Office 365 Configuration Document

**AFG-EIT-IO-MN-133-v1.0**

|  |  |  |
| --- | --- | --- |
| Author:  Abu Shaeed | Business Unit:  Enterprise IT | Classification:  Internal |
| Reviewer:  Saleh Abubakar | Business Function:  IO | Status:  Published |
| Approver:  Saleh Abubakar | Publish Date:  25nd September 2018 | Version: 1.0 |

TABLE OF CONTENTS

[1 Design 2](#_Toc5545090)

[2 Hybrid Configuration 3](#_Toc5545091)

[2.1 Hybrid Organization Relationship Configuration 3](#_Toc5545092)

[2.2 Organization Sharing Policy 3](#_Toc5545093)

[3 Connector Configuration for Mail Routing 4](#_Toc5545094)

[4 Retention Policy 5](#_Toc5545095)

[5 AAD Connect 6](#_Toc5545096)

[5.1 Staging mode 7](#_Toc5545097)

[6 Permissions 11](#_Toc5545098)

[7 Adding New domain in Office 365 12](#_Toc5545099)

[8 OneDrive Configuration 18](#_Toc5545100)

[9 Remove access permissions on One Drive data of separated users. 21](#_Toc5545101)

[10 International Locations 22](#_Toc5545102)

[11 Email relay for applications 24](#_Toc5545103)

[12 Reclaim D drive space consumed due to Mail.que files- 30](#_Toc5545105)

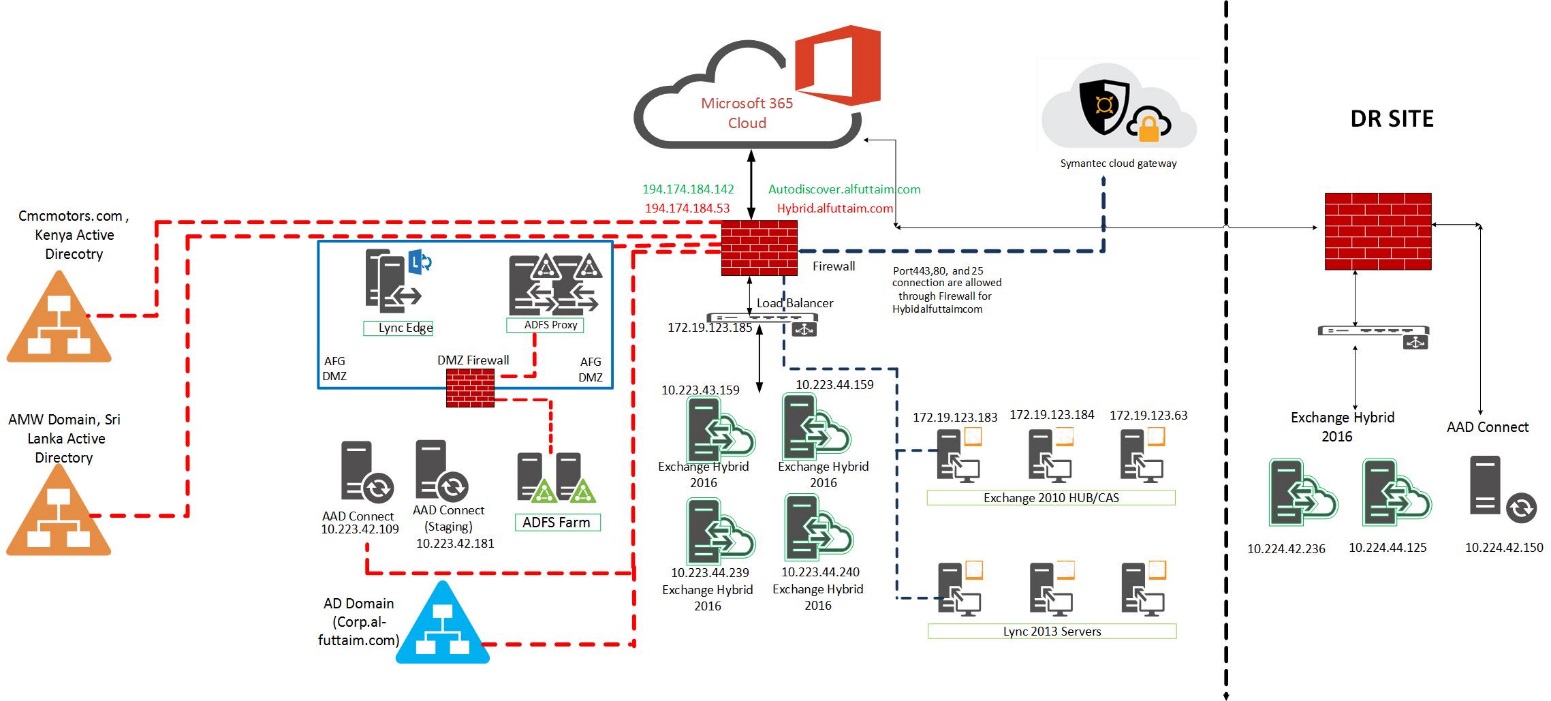
[13 Tasks Yet to Complete 31](#_Toc5545106)

[14 Offline Employees (MYALFUTTAIM.COM) 31](#_Toc5545107)

[15 Version Control 32](#_Toc5545108)

[Table 4‑1 Version Control and History 32](#_Toc5545109)

# Design



**Office365 tenant domain:** XXXXXXXXXXXXXXXXXx

**Routing domain:** XXXXXXXXXXXXXXXXx

Al-Futtaim Infrastructure and Office365 is configured in Hybrid mode and Organization relationship has been setup.

Hybrid Organization relationship is configured with the URL **XXXXXXXXXXXXX** (Custom URL).

The IP address for this URL is configured to IP **XXXXXXXXXXXXX,** this is load balanced to all the 4 Hybrid 2016 Exchange servers**: -**

**XXXXXXXXXXXX**

**XXXXXXXXX**

**XXXXXXXXXXXx**

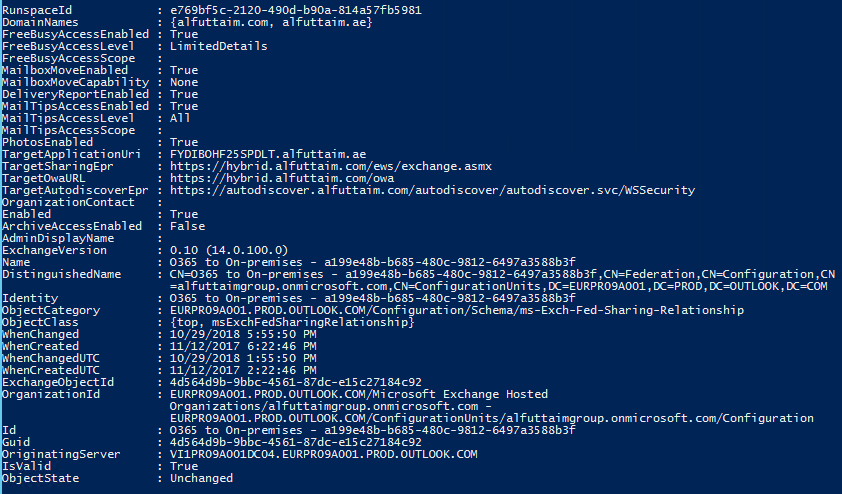
**XXXXXXXXXXXXXXXX**

Port numbe**r 443, 80, 25** and **3478 (UDP)** are allowed in the Firewallfor HTTPS, HTTP, SMTP and STUN protocols respectively.

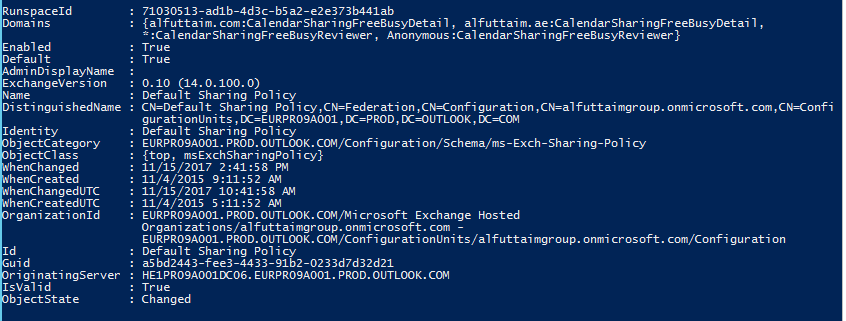
# Hybrid Configuration

A hybrid deployment provides the seamless look and feel of a single Exchange organization between an on-premises Exchange organization and Exchange Online in Microsoft Office 365. In addition, a hybrid deployment can serve as an intermediate step to moving completely to an Exchange Online organization.

## Hybrid Organization Relationship Configuration



## Organization Sharing Policy



The sharing policy for domains from Office 365 is set to the following:

***Alfuttaim.com*** - View free busy with subject and details

***Alfuttaim.ae*** - View free busy with subject and details

**\*** - View free busy

**Anonymous** - View free busy

# Connector Configuration for Mail Routing

We have the following connectors in Office 365:

1. **Inbound from XXXXXXXXXXXXXXXXXXXXX (Default)**

This connector is configured to accept emails from IP address **XXXXXXXXXXXXXXxxxx** and if the domain is an accepted domain in Office 365.

1. **Outbound to XXXXXXXXXXXXXXXXXXXXXXx (Default)**

This connector is configured to route the emails to XXXXXXXXXXXXXX over TLS for recipient domains: XXXXXXXXXXXXXXXX

1. **Outbound to Symantec for AFG**

This connector is configured to accept messages only if we have a Rule to redirect messages to this connector. The emails will be routed to **XXXXXXXXXXXXXXXXXx** (Symantec Gateway).

We have a rule created in Office 365:

1. **Outbound to Symantec for alfuttaim.com users**

This rule is in place to route all the emails from domain 'XXXXXXX’ to Symantec Gateway, the message is routed using **Outbound to Symantec for AFG** connector, except if the recipient domain is one of the authoritative domain in Alfuttaim on-premise or the email is submitted from **Outsize the organization**.

