

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:

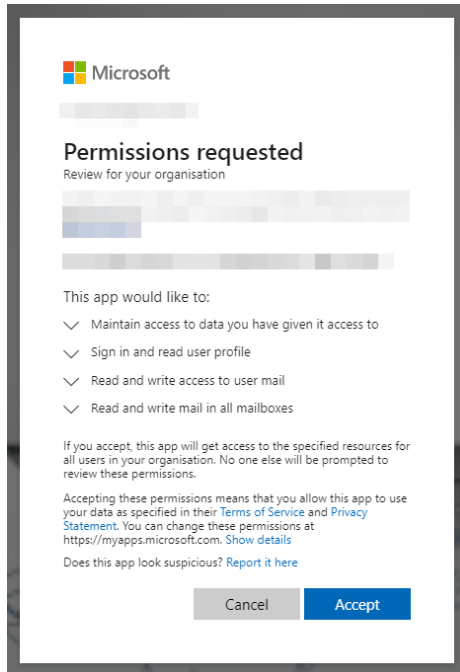
- The Azure Active Directory Tenant Id (GUID).
- The mailbox to connect to. This can be either a user or a shared mailbox.
- The folder in the mailbox from which to retrieve email. Normally, this will simply be "Inbox". If users are sorting email, or rules apply, this can be any accessible folder specified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

The screenshot shows the 'Settings > Integrations' page. The top section is titled 'Mailbox Connector - Azure AD Application Access'. It has an 'AUTHORISE' button in the top right. Below the title, there is a 'Schedules' section with a clock icon and the text 'Configuration values must be set before creating schedule'. To the right of this section is a 'Configure' section with three input fields: 'TenantId*', 'Mailbox*', and 'InvoicesFolder*'. Each field has a blue arrow pointing to it from the right. Below these fields is a 'SAVE' button. The bottom section is titled 'Mailbox Connector - Azure AD Delegated Access'. It also has an 'AUTHORISE' button in the top right. Below the title, there is a 'Schedules' section with a clock icon and the text 'Authorise must be performed before creating schedule'. To the right of this section is a 'Configure' section with one input field: 'InvoicesFolder*'. Below this field is a 'SAVE' button.

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.

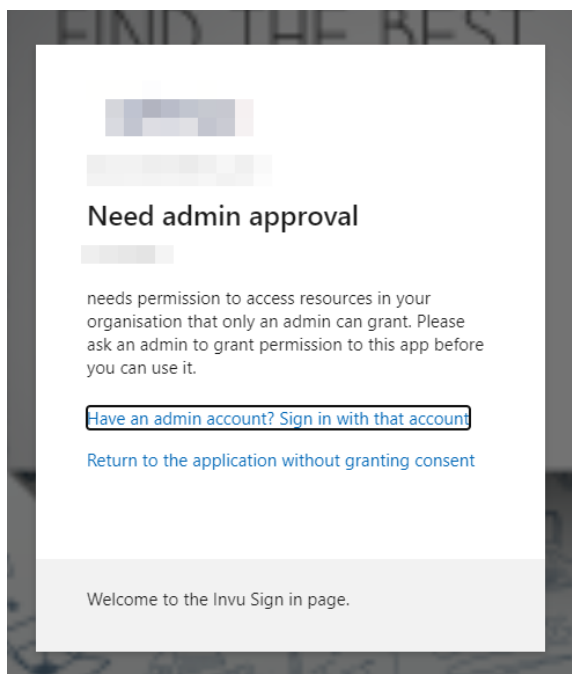
There are two possible options here:

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:



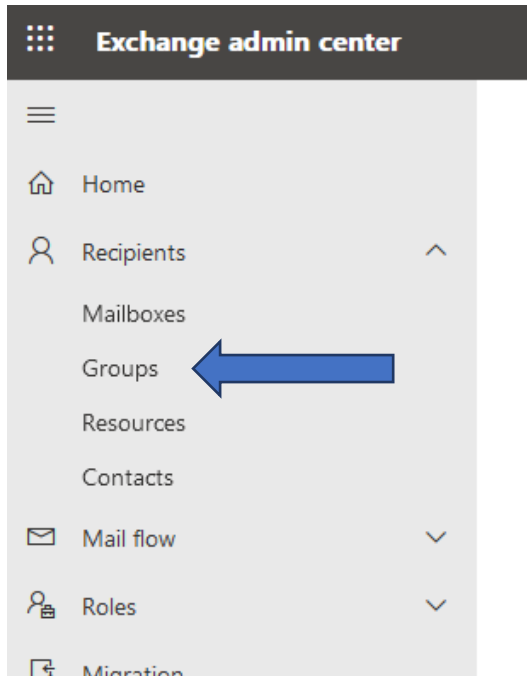
At this point, an admin consent request should be sent to the customer Azure administrator.

