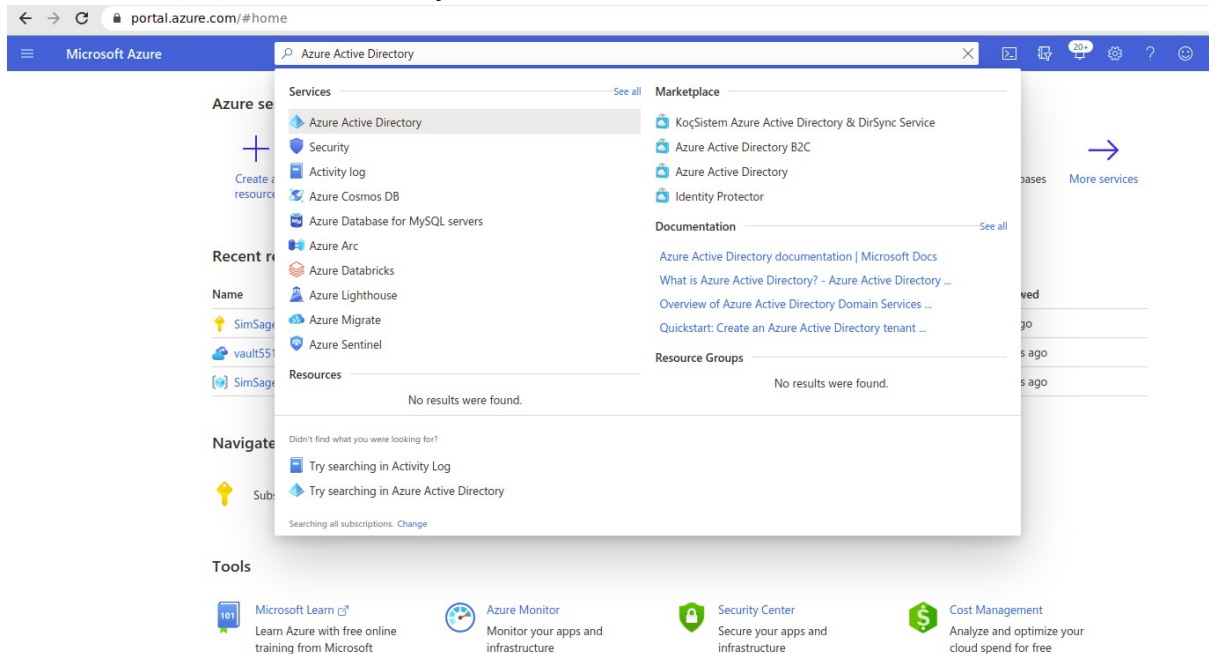


This is a short guide aimed at showing how to configure Microsoft Azure to enable the SimSage Office 365 crawler.

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. This is your “Tenant Id” in SimSage.

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo and a search bar. The left sidebar contains a menu with options like Overview, Getting started, Preview features, Diagnose and solve problems, and a Manage section with various tools. The main content area displays the SimSage Overview page. A red box highlights the Tenant ID, which is 530fb...36... The page also shows other information such as the role (Global administrator), license (Azure AD Premium P2), and primary domain (simsage.co.uk).

portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Overview

Microsoft Azure

Search resources, services, and docs (G+)

Home >

SimSage | Overview

Azure Active Directory

Switch tenant Delete tenant Create a tenant What's new Preview features Got feedback?

Azure Active Directory can help you enable remote work for your employees and partners. [Learn more](#)

SimSage

Search your tenant

Tenant information

Your role
Global administrator and 7 other roles
[More info](#)

License
Azure AD Premium P2

Tenant ID
530fb...36... [Copy](#)

Primary domain
simsage.co.uk

Azure AD Connect

Status
Not enabled

Last sync
Sync has never run

Sign-ins

60
50
40
30
20
10
0

Feb 21 Feb 28 Mar 7 Mar 14

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.


portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/RegisteredApps

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

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  ignore

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

By proceeding, you agree to the Microsoft Platform Policies 

Register  click Register

Copy the Client ID once this app has been created.

portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/RegisteredApps

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

Home > SimSage


SimSage | App registrations


Azure Active Directory

Overview
Getting started
Preview features
Diagnose and solve problems

Manage
Users
Groups
External Identities
Roles and administrators
Administrative units
Enterprise applications
Devices
App registrations
Identity Governance




+ New registration Endpoints Troubleshooting Download Preview features Got feedback?

