Sharepoint 365 Setup Documentation

- Introduction
- Prerequisites
  - Alternative installation
  - Manual installation

Introduction

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

> ℹ Sharepoint is an incremental crawler. This means that Sharepoint will only communicate changes with SimSage after it has been crawler the first time. You will need to re-process all files if you change settings like Similarity Calculations.

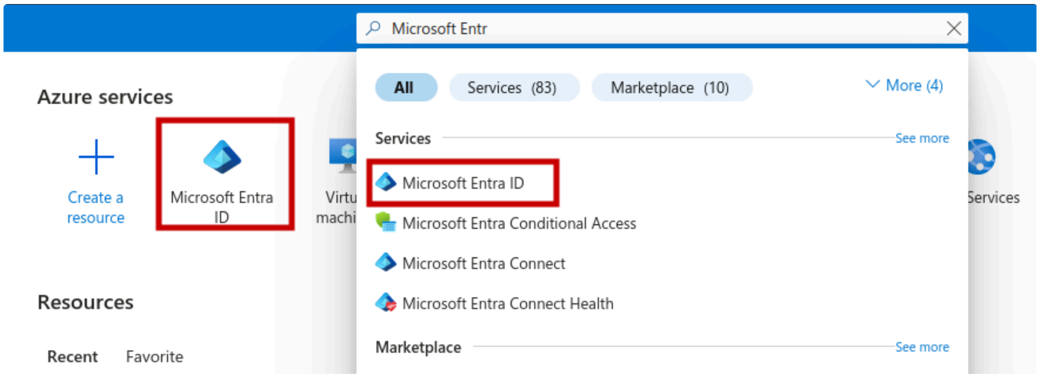
Prerequisites

Alternative installation

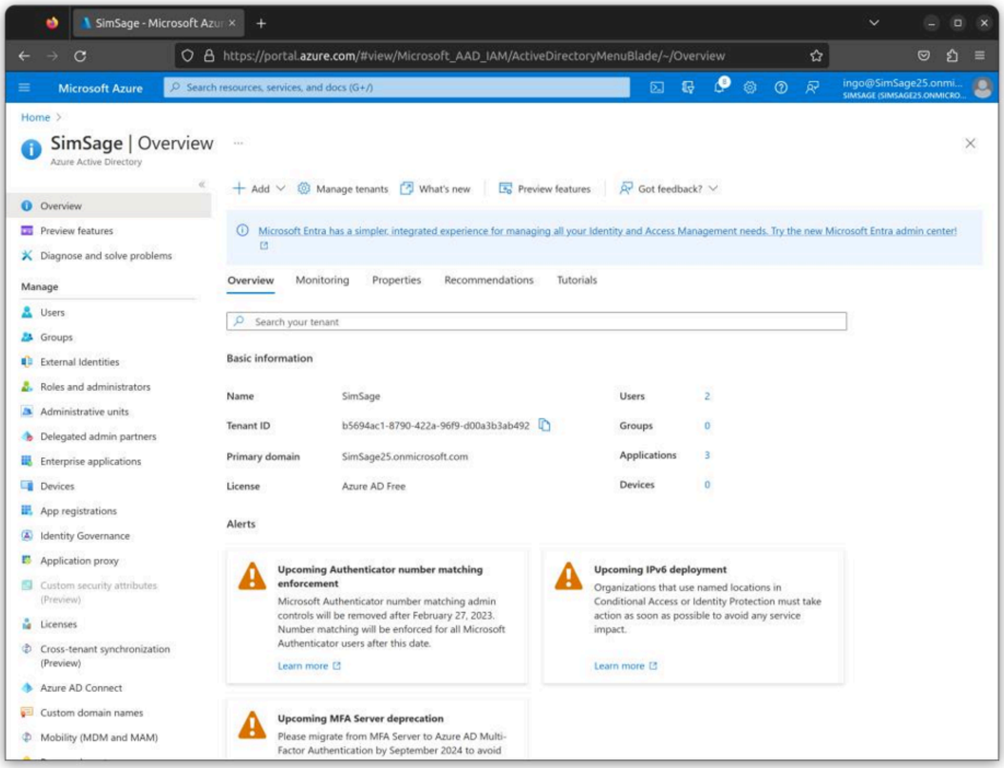
We have a series of Python scripts, including one for Sharepoint, that automate the process shown below. This requires you to be an administrator, and install the azure cli utility on your operating system. Please view our repository at https://github.com/simsage/azure-create-apps Connect your Github account (permissions required), or use our SharePoint configuration app SimSage Azure set up

