

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:

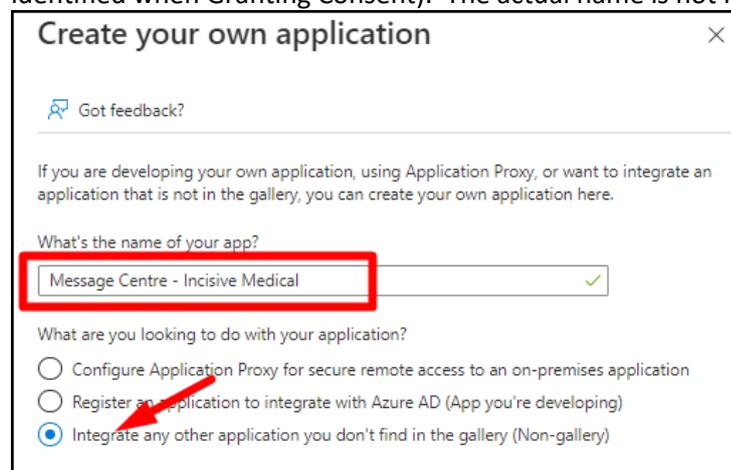
- Ensure you are running SPM/PHM version 412.4 or newer
- Edge, Safari, Chrome or Firefox browser – not Internet Explorer

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

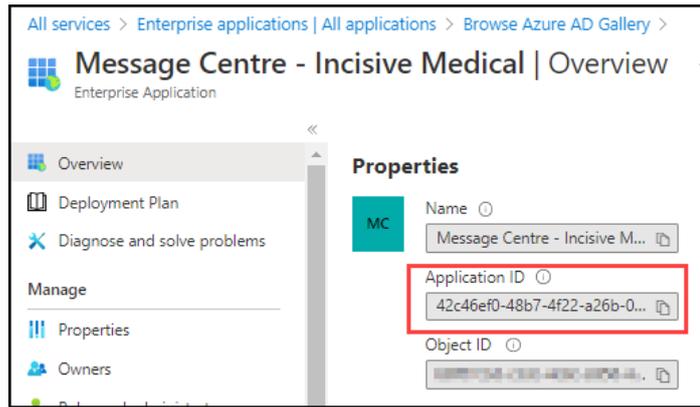
1. Log in to the Azure portal tenancy, that provides the Microsoft 365 service, with an Administrator account.
2. Go to Identity > Enterprise Applications
3. Create a new Application.
 - a. Choose '+ New Application'
 - b. Choose '+ Create your own application'

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



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

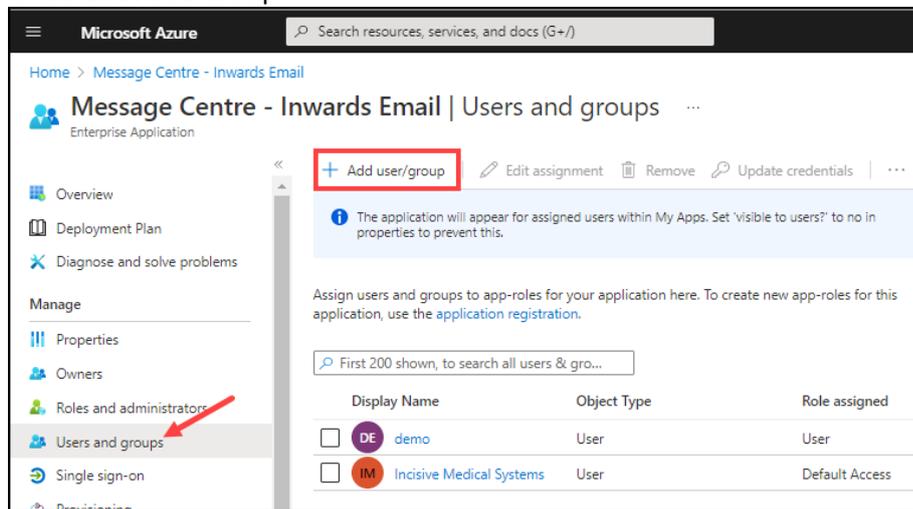
The 'Application ID' (App ID) will now be displayed. You'll need this Application ID number in SPM/PHM



