



# 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](mailto:support@sytel.com).

## Gmail Application Password

Gmail accounts ([xxx@gmail.com](mailto: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 gmail.com account using IMAP.

- 1) Go to your Google Account Page

Home

Personal info

Data and privacy

Security

People and sharing

Payments and subscriptions

About



Welcome, Presales 2

Manage your info, privacy and security to make Google work better for you. [Find out more](#)

### Privacy & personalisation

See the data in your Google Account and choose what activity is saved, to personalise your Google experience

[Manage your data and privacy](#)

### You have security recommendations

Recommended actions found in the Security Check-Up

[Protect your account](#)

### Privacy suggestions available

Take the Privacy Check-Up and choose the settings that are right for you

[Review suggestion \(1\)](#)

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

Home

Personal info

Data and privacy

Security

People and sharing

Payments and subscriptions

About

## Security

Settings and recommendations to help you keep your account secure

### You have security recommendations

Recommended actions found in the Security Check-Up

[Protect your account](#)

### Recent security activity

No security activity or alerts in the last 28 days

### Signing in to Google



Password

Last changed 30 Oct 2020



2-Step Verification

✓ On



App passwords

1 password



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

Google Account

← App passwords

App passwords let you sign in to your Google Account from apps on devices that don't support 2-Step Verification. You'll only need to enter it once so you don't need to remember it. [Learn more](#)

You don't have any app passwords.

Select the app and device for which you want to generate the app password.

Select app: Mail, Calendar, Contacts, YouTube, Other (Custom name)

Select device: [dropdown]

GENERATE

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

Generated app password

Your app password for your device

xbme mbom ftli knlj

How to use it

Go to the settings for your Google Account in the application or device you are trying to set up. Replace your password with the 16-character password shown above. Just like your normal password, this app password grants complete access to your Google Account. You won't need to remember it, so don't write it down or share it with anyone.

EMAIL: securesally@gmail.com

PASSWORD: [masked]

DONE

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.

← App passwords

App passwords let you sign in to your Google Account from apps on devices that don't support 2-Step Verification. You'll only need to enter it once so you don't need to remember it. [Learn more](#)

Your app passwords

Name	Created	Last used
SCC Email Client	17:20	-

Select the app and device for which you want to generate the app password.

Select app: [dropdown] Select device: [dropdown]

GENERATE

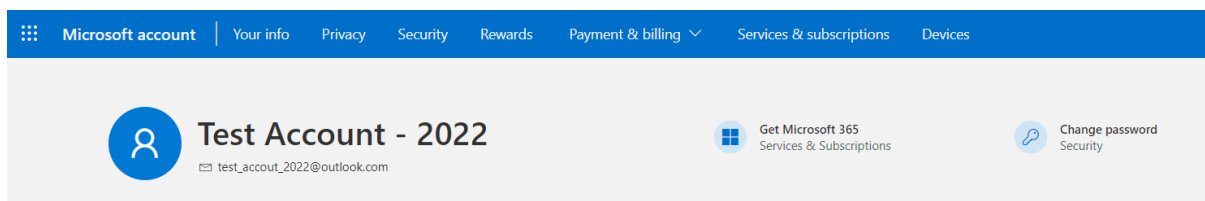
# Outlook.com Application Password

Outlook.com accounts ([xxx@outlook.com](mailto: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.

