# **O365 Client Credentials flow - Email Authentication**

### Contents

- Contents
- Introduction
- For Azure administrators
  - Application creation
  - Application registration and permissions
     Application secret
- For ECS organization administrators/implementers
  - Configure a mailbox
- Migrating from On behalf Of to Client Credentials / Hybrid application

### Introduction

As Microsoft has started to turn of Basic authentication for email protocols for tenants in favor of Modern Authentication (OAuth2) we have implemented one form of this for ECS email using an interactive flow, see also: O365 On Behalf Of - Email Authentication

This was done, because it was the quickest way for us to prevent users being unable to use email anymore, but it is not the optimal solution. We now have implemented the client credentials flow, which requires no user interaction and uses Microsoft Graph for email handling instead of STMP and IMAP.

The benefit for administrators/users is that there only needs to be one client secret provided in the Azure App which then needs to be configured in ECS once and then **all the tenant's mailboxes** can be used in ECS by just adding them to the ECS configuration. If there needs to be a restriction on allowed mailboxes, this can be controlled entirely by the Azure admin. For more information about this, please see: Limi ting application permissions to specific Exchange Online mailboxes

Also, the expiration is controllable on Azure side and can be set to a maximum of two years (at the time of writing), meaning that when it works, the ECS configuration only needs to be updated once every two years when a new secret needs to be issued. In comparison, the interactive flow needs a guarterly update, involving user interaction and (most likely) a MFA input - per mailbox!

#### All mailboxes are accessible

We emphasize again that all the tenant's mailboxes are available by default, you probably want to limit access in Azure to only the mailboxes you actually need in ECS.

For more information about this, please see: Limiting application permissions to specific Exchange Online mailboxes

### For Azure administrators

In Azure Active Directory you need to have an application that supports mail using MS Graph with a client secret available.

### **Application creation**

If you do not have the application set up yet, create one (else, proceed to add permissions or adding secrets as needed):

Azure Active Directory admin	center							
≪ ⊠ Dashboard S <sup>h</sup> ).	Dashboard > Enterprise applications Enterprise applicat Code Data Data Data	Dashbaard > Enterprise applications Thrterprise applications   All applications						
All'Services     All'Services     Favorites	evolve IP - ELS Development - Azure A	+ New application O Refresh 🞍 Downle	aad (Export) 🔰 🚺 Preview info 📄 🇮 Columns 📗 🔤	Preview features R Got feedback?				
Azure Active Directory     Users     Starryise applications	Overview     Overview     Diagnose and solve problems	View, filter, and search applications in your organization that are set up to use your Azure AD tenant as their Identity Provider. The list of applications that are maintained by your organization are in applications.						
	Manage	<ul> <li>Search by application name or object ID</li> <li>10 applications found</li> </ul>	Application type == Enterprise Applications X					
	Application proxy	Name	↑↓ Object ID	Application ID	Homepage URL	Created on		
	User settings	MD MT Demo too (Server mail)	32f33cf1-1f46-4985-a8d3-2f53aecba2d8	fcb35209+6aff+4aea+88b0+ec605e70be76		12/6/2022		
	App launchers	TE TestReg	46a6f89b-5d7d-4810-9f81-bcf3346fb53e	a83452c5-21d3-4e72-9d15-0f0c55e84e42	https://account.activedirectory.windowsazure.com:444/.	2/15/2023		
		ET ECS Test app	86bab196-178e-465a-a36f-9fd96531e62a	9edf26ef-7683-49e5-8899-e0b650ca8539		6/15/2022		
	Conditional Access	PO Postman	882a3dc4-f524-459d-8309-98f6ef546bce	ef3df4e3-d894-429f-bb0d-b7bb59699c25		6/21/2022		
	Concent and nermissions	TS Tutorial Sample App	965b172a-6fa9-4a99-8321-7bf0dd8debe8	6731de76-14a6-49ae-97bc-6eba6914391e		10/3/2022		
		MD MT Demo	ae67b24f-09f0-40dd-a88c-7f277e549b5f	91e54e2d-eb7e-456f-ab89-16316e207741		12/6/2022		
	Activity	Graph Explorer	b5ab5260-64ea-4396-b14f-89046c487b28	de8bc8b5-d9f9-48b1-a8ad-b748da725064	https://developer.microsoft.com/graph/graph-explorer	6/14/2022		
	Sign-in logs	ECS 0365 Mail Test On Behalf Of	ca0e91c8-be94-44f2-af08-a8dcc194b20f	9098be66-bcb4-49fa-b992-9b1f117efc27	https://account.activedirectory.windowsazure.com:444/.	10/3/2022		
	M Usage & insights	00 O365 On Behalf Of	d3e63072-35a1-4eed-b724-fc10080c9d21	7e598f54-35e3-42c3-a9fc-1aa006761acf	https://account.activedirectory.windowsazure.com:444/.	11/10/2022		
	Audit logs	ECS 0365 Mail Test - App	de9db444-1e58-4e2a-a799-6044cda05040	0bcb6009-a764-4d32-8da3-e024aeaed6ba	https://account.activedirectory.windowsazure.com:444/.	10/3/2022		
	Access reviews							
	Admin consent requests							
	Buik operation results							
	Troubleshooting + Support							
	New support request							

