Exchange Server 2019 Hybrid Setup

In this post, I will show you the steps to migrate Exchange Server 2019 to Exchange Online and Office 365. Within home lab, I am running Exchange Server 2019 CU6. Mail flow is working fine and Exchange Server 2019 is up to date with all patches. You can also follow this link from Microsoft - https://docs.microsoft.com/en-us/exchange/exchange-hybrid

Below is Exchange Lab Setup diagram

On the local DNS, I have these entries for Exchange Server 2019

autodiscover	Host (A)	5		static
EX2019	Host (A)	5		03-Jul-2020 1:00:00 PM
mail	Host (A)	5		static

On GoDaddy Public DNS, I have these entries for mail flow

Type	Name	Value	TTL	
A	@	99.	1 Hour	✎
A	autodiscover	99.	1 Hour	✎
A	mail	99.	1 Hour	✎
CNAME	enterpriseenrollment	enterpriseenrollment−s.manage.microsoft.co...	1 Hour	✎
CNAME	enterpriseregistration	enterpriseregistration.windows.net	1 Hour	✎
CNAME	ftp	@	1 Hour	✎
CNAME	sccmclouddp1	588a861c6563468db1ea72ba.cloudapp.net	1 Hour	✎
CNAME	www	@	1 Hour	✎
CNAME	_domainconnect	_domainconnect.gd.domaincontrol.com	1 Hour	✎
MX	@	mail.	1 Hour	✎
NS	@	ns45.domaincontrol.com	1 Hour	
NS	@	ns46.domaincontrol.com	1 Hour	
SOA	@	Primary nameserver: ns45.domaincontrol.co...	600 seconds	
TXT	@	MS=	1 Hour	✎
TXT	@	v=spf1 include:dnsexit.com −all	1 Hour	✎

On Office 365 Admin Center, I have added the Domain only. All users are synced. I did not create additional DNS entry at GoDaddy – reason, I am still in the process of migrating user to O365. Once the migration is complete – we can decommission Exchange 2019 On Premise and update all DNS Entry.
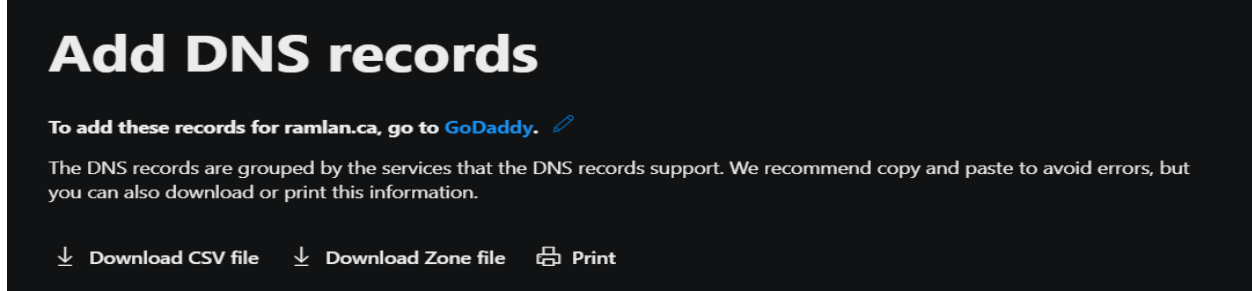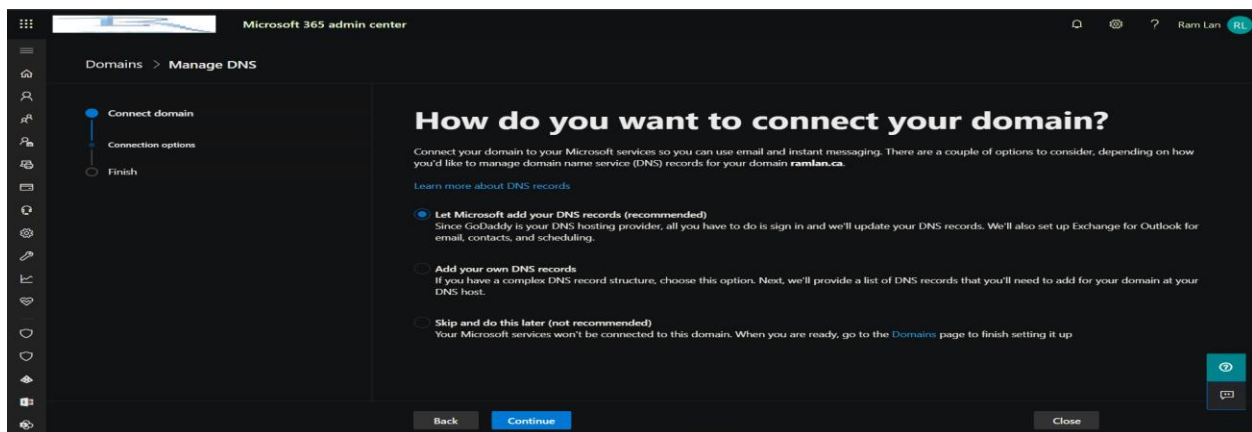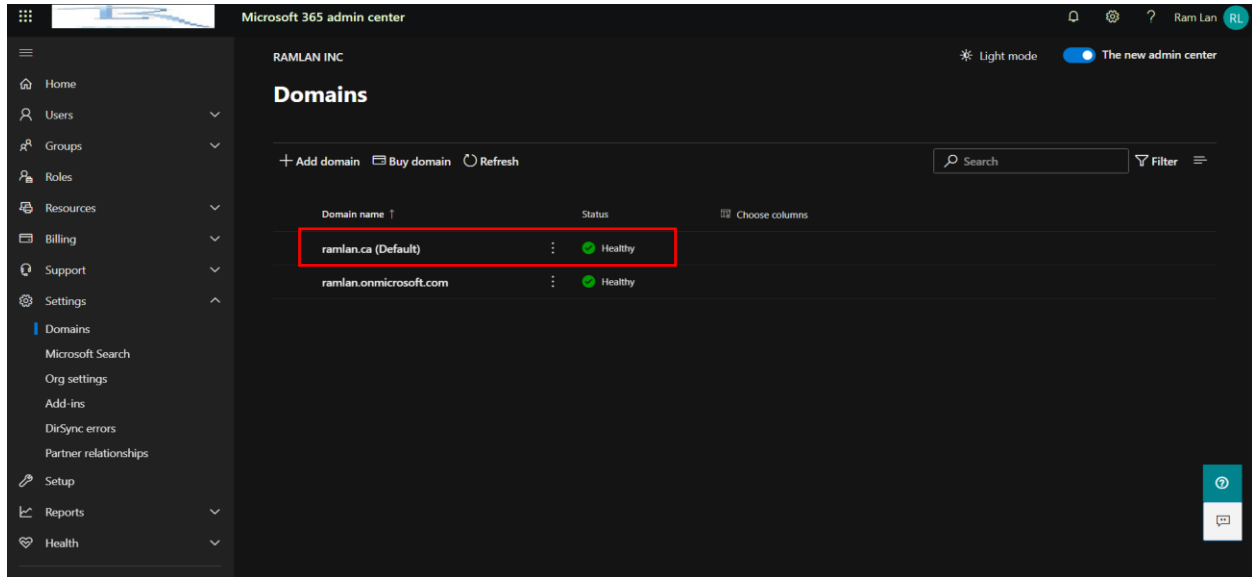
These are additional DNS entry that, I have to add at GoDaddy later.
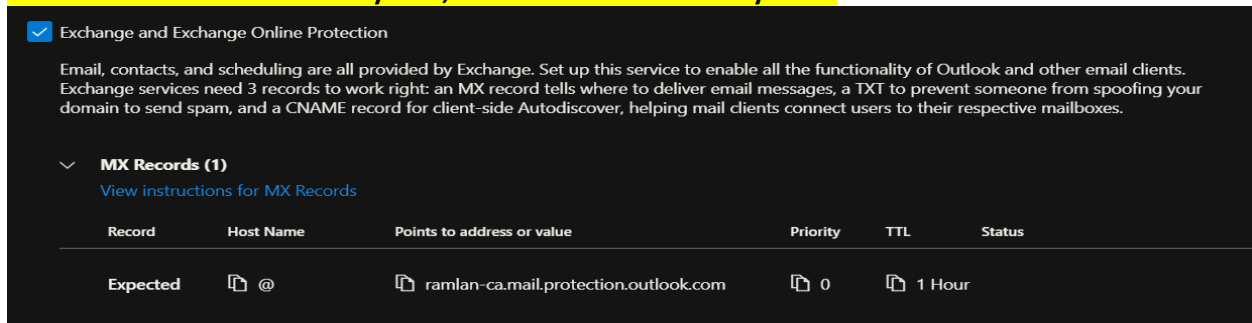
CNAME Records (1)
View instructions for CNAME Records