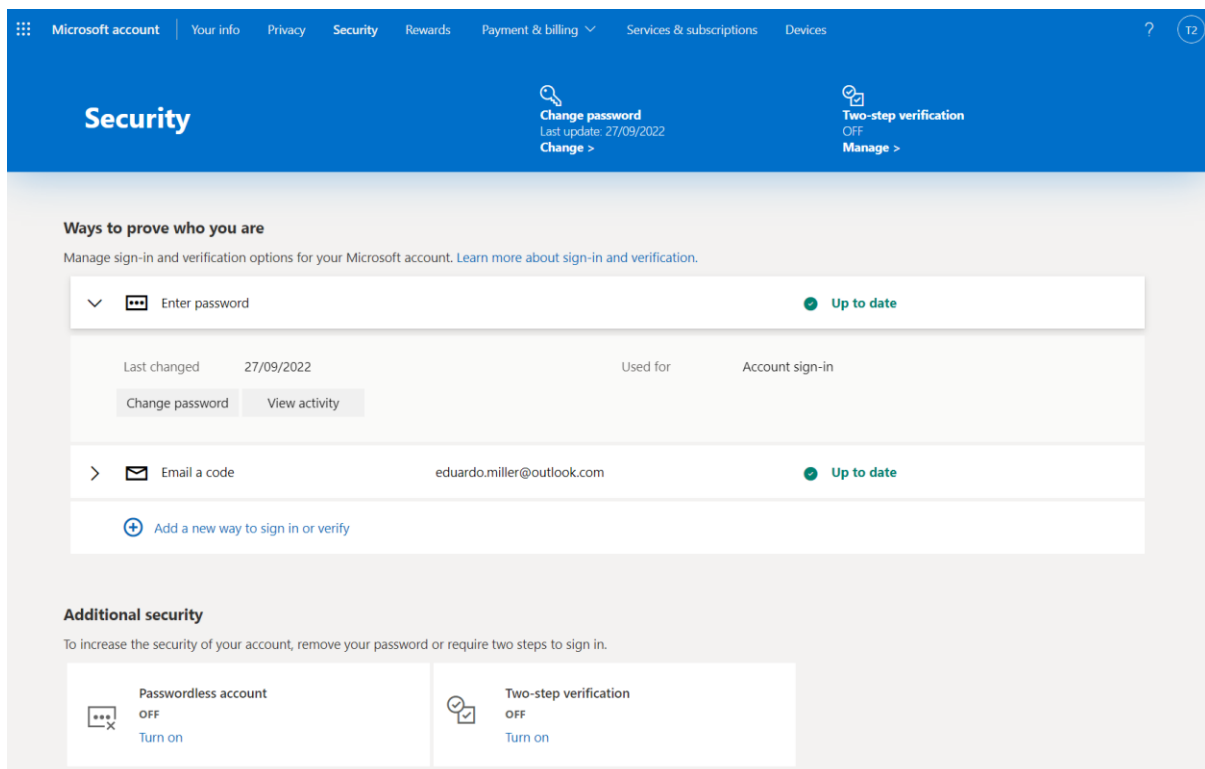
The following steps will guide you in creating an application token in your Microsoft account. This is a more secure IMAP authentication option because it needs MFA to create the application password.

