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:

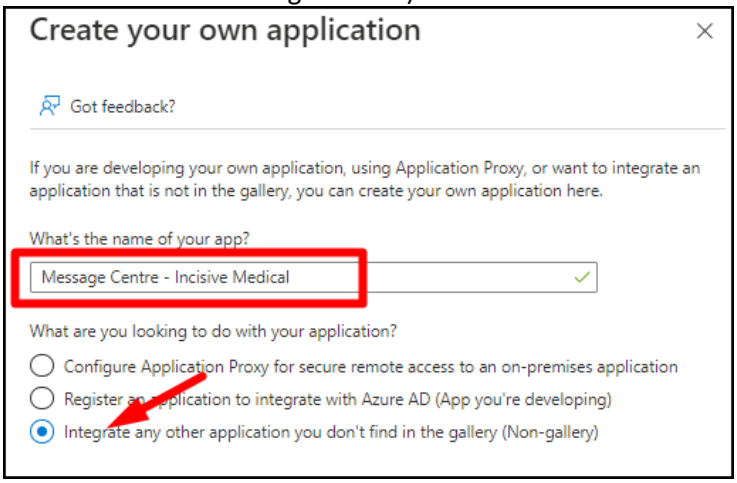
- Register the 'Message Centre' as an App
- Assign Users & Groups to the App
- Assign Permissions to the App
- Create a Secret
- Enter the App ID and Secret into the Incisive program

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'

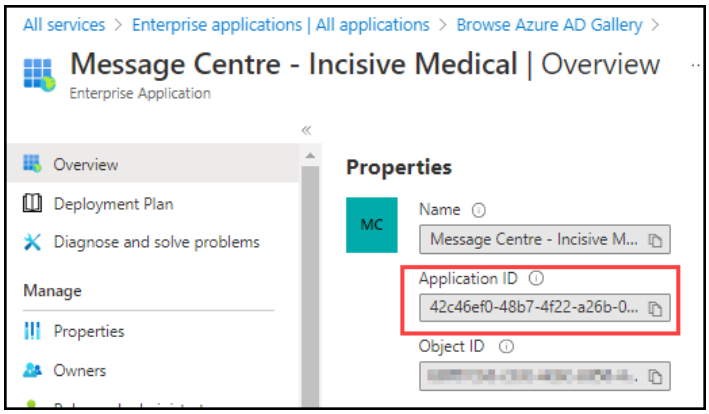
    Call it something like '**Message Centre - *practice/hospital name***' (so it can be identified when Granting Consent). The actual name is not important.



    i. Choose the option to 'Integrate any other application…'

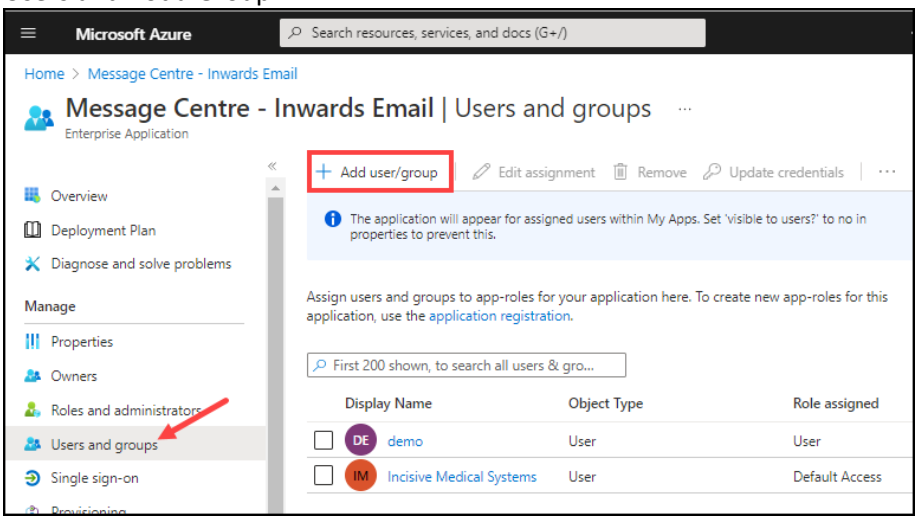
    ii. Click on the 'Create' button at the bottom