Record	Host Name	Points to address or value	TTL	Status
Expected	autodiscover	autodiscover.outlook.com	1 Hour	

TXT Records (1)
View instructions for TXT Records

Record	TXT name	TXT value	TTL	Status
Expected	@	v=spf1 include:spf.protection.outlook.com -all	1 Hour	

Advanced Options ︿

☑ Microsoft Teams and Skype for Business

Online communication services like chat, conference calls, and video calls are provided by Microsoft Teams and Skype for Business. Teams and Skype need 4 records: 2 SRV records for user-to-user communication, and 2 CNAME records to sign-in and connect users to the service.

CNAME Records (2)
View instructions for CNAME Records

Record	Host Name	Points to address or value	TTL	Status
Expected	sip	sipdir.online.lync.com	1 Hour	
Expected	lyncdiscover	webdir.online.lync.com	1 Hour	

SRV Records (2)
View instructions for SRV Records

Record	Service	Protocol	Port	Weight	Priority	TTL	Name	Target	Status
Expected	_sip	_tls	443	1	100	1 Hour	@	sipdir.online.lync.com	
Expected	_sipfederationtls	_tcp	5061	1	100	1 Hour	@	sipfed.online.lync.com	

☑ Intune and Mobile Device Management for Microsoft 365

This service helps you secure and remotely manage mobile devices that connect to your domain. Mobile Device Management needs 2 CNAME records so that users can enroll devices to the service.

CNAME Records (2)
View instructions for CNAME Records

Record	Host Name	Points to address or value	TTL	Status
Expected	enterpriseregistration	enterpriseregistration.windows.net	1 Hour	
Expected	enterpriseenrollment	enterpriseenrollment.manage.microsoft.com	1 Hour	

Microsoft 365 admin center | 🔔 ⚙ ? Ram Lan RL

RAMLAN INC   ☀ Light mode   🔵 The new admin center

Active users

- Home
- Users ⌄
  - Active users
  - Contacts
  - Guest users
  - Deleted users
- Groups ⌄
- Roles
- Resources ⌄
- Billing ⌄
- Support ⌄
- Settings ⌄
  - Domains
  - Microsoft Search
  - Org settings
  - Add-ins
  - DirSync errors
  - Partner relationships

ⓘ Due to a recent increase in Teams usage, when you assign a Teams license to a user it may take around 24 hours before they'll be fully set up. Until then, you won't be able to assign Teams policies to them, and they might not have access to some Teams features like calling and audio conferencing. Check status

⊕ Add a user   ☰ User templates   ⊕ Add multiple users   🔒 Multi-factor authentication   👤 Delete a user   ↻ Refresh   ⋯   🔍 Search   ▽ Filter

Display name ↑		Username	Licenses	⊞ Choose columns
agpmsvc	⋮	agpmsvc@RAMLAN.CA	Unlicensed	
Allan	⋮	allan@RAMLAN.CA	Microsoft Teams Exploratory	
CSEP_ALS_SVC	⋮	CSEP_ALS_SVC@RAMLAN.CA	Unlicensed	
Devon	⋮	devon@RAMLAN.CA	Unlicensed	
Ex Admin	⋮	exadmin@RAMLAN.CA	Unlicensed	
Exchange Online-ApplicationAccou...	⋮	Exchange_Online-ApplicationAccount@RAMLAN.CA	Unlicensed	
extest_49b71e1812bd4	⋮	extest_49b71e1812bd4@RAMLAN.CA	Unlicensed	
HealthMailbox-EX2019-001	⋮	HealthMailbox5e09af8b47344f63845ac35ea6db7ef4@RAM...	Unlicensed	

On Microsoft Azure I have completed AD Sync, User and Device Sync and no error with AD Sync

Dashboard >

RAMLAN INC | Overview
Azure Active Directory

Documentation ×

Overview
Getting started
Diagnose and solve problems

Manage
Users
Groups
External Identities
Roles and administrators
Administrative units (Preview)
Enterprise applications
Devices
App registrations
Identity Governance
Application proxy
Licenses
Azure AD Connect
Custom domain names
Mobility (MDM and MAM)

⊗ Switch tenant 🗑 Delete tenant + Create a tenant What's new ♡ Got feedback?

Azure Active Directory can help you enable remote work for your employees and partners. Learn more ×

RAMLAN INC

Search your tenant

Tenant information
Your role
Global administrator and 1 other roles
More info
License
Azure AD for Office 365
Tenant ID
5e11113d-da15-40e6-b616-07c...
Primary domain
ramlan.ca

Azure AD Connect
Status
Enabled
Last sync
Less than 1 hour ago

Sign-ins

Dashboard > RAMLAN INC >

Users | All users (Preview)
RAMLAN INC - Azure Active Directory

Documentation ×

All users (Preview)
Deleted users
Password reset
User settings
Diagnose and solve problems

Activity
Sign-ins
Audit logs
Bulk operation results

Troubleshooting + Support
New support request

+ New user + New guest user Bulk activities ↻ Refresh ⟳ Reset password Multi-Factor Authentication 🗑 Delete user ⋯

