Using “modern” auth for IMAP

A guide to setup OAuth email authentication to work with SCC

Using “modern” auth for IMAP with SCC

Introduction

For many years, client apps have used Basic Authentication to connect to servers, services and endpoints. It is enabled by default on most servers and services and is super simple to set up. Basic Authentication means the application sends a username and password with every request (often stored or saved on the device).

Simplicity isn’t at all bad in itself. Still, Basic Authentication makes it easier for attackers armed with today’s tools and methods to capture users’ credentials (particularly if not TLS protected), increasing the risk of credential re-use against other endpoints or services. Multi-factor authentication (MFA) isn’t easy to enable when you are using Basic Authentication, and so all too often, it isn’t used.

With these threats and risks in mind, many email providers are improving data security by implementing MFA and modern authentication methods like Open Authorization or OAuth.

When using email apps on the web (or desktop), end users must enable MFA to authorise it to connect and read emails. On the other hand, SCC is designed to use a business inbox to read emails from and then distribute them to agents using the ASD. The interaction, in this case, can be understood as machine-to-machine and needs to happen without human intervention. This is the use case for the OAuth Client Credentials Flow, where applications pass their Client Secret and Client ID to an authorisation server, which authenticates the user, and returns a token. This happens without any user intervention.

This document describes how to configure authentication tokens for Gmail, Outlook.com and Office365 and how to use them in the Softdial Contact Center.

To date, the information is that this change does not affect SMTP AUTH – and all known email providers will continue supporting Basic Authentication for the time being.

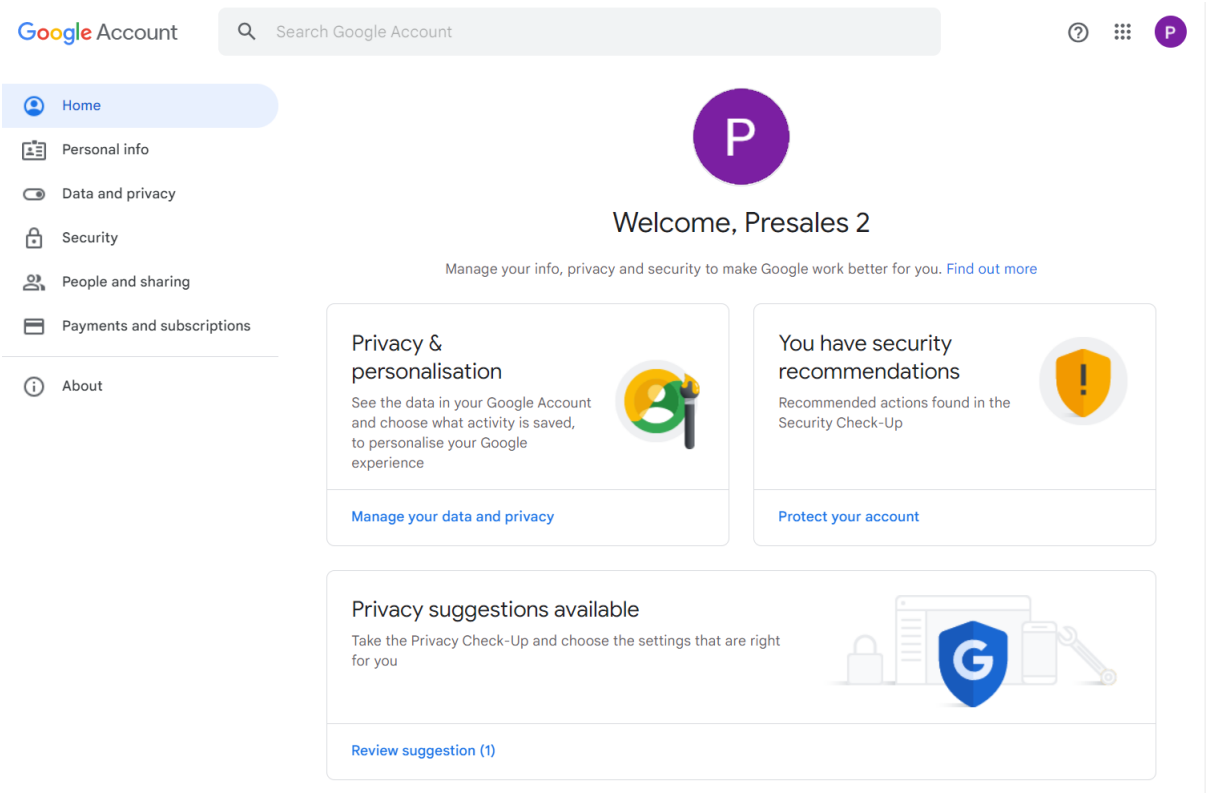
In the following sessions, the necessary configurations will be discussed for most of the known email platforms. Further questions can be addressed to support@sytel.com.

Gmail Application Password

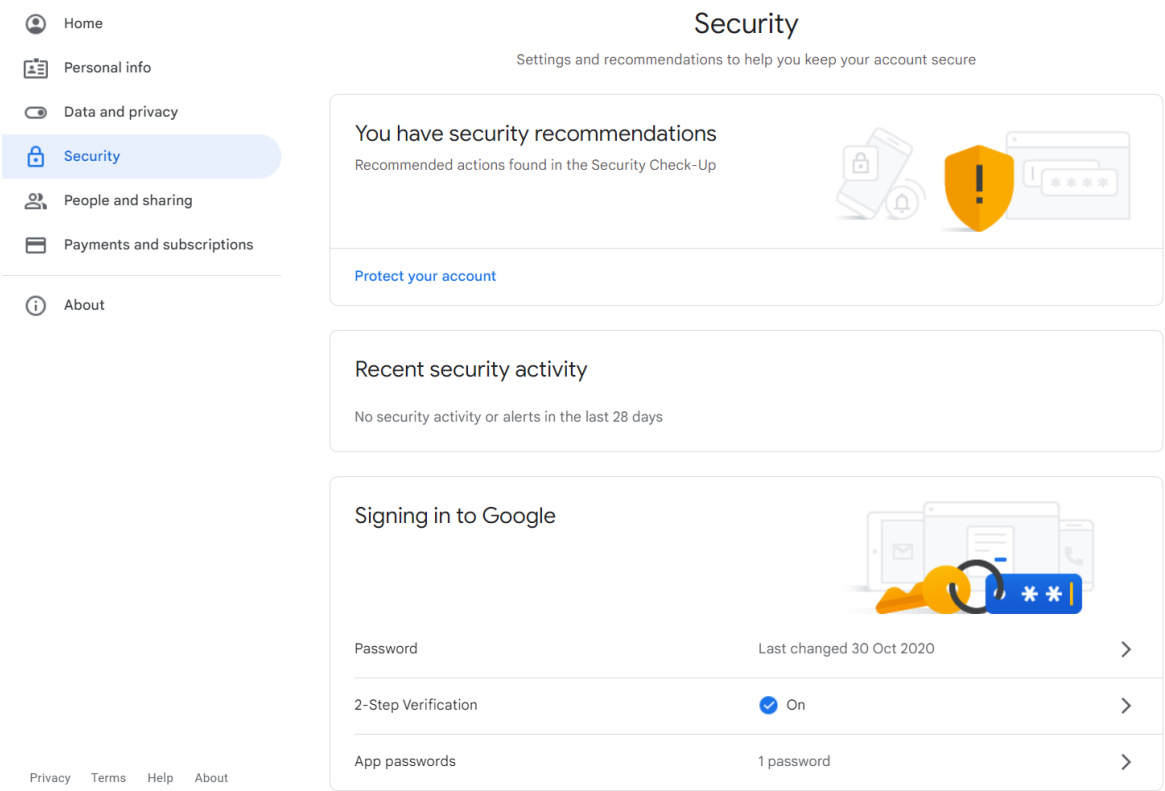
Gmail accounts (xxx@gmail.com) will demand that users enable Two-factor Authentication to proceed with the application token creation. The following steps will guide you on how to create an application token. This is a more secure IMAP authentication option because it needs MFA to create the application password.

Please follow these steps to create an application password to enable a service to connect to a gmal.com account using IMAP.

