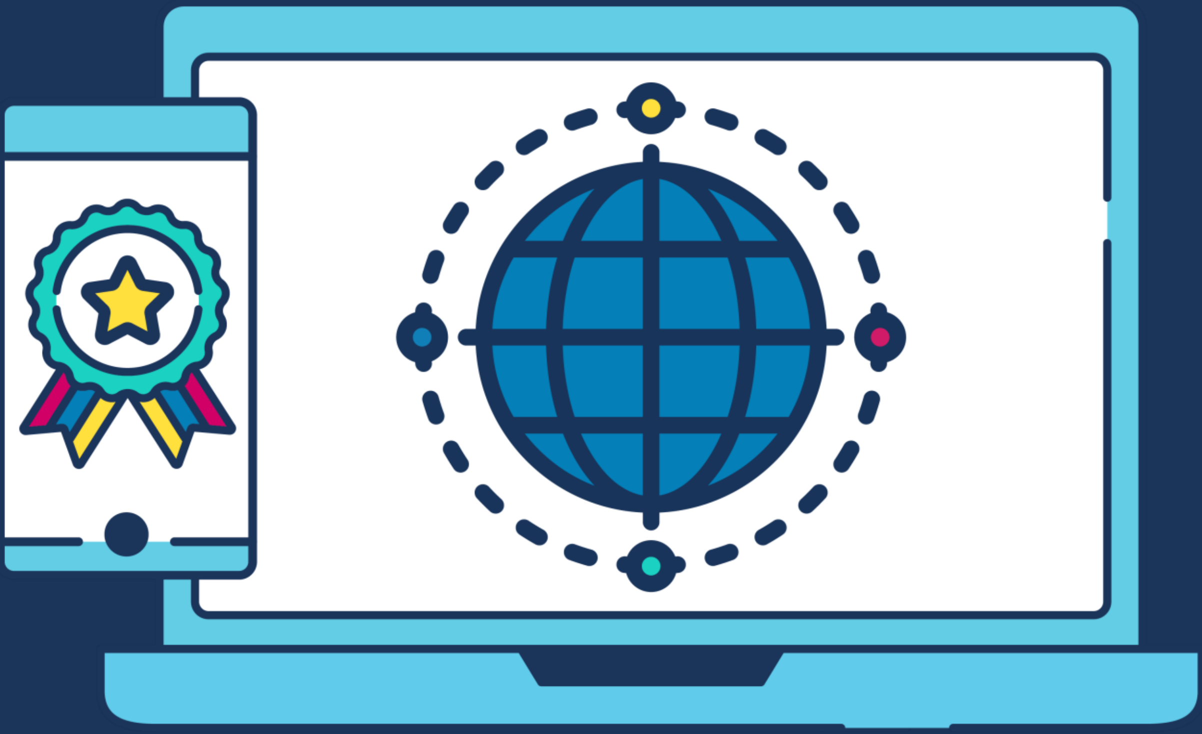
Setting up Microsoft Office 365 for OAuth2

PASS (TIMEGATE RECRUIT)

November 2021



COMMERCIAL STATEMENT

This document is subject to any terms as per teamsoftware.com/legal.

TABLE OF CONTENTS

INTRODUCTION

To authenticate to Office 365 using OAuth2, rather than the Basic Authentication (username/password) which is being phased out, the application must be registered and configured in Azure first.

The first point to note is that the account to be used cannot be configured to require Multi-Factor Authentication.

The following non-TEAM Software websites are useful for showing how to register PASS (Timegate Recruit), but an example is also given below.

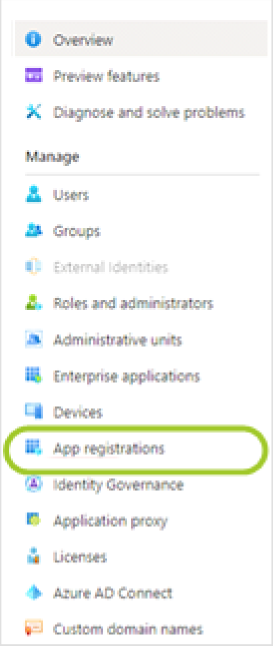
- Quickstart: Register an app in the Microsoft identity platform | Microsoft Docs
- OAuth 2.0 with Office365/Exchange IMAP/POP3/SMTP | Blog | Limilabs

This setup guide is for use with the PASS Server Service Mailbox Monitor plugin but may also be used with other elements of the PASS family that require OAuth2 access to Microsoft's Office 365.