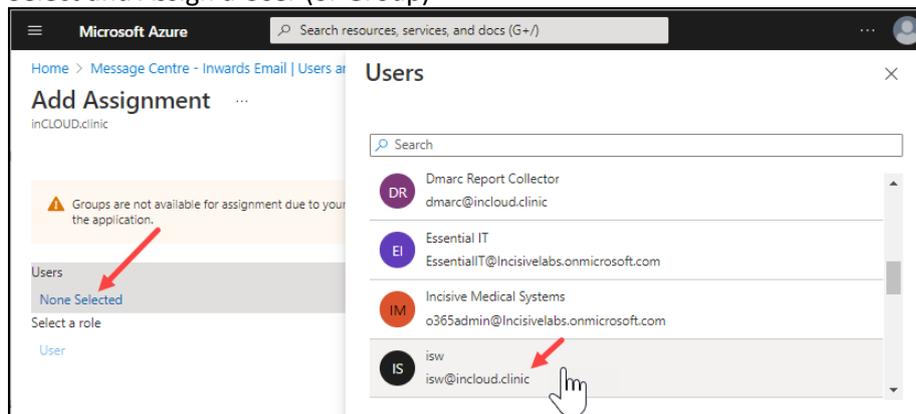
4. Assign Users & Groups to the Application

- a. Go to Identity > Enterprise Applications > Users and groups then choose **+ Add User/group**

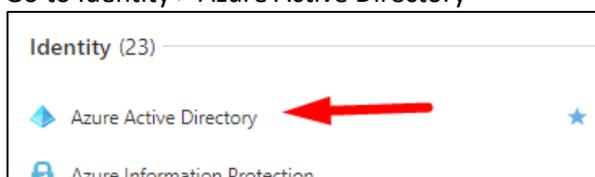
Note – if you are using the 'Free Azure Active Directory' you can only add individual Users and not a Group



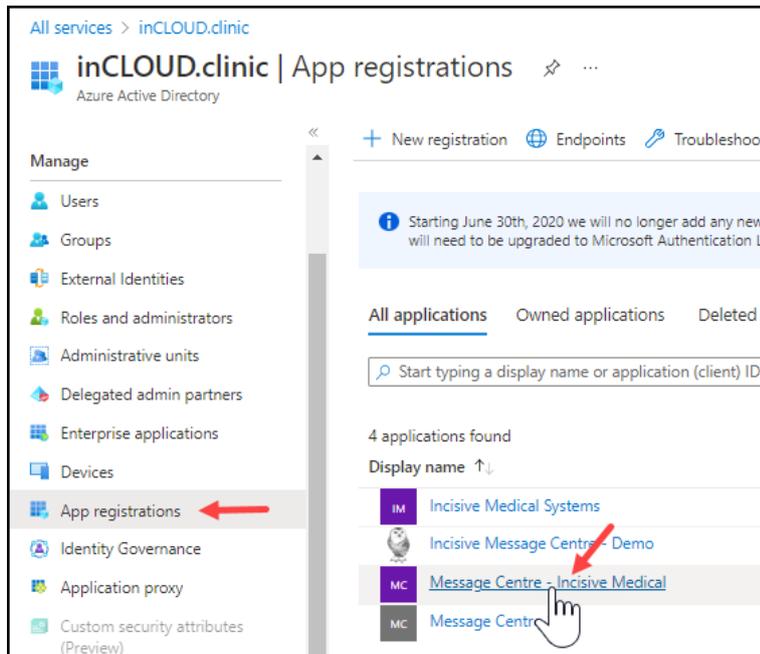
- b. Select and Assign a User (or Group)



