Microsoft 365 Mail Configuration (OAuth Server)

October 2022

Table of Contents

1 About this Document

This document is for administrators who want to use OAuth Server authentication when fetching email and gives an example configuration of the Microsoft 365 server. Since the procedure may change you should always check the official Microsoft documentation.

The MS365 mail configuration consists of two parts:

1. Mail server (application registration)
2. Mailbox creation.

2 Mail Server Configuration

To configure MS365 as mail server, System Configurator configuration requires *Application registration ID*. Follow the steps below to register application at Azure Active Directory (AD).

2.1 Registration

Register the application with your Azure Active Directory tenant. Some registration is required for Microsoft to act as an authority for your application.

2.2 Configuration

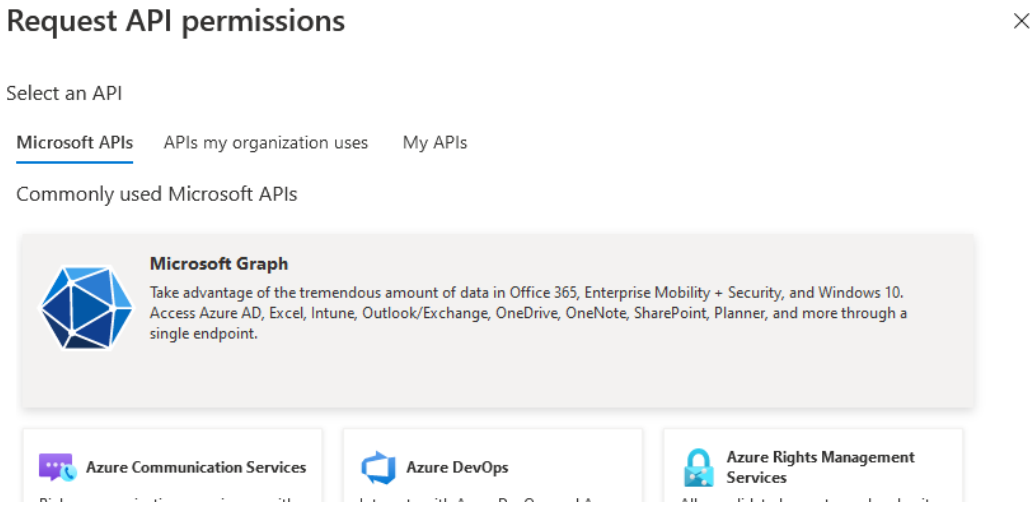
1. Choose the Azure AD tenant where you want to create your applications.
2. Sign in to the Azure portal.

   If your account is present in more than one Azure AD tenant, select *Directory* + *Subscription*, which is an icon of a notebook with a filter next to the alert icon, and switch your portal session to the desired Azure AD tenant.
3. Select *Manage Azure Active Directory*.
4. Select *App registrations* from the new navigation blade.
5. Register the client app:
   1. In the *App registrations* page, select *+New registration*.
   2. When the *Register an application page* appears, enter your application's registration information:

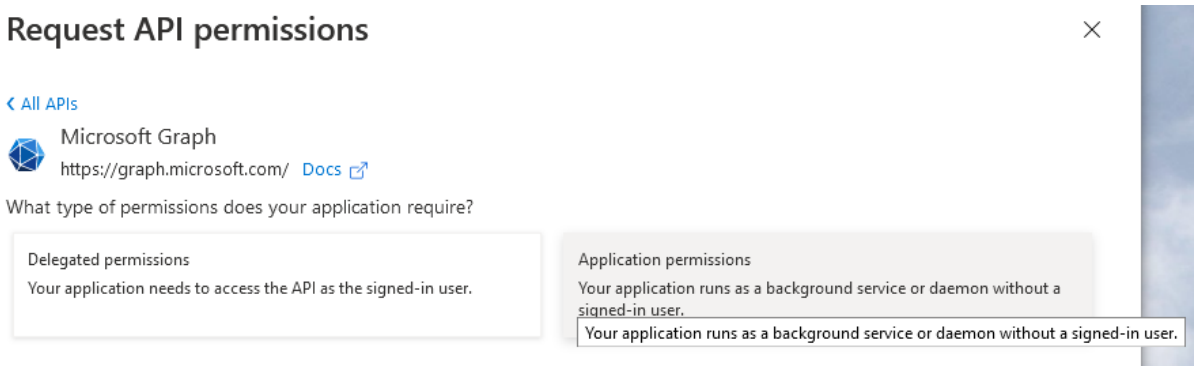
      - In the *Name* section, enter a meaningful application name. This is not used in System Configurator.
      - In the *Supported account types* section, select an option that suits your purposes.
      - No need to specify *Redirect URI* since it is not used in this case.
6. Select *Register* to create the application.
7. On the app *Overview* page, find the Application (client) ID value and copy it.
8. On the app *Overview* page, find the Directory (tenant) ID value and copy it.