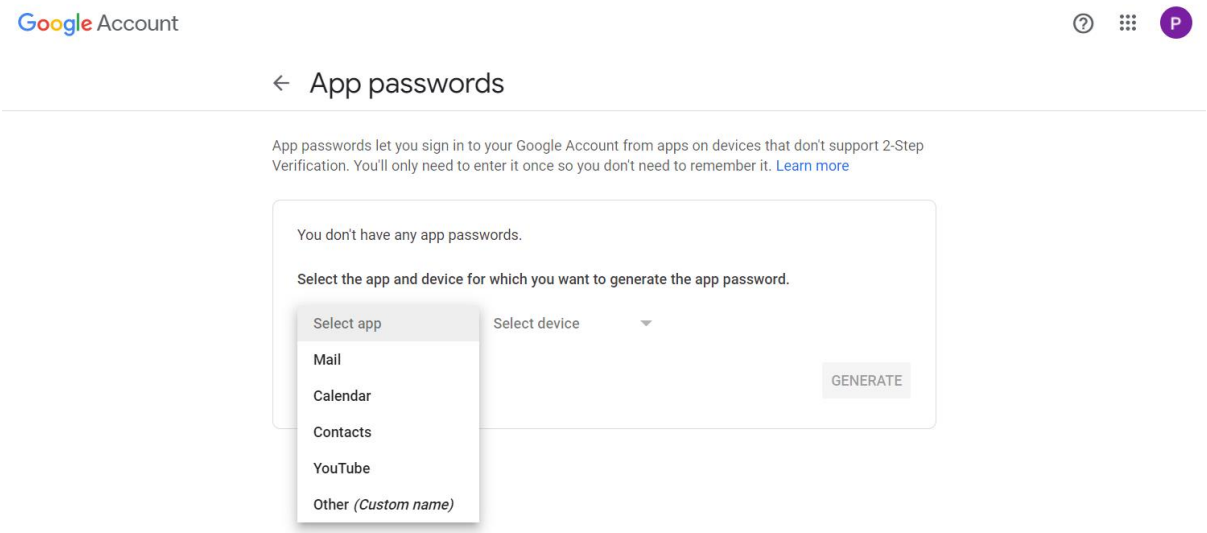
1) Go to your Google Account Page



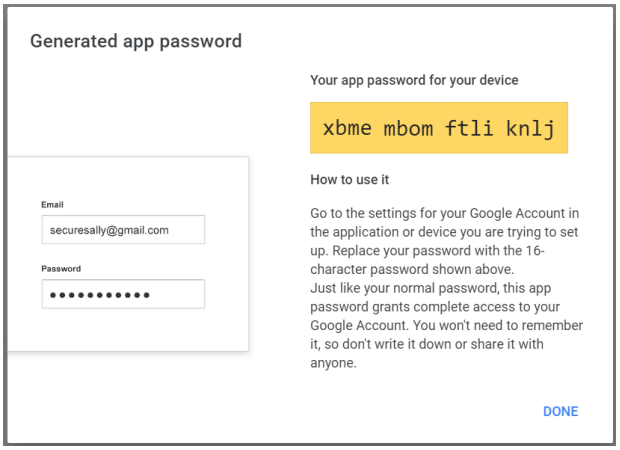
2) Go to Security options and “App passwords”. Please note that 2-Step Verification needs to enable at this point.



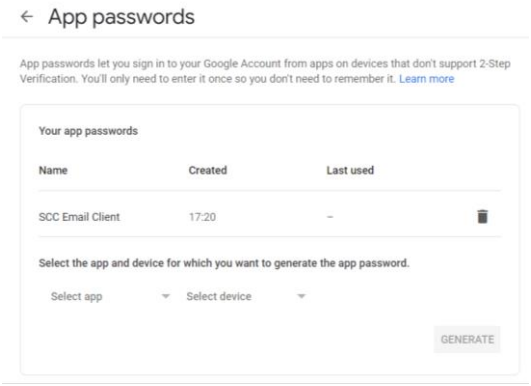
3) Select "*Other (Custom name)*" to create an application password for your account.



4) Define a relevant Application Name like "SCC Email Client" and click "Generate".



Read the instructions and copy the application password for SCC. This will be the password used in the SCC Workflow email configuration. Once your app password is created, you can see a record on the App passwords screen.



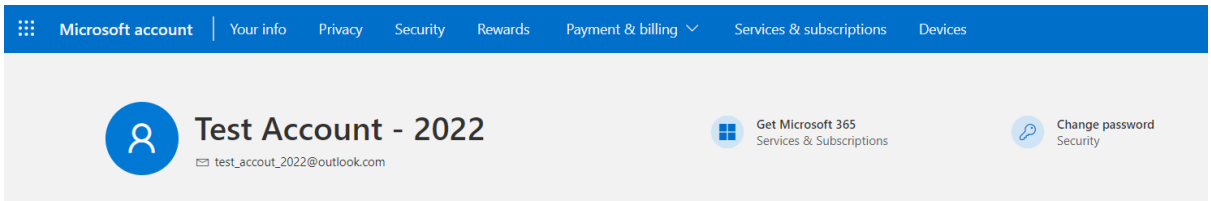
Outlook.com Application Password

Outlook.com accounts (xxx@outlook.com) will demand that users to enable Two-step Authentication to proceed with the application token creation. Microsoft will tend to ask users to use Microsoft Authenticator app as the preferred tool to implement MFA using smartphones.

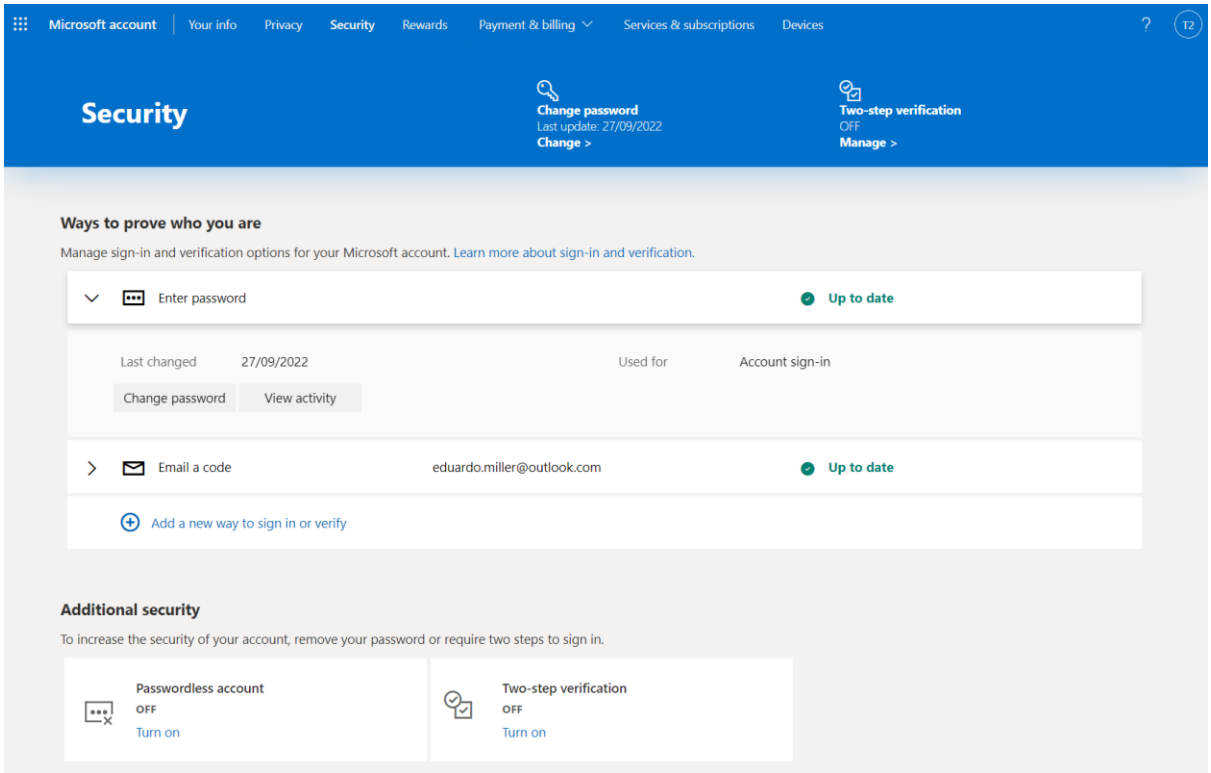
The following steps will guide you in creating an application token in your Microsoft account. This is a more secure IMAP authentication option because it needs MFA to create the application password.

Please follow these steps to create an application password to enable a service to connect to an outlook.com account using IMAP.