 Try out the new App registrations search preview! Click to enable the preview. →

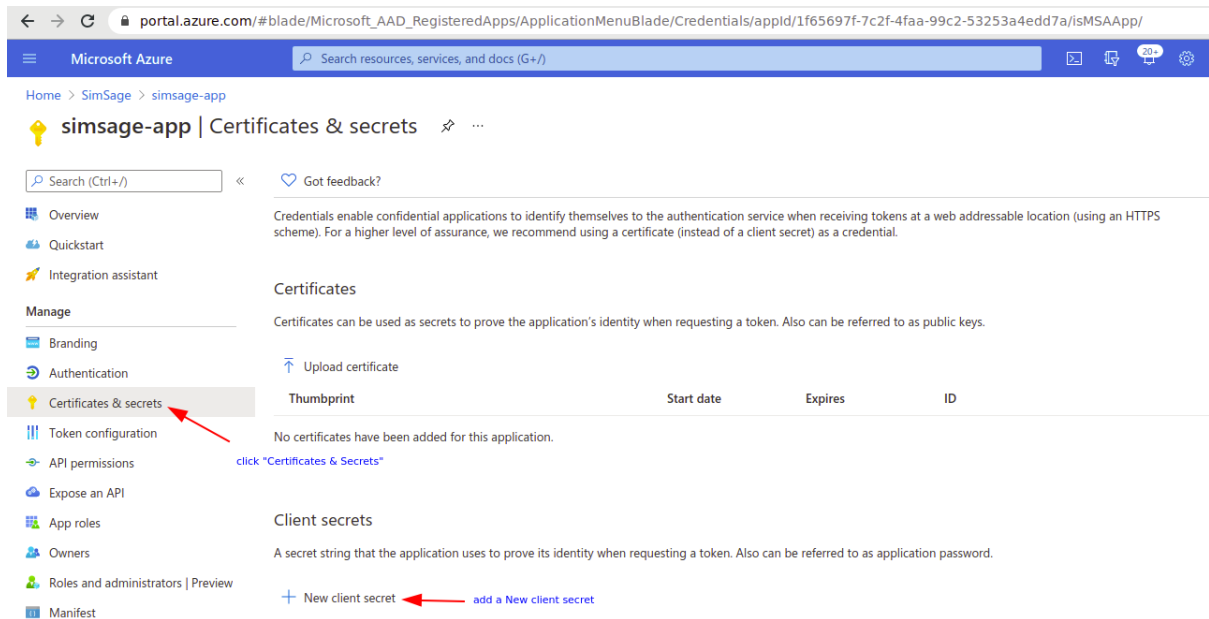
 Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft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

All applications **Owned applications** Deleted applications (Preview)

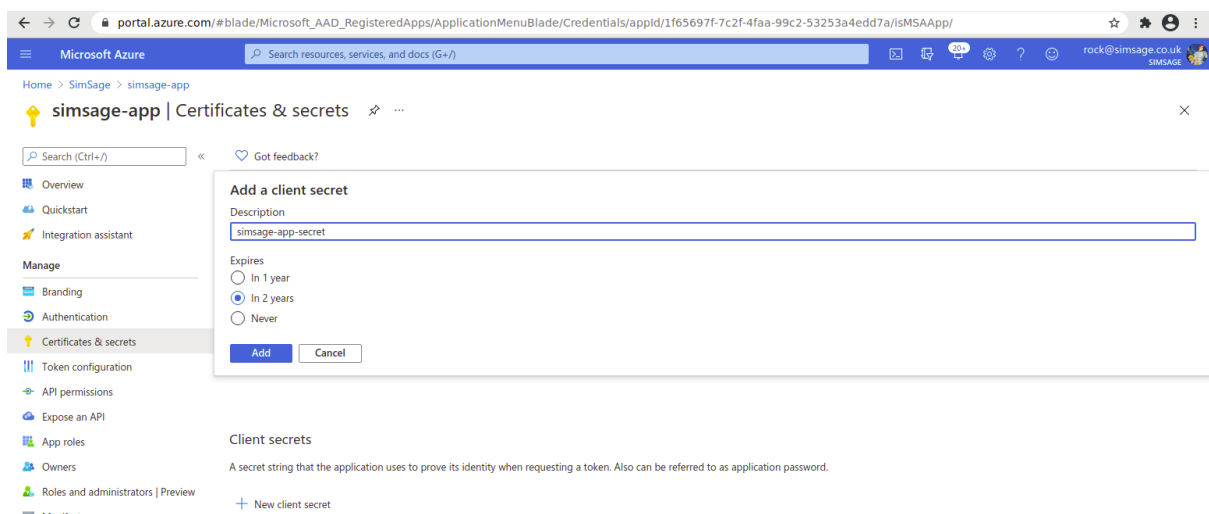
Start typing a name or Application ID to filter these results