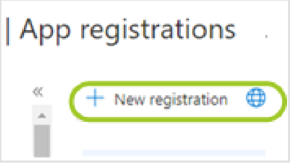
REGISTER PASS FOR USE WITH OAUTH2 FOR OFFICE 365

1. Log in to the Azure Active Directory page as an account administrator at: https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Overview

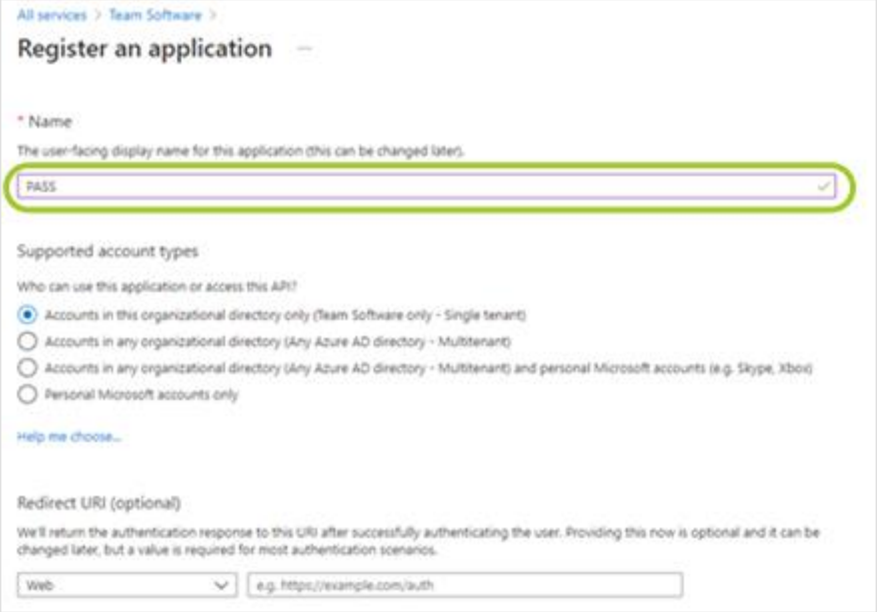
2. Select **Manage | App Registrations**



3. Select **New registration**



4. Enter a name for the registration. We suggest using **PASS** as the name, but it just needs to be meaningful to you



All services > Team Software >

Register an application

* Name

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

PASS

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (Team Software 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...

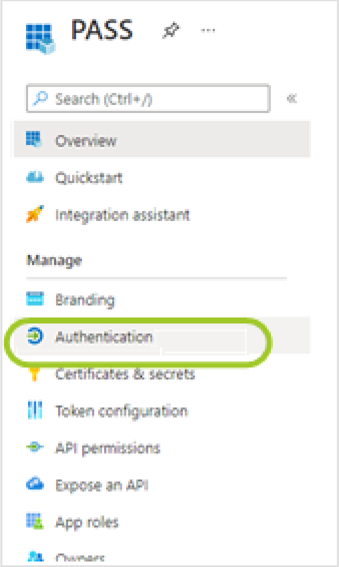
Redirect URI (optional)

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.

