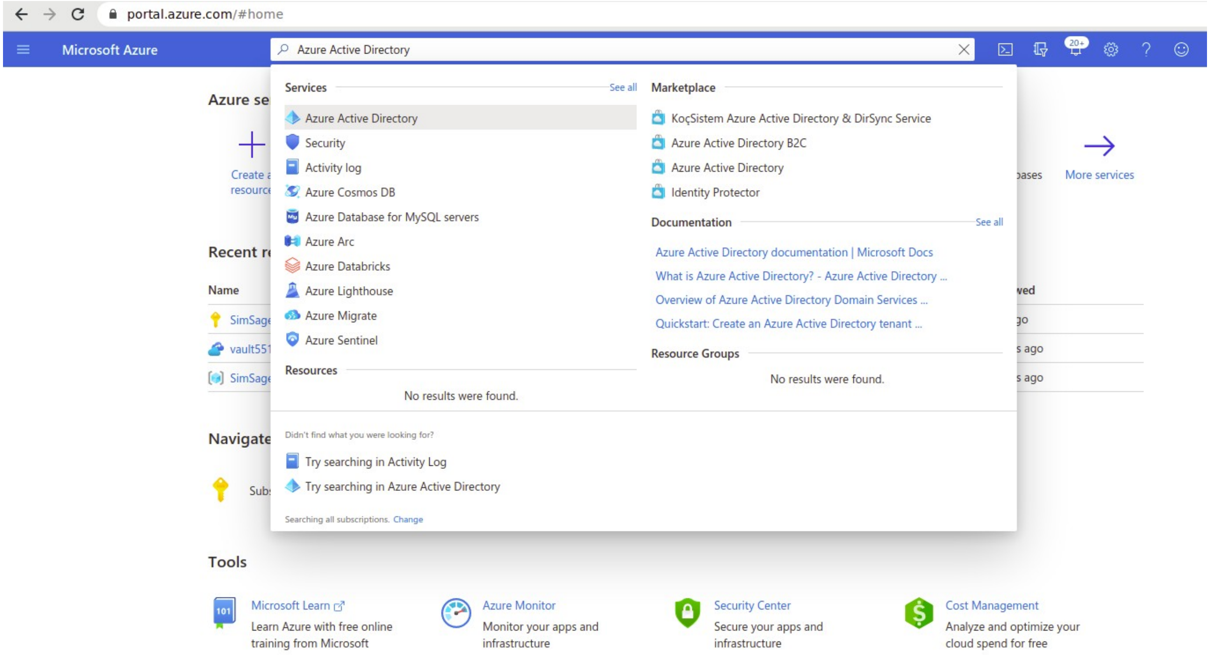
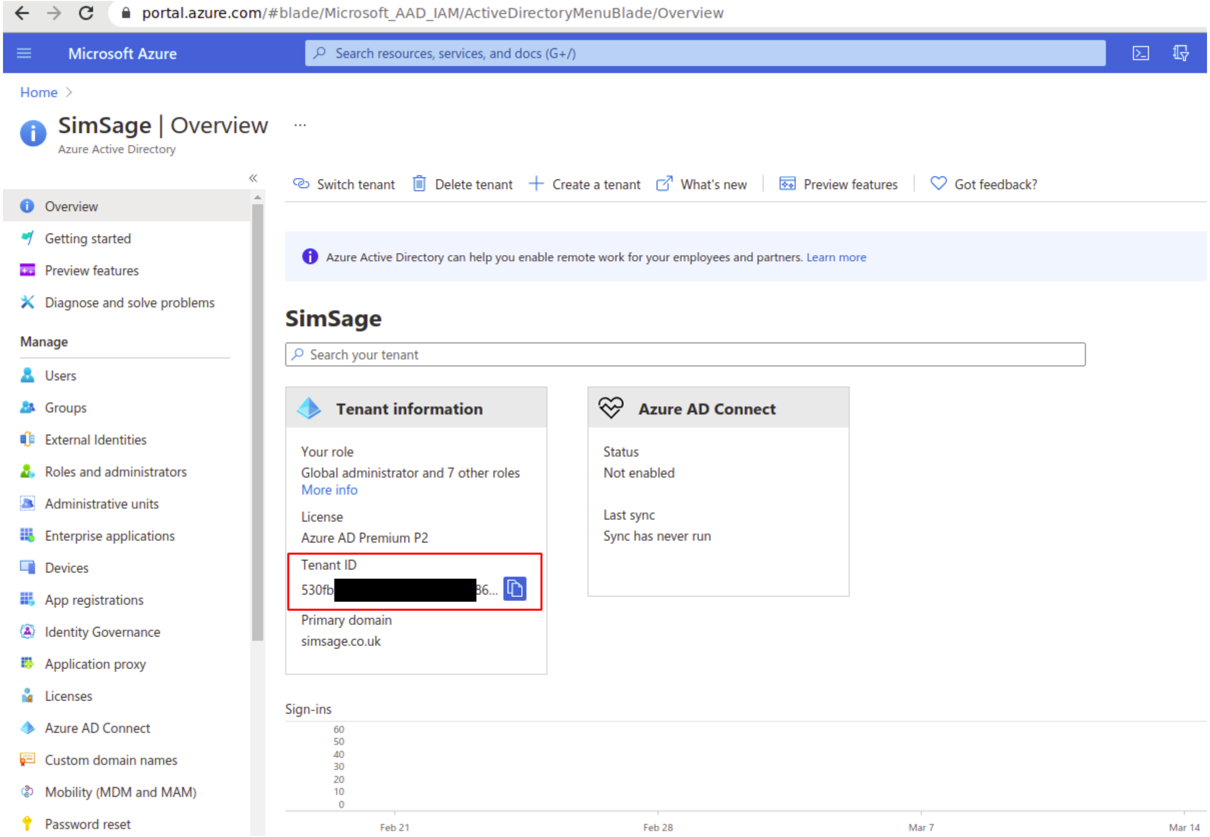
This is a short guide aimed at showing how to configure Microsoft Azure to enable the SimSage Exchange 365 crawler.