Display name	Application (client) ID	Created on	Certificates & secrets
 simsage-app	1165697f-7c2f-4faa-99c2-53253a4edd7a  this is your Client ID for SimSage, copy it.	3/22/2021	 Current

Next we setup a client-secret. Click on the app you just created, “simsage-app” in our example. Then click “Certificates & secrets” in the left-hand-side menu.



This brings pops-up an “Add a client secret” dialog. Select the right expiry time and secret-name for your application.



Click the “Add” button to finish adding this new secret.

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. This is the “client secret” value required by SimSage.

portal.azure.com/#blade/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/Credentials/appid/1f65697f-7c2f-4faa-99c2-53253a4edd7a/ISMSAAApp/

Microsoft Azure

Home > SimSage > simsage-app

simsage-app | Certificates & secrets

Search (Ctrl+/) Got feedback?

Overview
Quickstart
Integration assistant

Manage

Branding
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators | Preview
Manifest

Support + Troubleshooting
Troubleshooting
New support request

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.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Upload certificate

Thumbprint	Start date	Expires	ID
No certificates have been added for this application.			

Client secrets

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	ID
simsage-app-secret	3/22/2023	m.i*****	b5760f95-8f73-48b7-9fde-985f9ddd5ad4

Revisiting the secret at a later stage will no longer show the secret's value. You can never recover this value. If you lose the secret, delete the existing one, and create it anew.

Next we need to set permissions for the SimSage Office 365 crawler.

portal.azure.com/#blade/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/CallAnAPI/appid/1f65697f-7c2f-4faa-99c2-53253a4edd7a/ISMSAAApp/

Microsoft Azure

Home > SimSage > simsage-app

simsage-app | API permissions

Search (Ctrl+/) Refresh Got feedback?

Overview
Quickstart
Integration assistant

Manage

Branding
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators | Preview
Manifest

Support + Troubleshooting
Troubleshooting
New support request

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

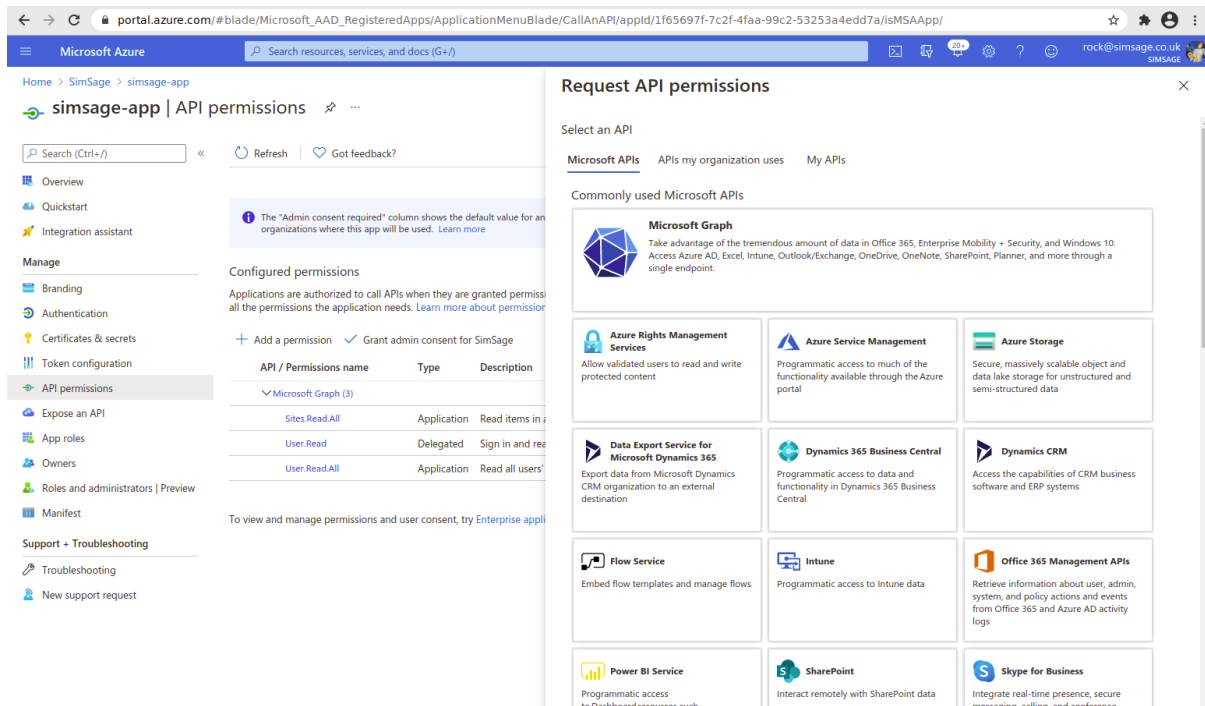
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission Grant admin consent for SimSage