- Go to "Enterprise applications"
   Select "+ New application"

Azure Active Directory admin o	enter				
<ul> <li>Cashboard</li> <li>All services</li> <li>FAVORITES</li> <li>Azure Active Directory</li> <li>Users</li> </ul>	Dashboard > Enterprise applications   All applications >         Browse Azure AD Gallery         + Create your own application         R         Got feedback?    The Azure AD App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automated use into the Azure AD Gallery for other organizations to discover and use, you can file a request using the process described in this article.				
Enterprise applications	Enterprise applications  Single Sign-on : All User Account Management : All Cloud platforms				
	Amazon Web Services (AWS)	Google Cloud Platform	or		

1. Then select "+ Create your own application"

Create your own application				
🖗 Got feedback?				
If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.				
What's the name of your app?				
O365 Email Client Credential Demo				
<ul> <li>What are you looking to do with your application?</li> <li>Configure Application Proxy for secure remote access to an on-premises application</li> <li>Register an application to integrate with Azure AD (App you're developing)</li> <li>Integrate any other application you don't find in the gallery (Non-gallery)</li> </ul>				

Give it a logical name so you or others can easily identify it in the future and select the correct application type, for us it is "Integrate any other... ".

### Application registration and permissions

Now go to the application registration page.

Azure Active Directory admin	center		6	4 🖗 © 0 R	0					
«	Dashboard > Evolve IP - ECS Developm	ent								
Deshboard     All services	Evolve IP - ECS Dev	Evolve IP - ECS Development   App registrations * ×								
* FAVORITES	«	+ New registration 🔀 Endpoints 🧷 Troubleshooting 🜔 Refresh 🞍 Download 🗔 Preview features 🛛 🕂 Got feedback?								
Azure Active Directory	0 Overview									
Lusers	Preview features	() Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security update	is but we will no longer provide feature updates. Applications will need to be upgraded to Micro	soft Authentication Library (MSAL) and P	Microsoft Graph. Learn. ×					
Enterprise applications	X Diagnose and solve problems	more								
	Manage									
	👗 Users	All applications Dwited applications Deleted applications								
	🚨 Groups	P Start typing a display name or application (client) ID to filter these r								
	External Identities									
	<ol> <li>Roles and administrators</li> </ol>	6 applications found	Application (client) ID	Created on \$1	Contificator & correte					
	Administrative units	A Second Se		10/2/0002	O Current					
	Delegated admin partners		00 3003	10/3/2022	Current					
	Enterprise applications	Color of the fact of behavior	91 27	10/3/2022	Current					
	Devices		96 339	6/15/2022	Current					
2	App registrations		10 76	12/6/2022	· · · · · · · · · · · · · · · · · · ·					
-	Identity Governance	S Oso Bian Cient Credenta Deniu 3	30475cbd-6091-4dec-9720-76cfb9e18ase	3/2/2023						
	Application proxy		120	11/10/2022						

- 1. Select "Azure Active Directory" in the main menu
- 2. Select "App registrations" in the sub menu
- 3. As you can see here, the application does not have a secret yet. (far right column)
- Now select the application by clicking the name, this will bring you to the application overview page.

