



# One Drive Crawler Documentation

[Introduction](#)

[Prerequisites](#)

[Tenant ID via Microsoft Entra ID](#)

[Client ID](#)

[Client Secret](#)

[Checking Permissions](#)

[Request API Permissions](#)

[Basic Crawler Setup](#)

[Crawl Through Specific One Drive Accounts](#)


## Introduction

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

## Prerequisites

To setup the One Drive crawler in SimSage, be sure you have the following credentials at hand:

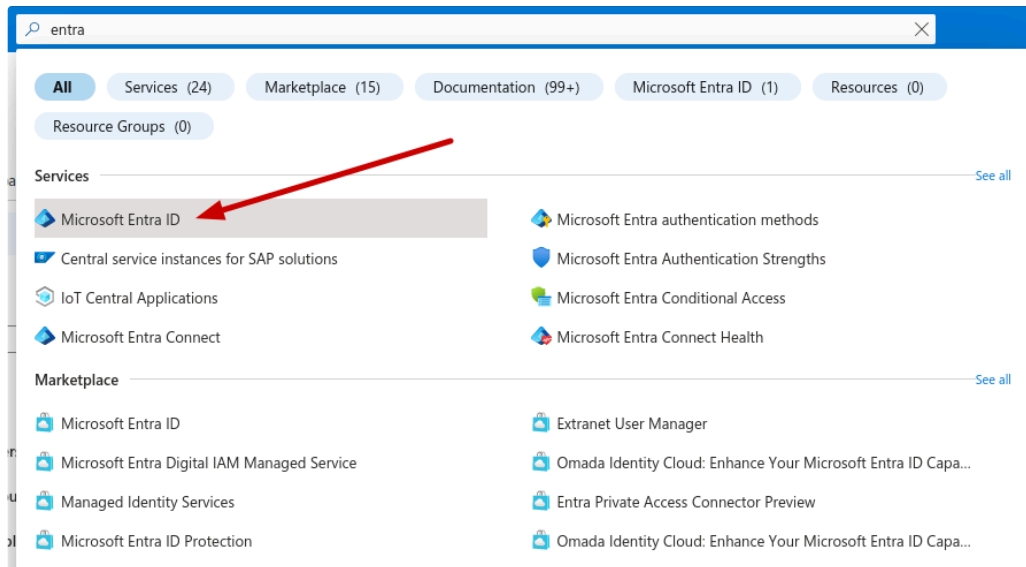
- **Tenant ID** - the ID
- **Client ID**
- **Client Secret**
- **Redirect URL**

 You need to be an administrator for your Office 365 setup for this to work.

If you do not have these credentials at hand, continue reading.

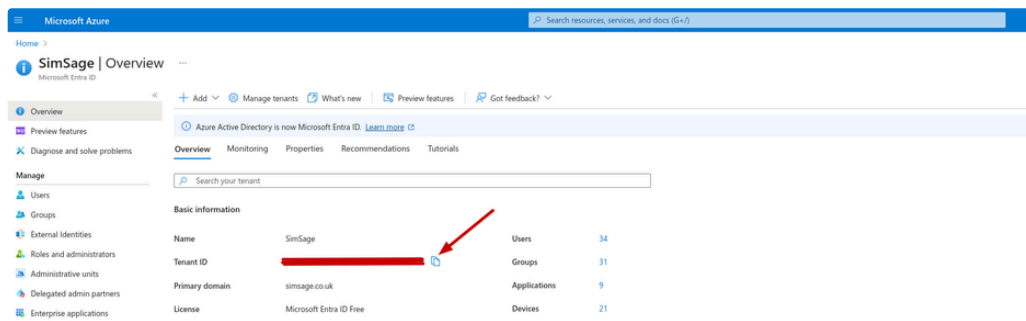
## Tenant ID via Microsoft Entra ID

Sign-in to [Microsoft Azure](#) and search for *Microsoft Entra ID*; select it:




Searching for Microsoft Entra ID

You should be greeted with the following page, which will describe you **tenant ID**:



Tenant ID

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

## Client ID

Assuming you are currently on the *Microsoft Entra ID* page (see above); 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:

Microsoft Azure

Home > SimSage | Overview

Microsoft Entra ID

Overview | Manage tenants | What's new | Preview features | Got feedback?