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

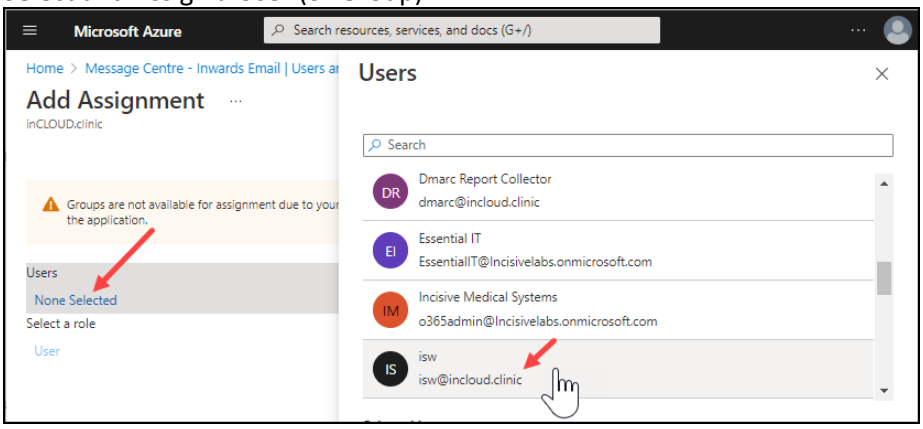


4. Assign Users & Groups to the Application

   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

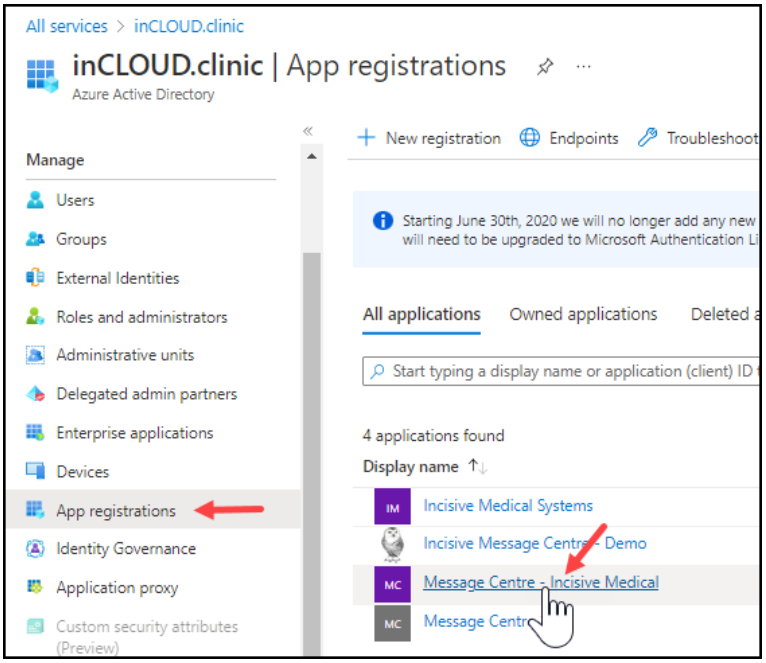


   b. Select and Assign a User (or Group)

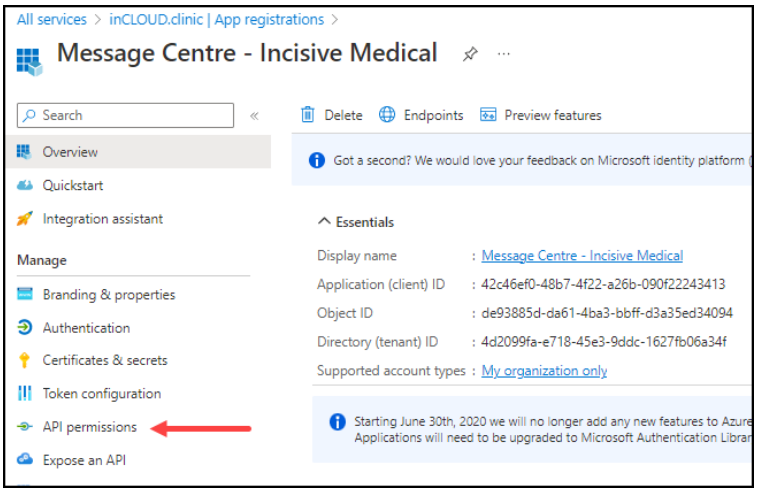


5. Assign Permissions to the App
   Go to Identity > Azure Active Directory

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

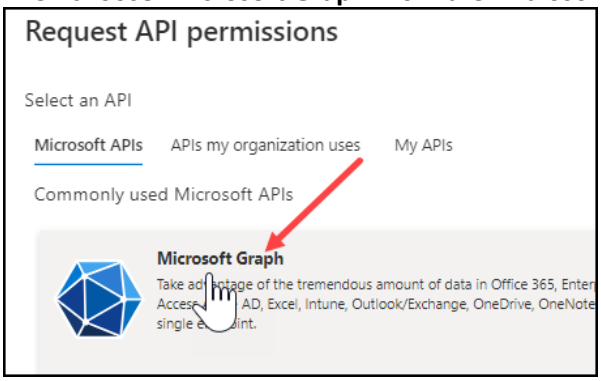


b. Choose 'API Permissions'

