

# Microsoft Account

## Creating OAuth Applications

### Contents

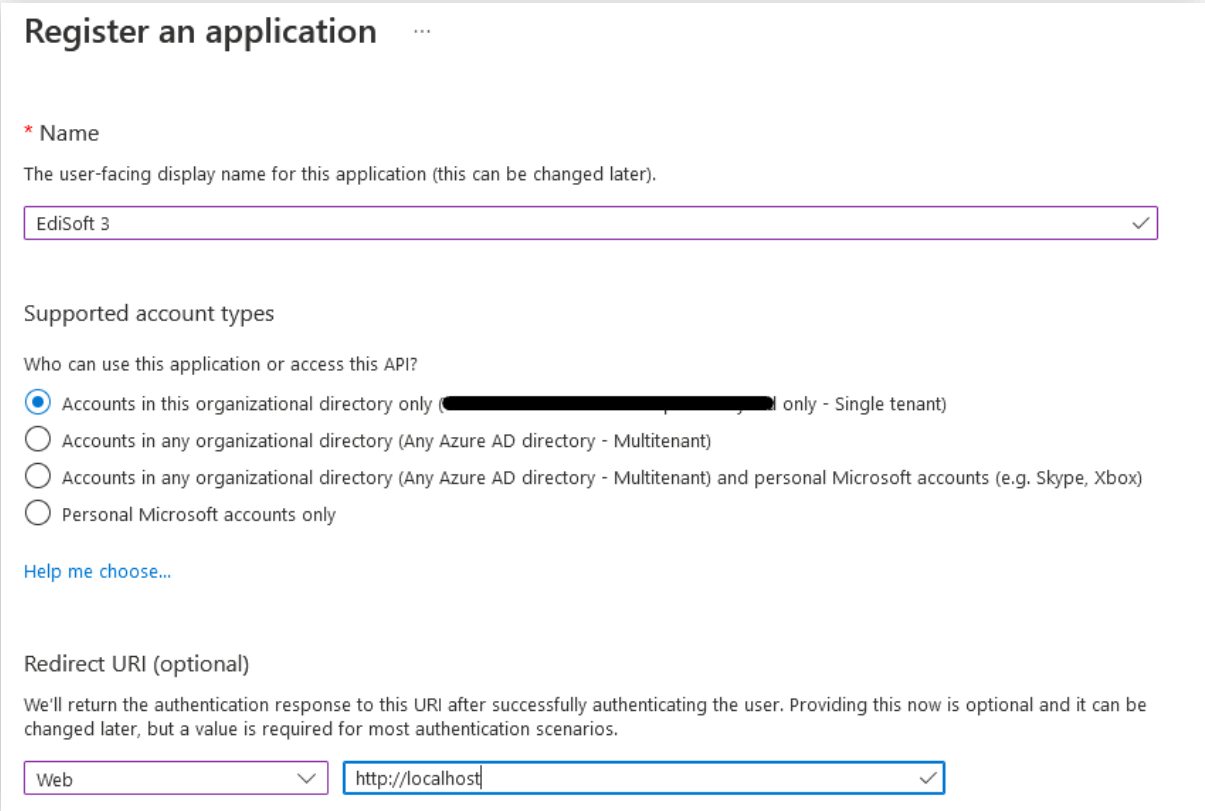
- Microsoft Account..... 1**
- Creating OAuth Applications..... 1**
- Create OAuth Application ..... 2**
- Create your application in Azure Portal..... 2**
- Single tenant in account type..... 2**
- Redirect URI ..... 2**
- API permission ..... 3**
- Client Id and client secrets ..... 4**
- Branding ..... 4**
- Client id and tenant ..... 4**
- Microsoft Account..... 5**
- Adding OAuth Details to Edisoft ..... 5**

# Create OAuth Application

## Create your application in Azure Portal

To use Microsoft365 OAuth (Modern Authentication) in your application, you must create an application in [Azure Portal](#).

- Sign in to the Azure portal using your work Microsoft365 Admin Account
- If your account gives you access to more than one tenant, select your account in the top right corner, and set your portal session to the Azure AD tenant that you want.
- In the left-hand navigation pane, select the Azure Active Directory service, and then select App registrations -> New registration.



**Register an application** ...

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

EdiSoft 3 ✓

**Supported account types**

Who can use this application or access this API?

Accounts in this organizational directory only (████████████████████) 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 ✓ http://localhost ✓

## Single tenant in account type

When the register an application page appears, enter a meaningful application name and select the account type.

- Select "Accounts in this organization directory only" (single tenant)

## Redirect URI

Under Redirect URI select Web from the Dropdown and enter the redirect URI;

- <http://localhost>

Then click Register.

## API permission

Now we need to add permission to the application:

- Click API Permission In the left hand menu.
- Add a permission -> Microsoft Graph -> Delegated Permission then use the search bar to find and select; User.Read, email, offline\_access, openid, profile, SMTP.Send, POP.AccessAsUser.All, Mail.Send.

**Request API permissions**

[← All APIs](#)

Microsoft Graph  
<https://graph.microsoft.com/> [Docs](#) [↗](#)

**i** Applications that sign in personal Microsoft accounts don't support permissions that require admin consent.

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 with signed-in user.