#### Application id

Also take note of the application id, this is part of the configuration we need. You can copy it now for later use. or from the application overview page which might be easier since it has copy buttons next to the id. In our example this is "a0475c6d-6091-4dec-9720-76cfb9e18a8e"

#### From this page (after you copied the application id and pasted it somewhere) we will add the needed permissions:



- 1. Select "API permissions"
- 2. Select "+ Add a permission"
- 3. Select "Microsoft Graph"

#### On the API sidebar:

Request API permissions	>
All APIs           Microsoft Graph           https://graph.microsoft.com/	1
What type of permissions does your application requir Delegated permissions Your application needs to access the API as the signed-in use	e? Application permissions er. Your application runs as a background service or daemon without a signed-in user.
Select permissions	expand
Permission	Admin consent required
✓ Mail (2) Mail.Read ① Decidenci i in all scalesce	
Mail.ReadBasic ① Read basic mail in all mailboxes	Yes
Mail.ReadBasic.All ① Read basic mail in all mailboxes	Yes
Mail.ReadWrite ① Read and write mail in all mailboxes	Yes
Mail.Send ① Send mail as any user	Yes

1. Select "Application permissions"



For the next step note that you can do a partially search for "mail." in the search box as show in the screenshot.

2. Select both:

- a. Mail.ReadWrite
- b. Mail.Send

Dashboard > O365 Email Client Credent	Dashboard > O365 Email Client Credential Demo				
<sub> -</sub> O365 Email Client C	redential Demo   A	PI permis	sions 🖈 …		
> Search «	C Refresh   Xr Got feedb	аск?			
Overview	A You are editing permission(s	) to your applicatio	on, users will have to consent even if they've already o	done so previously.	
🗳 Quickstart					
💉 Integration assistant					
Manage	1 The "Admin consent require	d" column shows tl	he default value for an organization. However, user co	onsent can be customized per permissio	on, user, or app. This column may not reflect the value
🔤 Branding & properties	Confirmed a series in a				
Authentication	Applications are authorized to ca	II ADIs when they	are granted permissions by users (admins as part	of the concept process. The list of c	opfigured permissions should include
📍 Certificates & secrets	all the permissions the application	n needs. Learn mo	ore about permissions and consent	of the consent process. The list of the	oningarea permissions snoula include
Token configuration	🕂 Add a permission 🗸 Gra	ant admin consent	t for Evolve IP - ECS Development		
API permissions	API / Permissions name	Туре	Description	Admin consent requ	Status
Expose an API	∽ Microsoft Graph (2)				
App roles	Mail.ReadWrite	Application	Read and write mail in all mailboxes	Yes	▲ Not granted for Evolve I •••
A Owners	Mail.Send	Application	Send mail as any user	Yes	▲ Not granted for Evolve I, ••••
Roles and administrators					
0 Manifest	To view and manage consented p	ermissions for inc	dividual apps, as well as your tenant's consent set	ttings, try Enterprise applications.	
Support + Troubleshooting					
Troubleshooting					
New support request					

When you confirm your permissions you should see they are added, but not have not been granted access yet. You can grant access here by clicking on the "Grant admin consent for..." title.

### **Application secret**

We now are ready to create a secret we can use in ECS to get access to the mailboxes.

### (i) Expiration

If the secret is about to expire or is already expired, return here to create a new secret. You will of course need to update ECS configuration afterwards as well in order to use the new key.

Azure Active Directory admin center								
«	Dashboard > O365 Email Client Credentia	al Demo						
📶 Dashboard	🔶 O365 Email Client Cr	edential Demo   Certifi	cates & secrets	\$				
I All services	•	•						
* FAVORITES		« R Got feedback?						
Azure Active Directory	Overview							
Lusers	🗳 Quickstart	Quickstart Credentials enable confidential 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.						
Enterprise applications	applications 🚀 Integration assistant							
Manage						×		
	Branding & properties	Application registration certificates, secrets and federated credentials can be found in the tabs below.						
	Authentication	ets Certificates (0) Client secrets (0) Federated credentials (0) A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.						
1	📍 Certificates & secrets							
-	Token configuration							
	→ API permissions	+ New client secret						
	🛆 Expose an API	Description	Expires	Value 🛈	Secret ID			
	App roles	No client secrets have been created for th	nis application.					
	A Owners							
	& Roles and administrators							
	Troubleshooting							
	New support request							

- 1. In the submenu select "Certificates and secrets"
- 2. Select "+ New client secret"

On the client secret sidebar:

Add a client secret		×
Description	ECS access for Dev Org	
Expires	Custom	$\sim$
Start End	Recommended: 180 days (6 months) 90 days (3 months) 365 days (12 months) 545 days (18 months)	
	730 days (24 months)	
	Custom	Ŀ

- Give it a logical description so you or others can easily identify it in the future
  Select the desired expiration, using the "custom " option you can also set a start date if desired

When the secret is generated you will see its value on the page.

#### Only chance to copy 0

Be aware that this is the **only** chance to copy the secret's value, if you navigate away and return it is no longer visible or copyable and you will need to generate a new secret!