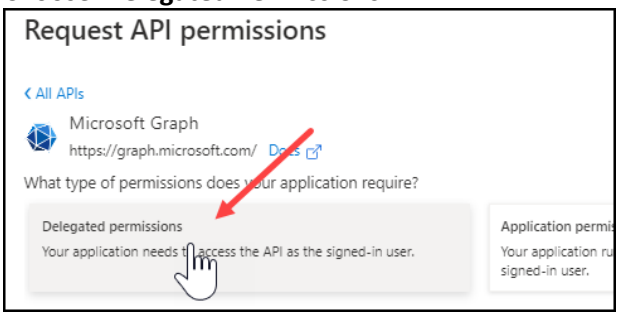


c. Click 

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

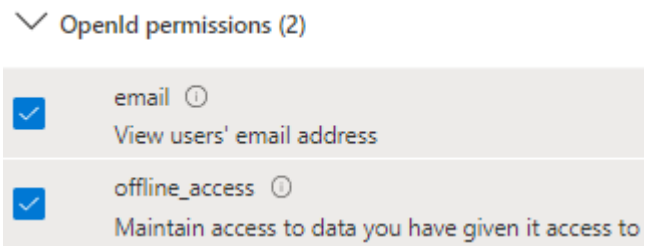


e. Choose '**Delegated Permissions**'

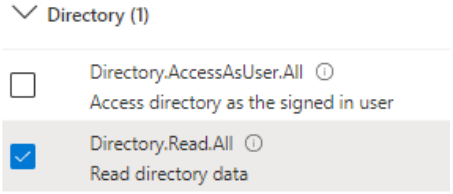


f. Add the following Permissions

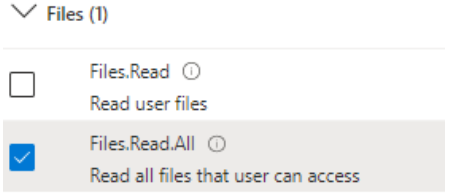
i. **OpenID permissions > email + offline_access**



