



Exchange365 Crawler Setup

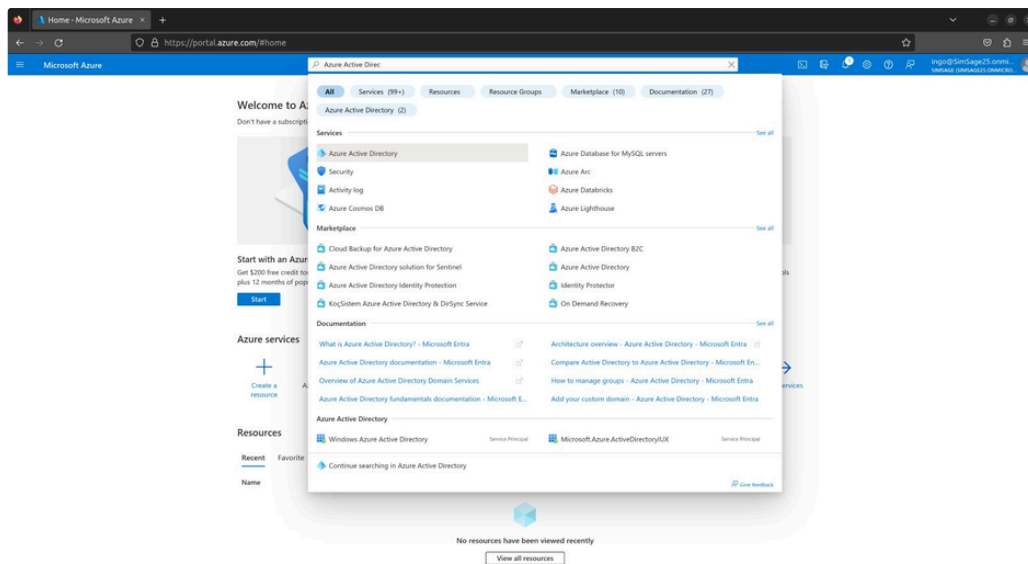
Introduction

Introduction

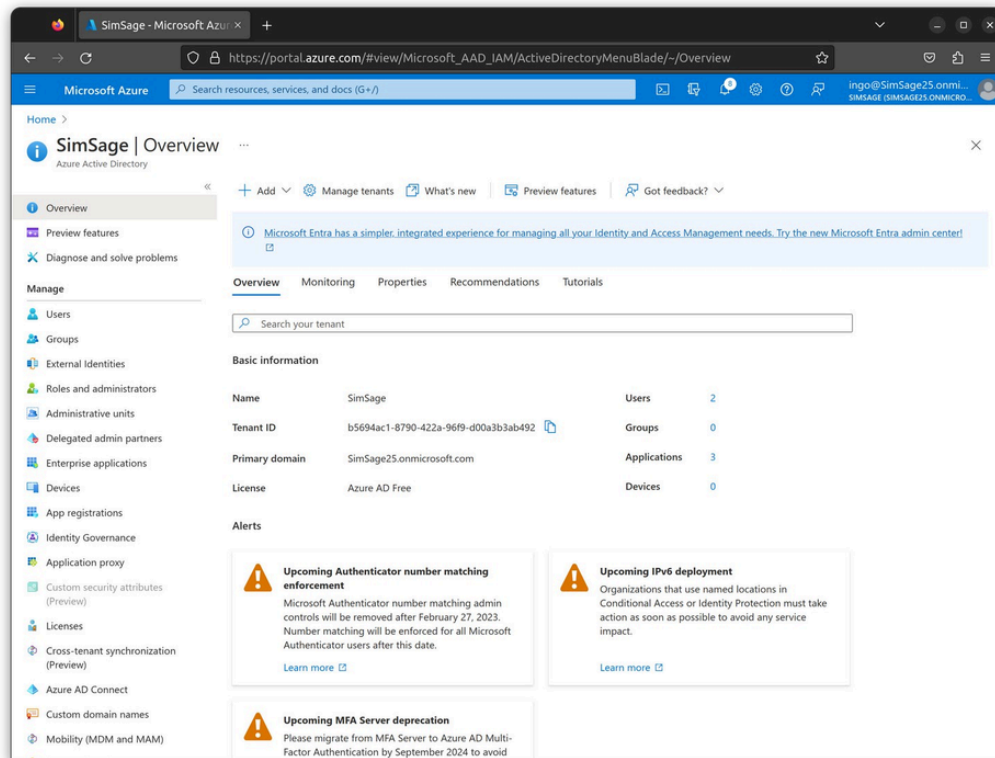
This is a short guide aimed at showing how to configure Microsoft Azure to enable the SimSage Exchange 365 crawler.