Search users   Add filters

Name	User name	User type	Source
agpmsvc	agpmsvc@RAMLAN.CA	Member	Windows Server AD
Allan	allan@RAMLAN.CA	Member	Windows Server AD
CSEP_ALS_SVC	CSEP_ALS_SVC@RAMLAN.CA	Member	Windows Server AD
Devon	devon@RAMLAN.CA	Member	Windows Server AD
Ex Admin	exadmin@RAMLAN.CA	Member	Windows Server AD
Exchange Online-ApplicationAc	Exchange_Online-ApplicationAccount...	Member	Windows Server AD
extest_49b71e1812bd4	extest_49b71e1812bd4@RAMLAN.CA	Member	Windows Server AD
HealthMailbox-EX2019-001	HealthMailbox5e09af8b47344f63845a...	Member	Windows Server AD
HealthMailbox-EX2019-002	HealthMailboxc1536b1574bb40da839...	Member	Windows Server AD
HealthMailbox-EX2019-003	HealthMailbox74de48b2bb9542feb58...	Member	Windows Server AD
HealthMailbox-EX2019-004	HealthMailbox440e1d69a16148c4b5e...	Member	Windows Server AD
HealthMailbox-EX2019-005	HealthMailbox4e609791b3ff4f309c431...	Member	Windows Server AD
HealthMailbox-EX2019-006	HealthMailbox659d011f15934de3bad...	Member	Windows Server AD
HealthMailbox-EX2019-007	HealthMailbox92973a16b1274a63b54...	Member	Windows Server AD
HealthMailbox-EX2019-008	HealthMailbox6526cc99caf24a4a8dc2...	Member	Windows Server AD

Dashboard > RAMLAN INC >

Devices | All devices
RAMLAN INC - Azure Active Directory

×

All devices
Device settings
Diagnose and solve problems

Activity
Audit logs

Troubleshooting + Support
New support request

✓ Enable ⊘ Disable 🗑 Delete ⚙ Manage ↻ Refresh ≡ Columns | ♡ Got feedback?

Try out the new devices filtering improvements. Click to enable the preview. →

You can use the activity timestamp to efficiently manage stale devices in your environment. Learn more

Search
Search by name or device ID or object ID

Enabled
All

Activity
All

Name	Enabled	OS	Version	Join Type	Owner	MDM
OM	● Yes	Windows Server 201...	10.0 (17763)	Hybrid Azure AD joi...	N/A	None
ORCH	● Yes	Windows	10.0.17763.0	Hybrid Azure AD joi...	N/A	None
SFB	● Yes	Windows Server 201...	10.0 (17763)	Hybrid Azure AD joi...	N/A	None
TP1	● Yes	Windows	10.0.17763.0	Hybrid Azure AD joi...	N/A	None
SP2019	● Yes	Windows	10.0.17763.0	Hybrid Azure AD joi...	N/A	None
DPM	● Yes	Windows	10.0.17763.0	Hybrid Azure AD joi...	N/A	None
OFFICESERVER	● Yes	Windows Server 201...	10.0 (17763)	Hybrid Azure AD joi...	N/A	None
EX2019	● Yes	Windows Server 201...	10.0 (17763)	Hybrid Azure AD joi...	N/A	None
VMM	● Yes	Windows	10.0.17763.0	Hybrid Azure AD joi...	N/A	None
SM1	● Yes	Windows	10.0.17763.0	Hybrid Azure AD joi...	N/A	None
CB	● Yes	Windows Server 201...	10.0 (17763)	Hybrid Azure AD joi...	N/A	None

---

Dashboard >

Azure Active Directory Connect Health | Sync errors
RAMLAN INC

×

↓ Export   ✉ Notification Settings

Quick start

Azure Active Directory Connect (Sync)
Sync errors
Sync services

Active Directory Federation Services
AD FS services

Active Directory Domain Services
AD DS services

Configure
Settings
Role based access control (IAM)

TROUBLESHOOTING + SUPPORT
Troubleshoot
New support request

Sync Error by Type

Duplicate Attribute	Data Mismatch	Data Validation Failure	Large Attribute	Federated Domain C...
AadSyncService-ramlan.onmicr...	AadSyncService-ramlan.onmicr...	AadSyncService-ramlan.onmicr...	AadSyncService-ramlan.onmicr...	AadSyncService-ramlan.onmicr...
0	0	0	0	0

Existing Admin Role ...	Other			
AadSyncService-ramlan.onmicr...	AadSyncService-ramlan.onmicr...			
0	0			

On AzureADConnect, I did the following (**Hybrid & Device Options**)

Additional tasks

The required tasks for the scenario have been completed. Choose from the list below to perform additional tasks.

Privacy settings

View current configuration

Customize synchronization options

Configure device options ❓ ⬅

Refresh directory schema

Configure staging mode

Change user sign-in

Manage federation ❓

Troubleshoot

Previous   Next

Overview

With device management in Azure AD, you can ensure that users are accessing your resources from devices that meet your standards for security and compliance. Learn more

Hybrid Azure AD join enables devices in your Active Directory forest to register with Azure AD for access management. Computers in your organization will automatically discover Azure AD using a service connection point (SCP) object that is created in your Active Directory forest. Learn more

Device writeback is a prerequisite for enabling on-premises conditional access using AD FS and Windows Hello for Business. Device writeback synchronizes all devices registered in Azure AD back to on-premises. The devices are synchronized to a device container that is created in your Active Directory forest. Learn more

Device writeback requires the Active Directory schema version to be Windows Server 2012 R2 (level 69) or higher.

Previous   Next

Microsoft Azure Active Directory Connect

Device options

Select the device option to configure.

◉ Configure Hybrid Azure AD join

○ Configure device writeback

○ Disable device writeback

Sidebar navigation:
- Welcome
- Tasks
- Overview
- Connect to Azure AD
- **Device options**
- Hybrid Azure AD join
  - Device systems
  - SCP
- Configure

[Previous] [Next]

Microsoft Azure Active Directory Connect

Configuration complete

The task to configure Hybrid Azure AD join completed successfully.

You must now carry out additional steps that are required to enable your devices for Hybrid Azure AD join. Learn more

Sidebar navigation:
- Welcome
- Tasks
- Overview
- Connect to Azure AD
- Device options
- Hybrid Azure AD join
  - Device systems
  - SCP
- **Configure**

[Previous] [Exit]

https://docs.microsoft.com/en-us/azure/active-directory/devices/hybrid-azuread-join-managed-domains

I have to get Office 365 license for testing and, I am going with this that has one month trial FREE.

Mailbox Replication Proxy Service – Enable before hybrid configuration + make sure service is running

Now we have all the pre req taken care – we are ready for hybrid configuration. To be on the safe side, I did restart exchange server.

After download – run this application

I was getting below error. The fix – run through I E – not Chrome or Edge or Firefox

Got this obnoxious error after downloding the Office 365 – Exchange Hybrid Deployment Wizard using Chrome and tried to run.

This is just a fancy way of saying "You need to download and run this applet using internet explorer."

Application Install - Security Warning

Do you want to install this application?

Name:
Microsoft Office 365 Hybrid Configuration Wizard

From (Hover over the string below to see the full domain):
shcwreleaseprod.blob.core.windows.net

Publisher:
Microsoft Corporation

[Install] [Don't Install]

⚠ While applications from the Internet can be useful, they can potentially harm your computer. If you do not trust the source, do not install this software. More Information...

(92%) Installing Microsoft Office 365 Hybrid Configuration Wizard

Installing Microsoft Office 365 Hybrid Configuration Wizard

This may take several minutes. You can use your computer to do other tasks during the installation.

