MANUAL

MS AZURE APPLICATION REGISTRATION FOR EASY DISTRIBUTION

EASY SYSTEMS

PART OF 4CEE

Index

1 Introduction

This document shows you how to add and register an application using the App registrations experience in the Azure portal so that your app can be integrated with the Microsoft identity platform.

In this document the purpose for the application registration is for the reading mailboxes with the Easy Distribution application with the use of MS Graph API.

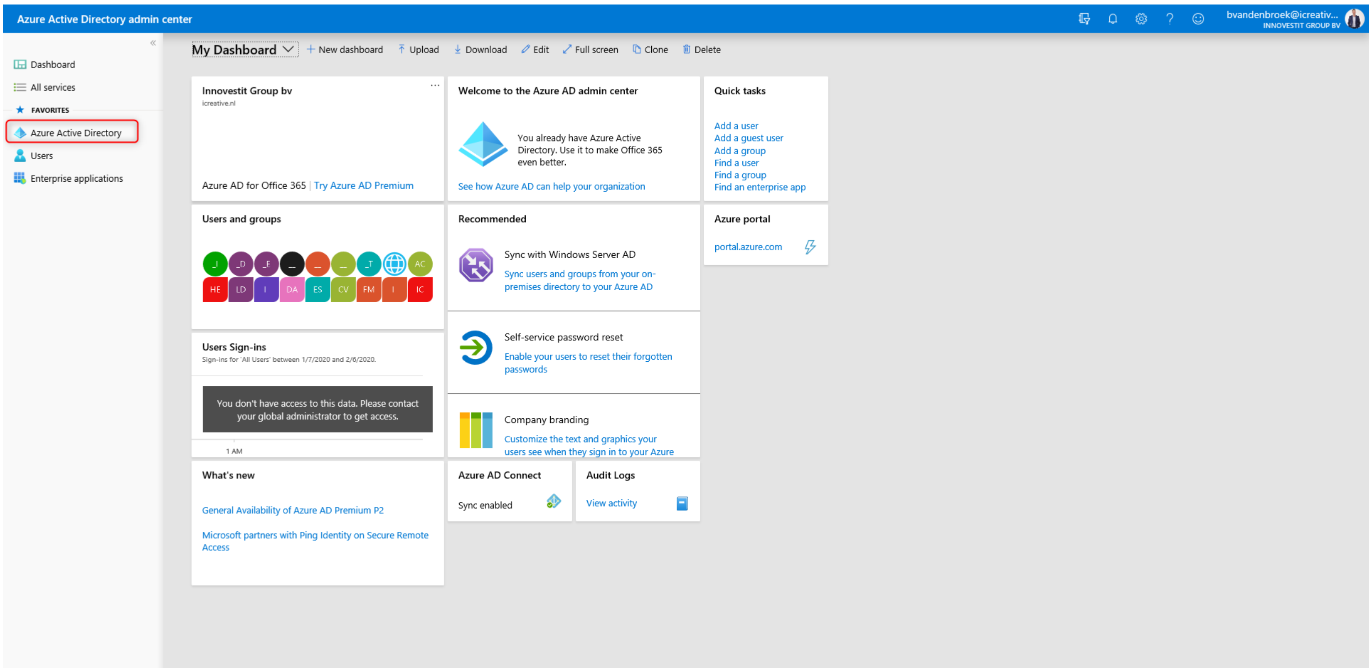
For more information regarding Azure applications usage in general please see:
https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app

For more information regarding the MS Graph API please see:
https://developer.microsoft.com/en-us/graph

2 Application registration steps

The following steps are needed for the registration of the Azure application. These are based on the usage of the Easy Distribution application for reading out mailboxes.

1. Log in to the Azure Active Directory admin center of your tenant with administrator privileges.
2. On the home screen go to: Azure Active Directory.



Innovestit Group bv
icreative.nl

Azure AD for Office 365 | Try Azure AD Premium

Welcome to the Azure AD admin center

You already have Azure Active Directory. Use it to make Office 365 even better.