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

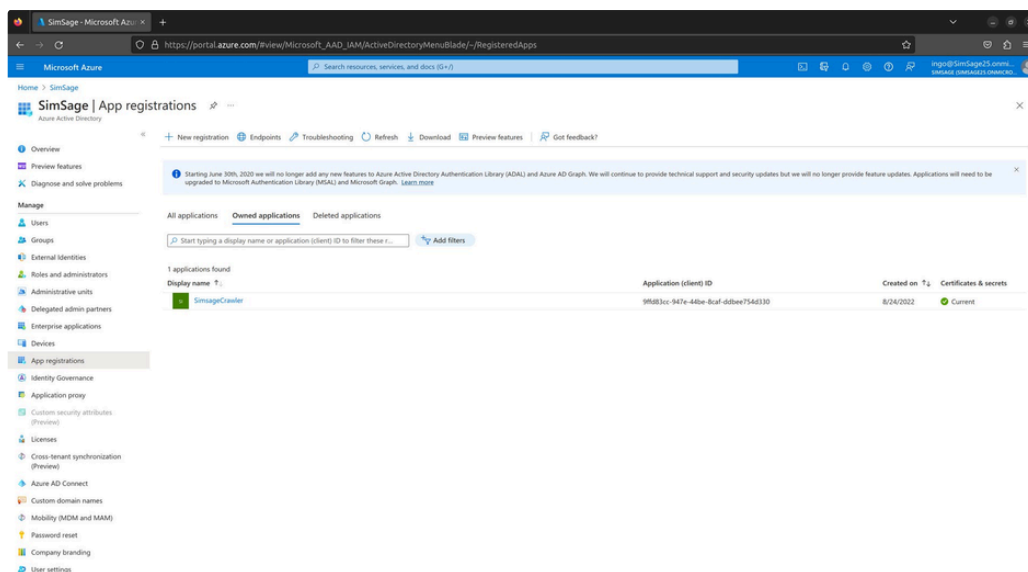
[Microsoft Azure](#) Search for “Azure Active Directory” and select it.



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.

 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 >

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

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

+ 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](#)

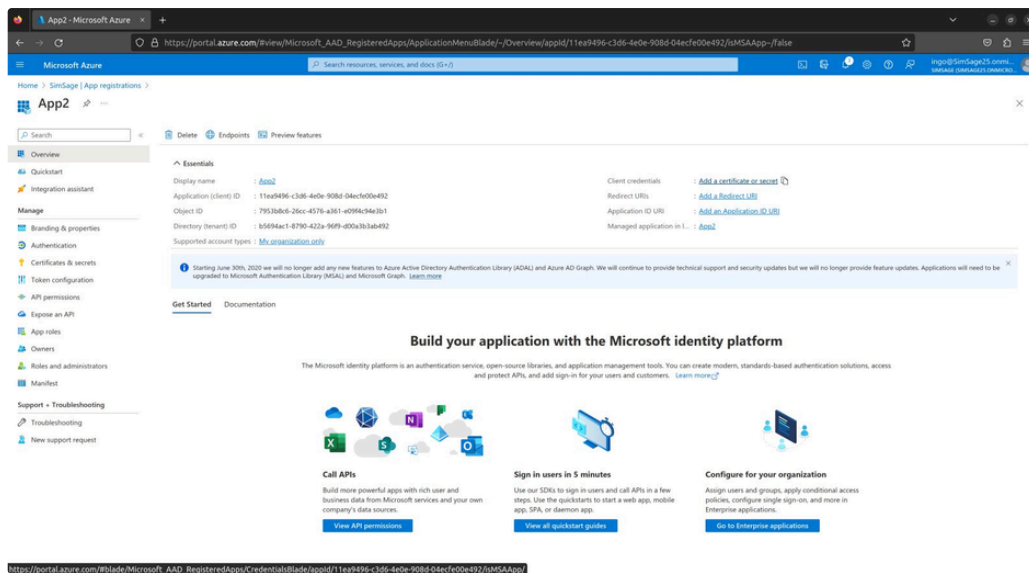
All applications Owned applications Deleted applications (Preview)