Name: **Microsoft Office 365 Hybrid Configuration Wizard**

From: **shcwreleaseprod.blob.core.windows.net**
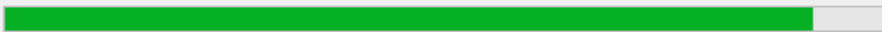
Downloading: 2.23 MB of 2.42 MB

[Cancel]

Office 365   Office 365 Hybrid Configuration

Hybrid Configuration Wizard

Office 365 Worldwide
EX2019 - RAMLAN\Administrator
17.0.4544.0
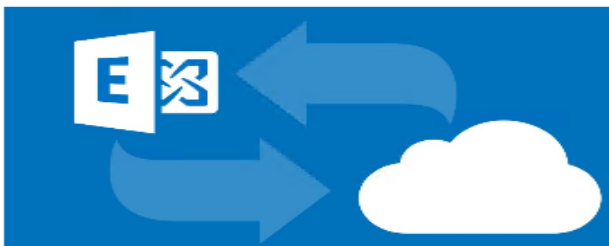
Running this wizard will configure coexistence between your on-premises environment and Exchange online.

What does this application do?

[back] [next] [cancel]

On-premises Exchange Server Organization

◉ Detect the optimal Exchange server

EX2019
Domain	RAMLAN.CA
Version	Version 15.2 (Build 659.4) *Enterprise Edition*
Roles	Mailbox
Site	RAMLAN.CA/Configuration/Sites/Default-First-Site-Name
Product ID	00433-60000-00000-AA523

○ Specify a server running Exchange 2010, 2013 or 2016

Exchange Hybrid setup requires a connection to an Exchange 2010, 2013 or 2016 server in your environment to perform management tasks. On Exchange 2010 or 2013 this must be a server running the Client Access Server role.

Client Access server:

EX2019.RAMLAN.CA

Office 365 Exchange Online

My Office 365 organization is hosted by:

Office 365 Worldwide ⌄

[back] [next] [cancel]

On-premises Exchange Account

Please provide your on-premises Exchange administrator account credentials.

RAMLAN\Administrator
Type	Current Windows Identity
Name	
Email	Administrator@ramlan.ca

[change...]

Office 365 Exchange Online Account

Please use your tenant administrator account credentials for Office 365 Worldwide.

administrator@ramlan.ca
Type	https://officeapps.live.com
Name	Ram Lan
Email	administrator@ramlan.ca

[change...]

[back] [next] [cancel]

Office 365 Worldwide - administrator@ramlan.ca
EX2019.RAMLAN.CA - RAMLAN\Administrator
Exchange Server 2019 15.2.659.4 RTM
17.0.4544.0

Gathering Configuration Information

● ● ● ● ● ●

Succeeded

Exchange

● ● ● ● ● ●

Succeeded

Office 365

[back] [next] [cancel]

Office 365 Worldwide - administrator@ramlan.ca
EX2019.RAMLAN.CA - RAMLAN\Administrator
Exchange Server 2019 15.2.659.4 RTM
RAMLAN.CA
Minimal Hybrid 17.0.4544.0

Hybrid Features

Select the Hybrid features you want to be part of your Hybrid Configuration.

learn more

○ **Minimal Hybrid Configuration (Recommended)**
Selecting this option will configure Exchange with the minimal settings needed so you can seamlessly move your mailboxes to Exchange Online.

◉ **Full Hybrid Configuration**
Selecting this option will configure Exchange with the full Hybrid feature set. This includes Free/busy sharing, enhanced mail flow, eDiscovery and other advanced features. This is typical for larger scale or long term coexistence scenarios.

┌─ Other Options ──┐
│   │
│ ☑ **Organization Configuration Transfer**   │
│ Selecting this option will perform a one-time transfer of organization objects from your on-premises environment to Exchange online. After the transfer, you will need to make changes in both locations to keep the objects in sync. │
│ learn more   │
│   │
└──┘

[back] [next] [cancel]

Office 365 Worldwide - administrator@ramlan.ca
EX2019.RAMLAN.CA - RAMLAN\Administrator
Exchange Server 2019 15.2.659.4 RTM
RAMLAN.CA
Full Hybrid 17.0.4544.0

Hybrid Topology

Please select a Hybrid Topology for your Exchange configuration.

learn more

- ● **Use Exchange Classic Hybrid Topology**
  - Provides full Exchange Hybrid experience
  - Requires Exchange Client Access and Transport connections to and from Internet

- ○ **Use Exchange Modern Hybrid Topology**
  - Installs the Hybrid Agent to provide Free/Busy and Mailbox Migrations
  - Requires Exchange Client Access connections to the Internet
  - Requires Exchange Transport service connections to and from the Internet

back   next   cancel

Office 365   _ ✕

Please provide your on-premises credentials used for Exchange Web Services and/or migration functionality.

Domain\username:

RAMLAN\Administrator

Password:

●●●●●●●●●

ok   cancel

On-premises Account for Migration

Office 365 Exchange Online requires the complete on-premises credential to create a migration endpoint.
learn more

Use the following credential when connecting to your on-premises Exchange Web Service.

RAMLAN\Administrator
Type   Windows Basic
Name
Email   Administrator@ramlan.ca

[change...]

[back] [next] [cancel]

Hybrid Agent Setup

✔ Download Hybrid Updater Agent

✔ Install Hybrid Updater Agent

✔ Download Hybrid Agent

✔ Install Hybrid Agent

✔ Register Hybrid Agent .... 2 seconds

✖ Validate Hybrid Agent for Exchange usage .... 307 seconds
   The connection to the server '633b95d6-2f73-44f0-a8a3-2e23f542b541.

Faced above error. I looked at the hybrid logs – here is the issue

2020.07.29 17:06:32.954 *ERROR* 10349 [Client=UX, Page=HybridConnectorInstall, Thread=16] The connection to the server '633b95d6-2f73-44f0-a8a3-2e23f542b541.resource.mailboxmigration.his.msappproxy.net' could not be completed., The call to 'https://633b95d6-2f73-44f0-a8a3-2e23f542b541.resource.mailboxmigration.his.msappproxy.net/EWS/mrsproxy.svc' failed. Error details: The HTTP request was forbidden with client authentication scheme 'Negotiate'. --> The remote server returned an error: (403) Forbidden., The HTTP request was forbidden with client authentication scheme 'Negotiate'., The remote server returned an error: (403) Forbidden.

Through Google – I reached this site who had similar issue with solution.

https://blog.misjageuskens.nl/2020/01/30/o365-hybrid-wizard-hybrid-agent-fails-to-validate/#comment-3332

Ran these commands in EMS

Get-ClientAccessServer | Add-AdPermission -AccessRights ExtendedRight -ExtendedRights "ms-exch-epi-token-serialization" -User "ramlan\Exchange Servers"

Get-ClientAccessServer | Add-ADPermission -AccessRights ExtendedRight -ExtendedRights "ms-Exch-EPI-Impersonation" -User "ramlan\Exchange Servers"

Get-MailboxServer | Add-AdPermission -AccessRights ExtendedRight -ExtendedRights "ms-exch-epi-token-serialization" -User "ramlan\Exchange Servers"

Get-MailboxServer | Add-AdPermission -AccessRights ExtendedRight -ExtendedRights "ms-Exch-EPI-Impersonation" -User "ramlan\Exchange Servers"

By the way after running above commands the permission are FALSE FALSE (Deny / Inherited) Here is screen shot (For User Administrator and same for Exchange Servers)

Now, I get a different error – 504 Gateway timeouts

Tried HCW again and this time it was successful.