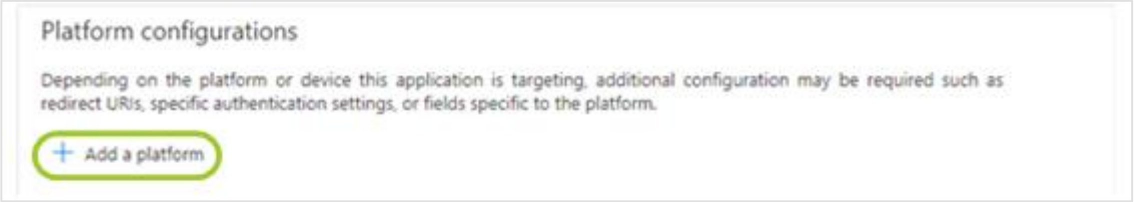
Web | e.g. https://example.com/auth

5. Select **Register**

6. Select **Manage | Authentication**

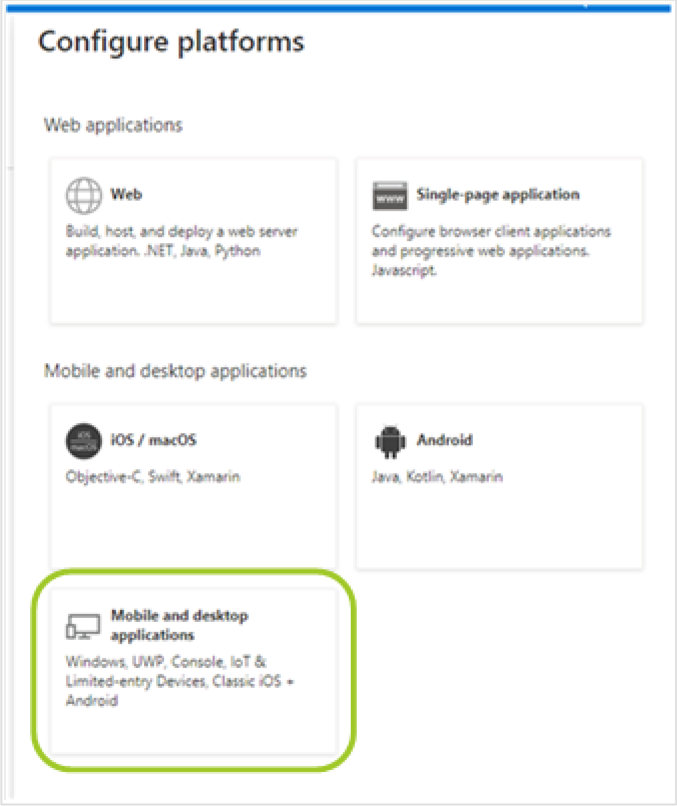


7. Select **Add a platform**


Platform configurations

Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.

8. On the pop-out pane (on the right-hand side), select **Mobile and desktop applications**


Configure platforms

Web applications

Build, host, and deploy a web server application. .NET, Java, Python

Configure browser client applications and progressive web applications. Javascript.

Mobile and desktop applications

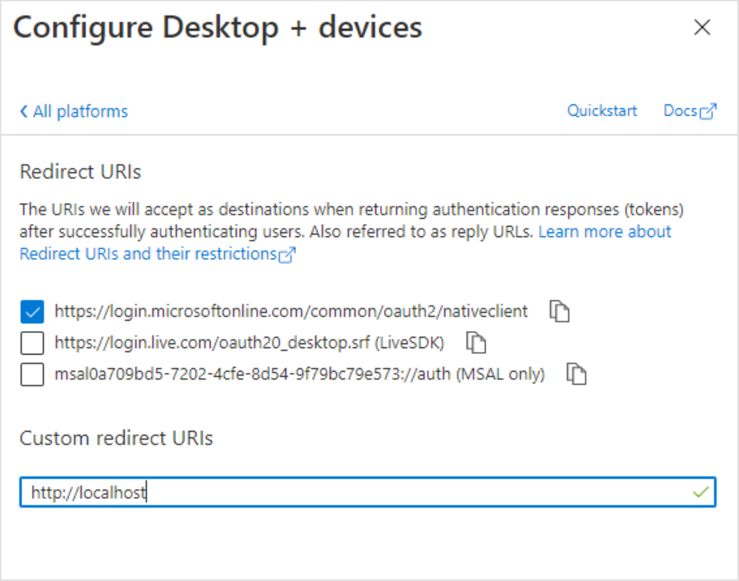
Objective-C, Swift, Xamarin

Java, Kotlin, Xamarin

Windows, UWP, Console, IoT & Limited-entry Devices, Classic iOS + Android

9. Tick the **https://login.microsoftonline.com/common/oauth2/nativeclient** option

10. Enter **http://localhost** in the custom URIs box as shown:



Configure Desktop + devices

Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating users. Also referred to as reply URLs. Learn more about Redirect URIs and their restrictions