Overview | Monitoring | Properties | Recommendations | Tutorials

Search your tenant

Basic information

Name	SimSage	Users	34
Tenant ID	[REDACTED]	Groups	31
Primary domain	simsage.co.uk	Applications	9
License	Microsoft Entra ID Free	Devices	21

Alerts

- Microsoft Entra Connect v1 Retirement**  
All version 1.x builds of Microsoft Entra Connect (formerly AAD Connect) will soon stop working between October 2023 – March 2024. You must move to Cloud Sync or Microsoft Entra Connect v2.x.  
[Learn more](#)
- Azure AD is now Microsoft Entra ID**  
Microsoft Entra ID is the new name for Azure Active Directory. No action is required from you.  
[Learn more](#)

Select 'App Registrations' from sidebar (left)

Microsoft Azure

Home > SimSage

SimSage | App registrations

Microsoft Entra ID

+ New registration | Endpoints | Troubleshooting | Refresh | Download | Preview features | Got feedback?

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

All applications | Owned applications | Deleted applications

Start typing a display name or application (client) ID to filter these r... Add filters

Select '+ New Registration' from tab-bar

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:

Microsoft Azure

Home > SimSage | App registrations >

## Register an application

\* Name

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

simsage-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 Microsoft Entra ID tenant - Multitenant)

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

☐ Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional) Web here, ignore the rest

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 ✓

New Application

Redirect URL is *not* required here.

Once this has been created, you will be redirected to the previous page, copy the client ID, we will need it later to set up the Crawler (see below):

Details Endpoints Preview features

Essentials

Display name: simsage-app

Application (client) ID: [REDACTED]

Object ID: [REDACTED]

Directory (tenant) ID: [REDACTED]

Supported account types: My organization only

Client credentials: Add a certificate or secret

Redirect URIs: Add a Redirect URI

Application (ID URI): Add an Application ID URI

Managed application in: simsage-app

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](#)

Client ID

This lends us nicely to grabbing our client secret.

## Client Secret

Assuming you have done the above, *click* on the application and select "Add a certificate or secret" in the following screen:

Details Endpoints Preview features

Essentials

Display name: simsage-app

Application (client) ID: [REDACTED]

Object ID: [REDACTED]

Directory (tenant) ID: [REDACTED]

Supported account types: My organization only

Client credentials: Add a certificate or secret

Redirect URIs: Add a Redirect URI

Application (ID URI): Add an Application ID URI

Managed application in: simsage-app

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](#)

Selecting "Add a certificate or secret" via app registrations page

You should now be redirected to the below page. Select "+ New client secret":

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.			

Selecting "+ New client secret"

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

simSage-app | Certificates & secrets

+ New client secret

Add a client secret

Description:

Expires:

Adding client secret via sidebar (right)

Select 'Add' at the bottom of this side-bar to generate the secret - copy 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.

## Checking Permissions

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.