See how Azure AD can help your organization

Quick tasks

Add a user
Add a guest user
Add a group
Find a user
Find a group
Find an enterprise app

Users and groups

Recommended

Sync with Windows Server AD
Sync users and groups from your on-premises directory to your Azure AD

Self-service password reset
Enable your users to reset their forgotten passwords

Company branding
Customize the text and graphics your users see when they sign in to your Azure

Azure portal
portal.azure.com

Users Sign-ins
Sign-ins for 'All Users' between 1/7/2020 and 2/6/2020.

You don't have access to this data. Please contact your global administrator to get access.

What's new

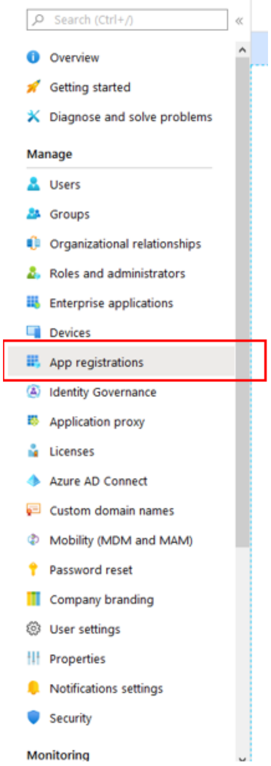
General Availability of Azure AD Premium P2