Manual installation

You need to be an administrator for your Office 365 setup for this to work. Sign-in to Microsoft Azure Search for “Microsoft Entra ID” and select it:



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



Microsoft Entra has a simpler, integrated experience for managing all your Identity and Access Management needs. Try the new Microsoft Entra admin center!

Basic information

Name	SimSage	Users	2
Tenant ID	b5694ac1-8790-422a-96f9-d00a3b3ab492	Groups	0
Primary domain	SimSage25.onmicrosoft.com	Applications	3
License	Azure AD Free	Devices	0

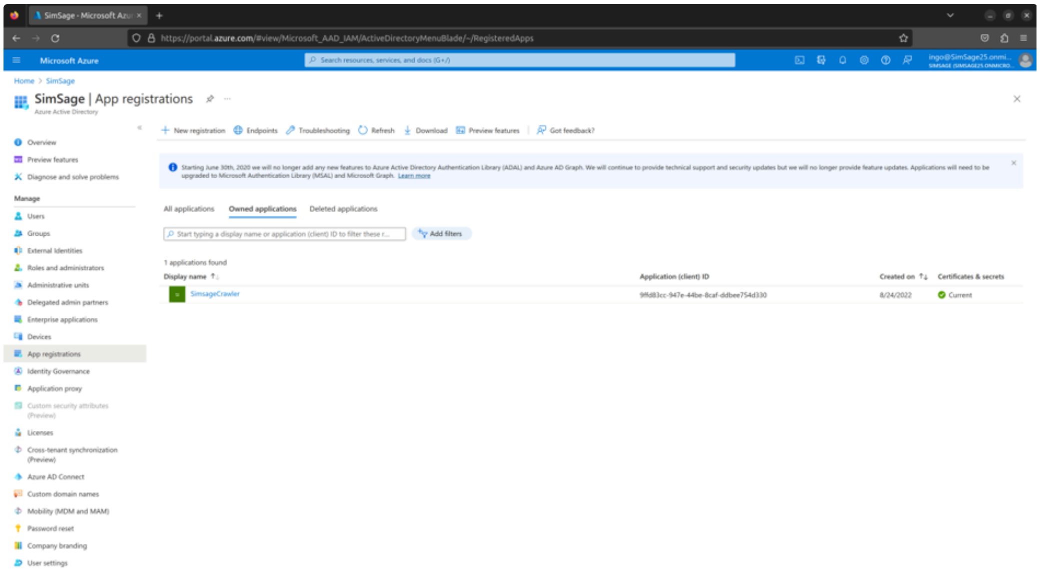
Alerts

Upcoming Authenticator number matching enforcement
Microsoft Authenticator number matching admin controls will be removed after February 27, 2023. Number matching will be enforced for all Microsoft Authenticator users after this date.
Learn more

Upcoming IPv6 deployment
Organizations that use named locations in Conditional Access or Identity Protection must take action as soon as possible to avoid any service impact.
Learn more

Upcoming MFA Server deprecation
Please migrate from MFA Server to Azure AD Multi-Factor Authentication by September 2024 to avoid

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.