Microsoft Azure

simSage-app | API permissions

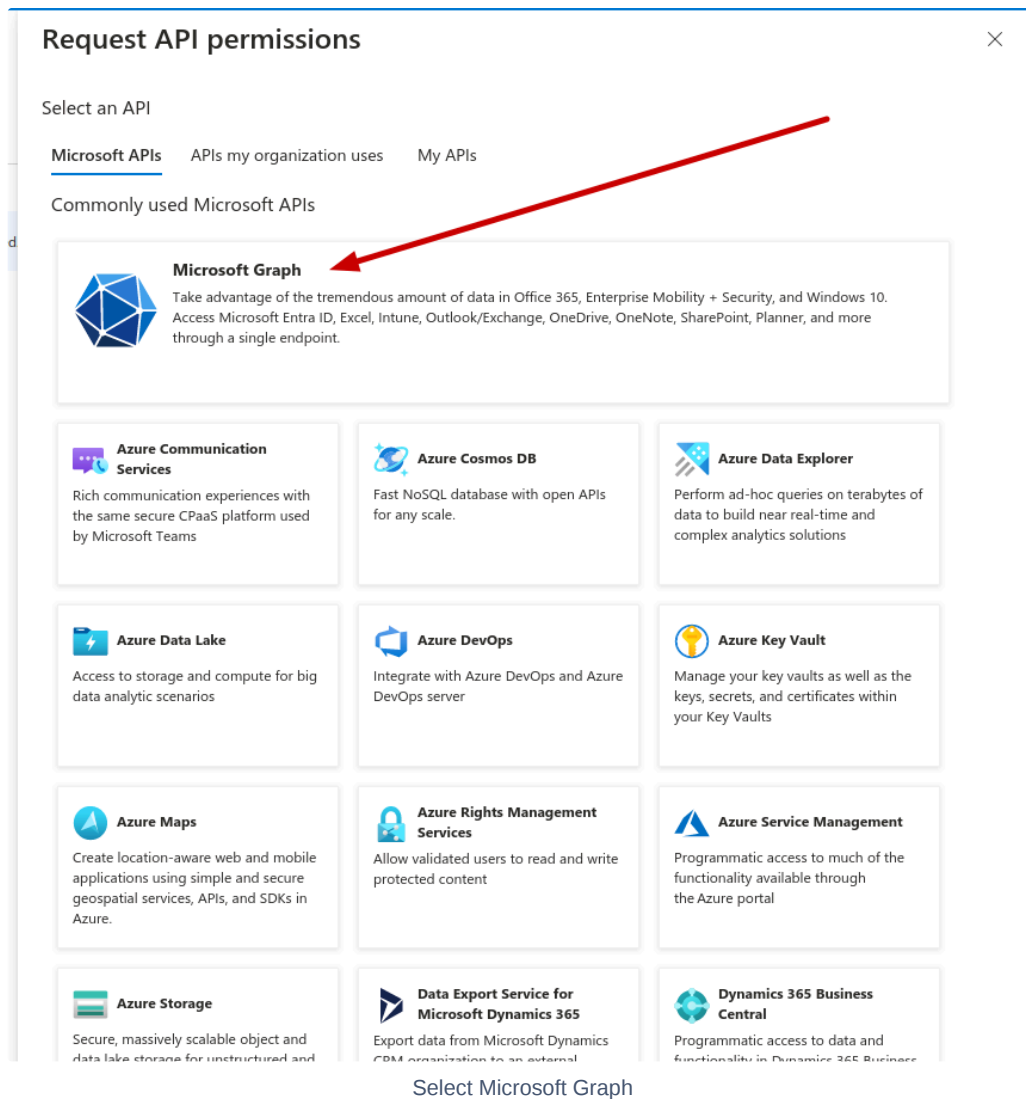
+ Add a permission

Grant admin consent for simSage

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user profile	No	...

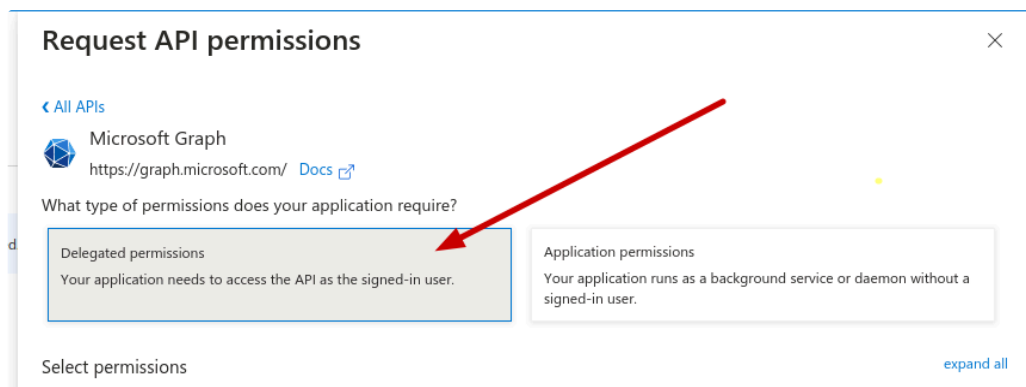
Selecting 'Add a permission' via API permissions page

Select "Microsoft Graph" and select "Application permissions":



## Request API Permissions

Select the 'Delegated permissions' option



Selecting Delegated Permissions Option

Then start typing in the "Select permissions" text box. You need to select the following permissions:

- Files.Read.All
- User.Read
- User.ReadBasic.All

Use the provided search bar and type “files” and/or “user” if you struggle to find these.