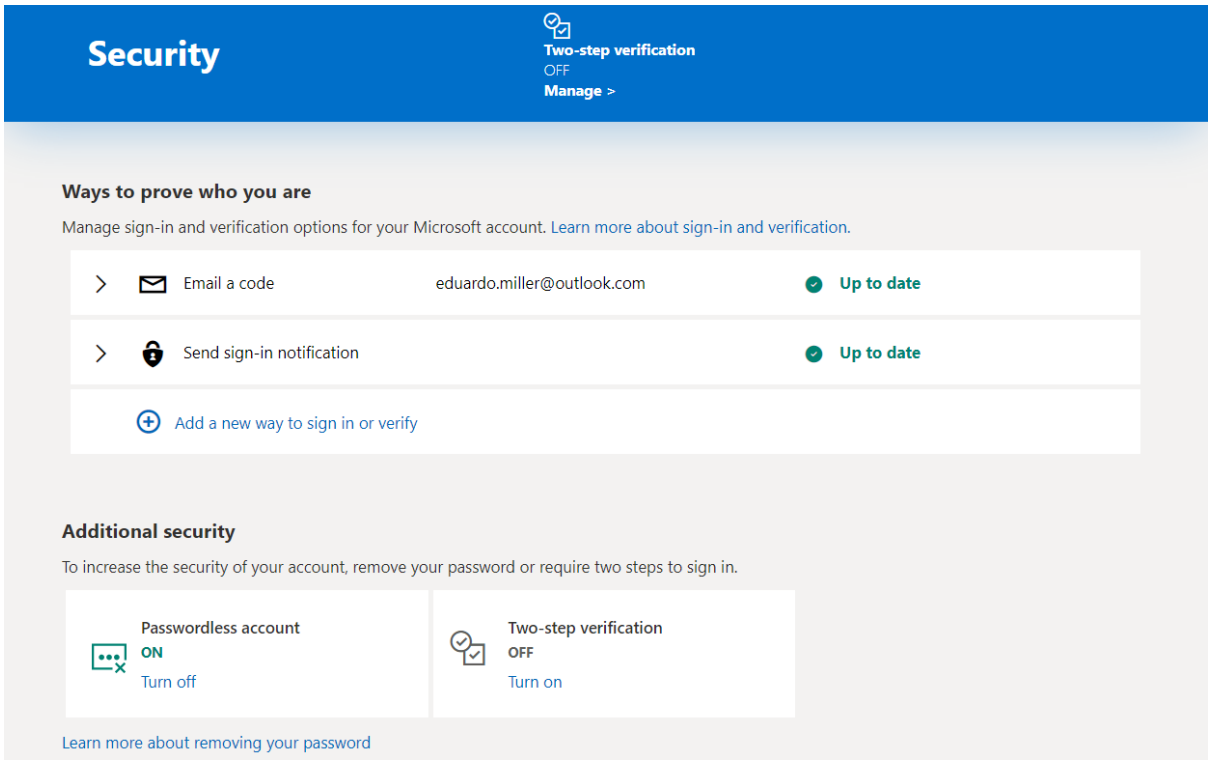
1) Open your Microsoft Account



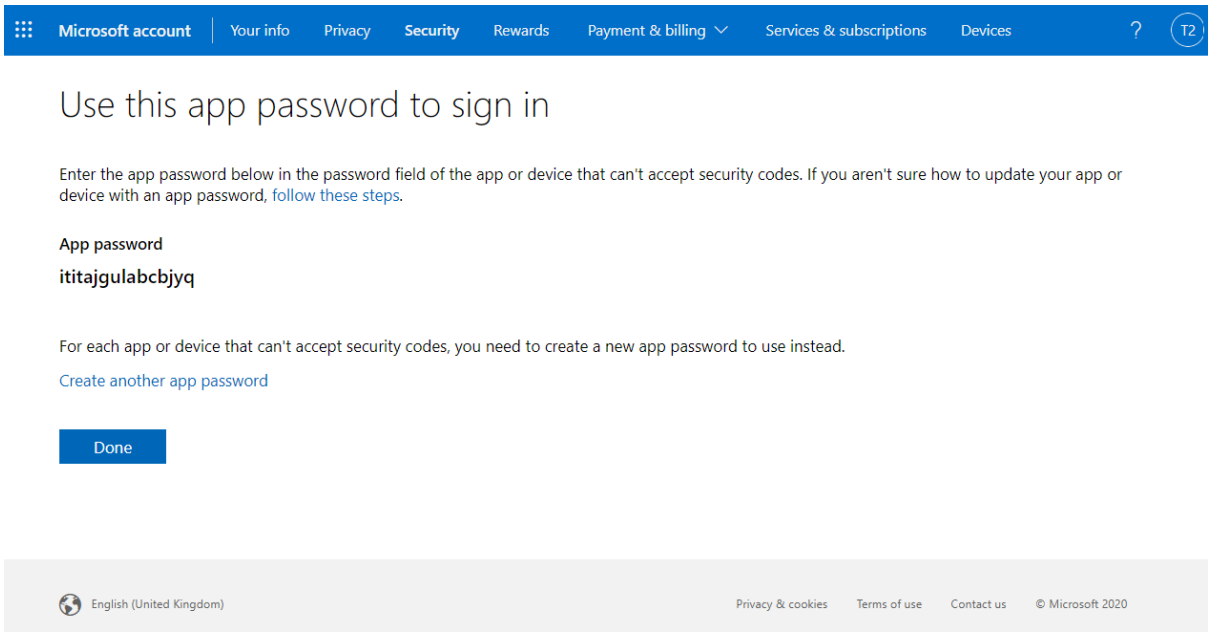
2) Open the Security options and enable the "Passwordless account" for your account.



3) After enabling the “Passwordless account”, an extra option for App passwords is enabled.



4) Create a new app password.



Read the instructions and copy the application password for SCC. This will be the password used in the SCC Workflow email configuration. Once your app password is created, you can see an option to delete it in the App passwords screen.

Office 365 Application Registration

Office 365 accounts (xxx@yourdomain) will demand users to enable Two-step Authentication to proceed with the application registration. Microsoft will tend to ask users to use Microsoft Authenticator app as the preferred tool to implement MFA using smartphones.

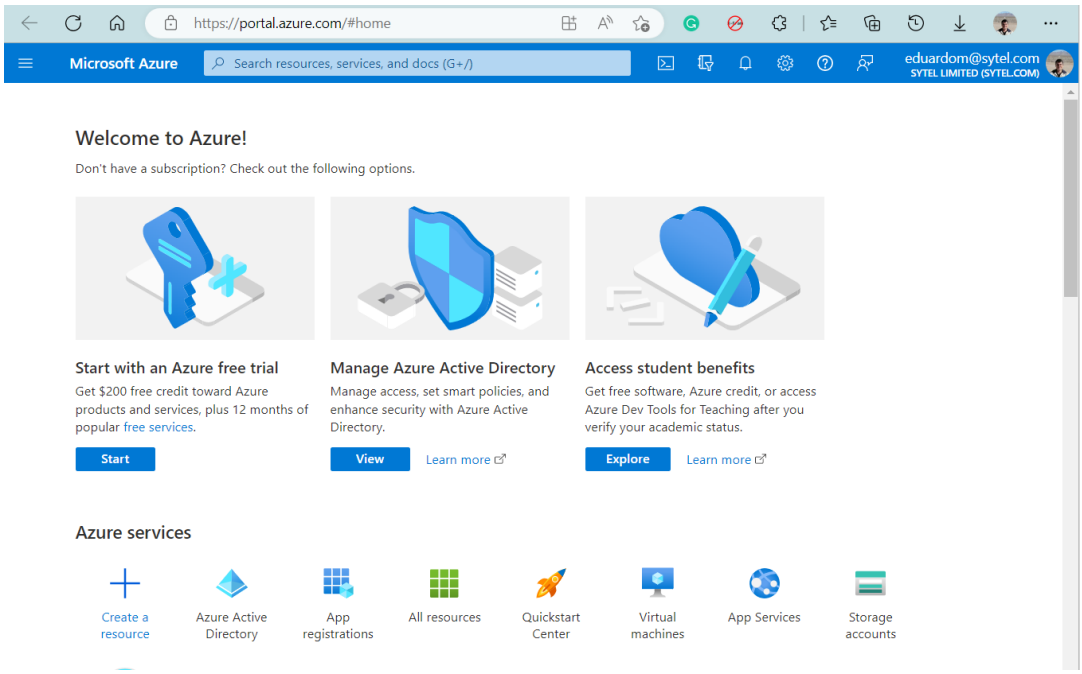
The paid email service from Microsoft requires the use of OAuth APIs, and the application connecting to your company's domain to read emails needs to be registered. The Microsoft identity platform performs identity and access management (IAM) only for registered applications. Whether a client application like a web or mobile app or a web API that backs a client app, registering it establishes a trust relationship between your application and the identity provider, the Microsoft identity platform.

Please note that Office 365, the paid version of Microsoft Mail, has other options available, and this document will also cover those.

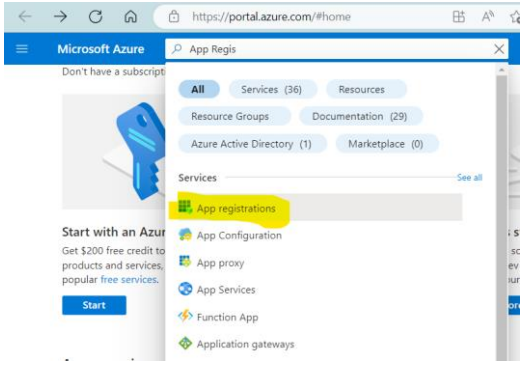
Please follow these steps to create an application password to enable a service to connect to an outlook.com account using IMAP.