SimSage | App registrations

Azure Active Directory

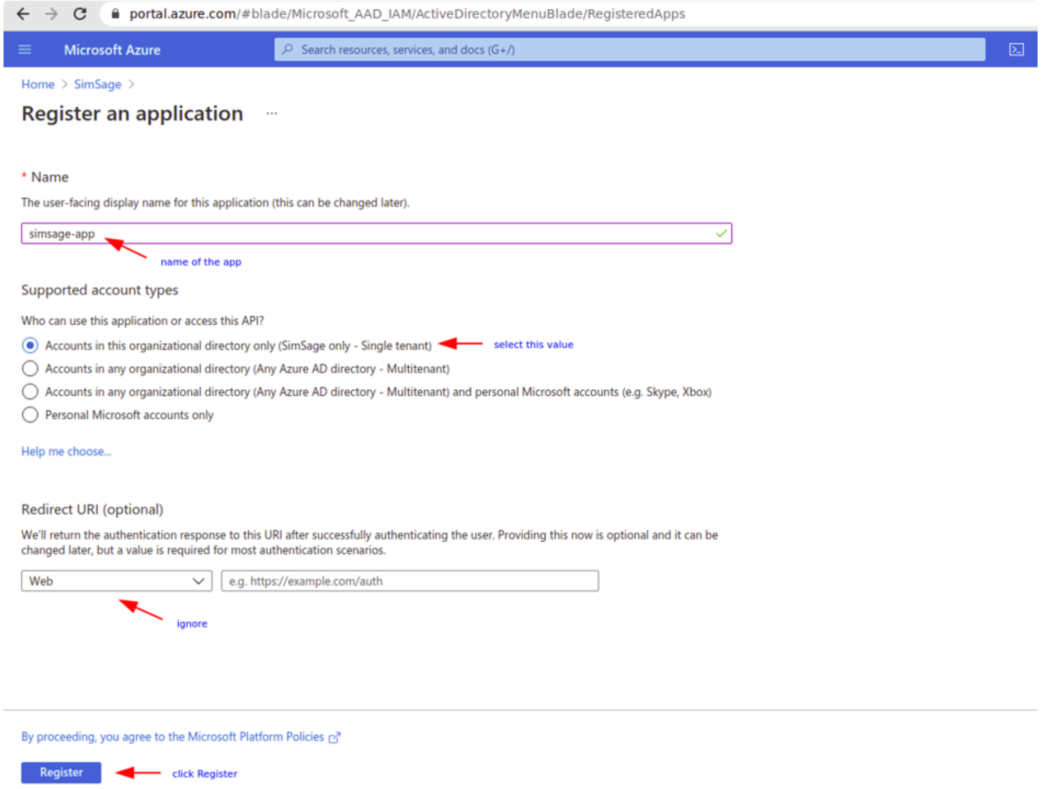
Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

1 applications found

Display name ↑↓	Application (client) ID	Created on ↑↓	Certificates & secrets
SimsageCrawler	9ffd83cc-947e-44be-8caf-ddbee754d330	8/24/2022	✓ Current

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.

No redirect URL is required here.



portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/RegisteredApps
Microsoft Azure
Search resources, services, and docs (G+/)
Home > SimSage >
Help me choose...
By proceeding, you agree to the Microsoft Platform Policies
Register

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)

○ 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

select this value

Redirect URI (optional)

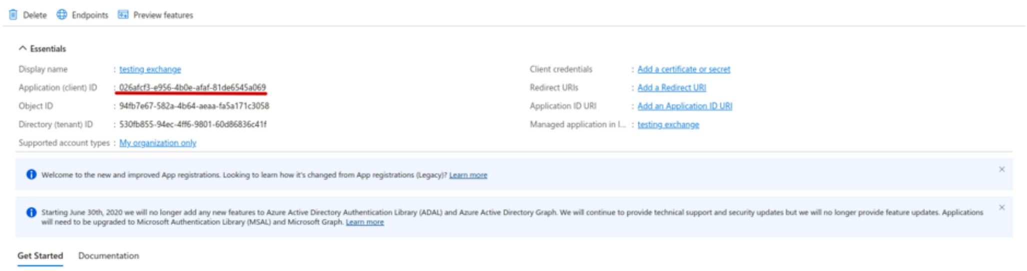
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

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

ignore

click Register

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



Delete Endpoints Preview features

Essentials

Display name	: testing exchange	Client credentials	: Add a certificate or secret
Application (client) ID	: 026afcf3-e956-4b0e-afaf-81de6545a069	Redirect URIs	: Add a Redirect URI
Object ID	: 94fb7e67-582a-4b64-aeaa-fa5a171c3058	Application ID URI	: Add an Application ID URI
Directory (tenant) ID	: 530fb855-94ec-4ff6-9801-60d86836c41f	Managed application in l...	: testing exchange
Supported account types	: My organization only		