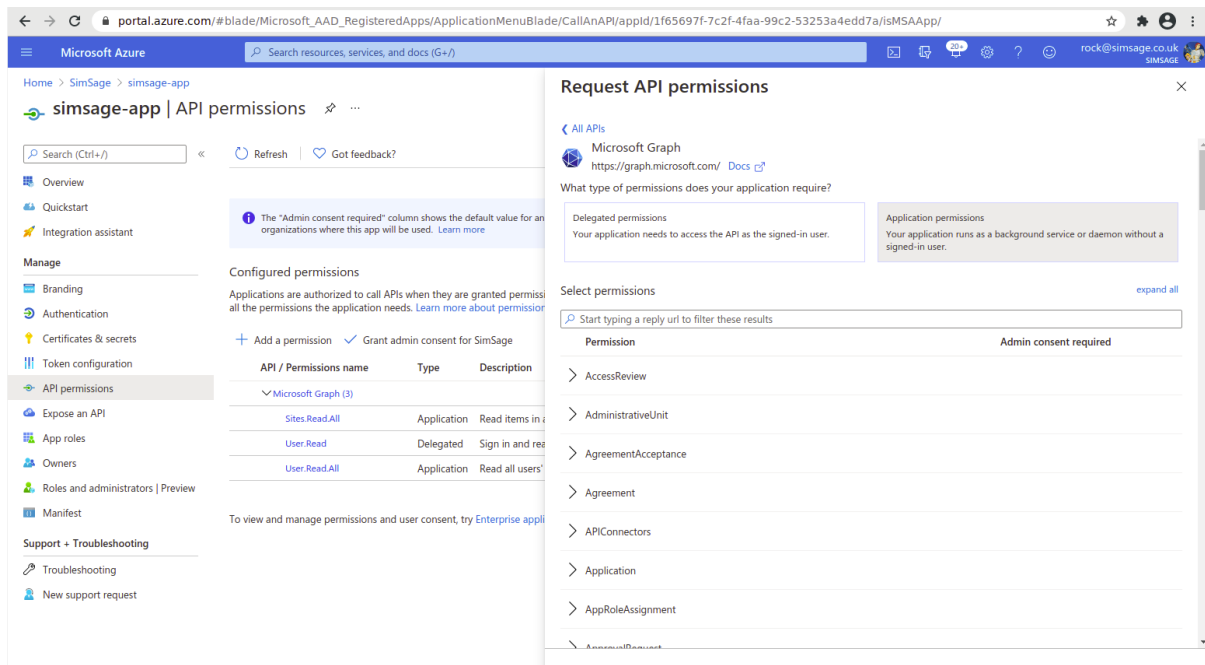
API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph				
User.Read	Delegated	Sign in and read user profile	No	Granted for SimSage

To view and manage permissions and user consent, try [Enterprise applications](#).

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



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



You need to select the following permissions. You can do this in one go if you like, or repeat the above step three times. We only require three permissions. These are:

Files.Read.All for reading OneDrive files

Sites.Read.All
User.Read.All

for reading SharePoint files
for reading User data for security permissions and OneDrive

We only ever “read” from these systems.

The finished permissions are shown in the screenshot below. Make sure you click the “Grant admin consent for <name>” button. This finalizes and activates the permissions.

