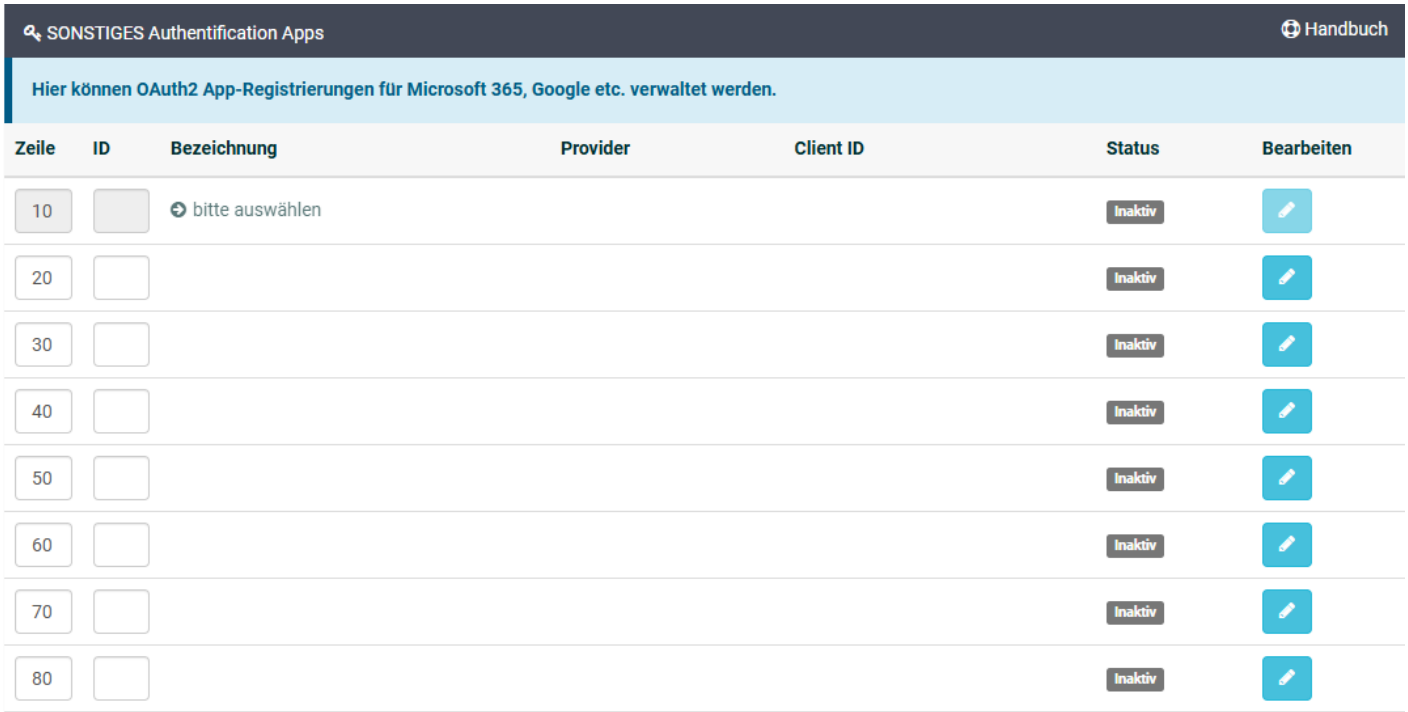
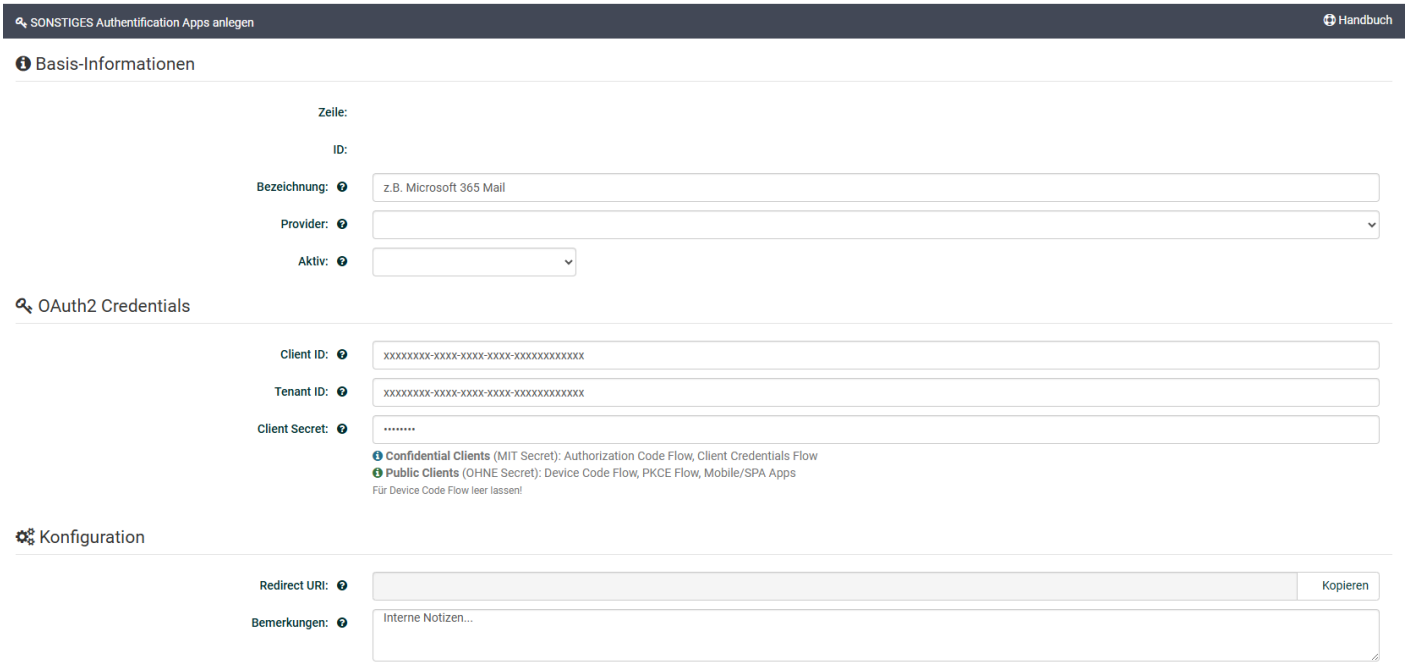
OAuth2 / Microsoft 365 E-Mail-Authentifizierung