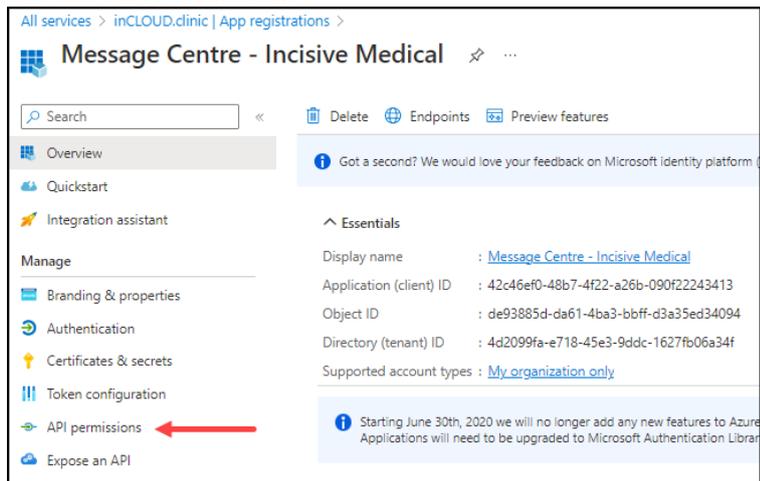
5. Assign Permissions to the App Go to Identity > Azure Active Directory



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

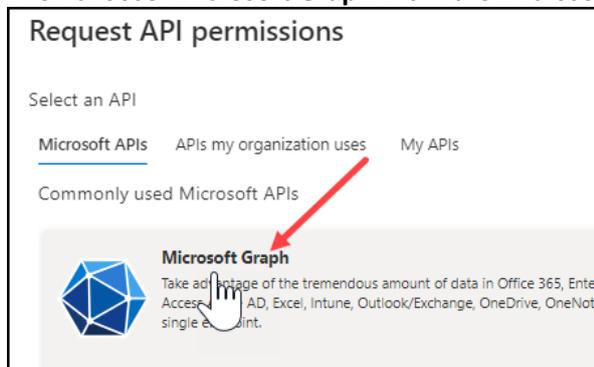


- b. Choose 'API Permissions'

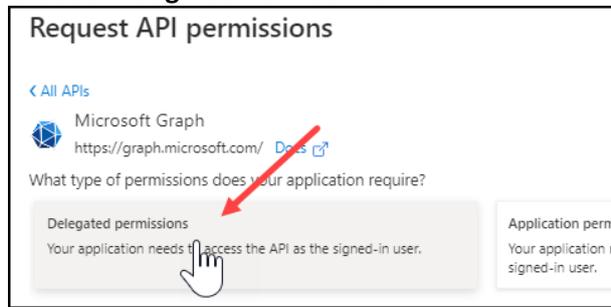


- c. Click [+ Add a permission](#)

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



e. Choose 'Delegated Permissions'



f. Add the following Permissions

i. **OpenID permissions > email + offline_access**

OpenId permissions (2)

- email ⓘ
View users' email address
- offline_access ⓘ
Maintain access to data you have given it access to

ii. **Directory > Directory.Read.All**

Directory (1)

- Directory.AccessAsUser.All ⓘ
Access directory as the signed in user
- Directory.Read.All ⓘ
Read directory data

iii. **Files > Files.Read.All**

Files (1)

- Files.Read ⓘ
Read user files
- Files.Read.All ⓘ
Read all files that user can access

iv. **IMAP > IMAP.AccessAsUser.All**

IMAP (1)

- IMAP.AccessAsUser.All ⓘ
Read and write access to mailboxes via IMAP.

v. **Sites > Sites.ReadWrite.All**

Sites (1)

- Sites.FullControl.All ⓘ
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**

User (1)

