

Anleitung Microsoft Exchange Konfiguration OAuth

1. Vorbemerkung

Microsoft hat zum 01.01.2023 die Standardauthentifizierung in Exchange Produkten deaktiviert und lässt ab sofort nur noch die moderne Authentifizierung zu. Folgend wird erklärt welche Schritte unternommen werden müssen, um weiterhin mit OpenHearts E-Mails Senden und Empfangen zu können.

2. App-Registrierung für OpenHearts

Die Anwendung OpenHearts muss in Microsoft Exchange registriert werden. Gehen Sie hierzu bitte wie folgt vor. Ausgangspunkt für die folgenden Schritte ist jeweils die Seite <https://portal.azure.com>. Melden Sie sich hier mit einem Konto mit ausreichenden Rechten an.

APP-REGISTRIERUNG FÜR OPENHEARTS ANLEGEN

- Klicken Sie auf der linken Seite im Menü auf „Azure Active Directory“
- Klicken Sie auf der linken Seite im Menü auf „App-Registrierungen“
- Klicken Sie auf die Schaltfläche „Neue Registrierung“
 - Vergeben Sie einen Namen, z.B. „OpenHearts Mail“
 - Wählen Sie bei „Umleitungs-URI“ die Plattform „Öffentlicher Client/nativ“ aus und geben daneben <http://localhost> ein
 - Klicken Sie dann auf „Registrieren“

API-BERECHTIGUNGEN DER APP-REGISTRIERUNG FÜR OPENHEARTS KONFIGURIEREN

- Klicken Sie auf der linken Seite im Menü auf „Azure Active Directory“
- Klicken Sie auf der linken Seite im Menü auf „App-Registrierungen“
- Wählen Sie die App-Registrierung „OpenHearts Mail“ aus
- Klicken Sie auf der linken Seite im Menü auf „API-Berechtigungen“
- Klicken Sie dann auf „Berechtigung hinzufügen“
- Klicken Sie auf der rechten Seite unter „Microsoft APIs“ auf „Microsoft Graph“
- Klicken Sie auf „Delegierte Berechtigungen“
- Setzen Sie bei mindestens den folgenden Berechtigungen einen Haken
 - offline_access
 - email
 - IMAP.AccessAsUser.All
 - SMTP.Send
 - User.Read
- Übernehmen Sie die Änderungen mit einem Klick auf „Berechtigungen hinzufügen“
- Klicken Sie außerdem in der Übersicht zu den Berechtigungen auf „Administratorzustimmung erteilen“

FÜR OPENHEARTS BENÖTIGTE FELDER HERAUSFINDEN

Diese Felder werden in OpenHearts unter Verwaltung → Benutzereinstellungen → E-Mail-Konto benötigt, um ein gültiges Token anfordern zu können.

ANWENDUNGS-ID (CLIENT-ID) HERAUSFINDEN

- Klicken Sie auf der linken Seite im Menü auf „Azure Active Directory“
- Klicken Sie auf der linken Seite im Menü auf „App-Registrierungen“
- Hier finden Sie neben dem Eintrag „OpenHearts Mail“ die Anwendungs-ID

MANDANTEN-ID (TENANT-ID) HERAUSFINDEN

- Klicken Sie auf der linken Seite im Menü auf „Azure Active Directory“
- Klicken Sie auf der linken Seite im Menü auf „Eigenschaften“
- Hier finden Sie die Mandanten-ID

3. SMTP AUTH, moderne Authentifizierung und TLS

Die Anwendung OpenHearts benötigt SMTP AUTH für den Versand von E-Mails. Weiterhin muss in Microsoft Exchange gegebenenfalls die moderne Authentifizierung aktiviert werden. Gehen Sie hierzu bitte wie folgt vor. Ausgangspunkt für die folgenden Schritte ist jeweils die Seite <https://admin.microsoft.com/>. Melden Sie sich hier mit einem Konto mit ausreichenden Rechten an.

SMTP-AUTH FÜR EXCHANGE-BENUTZER AKTIVIEREN

- Klicken Sie auf der linken Seite auf „Benutzer“
- Klicken Sie auf der linken Seite auf „Aktive Benutzer“
- Klicken Sie auf den jeweiligen Benutzer
- Wählen Sie den Reiter „E-Mail“ aus
- Klicken Sie auf „E-Mail-Apps verwalten“
- Aktivieren Sie den Haken „Authentifiziertes SMTP“
- Klicken Sie auf „Änderungen speichern“

MODERNE AUTHENTIFIZIERUNG AKTIVIEREN

- Klicken Sie auf der linken Seite auf „Alle anzeigen“
- Klicken Sie auf der linken Seite auf „Einstellungen“
- Klicken Sie auf der linken Seite auf „Einstellungen der Organisation“
- Wählen Sie den Punkt „Moderne Authentifizierung“ aus
- Aktivieren Sie den Haken „Moderne Authentifizierung einschalten“

TLS AUF CLIENTS UND SERVER ABSICHERN

Auf den Clients, auf denen OpenHearts installiert ist, sowie auf dem Server, auf dem OpenHearts im IIS gehostet wird, müssen die unsicheren Protokolle TLS 1.0 und TLS 1.1 deaktiviert werden und mindestens TLS 1.2 aktiviert werden. Das Vorgehen wird unter folgendem Link beschrieben:

<https://learn.microsoft.com/de-de/windows-server/identity/ad-fs/operations/manage-ssl-protocols-in-ad-fs>