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

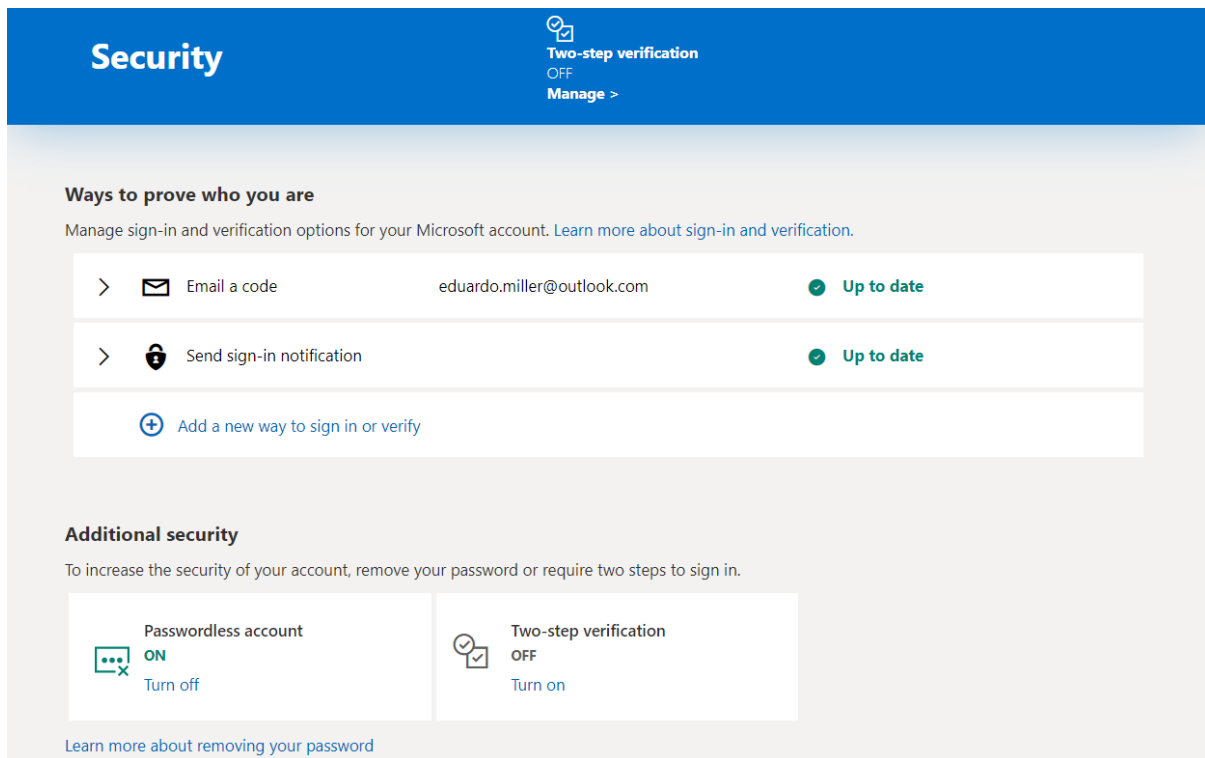
## 1) Open your Microsoft Account



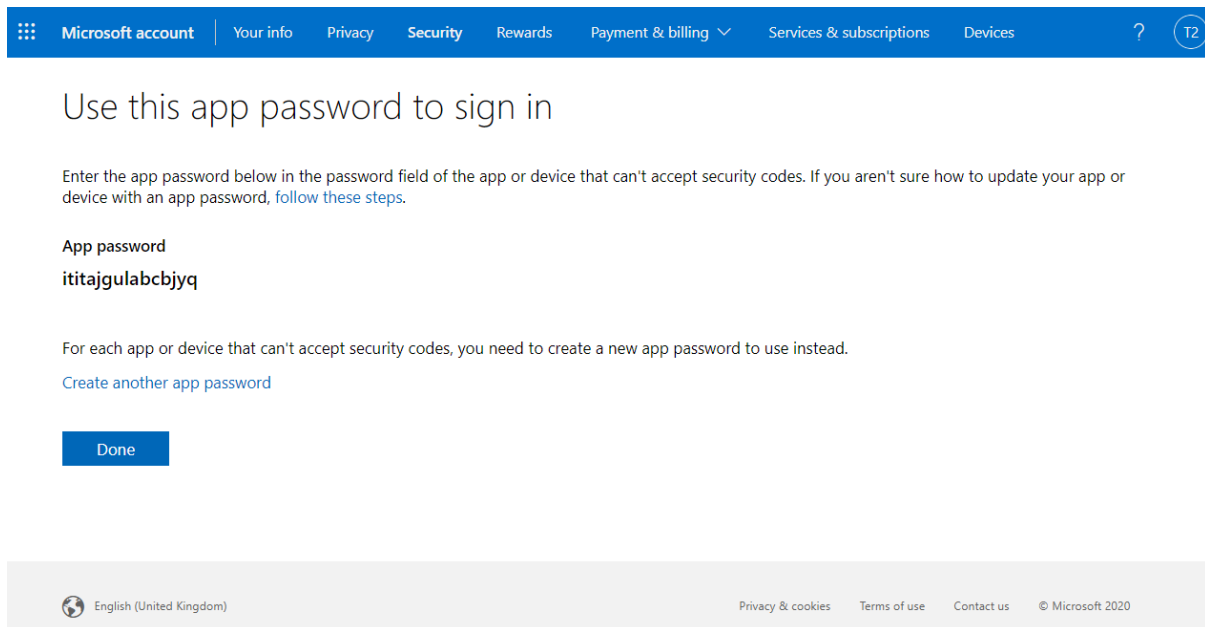
## 2) Open the Security options and enable the "Passwordless account" for your account.