File   Tools   Window   Help

Log Text

2020.07.29 20:44:50.760   10265 [Client=UX, Page=HybridConnectorInstall, Thread=1] START via Next
2020.07.29 20:44:50.785   10340 [Client=UX, Page=HybridConnectorInstall, Thread=33] START
2020.07.29 20:44:50.806   10439 [Client=UX, fn=.ctor, Thread=33] Downloading https://hybridconfiguration.blob.core.windows.net/connector/MSHybridAutoUpdater.msi
2020.07.29 20:44:51.176   10317 [Client=UX, fn=.ctor, Thread=36] C:\Users\Administrator.RAMLAN\AppData\Local\Temp\2\MSHybridAutoUpdater.msi already exists with same time date stamp and size. File Date=28-Jun-2019 5:53:43 ...
2020.07.29 20:44:51.197   10437 [Client=UX, Page=HybridConnectorInstall, Thread=33] DownloadState: ExistingContent
2020.07.29 20:44:51.222   10341 [Client=UX, Page=HybridConnectorInstall, Step=DownloadUpdaterAgent, Thread=33] FINISH Time=436.9ms Results=Succeeded
2020.07.29 20:44:51.240   10340 [Client=UX, Page=HybridConnectorInstall, Thread=33] START
2020.07.29 20:44:51.262   10341 [Client=UX, Page=HybridConnectorInstall, Step=InstallUpdaterAgent, Thread=33] FINISH Time=22.0ms Results=Succeeded
2020.07.29 20:44:51.280   10340 [Client=UX, Page=HybridConnectorInstall, Thread=33] START
2020.07.29 20:44:51.302   10439 [Client=UX, fn=.ctor, Thread=33] Downloading https://hybridconfiguration.blob.core.windows.net/connector/MSHybridService.msi
2020.07.29 20:44:51.718   10317 [Client=UX, fn=.ctor, Thread=36] C:\Users\Administrator.RAMLAN\AppData\Local\Temp\2\MSHybridService.msi already exists with same time date stamp and size. File Date=26-Jun-2019 6:22:36 PM -...
2020.07.29 20:44:51.740   10342 [Client=UX, Page=HybridConnectorInstall, Thread=33] DownloadState: ExistingContent
2020.07.29 20:44:51.759   10341 [Client=UX, Page=HybridConnectorInstall, Step=DownloadConnector, Thread=33] FINISH Time=478.1ms Results=Succeeded
2020.07.29 20:44:51.778   10340 [Client=UX, Page=HybridConnectorInstall, Thread=33] START
2020.07.29 20:44:51.797   10341 [Client=UX, Page=HybridConnectorInstall, Step=InstallConnector, Thread=33] FINISH Time=19.0ms Results=Succeeded
2020.07.29 20:44:51.818   10340 [Client=UX, Page=HybridConnectorInstall, Thread=33] START
2020.07.29 20:44:51.839   10389 [Client=UX, Page=HybridConnectorInstall, Thread=33] Connector is already published with the correct values.
2020.07.29 20:44:51.862   10341 [Client=UX, Page=HybridConnectorInstall, Step=ConfigOrgRoute, Thread=33] FINISH Time=43.4ms Results=Succeeded
2020.07.29 20:44:51.880   10340 [Client=UX, Page=HybridConnectorInstall, Thread=33] START
2020.07.29 20:44:51.888   10341 [Client=UX, Page=HybridConnectorInstall, Step=TestOrgRoute, Thread=33] FINISH Time=8.5ms Results=Succeeded

Date/Time: Component:
Thread: Source:

2020.07.29 20:44:51.888   10341 [Client=UX, Page=HybridConnectorInstall, Step=TestOrgRoute, Thread=33] FINISH Time=8.5ms Results=Succeeded

---

Office 365   Office 365 Hybrid Configuration   _ X

Office 365 Worldwide - administrator@ramlan.ca
EX2019.RAMLAN.CA - RAMLAN\Administrator
Exchange Server 2019 15.2.659.4 RTM
RAMLAN.CA
Full Hybrid 17.0.4544.0

Hybrid Configuration

How do you want to configure your on-premises organization for secure bi-directional mail transport with your Exchange Online organization?

learn more

◉ Configure my Client Access and Mailbox servers for secure mail transport (typical)

◯ Configure my Edge Transport servers for secure mail transport

Advanced...

[back]   [next]   [cancel]

Receive Connector Configuration

Choose one or more on-premises Exchange Servers to host receive connectors for secure mail transport with Exchange Online. If you are using Exchange 2013 these servers must have the Client Access Server role.

learn more

EX2019 ▲

EX2019
☑ Domain   RAMLAN.CA
    Version   Version 15.2 (Build 659.4)   *Enterprise Edition*
    Roles   Mailbox
    Site   RAMLAN.CA/Configuration/Sites/Default-First-Site-Name
    Product ID   00433-60000-00000-AA523

back   next   cancel

Send Connector Configuration

Choose one or more on-premises Exchange Servers to host send connectors for secure mail transport with Exchange Online. If you are using Exchange 2013 these servers must have the Mailbox Server role.

learn more

EX2019 ▲

EX2019
☑ Domain   RAMLAN.CA
    Version   Version 15.2 (Build 659.4)   *Enterprise Edition*
    Roles   Mailbox
    Site   RAMLAN.CA/Configuration/Sites/Default-First-Site-Name
    Product ID   00433-60000-00000-AA523

back   next   cancel

Transport Certificate

Choose a certificate to use with securing hybrid mail transport.

learn more

mail.ramlan.ca
Subject   CN=mail.ramlan.ca
Issuer
Valid
Thumbprint   4EAD257D731D09D37227B14588C108566EE4F57B

[back]   [next]   [cancel]

Organization FQDN

Enter a fully qualified domain name for your on-premises organization. This will configure the outbound mail connector to route mail from the Exchange Online Protection (EOP) service to your on-premises organization.

learn more

For example: RAMLAN.CA

[back]   [next]   [cancel]

Office 365 — Office 365 Hybrid Configuration

Ready for Update

Your Exchange hybrid configuration settings are now complete. Click Update to configure and enable the hybrid features in your Enterprise and Office 365 organizations.

This process may take several minutes to complete. Please don't close the window unless you want to cancel the process.

[back]   [update]   [cancel]

Office 365 — Office 365 Hybrid Configuration

Congratulations!

⚠ Your Exchange Hybrid Configuration has completed but a few items need to addressed or potentially configured manually. Please see the details below.

HCW8110 - *Encountered errors while running organization configuration transfer.*
learn more

F12 Diagnostic Tools

| Open Exchange Management Shell | Open Log File | Open Logging Folder |
| Open Exchange Online PowerShell | Create Support Package... | Open Process Folder |

[close]

Exchange On-premises PowerShell - ex2019.ramlan.ca

```
WARNING: The names of some imported commands from the module 'tmp_25nf31e3.1zb' include unapproved verbs that might
make them less discoverable. To find the commands with unapproved verbs, run the Import-Module command again with the
Verbose parameter. For a list of approved verbs, type Get-Verb.

ModuleType Version    Name                    ExportedCommands
---------- -------    ----                    ----------------
Script     1.0        tmp_25nf31e3.1zb        {Add-ADPermission, Add-AvailabilityAddressSpace, Add-Conte...
```

Exchange Online PowerShell - outlook.office365.com

```
WARNING: The names of some imported commands from the module 'tmp_ulkrb3rz.2c5' include unapproved verbs that might
make them less discoverable. To find the commands with unapproved verbs, run the Import-Module command again with the
Verbose parameter. For a list of approved verbs, type Get-Verb.

ModuleType Version    Name                    ExportedCommands
---------- -------    ----                    ----------------
Script     1.0        tmp_ulkrb3rz.2c5        {Add-AvailabilityAddressSpace, Add-DistributionGroupMember...
```

HCW8110

This is an exception that catches errors that are encountered when you run the Organization Configuration transfer feature. This error occurs if objects can't be copied over from on-premises to cloud.

