Mailit: OAuth for Microsoft Graph (Application) — Shared Mailbox — Quick Start

Mailit Documentation

Version for Mailit 11

1 OAuth for Microsoft Graph (Application) — Shared Mailbox

This guide explains how to access a shared mailbox using Microsoft Graph and Application permissions, without interactive user login. This setup requires administrator access.

Step 1: Prepare your account (Administrator)

You are performing this setup as a Microsoft 365 administrator. Application permissions grant access to all mailboxes in the tenant. To restrict access to a specific shared mailbox, you must configure Exchange Application RBAC (Resource Scoping) in Exchange Online.

Step 2: Register the application

- Sign in to the Microsoft Entra admin center as an administrator.
- Create a **New registration**.
- **Name:** `Mailit Service`.
- **Supported account types: Accounts in this organizational directory only** (Single tenant).
- **Redirect URI:** Leave blank.

Copy the **Application (client) ID** and **Directory (tenant) ID**. Go to **Certificates & secrets** and create a new **Client Secret**. Copy the secret value immediately.

Step 3: Add application permissions

Go to **API permissions** → **Microsoft Graph** → **Application permissions**. Add `Mail.Read`, `Mail.ReadWrite`, and `Mail.Send`. Click **Grant admin consent**.

Step 4: Configure OAuth in Mailit

Open `Simple Receiving.fmp12`, select **graphRest**, and choose **OAuth**.

- Select the `Microsoft Graph (Application)` preset.
- Enter the Application (client) ID and the Client Secret Value.
- On the **Additional Settings** tab, replace `{tenant}` with your Directory (tenant) ID in both URLs.
- Enter the **shared mailbox email address** in **User Name**.

Step 5: Test receiving and sending

Ensure the **Mailit Assets** folder is installed. No browser login is required; the application authenticates directly. Click **Test Connection** and **Get Mail**. To send, use the same configuration in your sending script.

If something goes wrong

If you encounter an error, check the following common issues:

- `AADSTS50011` — Redirect URI mismatch. Ensure it is exactly `http://localhost:1234/oauth/` and has a trailing slash.
- `invalid_scope` — Scopes in Mailit do not match the permissions in Microsoft Entra. Check against section 4.4.
- `invalid_grant` — Refresh token revoked or expired. Re-authorize via the browser.
- `invalid_client` — Client Secret issue. Check the secret value and `OAuth Add Secret To Request` setting.
- `localhost` unreachable — Check that the Mailit Assets folder is installed, port 1234 is free, and FileMaker is running.
- `unauthorized_client` — Check that the app is registered as Single tenant and admin consent has been granted.

For more details, refer to **section 15 (Troubleshooting)** in the Microsoft manual.