

# Microsoft 365 – Managed Authentication (OAuth2)

Microsoft requires third-party applications, that want to interact with Microsoft 365 (Office 365) IMAP services, to use an access token for authenticated connection requests. The Incisive application will automatically recognise whether the Microsoft account is configured to only allow 'Managed Authentication' connections.

You need to register the Incisive application in your Azure Active Directory tenancy that hosts your Exchange Online and grant it permissions. The AppID and Secret Value, of the app you register, are required for SPM/PHM to access the Microsoft 365 account.

**Requirements:** 

- Ensure you are running SPM/PHM version 412.4 or newer
- Edge, Safari, Chrome or Firefox browser not Internet Explorer

The steps are:

- Register the 'Message Centre' as an App
- Assign Users & Groups to the App
- Assign Permissions to the App
- Create a Secret
- Enter the App ID and Secret into the Incisive program
- 1. Log in to the Azure portal tenancy, that provides the Microsoft 365 service, with an Administrator account.
- 2. Go to Identity > Enterprise Applications
- 3. Create a new Application.
  - a. Choose '+ New Application'
  - b. Choose '+ Create your own application'

Call it something like '**Message Centre** - *practice/hospital name*' (so it can be identified when Granting Consent). The actual name is not important.

Create your own application $\times$		
🖗 Got feedback?		
If you are developing your own application, u application that is not in the gallery, you can	sing Application Proxy, or want to integrate an reate your own application here.	
What's the name of your app?		
Message Centre - Incisive Medical	✓	
What are you looking to do with your applica	tion?	
O Configure Application Proxy for secure remote access to an on-premises application		
Register an application to integrate with Azure AD (App you're developing)		
<ul> <li>Integrate any other application you don't find in the gallery (Non-gallery)</li> </ul>		

- i. Choose the option to 'Integrate any other application...'
- ii. Click on the 'Create' button at the bottom

The 'Application ID' (App ID) will now be displayed. You'll need this Application ID number in SPM/PHM



- 4. Assign Users & Groups to the Application
  - a. Go to Identity > Enterprise Applications > Users and groups then choose + Add User/group

Note – if you are using the 'Free Azure Active Directory' you can only add individual Users and not a Group



b. Select and Assign a User (or Group)

	esources, services, and docs (G+/)	Q
Home > Message Centre - Inwards Email   Users ar	Users	×
Add Assignment … InCLOUD.clinic		
Groups are not available for assignment due to your	Dmarc Report Collector	•
the application.	Essential IT EssentialIT@Incisivelabs.onmicrosoft.com	
None Selected Select a role	Incisive Medical Systems o365admin@Incisivelabs.onmicrosoft.com	
User	isw isw@incloud.clinic	

 Assign Permissions to the App Go to Identity > Azure Active Directory



a. Choose 'App Registrations' in the Manage section and select the App you have created



#### b. Choose 'API Permissions'

All services > inCLOUD.clinic   App regist	rations >	
Message Centre - In	cisive Medical	\$ <sup>2</sup> ···
✓ Search «	📋 Delete 🌐 Endpoint	ts 💀 Preview features
👯 Overview	Got a second? We would be a second?	uld love your feedback on Microsoft identity platform (
📣 Quickstart		
💉 Integration assistant	↑ Essentials	
Manage	Display name	: Message Centre - Incisive Medical
Branding & properties	Application (client) ID	: 42c46ef0-48b7-4f22-a26b-090f22243413
	Object ID	: de93885d-da61-4ba3-bbff-d3a35ed34094
Authentication	Directory (tenant) ID	: 4d2099fa-e718-45e3-9ddc-1627fb06a34f
📍 Certificates & secrets	Supported account type	es : My organization only
Token configuration		
→ API permissions	Starting June 30th, Applications will n	2020 we will no longer add any new features to Azure eed to be upgraded to Microsoft Authentication Librar

c. Click

d. Then choose 'Microsoft Graph' from the Microsoft APIs tab

+ Add a permission



# e. Choose 'Delegated Permissions'

Request API permissions	
All APIs     Microsoft Graph     https://graph.microsoft.com/ Dges p?	
What type of permissions does your application require?	
Delegated permissions Your application needs thaccess the API as the signed-in user.	Application permis Your application ru signed-in user.