Obility unterstützt nun die Authentifizierung für den E-Mail-Versand über OAuth2 mit Microsoft 365. Die App-Konfiguration erfolgt in der Tabelle "auth_apps", die sowohl für Mailaccounts zum Versenden in der Tabelle "smtp", wie auch für Mailaccounts zum Mail-Import "mail_archiv" genutzt werden können.



In der Tabelle "auth_apps", können über den Stift-Button auf der rechten Seite neue Apps registriert werden.



Wählen Sie als Provider "Microsoft" aus und aktivieren sie die App. Sie benötigen aus Ihrer Tenant-Konfiguration die **Client ID** und die **Tenant ID (GUID)**. Das Client Secret wird für den **Device Code Flow nicht benötigt** – dieses Feld kann leer bleiben.

Kurz-Anleitung für den Microsoft-Tenant:

1. Azure-Portal (App-Registrierung & Berechtigungen):
- Weg: Azure-Portal ? Microsoft Entra ID ? App-Registrierungen ? Neue Registrierung (oder bestehende wählen) ? API-Berechtigungen ? Berechtigung hinzufügen.
- API wählen: Reiter Von meiner Organisation verwendete APIs ? Suche nach Office 365 Exchange Online ? Anwendungsberechtigungen auswählen.
- Berechtigungen: Setze die Haken bei SMTP.Send (für Versand) und POP.AccessAsApp (für Abruf).
- Admin-Zustimmung: Klicke zwingend auf den Button Administratorzustimmung für [Tenant-Name] erteilen, da die App sonst keine Rechte erhält.