Register an application with the Microsoft identity platform

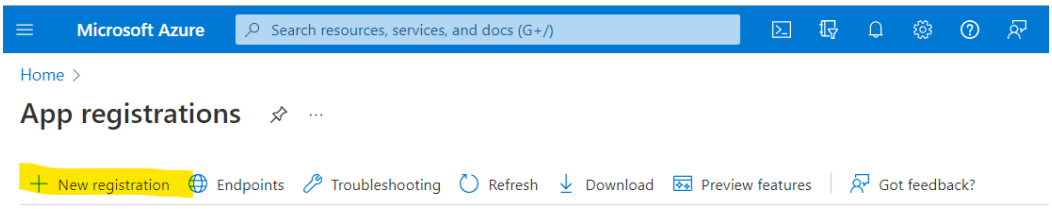
Go to Azure Portal using a user from your Office365 subscription. The Azure account must have permission to manage applications in Azure Active Directory (Azure AD). Any of the following Azure AD roles include the required permissions: Application administrator, Application developer or Cloud application administrator.



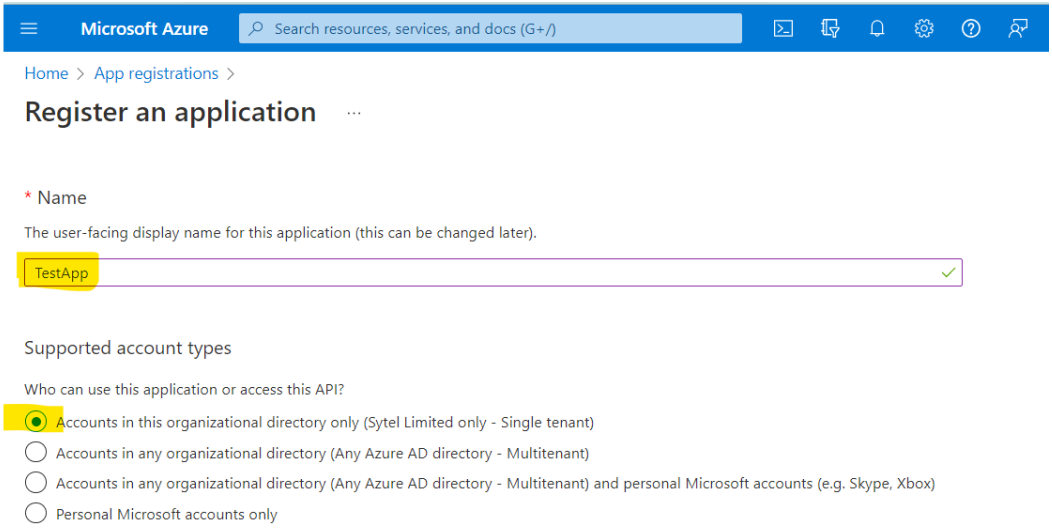
Open App Registrations to Register an application.



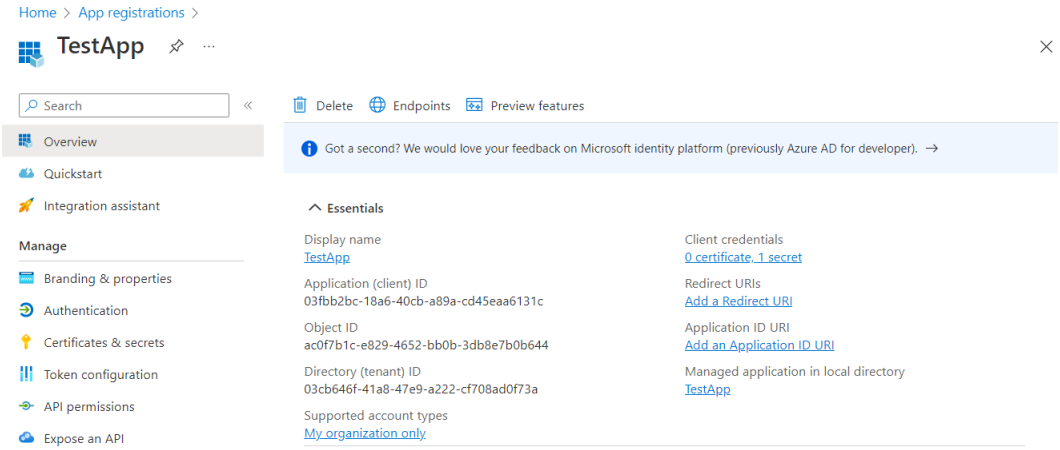
Choose a New Registration.



Fill only the field in yellow and click “Register” at the bottom.



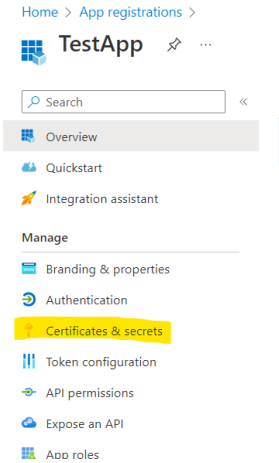
In the next screen, copy the values *Client ID* and *Tenant ID*.



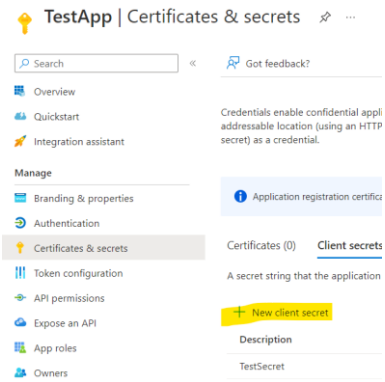
The application is now created. Client ID and Tenant ID will be used later.

Generate Client Secret

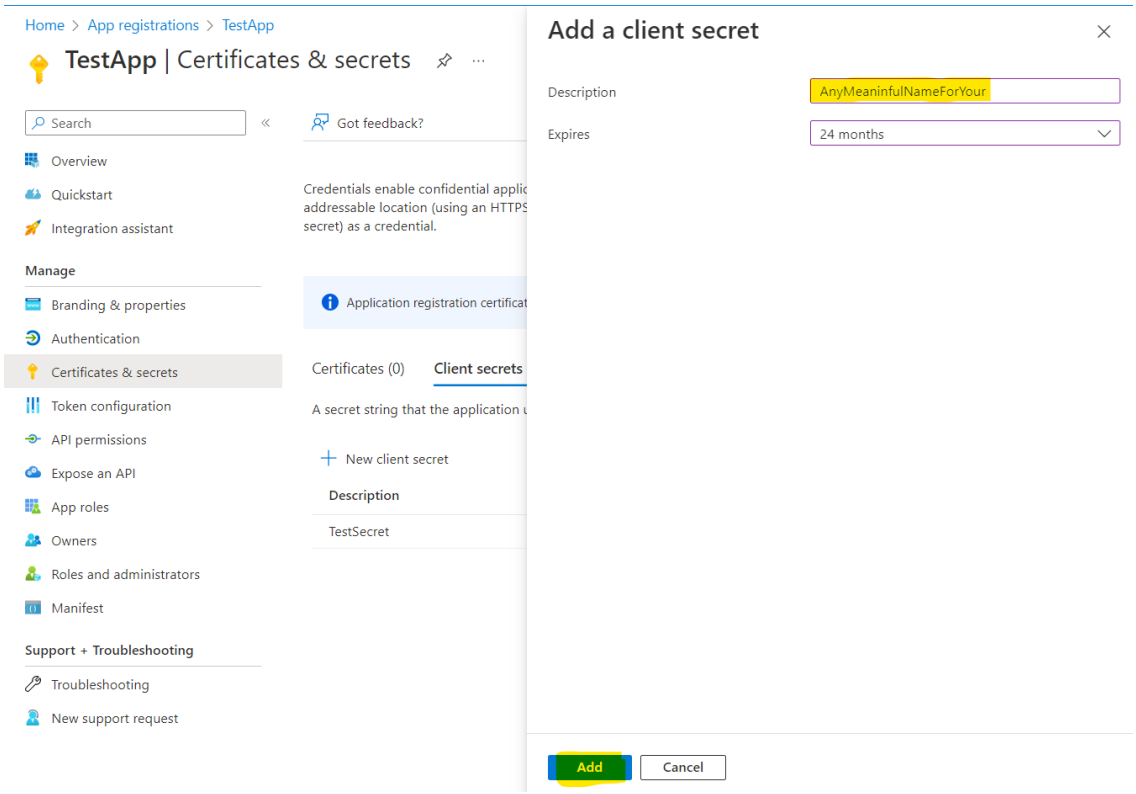
Go to Certificates & Secrets.