Microsoft partners with Ping Identity on Secure Remote Access

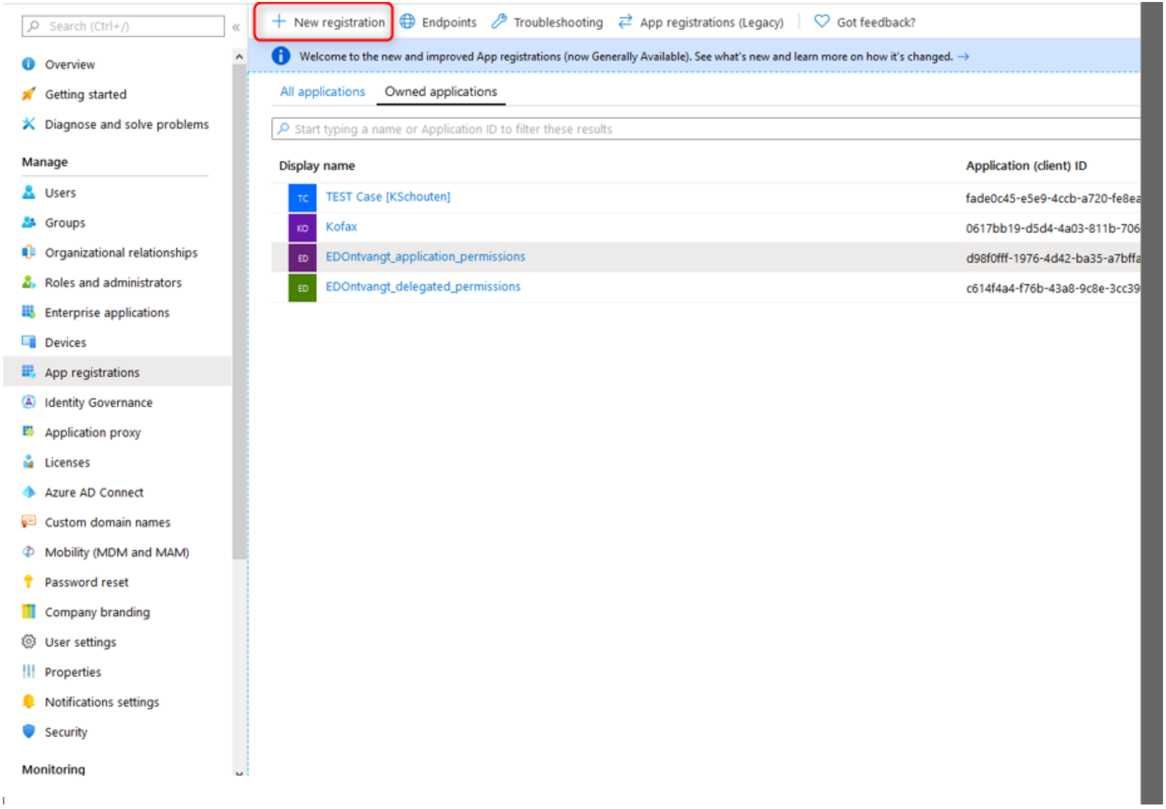
Azure AD Connect
Sync enabled

Audit Logs
View activity

3. On the left side navigate to “App registrations”.



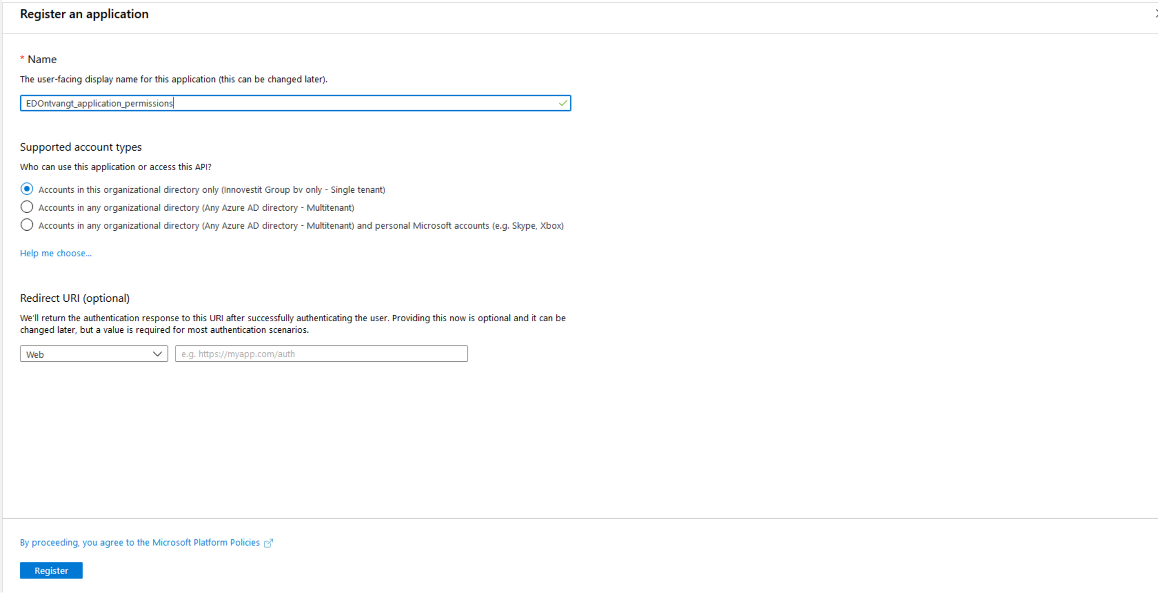
4. Click on “New Registration”



Welcome to the new and improved App registrations (now Generally Available). See what's new and learn more on how it's changed. →

Display name		Application (client) ID
TC	TEST Case [KSchouten]	fade0c45-e5e9-4ccb-a720-fe8ea
KO	Kofax	0617bb19-d5d4-4a03-811b-706
ED	EDOntvangt_application_permissions	d98f0fff-1976-4d42-ba35-a7bffa
ED	EDOntvangt_delegated_permissions	c614f4a4-f76b-43a8-9c8e-3cc39

5. Give the application a name (best practice would be to include the purpose of the application).
   Support accounts types should be set as shown below.
   Redirect URL is not needed for Easy Distribution.



Register an application

* Name

The user-facing display name for this application (this can be changed later).

EDOntvangt_application_permissions

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (Innovestit Group bv only - Single tenant)
○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)
○ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

Help me choose...