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.


portal.azure.com/#home
Microsoft Azure
Azure Active Directory
Services
See all
Azure Active Directory
Security
Activity log
Azure Cosmos DB
Azure Database for MySQL servers
Azure Arc
Azure Databricks
Azure Lighthouse
Azure Migrate
Azure Sentinel
Resources
No results were found.
Marketplace
KoçSistem Azure Active Directory & DirSync Service
Azure Active Directory B2C
Azure Active Directory
Identity Protector
Documentation
See all
Azure Active Directory documentation | Microsoft Docs
What is Azure Active Directory? - Azure Active Directory ...
Overview of Azure Active Directory Domain Services ...
Quickstart: Create an Azure Active Directory tenant ...
Resource Groups
No results were found.
Didn't find what you were looking for?
Try searching in Activity Log
Try searching in Azure Active Directory
Searching all subscriptions. Change
Azure se
Create a resource
Recent r
Name
SimSage
vault551
SimSage
Navigate
Subs
More services
Tools
Microsoft Learn
Learn Azure with free online training from Microsoft
Azure Monitor
Monitor your apps and infrastructure
Security Center
Secure your apps and infrastructure
Cost Management
Analyze and optimize your cloud spend for free

Copy the Tenant Id. This is your “Tenant Id” in SimSage.



Tenant information

Your role
Global administrator and 7 other roles
More info

License
Azure AD Premium P2

Tenant ID
530fb[redacted]6...