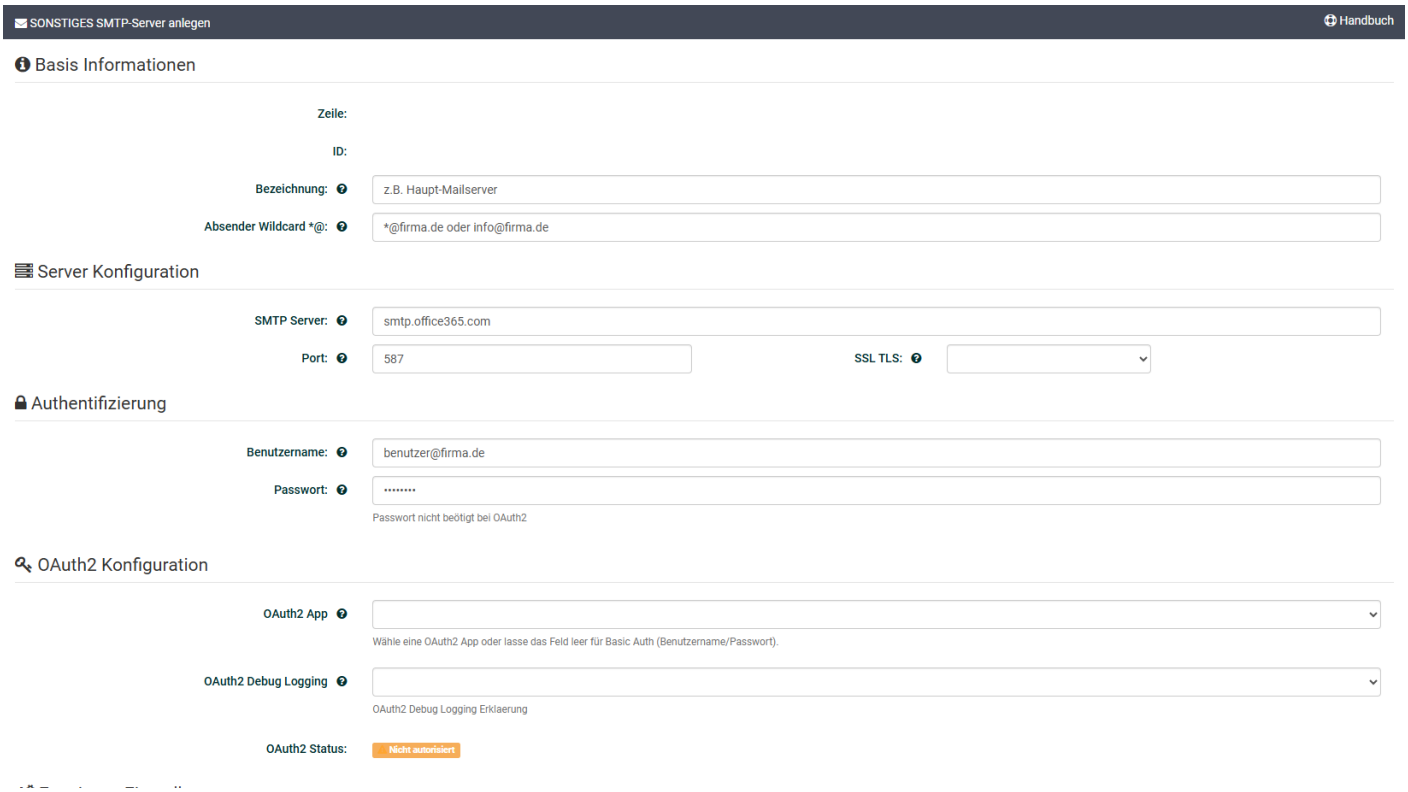
2. Microsoft Entra Admin Center (Öffentliche Clientflows / Device Code Flow aktivieren):
- Im Microsoft Entra Admin Center (entra.microsoft.com) einloggen.
- Links im Menü auf **„App-Registrierungen"** klicken.
- Über der Liste den Filter-Tab von **„Anwendungen mit Besitzer"** auf **„Alle Anwendungen"** ändern.
- Die erstellte App für die OAuth2-Verbindung mit Obility suchen und per Klick öffnen.
- Im linken Bereich auf **„Authentication"** klicken (manchmal mit dem Zusatz „Preview").
- In den Tabs über der Liste von **„Umleitungs-URI-Konfiguration"** auf **„Einstellungen"** wechseln.
- Den Schiebeschalter unter der Überschrift **„Öffentliche Clientflows zulassen"** auf **„Aktiviert"** stellen.
- Die Einstellungen mit dem Speichern-Button unten auf der Seite sichern.
- Hinweis: Bei aktiviertem Device Code Flow wird **kein Client Secret** benötigt. Die App gilt als Public Client.