# f. Add the following Permissions

# i. OpenID permissions > email + offline\_access

to

✓ OpenId permissions (2)

		email 🛈	
	<u> </u>	View users' email address	
	_	offline access ①	
	$\sim$	Maintain access to data you have	given it access
ii.	Direct	tory > Directory.Read.All	2
	$\checkmark$ Di	rectory (1)	
		Directory AccessAddlean All	
		Access directory as the signed in user	
		Directory.Read.All 🕕	
		Read directory data	
iii.	Files >	Files.Read.All	
	∨ File	es (1)	
		Files.Read ①	
		Read user files	
		Files.Read.All 🛈	
	_	Read all files that user can access	
iv.	IMAP	> IMAP.AccessAsUser.All	
	✓ IM/	AP (I)	
		IMAP.AccessAsUser.All	
		Read and write access to mailboxes via IMAP.	
v.	Sites	> Sites.ReadWrite.All	
	✓ SIT	es (I)	
		Sites.FullControl.All ①	
		Have full control of all site collections	
		Sites.Manage.All () Create edit and delete items and lists in all s	
	_	Sites.Read.All	
		Read items in all site collections	
vi.	User >	> User.Read.All	
	$\sim$ Us	er (1)	
		User.Export.All 🕕	
		Export user's data	
		User.Invite.All	
		Invite guest users to the organization	
		Manage user identities	
		User.Read ①	
		Sign in and read user profile	
	<b>~</b>	User.Read.All ①	
		Read all users' full profiles	

# g. Check they have been 'Granted Consent'

The 'Grant Consent' option needs to be enabled using Microsoft365 Administrator login.

#### Each of the API Permissions needs to show that it has been granted consent.

API	/ Permissions name	Туре	Description	Admin consent requ	Status
$\sim$ N	licrosoft Graph (7)			Г	
	Directory.Read.All	Delegated	Read directory data	Yes	🔮 Granted for inCLOUD.cli 🚥
	email	Delegated	View users' email address	No	Sranted for inCLOUD.cli, •••
	Files.Read.All	Delegated	Read all files that user can access	No	🔮 Granted for inCLOUD.cli, ***
	IMAP.AccessAsUser.All	Delegated	Read and write access to mailboxes via IMAP.	No	📀 Granted for inCLOUD.cli 🚥
	offline_access	Delegated	Maintain access to data you have given it access to	No	📀 Granted for inCLOUD.cli,,, 🚥
	Sites.Read.All	Delegated	Read items in all site collections	No	🥑 Granted for inCLOUD.cli,,, 🚥
	User.Read.All	Delegated	Read all users' full profiles	Yes	🔮 Granted for inCLOUD.cli 🚥

#### i. To Grant Consent, click on the 'Grant admin consent for ...' button

Configured permissions		
Applications are authorized to call all the permissions the application	II APIs when they are granted permissions by users/admins as part of the c n needs. Learn more about permissions and consent	onsent process. The list of configured permissions should include
+ Add a permission 🗸 Gra	nt admin consent for inCLOUD.clinic	
API / Permissions name	Type	Admin consent requ Status
Microsoft Graph (7)	$\bigcirc$	
Directory.Read.All	Delegated Read directory data	Yes 🔥 Not granted for inCLOU •••
email	Delegated View users' email address	No ***
Files.Read.All	Delegated Read all files that user can access	No ***
IMAP.AccessAsUser.All	Delegated Read and write access to mailboxes via IMAP.	No ····
offline_access	Delegated Maintain access to data you have given it access to	No ***
Sites.Read.All	Delegated Read items in all site collections	No
User.Read.All	Delegated Read all users' full profiles	Yes 🔥 Not granted for inCLOU, •••

## ii. Approve the granting of consent



- 6. Configure AuthenticationGo to Other > App registrations > Authentication
  - a. Add a Platform



b. Choose 'Web'

Configure platforms	
Web applications Web Build, host, and deploy a web server applicationNET, Java, Python United States of the server application applications	Single-page application Configure browser client applications and progressive web applications. Javascript.
iOS / macOS Objective-C, Swift, Xamarin	<b>Android</b> Java, Kotiin, Xamarin
Mobile and desktop applications Windows, UWP, Console, IoT & Limited-entry Devices, Classic IOS + Android	

c. Set the Redirect URI to 'http://localhost' and Implicit grant... to 'ID Token'

Configure Web		$\times$
All platforms	Quickstart	Docs 🗗
* Redirect URIs		
The URIs we will accept as destinations when returning authentication ret after successfully authenticating or signing out users. The redirect URI yo request to the login server should match one listed here. Also referred to more about Redirect URIs and their restrictions	sponses (tok u send in th as reply UR	cens) e :Ls, Learn
http://localhost		~
Front-channel logout URL This is where we send a request to have the application clear the user's se required for single sign-out to work correctly. e.g. http://www.mple.com/logout	ession data.	This is
Implicit grant and hybrid flows		
Request a token directly from the authorization endpoint. If the applicati architecture (SPA) and doesn't use the authorization code flow, or if it inv JavaScript, select both access tokens and ID tokens. For ASP.NET Core we web apps that use hybrid authentication, select only ID tokens. Learn mo	on has a sin okes a web b apps and re about to	gle-page API via other cens.
Select the tokens you would like to be issued by the authorization endpo	int:	
Access tokens (used for implicit flows)		
ID tokens (used for implicit and hybrid flows)		

d. Choose Single tenant or Multi-tenant as the 'Supported account types' If the email domain is different from your Active Directory account, choose 'Multitenant'.