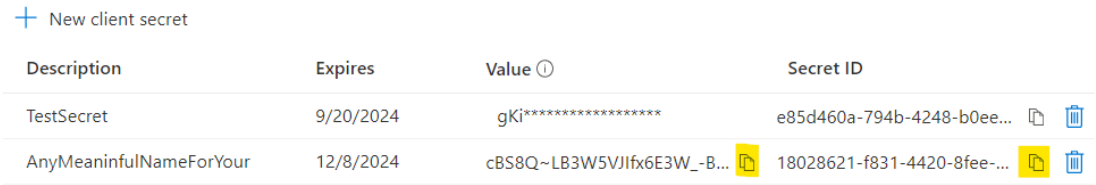
Click New client secret.



Fill out the form - any meaningful name for the secret – choose the relevant expiration. Once the secret expires, the process from this point needs to be done again.



Copy the secret value and the secret id.

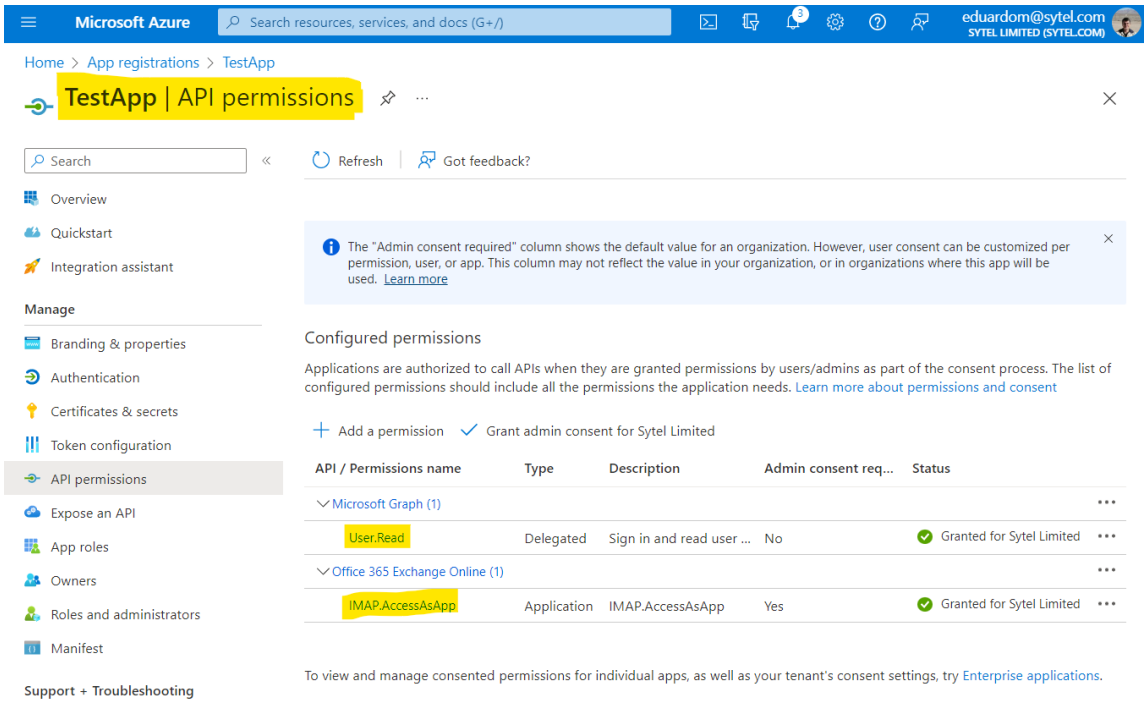


The fields “Secret Value” and Secret ID will be used later. Keep them safe.

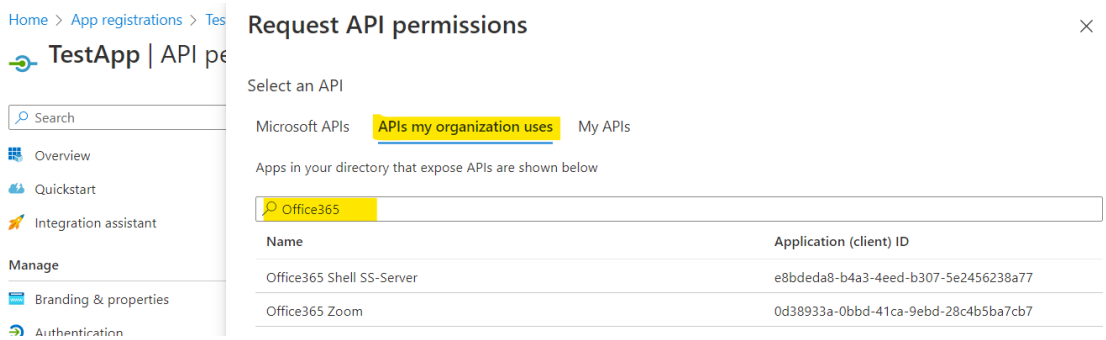
Note the secret value, as it is shown only during creation.

Give the app the correct permissions to access the Exchange using IMAP

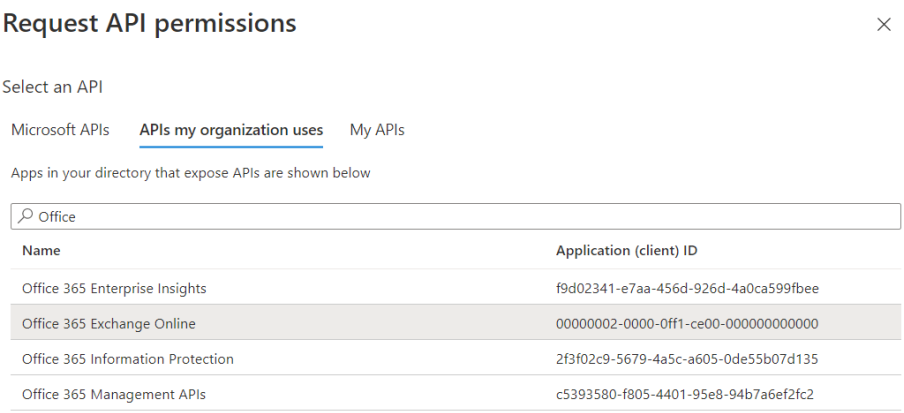
Open API Permissions to set the permissions for the application.



Click Add permission.

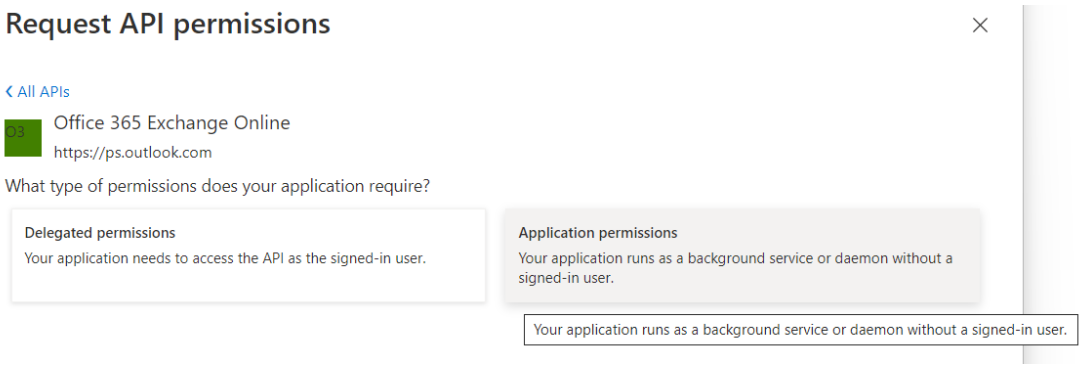


Choose APIs my organisation uses. Search Office365 (use the search bar).