Primary domain
simsage.co.uk

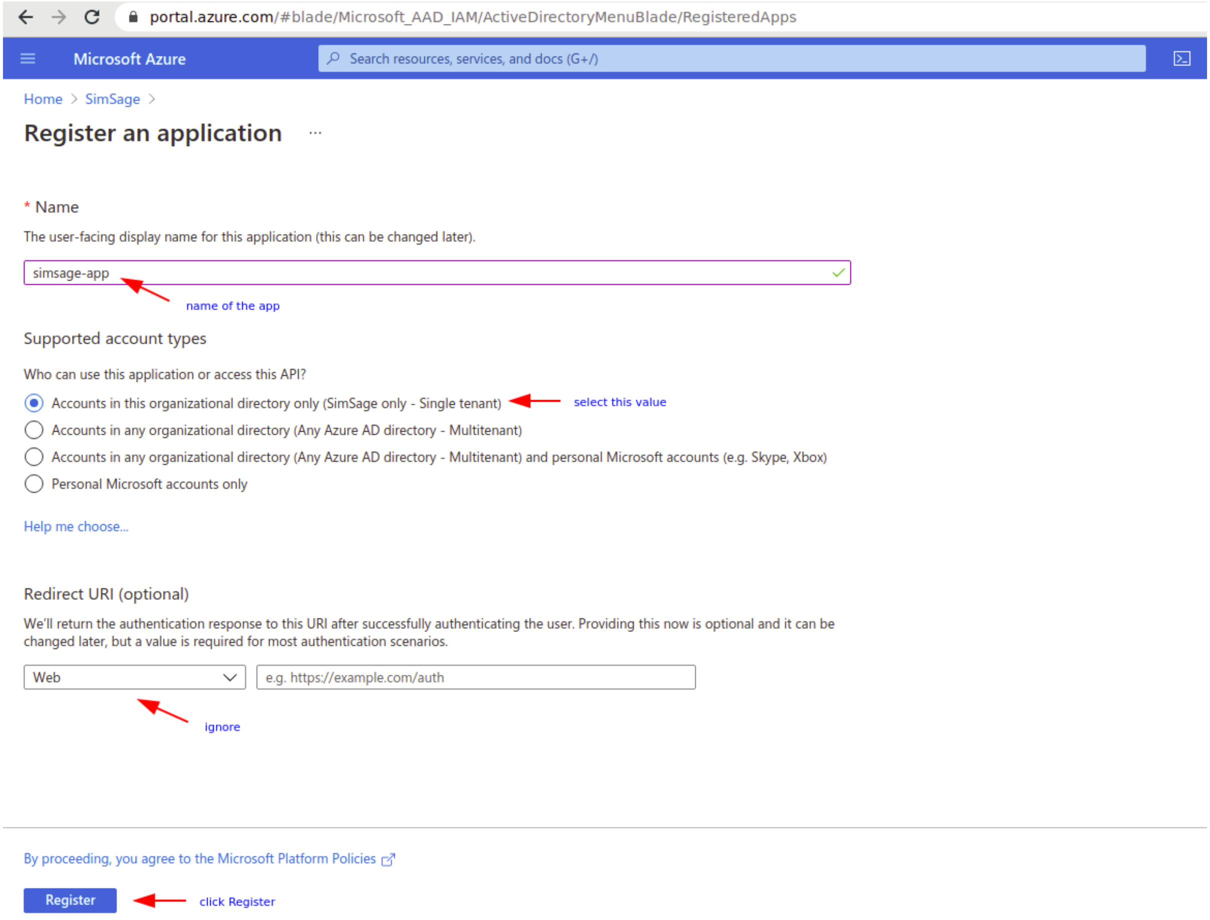
Azure AD Connect

Status
Not enabled

Last sync
Sync has never run

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.

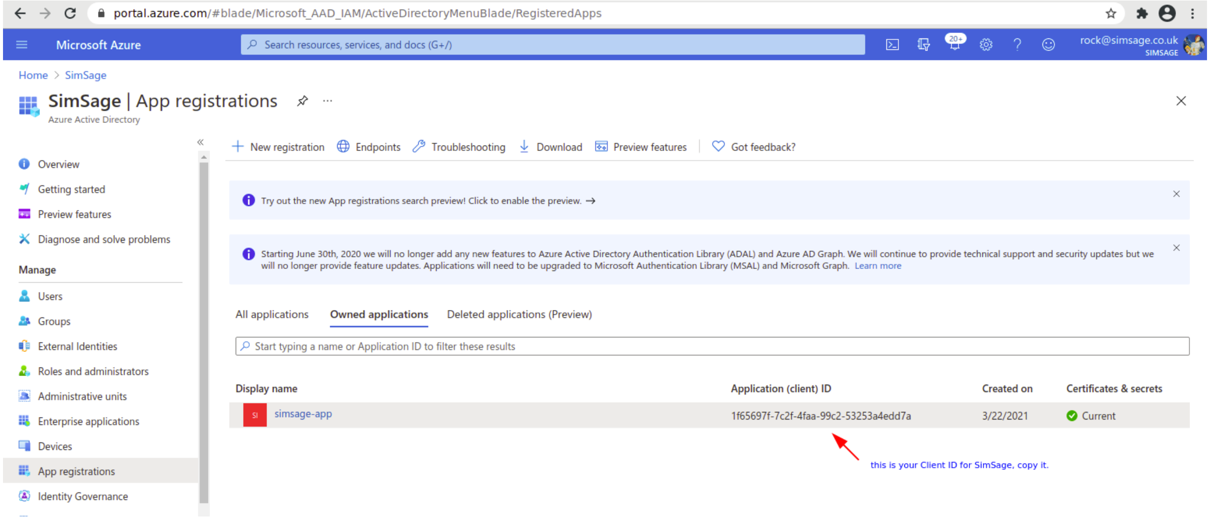
Web | e.g. https://example.com/auth

ignore

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+/)

rock@simsage.co.uk
SIMSAGE

Home > SimSage

SimSage | App registrations

Azure Active Directory

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

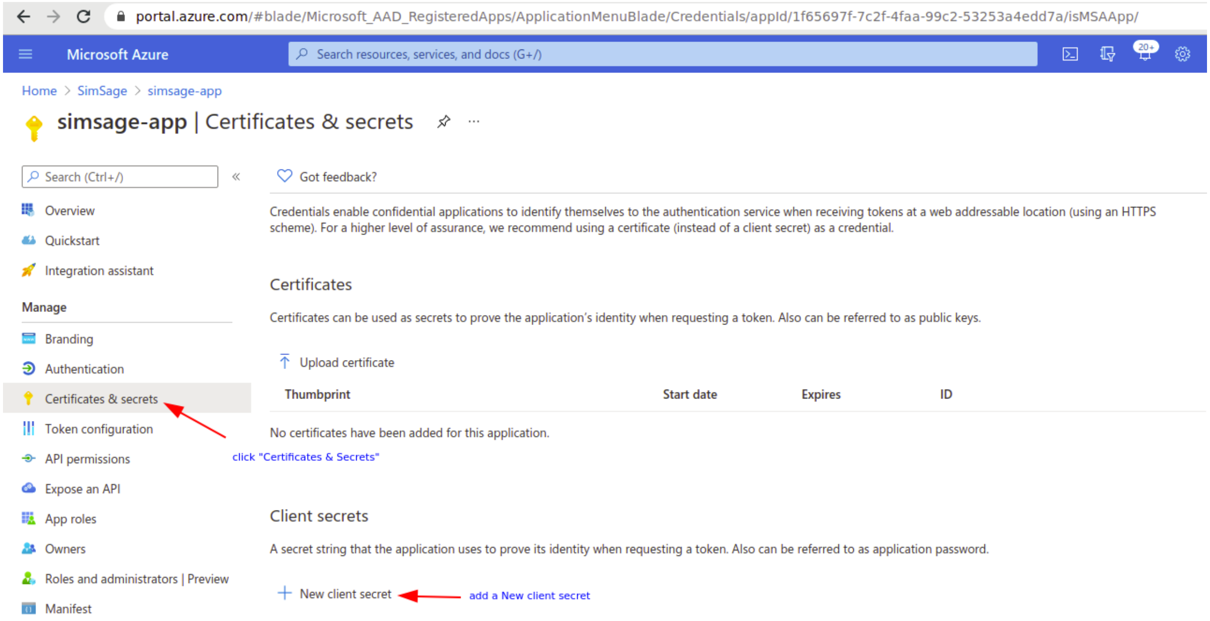
All applications | **Owned applications** | Deleted applications (Preview)

