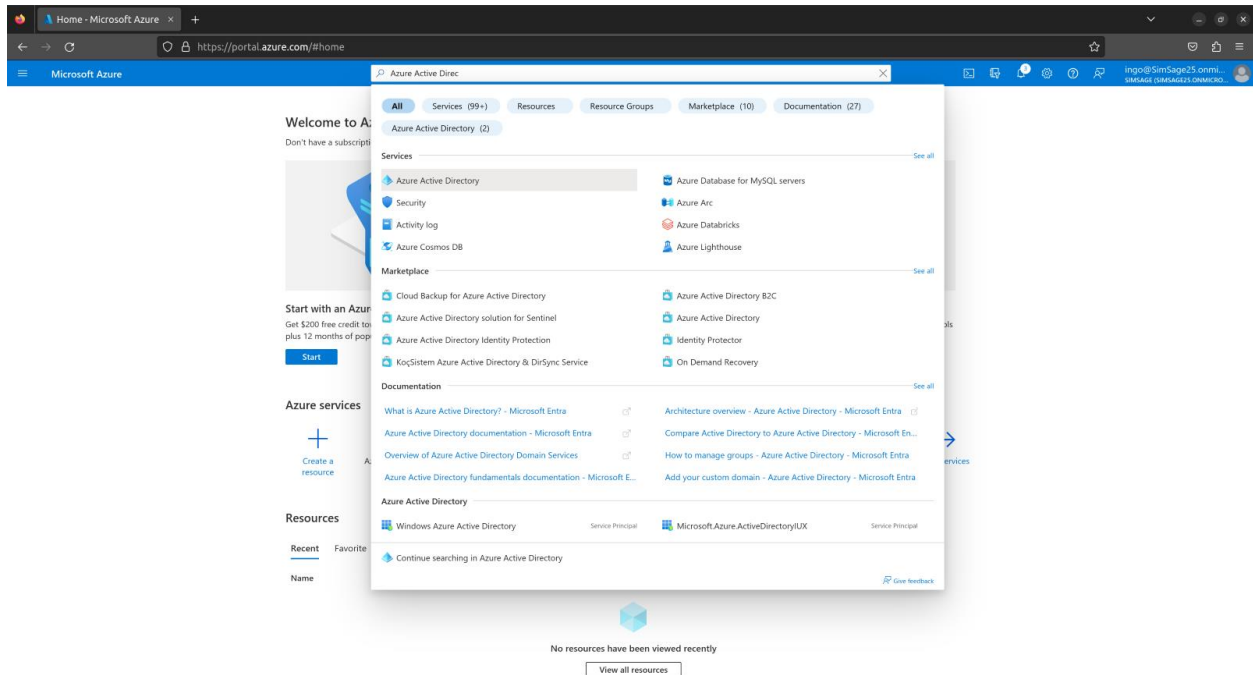


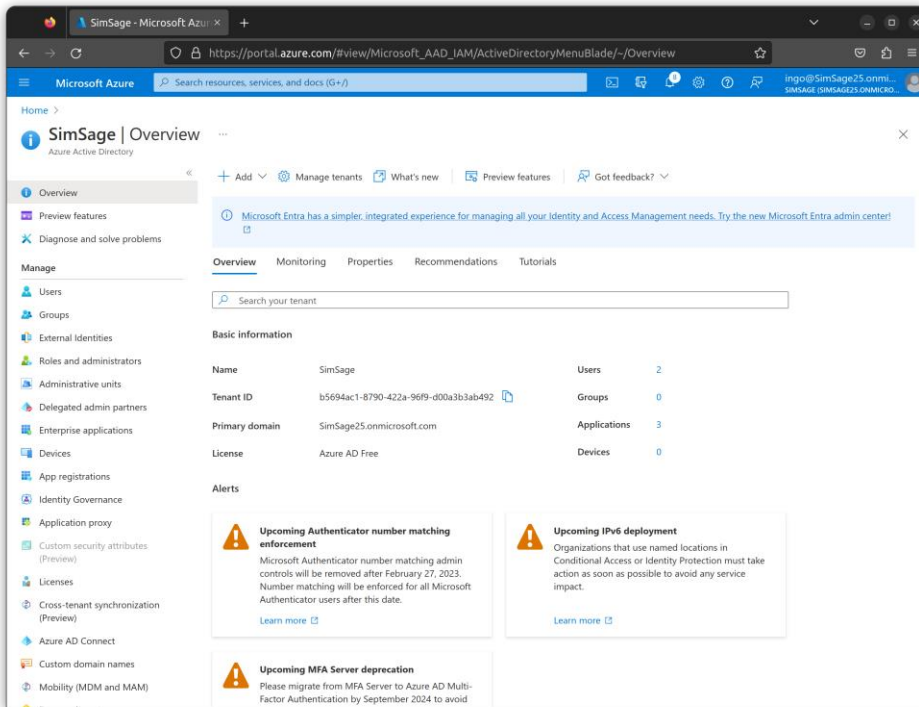
## Sharepoint 365 Crawler Setup

This is a short guide aimed at showing how to configure Microsoft Azure to enable the SimSage Sharepoint 365 crawler.

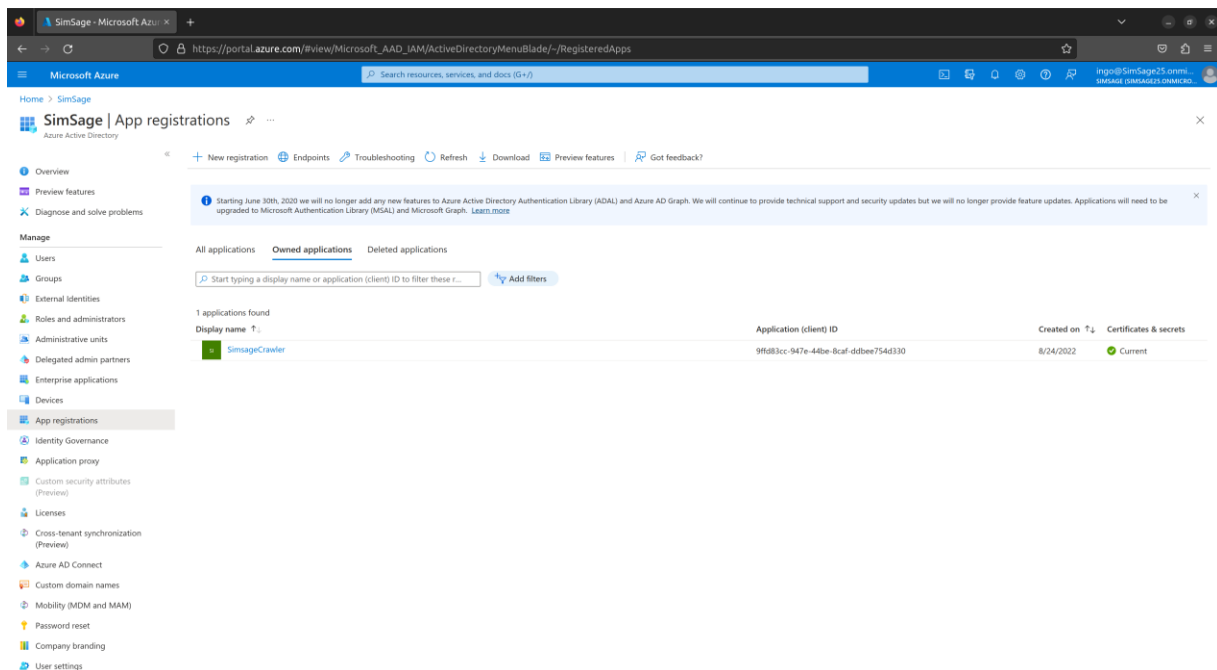
You need to be an administrator for your Office 365 setup for this to work. Sign-in to <https://portal.azure.com/> Search for “Azure Active Directory” and select it



Copy the Tenant Id. We will need this later to configure the crawler



Next click on “App registrations” on the left-hand side menu and click on “+ New registration” at the top menu bar of the App registrations screen.