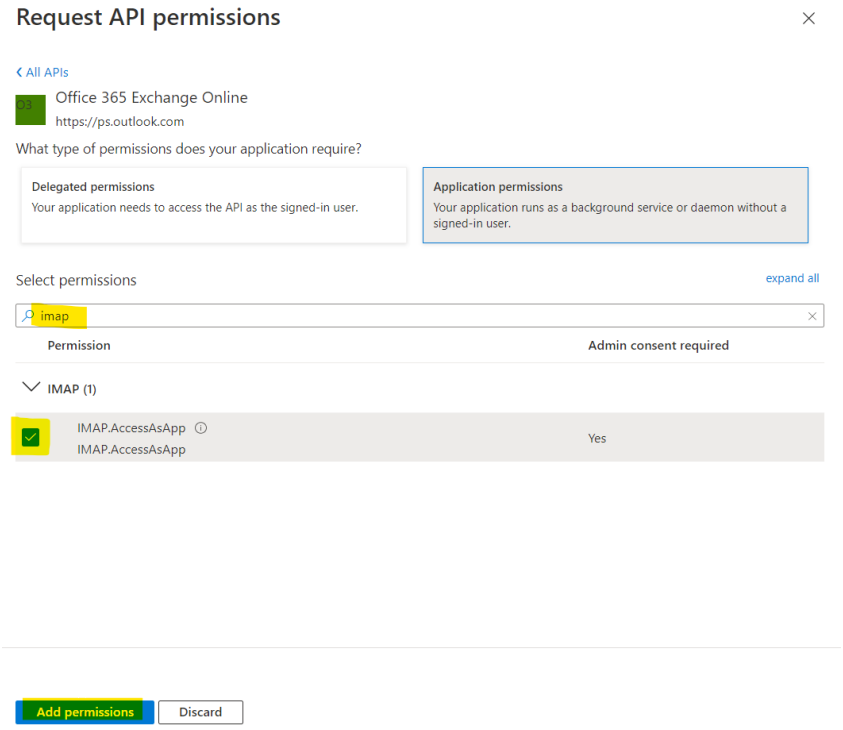


Select Office 365 Exchange Online.

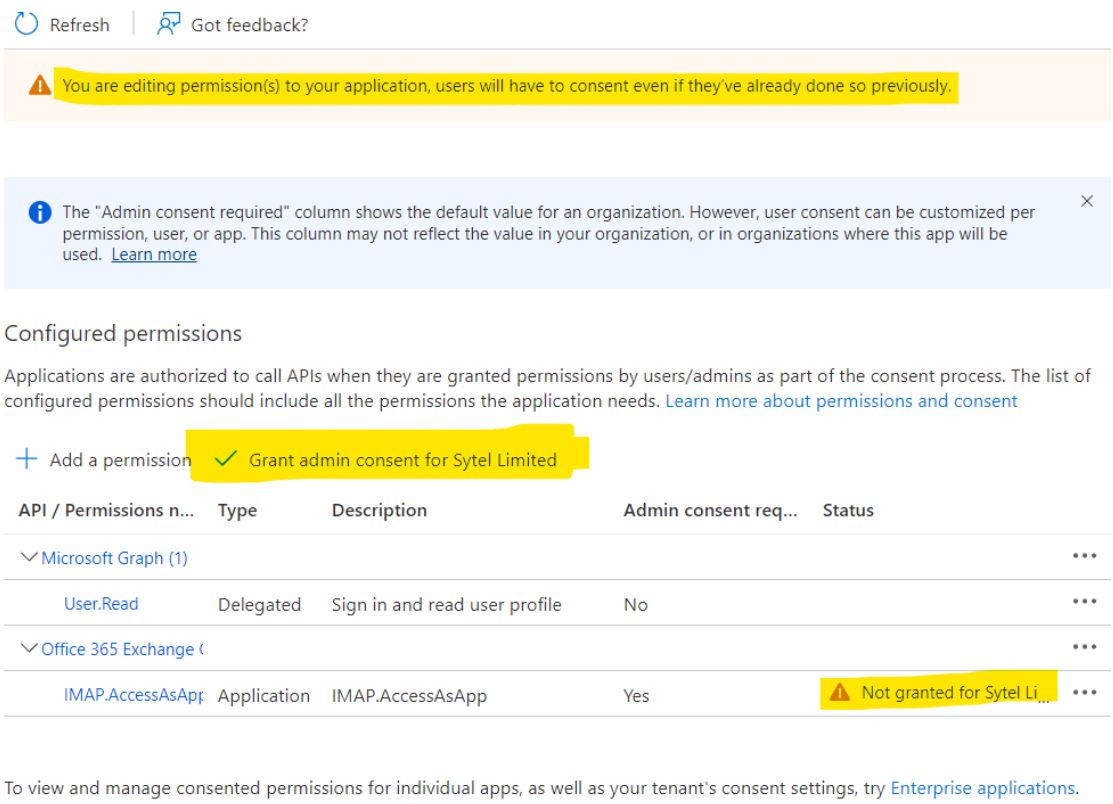
In the next screen, select Application Permissions.



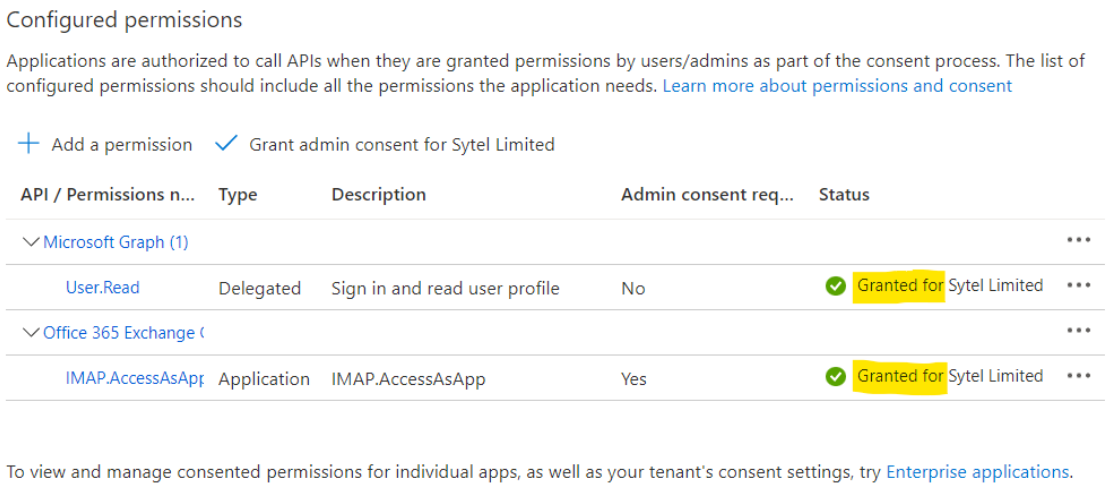
Then, search for IMAP. Check *IMAP.AccessAsApp*. Click Add Permissions.



In the next screen, click Grant admin consent for “<your customer’s tenant name>”.

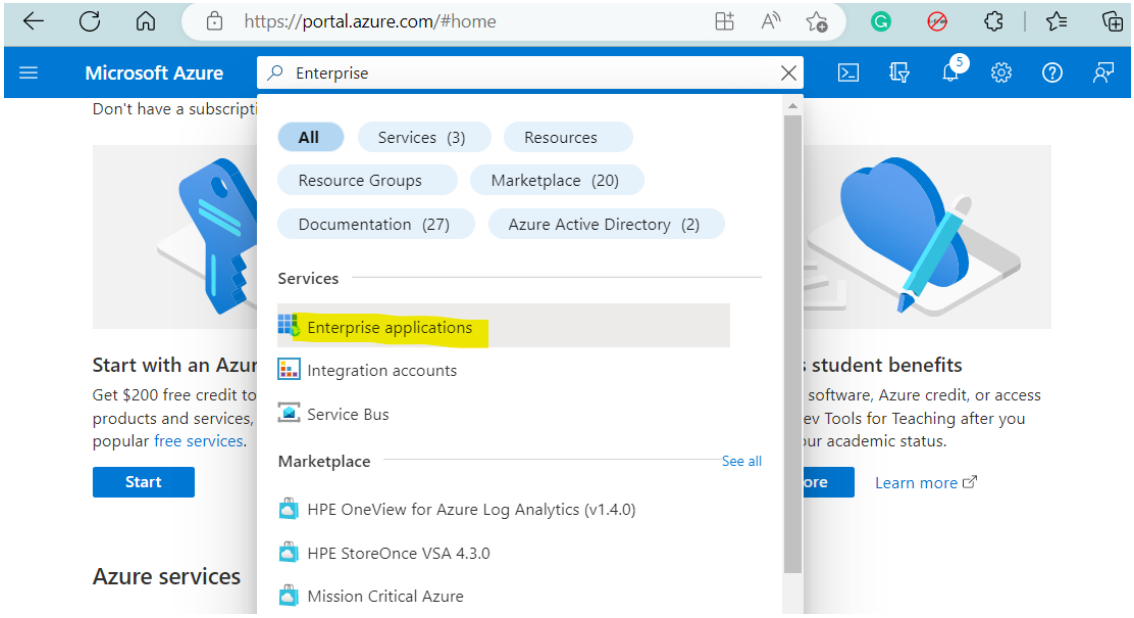


The result will be.