Start typing a name or Application ID to filter these results

Display name	Application (client) ID	Created on	Certificates & secrets
SI simsage-app	1f65697f-7c2f-4faa-99c2-53253a4edd7a	3/22/2021	✓ Current

this is your Client ID for SimSage, copy it.

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.



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

simsage-app | 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.

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.

Thumbprint	Start date	Expires	ID

No certificates have been added for this application.

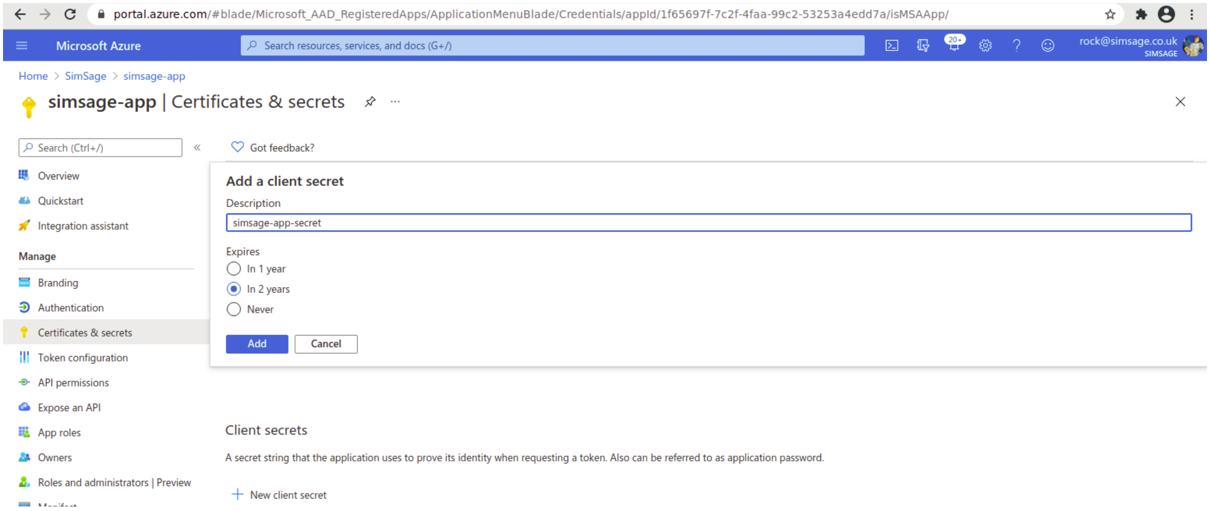
Client secrets

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

click "Certificates & Secrets"