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.

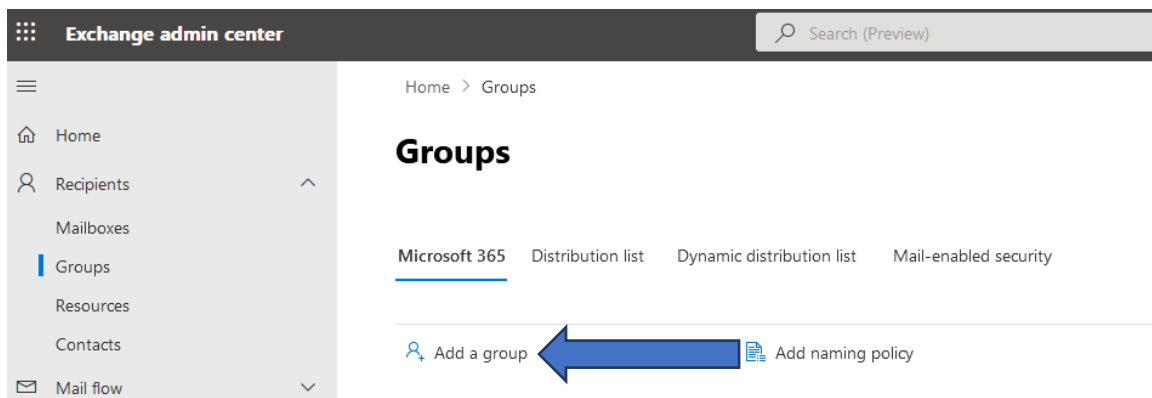
Creating a mail-enabled security group

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

The screenshot shows the Exchange Admin Center interface for adding a group. The left sidebar contains navigation options like Home, Recipients, Mailboxes, Groups, Resources, Contacts, Mail flow, Roles, Migration, Mobile, Reports, Insights, Organization, Public folders, Settings, and Other features. The main content area is titled 'Groups > Add a group'. A progress indicator on the left shows 'Group type' as the current step, with other steps being Basics, Owners, Members, Settings, and Finish. The 'Choose a group type' section offers four options: Microsoft 365 (recommended), Distribution, Mail-enabled security (selected with a blue arrow), and Dynamic distribution. Each option includes a brief description of its functionality. At the bottom, there are 'Next' and 'Cancel' buttons.

Give the group a meaningful name and description.

The screenshot shows the 'Set up the basics' step of the 'Add a group' wizard. The progress indicator now shows 'Basics' as the current step. The main content area prompts the user to fill out basic information. It includes a 'Name *' field with the text 'Agilico Verify Email Processing' and a 'Description' field with the text 'Restrict access for Agilico Verify to a particular mailbox.' At the bottom, there are 'Back', 'Next', and 'Cancel' buttons.