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.

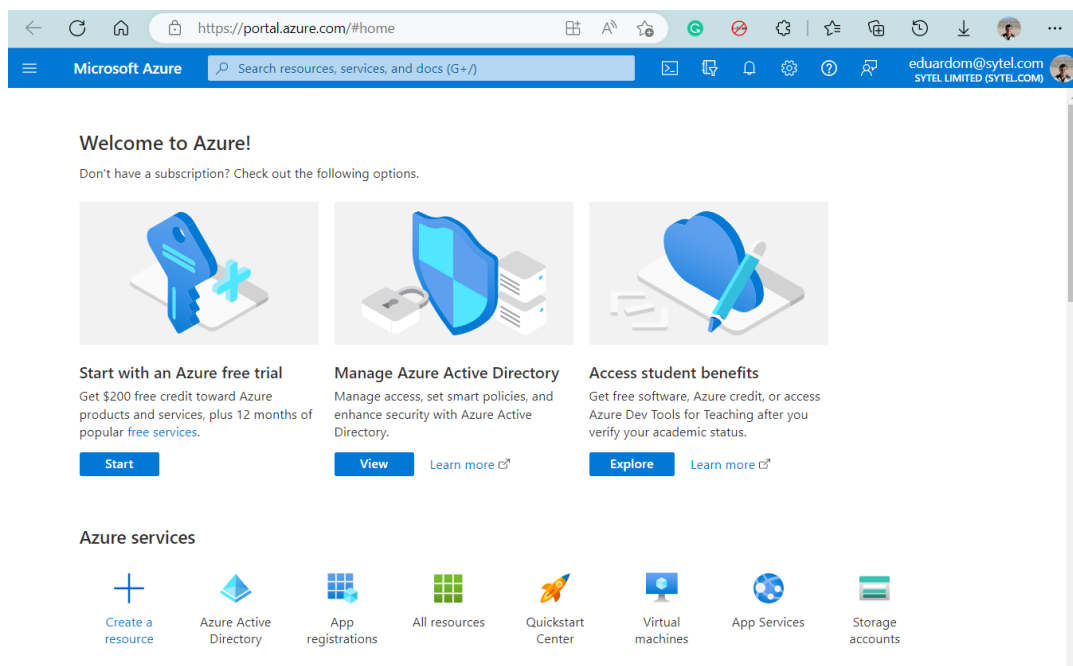
The paid email service from Microsoft requires the use of OAuth APIs, and the application connecting to your company's domain to read emails needs to be registered. The Microsoft identity platform performs identity and access management (IAM) only for registered applications. Whether a client application 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.

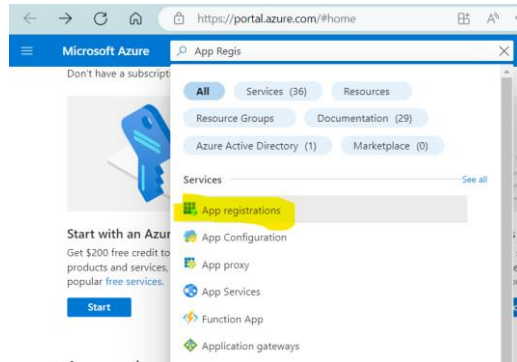
Please follow these steps to create an application password to enable a service to connect to an outlook.com account using IMAP.

