

# Using modern authentication (OAuth2) as email authentication method with O365

**NOTE! O365 (Exchange Online) has some limitations with emails that can have affect to ESM's operation if not taken into account.**

1. Only IMAP and SMTP can be used with OAuth2
2. Authenticated SMTP limits outgoing emails to 30 messages per minute / 10,000 recipients per day (<https://docs.microsoft.com/en-us/exchange/troubleshoot/send-emails/smtp-submission-improvements>)

**The modern authentication described in this document is supported in ESM version 2021.1 and more recent versions.**

To configure modern authentication (OAuth2) instead basic authentication for the SMTP and IMAP protocols in ESM, we need to do three steps:

1. ESM needs to be registered as an approved application in the Azure Active Directory through Microsoft Azure portal
2. The registered application needs to be granted access for the O365 mailbox account used for Efecte
3. ESM platform settings need to be updated to be in sync with the Microsoft Azure settings

It is recommended to do steps 1-2 using the same O365 account the emails are read from to ESM. If not possible the application needs an Owner to be set up in the Azure AD.

## 1. Registering ESM as an Application in Microsoft Azure

### Prerequisites

- A Microsoft Azure account with an active subscription (the O365 email account to be used with ESM).
- An Azure tenant available under which you will register your application.

**For testing purposes you can follow these instructions to create a free azure account and tenant with your O365 email id:**


<https://azure.microsoft.com/en-us/free>

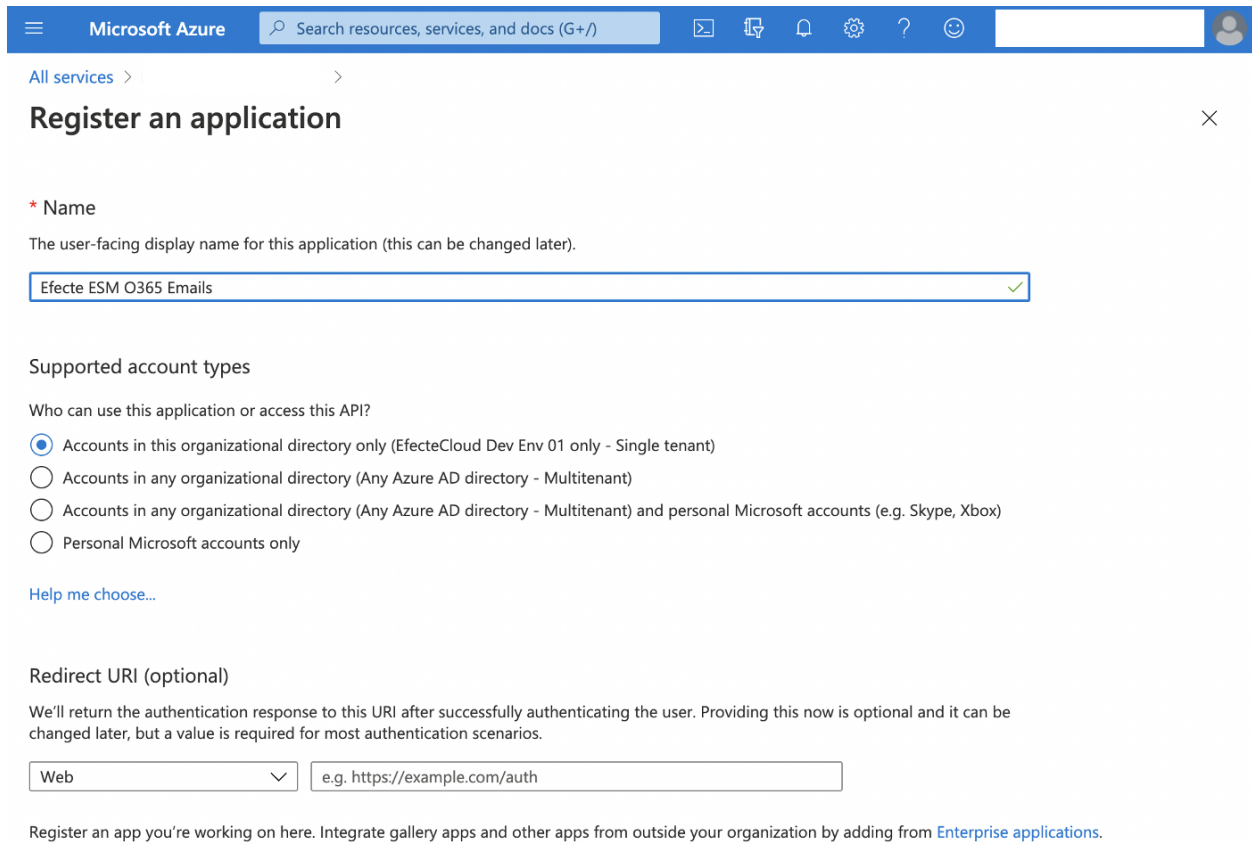
<https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-create-new-tenant>

# Register an application

Registering an application establishes the trust relationship between ESM and the Microsoft identity platform. The trust with registered application is unidirectional: application (ESM) trusts the Microsoft identity platform, and not the other way around. Trust is based on the id created in the registration process.