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

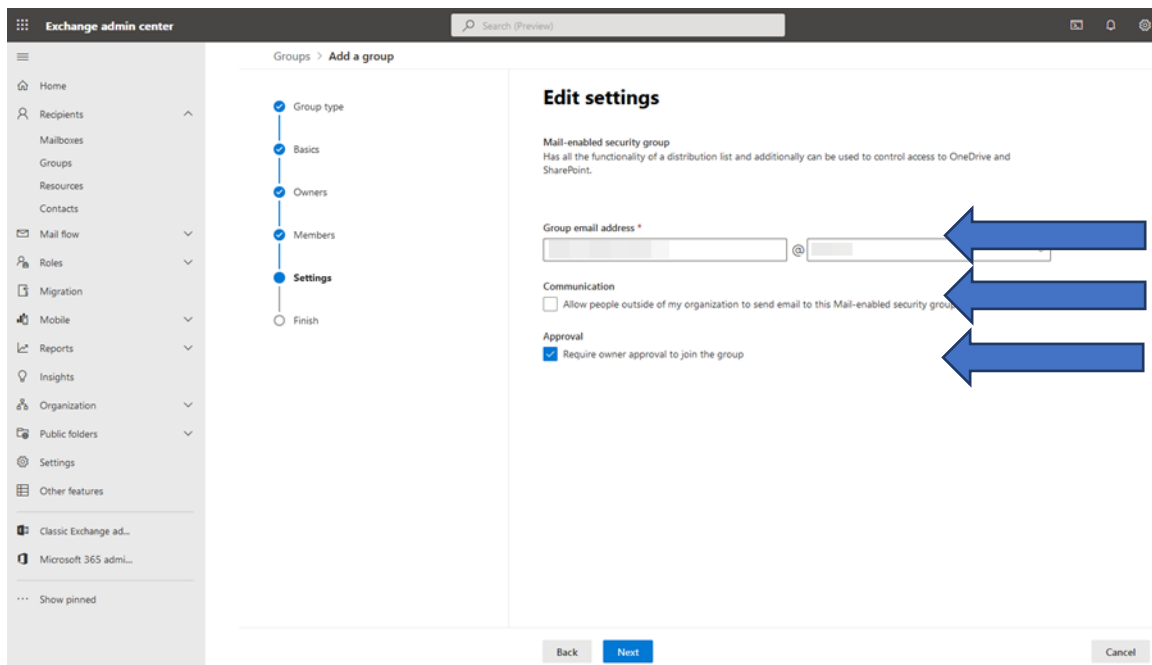
The screenshot shows the Exchange Admin Center interface for adding a group. The left-hand navigation pane is visible, with the 'Owners' step selected in the 'Add a group' progress bar. The main content area is titled 'Assign owners' and includes a warning message: 'You have to have at least one owner. We recommend adding two, so one can help out in the other's absence.' Below this, there is a section for '+ Assign owners' with a list of users. The first user, 'CK', is selected, and a blue arrow points to their name. At the bottom, there are 'Back', 'Next', and 'Cancel' buttons.

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

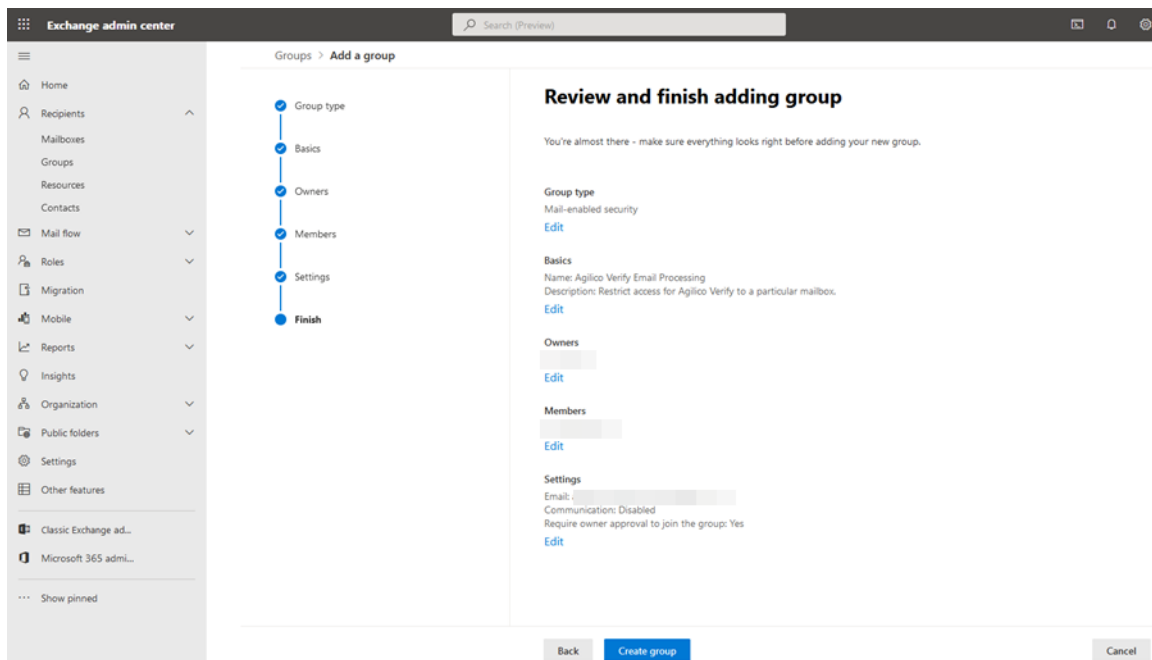
The screenshot shows the Exchange Admin Center interface for adding a group, now at the 'Add members' step. The left-hand navigation pane is visible, with the 'Members' step selected in the 'Add a group' progress bar. The main content area is titled 'Add members' and includes a warning message: 'Group members have access to everything the group can access, and will receive email messages sent to the group email address. By default, they can invite guests to join your group, but they can't edit group settings.' Below this, there is a section for '+ Add members' with a list of users. The first user, 'V', is selected, and a blue arrow points to their name. At the bottom, there are 'Back', 'Next', and 'Cancel' buttons.

