Microsoft 365 Mail Configuration (OAuth User)

June 2022

Table of Contents

1 About this Document

This document is for administrators who want to use OAuth User 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.
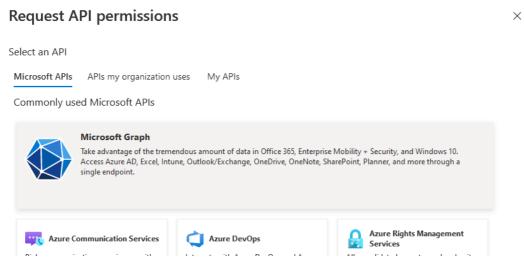
3. Select Manage Azure Active Directory.
4. Select *App registrations* from the new navigation blade.
5. Register the client app:

    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 any option.

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. Go to Advanced settings and set Allow public client flows to Yes and then save.

> **NOTE** If this is not available on the user interface, complete other steps, register application and select registered application to see details. On the left navigation bar, select section *Authentication* and in *Advanced settings* section choose *Treat application as a public client*. By default, *No* is selected. Select *Yes* and click *Save*.

10. In the list of pages for the app, select *View API permissions*:

   1. Click the *Add a permission* button and then ensure that the *Microsoft APIs* tab is selected.

   2. In the Commonly used Microsoft APIs section, click on the Microsoft Graph.

   3. In the *Delegated permissions* section, ensure that the right permissions are checked: *User.Read*, *User.ReadBasic.All*, *Mail.Mail.ReadWrite*. Use the search box if necessary.

Request API permissions

✕

‹ All APIs

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

What type of permissions does your application require?

Delegated permissions	Application permissions
Your application needs to access the API as the signed-in user.	Your application runs as a background service or daemon without a signed-in user.

Select permissions   expand all

🔍 mail   ✕

ℹ 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   ✕

Permission	Admin consent required
› OpenId permissions	
› MailboxSettings	
˅ **Mail (1)**	
☐ Mail.Read ⓘ Read user mail	No
☐ Mail.Read.Shared ⓘ Read user and shared mail	No
☐ Mail.ReadBasic ⓘ Read user basic mail	No
☑ Mail.ReadWrite ⓘ Read and write access to user mail	No
☐ Mail.ReadWrite.Shared ⓘ Read and write user and shared mail	No
☐ Mail.Send ⓘ Send mail as a user	No

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.

Azure AD configuration is completed.

3 Mailbox Configuration

1. Open Microsoft 365 admin center
   https://admin.microsoft.com/Adminportal/Home#/homepage.
2. Select *Users > Active users*.
3. Select *Add a user*.
4. Enter user details.
5. Copy username value. It will be used to add an email address to the queue.

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

---

6. Select *Next*.
7. Assign application Office for the Web.
8. 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.