To fix this error, check the logs to view the detailed reason for the error.

https://docs.microsoft.com/en-ca/exchange/troubleshoot/administration/hybrid-configuration-wizard-errors-organization-configuration-transfer

Unison ✅ Mar 19, 2020 at 6:51 PM
And now the fun begins :)

With HCW8110 - i would ignore this one and not worry about it.
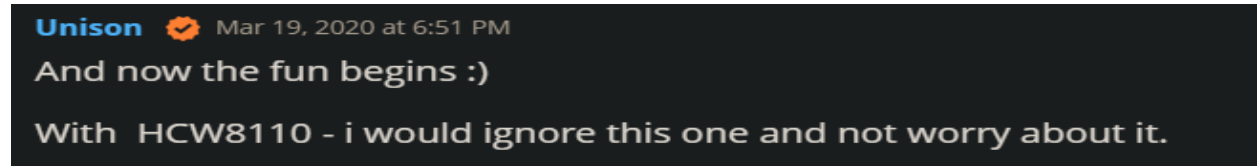
The only error reported in the log pertain to the following. **I guess HCW8110 can be ignored.**

2020.07.29 20:59:54.027 *ERROR* 10277 [Client=UX, Session=Tenant, Cmdlet=Get-DlpPolicy, Thread=31] FINISH Time=166.2ms Results=Command not recognized. Please verify you have the correct Management Role assigned to your account.

2020.07.29 21:03:00.516 WARNING 10086 [Client=UX, Provider=OnPremises, Thread=29] PowerShell Warning Record: Please check that the Autodiscover endpoint of "https://mail.ramlan.ca/autodiscover/autodiscover.svc" is correct and can be accessed externally. If it's incorrect or can't be accessed externally, use an existing Autodiscover endpoint that can be accessed externally for the configuration of the intra-organization connector.

I forgot to enable Federation Trust. Just Enabled from Organization ECP

recipients

permissions

compliance management

organization

protection

mail flow

mobile

public folders

servers

hybrid

sharing   add-ins   address lists

Federation Trust
Your federation trust is enabled but is pending verification of shared domains. You must select domains for sharing calendar free/busy information with external individuals and organizations. Learn more

| modify | remove |

The federation trust has been created successfully.

You've completed the operation.

Close

To confirm the Hybrid Configuration is complete – we can test the following

EMS command – Get-HybridConfiguration

Get-EmailAddressPolicy | FL Name,EnabledEmailAddressTemplates

Get-AcceptedDomain

Get-OrganizationalRelationship | Fl

```
[PS] C:\Windows\system32>Get-OrganizationRelationship | Fl


RunspaceId              : 63377da4-8e9c-4a68-b6dc-fc1a6c01a267
DomainNames             : {ramlan.mail.onmicrosoft.com}
FreeBusyAccessEnabled   : True
FreeBusyAccessLevel     : LimitedDetails
FreeBusyAccessScope     :
MailboxMoveEnabled      : True
MailboxMoveDirection    : None
DeliveryReportEnabled   : True
MailTipsAccessEnabled   : True
MailTipsAccessLevel     : All
MailTipsAccessScope     :
PhotosEnabled           : True
TargetApplicationUri    :
TargetSharingEpr        :
TargetOwaURL            :
TargetAutodiscoverEpr   :
OrganizationContact     :
Enabled                 : True
ArchiveAccessEnabled    : True
AdminDisplayName        :
ExchangeVersion         : 0.10 (14.0.100.0)
Name                    : On-premises to O365 - 692fd8a5-c326-4963-b948-7a981393c6e2
DistinguishedName       : CN=On-premises to O365 - 692fd8a5-c326-4963-b948-7a981393c6e2,CN=Federation,CN=RAMLAN
                          INC,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=RAMLAN,DC=CA
Identity                : On-premises to O365 - 692fd8a5-c326-4963-b948-7a981393c6e2
Guid                    : 0ddbd0f2-5343-439c-aca3-4955ca2e5597
ObjectCategory          : RAMLAN.CA/Configuration/Schema/ms-Exch-Fed-Sharing-Relationship
ObjectClass             : {top, msExchFedSharingRelationship}
WhenChanged             : 29-Jul-2020 5:02:50 PM
WhenCreated             : 29-Jul-2020 5:02:49 PM
WhenChangedUTC          : 29-Jul-2020 9:02:50 PM
WhenCreatedUTC          : 29-Jul-2020 9:02:49 PM
OrganizationId          :
Id                      :
OriginatingServer       :
IsValid                 : True
ObjectState             : Unchanged
```

Send Connectors

rules   delivery reports   accepted domains   email address policies   receive connectors   **send connectors**

+ ✎ 🗑 ⟳ ···

NAME	STATUS
DNS Exit	Enabled
Outbound to Office 365	Enabled

Receive Connectors – Default

Select server: EX2019.RAMLAN.CA

+ ✎ 🗑 ⟳ ···

Default EX2019

NAME
Client Frontend EX2019
Client Proxy EX2019
Default EX2019
Default Frontend EX2019
Outbound Proxy Frontend EX2019

general
▸ security
scoping

Specify the security mechanism or mechanisms for incoming connections.

☑ Transport Layer Security (TLS)
  ☐ Enable domain security (mutual Auth TLS)
☑ Basic authentication
  ☑ Offer basic authentication only after starting TLS
☑ Integrated Windows authentication
☑ Exchange Server authentication
☐ Externally secured (for example, with IPsec)

Permission groups:
Specify who is allowed to connect to this receive connector.

☑ Exchange servers
☑ Legacy Exchange servers
☐ Partners
☑ Exchange users
☐ Anonymous users