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

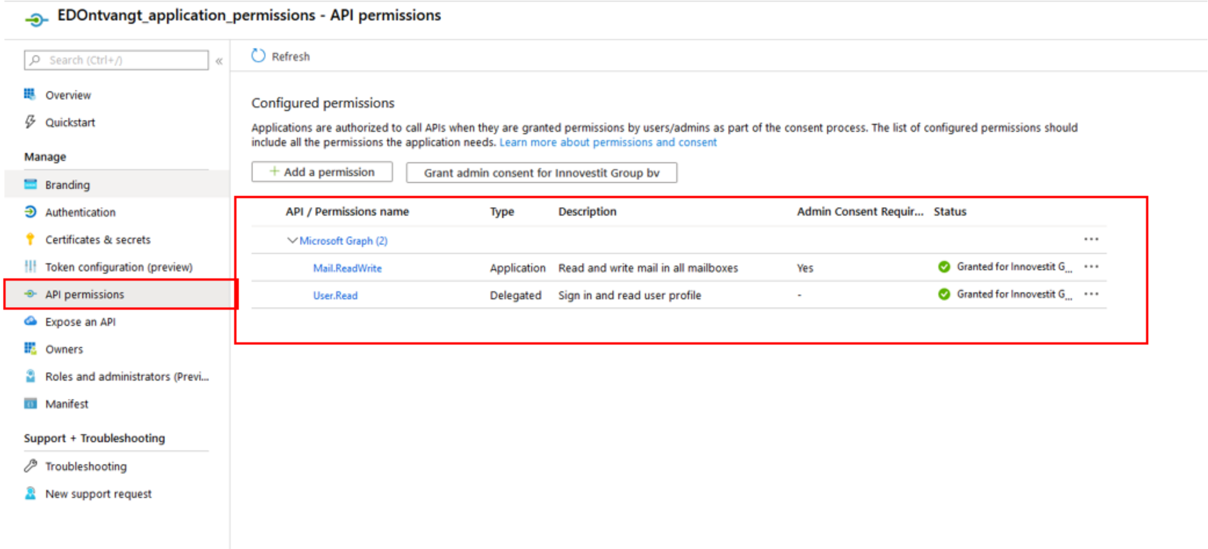
Web | e.g. https://myapp.com/auth

By proceeding, you agree to the Microsoft Platform Policies

6. Click on “Register”.

Now the application is created, we need to set the correct API permissions for the application. These are based on the permissions Easy Distribution will need for the read email process.

7. On the left-hand side go to “API permissions” and add the permissions as shown below:



EDOntvangt_application_permissions - API permissions

Configured permissions

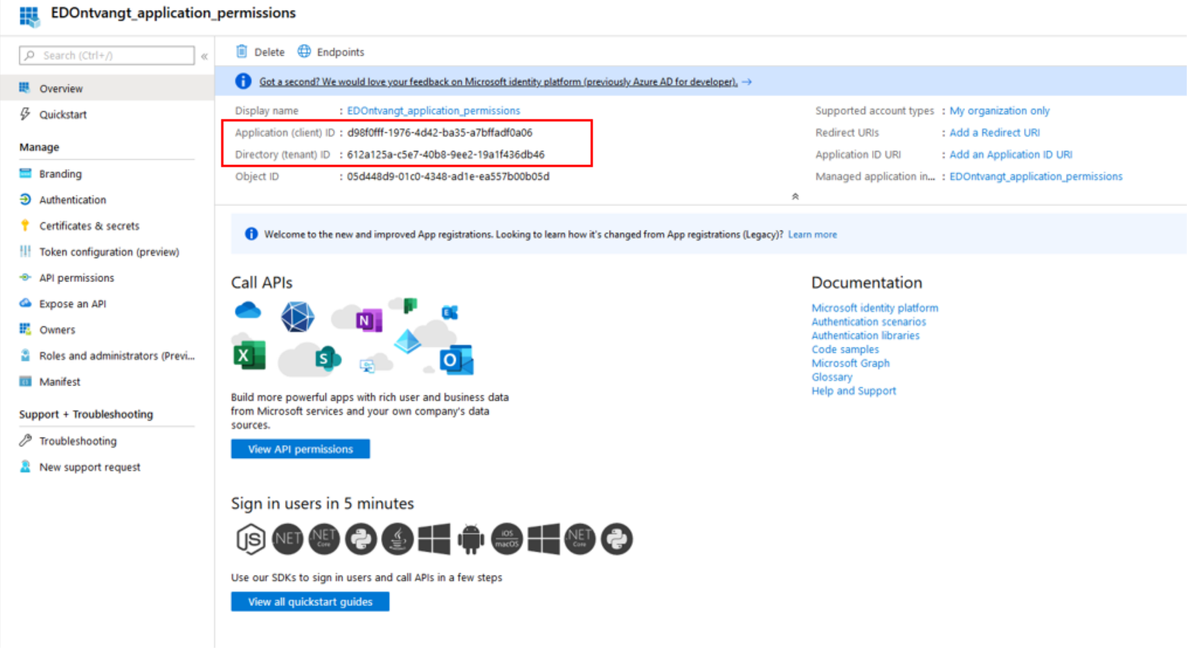
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description	Admin Consent Requir...	Status
Microsoft Graph (2)				
Mail.ReadWrite	Application	Read and write mail in all mailboxes	Yes	✓ Granted for Innovestit G...
User.Read	Delegated	Sign in and read user profile	-	✓ Granted for Innovestit G...