In the Name section, enter a meaningful application name, for example simsage-app. In the Supported account types section, select Accounts in this organizational directory only (<tenant name> only – Single tenant), where <tenant name> is the name of your Azure tenant. Click “Register” button at the bottom to create the application.

**Note, no redirect URL is required here.**

Home > SimSage >

## Register an application ...

### \* Name

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

simsage-app ✓

name of the app

### Supported account types

Who can use this application or access this API?

- ☒ Accounts in this organizational directory only (SimSage only - Single tenant) select this value
- ☐ 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

Ignore

By proceeding, you agree to the Microsoft Platform Policies

Register

click Register

Copy the client Id, we will need it later to set up the Crawler

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo and a search bar. The left sidebar shows the 'App registrations' menu. The main content area displays the 'App registrations' page for 'SimSage'. A table lists the applications, with one application named 'simsage-app' having a client ID of '11e9496-c3d6-4e0e-908d-04ecfe00e492'. A red arrow points to this client ID, with a text label 'this is your Client ID for SimSage, copy it.' below it.

Display name	Application (client) ID	Created on	Certificates & secrets
simsage-app	11e9496-c3d6-4e0e-908d-04ecfe00e492	3/22/2021	Current

Next, we will need to add a secret to the application

Click on the application and select “Add a Certificate or secret” in the following screen:

The screenshot shows the Microsoft Azure portal interface for the 'App2' application. The top navigation bar includes the Microsoft Azure logo and a search bar. The left sidebar shows the 'App2' menu. The main content area displays the 'App2' application details. A red arrow points to the 'Add a certificate or secret' link in the 'Client credentials' section.

Build your application with the Microsoft identity platform

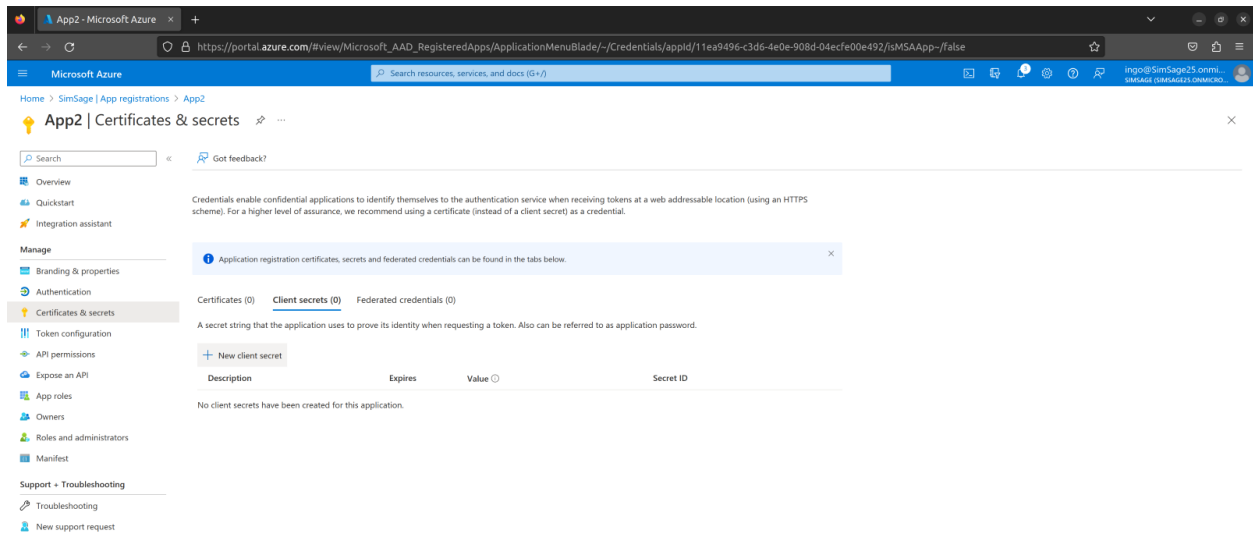
The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. [Learn more](#)