[Save] [Cancel]

```
========================================================================================================
Send Connector
--------------------------------------------------------------------------------------------------------
Name              | Equals | Actual                               | Expected
--------------------------------------------------------------------------------------------------------
Name              | True  | Outbound to Office 365                | Outbound to Office 365
AddressSpaces     | True  | smtp:ramlan.mail.onmicrosoft.com;1    | smtp:ramlan.mail.onmicrosoft.com;1
CloudServicesMailEnabled | True | True                            | True
DNSRoutingEnabled | True  | True                                  | True
ErrorPolicies     | True  | Default                               | Default
Fqdn              | True  | mail.ramlan.ca                        | mail.ramlan.ca
RequireTLS        | True  | True                                  | True
SmartHosts        | True  | 0                                     | 0
SourceTransportServers | True | EX2019                           | EX2019
TLSAuthLevel      | True  | DomainValidation                      | DomainValidation
TLSCertificateName    | True | <I>CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US<S>CN=mail.ramlan.ca | <I>CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US<S>CN=mail.ramlan.ca
TLSDomain         | True  | mail.protection.outlook.com           | mail.protection.outlook.com


Receive Connector
--------------------------------------------------------------------------------------------------------
Name              | Equals | Actual                               | Expected
--------------------------------------------------------------------------------------------------------
Name              | True  | Default Frontend EX2019               | Default Frontend EX2019
AuthMechanism     | True  | Tls, Integrated, BasicAuth, BasicAuthRequireTLS, ExchangeServer | Tls, Integrated, BasicAuth, BasicAuthRequireTLS, ExchangeServer
Bindings          | True  | [::]:25, 0.0.0.0:25                   | [::]:25, 0.0.0.0:25
Fqdn              | True  | EX2019.RAMLAN.CA                      | EX2019.RAMLAN.CA
PermissionGroups  | True  | AnonymousUsers, ExchangeServers, ExchangeLegacyServers | AnonymousUsers, ExchangeServers, ExchangeLegacyServers
RequireTLS        | True  | False                                 | False
Server            | True  | EX2019                                | EX2019
TLSDomainCapabilities | True | Microsoft.Exchange.Data.SmtpReceiveDomainCapabilities[] | Microsoft.Exchange.Data.SmtpReceiveDomainCapabilities[]
TLSCertificateName    | True | <I>CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US<S>CN=mail.ramlan.ca | <I>CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US<S>CN=mail.ramlan.ca
```

Get-RemoteDomain

You can use the Exchange Management Shell on an Exchange Server to check for users with the Email Address Policy disabled using the following cmdlet:

Get-Mailbox -ResultSize Unlimited | Where {$_.EmailAddressPolicyEnabled -eq $False}

For me in the lab, I had one user that did not have the correct smtp address

This is what you should see for all users (example Administrator) - See what we have for user Ram Lan

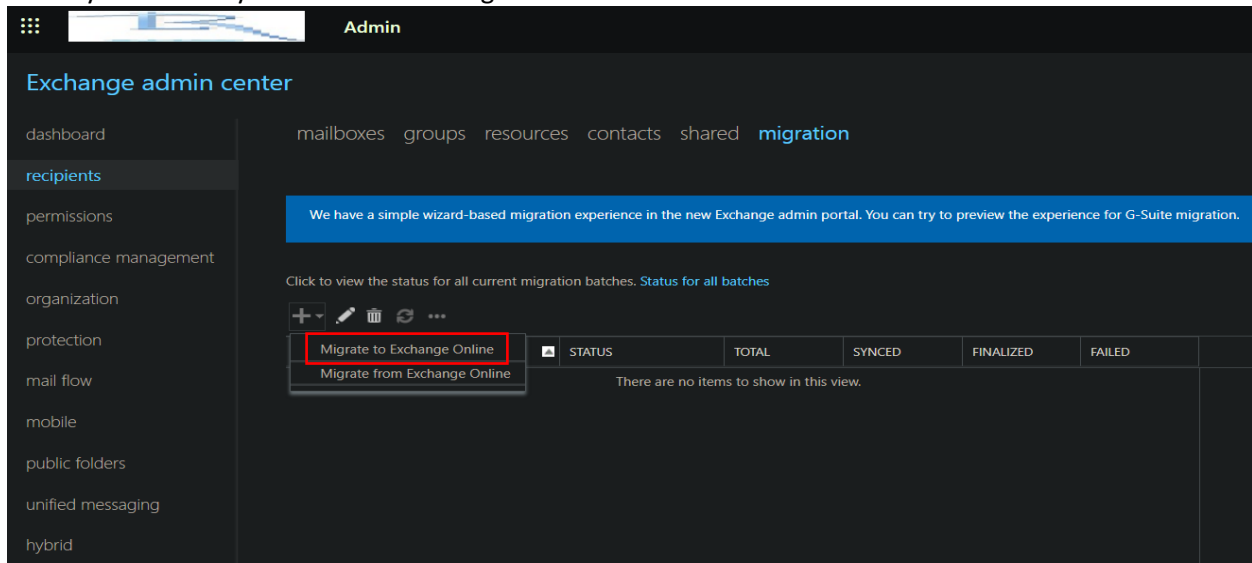I added another smtp with the following

I also logged into Office365 Exchange Admin Center. Here it is
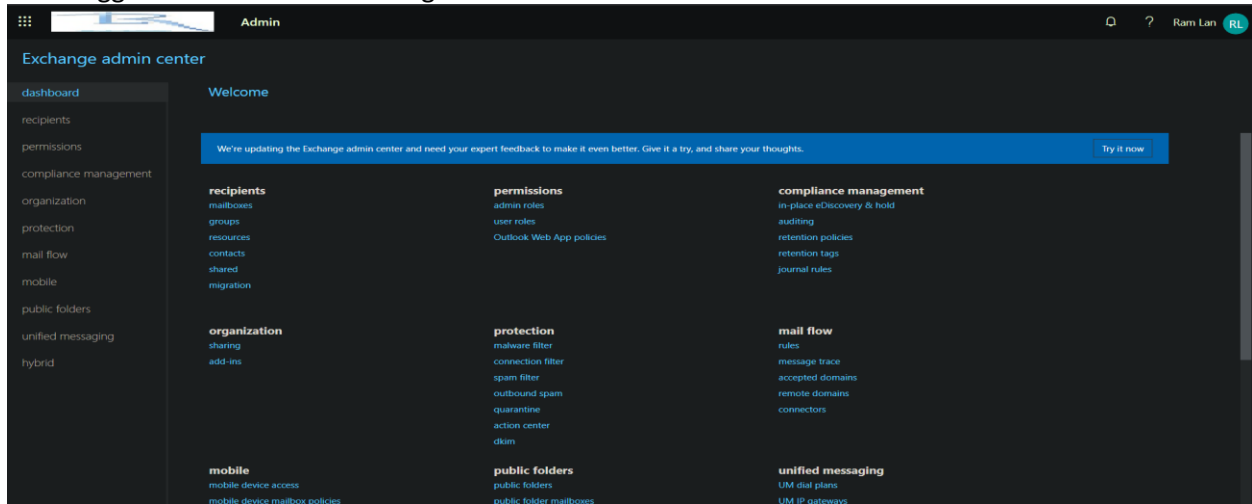
As you see the mailbox is EMPTY. We have not migrated any mailbox from on premise.
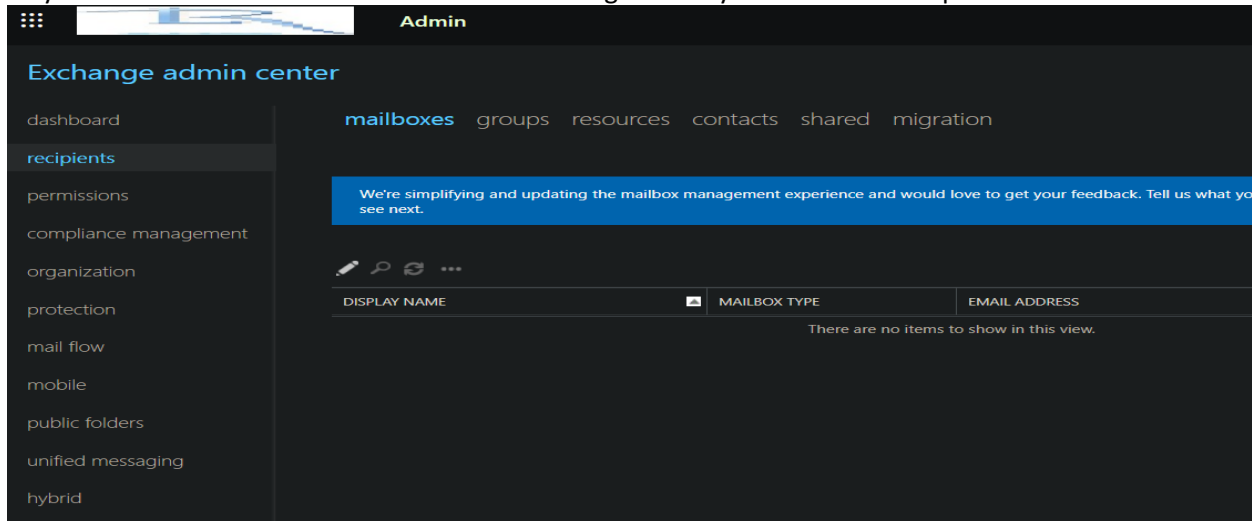