The screenshot shows the 'API permissions' page for the 'simsage-app' in the Microsoft Azure portal. The page has a left-hand navigation menu with options like Overview, Quickstart, Integration assistant, Manage, Branding, Authentication, Certificates & secrets, Token configuration, API permissions (selected), Expose an API, App roles, Owners, Roles and administrators | Preview, Manifest, Support + Troubleshooting, Troubleshooting, and New support request. The main content area shows a message 'Successfully granted admin consent for the requested permissions.' and a section titled 'Configured permissions' with a sub-header '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'. Below this is a table of permissions:

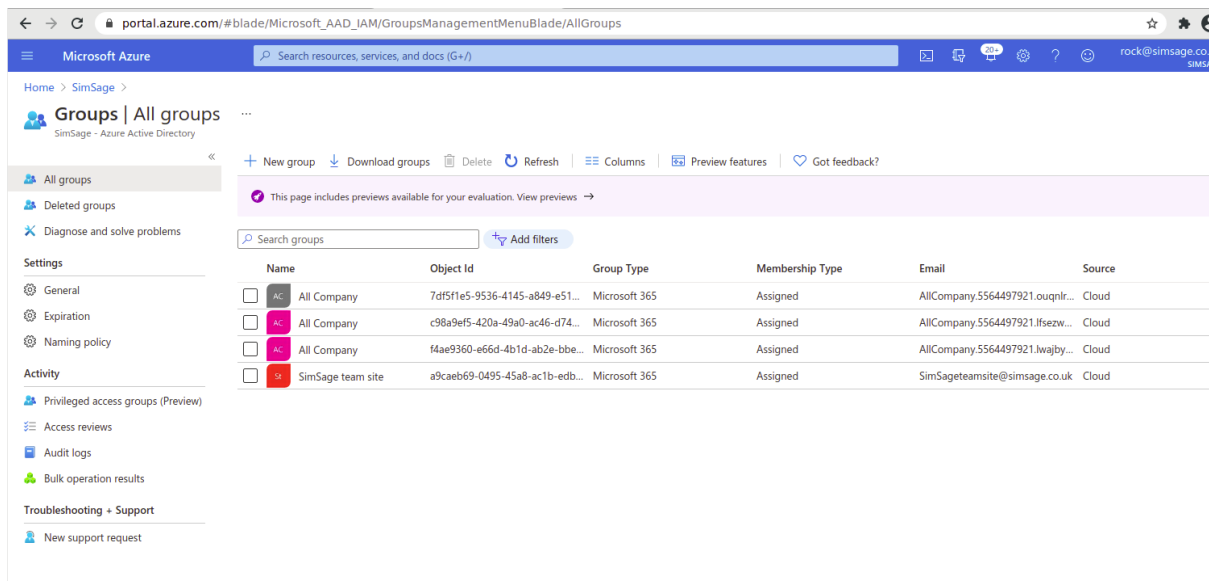
API / Permissions name	Type	Description	Admin consent req...	Status
▼ Microsoft Graph (4)				
Files.Read.All	Application	Read files in all site collections	Yes	Granted for SimSage
Sites.Read.All	Application	Read items in all site collections (preview)	Yes	Granted for SimSage
User.Read	Delegated	Sign 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 permissions and user consent, try [Enterprise applications](#).