## Register an application with the Microsoft identity platform

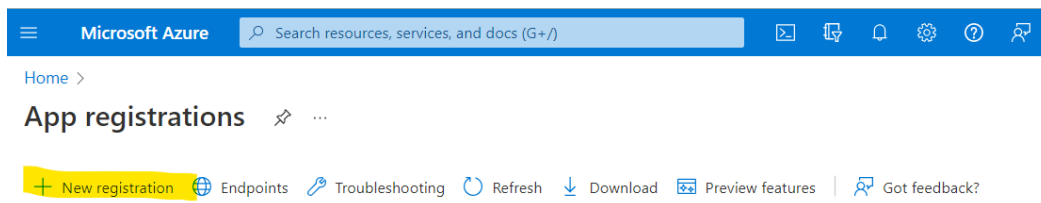
Go to [Azure Portal](#) using a user from your Office365 subscription. The Azure account must have permission to manage applications in Azure Active Directory (Azure AD). Any of the following Azure AD roles include the required permissions: Application administrator, Application developer or Cloud application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



Open App Registrations to Register an application.



Choose a New Registration.



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

Microsoft Azure Search resources, services, and docs (G+/)

Home > App registrations >

## Register an application

\* Name

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

TestApp ✓

Supported account types

Who can use this application or access this API?

☒ Accounts in this organizational directory only (SysTel Limited only - Single tenant)

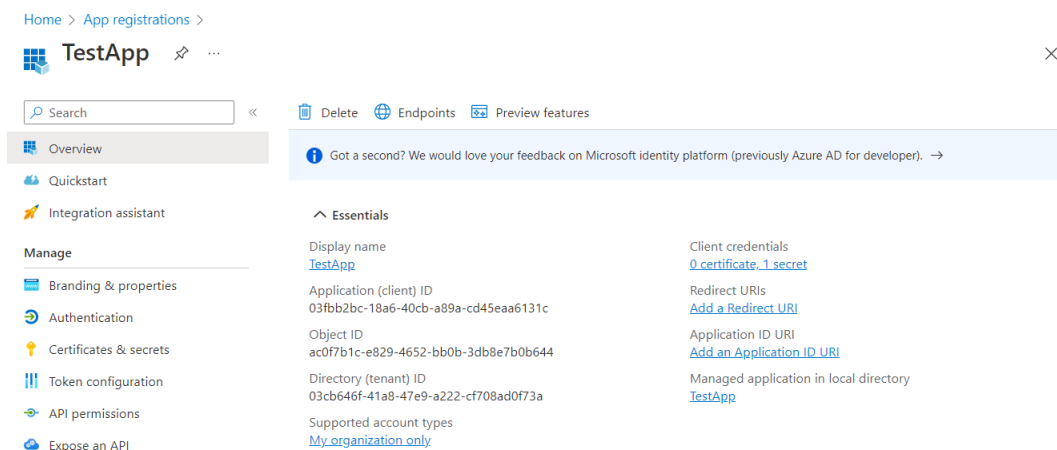
☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

☐ Personal Microsoft accounts only



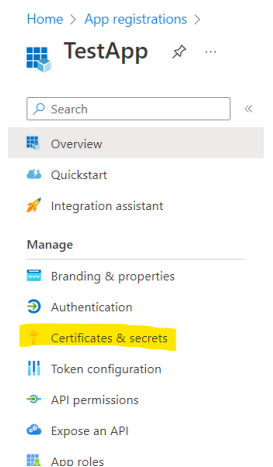
In the next screen, copy the values *Client ID* and *Tenant ID*.



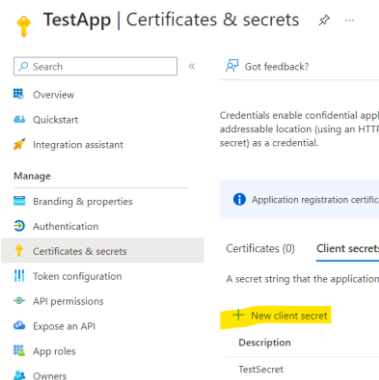
The application is now created. Client ID and Tenant ID will be used later.