8. Admin consent is needed after adding these permissions. Use the button “Grant admin consent for <active directory name>” or if this step needs to be done by another administrator please forward this request.

9. Go the “Overview”

10. On this page please copy the values of “Application (client) ID” and “Directory (tenant)ID”. These values are needed by the consultant for the configuration of Easy Distribution.



Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Display name : EDOntvangt_application_permissions
Application (client) ID : d98f0fff-1976-4d42-ba35-a7bffadf0a06
Directory (tenant) ID : 612a125a-c5e7-40b8-9ee2-19a1f436db46
Object ID : 05d448d9-01c0-4348-ad1e-ea557b00b05d

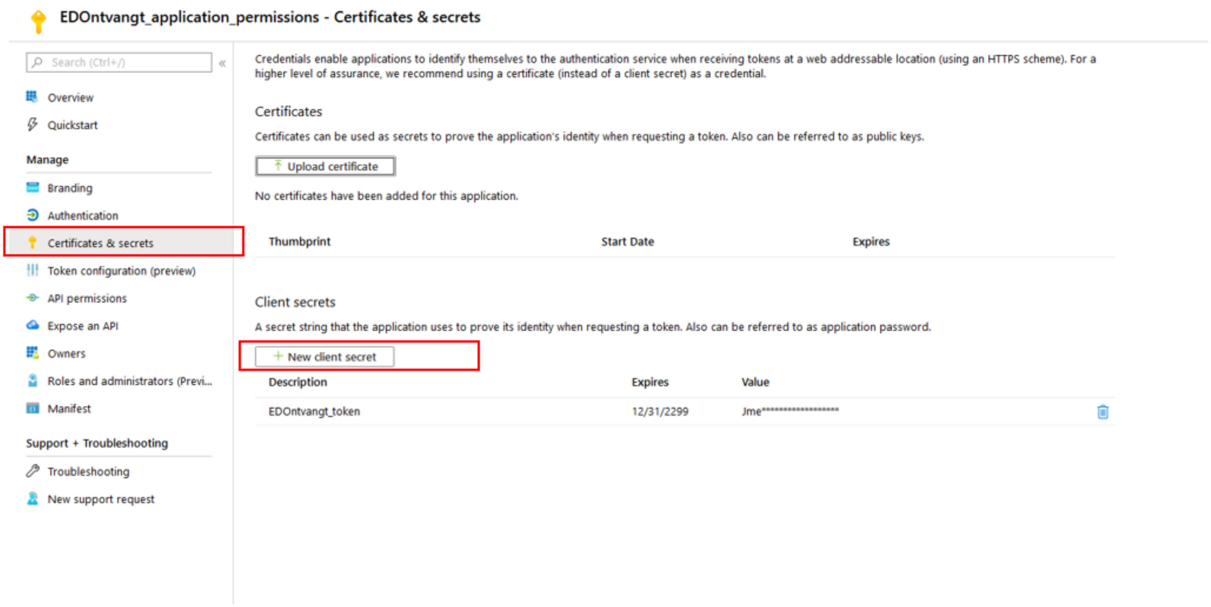
Supported account types : My organization only
Redirect URIs : Add a Redirect URI
Application ID URI : Add an Application ID URI
Managed application in... : EDOntvangt_application_permissions

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? Learn more

Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.

Use our SDKs to sign in users and call APIs in a few steps

11. Go to “Certificates & Secrets”



EDOntvangt_application_permissions - Certificates & secrets

Credentials enable applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

No certificates have been added for this application.

Thumbprint	Start Date	Expires

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value
EDOntvangt_token	12/31/2299	Jme******************

On this page a new Client secret must be created, this can be done with the button “New client secret”.