add a New client secret

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



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

simsage-app | Certificates & secrets

Add a client secret

Description: simsage-app-secret

Expires

○ In 1 year

● In 2 years

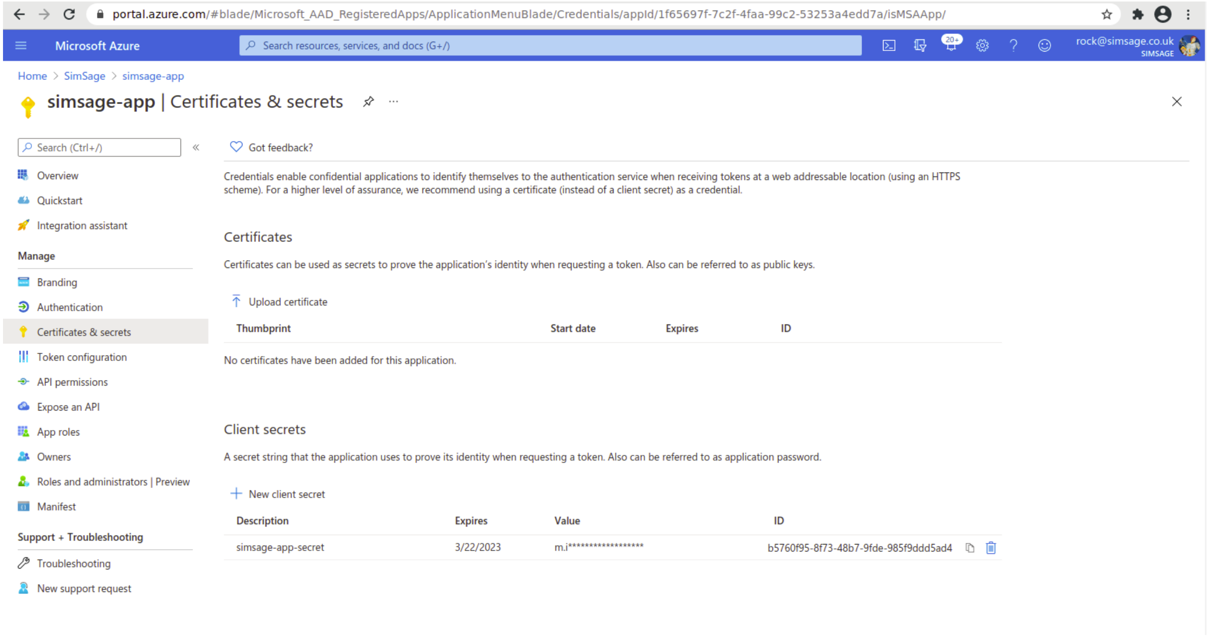
○ Never

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.

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/isMSAApp/
Microsoft Azure
Search resources, services, and docs (G+/)
20+
rock@simsage.co.uk
SIMSAGE
Home > SimSage > simsage-app
simsage-app | Certificates & secrets
Search (Ctrl+/)
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
Got feedback?

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.

Thumbprint	Start date	Expires	ID

No certificates have been added for this application.

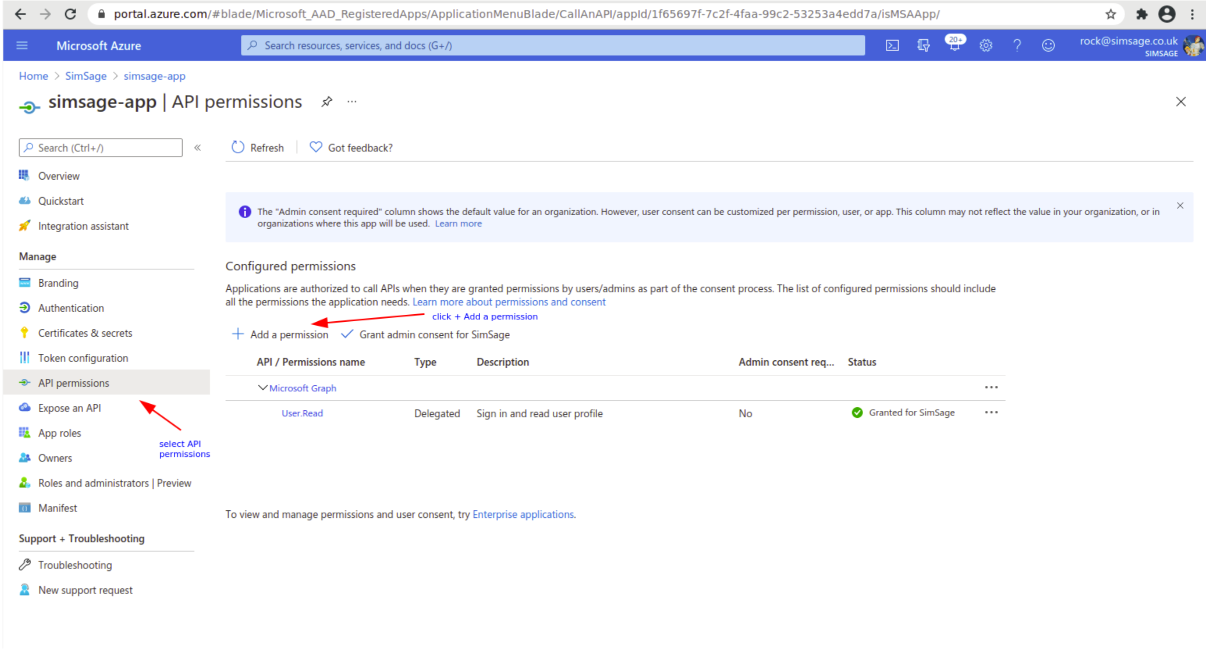
Client secrets

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

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/isMSAApp/
Microsoft Azure
Search resources, services, and docs (G+/)
20+
rock@simsage.co.uk
SIMSAGE
Home > SimSage > simsage-app
simsage-app | API permissions
Search (Ctrl+/)
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
Refresh
Got feedback?