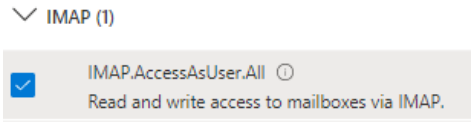
ii. **Directory > Directory.Read.All**



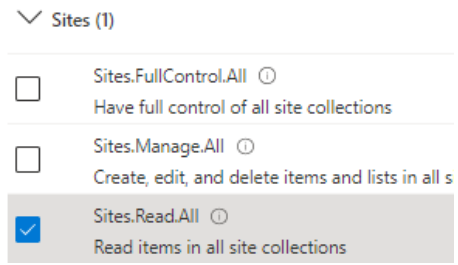
iii. **Files > Files.Read.All**



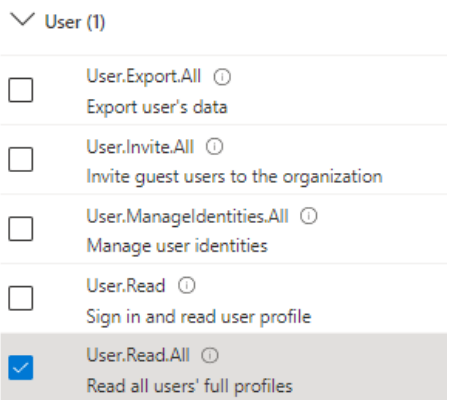
iv. **IMAP > IMAP.AccessAsUser.All**



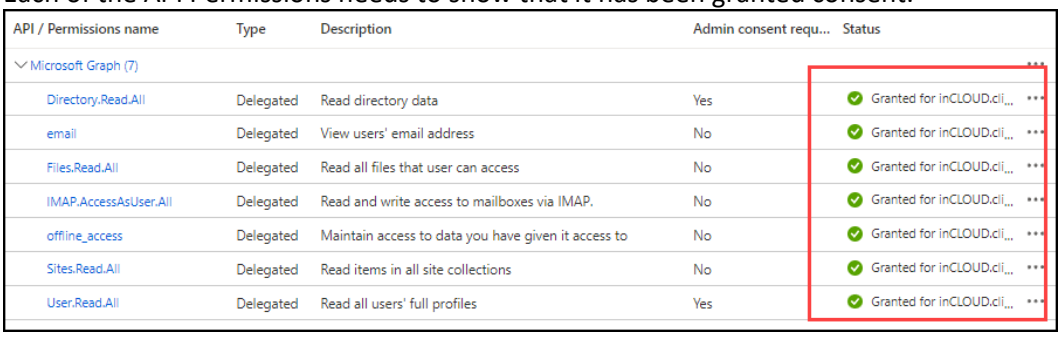
v. **Sites > Sites.ReadWrite.All**



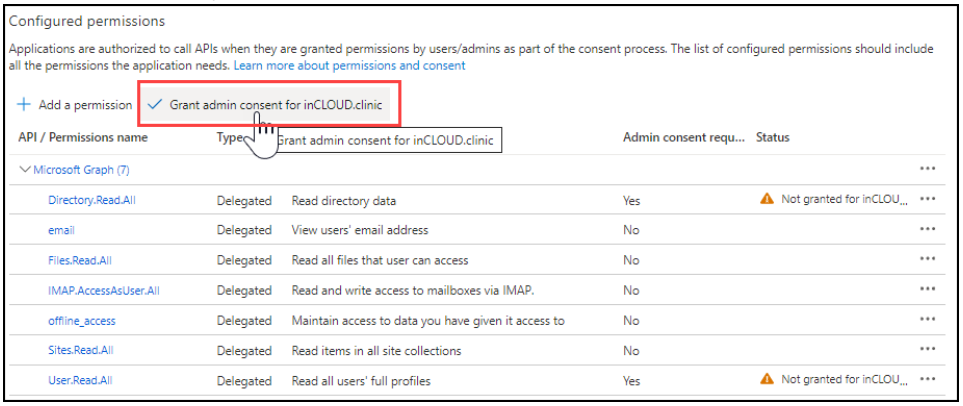
vi. **User > User.Read.All**



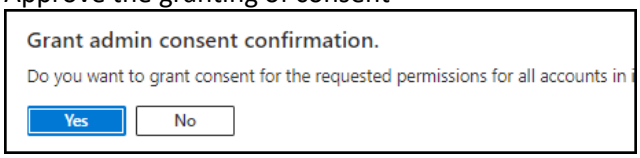
g. Check they have been 'Granted Consent'
The 'Grant Consent' option needs to be enabled using Microsoft365 Administrator login.
Each of the API Permissions needs to show that it has been granted consent.