All the 4 Hybrid servers are the Submission server for Outbound to O365:

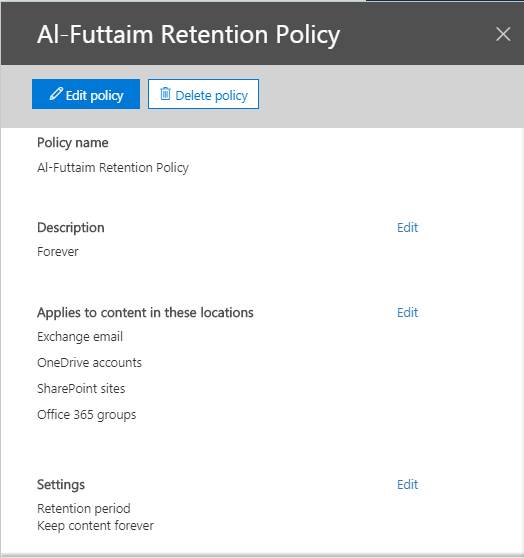
XXXXXXXXX, XXXXXXXX, XXXXXXXXXXXXX and XXXXXXXXXXXXXXXx

AutodiscoverURI: XXXXXXXXXXXXXXXXx

# **Retention Policy**

We have retention policy **Al-Futtaim Retention Policy** created and applied for below applications to retain all the items forever: -

1. Exchange email
2. OneDrive accounts
3. SharePoint sites
4. Office 365 groups



**Note:** This policy will be applied by default for all the E3 licensed users but for E1 licensed users it will be applied only if they have “***Exchange Online Archiving for Exchange Online”*** *license* assigned.

# AAD Connect

AAD connect server is responsible to sync the changes made in the on-premise AD to Office365. We have specific set of OU’s selected in the AAD configuration and changes made to the objects in those OU’s will only get synced.

Below are the OU’s which are currently enabled to sync:

XXXXXXXXXXXXXXX

We have 3 Servers for AAD Connect including 2 in primary site and 1 in DR site. Server details below:

XXXXXXXXXXX - Primary server

XXXXXXXXXXX - **Staging** server

XXXXXXXXXXX - Staging server in the DR site

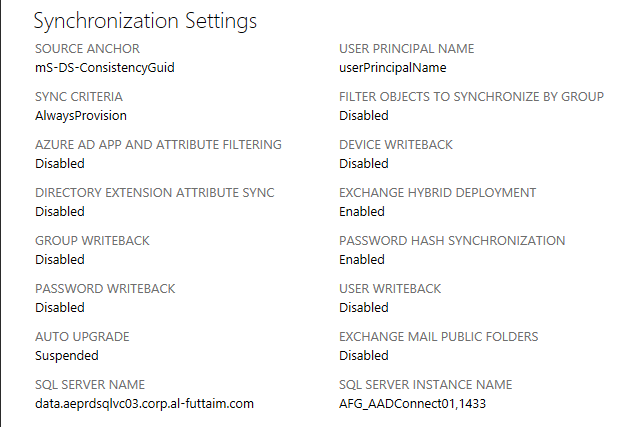
Below two connectors are created and configured under AAD:

1. XXXXXXx 🡪 Responsible to sync AD changes for Al Futtaim users.
2. XXXXXXx 🡪 Responsible to sync AD changes for cmcmotors.com domain, Kenya.

**Service accounts: -**

|  |  |
| --- | --- |
| Directory | Account |
| XXXXXXXXXXXXx | XXXXXXXXXXXXXXX\XXXXXXXXXx |
| XXXXXXXXXXXXXXXx | XXXXXXXXXXXXXX\XXXXXXXXX |

**Synchronization Settings for AAD connect as below:**



## Staging mode

Staging mode can be used for:

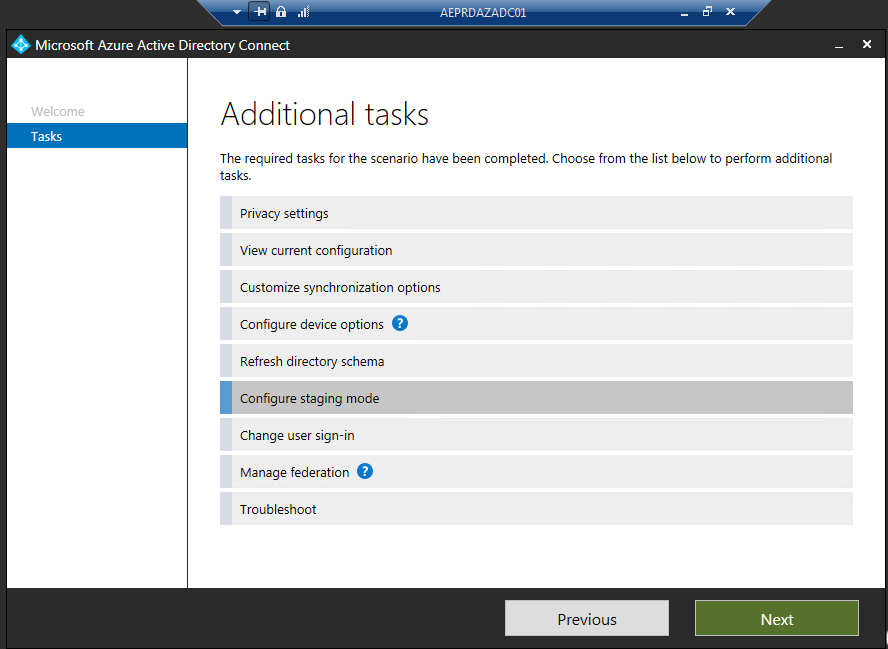
* High availability
* Introduce a new server and decommission the old.

Enabling staging mode on the AD connect makes the server active for import and synchronization, but it does not run any exports. A server in staging mode is not running password sync or password writeback, even if its selected during installation. When you disable staging mode, the server starts exporting, enables password sync, and enables password writeback.

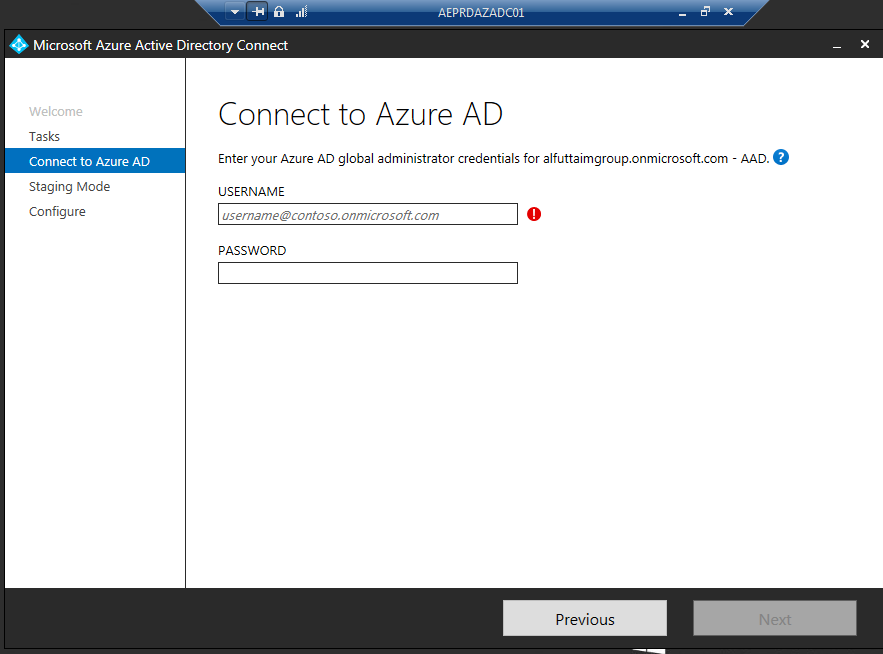
A server in staging mode continues to receive changes from Active Directory and Azure AD. It always has a copy of the latest changes and can very fast take over the responsibilities of another server. If you make configuration changes to your primary server, it is your responsibility to make the same changes to the server in staging mode.

**Steps to Switch active server: -**

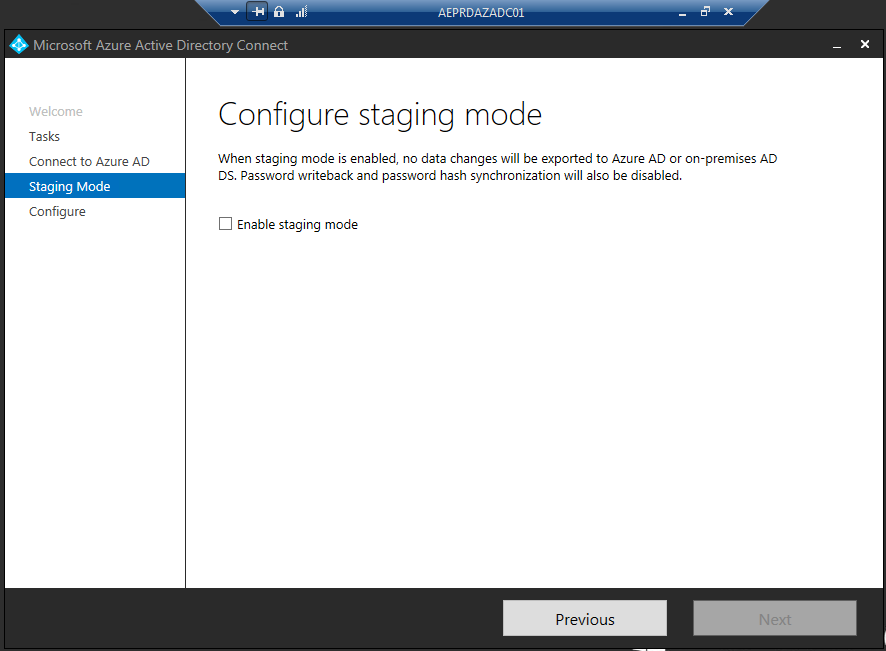
1. On the currently active server “XXXXXXXXXX”, launch Azure AD Connect console and click **Configure**.
2. Select **Configure staging mode** option and click Next