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

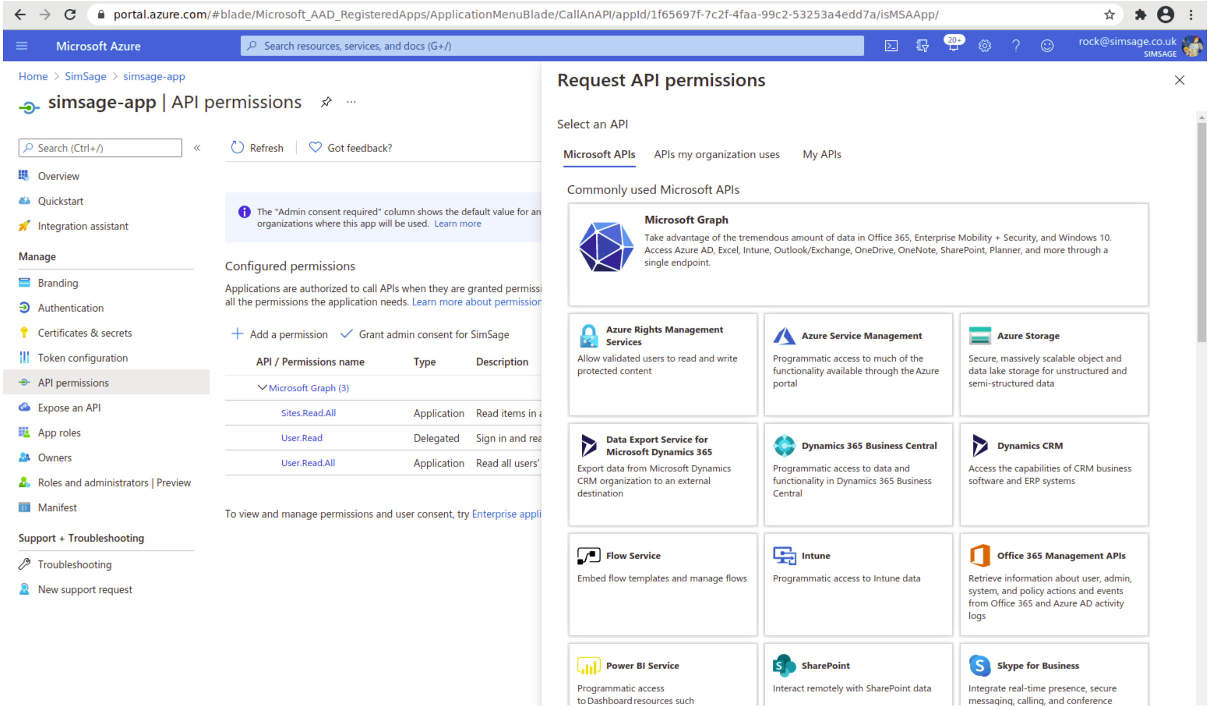
click + Add a permission

select API permissions

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.



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

Microsoft Azure — Search resources, services, and docs (G+/) — rock@simsage.co.uk SIMSAGE

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 organizations where this app will be used. Learn more

Configured permissions

Applications are authorized to call APIs when they are granted permissi all the permissions the application needs. Learn more about permission

+ Add a permission ✓ Grant admin consent for SimSage

API / Permissions name	Type	Description
Microsoft Graph (3)		
Sites.Read.All	Application	Read items in a
User.Read	Delegated	Sign in and rea
User.Read.All	Application	Read all users'

To view and manage permissions and user consent, try Enterprise appli

Request API permissions

Select an API

Microsoft APIs — APIs my organization uses — My APIs

Commonly used Microsoft APIs

Microsoft Graph
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

Azure Rights Management Services
Allow validated users to read and write protected content

Azure Service Management
Programmatic access to much of the functionality available through the Azure portal

Azure Storage
Secure, massively scalable object and data lake storage for unstructured and semi-structured data

Data Export Service for Microsoft Dynamics 365
Export data from Microsoft Dynamics CRM organization to an external destination

Dynamics 365 Business Central
Programmatic access to data and functionality in Dynamics 365 Business Central