Follow these steps to create the app registration:

- Sign in to the Microsoft Azure portal (<https://portal.azure.com/>).
- If you have access to multiple tenants, use the **Directory + subscription** filter  in the top menu to select the tenant in which you want to register an application.
- Search for and select **Azure Active Directory**.
- Under **Manage**, select **App registrations** > **New registration**.
- Enter a **Name** for your application. Users of your app might see this name, and you can change it later.
- Specify who can use the application, sometimes referred to as the *sign-in audience*. For ESM, choose **Accounts in this organizational directory only** option
- Don't enter anything for **Redirect URI (optional)**.
- Select **Register** to complete the initial app registration.



Microsoft Azure Search resources, services, and docs (G+)

All services >

## Register an application

\* Name

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

Efecte ESM O365 Emails ✓

Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (EfecteCloud Dev Env 01 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)
- Personal Microsoft accounts only

[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://example.com/auth

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

When registration completes, the Azure portal displays the app registration's **Overview** pane, which includes its **Application (client) ID**. Also referred to as just *client ID*, this value uniquely identifies your application in the Microsoft identity platform.

The screenshot shows the Microsoft Azure portal interface. At the top, there's a navigation bar with the Microsoft Azure logo, a search bar, and various utility icons. Below the navigation bar, the page title is 'Efecte ESM O365 Emails'. A left-hand navigation pane lists various management options like Overview, Quickstart, Integration assistant, Branding, Authentication, etc. The main content area is titled 'Essentials' and displays key application information:

- Display name: Efecte ESM O365 Emails
- Application (client) ID: [Redacted]
- Directory (tenant) ID: [Redacted]
- Object ID: [Redacted]
- Supported account types: My organization only
- Redirect URIs: Add a Redirect URI
- Application ID URI: Add an Application ID URI
- Managed application in local directory: Efecte ESM O365 Emails


Below this, there are sections for 'Call APIs' (with a 'View API permissions' button) and 'Documentation' (with links to Microsoft identity platform, Authentication scenarios, etc.). At the bottom, it says 'Sign in users in 5 minutes'.

## 2. Add permissions to access the O365 mailbox

In order to send and receive emails from O365 mailbox with OAuth, we need to define API permissions scopes for the ESM application we previously registered to the Azure Active Directory.

### Delegated permission to Microsoft Graph

Configure delegated permission to Microsoft Graph to enable ESM to perform operations on behalf of the APP owners, for example reading or sending their emails.

- Sign in Microsoft Azure portal (<https://portal.azure.com/>).
- If you have access to multiple tenants, use the **Directory + subscription** filter  in the top menu to select the tenant containing your previously registered ESM application.

- Select **Azure Active Directory > App registrations**, and then select your client application (if not shown on the list, check that the page is showing **All applications**)
- Select **API permissions > Add a permission > Microsoft Graph**
- Select **Delegated permissions**. Microsoft Graph exposes many permissions, with the most commonly used shown at the top of the list.
- Under **Select permissions**, select the following permissions:

Permission	Description
IMAP.AccessAsUser.All	Read and write access to mailboxes via IMAP.
SMTP.Send	Send emails from mailboxes using SMTP AUTH.
openid	Sign users in
User.Read	Sign in and read user profile
offline_access	Maintain access to data you have given it access to

- Select **Add permissions** to complete the process.

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo, a search bar, and various utility icons. The main content area is titled 'Efecte ESM O365 Emails | API permissions'. A warning banner at the top states: 'You are editing permission(s) to your application, users will have to consent even if they've already done so previously.' Below this, the 'Configured permissions' section explains that applications are authorized to call APIs when granted permissions by users/admins. A table lists the configured permissions for the Microsoft Graph API:

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (5)				
IMAP.AccessAsUser.All	Delegated	Read and write access to mailboxes via IMAP.	-	...
offline_access	Delegated	Maintain access to data you have given it access to	-	...
openid	Delegated	Sign users in	-	...
SMTP.Send	Delegated	Send emails from mailboxes using SMTP AUTH.	-	...
User.Read	Delegated	Sign in and read user profile	-	...

At the bottom of the permissions list, there is a note: 'To view and manage permissions and user consent, try Enterprise applications.'

As an admin, you should also grant consent on behalf of all ESM Admin users, so they're not prompted to do so when they log into the mailbox. Admin consent is discussed in the next subchapter. If you define Admin consent beforehand, then the users who log into the mailboxes are not prompted to ask separately for Admin consent.

ESM admins should log in weekly to the email accounts that are read into ESM to check if the spam folder contains actual customer emails and move them to the folder from which the emails are fetched to ESM (usually inbox folder).

Also, admins should check for cases if emails are not fetched successfully into ESM. If there are large emails in the inbox that cannot be fetched into ESM, those should be moved into another folder to avoid errors.

## Admin consent button

The **Grant admin consent for {your tenant}** button allows an admin to grant admin consent to the permissions configured for the application. When you select the button, a dialog is shown requesting that you confirm the consent action.