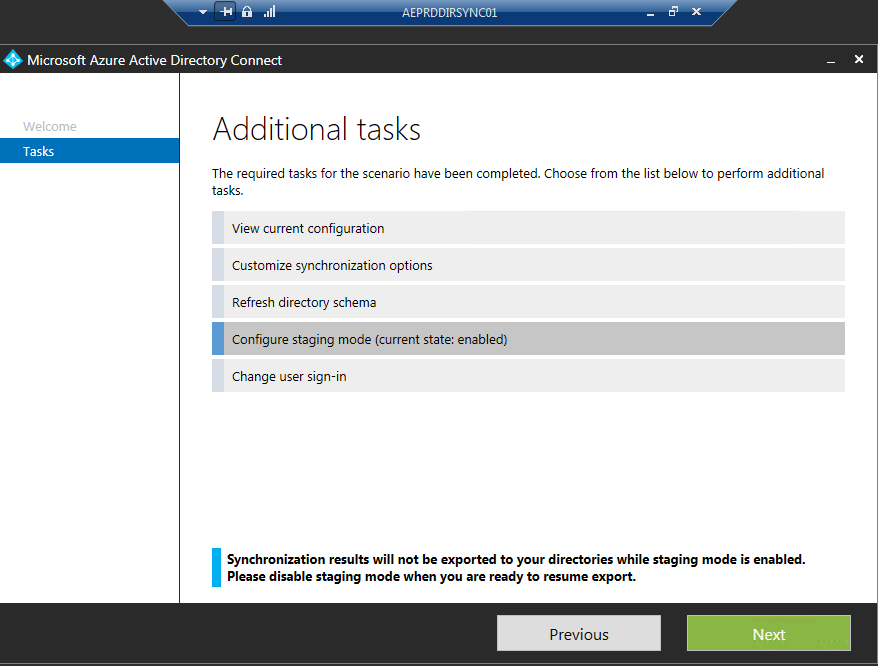
1. Enter the Global admin credentials and click **Next**



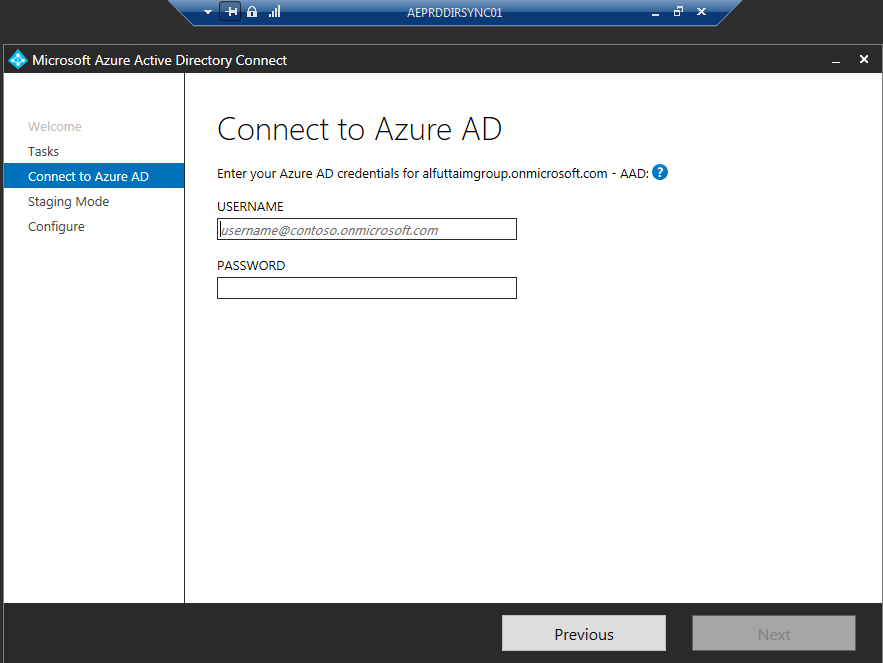
1. Credential will be verified, and we will get the page to configure staging mode. Select the check box “**Enable staging mode**” and click **Next**



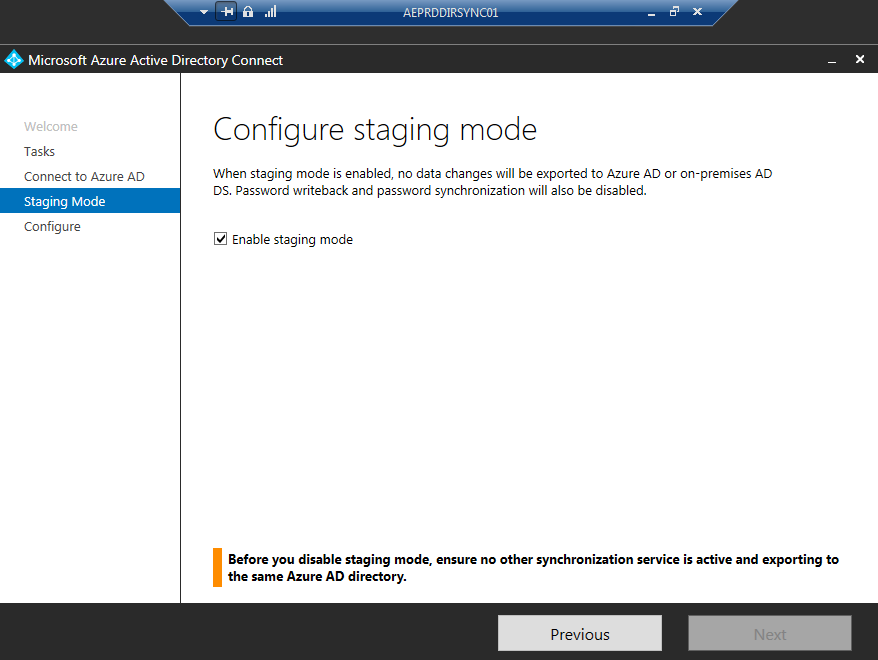
1. The above steps will set the currently primary server into Staging mode. Now, login to the server already in staging mode “**XXXXXXXX**” and launch Azure AD Connect console and click **Configure**.
2. Select “Configure staging mode (current state: enabled) and Select **Next**



1. Enter the Global admin credentials and click Next



1. Credential will be verified, and we will get the page to configure staging mode. Uncheck the check box “Enable staging mode” and click Next



This will disable staging mode on this server and it will become the primary server. Going forward, this server will import and synchronize and will also run exports to Azure AD.

# Permissions

Users when on Exchange On-premise have FullAccess, SendAs or SendOnBehalf permission on the user or common mailboxes for business requirement. If any mailbox having any type of permission on any other mailbox is getting migrated to Office365, we need to grant the permission again post the migration is completed.

Below are the commands to grant the permissions as required:

**FullAccess:**

1. Office365 user needs FullAccess to the On-prem mailbox, in this case run the below command from the on-prem Exchange Management Shell:

*Add-MailboxPermission -Identity* ***User A*** *-User* ***User B*** *-AccessRights FullAccess -InheritanceType All -AutoMapping $false*

This example assigns the user **User B** Full Access permission to **User A’s** mailbox and without Automapping the profile in Outlook.

1. Exchange On-prem user needs FullAccess to the Office365 mailbox, in this case run the below command from the Office365 PowerShell:

*Add-MailboxPermission -Identity* ***User A*** *-User* ***User B*** *-AccessRights FullAccess -InheritanceType All -AutoMapping $false*

This example assigns the user **User B** Full Access permission to **User A’s** mailbox and without Automapping the profile in Outlook

**SendAs:**

1. Office365 user needs SendAs permission on the On-prem mailbox, in this case run the below command from the Office365 PowerShell:

*Add-RecipientPermission -Identity* ***On-Prem User*** *-AccessRights SendAs -Trustee* ***MigratedUser***

The above example assigns the **MigratedUser** SendAs permission on **On-prem User**

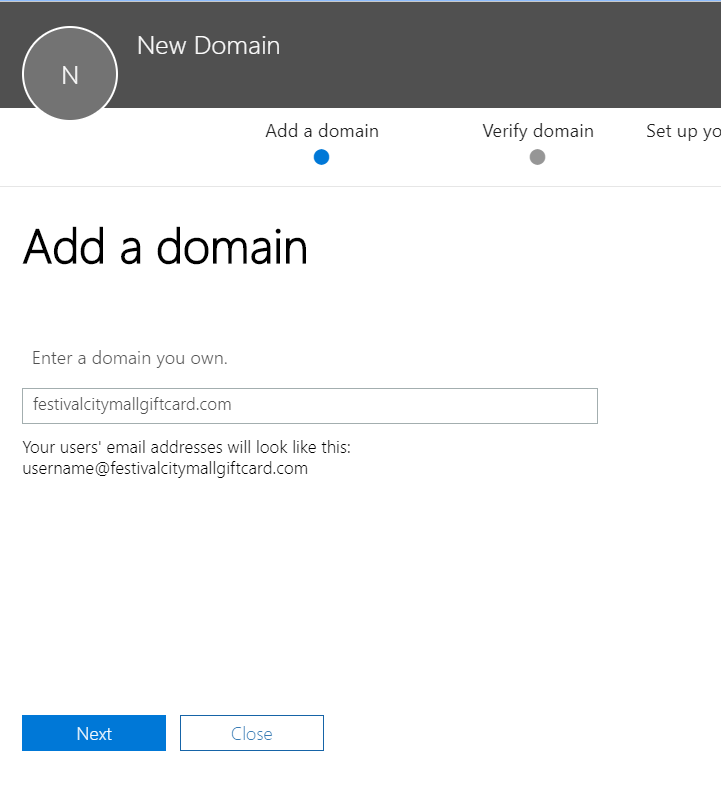
1. Exchange On-prem user needs SendAs permission on the Office365 mailbox, in this case run the below command from the Exchange Management Shell:

*Add-ADPermission -Identity* ***migrated use****r -AccessRights SendAs -user* ***On-prem user***

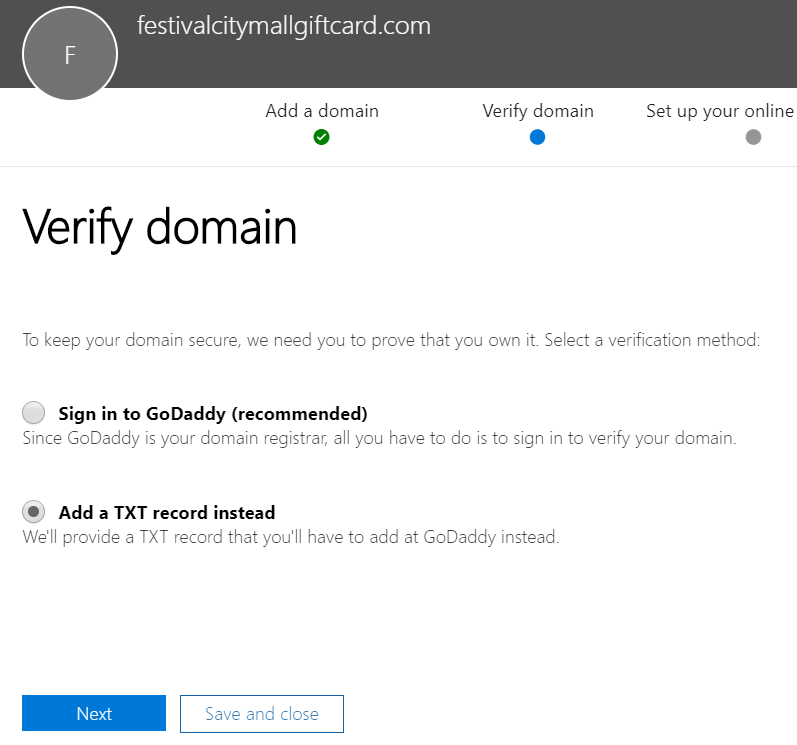
The above example assigns the **On-prem user** SendAs permission on **migrated user**

# Adding New domain in Office 365

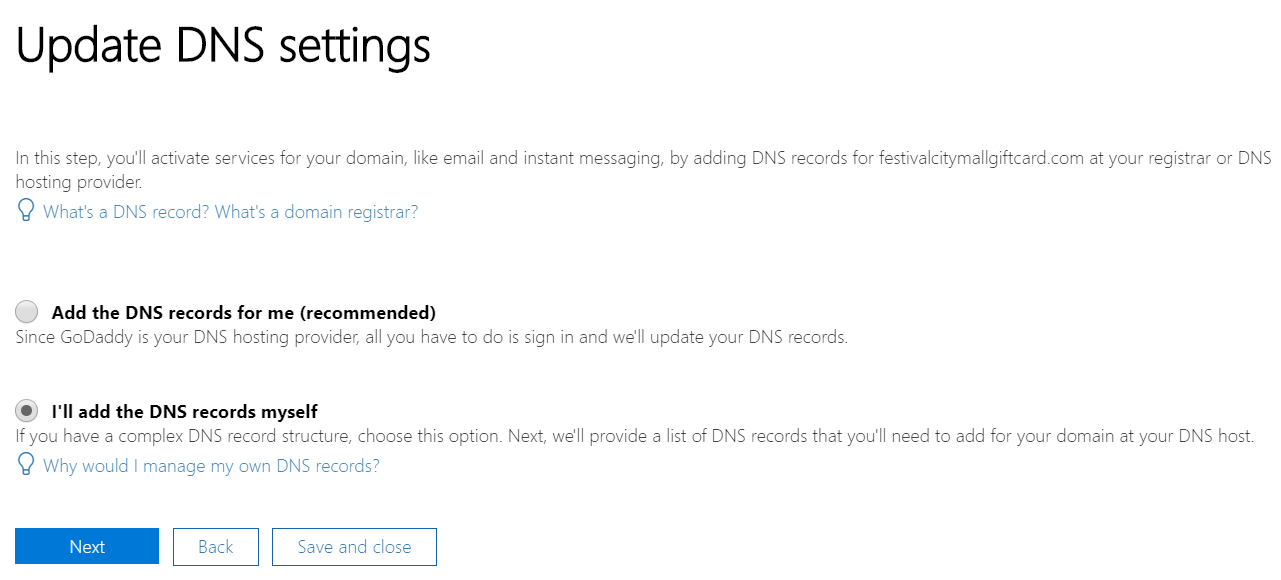
1. Open the Office 365 admin center <https://admin.microsoft.com>
2. In the left pane select Setup and click Domains
3. Under the Domains click Add Domain button enter the Domain name you wish to Add and click Next.



1. In the Verify domain section select Add TXT record and click Next.



1. Copy the TXT value and add a new TXT record in DNS provided by your domain registrar. (This is to prove you own this domain).
2. Once the TXT record is added in the public DNs, click on Verify button and on the next tab select “**I’ll add the DNS records myself.**”



1. Choose the online services Exchange and Skype for Business and click Next.
2. At the end click on Skip the DNS Records verification step and the Finish the setup.
3. Now the domain is verified on Office 365 and status will show “**Possible service issues**” as we have selected the option as **“I'll manage my own DNS records”**

Once the domain is added and verified in Office365, it will now sync objects from AD with the associated domain and for the email flow routing to work the domain needs to be added in the below connector and transport rule-

**Connector Name:** XXXXXXXXXXXXXXXXXXxxxxxxx

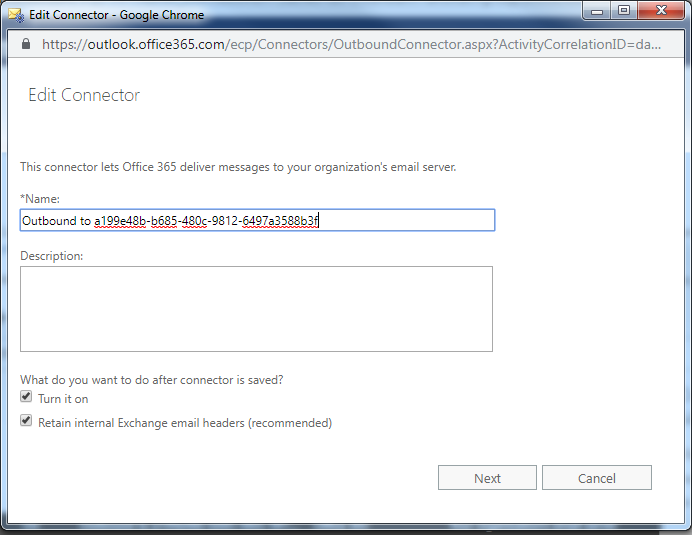
**Transport Rule:** XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXxx

**Steps to add domain in the connector –**

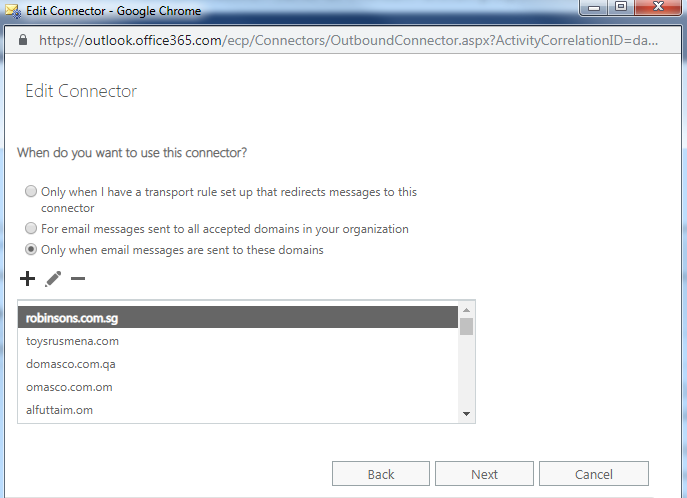
Open the Exchange online admin center –

Click mail flow –

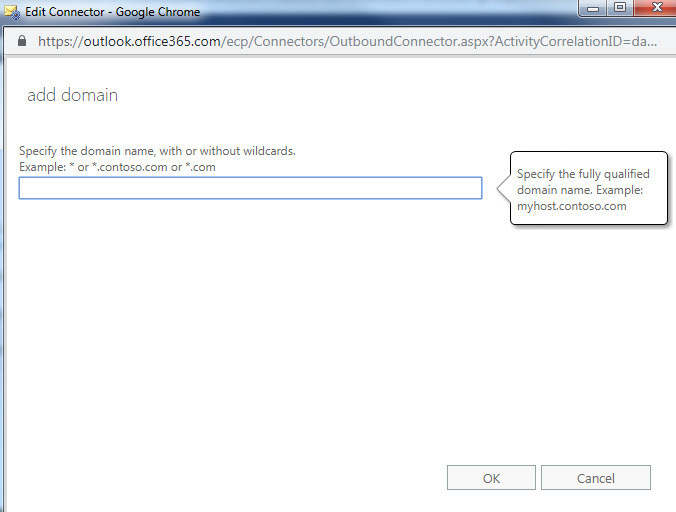
Click connectors and select **XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXxxx**



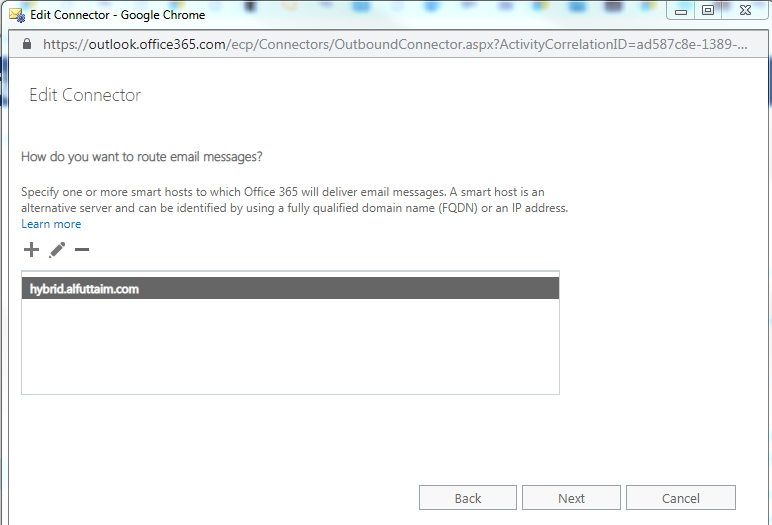
Click Next and option **“Only when email messages are sent to these domains”** should be selected, Click **+**