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

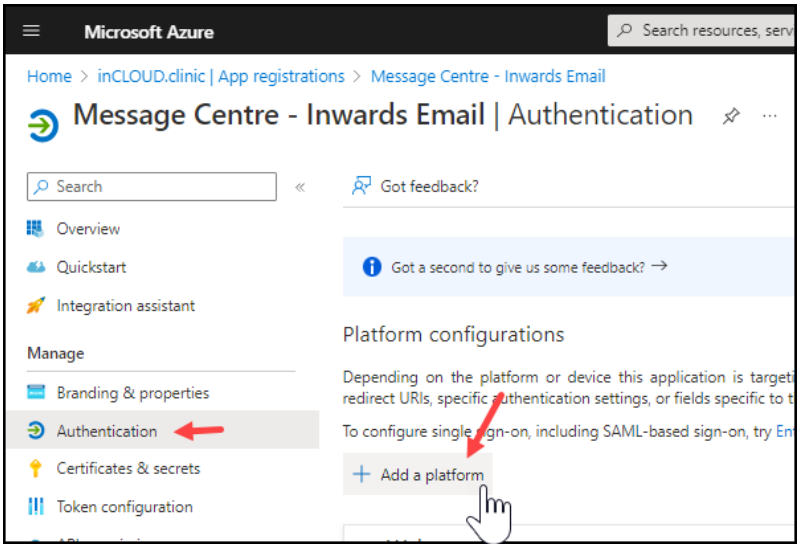


ii. Approve the granting of consent

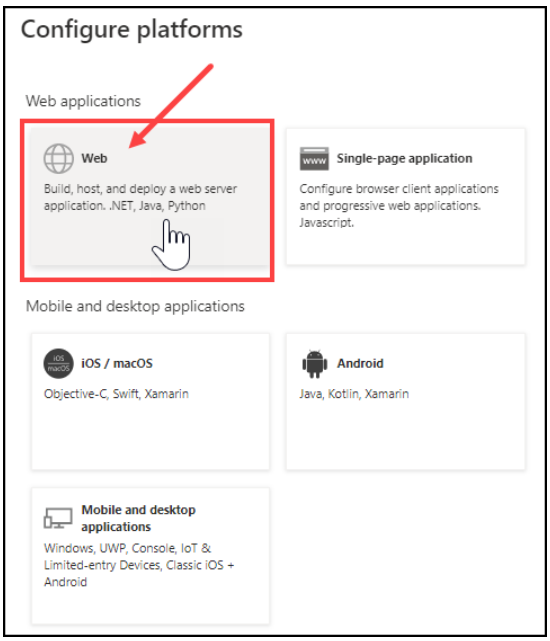


6. Configure Authentication
Go to Other > App registrations > Authentication

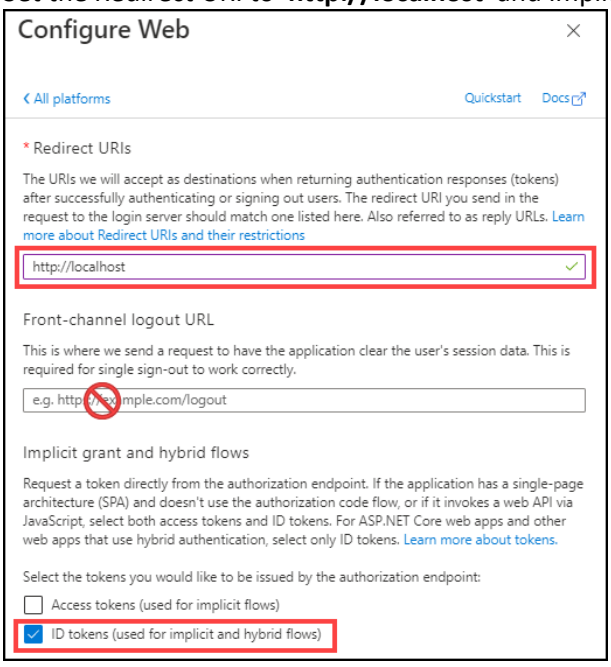
a. Add a Platform



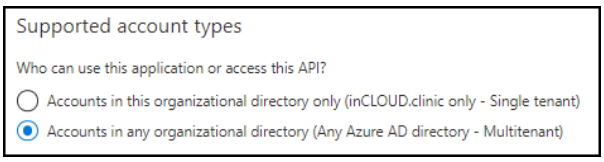
b. Choose ‘Web’



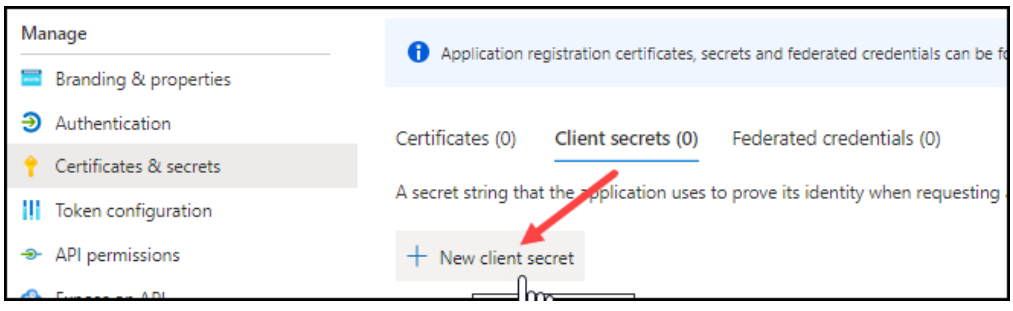
c. Set the Redirect URI to '**http://localhost**' and Implicit grant… to **‘ID Token’**



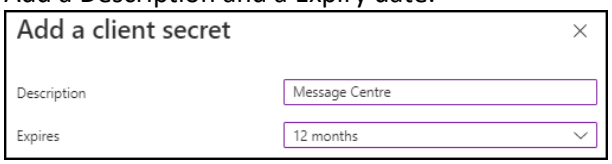
d. Choose Single tenant or Multi-tenant as the ‘Supported account types’
If the email domain is different from your Active Directory account, choose ‘Multi-tenant’.



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

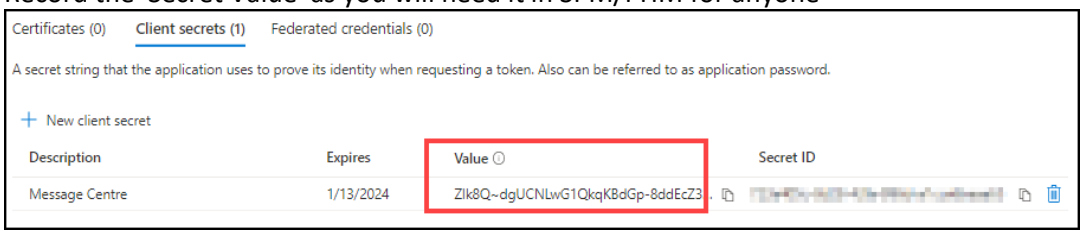


Add a Description and a Expiry date.