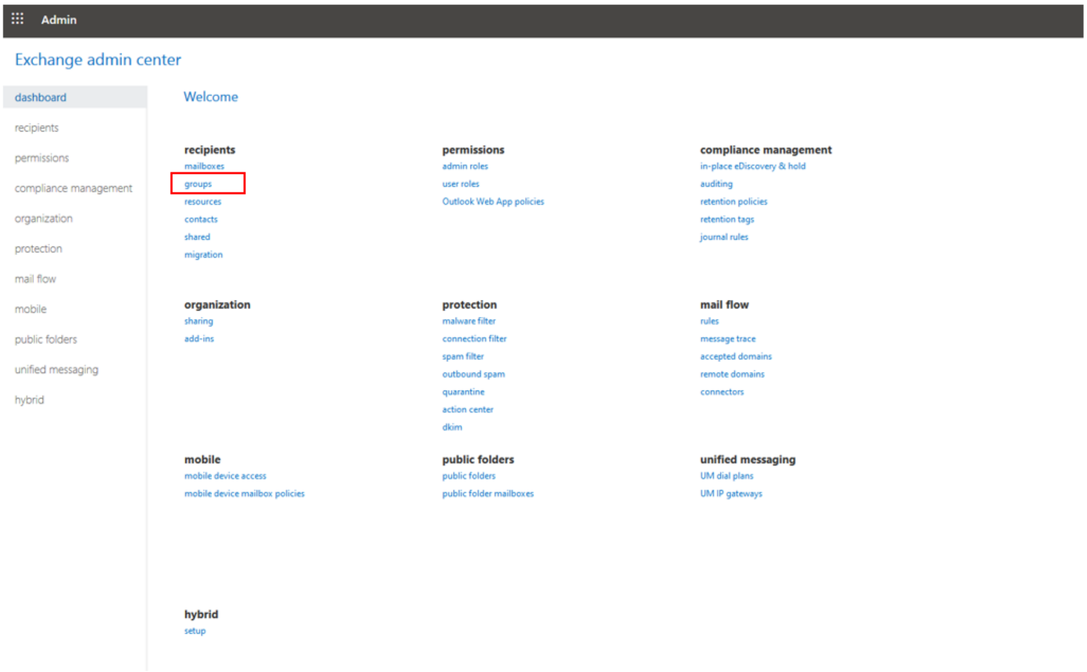
Important: Once this is created please copy this value and save this on a secure environment or password solution. This value is needed by the Easy Distribution consultant for the configuration!

The application registration process is now done.

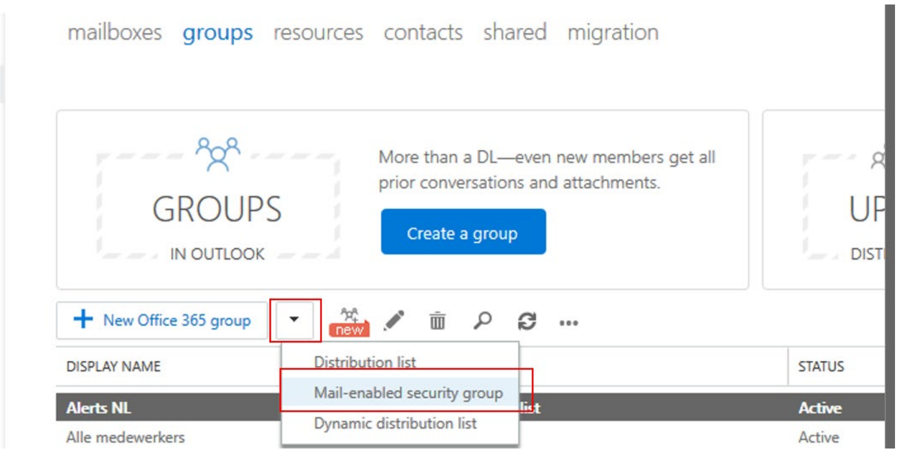
3 Exchange group configuration

For the mailboxes that Easy Distribution needs to read we need to create a new “Mail security group” in the Exchange Admin center.