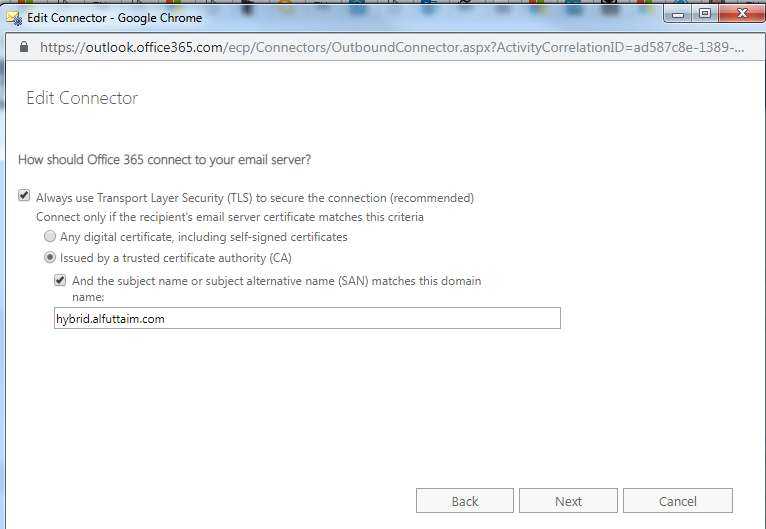
Specify the fully qualified domain and select **OK**



Once the domain is added to the list, Click **Next**



NO changes need to be done under TLS configuration and click **Next**



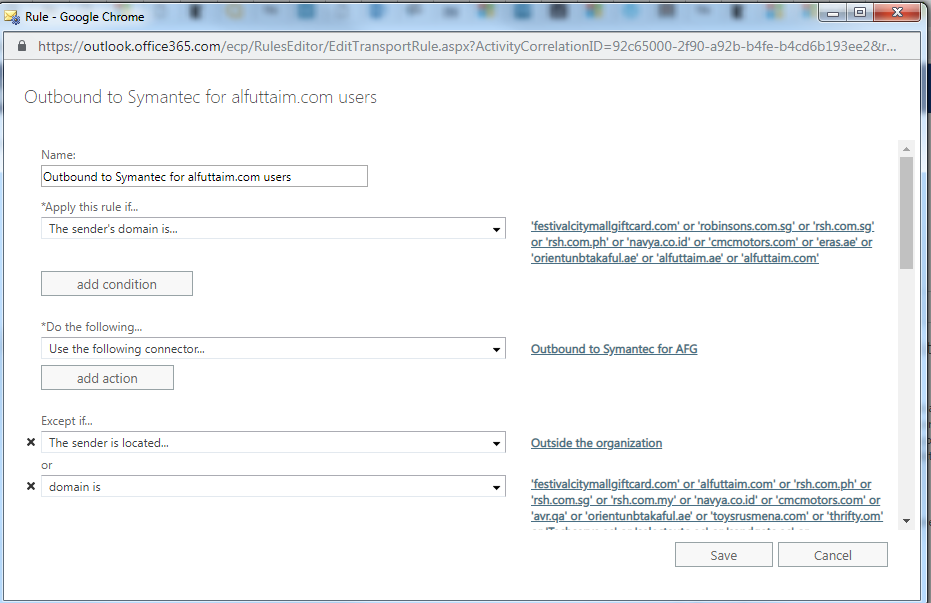
Under **“Confirm your settings”** check the configuration and click **Next**. Validation will be performed, and Domain will be part of the connector.

**Steps to add domain in the rule –**

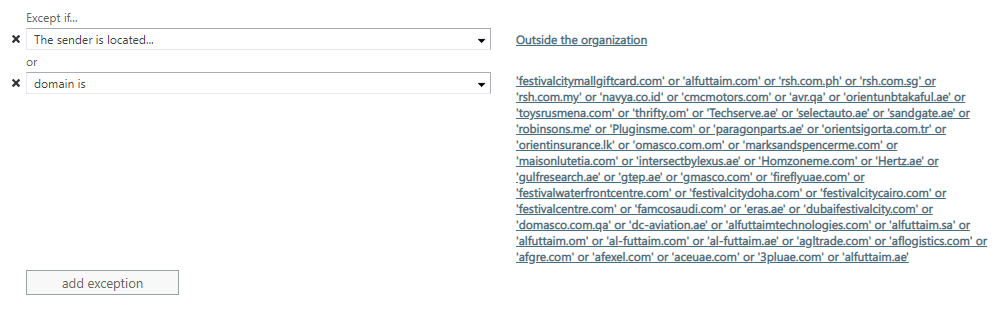
Open the Exchange online admin center –

Click mail flow –

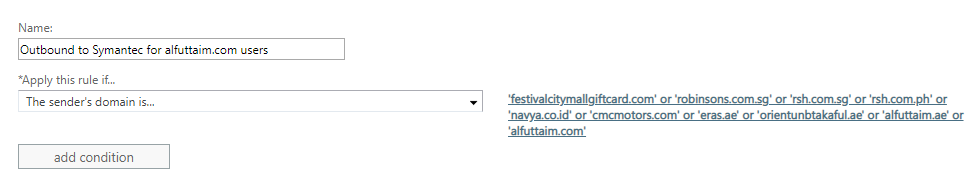
Click rules and select **Outbound to Symantec for alfuttaim.com users**



Add the newly added and verified domain under the exception category as shown below –



If the domain that we have just added and verified will be used for sending emails as primary SMTP address, then add it under **“The sender’s domain is…”** as well -

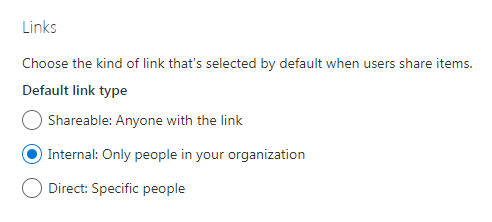


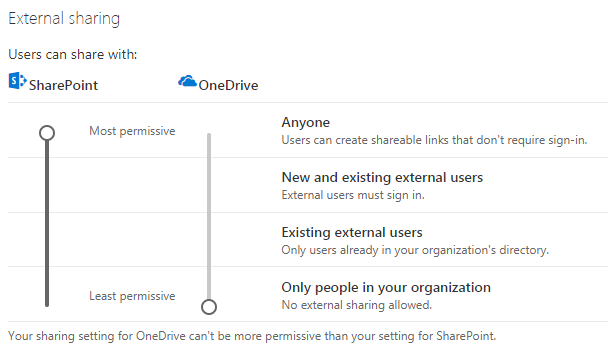
No other configuration/settings need to be altered for this rule.

# OneDrive Configuration

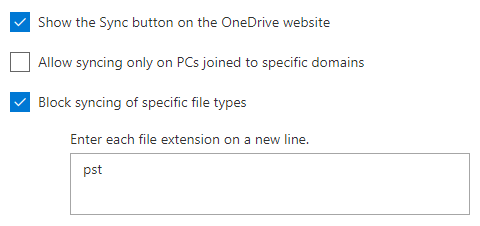
Default storage for users having OneDrive access is 1 TB.

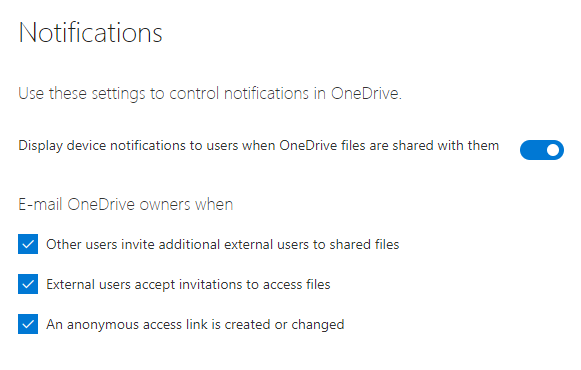
OneDrive is configured as below:





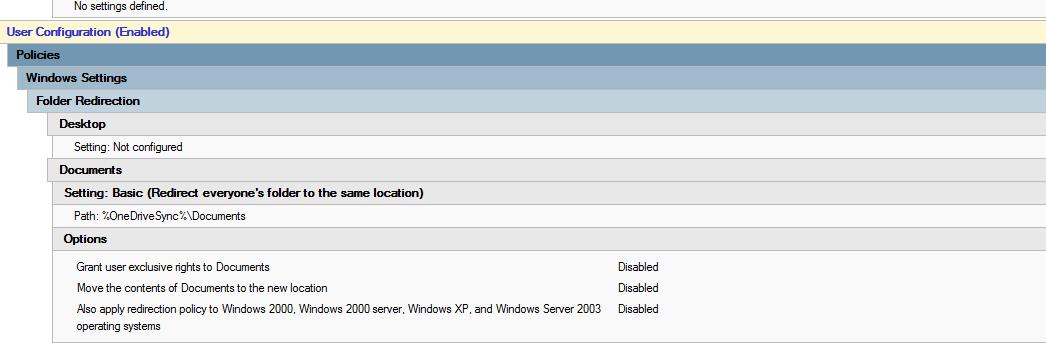
Syncing .pst files to OneDrive is not recommended, so pst file type is blocked from Syncing to Onedrive-