9. Click *View API permissions* button or *API permissions* left navigation item

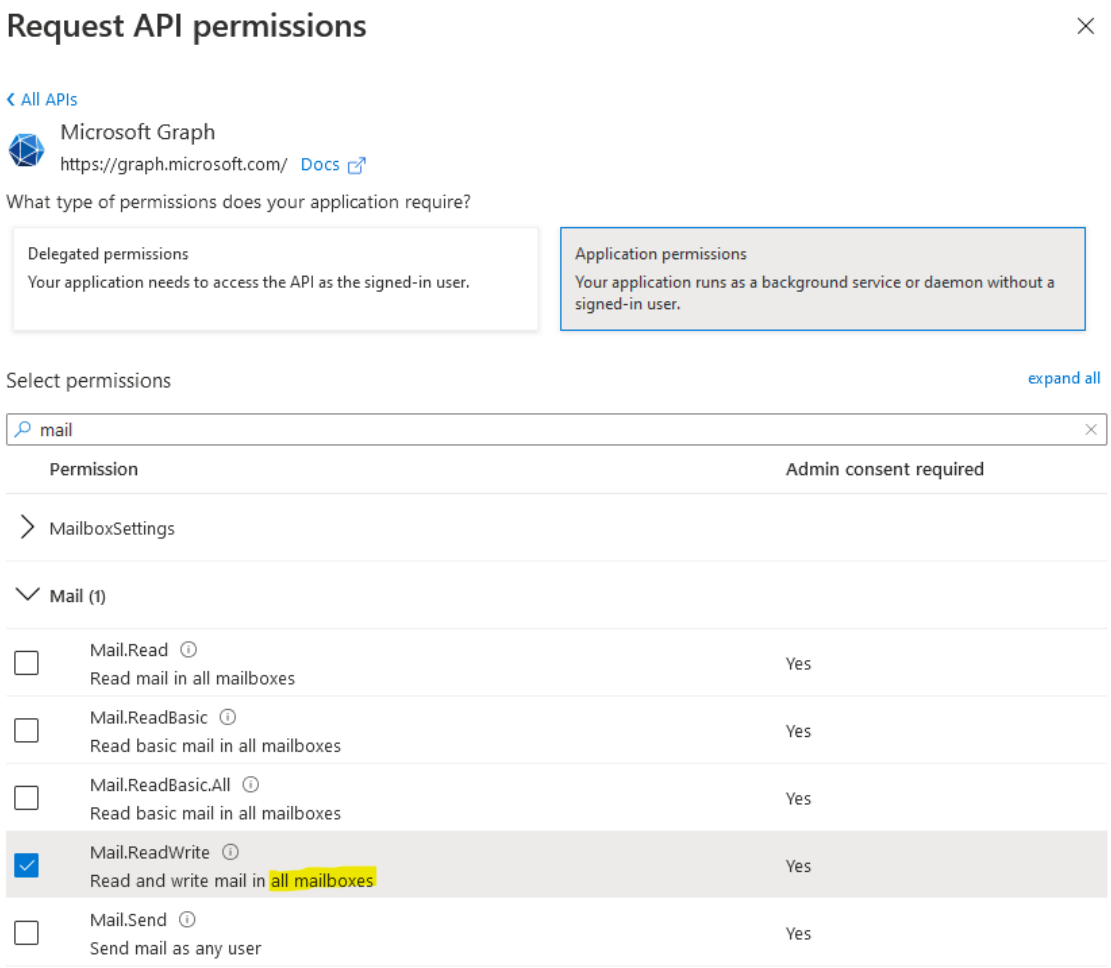
    1. Click the *Add a permission* button and then ensure that the *Microsoft APIs* tab is selected (by default, it is selected).
    2. In the *Commonly used Microsoft APIs* section, click on the *Microsoft Graph*.