Start typing a name or Application ID to filter these results

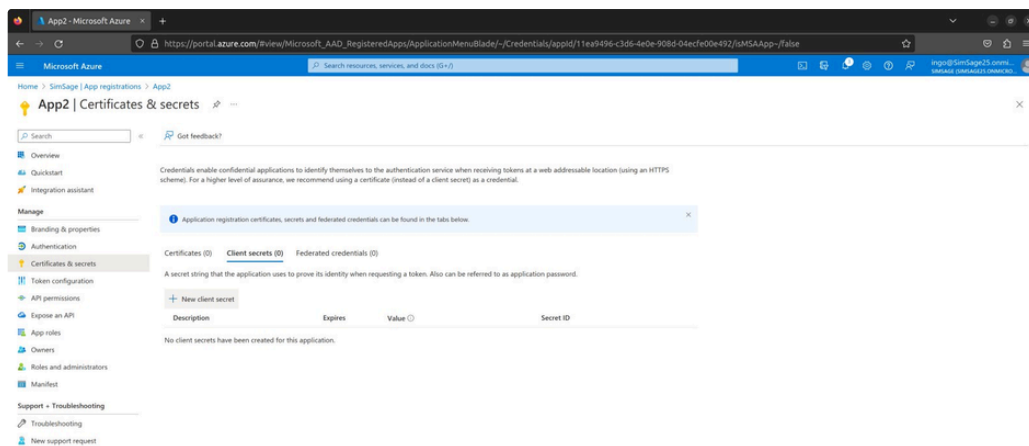
Display name	Application (client) ID	Created on	Certificates & secrets
simsage-app	11656971-7c2f-4faa-99c2-53253a4edd7a	3/22/2021	Current

this is your Client ID for SimSage, copy it.

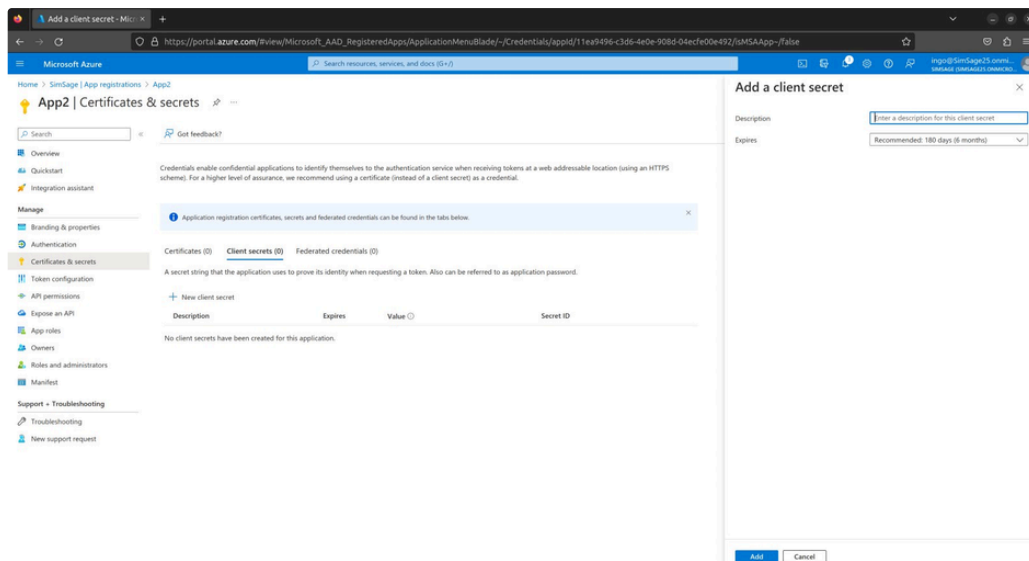
Next, we will need to add a secret to the application. Click on the application and select "Add a Certificate or secret" in the following screen:




Select Client secrets and press “+ New client secret”