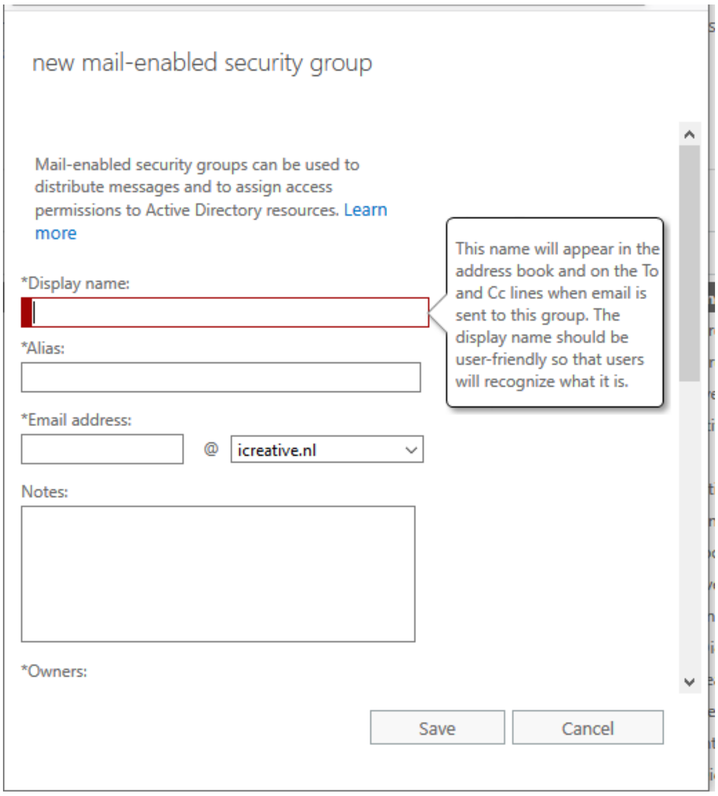
1. Log in to the Exchange admin center of your tenant with administrator privileges.
2. Go to “Groups” on the welcome page



3. Click on the arrow down button and select ”Mail-enabled security group”



4. Fill on the required fields on this page:



new mail-enabled security group

Mail-enabled security groups can be used to distribute messages and to assign access permissions to Active Directory resources. Learn more

*Display name:

*Alias:

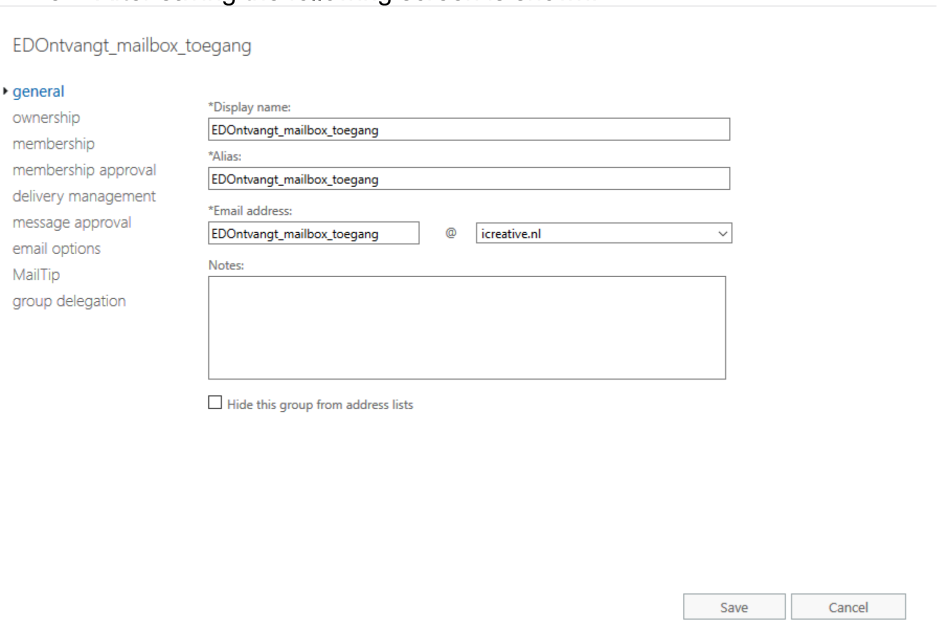
*Email address:
@ icreative.nl

Notes:

*Owners:

This name will appear in the address book and on the To and Cc lines when email is sent to this group. The display name should be user-friendly so that users will recognize what it is.