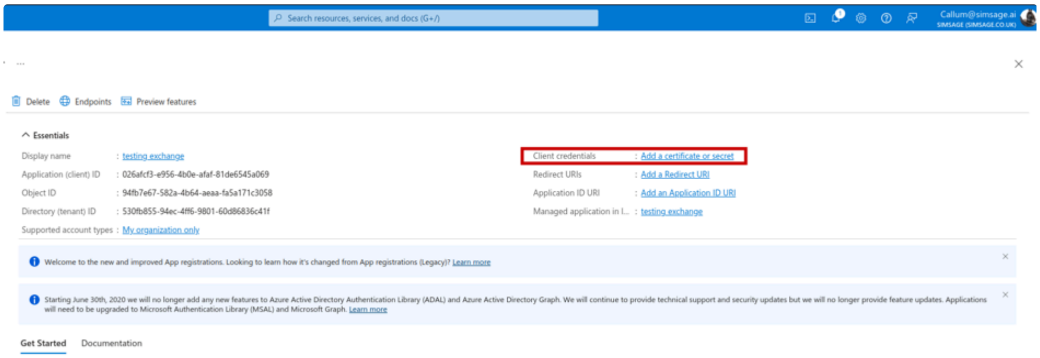
Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? Learn more

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

Get Started Documentation

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:



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

Callum@simsage.ai
SIMSAGE (SIMSAGE.CO.UK)

Delete Endpoints Preview features

Essentials

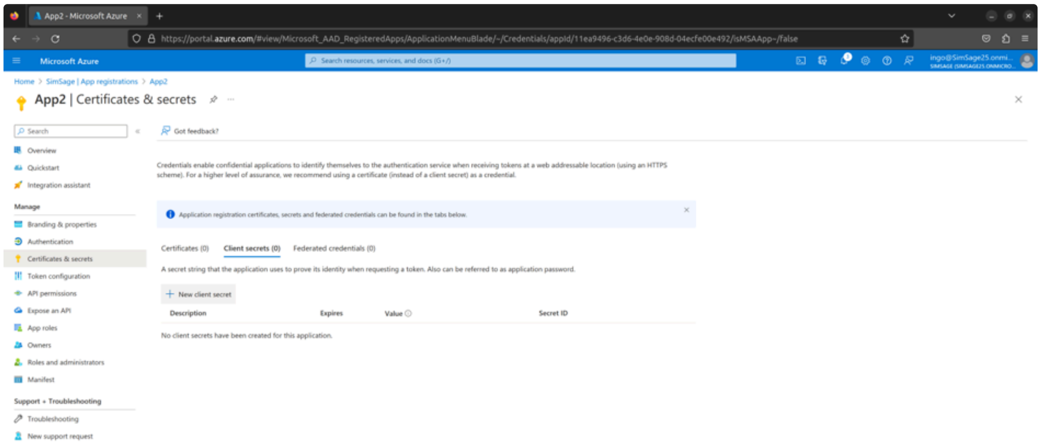
Display name	: testing exchange	Client credentials	: Add a certificate or secret
Application (client) ID	: 026afcf3-e956-4b0e-afaf-81de6545a069	Redirect URIs	: Add a Redirect URI
Object ID	: 94fb7e67-582a-4b64-aeaa-fa5a171c3058	Application ID URI	: Add an Application ID URI
Directory (tenant) ID	: 530fb855-94ec-4ff6-9801-60d86836c41f	Managed application in l...	: testing exchange
Supported account types	: My organization only		

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? Learn more

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

Get Started Documentation

Select Client secrets and press “+ New client secret”



App2 - Microsoft Azure

https://portal.azure.com/#view/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/~/Credentials/appId/11ea9496-c3d6-4e0e-908d-04ecfe00e492/isMSAApp~/false

Microsoft Azure

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

ingo@SimSage25.onmi...
SIMSAGE (SIMSAGE25.ONMICRO...