☑ https://login.microsoftonline.com/common/oauth2/nativeclient

□ https://login.live.com/oauth20_desktop.srf (LiveSDK)

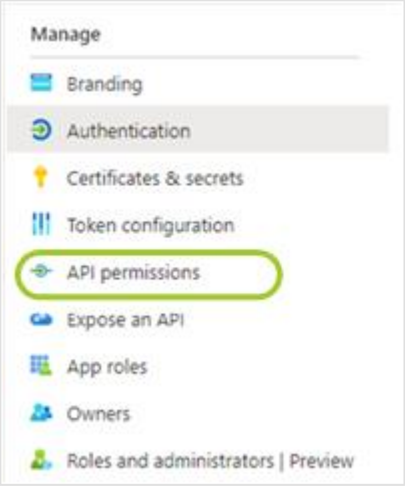
□ msal0a709bd5-7202-4cfe-8d54-9f79bc79e573://auth (MSAL only)

Custom redirect URIs

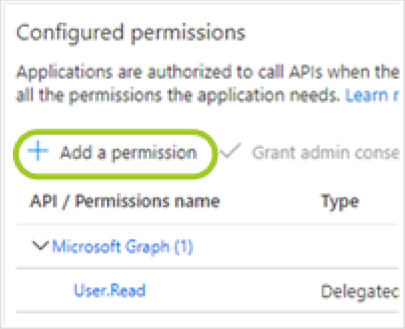
http://localhost

11. Select **Configure**

12. Select **Manage | API Permissions**



13. Select **Add a permission**

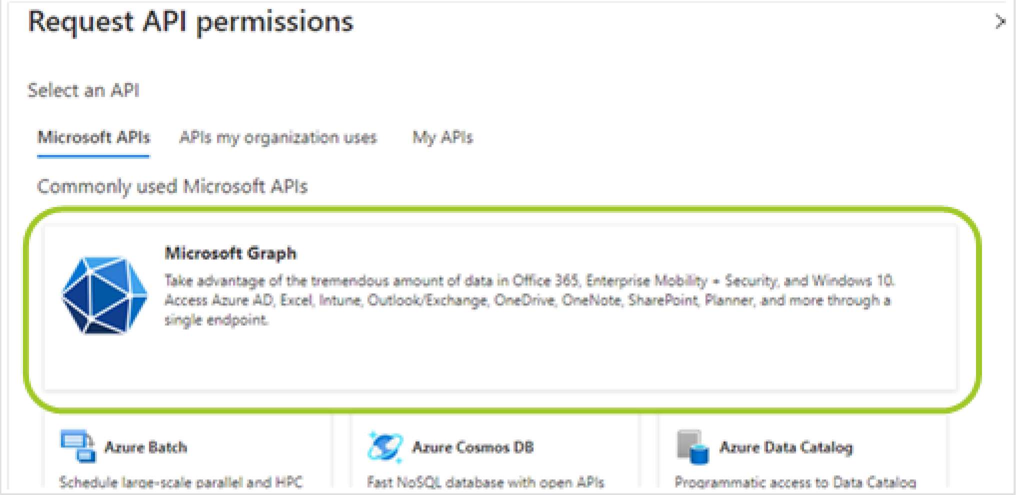


Configured permissions

Applications are authorized to call APIs when the all the permissions the application needs. Learn r

API / Permissions name	Type
Microsoft Graph (1)	
User.Read	Delegatec

14. In the **Request API permissions** pop-out pane on the right-hand side, select the **Microsoft Graph** tile:



Request API permissions

Select an API

Microsoft APIs | APIs my organization uses | My APIs

Commonly used Microsoft APIs

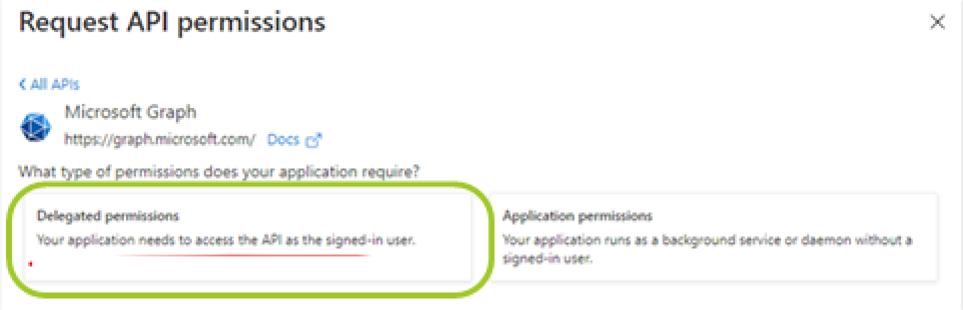
Microsoft Graph
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