## 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.

Home > App registrations > TestApp

TestApp | Certificates & secrets

Search

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support + Troubleshooting

Troubleshooting

New support request

Application registration certificate

Certificates (0)

Client secrets

A secret string that the application uses to identify itself to the resource.

+ New client secret

Description

TestSecret

Add a client secret

Description

AnyMeaninfulNameForYour

Expires






24 months

Add

Cancel

Copy the secret value and the secret id.

+ New client secret

Description	Expires	Value ⓘ	Secret ID
TestSecret	9/20/2024	gKi*****	e85d460a-794b-4248-b0ee...  
AnyMeaninfulNameForYour	12/8/2024	cBS8Q~LB3W5VJifx6E3W_-B... 	18028621-f831-4420-8fee-...  

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.

Microsoft Azure | Search resources, services, and docs (G+)

Home > App registrations > TestApp

### TestApp | API permissions

Search | Refresh | Got feedback?

Overview  
Quickstart  
Integration assistant

**Manage**

- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions**
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

Support + Troubleshooting

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. [Learn more](#)

#### 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 Sytel Limited

API / Permissions name	Type	Description	Admin consent req...	Status
▼ Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user ...	No	✓ Granted for Sytel Limited
▼ Office 365 Exchange Online (1)				
IMAP.AccessAsApp	Application	IMAP.AccessAsApp	Yes	✓ Granted for Sytel Limited

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

Click Add permission.

### Request API permissions

Select an API

Microsoft APIs | **APIs my organization uses** | My APIs

Apps in your directory that expose APIs are shown below

Office365

Name	Application (client) ID
Office365 Shell SS-Server	e8bdeda8-b4a3-4eed-b307-5e2456238a77
Office365 Zoom	0d38933a-0bbd-41ca-9ebd-28c4b5ba7cb7

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

# Request API permissions



Select an API

Microsoft APIs   APIs my organization uses   My APIs

Apps in your directory that expose APIs are shown below

<input type="text" value="Office"/>	
Name	Application (client) ID
Office 365 Enterprise Insights	f9d02341-e7aa-456d-926d-4a0ca599fbee
Office 365 Exchange Online	00000002-0000-0ff1-ce00-000000000000
Office 365 Information Protection	2f3f02c9-5679-4a5c-a605-0de55b07d135
Office 365 Management APIs	c5393580-f805-4401-95e8-94b7a6ef2fc2

Select Office 365 Exchange Online.

In the next screen, select Application Permissions.

# Request API permissions



[All APIs](#)

Office 365 Exchange Online  
<https://ps.outlook.com>

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.

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

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

# Request API permissions



[All APIs](#)

Office 365 Exchange Online  
<https://ps.outlook.com>

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.

Select permissions [expand all](#)

<input type="text" value="imap"/>	
Permission	Admin consent required
IMAP (1)	
<input checked="" type="checkbox"/> IMAP.AccessAsApp ⓘ IMAP.AccessAsApp	Yes

[Add permissions](#) [Discard](#)

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

Refresh

Got feedback?

You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

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. [Learn more](#)

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 Sytel Limited

API / Permissions n...	Type	Description	Admin consent req...	Status
Microsoft Graph (1)				...
User.Read	Delegated	Sign in and read user profile	No	...
Office 365 Exchange (				...
IMAP.AccessAsApp	Application	IMAP.AccessAsApp	Yes	<div><div></div>Not granted for Sytel Li...</div> ...

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

The result will be.

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

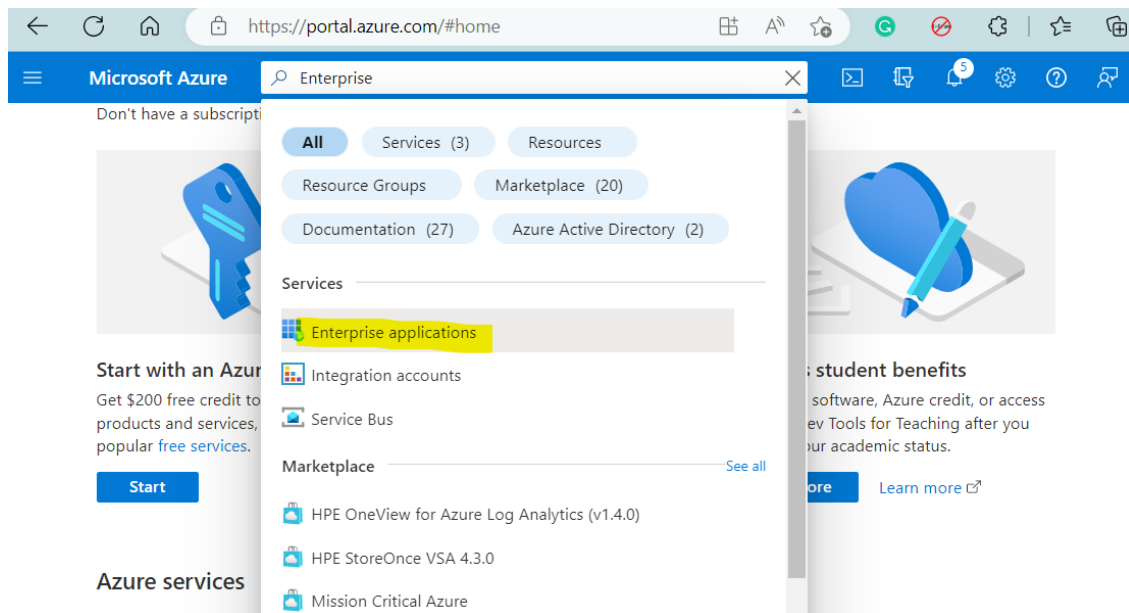
Grant admin consent for Sytel Limited

API / Permissions n...	Type	Description	Admin consent req...	Status
Microsoft Graph (1)				...
User.Read	Delegated	Sign in and read user profile	No	<div><div></div>Granted for Sytel Limited</div> ...
Office 365 Exchange (				...
IMAP.AccessAsApp	Application	IMAP.AccessAsApp	Yes	<div><div></div>Granted for Sytel Limited</div> ...

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

## 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.

+ New application   Refresh   Download (Export)   Preview info   Columns   ...

View, filter, and search applications in your organization that are set up to use your Azure AD tenant as their Identity

The list of applications that are maintained by your organization are in [application registrations](#).

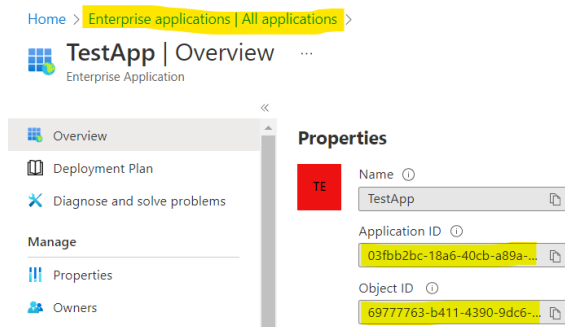
Search:

Application type == **Enterprise Applications**   Application ID starts with   Add filters

1 application found

Name	↑↓	Object ID	Application ID	Homepage URL	Created on
<b>TestApp</b>		69777763-b411-439...	03fbb2bc-18a6-40cb...		9/20/2022

Copy the Application ID 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:*

```
1 Add-MailboxPermission  
2   -Identity "shared@your-domain.onmicrosoft.com"  
3   -User <OBJECT_ID>  
4   -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 tool to validate the Office 365 configurations. The below standalone application can help you to validate your Azure Business configuration.



IMAP\_OAuth\_Tester.  
xe

The application IMAP\_OAuth\_Tester.exe can be requested to [support@sytel.com](mailto:support@sytel.com).

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







## 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](http://www.sytel.com)

[info@sytel.com](mailto:info@sytel.com)

+44 (0)1296 381 200