Supported account types
Who can use this application or access this API?
Accounts in this organizational directory only (inCLOUD.clinic only - Single tenant)
Accounts in any organizational directory (Any Azure AD directory - Multitenant)

7. In 'Certificates & Secrets' create a + New client secret



Add a Description and a Expiry date.

Add a client secret		$\times$
Description	Message Centre	
Expires	12 months	$\sim$

You should discuss the Expiry option with your IT provider so that it adheres to your security requirements.

A short Expiry period means you will need to renew the Secret and update it within the Incisive application, frequently.

You can choose a 'Custom' expiry and enter in your own expiry date.

#### Record the 'Secret Value' as you will need it in SPM/PHM for anyone

Certificates (0) Client secrets (1) 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.			
Expires	Value 🛈	Secret ID	
1/13/2024	Zlk8Q~dgUCNLwG1QkqKBdGp-8ddEcZ3		
	ederated credentials (0 prove its identity when re Expires 1/13/2024	ederated credentials (0) prove its identity when requesting a token. Also can be referred to as a Expires Value O 1/13/2024 ZIk8Q~dgUCNLwG1QkqK8dGp-8ddEcZ3	

- 8. Enter the Application ID & Secret Value in SPM/PHM
  - a. Select the Provider (F2) and go to Setup > Provider > Config 3
  - b. Enter the Application ID & Secret Value (not Secret ID) into the fields

onebilite scolage o	containing
App ID	42c46ef0-
Secret	723a405c
Azure Container	

- 9. Test the connection to the Microsoft 365 IMAP account
  - a. Go to setup > Personnel > Operator, select an Operator and choose 'Messaging Options' from the toolbar menu.
  - b. Enter in the Microsoft 365 IMAP and Account details and click on the 'Test' button

perator: incisive sortw	are				
		Email ser	narc		
		Email Ser	vers		
Server		Username	Password	SSL	
▶ outlook.office3	65.com	demo@incloud.clinic	******		Test
•					

i. Unless previously configured, Windows will prompt for an exclusion to be created in the Firewall



ii. You will be prompted to sign-in to your Microsoft 365 account

1	
ii	
nt?	
Back	Next
	! nt? Back

iii. If authentication is successful, the following will appear: A Success page

incisive	
Authorisation Successful	
The emailing component is now authorised.	
You can close this page and continue.	

# A green tick

Email ser	il servers		1
	Password	SSL	
clinic	*******		$\checkmark$

# A message box



If authentication is unsuccessful, you will receive technical responses with the reason.

Error	:	× ]
4	Authentication Error Email server: outlook.office365.com Username: demo@incloud.clinic No response from the browser!	
	ОК	)

A one-off prompt will appear to accept access to your data by the Message Centre

Permissions	requested	
Incisive Messa incloud.clinic	age Centre - Den	no
This application is r	not published by	Microsoft.
This app would like	to:	
View your basic pr	rofile	
✓ Maintain access to	o data you have giv	en it access to
✓ Read and write ac	cess to your mail.	
Accepting these permissi your data as specified in t statement. The publisher for you to review. You c https://myapps.microsoft	ons means that you a their terms of service r <b>has not provided lin</b> an change these perr t.com. Show details	allow this app to use and privacy <b>hks to their terms</b> nissions at
Does this app look suspic	ious? Report it here	

# **Trouble-shooting**

Microsoft login differs from the email account specified for the IMAP email import. Login using the correct email address



### Users not assigned to the App Add them in Users & Groups

Microsoft

# Message Centre - Incisive Medical

Sorry, but we're having trouble with signing you in.

AADSTS50105: Your administrator has configured the application Message Centre -Incisive Medical ('42c46ef0-48b7-4f22-a26b-090f22243413') to block users unless they are specifically granted ('assigned') access to the application. The signed in user 'demo@incloud.clinic' is blocked because they are not a direct member of a group with access, nor had access directly assigned by an administrator. Please contact your administrator to assign access to this application.

# Domain of the email account differs from your Active Directory login Choose Multi-tenant in Authentication



Supported account types

Who can use this application or access this API?

Accounts in this organizational directory only (inCLOUD.clinic only - Single tenant)

Accounts in any organizational directory (Any Azure AD directory - Multitenant)

## AppID or Client Secret value not added for the Provider in Setup > Provider > Config3



## Internet Explorer is your default browser. Change to Edge, Chrome, Safari or Firefox



# Redirect URI not specified

Add <a href="http://localhost">http://localhost</a> to the Redirect URI field in Authentication

 Microsoft

 Sign in

 Sorry, but we're having trouble with signing you in.

 AADSTS500113: No reply address is registered for the application.

 Image: Microsoft Acure P Search resources, services, and docs (G+/)

 Image: Microsoft Acure P Search resources, services, and docs (G+/)

 Sorry Message Centre - Inwards Email P microsoft