Azure Batch
Schedule large-scale parallel and HPC

Azure Cosmos DB
Fast NoSQL database with open APIs

Azure Data Catalog
Programmatic access to Data Catalog

15. Select **Delegated permissions**



Request API permissions

< All APIs

Microsoft Graph
https://graph.microsoft.com/ Docs

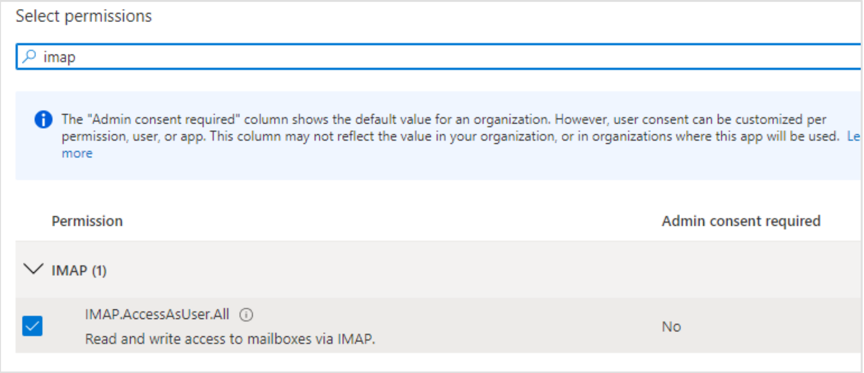
What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

16. Find the following permission scopes and tick the boxes next to them as shown:

- **IMAP.AccessAsUser.All**
- **SMTP.Send**

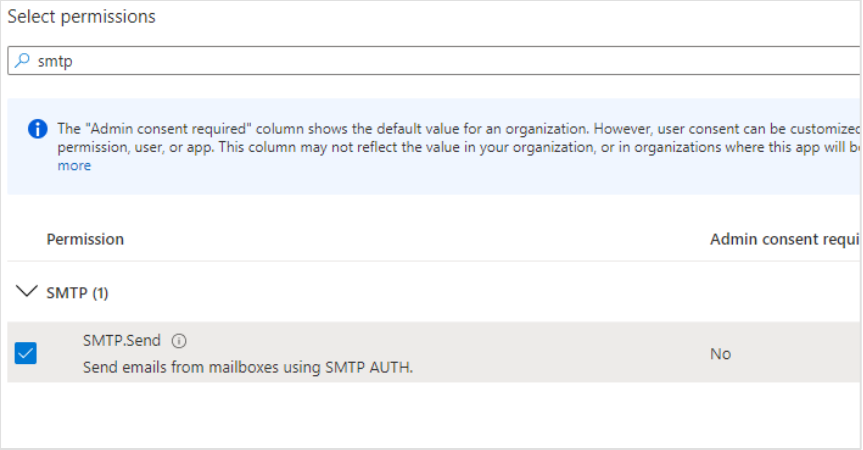


Select permissions

imap

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. Le more

	Permission	Admin consent required
	IMAP (1)	
☑	IMAP.AccessAsUser.All Read and write access to mailboxes via IMAP.	No



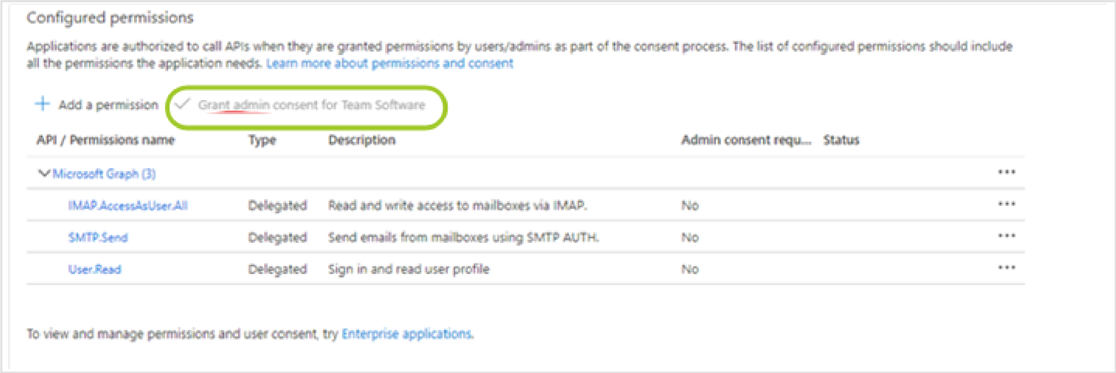
Select permissions

smtp

The "Admin consent required" column shows the default value for an organization. However, user consent can be customizec permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will b more

	Permission	Admin consent requi
	SMTP (1)	
☑	SMTP.Send Send emails from mailboxes using SMTP AUTH.	No

17. Select **Add permissions**



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

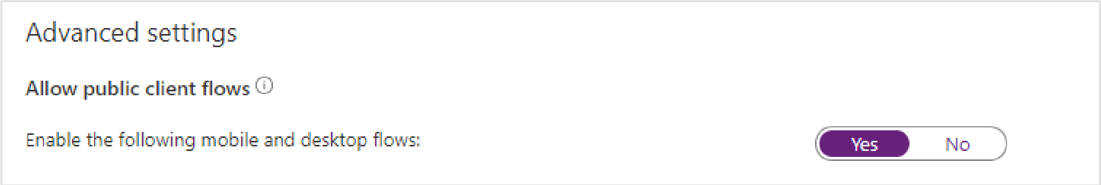
API / Permissions name	Type	Description	Admin consent requ...	Status	
∨ Microsoft Graph (3)					···
IMAP.AccessAsUser.All	Delegated	Read and write access to mailboxes via IMAP.	No		···
SMTP.Send	Delegated	Send emails from mailboxes using SMTP AUTH.	No		···
User.Read	Delegated	Sign in and read user profile	No		···

To view and manage permissions and user consent, try Enterprise applications.

18. If Admin consent needs to be granted, then select **Grant admin** which will be next to **Add a permission** (as highlighted above in green)

19. Select **Manage | Authentication**

20. Enable Public client flows - ensure **Yes** is selected for **Enable the following mobile and desktop flows**:

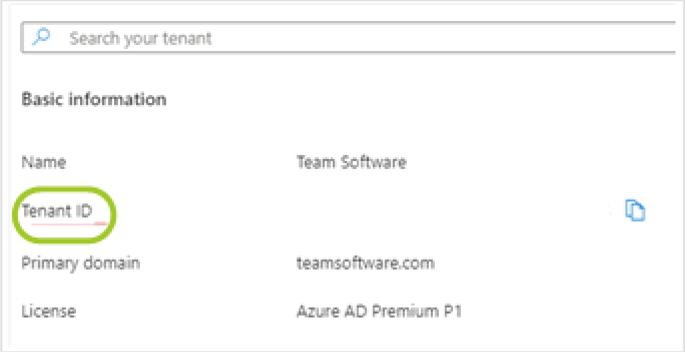


Advanced settings

Allow public client flows ⓘ

Enable the following mobile and desktop flows: ● Yes ○ No

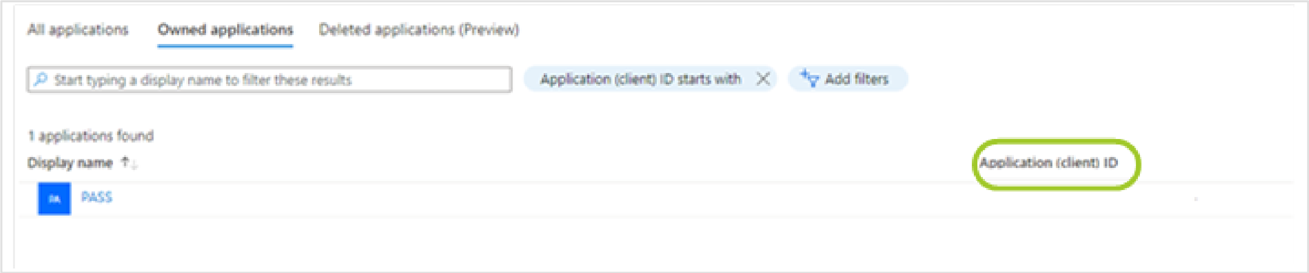
21. Select **Overview**. Make a note of the **Tenant ID**



Basic information

Name	Team Software
Tenant ID	
Primary domain	teamsoftware.com
License	Azure AD Premium P1

22. Select **Manage | App registrations** and make a note of the **Application (client) ID**



All applications
Owned applications
Deleted applications (Preview)
Start typing a display name to filter these results
Application (client) ID starts with ×
Add filters

1 applications found

Display name ↑↓	Application (client) ID
PASS	

These are stored, encrypted, in PASS, on the **Plugin Settings** tab of **General System Settings**, so that the plugin can access the mailbox.

SENDING AN INTERACTIVE USER AUTHORISATION

Authorisation can be granted either to the whole tenant or just the individual user account.

We recommend just granting it to the specific user account, using the following method:

Substitute your tenant and client IDs into the following URL (removing everything in blue and keeping it on one line):

https://login.microsoftonline.com/<tenant id>/oauth2/v2.0/authorize?client_id=<client id>&response_type=code&redirect_uri=https%3A%2F%2Flogin.microsoftonline.com%2Fcommon%2Foauth2%2Fnativeclient&response_mode=query&scope=https%3A%2F%2Fgraph.microsoft.com%2FIMAP.AccessAsUser.All https%3A%2F%2Fgraph.microsoft.com%2FSMTP.Send https%3A%2F%2Fgraph.microsoft.com%2FUser.Read

Note that there is a space between each of the scopes in the URL; these are the only spaces that should be present.

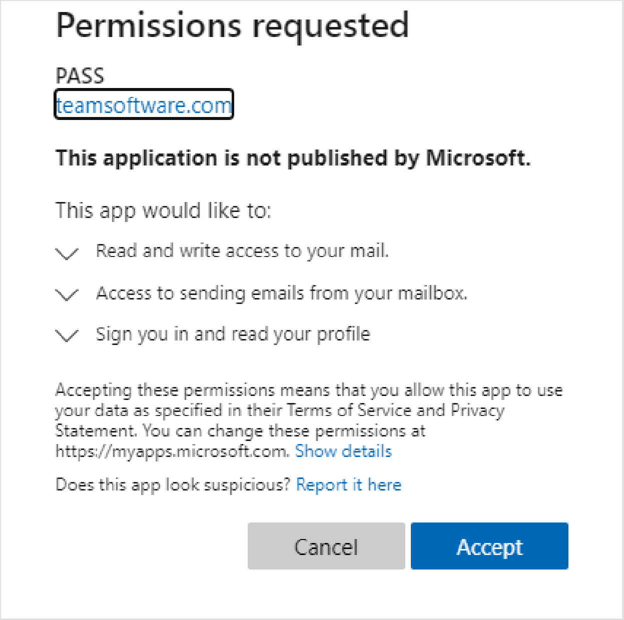
The scopes (permissions) being requested are:

https://graph.microsoft.com/IMAP.AccessAsUser.All	Grants IMAP access to download the emails, mark them as read and move them when required
https://graph.microsoft.com/SMTP.Send	Grants SMTP access to send emails through this account if failed emails are to be forwarded
https://graph.microsoft.com/User.Read	Grants read access to the user account

Copy and paste the whole URL into a browser. The spaces mean that just clicking will not pick up the whole link.

This will take you to a log on page where you need to enter the details of the mailbox email account. If you do not get a logon page you may need to use an Incognito session.

You will then be shown a page similar to this:



Permissions requested

PASS
teamsoftware.com

This application is not published by Microsoft.

This app would like to:

- Read and write access to your mail.
- Access to sending emails from your mailbox.
- Sign you in and read your profile

Accepting these permissions means that you allow this app to use your data as specified in their Terms of Service and Privacy Statement. You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

Select **Accept**

TEAM Software by WORKWAVE