**Call APIs**  
Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.  
[View API permissions](#)

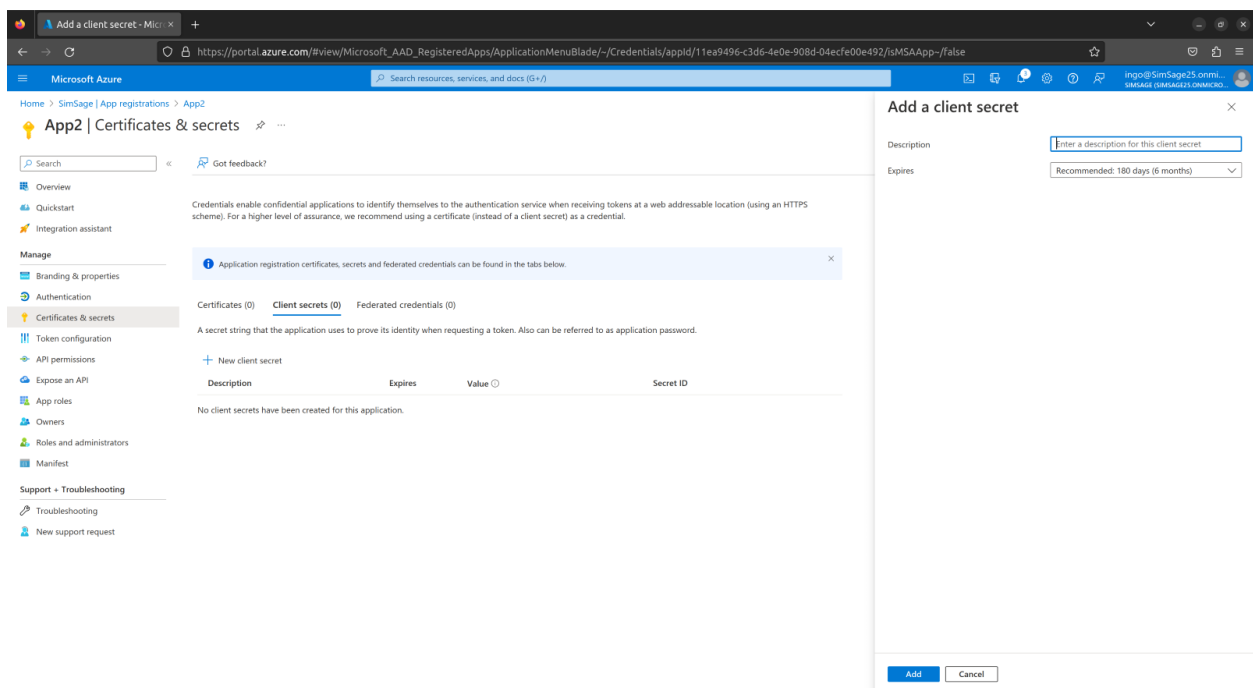
**Sign in users in 5 minutes**  
Use our SDKs to sign in users and call APIs in a few steps. Use the quickstarts to start a web app, mobile app, SPA, or daemon app.  
[View all quickstart guides](#)

**Configure for your organization**  
Assign users and groups, apply conditional access policies, configure single sign-on, and more in Enterprise applications.  
[Go to Enterprise applications](#)

Select Client secrets and press “+ New client secret”



In the Sidebar now displayed, give the Secret an appropriate description and expiry period:



Copy the secret and keep it safe for the crawler configuration.

**IMPORTANT** this new secret will only show itself once. Copy its value and keep it somewhere safe so you can refer to it when asked by SimSage later.



Lastly, we need to add the relevant Permissions to our Application

Click “API permissions” in the left-hand-side menu. Click “+ Add a permission” in the new pane that appears.