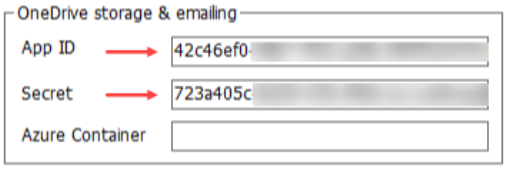


You should discuss the Expiry option with your IT provider so that it adheres to your security requirements.
A short Expiry period means you will need to renew the Secret and update it within the Incisive application, frequently.
You can choose a ‘Custom’ expiry and enter in your own expiry date.

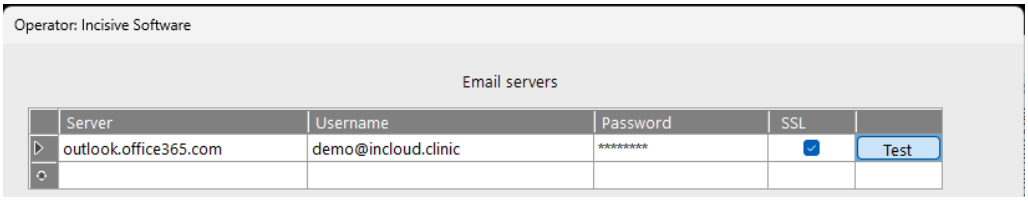
Record the 'Secret Value' as you will need it in SPM/PHM for anyone



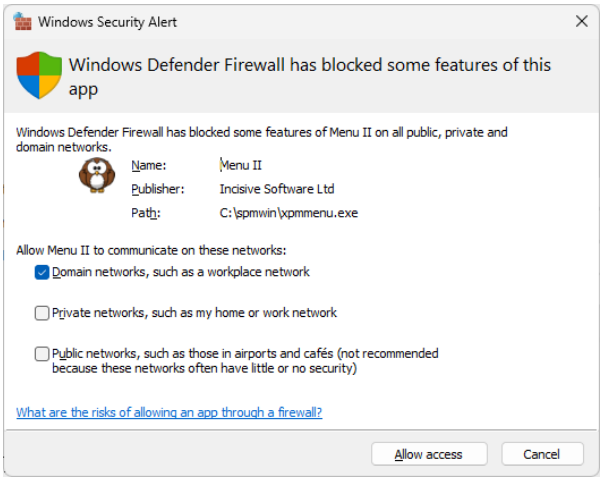
8. Enter the Application ID & Secret Value in SPM/PHM
    a. Select the Provider (F2) and go to Setup > Provider > Config 3
    b. Enter the Application ID & Secret Value (not Secret ID) into the fields



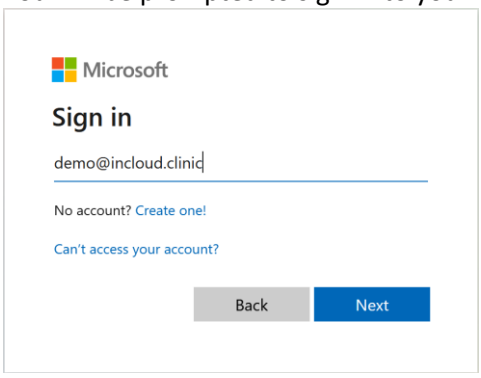
9. Test the connection to the Microsoft 365 IMAP account
    a. Go to setup > Personnel > Operator, select an Operator and choose ‘Messaging Options’ from the toolbar menu.
    b. Enter in the Microsoft 365 IMAP and Account details and click on the ‘Test’ button



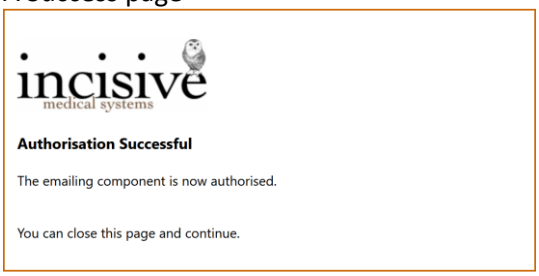
    i. Unless previously configured, Windows will prompt for an exclusion to be created in the Firewall



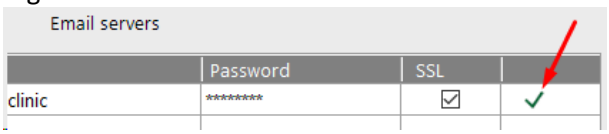
ii. You will be prompted to sign-in to your Microsoft 365 account