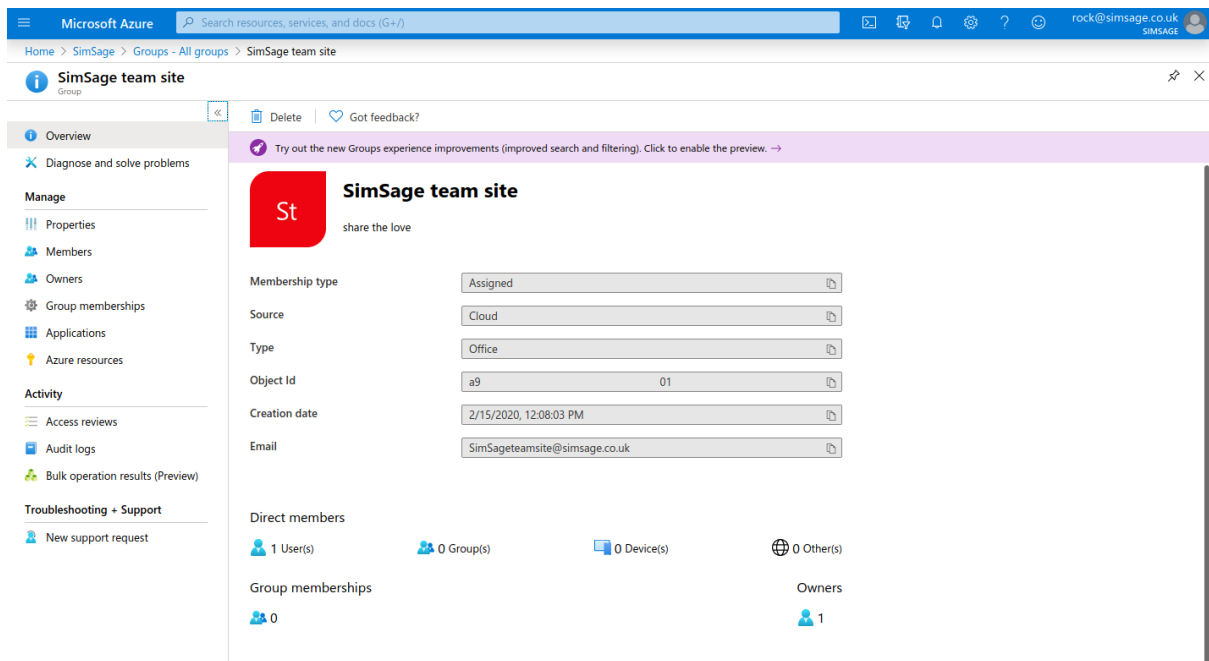
SharePoint site IDs

SharePoint site IDs are required if you want to index sites other than the default site. These site IDs can only be gotten through Azure Active Directory. Go back to the top level “Azure Active Directory” by typing it in the “Search resources, ...” bar at the top. Once selected, click on “All groups”.

Click on “All groups” on the left-hand-side of your Azure Active Directory menu. The pane on the right-hand-side shows all your SharePoint sites by name.



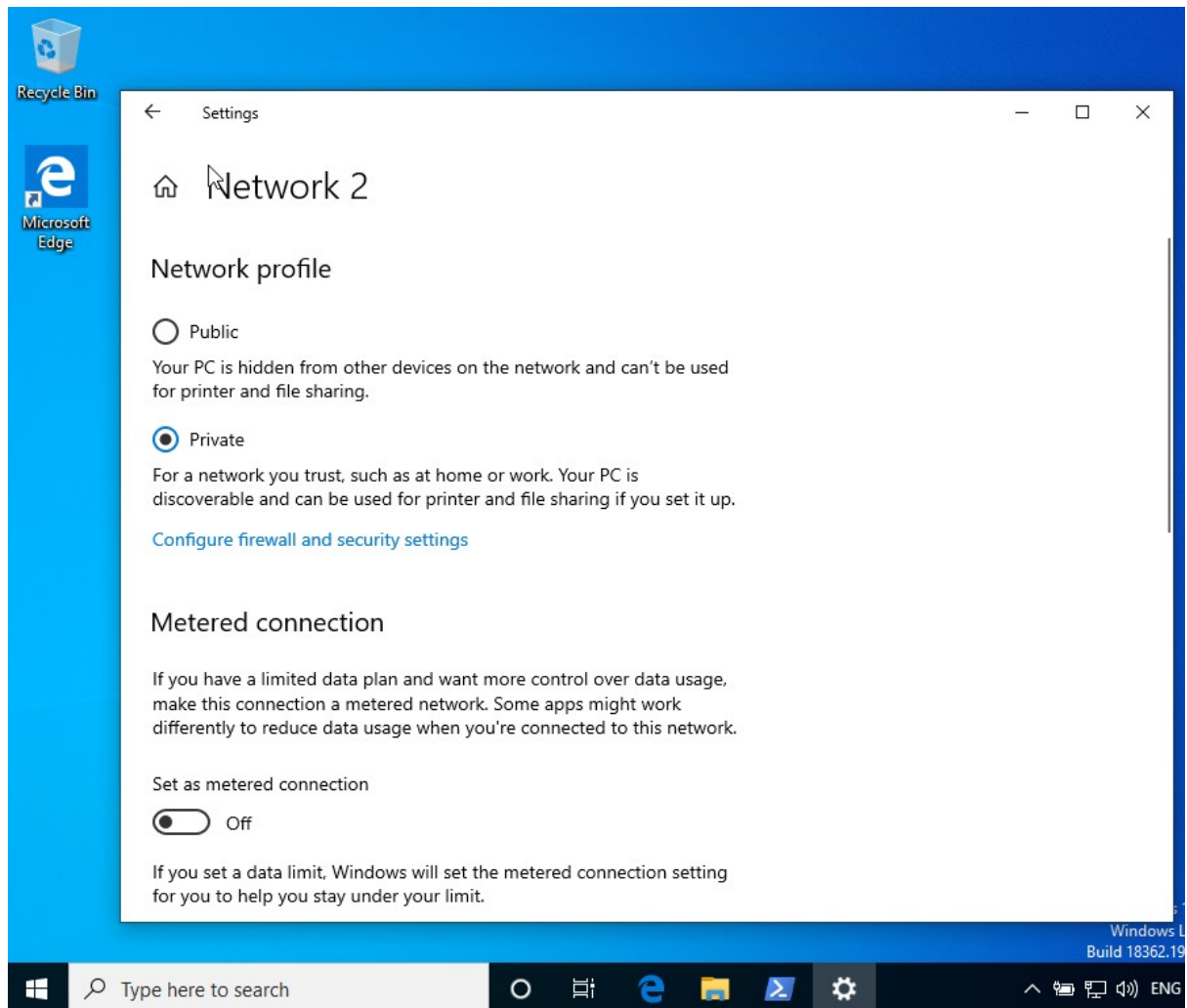
Click on the site whose id you need to view all its details.