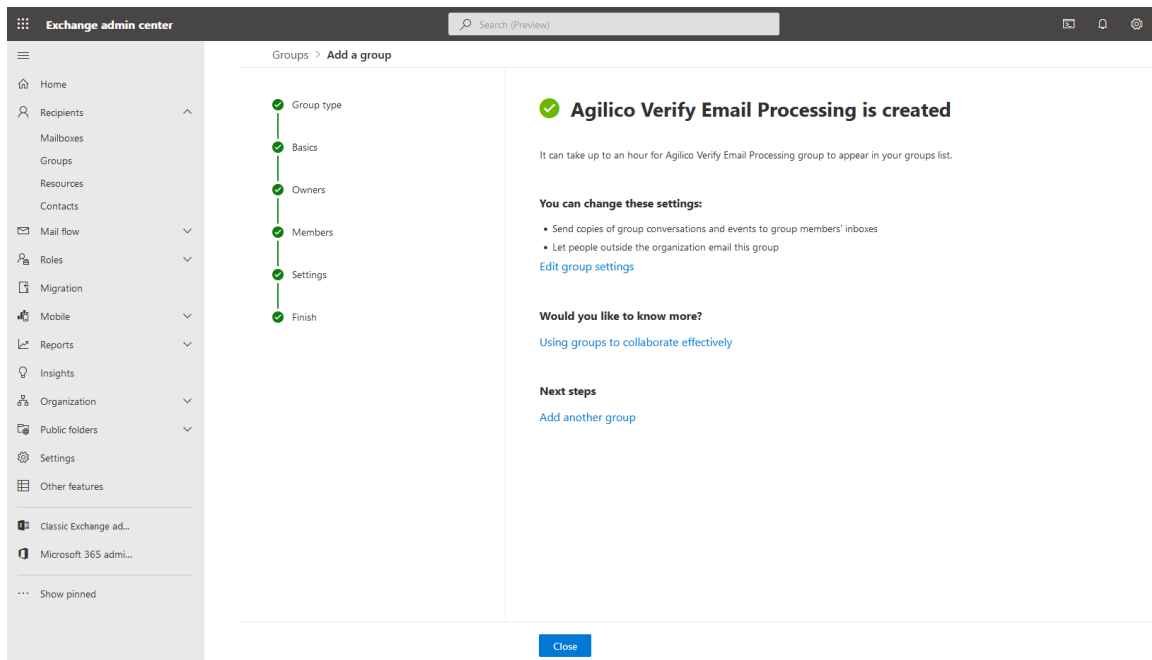
The group requires its own email address. This will not be used, so name it accordingly. It is recommended to:

- **Disable** “Allow people outside of my organisation to send email to 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 [redacted]
-----
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 feedback 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 [redacted] -PolicyScopeGroupId agilicoverifysecuritygroup@invu.net -AccessRight RestrictAccess
-Description "Restrict this Agilico Verify to members of the AgilicoVerifySecurityGroup distribution group."
-----
RunspaceId      : [redacted]
ScopeName       : Agilico Verify Email Processing
ScopeIdentity    : Agilico Verify Email Processing20220907073226
Identity        : [redacted]
AppId           : [redacted]
ScopeIdentityRaw : [redacted]
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.