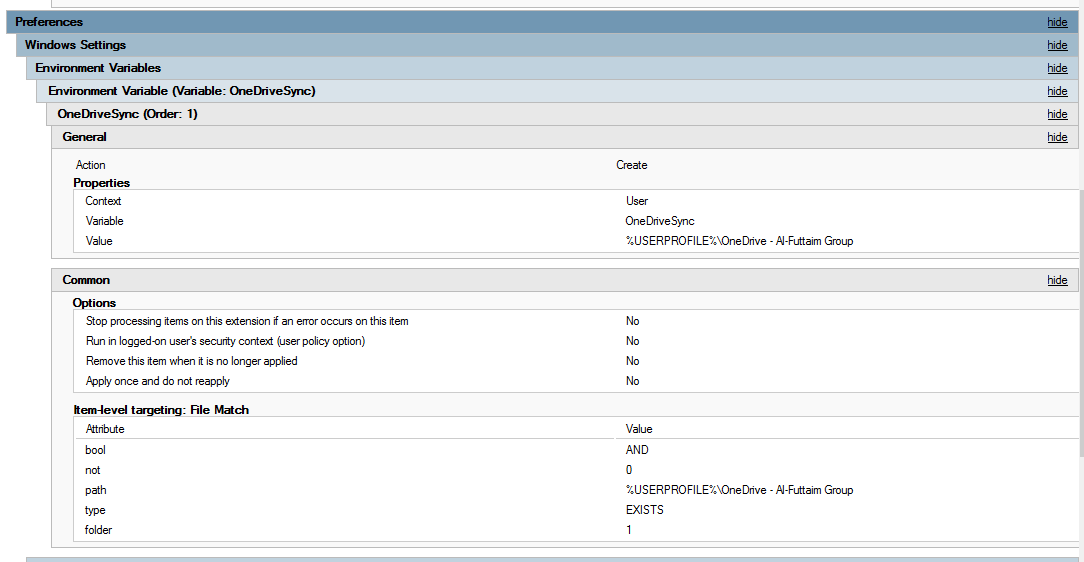




We have group policy created in local AD for OneDrive syncing. Once OneDrive is configured in user’s computer, OneDrive sync client will create the OneDrive directory with tenant ID “OneDrive – Al-Futtaim Group” in the user’s computer.

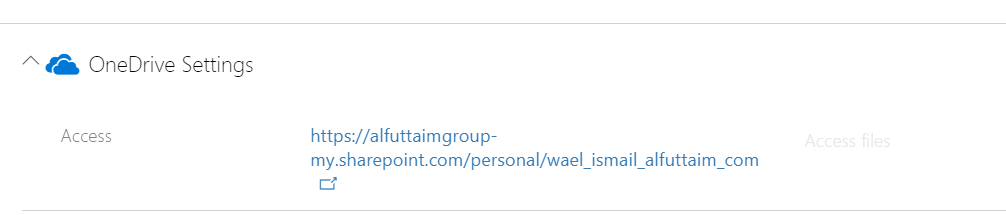
When the user logoff and login back to the computer, the group policy will get assigned to the machine and GPO will check whether the tenant id is available. If it’s available, the GPO will create a folder named “Documents” inside the OneDrive directory and create an environment variable which points the local *“My Documents”* folder to the new documents folder in OneDrive directory i.e., the path of My Documents folder (D:\users\user name\My Documents) will change to %userprofile%/OneDrive-Al-Futtaim Group.



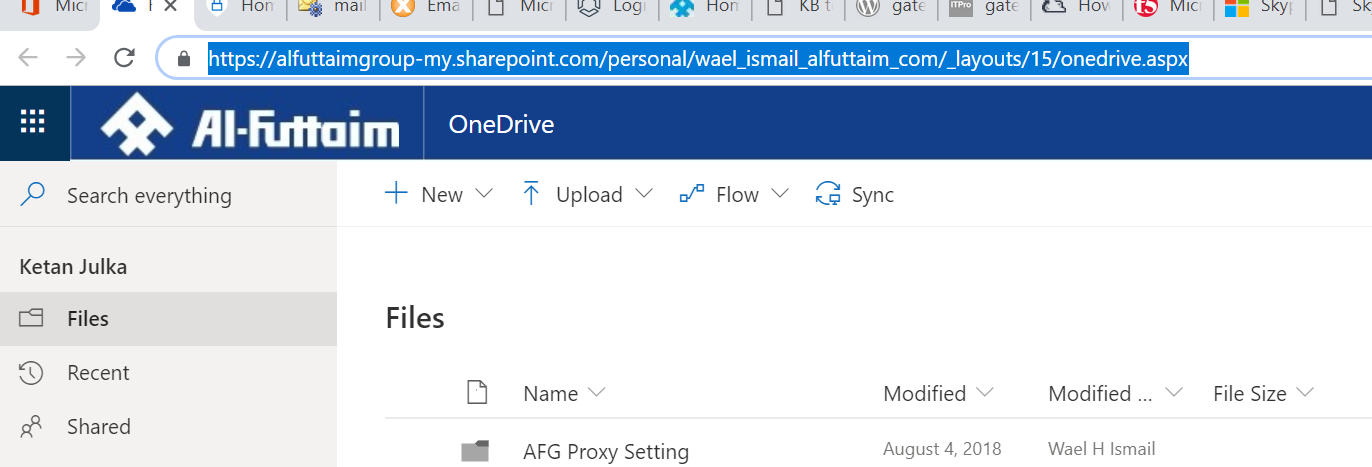


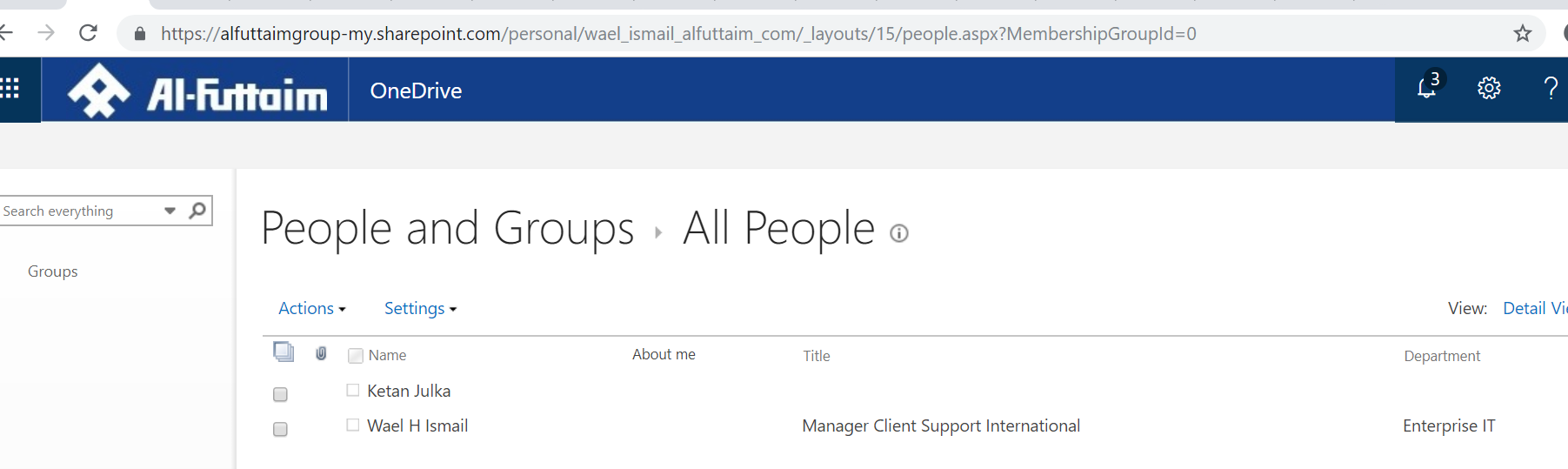
# Remove access permissions on One Drive data of separated users.

1. Search for the separated user in <https://admin.microsoft.com>
2. Scroll to One Drive settings and click Access Files and click on the one drive link which appears.



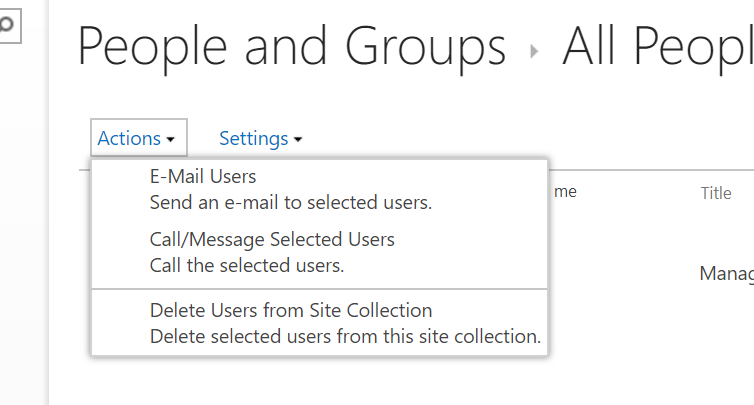
1. Modify the link in the address bar of the browser and replace “15/onedrive.aspx” with “people.aspx?MembershipGroupId=0”





1. Select all the Names and from the Actions Menu select “Delete users from Site Collection”

Once all the Names are removed no one will be able to access the Shared Files and Folders.