Copy the “Object Id” (it has been masked for security reasons in the image shown above). This is your SharePoint site ID.

Enabling Microsoft Exchange for Office 365

This process requires a Microsoft Windows installation with PowerShell. Windows 8.1, Windows 10, or Windows 2016 with GUI.



Make sure your network connection is set to private or domain.

Open a PowerShell session as Administrator. We've taken our instructions from:

<https://docs.microsoft.com/en-us/powershell/exchange/exchange-online/connect-to-exchange-online-powershell/connect-to-exchange-online-powershell?view=exchange-ps>

We will go through this guide in an abbreviated manner now. All commands following are PowerShell commands and must be issued as the administrator on your Windows machine.

```
> Set-ExecutionPolicy RemoteSigned
```

See if "Basic" is enabled for "winrm"

```
> winrm get winrm/config/client/auth
```

If it is set to false, execute the following command

```
> winrm set winrm/config/client/auth @{Basic="true"}
```

Set your Microsoft Office 365 admin credentials

```
> $UserCredential = Get-Credential
```

NB. This will pop-up a GUI box asking for your user-name and password. These must be your Office 365 administrator credentials.

Then we setup a session with our remote Office 365 cloud server (all on one line)

```
> $Session = New-PSSession -ConfigurationName Microsoft.Exchange -  
ConnectionUri https://outlook.office365.com/powershell-liveid/  
-Credential $UserCredential  
-Authentication Basic  
-AllowRedirection
```

And finally we enable the Graph API through the following command:

```
> Import-PSSession $Session -DisableNameChecking
```

Finally, we need to enable our Microsoft Graph API inside the Azure portal as we did before. The combined permission set is shown below. Don't forget to click the "Grant admin consent for ..." button.

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo, a search bar, and user information (rock@simstage.co.uk). The left sidebar contains navigation links: Overview, Quickstart, Manage (Branding, Authentication, Certificates & secrets, Token configuration (preview), API permissions, Expose an API, Owners, Roles and administrators (Preview), Manifest), and Support + Troubleshooting (Troubleshooting, New support request). The main content area is titled "simstage - API permissions" and shows a notification: "Successfully granted admin consent for the requested permissions." Below this, the "Configured permissions" section lists permissions for the "Microsoft Graph (6)" application. The table below details these permissions.

API / Permissions name	Type	Description	Admin Consent Required	Status
Microsoft Graph (6)				
Files.ReadWrite.All	Application	Read and write files in all site collections	Yes	Granted for SimSage
Mail.Read	Application	Read mail in all mailboxes	Yes	Granted for SimSage
Mail.ReadBasic.All	Application	Read basic mail in all mailboxes	Yes	Granted for SimSage
Mail.ReadWrite	Application	Read and write mail in all mailboxes	Yes	Granted for SimSage
Sites.ReadWrite.All	Application	Read and write items in all site collections (pr...	Yes	Granted for SimSage
User.ReadWrite.All	Application	Read and write all users' full profiles	Yes	Granted for SimSage

The permissions to add are:

Mail.Read, Mail.ReadBasic.All, and Mail.ReadWrite