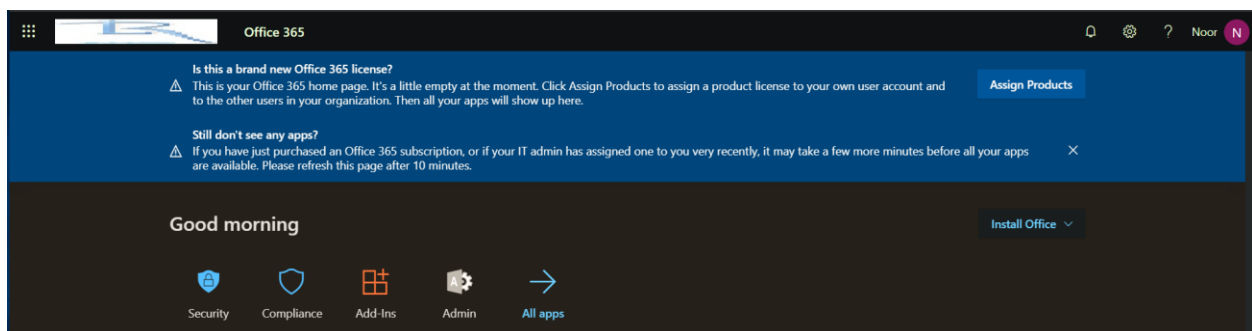When you are ready to start mailbox migration – You will see this menu

Based on all the above, it looks like our Hybrid migration to Exchange Online Office 365 is complete. I will start mailbox migration during the weekend after purchasing one or two O365 license.

Login to ECP on your Exchange 2019 Server and select Office 365 – the link might take you to Office 365 pricing page and not Office 365 Admin Center. The solution is simple

Click – Hybrid – Modify – Sign in Office 365 and you will see both Exchange Admin Center and Office 365 Admin Center on the same page like this.. I wish the theme was DARK and not WHITE.
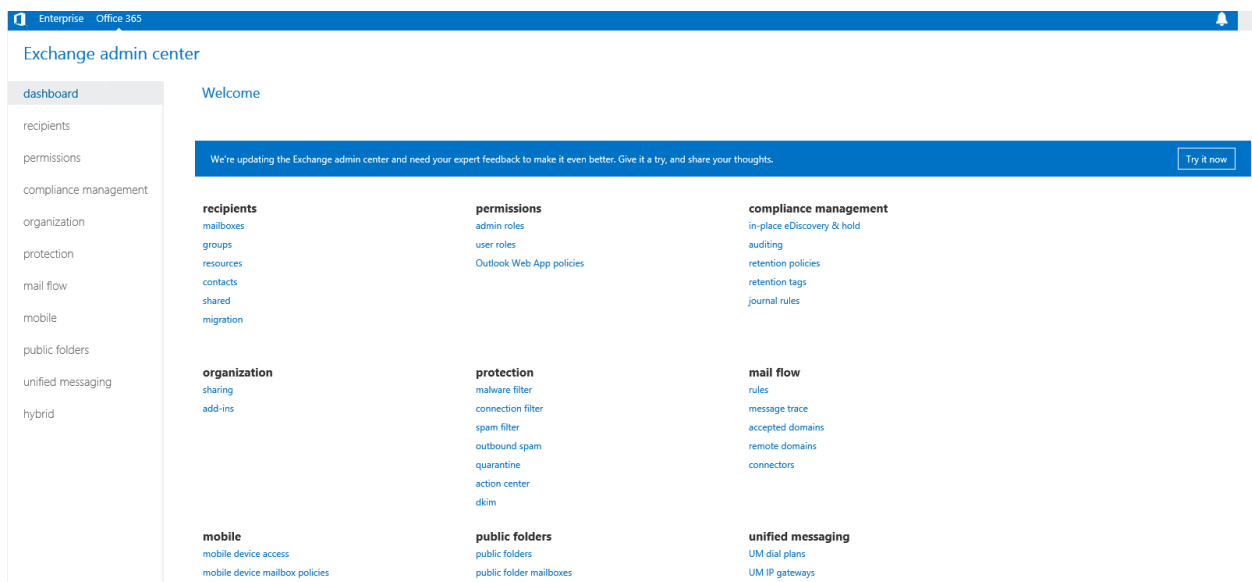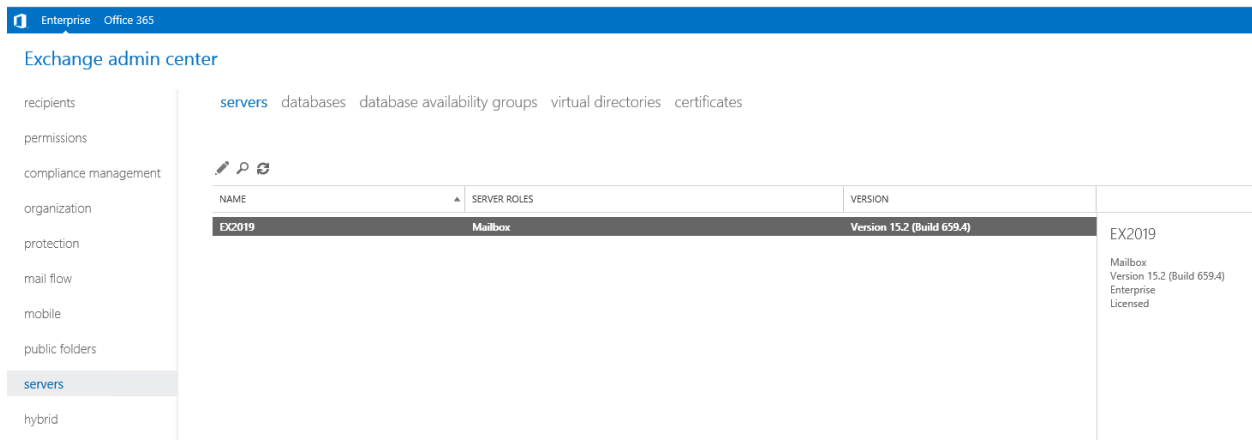
I am able to login to Office 365 as regular user and AD password works - https://portal.office.com/

Thanks

Ram Lan
30th July 2020