- User.Export.All ⓘ
Export user's data
- User.Invite.All ⓘ
Invite guest users to the organization
- User.ManageIdentities.All ⓘ
Manage user identities
- User.Read ⓘ
Sign in and read user profile
- User.Read.All ⓘ
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	Type	Description	Admin consent requ...	Status
Microsoft Graph (7)				
Directory.Read.All	Delegated	Read directory data	Yes	Granted for inCLOUD.cl... ***
email	Delegated	View users' email address	No	Granted for inCLOUD.cl... ***
Files.Read.All	Delegated	Read all files that user can access	No	Granted for inCLOUD.cl... ***
IMAP.AccessAsUser.All	Delegated	Read and write access to mailboxes via IMAP.	No	Granted for inCLOUD.cl... ***
offline_access	Delegated	Maintain access to data you have given it access to	No	Granted for inCLOUD.cl... ***
Sites.Read.All	Delegated	Read items in all site collections	No	Granted for inCLOUD.cl... ***
User.Read.All	Delegated	Read all users' full profiles	Yes	Granted for inCLOUD.cl... ***

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

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 inCLOUD.clinic

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (7)				
Directory.Read.All	Delegated	Read directory data	Yes	Not granted for inCLOUD... ***
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 inCLOUD... ***

- ii. Approve the granting of consent

Grant admin consent confirmation.

Do you want to grant consent for the requested permissions for all accounts in...

6. Configure Authentication

Go to Other > App registrations > Authentication

- a. Add a Platform

Microsoft Azure

Home > inCLOUD.clinic | App registrations > Message Centre - Inwards Email

Message Centre - Inwards Email | Authentication

Search

Overview
Quickstart
Integration assistant

Manage

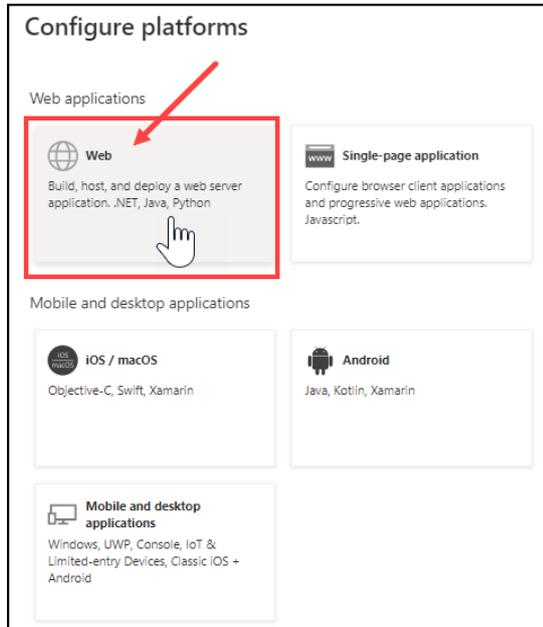
- Branding & properties
- Authentication **←**
- Certificates & secrets
- Token configuration

Platform configurations

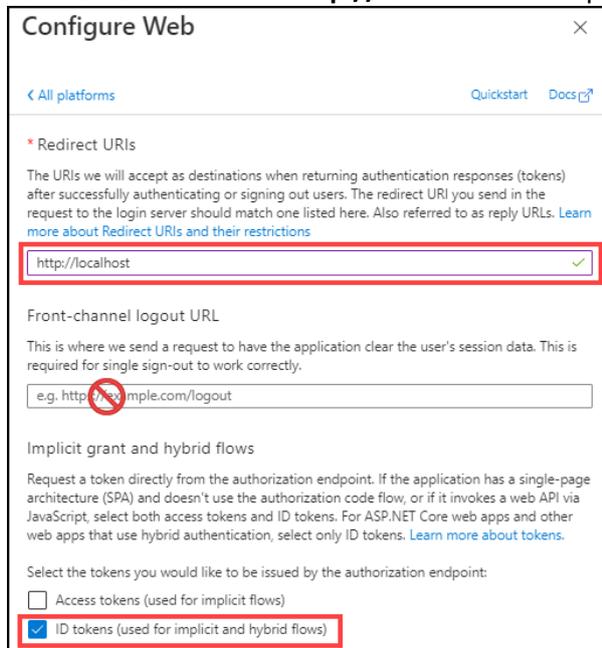
Depending on the platform or device this application is targeted to. To configure single sign-on, including SAML-based sign-on, try En...

+ Add a platform

b. Choose 'Web'

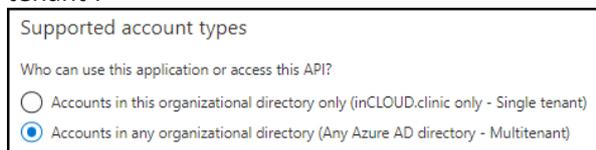


c. Set the Redirect URI to 'http://localhost' and Implicit grant... to 'ID Token'

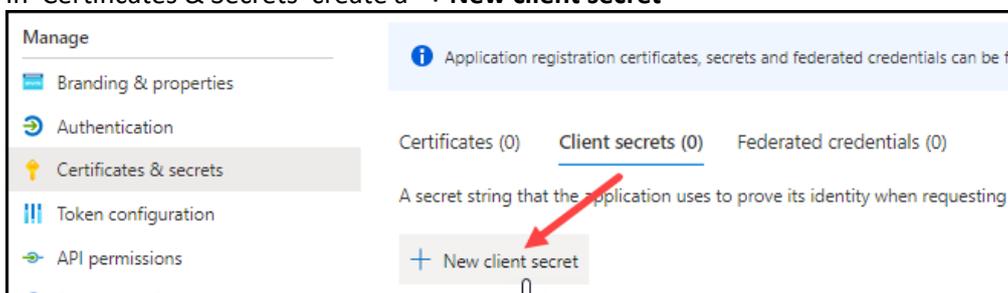


d. Choose Single tenant or Multi-tenant as the 'Supported account types'

If the email domain is different from your Active Directory account, choose 'Multi-tenant'.



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



Add a Description and a Expiry date.

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

Description	Expires	Value	Secret ID
Message Centre	1/13/2024	Zlk8Q~dgUCNLwG1QkqKBdGp-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

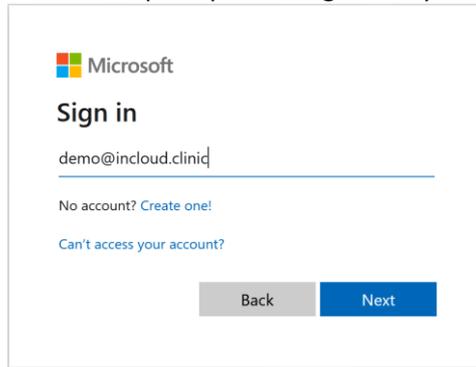
9. Test the connection to the Microsoft 365 IMAP account

- 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

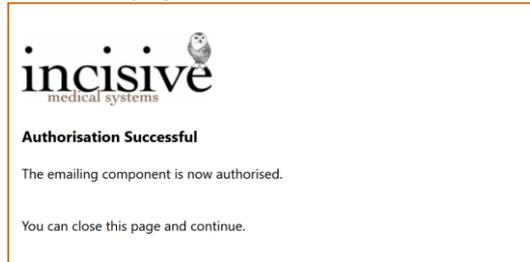
Server	Username	Password	SSL	
outlook.office365.com	demo@includ.clinic	*****	<input checked="" type="checkbox"/>	Test

- 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



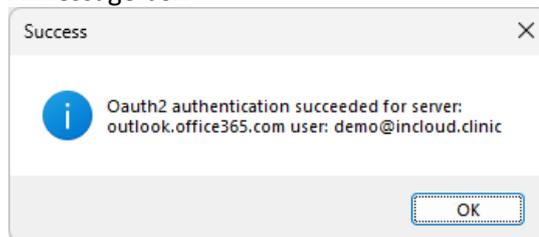
- iii. If authentication is successful, the following will appear:
A Success page



