to meet the current needs of your organization, it may not be in your best interest to remove the on-premises servers.

Microsoft scenario 3 (cont.)

Solution:

- **We recommend against removing Exchange and the hybrid configuration at this point.**
- If you were to even start the process by pointing the Autodiscover Records to Exchange Online, you would immediately break some features like hybrid public folder access.
- You could change the MX record to point to Exchange Online Protection if it is not already, you could even remove some of the on-premises Exchange servers
- However, you would need to keep enough in place to handle the remaining hybrid functions. Usually, this would lead to a very small on-premises footprint.

slido

What Directory Synchronisation are you using ?

ⓘ Start presenting to display the poll results on this slide.

The future

- As we stand, Microsoft are scheduled to retire Exchange Server 2016 and 2019 from extended support on the same date (14 Oct 2025).
- On this basis the general assumption is they will have given us a way to retire the Hybrid on premise Exchange server before this date.

Summary

- If you have a Hybrid Exchange configuration you MUST keep at least one Exchange Server present onsite.
- Unless you are wanting to host mailboxes on it you can use the FREE Exchange Server 2016 Hybrid license key - it is provided with Exchange Online for this reason.
- If you have no requirement for directory synchronisation between on premise AD and Azure AD you can get rid of any remaining on premise Exchange Servers, but remember they may be doing more than just host mailboxes (local relays, management, etc).
- If all your mailboxes and mailflow is M365 based - lock down your local firewall and Exchange server to only communicate with M365. This will reduce any potential attack surface.

slido

What frequency of cyber clinics would you prefer?

ⓘ Start presenting to display the poll results on this slide.

Staying in touch

Follow our progress

- Read our fortnightly sprint notes on Medium
- Follow LDCU on Twitter (@LDgovUK)
- Subscribe to our Cyber newsletter for progress updates and news relevant to those working in and around local government cyber security
- We'll also be sharing regular updates on the MHCLG Digital blog

Have your say

We welcome further collaboration and input, so if you would like to share with us any strong evidence to support our research please contact us by email:

- Cyber Support: cybersupport@localdigital.gov.uk
- Cyber Health: cyberhealth@localdigital.gov.uk

Ministry of Housing,
Communities &
Local Government

Thank you

[We welcome feedback on our cyber support service]

🐦 @LDgovUK

www.localdigital.gov.uk

#LocalDigital #FixThePlumbing

LOCAL
DIGITAL
Cyber

Further Reading

Here are some recommendations for further research into Exchange hybrid configurations, with particular reference to the need for an on premise server, and when it is not needed.

- *Exchange Server hybrid deployments:*

  https://docs.microsoft.com/en-us/exchange/exchange-hybrid

- *How and when to decommission your on-premises Exchange Server in a hybrid deployment:*

  https://docs.microsoft.com/en-us/exchange/decommission-on-premises-exchange https://practical365.com/how-to-decommission-an-exchange-server-after-office-365-migration/

- *Directory Synchronisation*

  https://docs.microsoft.com/en-us/microsoft-365/enterprise/plan-for-directory-synchronization?view=o365-worldwide

LOCAL DIGITAL Cyber

Appendices

On-premise Exchange Server

Although Exchange 2010SP3 and above are currently in scope of support for the on premise Exchange Hybrid Connection Server, Microsoft provides a license for Exchange Server 2016 Standard (Hybrid) as part of Exchange Online configurations (NOT Exchange 2019 though).

This license does not allow for the hosting of user mailboxes and is strictly for Exchange Online Hybrid Connectivity and Management.