Dynamics CRM
Access the capabilities of CRM business software and ERP systems

Flow Service
Embed flow templates and manage flows

Intune
Programmatic access to Intune data

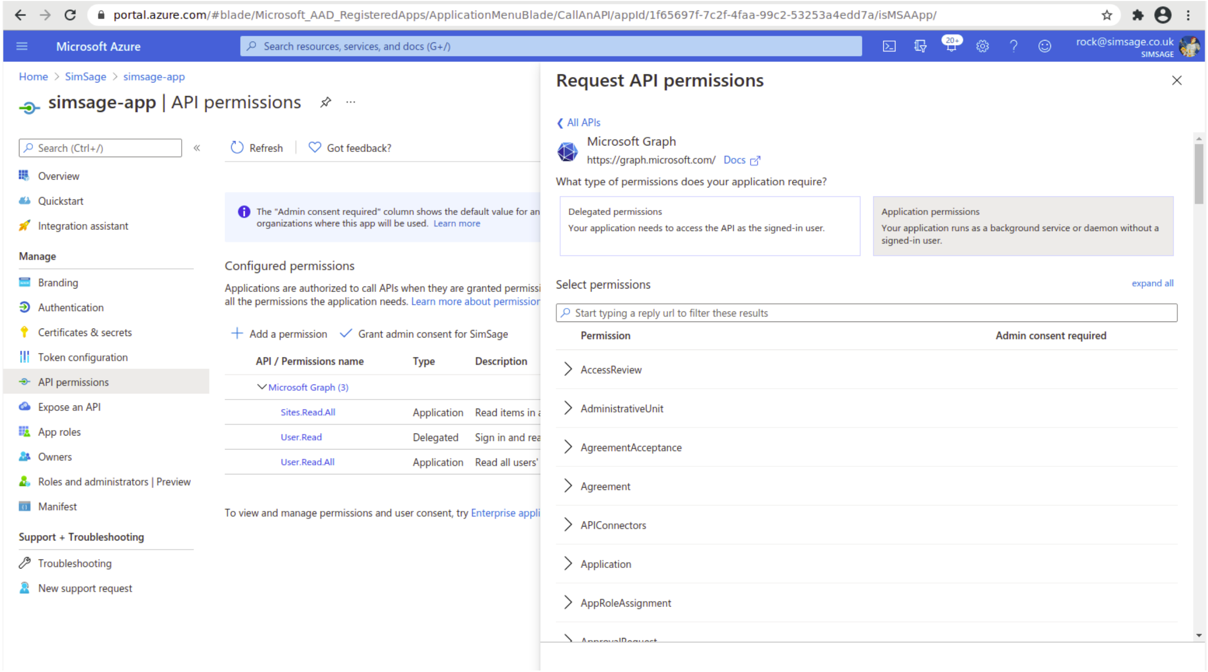
Office 365 Management APIs
Retrieve information about user, admin, system, and policy actions and events from Office 365 and Azure AD activity logs

Power BI Service
Programmatic access to Dashboard resources such

SharePoint
Interact remotely with SharePoint data

Skype for Business
Integrate real-time presence, secure messaging, calling, and conference

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



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

Microsoft Azure — Search resources, services, and docs (G+/) — rock@simsage.co.uk SIMSAGE

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 organizations where this app will be used. Learn more

Configured permissions

Applications are authorized to call APIs when they are granted permissi all the permissions the application needs. Learn more about permission

+ Add a permission ✓ Grant admin consent for SimSage

API / Permissions name	Type	Description
Microsoft Graph (3)		
Sites.Read.All	Application	Read items in a
User.Read	Delegated	Sign in and rea
User.Read.All	Application	Read all users'

To view and manage permissions and user consent, try Enterprise appli

Request API permissions

< All APIs

Microsoft Graph
https://graph.microsoft.com/ Docs

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 without a signed-in user.

Select permissions — expand all

Start typing a reply url to filter these results

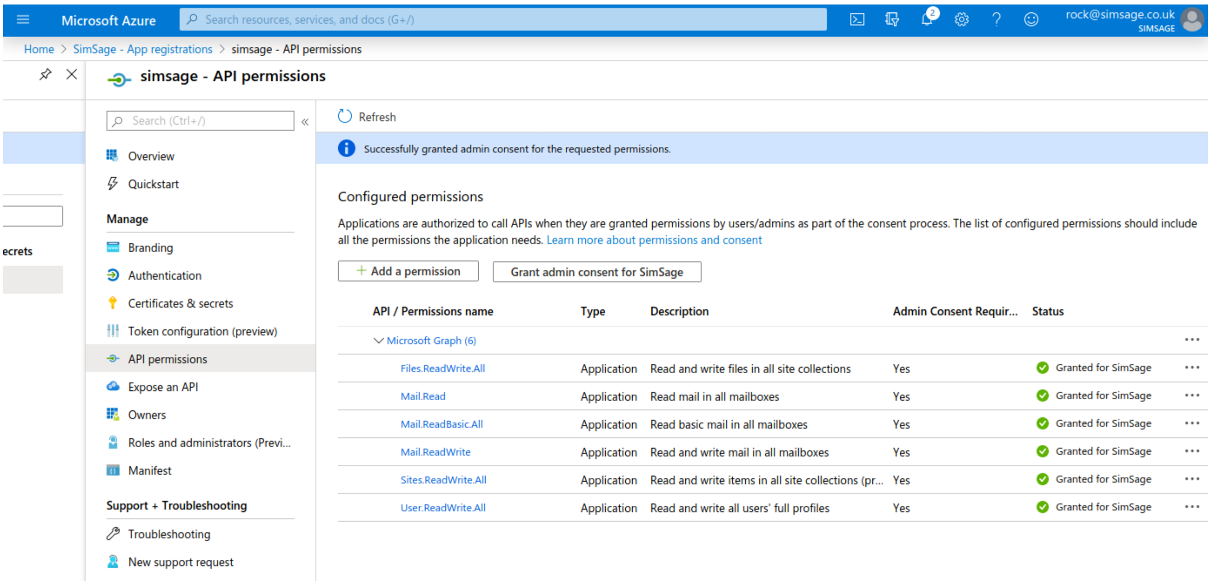
Permission	Admin consent required
> AccessReview	
> AdministrativeUnit	
> AgreementAcceptance	
> Agreement	
> APIConnectors	
> Application	
> AppRoleAssignment	
> ApprovalRequest	

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:

User.Read	for reading User data for security permissions
User.Read.All	
Mail.Read	read Exchange mail
Mail.ReadBasic.All	
Mail.ReadWrite	

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.