3. M365 Admin-Center (Postfach-Protokolle freischalten):
- Weg: Microsoft 365 Admin Center ? Benutzer ? Aktive Benutzer ? Auf den jeweiligen Benutzer klicken.
- Aktivierung: Reiter E-Mail ? Klick auf E-Mail-Apps verwalten.
- Setze die Häkchen bei Authentifiziertes SMTP und POP ? Änderungen speichern.

Da sich die Admin-Center und Masken bei Microsoft ändern können, ist dies nur eine grundlegende Info.

Nach erfolgreicher Einrichtung wird in der Übersicht die App auch als "aktiv" angezeigt.

Weiter geht es in der SMTP bzw. Mail-Archiv Tabelle. Da beide Tabellen identisch einzurichten sind, gehen wir exemplarisch die Schritte in der SMTP-Tabelle einmal durch.



Hier können mehrere Mail-Konten eingetragen werden. Die Bezeichnung ist frei wählbar.
Das Feld "Absender Wildcard *@" wird genutzt, um für das Versenden von Mail, das jeweils korrekte Mail-Konto zu identifizieren. Möchten Sie z.B. dass die Mails vom Anwender Max Mustermann mit seinem eigenen Mail-Konto gesendet werden, muss z.B. ein Eintrag "max.mustermann@ihre-domain.de" vorhanden sein. Ein Eintrag "*@ihre-domain.de" würde alle Mails mit dem Absender der Domain über dieses eine Konto senden. Dabei ist die Reihenfolge in der Tabelle wichtig. Möchten Sie einige persönliche Mail-Konten einrichten und auch ein Sammel-Mail-Konto, dann müssen die persönlichen Mail-Konten zuerst in der Tabelle sein (oben). Achten Sie außerdem bei der Nutzung von Wildcard-/Sammel-Mail-Konten auf die korrekte Einstellung im Tenant, damit die Mails auch akzeptiert werden vom Mail-Server.

Die Einträge für den Mail-Server, Ports und die Verschlüsselung sind für Microsoft-Konten soweit immer identisch.

Wählen Sie unten in der Maske die entsprechende App aus, die zur Authentifizierung genutzt werden soll. Ebenfalls können Sie ein erweitertes Logging aktivieren, dann wird der gesamte Austausch festgehalten, ohne Aktivierung werden nur Fehler festgehalten.

> Aus Sicherheitsgründen kann es durchaus Sinn machen, getrennte Apps im Tenant anzulegen, je nach Sende- oder Empfangsberechtigung. Dann muss auch darauf geachtet werden, dass in den Obility Tabellen die jeweils korrekte App gewählt wurde.

Revision #4
Created 2026-03-20 05:58:07 UTC by Marcus Silber
Updated 2026-07-24 13:37:54 UTC by Patrick Mallmann