# International Locations

1. **Kenya, Uganda** **and Tanzania.**

**XXXXXXXXXX domain**

1. XXXXXXXXXX have their own AD and creation of the new users/modifications are managed by XXXXXXXXXX, Kenya and AD objects are getting synced via Alfuttaim AAD connect servers to the alfuttaimgroup.onmicrosoft.com tenant.
2. Mailboxes are hosted in Alfuttaim Office365 tenant.
3. All the users have E3 license.
4. MX record for this domain is pointing to AFG Symantec email gateway and emails route to Office365 directly from Symantec without coming to the hybrid servers.
5. **Philippines**

**rsh.com.ph domain**

1. Rsh.com.ph domain had a requirement as they can’t change the primary email address to alfuttaim.com post migration, hence we have migrated the domain as well.
2. All the users have their primary email address as [Firstname.lastname@XXXXXXX.ph](mailto:Firstname.lastname@XXXXXXX.ph) and [Firstname.lastname@XXXXXXXXX.com](mailto:Firstname.lastname@XXXXXXXXX.com) and [firstname@XXXXXXX.ph](mailto:firstname@XXXXXXX.ph) as their additional addresses.
3. All the AD objects are created in the OU ***XXXXXXXXX/XXXXXXX/XXXXXXX– Philippines*** and remote mailbox is enabled.
4. MX is pointing to AFG Symantec email gateway and emails route via Hybrid server like Alfuttaim.com domain.
5. **Indonesia**

**XXXXXXXX.id domain**

1. Configuration for this domain is same as **XXXXXXXXX.ph** domain and all the objects are created under the OU ***XXXXXXXXX/XXXXXXXX/XXXXXX – Indonesia.***
2. **Thailand**

**rsh.co.th domain**

1. All the AD objects for ***XXXXXXX*** domain is created under OU ***XXXXXXX/XXXXX/XXXXXX – Thailand.***
2. All the users from this domain now have their primary email address as [Firstname.lastname@XXXXXXXXX.com](mailto:Firstname.lastname@XXXXXXXXX.com) and their old email address [firstname@XXXXXXXX.th](mailto:firstname@XXXXXXXX.th) is stamped as additional email address so that they can continue to receive emails.
3. MX is pointing to AFG Symantec email gateway and emails route via Hybrid server like Alfuttaim.com domain
4. **Hong Kong**

**XXXXXXXX.hk domain**

1. All the AD objects for ***XXXXXX*** domain is created under OU ***XXXXXXXX/XXXXXXX/XXXXXX- Hong Kong.***
2. All the users from this domain now have their primary email address as [Firstname.lastname@XXXXXXX](mailto:Firstname.lastname@XXXXXXX) and old email address [firstname@XXXXXXXXXX.hk](mailto:firstname@XXXXXXXXXX.hk) is stamped as additional email address only for 19 users as other accounts doesn’t need it anymore.
3. MX is pointing to AFG Symantec email gateway and emails route via Hybrid server like Alfuttaim.com domain.
4. **Singapore**

**rsh.com.sg domain**

1. All the AD objects for ***XXXXXXX*** domain is created under OU ***XXXXXXXX/XXXXXX/XXXXX - Singapore.***
2. All the users from this domain now have their primary email address as [Firstname.lastname@XXXXXXXX](mailto:Firstname.lastname@XXXXXXXX) and **no** old email address is stamped as additional email address except for below 3 accounts:

[XXXXX@XXXXXXX.sg](mailto:XXXXX@XXXXXXX.sg)

[XXXXX@XXXXXXXX.sg](mailto:XXXXX@XXXXXXXX.sg)

[XXXXX@XXXXXXX.sg](mailto:XXXXX@XXXXXXX.sg)

1. As per the business requirement, the email address shouldn’t change for the above 3 mailboxes post migration. Hence, we have stamped the primary email address as [firstname@XXXXXX.sg](mailto:firstname@XXXXXX.sg). All the outgoing emails from these mailboxes are going with ***XXXXXXXX*** domain as sending address.
2. MX is pointing to AFG Symantec email gateway and emails route via Hybrid server like Alfuttaim.com domain.

**XXXXXXX.sg domain**

1. All the AD objects for *XXXXXXX* domain is created under OU ***XXXXXXXXX/XXXXXX/XXXXXXs - Singapore.***
2. All the users from this domain now have their primary email address as [Firstname.lastname@xxxxxxxx](mailto:Firstname.lastname@xxxxxxxx) and **no** old email address is stamped as additional email address except for below 2 accounts:

[help@xxxxxxx.sg](mailto:help@xxxxxxx.sg)

[shop@xxxxxxx.sg](mailto:shop@xxxxxxx.sg)

1. As per the business requirement, the email address should not change for the above 2 mailboxes post migration. Hence, we have stamped the primary email address as [firstname@xxxxxx.sg](mailto:firstname@xxxxxx.sg). All the outgoing emails from these mailboxes are going with *XXXXXXXXX* domain as sending address.
2. MX is pointing to AFG Symantec email gateway and emails route via Hybrid server like Alfuttaim.com domain.
3. **Malaysia**

**XXXXXXX.my domain**

1. All the AD objects for ***XXXXXXXX*** domain is created under OU ***XXXXXXXXXXX/XXXXXX/XXXXXXX- Malaysia.***
2. All the users from this domain now have their primary email address as [Firstname.lastname@XXXXXXXXX.com](mailto:Firstname.lastname@XXXXXXXXX.com) and old email address [firstname@XXXXXXXX.my](mailto:firstname@XXXXXXXX.my) is stamped as additional email address only for 10 users as other accounts doesn’t need it anymore.
3. MX is pointing to AFG Symantec email gateway and emails route via Hybrid server like XXXXXXXX domain.

**robinsons.com.my domain**

1. All the AD objects for ***XXXXXXXX*** domain is created under OU ***XXXXXXX/XXX/XXXXX.***
2. All the users from this domain now have their primary email address as [Firstname.lastname@xxxxxxxx](mailto:Firstname.lastname@xxxxxxxx) and old email address [firstname@xxxxxxxxxx](mailto:firstname@robinsons.com.my) is stamped as additional email address only for below mentioned 4 users as other accounts doesn’t need it anymore.

[xxxxxxxx@xxxxxxxx](mailto:xxxxxxxx@alfuttaim.com)

[xxxxxxxx@xxxxxxxx](mailto:xxxxxxxx@alfuttaim.com)

[xxxxxxxx@xxxxxxxx](mailto:xxxxxxxx@alfuttaim.com)

[xxxxxxxx@xxxxxxxx](mailto:xxxxxxxx@alfuttaim.com)

1. MX is pointing to AFG Symantec email gateway and emails route via Hybrid server like Alfuttaim.com domain.
2. **Sri Lanka**

**AMW limited and Orient domain.**

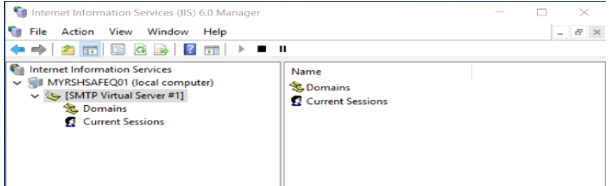
1. Migration yet to start.

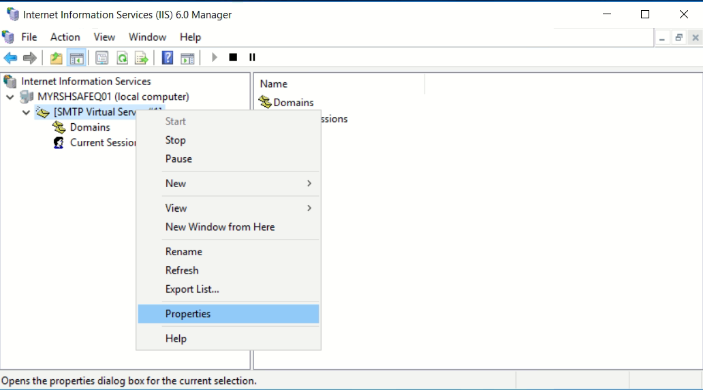
# Email relay for applications

Sometimes organizations need to set up a multifunction device or application to send email through Office 365 and they discover that the device or application can’t connect directly to Office 365. In these cases, we need to set up Internet Information Services (IIS) on a Windows server to work as an intermediary.

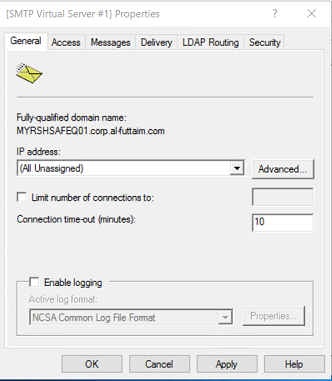
We have IIS relay server setup **only for Malaysia and Singapore** location with below configuration -

1. Launch Internet Information Services (IIS) 6.0 Manager on the windows sever designated for SMTP relay. Expand the local computer, right-click [**SMTP Virtual Server #1]**, and then select **Properties**.

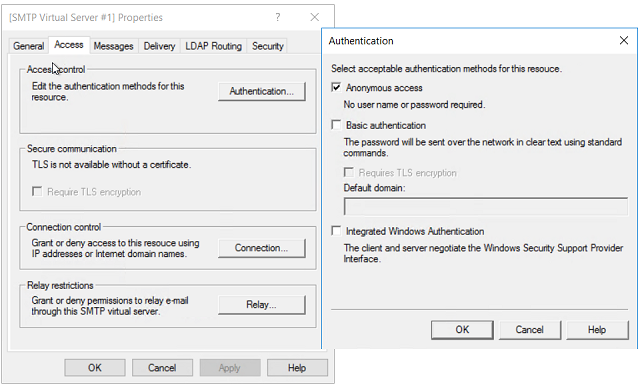




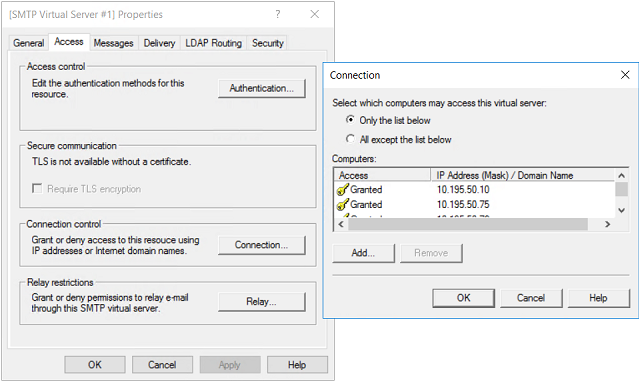
1. Below is the properties page for the SMTP virtual server and no configuration needed under **General** tab



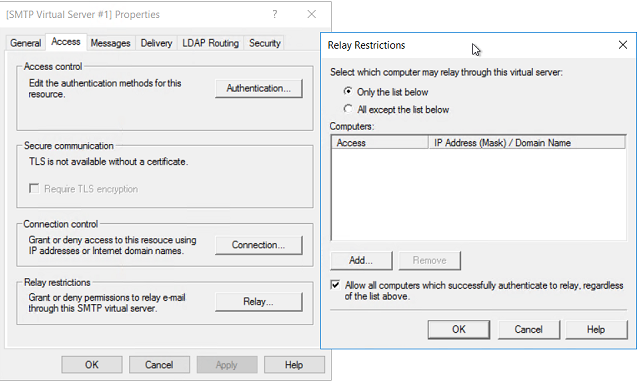
1. On the Access tab and select Authentication and make sure that Anonymous access is selected.