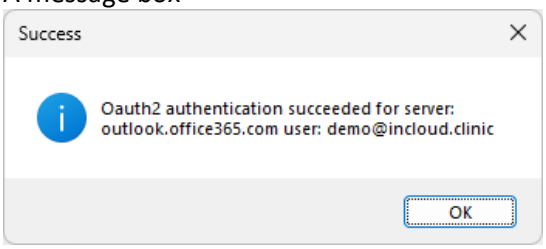
iii. If authentication is successful, the following will appear:
A Success page



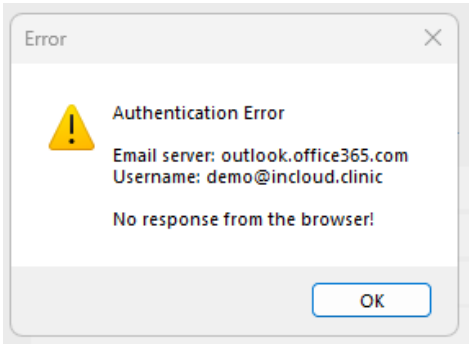
A green tick



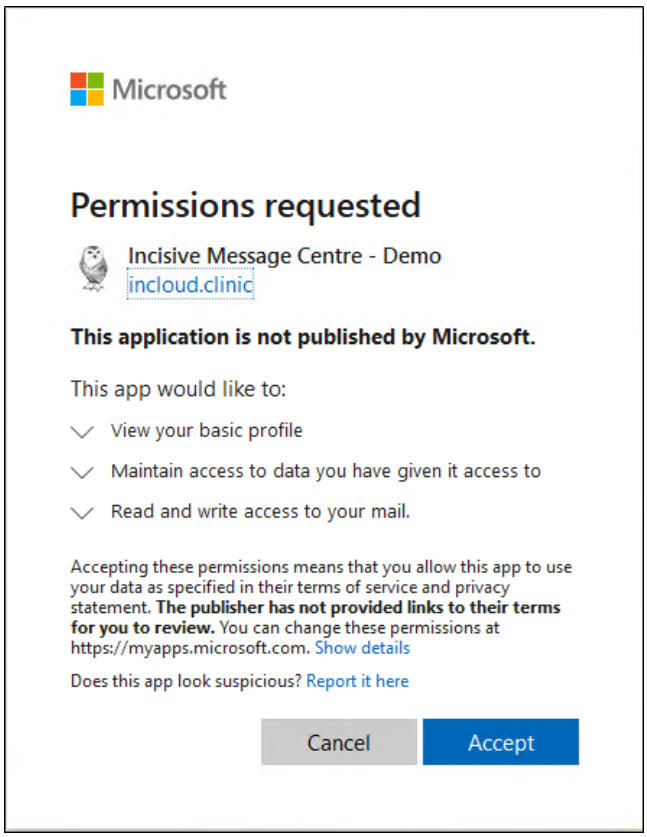
A message box



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

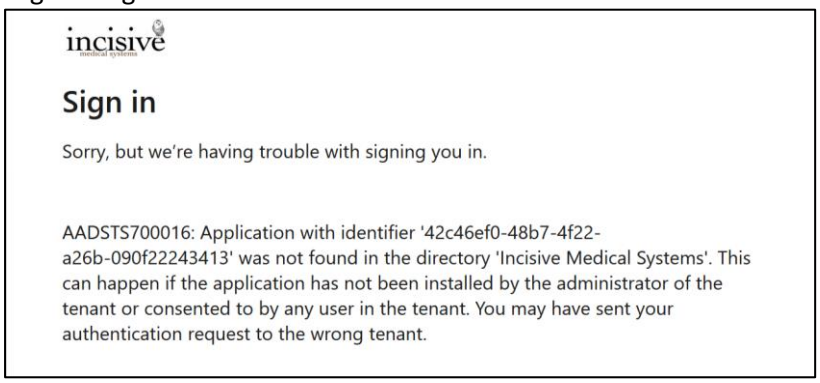


A one-off prompt will appear to accept access to your data by the Message Centre

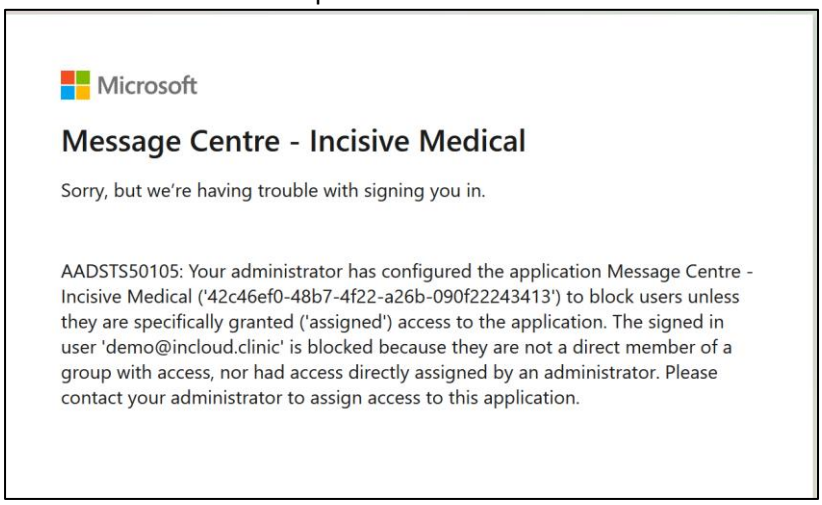


Trouble-shooting