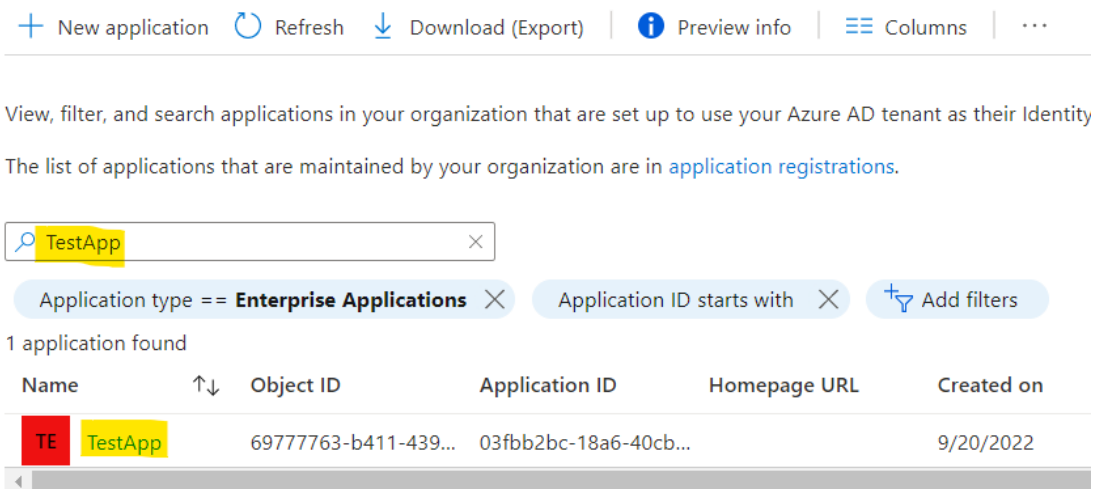


Get your Application Object Id from the Enterprise application.

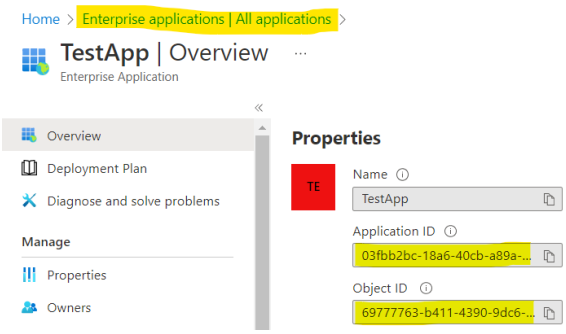
In the Azure portal home screen, search for Enterprise applications and open it.



Please search for your App and open it.



Copy the Application IF and the Object ID to be used later.



Granting Exchange Online permissions using PowerShell

Follow PowerShell commands to grant permission in the inbox to the app.

Use Windows PowerShell on your machine to Register service principals in Exchange.

Set execution policy first:

```
Set-ExecutionPolicy RemoteSigned
```

Install ***ExchangeOnlineManagement*** module:

```
Install-Module -Name ExchangeOnlineManagement
Import-Module ExchangeOnlineManagement
```

Connect and login as an administrator (you'll be prompted for a password):

```
Connect-ExchangeOnline -UserPrincipalName your-admin-account@your-domain.onmicrosoft.com
```

For Exchange running in hybrid mode, log in using the following code:

```
$lc = Get-Credential
Connect-ExchangeOnline -Credential $lc
```

Create service principal.

```
New-ServicePrincipal-AppId <APPLICATION_ID> -ServiceId <OBJECT_ID> -DisplayName <AMeaninfullName>
```

Example:

```
New-ServicePrincipal -AppId 061851f7-08c0-40bf-99c1-ebd489c11f16  -ServiceId 4352fc11-5c2f-4b0b-af40-447ff10664e8 -DisplayName "SCC EmailService"
```

Note: If you still get an error running the New-ServicePrincipal cmdlet after you perform these steps, it is likely due to the fact that the user doesn't have enough permissions in Exchange Online to perform the operation. By default, this cmdlet is available to users assigned the Role Management role

Add permissions to a specific mailbox:

```
Add-MailboxPermission
-Identity "<USER@your-domain.onmicrosoft.com>"
-User <OBJECT_ID>
-AccessRights FullAccess
```

Example:

```
Add-MailboxPermission -Identity "AdeleV@your-domain.onmicrosoft.com"  -User
4352fc11-5c2f-4b0b-af40-447ff10664e8 -AccessRights FullAccess
```

Shared mailboxes

You need to use Add-MailboxPermission for every shared mailbox you need access to:

```
Add-MailboxPermission
 -Identity "shared@your-domain.onmicrosoft.com"
 -User <OBJECT_ID>
 -AccessRights FullAccess
```

These instructions were compiled using the following links (valid in December 2022).

OAuth 2.0 client credential flow with Office365/Exchange IMAP/POP3 | Blog | Limilabs

Office 365 and IMAP with OAuth 2.0 authentication in unattended (app-only) mode

Understanding Client Credentials Flow in OAuth 2.0 | by DLT Labs | Medium

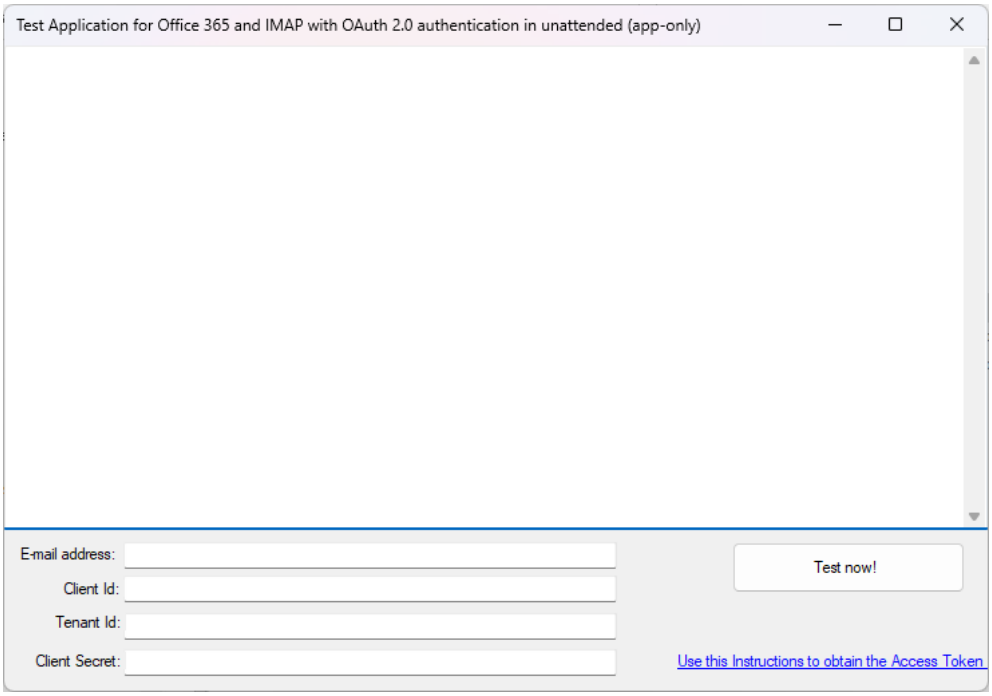
Testing the Azure Business Setup

Because of the complexity, Sytel provides a too to validate the Office 365 confidurations. The below standalone application can help you to validate your Azure Business configuration.

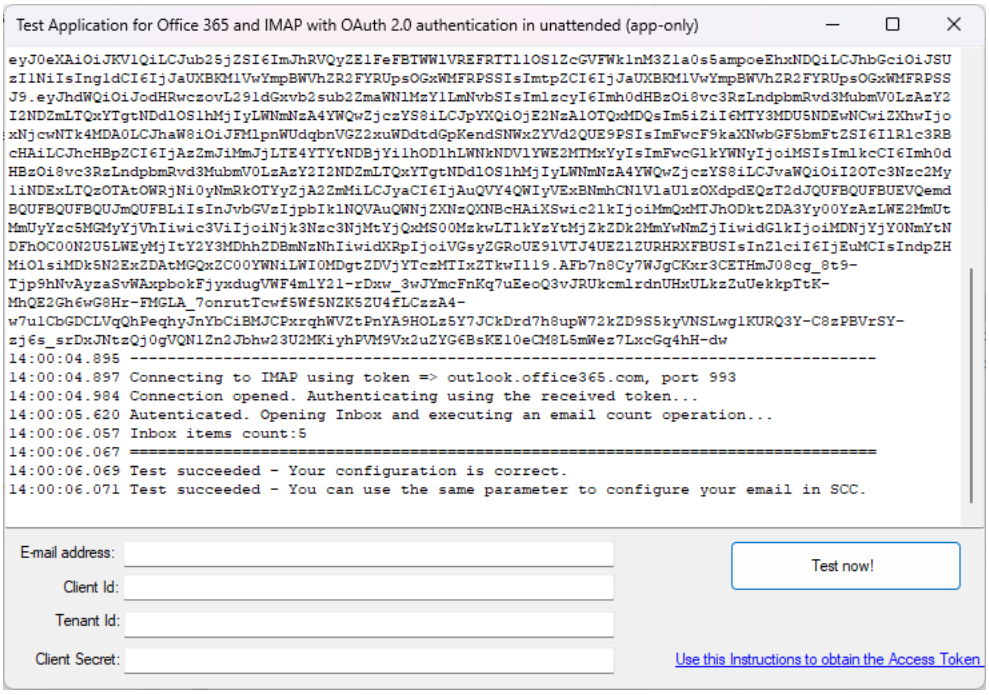
IMAP_OAuth_Tester.exe

The application IMAP_OAuth_Tester.exe can be requested to support@sytel.com.