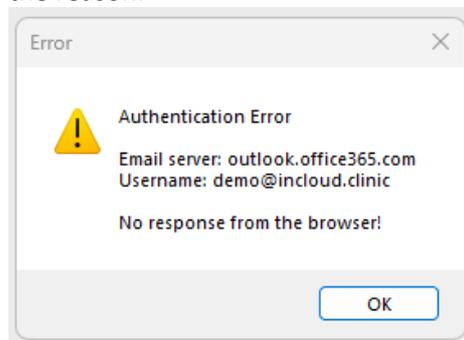
A green tick

Email servers			
	Password	SSL	
clinic	*****	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

A message box



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



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



Permissions requested

 Incisive Message Centre - Demo
incloud.clinic

This application is not published by Microsoft.

This app would like to:

- ✓ View your basic profile
- ✓ Maintain access to data you have given it access to
- ✓ Read and write access to your mail.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

Does this app look suspicious? [Report it here](#)

Trouble-shooting

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



Sign in

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

AADSTS700016: Application with identifier '42c46ef0-48b7-4f22-a26b-090f22243413' was not found in the directory 'Incisive Medical Systems'. This can happen if the application has not been installed by the administrator of the tenant or consented to by any user in the tenant. You may have sent your authentication request to the wrong tenant.

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



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



Sign in

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

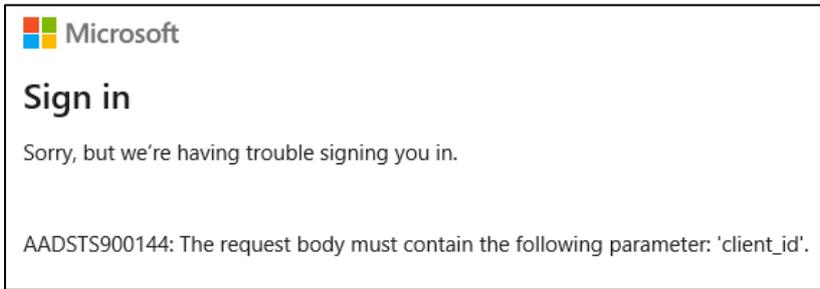
AADSTS50194: Application '42c46ef0-48b7-4f22-a26b-090f22243413'(Message Centre - Inwards Email) is not configured as a multi-tenant application. Usage of the /common endpoint is not supported for such applications created after '10/15 /2018'. Use a tenant-specific endpoint or configure the application to be multi-tenant.

Supported account types

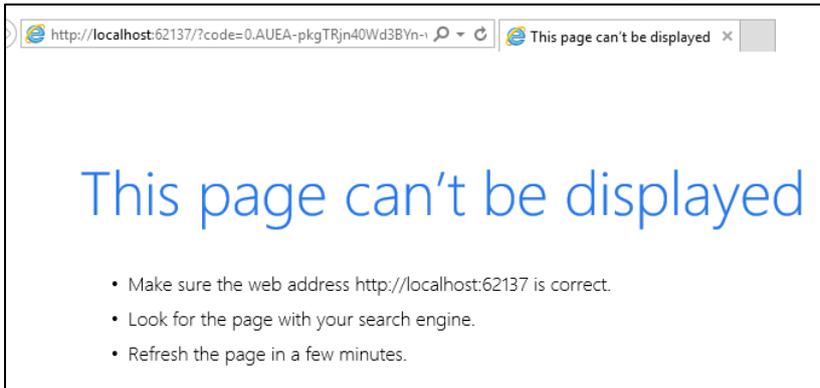
Who can use this application or access this API?

- 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 <http://localhost> to the Redirect URI field in Authentication