Home > SimSage | App registrations > App2

App2 | Certificates & secrets

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) Client secrets (0) Federated credentials (0)

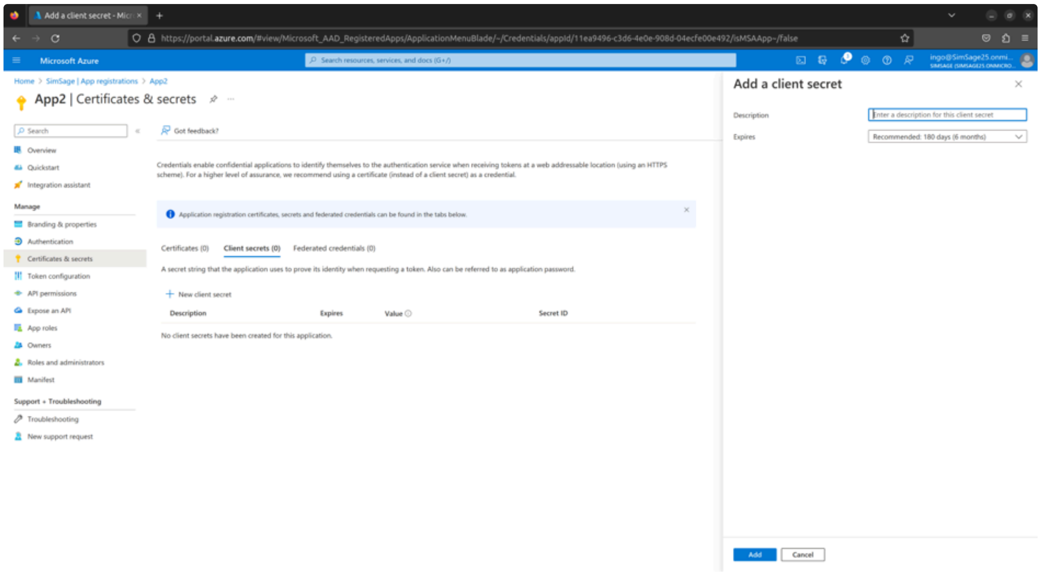
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value ⓘ	Secret ID

No client secrets have been created for this application.

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



Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value	Secret ID

No client secrets have been created for this application.

Description: Enter a description for this client secret

Expires: Recommended: 180 days (6 months)

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

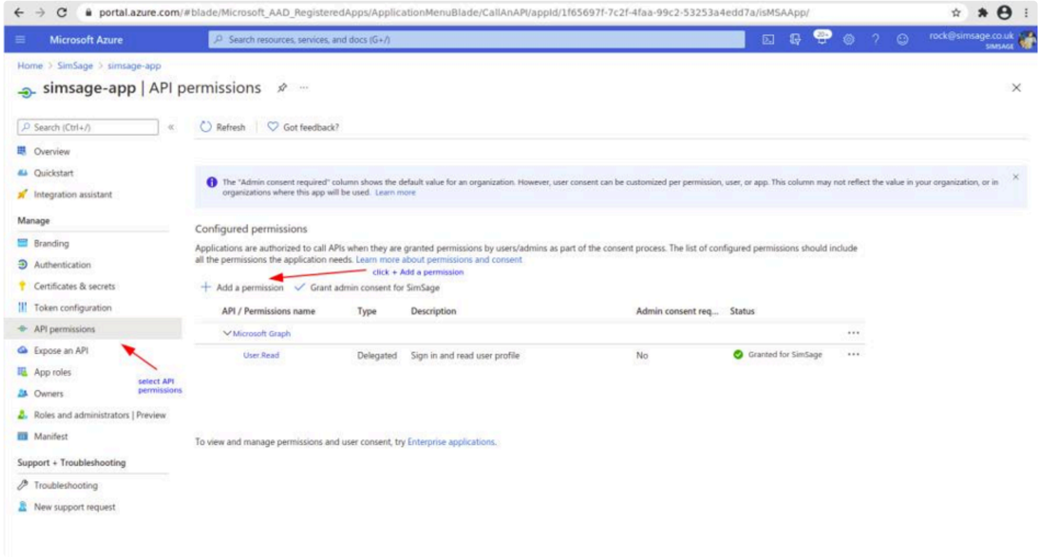
⚠ IMPORTANT this new secret will only show itself once. Copy its value and keep it somewhere safe so