Azure Active Directory admin center						
«	Dashboard > O365 Email Client Credent	tial Demo				
Dashboard All services	O365 Email Client Credential Demo   Certificates & secrets					
★ FAVORITES	₽ Search «	🖗 Got feedback?				
Azure Active Directory	Overview					
Lusers	📣 Quickstart	$\textcircled{\ }$ Got a second to give us some feedback? $\rightarrow$				
Enterprise applications	Integration assistant Manage     Branding & properties	Credentials enable confidential 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.				
	<ul> <li>Authentication</li> </ul>	Application registration certificates, secrets and federated credentials can be found in the tabs below.     X				
	📍 Certificates & secrets					
	Token configuration	Certificates (0) Client secrets (1) Federated credentials (0)				
	API permissions	A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.				
	<ul> <li>Expose an API</li> <li>App roles</li> </ul>	+ New client secret values cannot be viewed, except for immediately after creation. Be sure to save the secret when created before leaving the page.				
	A Owners	Description Expires Value In Secret ID				
	& Roles and administrators	ECS access for Dev Org 3/1/2025 bmg rbwv 🖸 5570aa7				
	III Manifest					
	Support + Troubleshooting	Make sure to copy				
	Troubleshooting	the secret				
	New support request					

- Use the copy button to copy the secret's value the ID is not relevant.
- Paste it somewhere for later reference

## For ECS organization administrators/implementers

When the Azure part is set up correctly, the mailboxes can be configured.

### **Configure a mailbox**

This step is much simpler than the interactive flow, open the organization's setup and then navigate to the email adapter:

	New Channel New Business Process New Agent Bulk Operations									
	🚡 🎭 Deployment 🕨 🄥 Email Adapter 1 🙎									
603	Supported Media									
6.5	Email Fax	Enul Fox								
SETUP	OAuth2 / Modern Authentication									
JETOP	About email authentication	Application Id / Client Id	Client Secret 4							
Blocked 🔒 🔕	Please see the nerp on the mailboxes tibe bar for decails about authentication.	a04/5cbd-6091-4dec-9720-76ctb9e18a8e								
📎 😨 🗢 🔿			- Incoming Emails							
🗄 🚵 🛡 🗸 ( 🗑 👘	Email Domain *	IMAP Server *	IHAP Port *	IMAP Requires SSL *						
Source: Delta User: Anonymous	eipecs.onmicrosoft.com	imap.gmail.com	993	S Yes						
Role: Admin Mode: Organization Admin	Haiboxes *									
Env: Dev Ernst	Authentication 0365 Client Credentials									
	User Name * @elpecs.onmicrosoft.com									
Search (0) ^	EndPoint * 🖉 200 (_Dutch Devving??) -									
Go Find on comen-	Usea for raxes Unity " 🖉 Disabled	Text Incoming Empir	×							
Michael (2)		MAP Server iman amail.com IMAP Port 993 Final Domain e	iners annirrasoft com							
Invalid (0)		Select Account:								
		Authentication: 0365 Client Credentials								
Subsystems ^		User Name:								
11 Aurin Structure	Outgoing Email Mode *	9								
<pre>spi bosiness subcibile</pre>	Client SMTP Server	Success! Number of Unrea	ad Emails: 2							
2 Staffing			ОК							
Definition	SMTP Server *			SMTP Requires SSL/TLS *						
	sinp.gmail.com	Get Unread Emails Count 8	Apply Cancel	V Yes						
	SMTP SSL/TLS Hode *									
Ceployment			LOS ENTR Carrier							
Resources										
Cronsimilian defaulte	Default From Email Address	Default Bcc Email Address								
			Email Tasta							
Virganizations			Email rests							
	7 Test incoming emails Test outgoing emails 10									
	End Briefe *									

- 1. Select "Deployment"
- 2. Select the email adapter (selection itself not shown in the screenshot, only the result, but it is under deployment software services email adapter)
- 3. Fill out the application id of your Azure application, in out example it is "a0475c6d-6091-4dec-9720-76cfb9e18a8e"
- 4. Paste the secret of your Azure application. In case you forgot to copy it earlier, you will need to create a new secret.
- 5. Fill out the domain, this is used as tenant identifier for logging in in Azure, which should normally match the domain of your user.