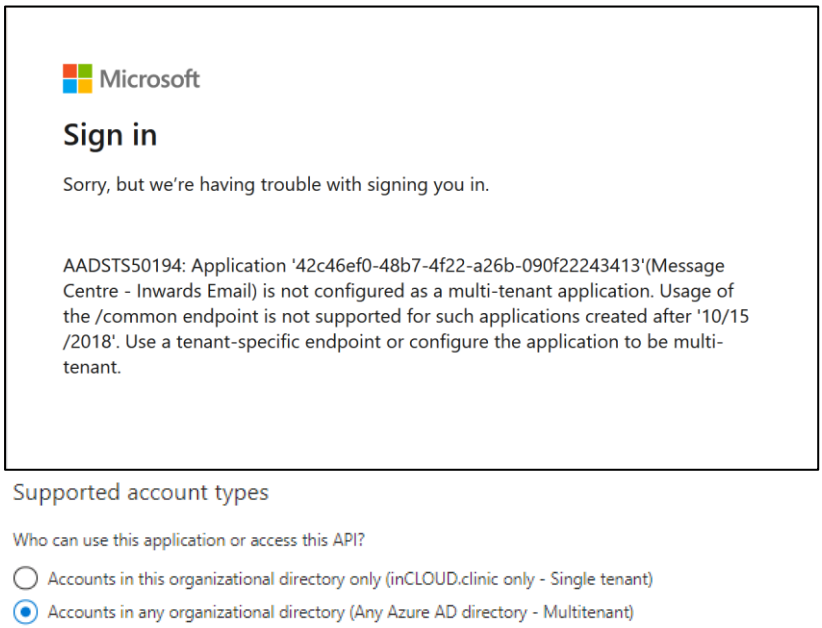
Microsoft login differs from the email account specified for the IMAP email import.
Login using the correct email address



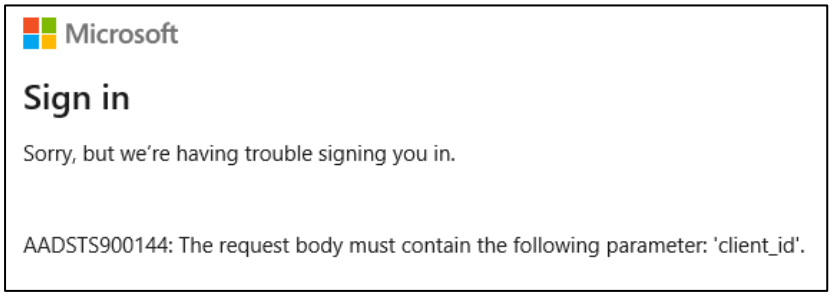
Users not assigned to the App
Add them in Users & Groups



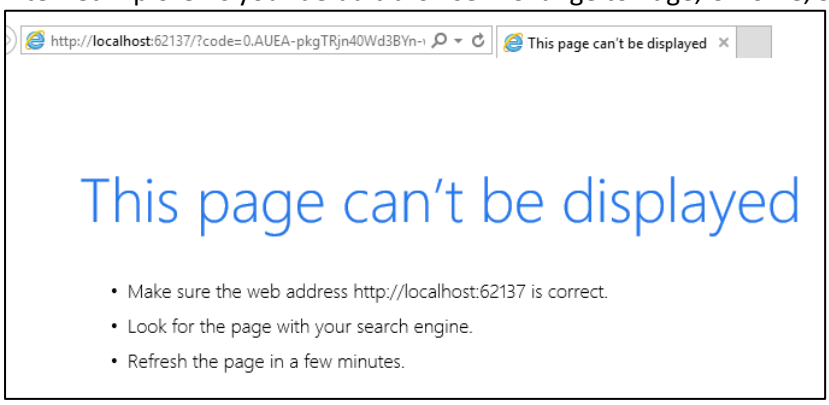
Domain of the email account differs from your Active Directory login
Choose Multi-tenant in Authentication



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