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

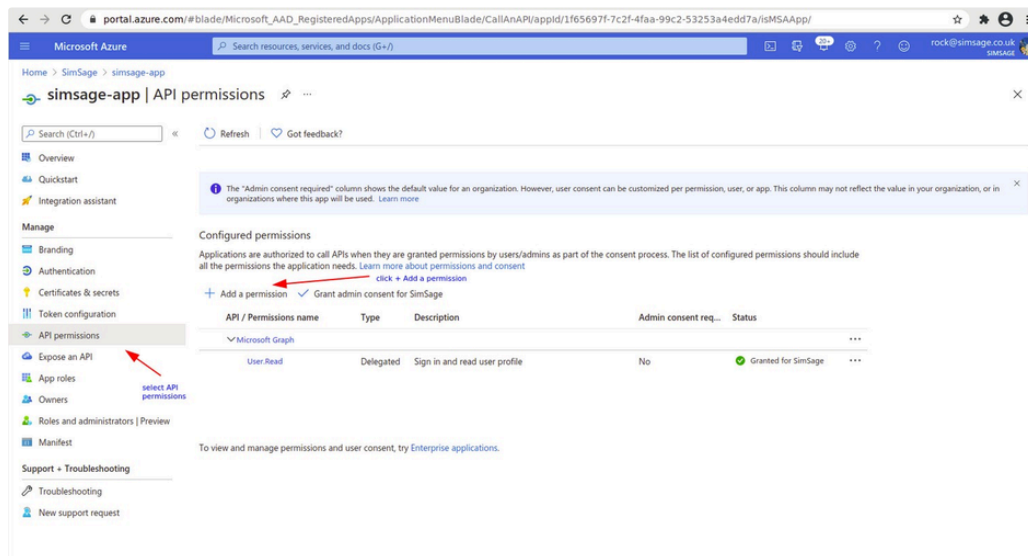


Copy the secret and keep it safe for the crawler configuration.

 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.

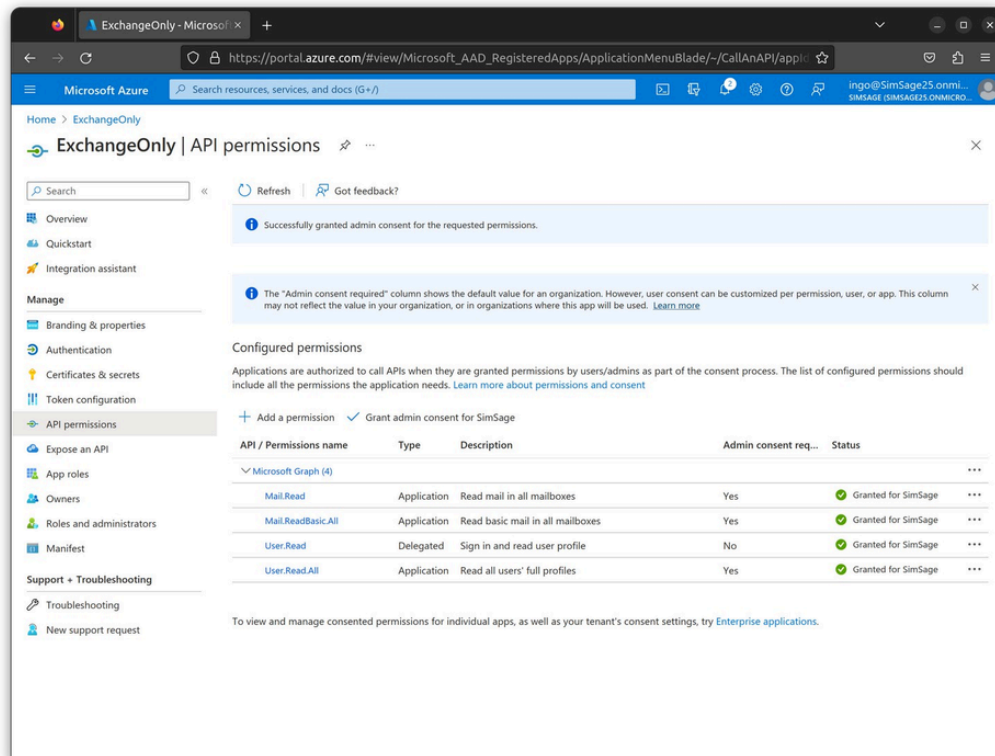


Select “Microsoft Graph” and select “Application permissions”. Then start typing in the “Select permissions” text box.

You need to select the following permissions:

- Mail.Read
- Mail.ReadBasic.All
- User.Read
- User.ReadAll

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 Exchange 365 crawler and on the "exchange 365 crawler" page add the following values:

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

Redirect Url: Add a random value to pass validation, will remove this box

Press save