    3. In the ***Application*** *permissions* section,



    ensure that the right permissions are checked: *Mail.ReadWrite*. (*Mail.Send* if you are going to use MS365 as an outgoing mail server.) Use the search box if necessary.



NOTE Pay attention to the text describing permission *Mail.ReadWrite - Read and write mail in **all** mailboxes*. These are very powerful permissions. The section Granting Permissions to Access Mailboxes tells how to limit application access to specified mailboxes.

4. Select the *Add permissions* button. Permissions are now assigned correctly but the client app does not allow interaction. Therefore, no consent can be presented via a user interface and accepted to use the service.
5. Click the *Grant/revoke admin consent for [tenant]* button, and then select *Yes* when you are asked if you want to grant consent for the requested permissions for all accounts in the tenant. You need to be an Azure AD tenant admin to do this.

10. In the left navigation pane, select *Certificates & secrets*.

11. Add the application password. The Sinch Contact Pro application will use this password to authenticate and request OAuth token at the MS365 Mail Server.

1. Click *New client secret*.
2. Specify *Description*. This is not used by Sinch Contact Pro.
3. Select expiration. If you choose a secret that expires in the future, you must repeat these steps when the secret expires.
4. You will be shown an *ID* and *value*. Copy the value field. You will not be able to retrieve it in the future. You get more information from the information message at the top of the page.

Azure AD configuration is completed.

3 Mailbox Configuration

1. Open Microsoft 365 admin center https://admin.microsoft.com/Adminportal/Home#/homepage.
2. Select *Groups* > *Shared mailboxes*.
3. Select *Add a shared mailbox*.
4. Enter name and email.
5. Copy name value. It will be used to add email address to the queue.

NOTE Full email address of the shared mailbox will be used as a queue address.

---

6. Select *Next*.
7. Click *Next* and *Finish*.

In System Configurator, you need to configure email settings and an email queue. For more information, see the section *Configuring OAuth Authentication for Microsoft 365* in Sinch Contact Pro System Configurator documentation.

3.1 Granting Permissions to Access Mailboxes

If no additional actions are performed, the registered application you created has access to every mailbox. To restrict the access to certain mailboxes only, follow the procedure below.

When you open the Microsoft 365 admin center, the left navigation pane may show a limited number of items. When you click *… Show all*, you will get access to every application in Microsoft 365. Use Exchange admin center to create a security group and grant authorization to the security group to access shared mailboxes. In next phase you will assign security group to application registration.

1. Open Exchange admin center https://admin.exchange.microsoft.com/#/homepage
2. Select *Groups* in the left navigation pane.

3. Click on *Add a group* in the top bar.
4. Choose *Mail-enabled security*.
5. Click *Next* and enter a group name and description.
6. Click *Next* and specify an email address. This will be used when granting application permission to the security group.
7. Click *Next* and *Finish*.

Now add shared mailboxes to which the security group will have access. Add all mailboxes that will be used by Sinch Contact Pro.

1. Select the security group you created.
2. On the right pane where group detailed info is shown, select the tab *Members*.
3. Click on *View all and manage members*. The right pane shows group members. Search for the mailbox you would like to add.
4. When all mailboxes are added, click on *Save changes*.
5. Assign the security group to the application registration. This is described in the Microsoft document Scoping application permissions to specific Exchange Online mailboxes.
6. To configure the application policy, see the Microsoft document https://docs.microsoft.com/en-us/graph/auth-limit-mailbox-access#configureapplicationaccesspolicy. You need to execute the following command:

```
New-ApplicationAccessPolicy `
    -AppId "e7e4dbfc-046f-4074-9b3b2ae8f144f59b" `
    -PolicyScopeGroupId "cctr_sec_group@your_tenant.com" `
    -AccessRight RestrictAccess `
    -Description "Restrict this app to members of distribution group cctr_sec_group@your_tenant.com";
```

The `AppId` is the ID or the application registration you created and the `PolicyScopeGroupId` is the email address of the security group. For more information about this command and its possible side effects, see

https://learn.microsoft.com/en-us/powershell/module/exchange/new-applicationaccesspolicy?view=exchange-ps.