You should have the following:

Files (1)

<input type="checkbox"/>	Files.Read ⓘ Read user files	No
<input checked="" type="checkbox"/>	Files.Read.All ⓘ Read all files that user can access	No
<input type="checkbox"/>	Files.Read.Selected ⓘ Read files that the user selects (preview)	No
<input type="checkbox"/>	Files.ReadWrite ⓘ Have full access to user files	No
<input type="checkbox"/>	Files.ReadWrite.All ⓘ Have full access to all files user can access	No
<input type="checkbox"/>	Files.ReadWrite.AppFolder ⓘ Have full access to the application's folder (preview)	No
<input type="checkbox"/>	Files.ReadWrite.Selected ⓘ Read and write files that the user selects (preview)	No

File Permission Settings

User (3)

<input type="checkbox"/>	User.EnableDisableAccount.All ⓘ Enable and disable user accounts	Yes
<input type="checkbox"/>	User.Export.All ⓘ Export user's data	Yes
<input type="checkbox"/>	User.Invite.All ⓘ Invite guest users to the organization	Yes
<input type="checkbox"/>	User.ManageIdentities.All ⓘ Manage user identities	Yes
<input checked="" type="checkbox"/>	User.Read ⓘ Sign in and read user profile	No
<input checked="" type="checkbox"/>	User.Read.All ⓘ Read all users' full profiles	Yes
<input checked="" type="checkbox"/>	User.ReadBasic.All ⓘ Read all users' basic profiles	No
<input type="checkbox"/>	User.ReadWrite ⓘ Read and write access to user profile	No
<input type="checkbox"/>	User.ReadWrite.All ⓘ Read and write all users' full profiles	Yes

User Permission Settings

Click 'Add permissions' at the bottom of the side bar:

▼ User (3)

<input type="checkbox"/>	User.EnableDisableAccount.All ⓘ Enable and disable user accounts	Yes
<input type="checkbox"/>	User.Export.All ⓘ Export user's data	Yes
<input type="checkbox"/>	User.Invite.All ⓘ Invite guest users to the organization	Yes
<input type="checkbox"/>	User.ManageIdentities.All ⓘ Manage user identities	Yes
<input checked="" type="checkbox"/>	User.Read ⓘ Sign in and read user profile	No
<input checked="" type="checkbox"/>	User.Read.All ⓘ Read all users' full profiles	Yes
<input checked="" type="checkbox"/>	User.ReadBasic.All ⓘ Read all users' basic profiles	No
<input type="checkbox"/>	User.ReadWrite ⓘ Read and write access to user profile	No
<input type="checkbox"/>	User.ReadWrite.All ⓘ Read and write all users' full profiles	Yes
> VirtualAppointmentNotification		
> VirtualAppointment		
> VirtualEvent		
> WindowsUpdates		
> WorkforceIntegration		

Add Permissions

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

ⓘ 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 SimSage

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (4)				...
Files.Read.All	Delegated	Read all files that user can access	No	Granted for SimSage
User.Read	Delegated	Sign in and read user profile	No	Granted for SimSage
User.Read.All	Delegated	Read all users' full profiles	Yes	Granted for SimSage
User.ReadBasic.All	Delegated	Read all users' basic profiles	No	Granted for SimSage

Granted Permissions

☒ Talk to your manager if you cannot select 'Grant admin consent for SimSage' - they may need to grant permissions on your behalf

## Basic Crawler Setup

In the Crawler Dialog select the OneDrive crawler and on the "OneDrive crawler" page add the following values:



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

## Crawl Through Specific One Drive Accounts