Microsoft Azure
Search resources, services, and docs (G+/)
rock@simsage.co.uk
SIMSAGE
Home > SimSage - App registrations > simsage - API permissions
simsage - API permissions
Search (Ctrl+/)
Overview
Quickstart
Manage
Branding
Authentication
Certificates & secrets
Token configuration (preview)
API permissions
Expose an API
Owners
Roles and administrators (Previ...
Manifest
Support + Troubleshooting
Troubleshooting
New support request
ecrets
Refresh
+ Add a permission
Grant admin consent for SimSage

Successfully granted admin consent for the requested permissions.

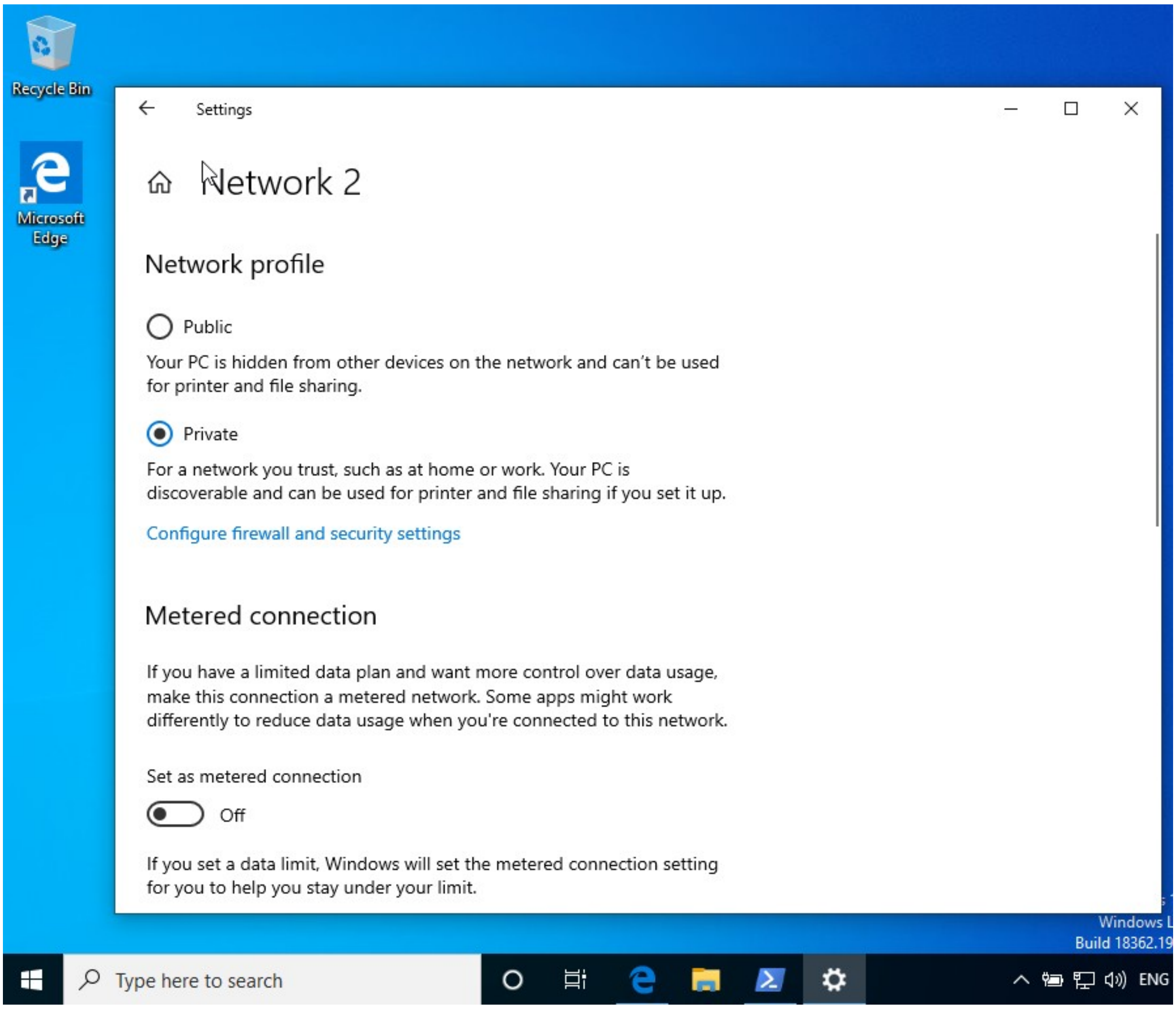
Configured permissions

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 Requir...	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

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.



Network 2

Network profile

○ Public

Your PC is hidden from other devices on the network and can't be used for printer and file sharing.

● Private

For a network you trust, such as at home or work. Your PC is discoverable and can be used for printer and file sharing if you set it up.

Configure firewall and security settings

Metered connection

If you have a limited data plan and want more control over data usage, make this connection a metered network. Some apps might work differently to reduce data usage when you're connected to this network.

Set as metered connection

Off

If you set a data limit, Windows will set the metered connection setting for you to help you stay under your limit.

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
```