Here is permissions list:

**Configured permissions**

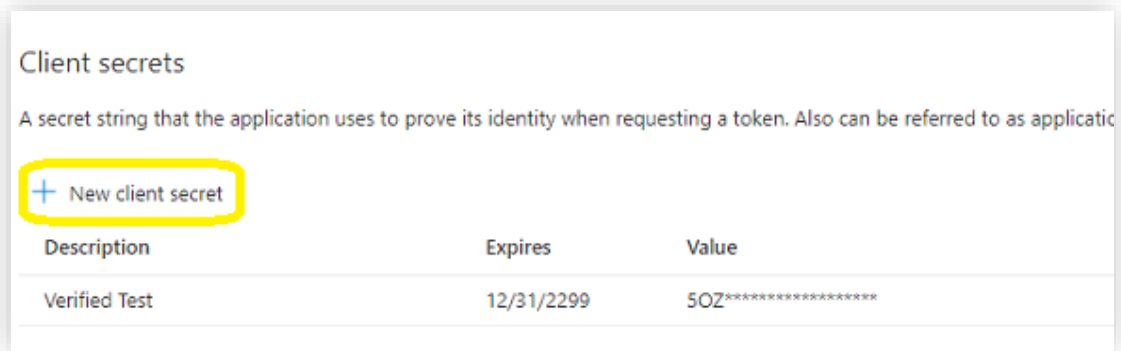
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

[+](#) Add a permission  Grant admin consent for [redacted]

API / Permissions name	Type	Description	Admin consent req...	Status
<a href="#">Microsoft Graph (6)</a>				...
<a href="#">offline_access</a>	Delegated	Maintain access to data you have given it access to	No	✔ Granted for [redacted] ...
<a href="#">openid</a>	Delegated	Sign users in	No	✔ Granted for [redacted] ...
<a href="#">POP.AccessAsUser.All</a>	Delegated	Read and write access to mailboxes via POP.	No	✔ Granted for [redacted] ...
<a href="#">profile</a>	Delegated	View users' basic profile	No	✔ Granted for [redacted] ...
<a href="#">SMTP.Send</a>	Delegated	Send emails from mailboxes using SMTP AUTH.	No	✔ Granted for [redacted] ...
<a href="#">User.Read</a>	Delegated	Sign in and read user profile	No	✔ Granted for [redacted] ...

## Client Id and client secrets

Now we need to create a client secret for the application, click Certificates and secrets -> client secrets and add a new client secret.



IMPORTANT - please store the client secret value straight after creating it in a safe place, as it will be hidden next time you go to view it.

## Branding

Now we click Branding, you can edit your company logo, URL and application name

## Client id and tenant

Now you can click Overview to find your client id and tenant.



- Use the tenant value in tokenUri and authUri instead of common.

Above client id and client secret support both "Office365 + SMTP/EWS".

# Microsoft Account

## Adding OAuth Details to Edisoft

Once you have created your App in Azure in EdiSoft 3 go into Setup >> OAuth

1. Fill in your TenantID, ClientID, Client Secret
2. Select the Provider as Microsoft
3. This should fill in the necessary URLs and Scopes

The screenshot shows the 'Post Box Details' window with the 'OAuth Details' tab selected. The fields for 'OAuth Tenant ID (Microsoft)', 'OAuth Client ID', 'OAuth Client Secret', and 'OAuth Authorisation String' are highlighted in yellow. The 'OAuth Provider' is set to 'MICROSOFT' and the 'Use Basic Auth for SMTP' checkbox is unchecked. The 'OAuth URLs' section is also visible but its fields are not highlighted.

4. To Authenticate, open a browser on the same computer and login to Microsoft using the **Edisoft** mailbox details.
5. Then return to Edisoft, click Authenticate and you'll be redirected to the authentication page (ensure this is logged in as the **Edisoft** mailbox)
6. On successful authentication the Authorisation String field should populate in EdiSoft
  - o If this doesn't happen please close and re-open EdiSoft and try the Authentication process again

The screenshot shows the 'Post Box Details' window with the 'OAuth Details' tab selected. The 'OAuth Authorisation String' field is highlighted in yellow. The 'OAuth Provider' is set to 'MICROSOFT' and the 'Use Basic Auth for SMTP' checkbox is unchecked. The 'OAuth URLs' section is also visible. At the bottom of the window, there are two buttons: 'Force Token Refresh' and 'Authenticate'.

Then go into Setup >> Internet Setup

7. POP3 remove the password but leave the hostname outlook.office365.com, port 995 and SSL enabled
8. SMTP remove the password but leave the hostname smtp.office365.com, port 587 and SSL / TLS enabled
9. Set SSL Mode to Automatic
10. Set SSL Protocol to TLS1.2

Post Box Details

Friday 12 August, 2022 (9:57 AM)

Address Details | Configuration | Printer Setup | ICS | EXDOC | PRA | BabelBridge | **Internet Setup** | Internet Logs | OAuth Details

**Internet Communications details**

EDI Messaging e-mail Address: edi@.com.au

Contact e-mail Address: .

**SMTP Settings**

Outgoing Mail Server (SMTP): smtp.office365.com  Manual  SSL / TLS

SMTP User ID: edi@.com.au  Send High Priority

SMTP Password: [Masked] SMTP Port: 587

**POP3 Settings**

Incoming Mail Server (POP3): outlook.office365.com  Manual  SSL

POP3 User ID: edi@.com.au

POP3 Password: [Masked] POP3 Port: 995

SSL Mode: Automatic SSL Protocol: TLS1.2

#### If users have issues Sending Messages (SMTP)

1. Open Setup >> OAuth
2. Tick Use Basic Auth for SMTP
3. Open Setup >> Internet Setup
4. POP3 remove the password but leave the hostname outlook.office365.com, port 995 and SSL enabled
5. SMTP **keep** your password, hostname smtp.office365.com, port 587 and SSL / TLS enabled
6. Set SSL Mode to Automatic
7. Set SSL Protocol to TLS 1.2