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](#)

+ Add a permission  Grant admin consent for Contoso AD (dev)

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (1)				
Files.Read.All	Application	Read files in all site collections	Yes	⚠ Not granted for Contos... <span>⋮</span>

After granting consent, the permissions that required admin consent are shown as having consent granted:

+ Add a permission  Grant admin consent for Contoso AD (dev)

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (1)				
Files.Read.All	Application	Read files in all site collections	Yes	✅ Granted for Contoso AD... <span>⋮</span>

The **Grant admin consent** button is *disabled* if you aren't an admin or if no permissions have been configured for the application. If you have permissions that have been granted but not yet configured, the admin consent button prompts you to handle these permissions. You can add them to configured permissions or remove them.

The screenshot shows the 'Certificates & secrets' page in the Azure portal. The left sidebar contains navigation options like Overview, Quickstart, Integration assistant, Manage (Branding, Authentication, Certificates & secrets, Token configuration, API permissions, Expose an API, App roles | Preview, Owners, Roles and administrators | Preview, Manifest), and Support + Troubleshooting. The main content area is divided into two sections: 'Certificates' and 'Client secrets'. The 'Certificates' section has an 'Upload certificate' button and a note that no certificates have been added. The 'Client secrets' section has a 'New client secret' button and a table with one entry:

Description	Expires	Value	ID
changeme	1/13/2022	GRH*****	b185792d-51fb-4334-a60b-f79c5fab6335

## Authentication Settings

To enable ROPC authorization flow to work properly for the application and for ESM to Authenticate and get access tokens, we need to enable **Default Client type** setting (as shown in screen shot) in **Authenticate** → **Advance Settings**.

By default, the setting is set to No (confidential client). Updating it to **Yes** converts the default client type to public client. This is a very important step , if not done then you will see below error:- **AADSTS7000218: The request body must contain the following parameter: client\_assertion or client\_secret when authenticating to Azure AD.**

The screenshot shows the 'Authentication' page in the Azure portal. The left sidebar is similar to the previous screenshot. The main content area includes 'Platform configurations', 'Supported account types', and 'Advanced settings'. Under 'Supported account types', the 'Accounts in this organizational directory only (EfecteCloud Dev Env 01 only - Single tenant)' option is selected. The 'Advanced settings' section has a toggle for 'Allow public client flows' set to 'Yes'. Below this, there is a list of advanced settings:

- App collects plaintext password (Resource Owner Password Credential Flow) [Learn more](#)
- No keyboard (Device Code Flow) [Learn more](#)
- SSO for domain-joined Windows (Windows Integrated Auth Flow) [Learn more](#)

We have now completed the process of application registration and set up. After this we just have to add following platform settings in ESM to use above setup.

### 3. ESM Platform Settings

NOTE! These settings are additional settings for the basic authentication. If emails have not used in the environment before additional properties are needed

To set up ESM to use the OAuth2 endpoint we just created in the Azure portal for emails, please go to ESM admin view and navigate to *Maintenance > System settings > Edit Platform Settings*. Use the filter field to find the following mail settings one by one and set the following properties:

```
mail.store.oauth.enabled = true

mail.transport.oauth.enabled = true

mail.oauth.authorize.endpoint =
https://login.microsoftonline.com/{tenantID}/oauth2/v2.0/authorize

mail.oauth.client.id = {clientId}

mail.oauth.scopes =
https://outlook.office365.com/IMAP.AccessAsUser.All,https://outlook.office365.com/SMTP.Send
```

The clientId and authorize endpoint can be found from the Azure Active Directory frontpage for the application we registered for ESM. Please check below on how to get them.

The screenshot displays the Azure portal interface for an application named "ESM O365 Integration". On the left, a navigation pane lists various management options like Overview, Quickstart, and Authentication. The main content area shows the application's "Essentials" with fields for Display name, Application (client) ID, Directory (tenant) ID, and Object ID. A red box highlights the Application (client) ID: 46a6627b-0fed-4f72-a212-95216e5b0f28. On the right, the "Endpoints" section is expanded, listing various OAuth and OpenID Connect endpoints. A red box highlights the "OAuth 2.0 authorization endpoint (v2)" with the URL: https://login.microsoftonline.com/b921b89c-a960-4187-9872-28191e34a8f3/oauth2/v2.0/authorize. A "Copy to clipboard" button is visible next to this URL.

Please note that mailtasks use the settings configured in their properties. In case connection and authentication settings have been defined in in the mailtask properties (instead of defining them centrally in platform settings for all mailtasks), please set the settings listed above directly into the mailtask properties for each mailtask.

**References:**

<https://docs.microsoft.com/en-us/exchange/client-developer/legacy-protocols/how-to-authenticate-an-imap-pop-smtp-application-by-using-oauth>

<https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app>

<https://docs.microsoft.com/en-us/azure/active-directory/develop/msal-authentication-flows>

<https://blogs.aaddevsup.xyz/2020/09/whats-the-security-implication-of-changing-the-default-client-type-from-confidential-to-public-in-azure-ad/>