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 "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

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

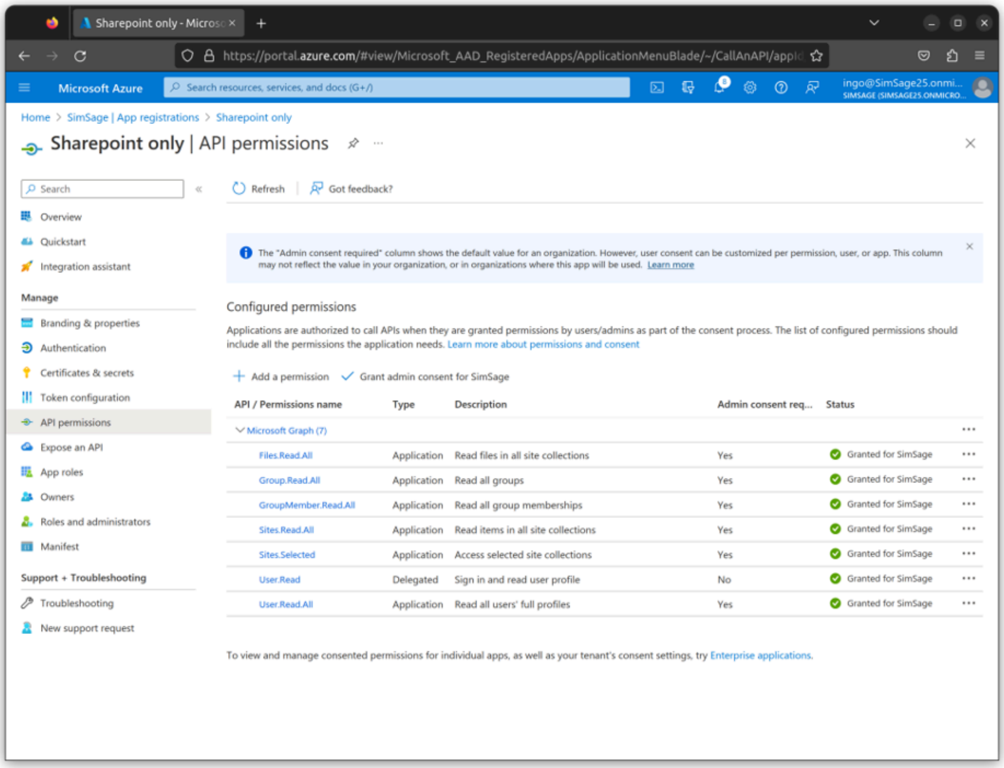
To view and manage permissions and user consent, try Enterprise applications.

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:


Sharepoint only - Microso
https://portal.azure.com/#view/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/~/CallAnAPI/appId
Microsoft Azure
Search resources, services, and docs (G+/)
ingo@SimSage25.onmi...
SIMSAGE (SIMSAGE25.ONMICRO...
Home > SimSage | App registrations > Sharepoint only
Sharepoint only | API permissions
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
Refresh
Got feedback?
Add a permission
Grant admin consent for SimSage

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

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (7)				
Files.Read.All	Application	Read files in all site collections	Yes	✓ Granted for SimSage
Group.Read.All	Application	Read all groups	Yes	✓ Granted for SimSage
GroupMember.Read.All	Application	Read all group memberships	Yes	✓ Granted for SimSage
Sites.Read.All	Application	Read items in all site collections	Yes	✓ Granted for SimSage
Sites.Selected	Application	Access selected site collections	Yes	✓ Granted for SimSage
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for SimSage
User.Read.All	Application	Read all users' full profiles	Yes	✓ Granted for SimSage

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

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 ...