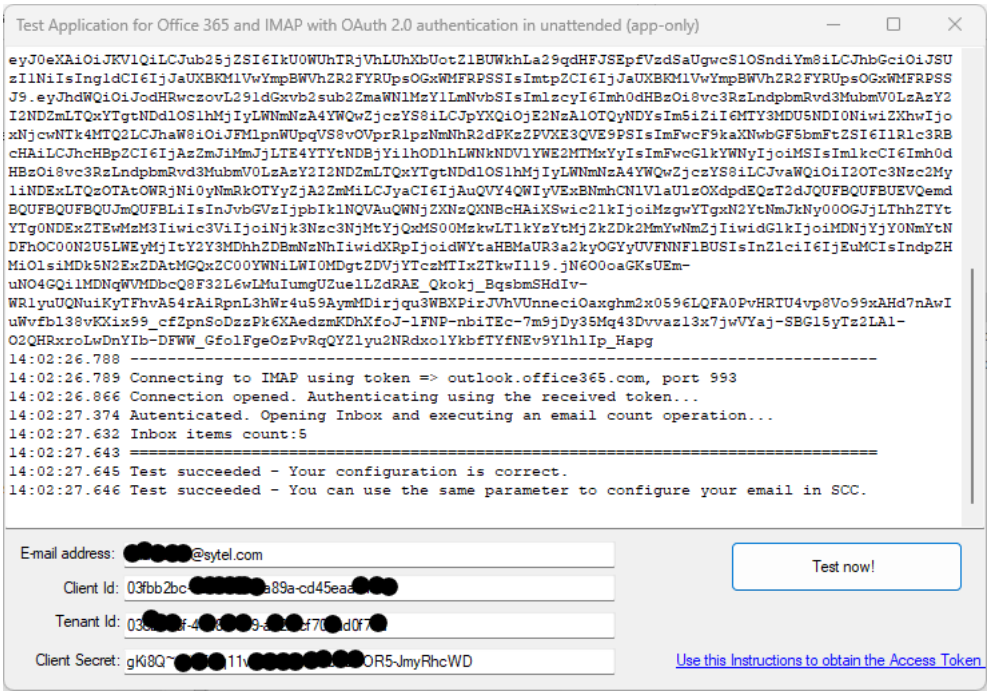
Run this application from any computer using Windows 10 or newer with internet access.



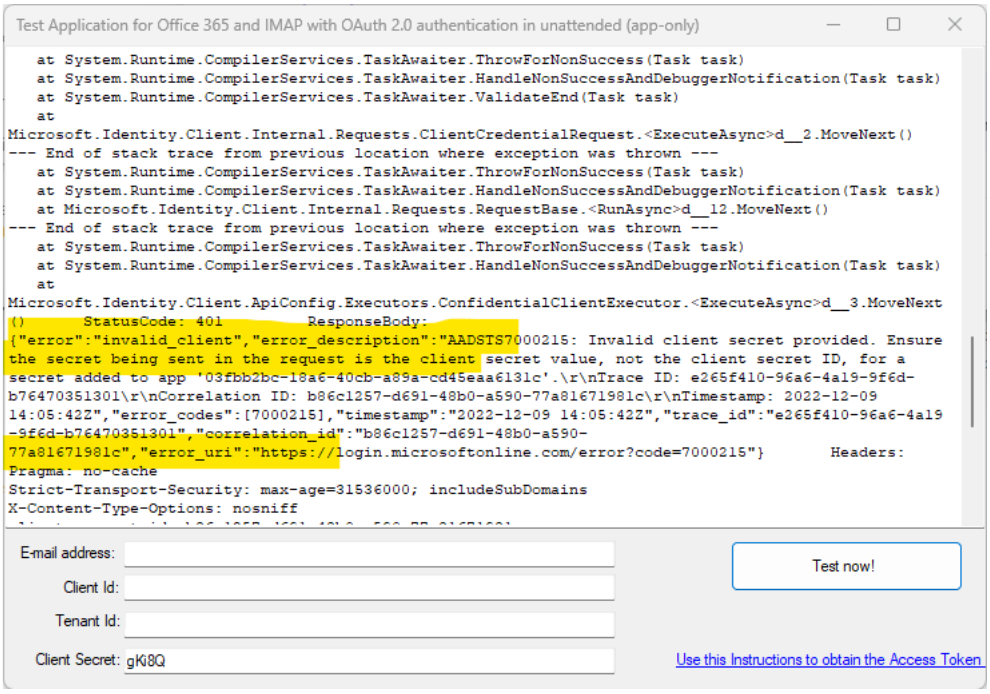
Firstly validate if your environment is appropriate for the execution of the test. Without adding any information just click “Test now!”. The application will run the test using some hardcoded information. A result will be shown in the logging area.



Fill the four fields with the information collected from the configuration process for Office365 and run the process again. Please note, for “Client Secret” you will need the secret Value and not the Secret ID.



If you receive an error message, check the logging area for the correct information to point you to fix the issue at the Azure Portal. The error message is a response from the Azure/Office 365 authentication servers. The image below shows an error related to an attempt using a wrong secret.



Email Setup in SCC

The email setup in SCC did not change, and the steps found on Sytel Help (for email)are updated to comply with this new authentication option.

In the Softdial Workflow config.xml file, you will find the email configurations.

```
<Campaign tenantID="default" name="CampaignNameGoesHere">
        <campaignType>0</campaignType>
       <className>InboundEmailImap</className>
        <assemblyName>WorkflowEmail.dll</assemblyName>
        <UserParams>
      <![CDATA[
      <EmailConfig>
        <UseBasicAuth>true</UseBasicAuth>
        <UseAzureBusinessAuth>false</UseAzureBusinessAuth>
        <AzureBusinessAuthClientId>paste client id here</AzureBusinessAuthClientId>
        <AzureBusinessAuthTenantId>paste tenant id here</AzureBusinessAuthTenantId>
        <AzureBusinessAuthSecret>paste secret value here</AzureBusinessAuthSecret>
        <LogsPath>C:\logs\Email</LogsPath>
        <SmtpServer>smtp server address</SmtpServer>
        <SmtpPort>587</SmtpPort>
        <ImapServer>imap server address</ImapServer>
        <ImapPort>993</ImapPort>
        <PopServer>pop server address</PopServer>
        <PopPort>995</PopPort>
        <EmailAccount>account goes here</EmailAccount>
        <AccountDomain>account domain without @ goes here </AccountDomain>
        <EmailAccountPass>password goes here</EmailAccountPass>
        <CC>One or more email address here(comma separated)</CC>
        <BCC>One or more email address here(comma separated)</BCC>
        <UseSsl>true</UseSsl>
        <DataSourceName>historical database odbc goes here</DataSourceName>
        <DataSourceUser>odbc user goes here</DataSourceUser>
        <DataSourcePass>odbc password goes here</DataSourcePass>
        <ControllerIp>controller ip goes here</ControllerIp>
        <EmailDiskSpace>100</EmailDiskSpace>
        <DiskSpaceWarningLimit>20</DiskSpaceWarningLimit>
        <EmailAlert></EmailAlert>
        <SendEmailAlert>false</SendEmailAlert>
        <EmailInboxFolder>C:\Softdial\WebServer\www\EmailInbox</EmailInboxFolder>
        <EmailCheckInterval>10</EmailCheckInterval>
        <SleepBeforeSendNewIc>10</SleepBeforeSendNewIc>
        <AnswerEmails>true</AnswerEmails>
  <ForwardEmails>false</ForwardEmails>
  </EmailConfig>
  ]]></UserParams>
</Campaign>
```

The new parameters in bold will define the IMAP authentication behaviour.

UseBasicAuth: When true, the IMAP authentication will be the basic authentication. It will use a user and password to authenticate access to an IMAP inbox. If False, SCC will use OAuth to authenticate.

In the case of Google Mail and Outlook.com, use the application token in the password field.

If you are using Office 365 Business, you need to define the next parameters:

UseAzureBusinessAuth: Set to yes.

AzureBusinessAuthClientId: The client ID.

AzureBusinessAuthTenantId: The tenant ID.

AzureBusinessAuthSecret: The application secret VALUE.

www.sytel.com
info@sytel.com
+44 (0)1296 381 200

Sytel Limited 1 Cromwell Court New Street Aylesbury Buckinghamshire HP20 2PB UK