The screenshot shows the Microsoft Azure portal interface. The left-hand navigation pane is expanded, showing the 'API permissions' option under the 'Manage' section. A red arrow points to this option with the text 'select API permissions'. The main content area displays the 'API permissions' page for the application 'simsage-app'. At the top, there is a search bar and a 'Refresh' button. Below this, a message states: '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'. The 'Configured permissions' section explains that applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. It includes a link to 'Add a permission' and a status 'Grant admin consent for Simsage'. Below this is a table with the following columns: 'API / Permissions name', 'Type', 'Description', 'Admin consent req...', and 'Status'. The table contains one entry: 'User Read' (Type: Delegated, Description: Sign in and read user profile, Admin consent req: No, Status: Granted for Simsage). At the bottom, there is a note: 'To view and manage permissions and user consent, try Enterprise applications.'

API / Permissions name	Type	Description	Admin consent req...	Status
User Read	Delegated	Sign in and read user profile	No	Granted for Simsage

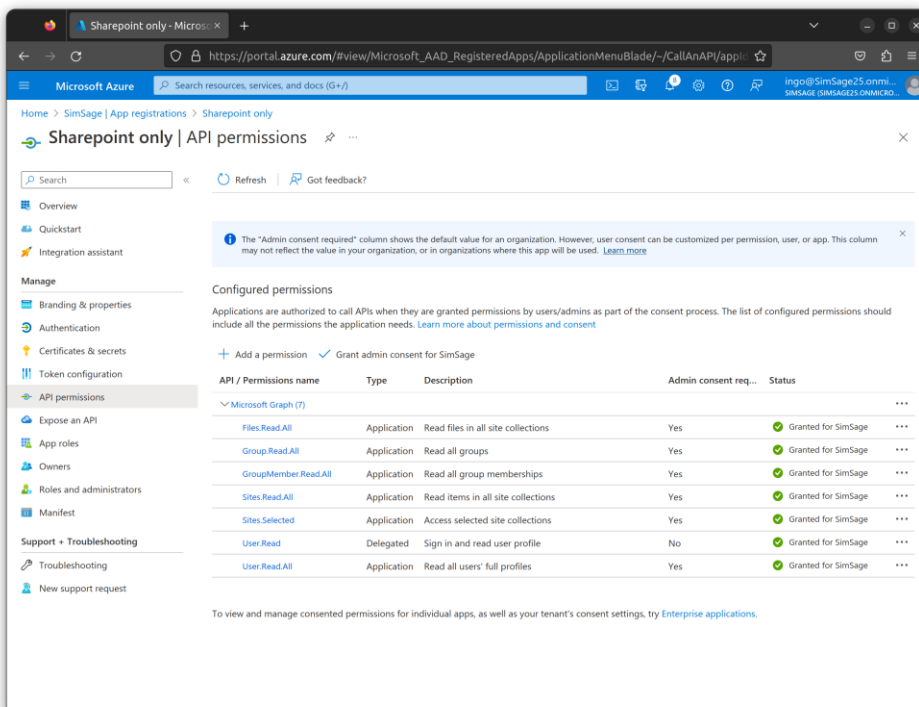


Select “Microsoft Graph” and select “Application permissions”. Then start typing in the “Select permissions” text box.

You need to select the following permissions:

- Files.Read.All
- Group.Read.All
- GroupMember.Read.All
- Sites.Read.All
- Sites.Selected
- User.Read
- User.Read.All

Once added make sure the permissions have Admin Consent by pressing “Grant Admin Consent” button:



Now configure the actual Crawler

In the Crawler Dialog select the Sharepoint 365 crawler and on the "shaprepoint 365 crawler" page add the following values:

- Domain name: <Your Azure Tenant Id>
- Client Id: <Application Client ID>
- Client Secret <Application Client Secret>

Now either select "crawl all Sites" to index all of the Sharepoint sites or add a list of comma separated site names to crawl specific sites only.

Press save ...