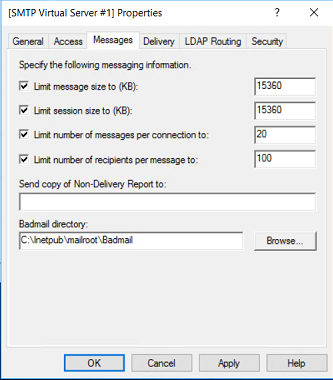
1. Select **Connection** under Access tab then select the radio button “Only the list below”. These are the IP address from which the connection will be accepted



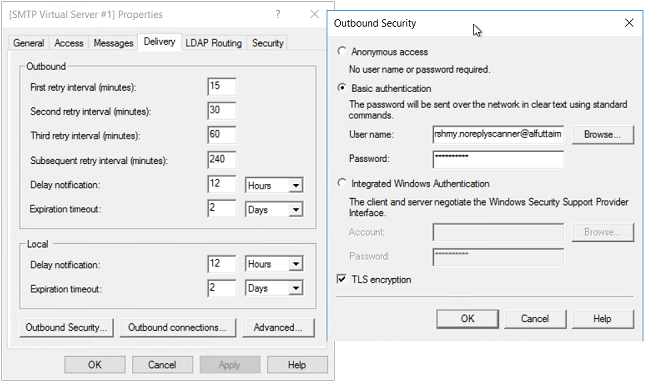
1. No configuration needed under “Relay…”. Keep it default -



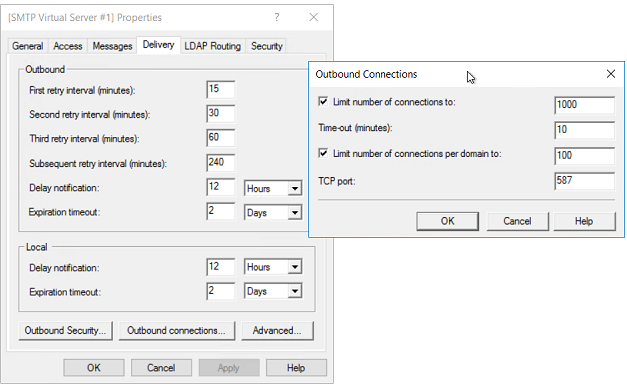
1. Under the **Messages** Tab you can configure the message size limits and the number of connections as per requirement. Below is the current configuration -



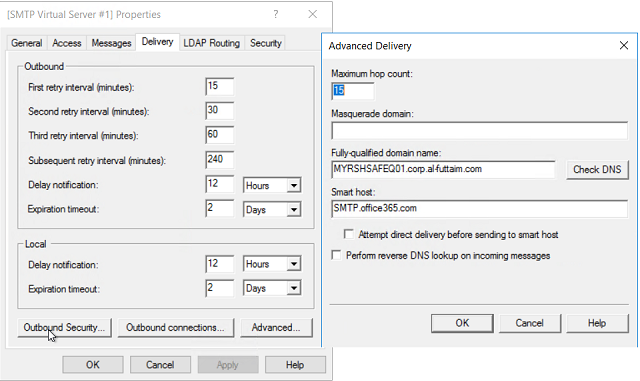
1. On the **Delivery** tab, select **“Outbound Security…”** and Select Basic Authentication. Enter the credentials of the Office 365 user who you want to use to relay SMTP mail and check the “TLS encryption” check box-



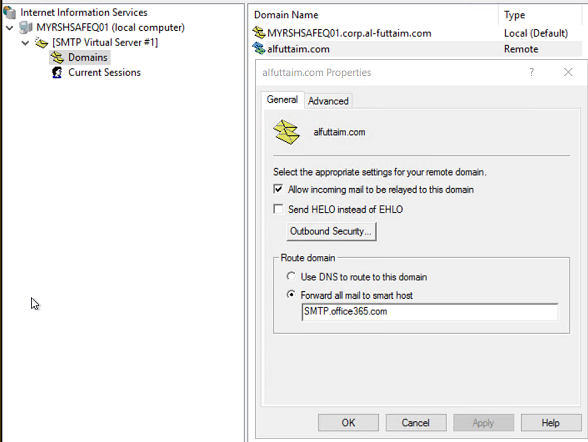
1. Click **Outbound** **Connections** and in the TCP Port box, enter 587 and select OK. 587 port is SMTP port with TLS.



1. Select Advanced and specify **SMTP.office365.com** as the Smart Host.



1. Restart the **IIS service** and the **SMTP service** on the server.
2. [SMTP Virtual server #1] configuration is done. Now, click Domains under it and add alfuttaim.com as Remote domain with the settings as per below screen shot-

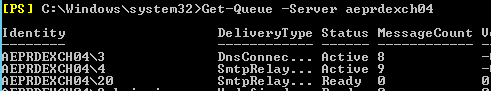


# Reclaim D drive space consumed due to Mail.que files-

Steps to remove the ‘mail.que’ files from the server when D drive disk space gets full due to mail.que-

1. Launch Exchange management Shell and run below command –

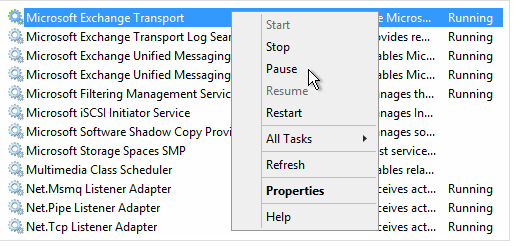
Get-Queue -Server “Name of the server for which D drive is full”



1. See the number of emails in the queues except for the DeliveryType as ShadowRed…

No. of emails showing in the queue means these many emails needs to be processed by the particular server.

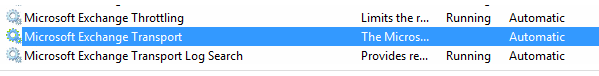
1. Launch Services.msc on the server and Pause the Microsoft Exchange Transport service. Pausing the service will make it process the emails which already in the queue and won’t accept new messages.



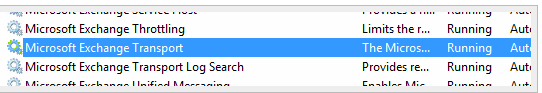
1. Monitor the queue by running the below command while the Transport service is paused, and the count should be going down constantly –

Get-Queue -Server “Name of the server for which D drive is full”

1. When the emails in the queue are empty and the count shows 0, stop the “Microsoft Exchange Transport” service -



1. After ensuring the queue as empty and stopping the Transport Service, Go to D:\Queue and move the folder called “QueueDB” to another location.
2. Now, Start the Microsoft Exchange Transport service and a new folder as “QueueDB” will be created again with new set of mail.que file in it with smaller size-



1. Disk space on the server is now reclaimed, Monitor the email flow is normal and everything is fine, the old mail.que (QueueDB folder which was moved to another location) can now be safely deleted.

# Tasks Yet to Complete

1. **Distribution Lists (DL’s) are yet to migrate** to Office365 and the owners of the groups won’t be able to manage (add/remove) membership until the DL’s are migrated.

Deleting the group from the AD and recreating it again on Office365 with the same details is approach for DL migration and while doing this we need to make sure LegacyExchangeDN is stamped on the newly created DL on office 365 so that the users don’t get NDR when using the cache entry in Outlook.

Once the DL is deleted from on-prem and recreated on Office365 with same details, we need to create a contact in the AD and it should be under ‘***Non Sync – Contacts’*** OU. This is specifically for the users who are not migrated yet and still wants to see the DL in the GAL. **~~once the DL is ready on Office365 so that the users can still see the DL in the GAL.~~**

1. **Room mailboxes** are yet to be migrated to Office365. Need to export the current configuration/permissions of the room mailboxes before migrating and perform the same configuration post the migration is done.
2. Common mailboxes and shared mailboxes are yet to be migrated to Office365.

# Offline Employees (XXXXXXXXXXX)

1. Offline Employees (myalfuttaim.com) are using corporate Office 365 tenant.
2. Offline Employees are provisioned in Office 365 as new users and able to access Exchange Online, SharePoint Online and OneDrive for Business Online without migrating any data.
3. Myalfuttaim.com users have F1 Plan license assigned.
4. Offline users are managed by HR.  Like Creation, Deletion, modification of accounts.
5. **Self-Password Reset Portal** and **SharePoint portal for User management** is made available. Below is the server detail for both for offline user’s management.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Server | IP address | Purpose | Access URL | AD Group for access permission |
| XXXXXXXXXX | XXXXXXXX | O365 Offline user password reset portal | <http://self-service.myalfuttaim.com/> |  |
| XXXXXXXXXX | XXXXXXXX | O365 Offline user management portal for HR | <http://aeprdo365hrmgt/CreateUser> | HRUserMgmtPortal |

Self-Password Reset Portal is developed to enable corporate offline employee users to reset the password based on supplying few unique attributes for the users.

**Service accounts: -**

|  |  |
| --- | --- |
| User | Details |
| XXX\XXXXXX | AEPRDO365HRMGT - O365 HR Mgmt Portal |
| XXXXX | AEPRDO365HRMGT - O365 HR Mgmt Portal. SQL instance "AEPRDO365HRMGT\SQLEXPRESS" |

**Scope of EIT:** To assist from the backend if any issues.

# Version Control

Table 4‑1 Version Control and History

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version No.** | **Changed Section** | **Change Description** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |