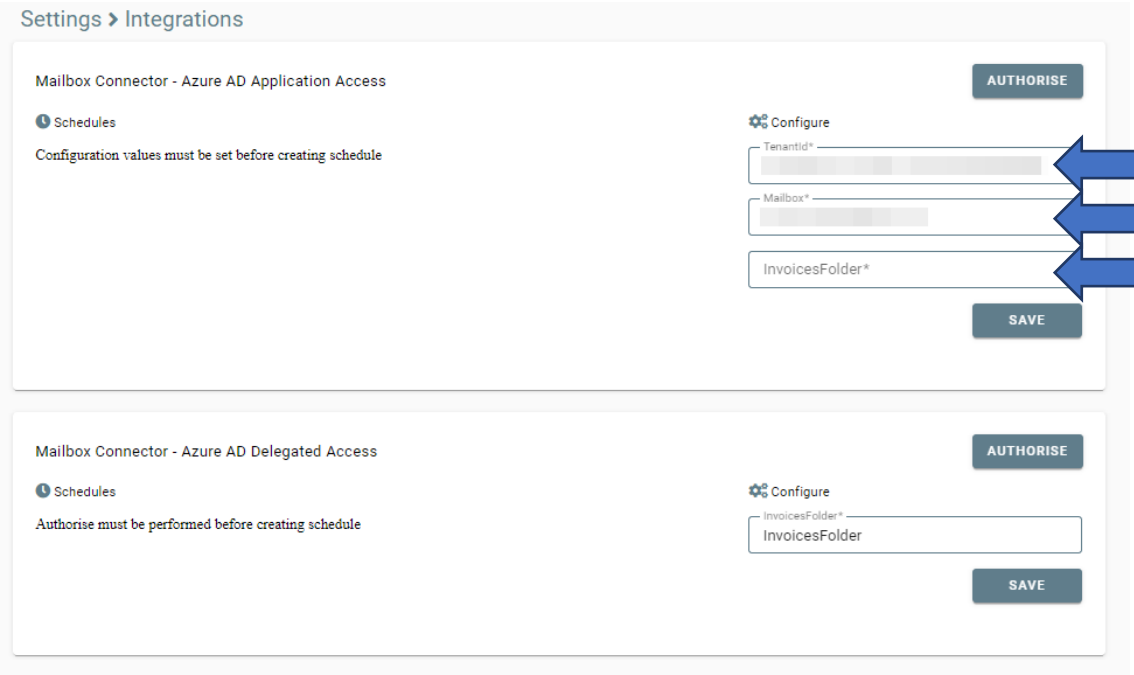
Initial configuration within Verify

It is recommended that an Azure administrator is on hand to immediately approve application access as part of the configuration.

As a Verify tenant administrator, navigate to Application Settings > Integrations. Complete the initial configuration for the Azure AD Application Access Mailbox Connector. To do this, the following information must be provided:

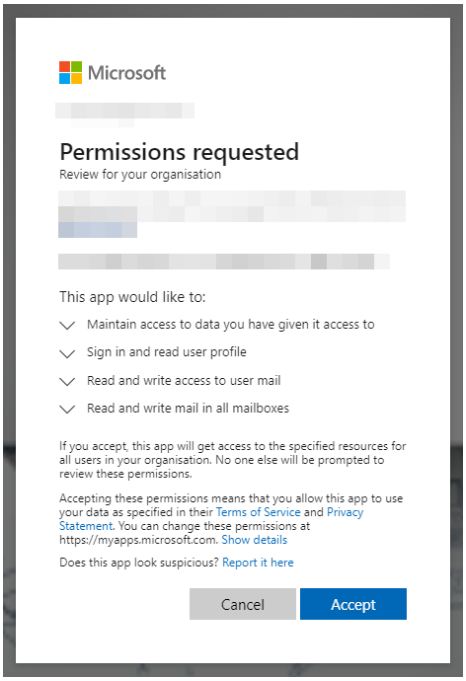
- The Azure Active Directory Tenant Id (GUID).
- The mailbox to connect to. This can be either a user or a shared mailbox.
- The folder in the mailbox from which to retrieve email. Normally, this will simply be “Inbox”. If users are sorting email, or rules apply, this can be any accessible folder specified as “Folder\Subfolder”-style paths if necessary.



Once completed, press SAVE and then press AUTHORISE. At this point, a new tab will open, asking the user to log in to authorise access to the specified Azure tenancy. This is an OAUTH process with the new tab being Microsoft-side authentication and authorisation.

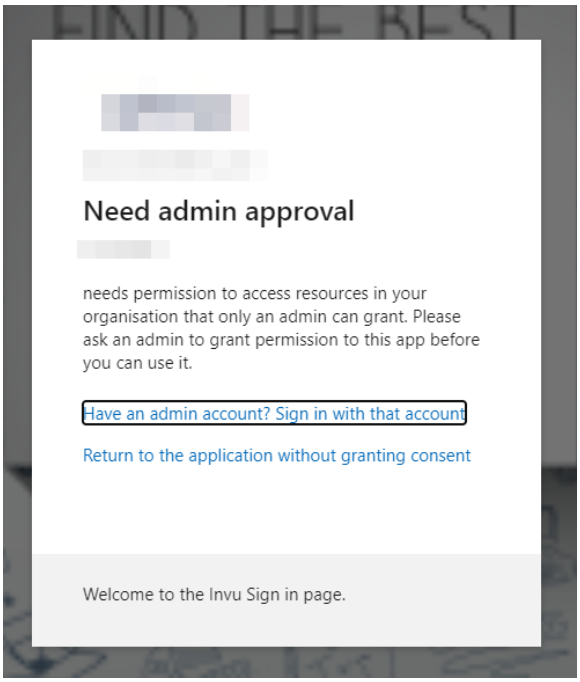
There are two possible options here:

1. Log in as a user with administrative privileges in Azure. This is recommended if possible as the administrator can immediately approve the required permissions and authorisation takes place immediately. Under these circumstances, once the user logs in they are presented with the following permissions request:



Note the “Read and write mail in all mailboxes” permission. This can be narrowed to a particular mailbox using security groups as detailed later in this document.

2. Use a normal user and follow the Azure administrator consent procedure. In this case, the non-privileged user will see the following:



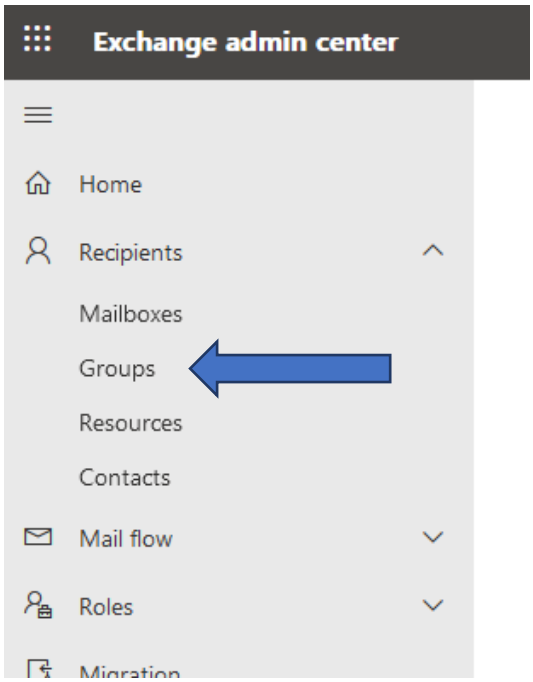
At this point, an admin consent request should be sent to the customer Azure administrator.

The administrator must approve the consent request, at which point the Verify Enterprise Application (essentially a service principal) is created in the customer’s Azure tenancy. The administrator can lock down the application as necessary (see later in this document) and must then notify the Verify tenant administrator who should be able to re-authorise the integration successfully at that point without further intervention.

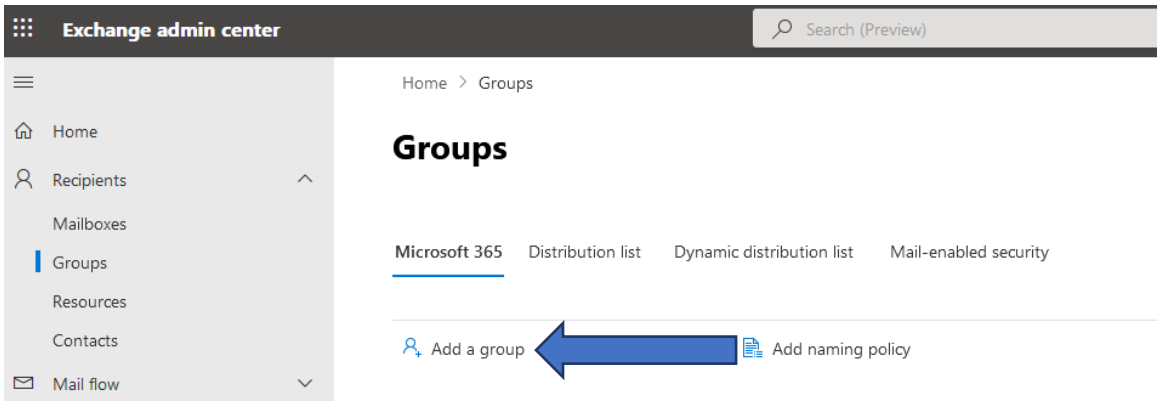
Creating a mail-enabled security group

This is done within the Exchange Online administration portal.

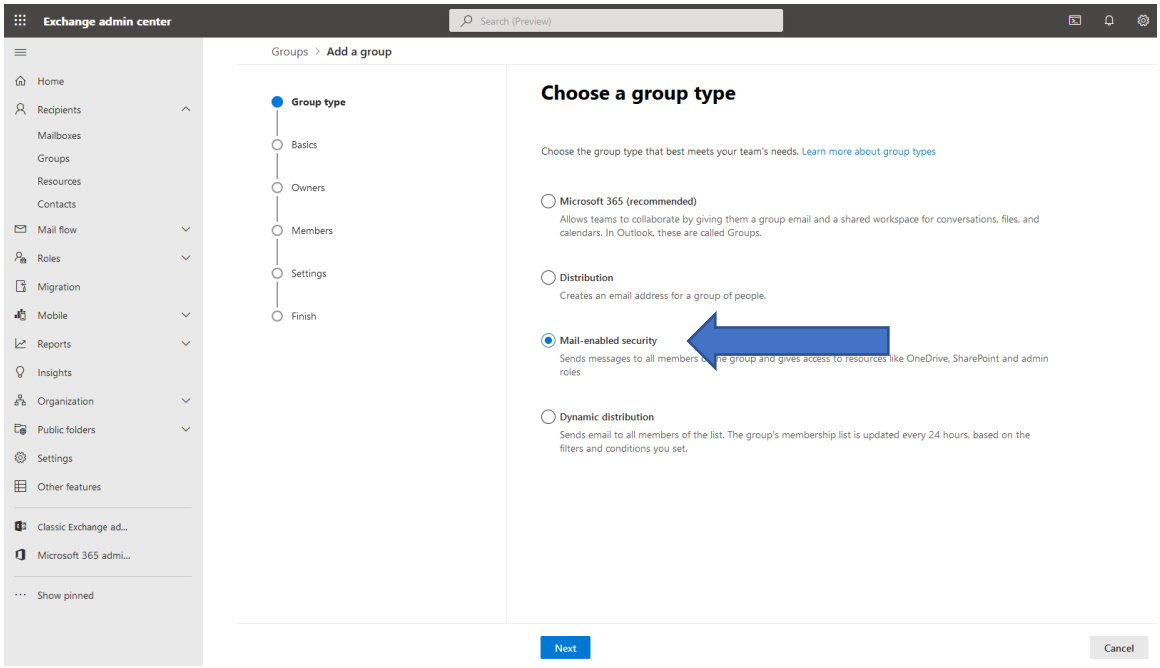
Navigate to **Recipients > Groups**



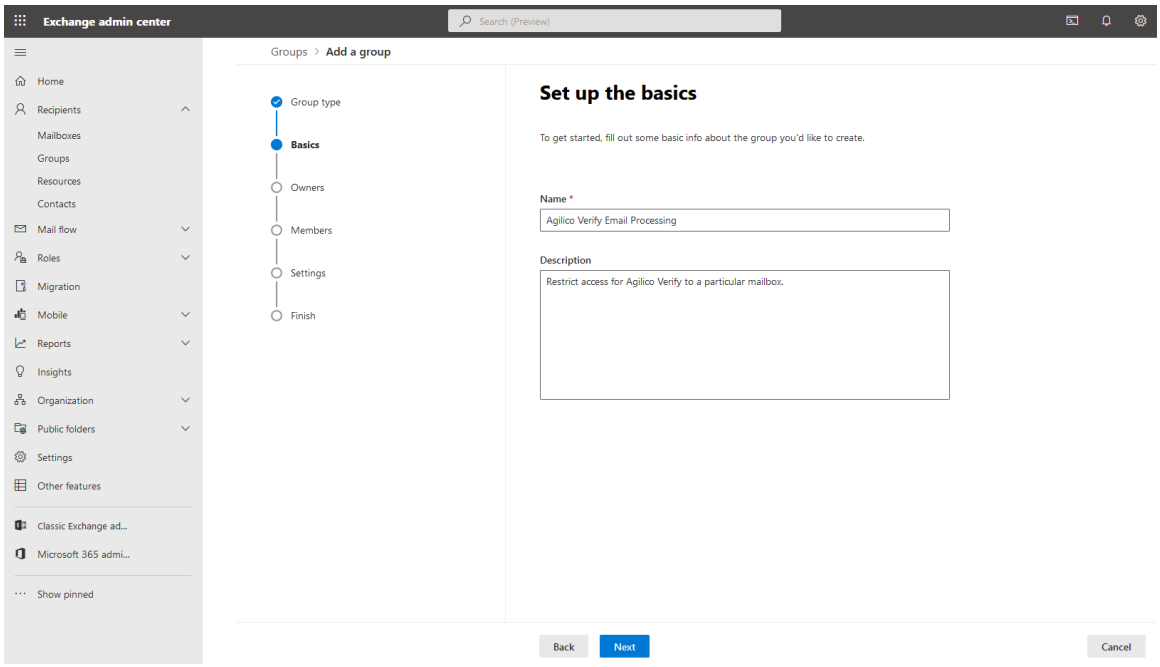
Choose **Add a group**



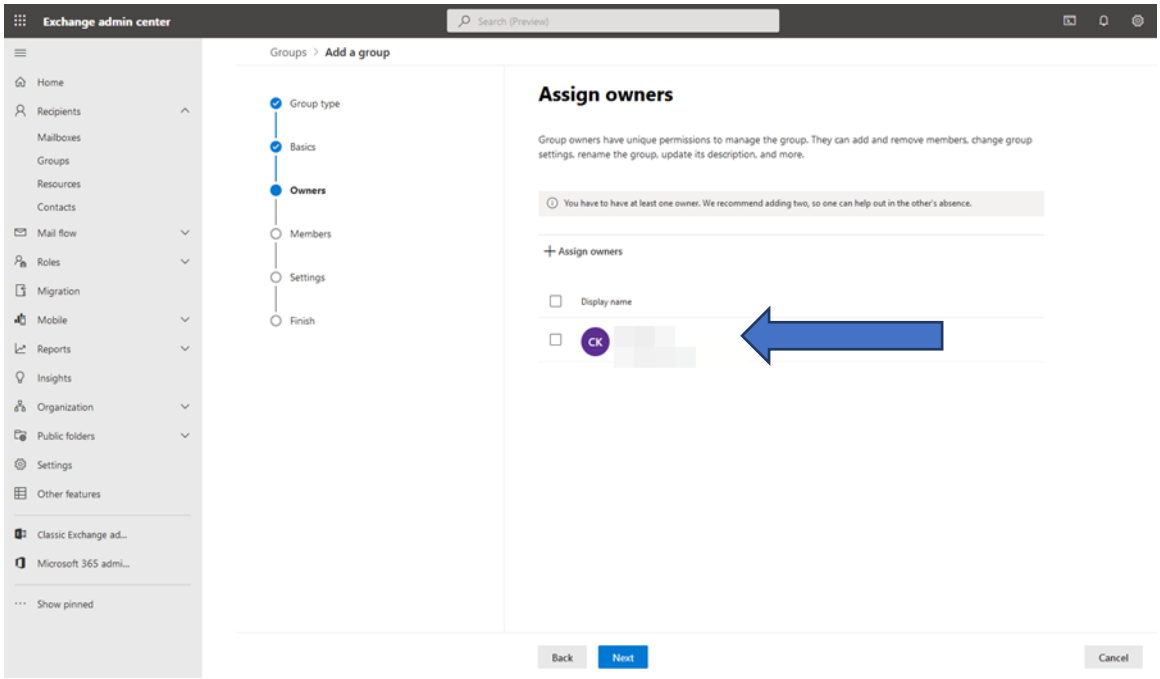
Select **Mail-enabled security** for the group type



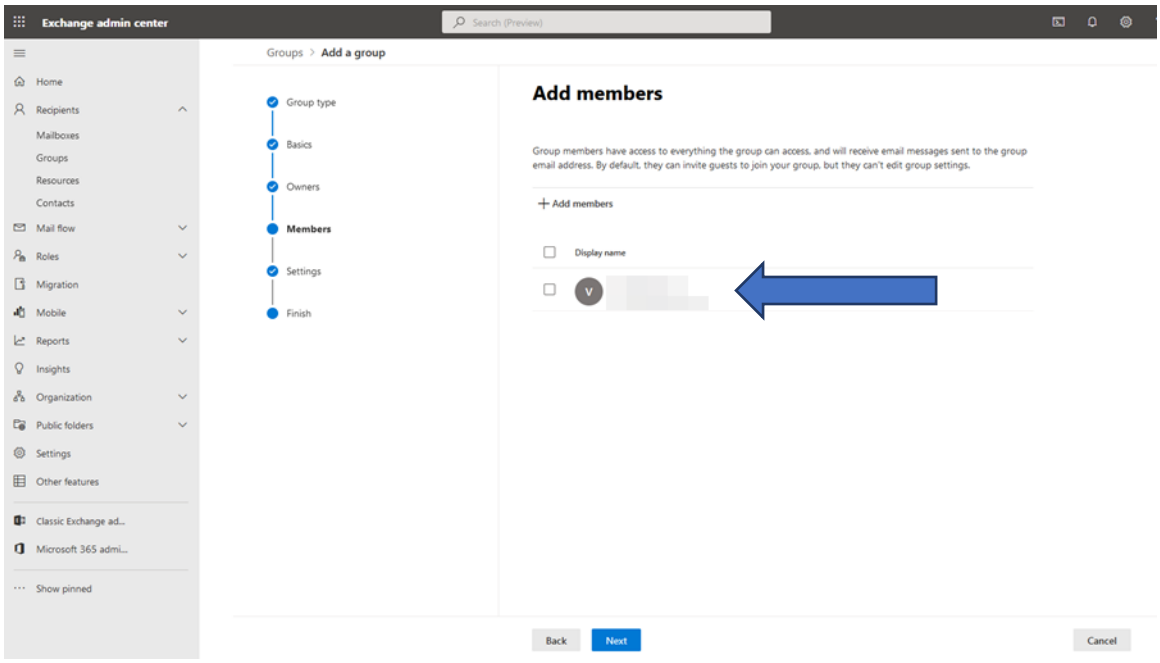
Give the group a meaningful name and description.



Assign an owner – given the purpose of the group, this should be an administrator.

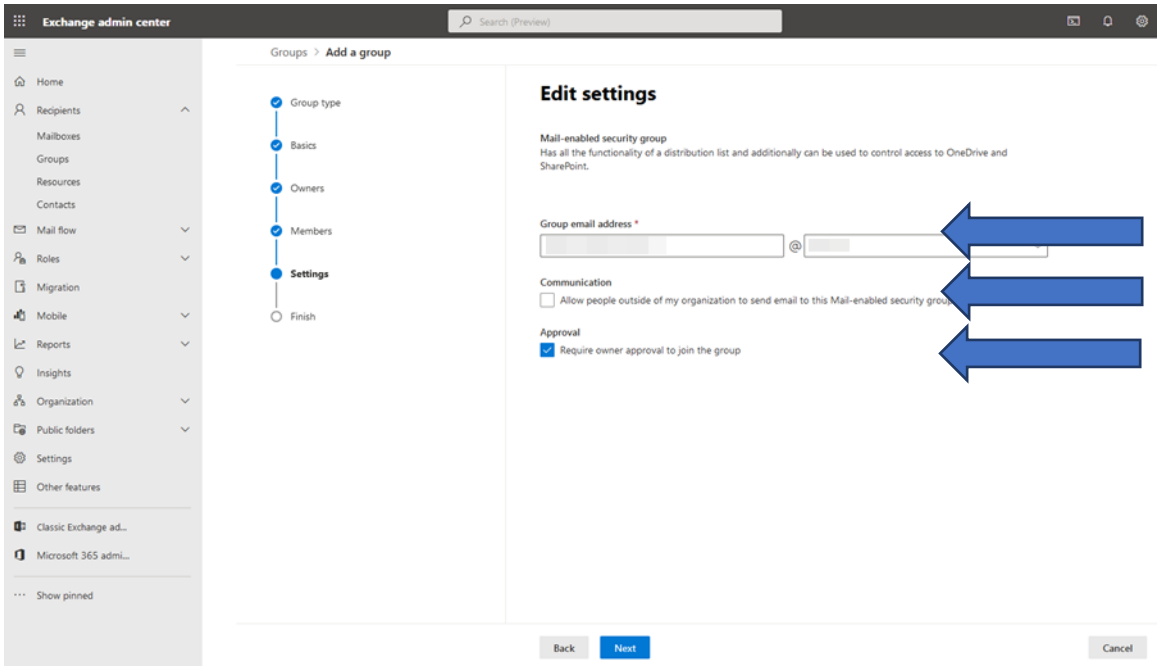


Add only the required mailbox that Verify will be using to the group.

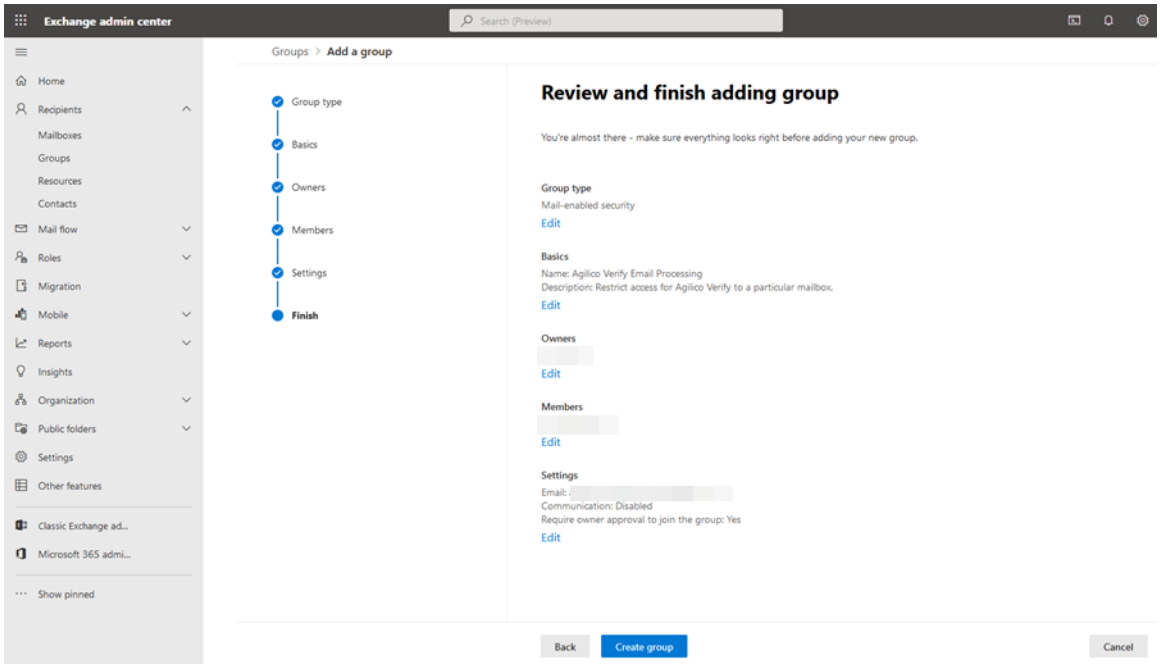


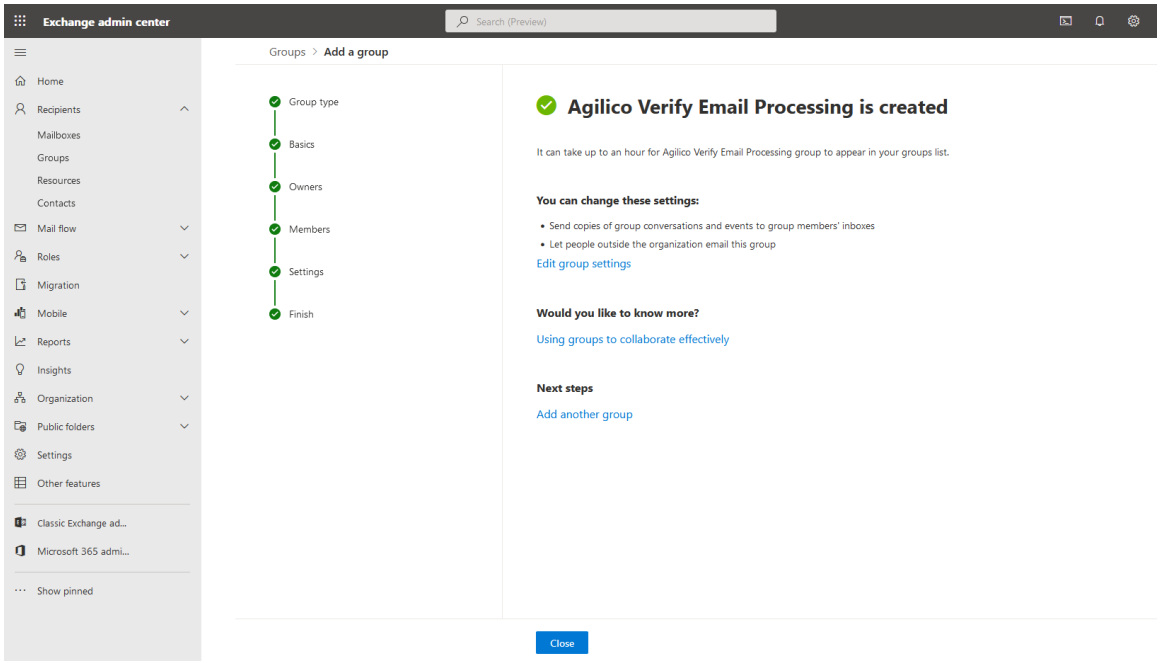
The group requires its own email address. This will not be used, so name it accordingly. It is recommended to:

- **Disable** "*Allow people outside of my organisation to send email top this Mail-enabled security group***"** because the group itself should not be externally accessible.
- **Enable "***Require owner approval to join the group"* in order to prevent other users inadvertently joining the group and exposing their email accounts.



Review the group settings carefully, then **Create group**





Restricting the Enterprise Application to the Mail-enabled Security Group

This process is accomplished via Powershell. An Administrator must connect to Exchange Online in order to create the required access policy.

In an **elevated** Powershell Command Prompt, install (if not already installed) and load the ExchangeOnlineManagement module from the Powershell gallery:

```
Install-Module ExchangeOnlineManagement
```

```
PS C:\Windows\system32> Install-Module ExchangeOnlineManagement

Untrusted repository
You are installing the modules from an untrusted repository. If you trust this repository, change its
InstallationPolicy value by running the Set-PSRepository cmdlet. Are you sure you want to install the modules from
'PSGallery'?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "N"): y
```

Import the module.

```
Import-Module ExchangeOnlineManagement
```

```
PS C:\Windows\system32> Import-Module ExchangeOnlineManagement
```

Connect to Exchange Online.

```
Connect-ExchangeOnline -UserPrincipalName <administrator account>
```

```
PS C:\Windows\system32> Connect-ExchangeOnline -UserPrincipalName

------------------------------------------------------------------------------
The module allows access to all existing remote PowerShell (V1) cmdlets in addition to the 9 new, faster, and more reliable cmdlets.


|-----------------------------------------------------------------------------|
|    Old Cmdlets                  |    New/Reliable/Faster Cmdlets            |
|-----------------------------------------------------------------------------|
|    Get-CASMailbox               |    Get-EXOCASMailbox                      |
|    Get-Mailbox                  |    Get-EXOMailbox                         |
|    Get-MailboxFolderPermission  |    Get-EXOMailboxFolderPermission         |
|    Get-MailboxFolderStatistics  |    Get-EXOMailboxFolderStatistics         |
|    Get-MailboxPermission        |    Get-EXOMailboxPermission               |
|    Get-MailboxStatistics        |    Get-EXOMailboxStatistics               |
|    Get-MobileDeviceStatistics   |    Get-EXOMobileDeviceStatistics          |
|    Get-Recipient                |    Get-EXORecipient                       |
|    Get-RecipientPermission      |    Get-EXORecipientPermission             |
|-----------------------------------------------------------------------------|

To get additional information, run: Get-Help Connect-ExchangeOnline or check https://aka.ms/exops-docs

Send your product improvement suggestions and feedback to exocmdletpreview@service.microsoft.com. For issues related to the module, contact Microsoft support. Don't use the feedbac
k alias for problems or support issues.
------------------------------------------------------------------------------
```

Add an application access policy.

New-ApplicationAccessPolicy -AppId **a173481b-692f-4236-b484-8db9419ed819** -PolicyScopeGroupId <the **security group** email address created previously> -AccessRight RestrictAccess -Description "Restrict Agilico Verify to members of the AgilicoVerifySecurityGroup distribution group."

```
PS C:\Windows\system32> New-ApplicationAccessPolicy -AppId  -PolicyScopeGroupId agilicoverifysecuritygroup@invu.net -AccessRight RestrictAccess
-Description "Restrict this Agilico Verify to members of the AgilicoVerifySecurityGroup distribution group."


RunspaceId       :
ScopeName        : Agilico Verify Email Processing
ScopeIdentity    : Agilico Verify Email Processing20220907073226
Identity         :

AppId            :
ScopeIdentityRaw :
Description      : Restrict this Agilico Verify to members of the AgilicoVerifySecurityGroup distribution group.
AccessRight      : RestrictAccess
ShardType        : All
IsValid          : True
ObjectState      : Unchanged
```

Note that the AppId is the application id for the Enterprise Application. This is defined by the Agilico App Registration and does not change.