5. After saving the following screen is shown:



EDOntvangt_mailbox_toegang

*Display name: EDOntvangt_mailbox_toegang

*Alias: EDOntvangt_mailbox_toegang

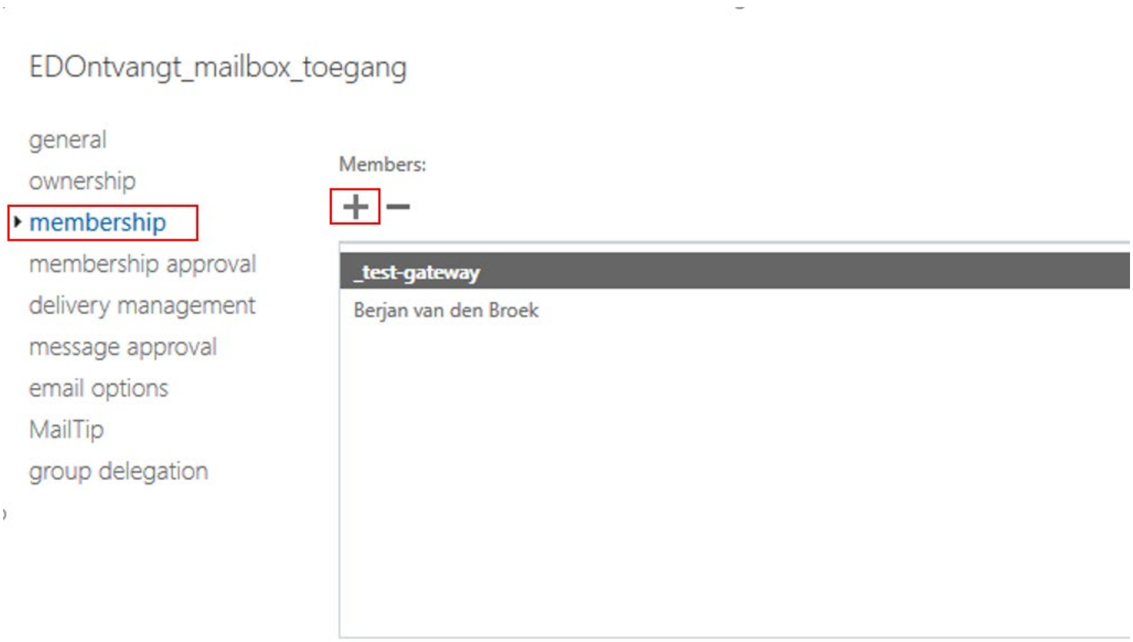
*Email address: EDOntvangt_mailbox_toegang @ icreative.nl

Notes:

□ Hide this group from address lists

Important: The value of the field “Alias” will be used later on, please save this value temporarily.

6. Navigate to “Membership”



EDOntvangt_mailbox_toegang

_test-gateway

Berjan van den Broek

7. With the “+” button you can. add Members to this mail security group.

Important: These members should contain all the users/mailboxes that Easy Distribution needs to read.

8. Finally click on “save”

4 Link Exchange group to application

Now we have created:

- Azure application with the correct API permissions. The following keys are saved and shared with the Easy Distribution consultant:
  - Application (client) ID
  - Directory (tenant) ID
  - Client secret
- Exchange mail security group with correct memberships (mailboxes needed for Easy Distribution)

The final step is to link (scope) the Application with the Exchange mail security group

1. For doing this we need to use the “Exchange Online PowerShell” tool.
   For more information of the general usage lease see:

https://docs.microsoft.com/en-us/powershell/exchange/exchange-online/connect-to-exchange-online-powershell/connect-to-exchange-online-powershell?view=exchange-ps

2. The statement that needs to be executed in Exchange Online PowerShell is:

   New-ApplicationAccessPolicy -AppId < Application (client) ID we just created> -PolicyScopeGroupId <Alias of mail security group we created> -AccessRight RestrictAccess -Description "<Description of the policy>”

For more information regarding this procedure please see:

https://docs.microsoft.com/en-us/graph/auth-limit-mailbox-access

In case of any questions please contact your Easy Systems Servicecenter

Tel no: +31 (0) 318 415 633.