### Other users

Note that you can have other users, but in that case they need to have been imported into your Azure Active Directory

- 6. Create a mailbox using "O365 Client Credentials" and the username of the mailbox you want to use
- 7. Select the "Test incoming emails" button
- 8. Select "Get unread emails count"
- 9. If configured correctly, you should see this window.
- Note that it can show 0 (zero), that depends on actual unread emails in the mailbox, but that will still mean the configuration works
- 10. Optionally you can also send out a test email

If the configuration works you can optionally add more mailboxes and then deploy the configuration.

### Migrating from On behalf Of to Client Credentials / Hybrid application

If you already are using the interactive flow, it should be fairly easy to migrate/upgrade to the client credentials flow. Since the application is already present, you can add the permissions and secrets as described above and as long as you do not remove the original API permissions you are able to use both types in ECS.

A hybrid configuration on Az	ure would look something	g like this:			
ECS O365 Mail Tes	t - Hybrid App   API	permissio	ns 🖈 …		
₽ Search «	🖔 Refresh 🕴 🖓 Got feedb	ack?			
Overview	A You are editing permission(s	;) to your applicatio	n, users will have to consent even if they've already done so p	eviously.	
🗳 Quickstart	· · · · · · · · · · · · · · · · · · ·				
💉 Integration assistant					
Manage	1 The "Admin consent require	d" column shows th	e default value for an organization. However, user consent ca	n be customized per pern	nission, user, or app. This column may not reflect the val
Branding & properties					
Authentication	Configured permissions	II a Dia sub an Abass		The Vet	-for affering the environment of the state
Certificates & secrets	all the permissions the application	n needs. Learn mo	re about permissions by users/admins as part of the co re about permissions and consent	onsent process. The list	of configured permissions should include
Token configuration	+ Add a permission 🗸 Gra	ant admin consent	for Evolve IP - ECS Development		
API permissions	API / Permissions name	Туре	Description	Admin consent	requ Status
Expose an API	✓ Microsoft Graph (5)				
App roles	1 IMAP.AccessAsUser.All	Delegated	Read and write access to mailboxes via IMAP.	No	✓ Granted for Evolve IP - E ***
A Owners	Mail.ReadWrite 2	Application	Read and write mail in all mailboxes	Yes	✓ Granted for Evolve IP - E ***
& Roles and administrators	Mail.Send	Application	Send mail as any user	Yes	♂ Granted for Evolve IP - E ***
0 Manifest	4 offline_access	Delegated	Maintain access to data you have given it access to	No	Granted for Evolve IP - E ***
Support + Troubleshooting	5 SMTP.Send	Delegated	Send emails from mailboxes using SMTP AUTH.	No	✓ Granted for Evolve IP - E <sub></sub> ***
7 Troubleshooting					
New support request	Other consistent constant	for Evolve ID	ECS Davelonment		

- The permissions 1, 4 & 5 are set for the "on behalf of" interactive flow as can be seen by the Type "Delegated".
- Permissions 2 & 3 are for the client credentials flow, Type "Application".
- \rm Note the warning above, on changes it may be necessary for users to give consent again, meaning acquiring a new token and following the • popup guidelines

In ECS setup, a hybrid configuration would look like:

	New Channel New Business Process New Agent Bulk Operations							
	🎍 💁 Deployment 🕨 🔥 Email Adapter 1							
Sec.	Supported Media							
2.2	Email Fax							
		OAuth2 / Mode	rn Authentication					
SETUP	About email authentication	Application Id / Client Id	Client Secret 2					
	Please see the help on the mailboxes title bar for details about authentication.	0bcb6009-a764-4d32-8da3-e024aeaed6ba	••••••					
		Incomi	ng Emails					
🔚 🖓 🥃 🗸 🛛 🕃 🛅	Email Domain *	IMAP Server *	IMAP Port *					
Source: Delta	eipecs.onmicrosoft.com	outlook.office365.com	993					
Role: Admin	Mailboxes *							
Mode: Organization Admin Env: Dev Ernst		ß						
	Authentication 0365 On Behalf Of							
Search (0)	Authentication	0365 Client Credentials -						
Search (0)	Token Status	(Delpecs.onmicrosoft.com						
Go	Remove token (log out)	w * O Disabled						
Find on screen »	Lised For Faxer Only * (2) Disphore	- Disabled						
Visited (2) v	Used For Faxes Unity - 🚫 Disabled							
Invalid (0) v								
		Outaoi	ng Emails					

- The application id (1) remains the same.
- The new client secret is added (2).
  Mailbox A is using a token, but note that if all settings are correct we could just change authentication type.
  Mailbox B is using the client credentials flow.