Flowfact Mail OAuth Einrichtung

<u>Inhalt</u>

Einleitung	1
1 Systemvoraussetzungen	1
2 Registrierung des Flowfact Maildienstes in AzureActiveDirectory	2
2.1 Anmelden im Azure Portal	2
2.2 Registrieren der Applikation	3
2.3 Einstellen der Umleitungs URI	5
2.4 Einstellen der API Berechtigungen	8
3 Berechtigungen für SMTP Versand überprüfen	<u>9</u>
4 Ermitteln der benötigten IDs	12
5 Administration - OAuth Konfiguration Performer Mail	13
5.1 Administration - Datenverteilung auf gleichartige Konten	18
6 Benutzer - OAuth Konfiguration Performer Mail	21
7 Abschluß	22
8 Danksagung	24

Einleitung

Diese Anleitung erklärt die Vorgehensweise zur Konfiguration des Flowfact Maildienstes zur Anmeldung an Office365 mittels oAuth2, oder der modernen Anmeldung, wie es bei Microsoft heißt.

Voraussetzung ist der administrative Zugriff auf das Office365 Konto und das Vorliegen einer aktuellen Performer-Version.

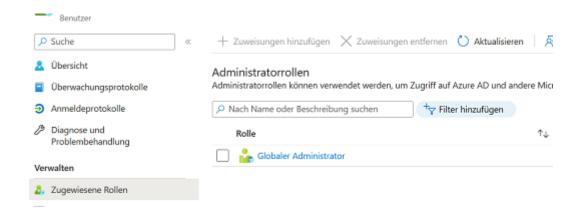
Zudem müssen die unter Punkt 1 aufgelisteten Softwarevoraussetzungen erfüllt sein.

1 Systemvoraussetzungen

Software	Version	Anmerkungen
Microsoft Windows	Ab Windows Server 2012 / Windows 10	Empfohlen
Flowfact Performer CRM	Ab 19.0.1090	Flowfact Performer Neo

2 Registrierung des Flowfact Maildienstes in AzureActiveDirectory

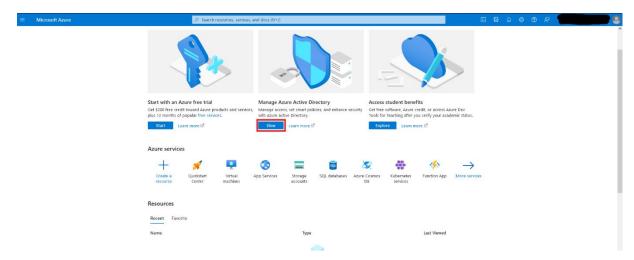
Um den Maildienst mit OAuth nutzen zu können muss die Anwendung zunächst im Azure Active Directory des Office365 Mandanten registriert werden. Hierfür benötigen Sie einen Account mit der zugewiesenen Rolle 'globaler Administrator'.



2.1 Anmelden im Azure Portal

Zur Anmeldung am Portal zur Adresse https://portal.azure.com navigieren und mit dem Administrator Benutzer anmelden.

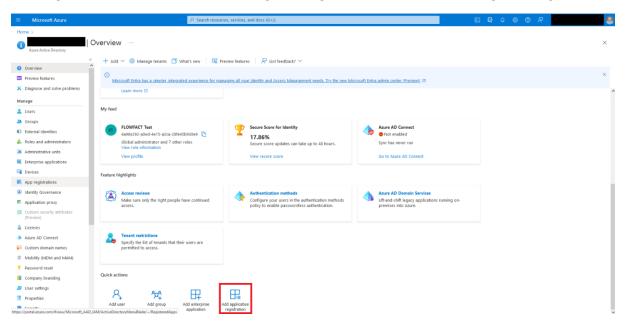
Nach erfolgreicher Anmeldung wechseln wir in die Active Directory Verwaltung.



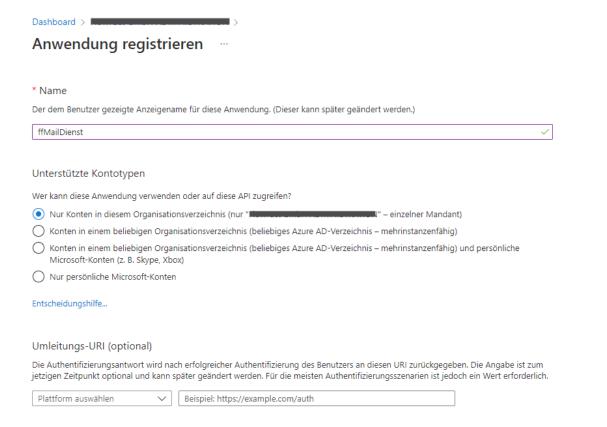
2.2 Registrieren der Applikation

In der Verwaltung scrollen wir ganz nach unten und wählen die Schaltfläche für die Registrierung einer Anwendung.

Achtung! Nicht "Unternehmensanwendung hinzufügen" wählen, sondern die Registrierung.



Auf der folgenden Seite vergeben wir einen beliebigen Namen für die Registrierung des Maildienstes und klicken auf "registrieren".



Indem Sie den Vorgang fortsetzen, stimmen Sie den Microsoft-Plattformrichtlinien zu. 🗗

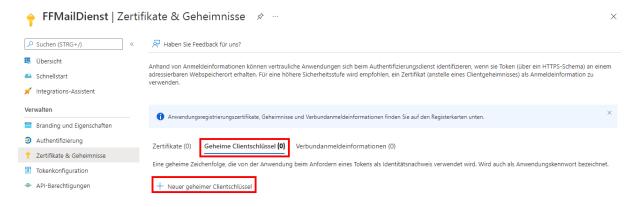
Wählen Sie als unterstützten Kontotyp den ersten Punkt – "Nur Konten in diesem Organisationsverzeichnis" und übernehmen Sie Ihre Änderungen indem Sie den "Registrieren" Button unten links anklicken.

Nun gelangen wir auf die Übersichtsseite der neu erstellten Registrierung.

Als erstes erstellen wir einen geheimen Clientschlüssel / Secret. Dieses wird bei der ersten Anmeldung zum Abrufen eines Access-tokens benötigt.



Erzeugen Sie einen neuen geheimen Clientschlüssel.



Geben Sie eine Beschreibung für dieses Geheimnis ein und eine Gültigkeitsdauer ...



Speichern Sie den <u>Wert</u> des geheimen Client-Secrets an einer sicheren Stelle, da er zu einem späteren Zeitpunkt nicht mehr angezeigt wird.



Gehen Sie wieder in die Übersicht der Registrierung

Als nächstes fügen wir hier die Umleitungs-URI hinzu ...



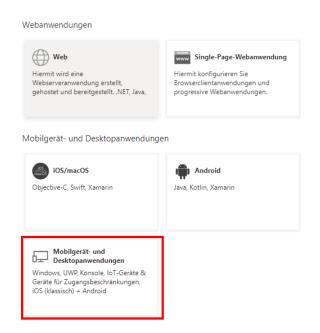
Dies führt uns in die Authentifizierungskonfiguration der Anwendungsregistrierung.

2.3 Einstellen der Umleitungs URI

In der Authentifizierungskonfiguration klicken wir zunächst auf Plattform hinzufügen.



Wir wählen den Eintrag für Mobilgerät- und Desktopanwendungen: Plattformen konfigurieren ×



Als Umleitungs-URI setzen wir den Haken bei dem ersten der drei vorgegebenen Einträge.



Nun können wir die Konfiguration speichern.

Erweiterte Einstellungen

Öffentliche Clientflows zulassen ①

Folgende Mobilgerät- und Desktopflows aktivieren:



- App erfasst Klartextkennwort (Flow f
 ür Kennwortanmeldeinformationen des Ressourcenbesitzers) Weitere Informationen
 ☐
- SSO für in die Domäne eingebundene Windows-Geräte (in Windows integrierter Authentifizierungsflow)
 Weitere Informationen



Nachdem wir gespeichert haben, wählen wir nun den Punkt API Berechtigungen aus der Navigationsleiste am linken Rand.

2.4 Einstellen der API Berechtigungen



Im API Berechtigungsfenster klicken wir zunächst auf Berechtigung hinzufügen. Im Anforderungsfenster für Berechtigungen wählen wir zunächst "Microsoft Graph"



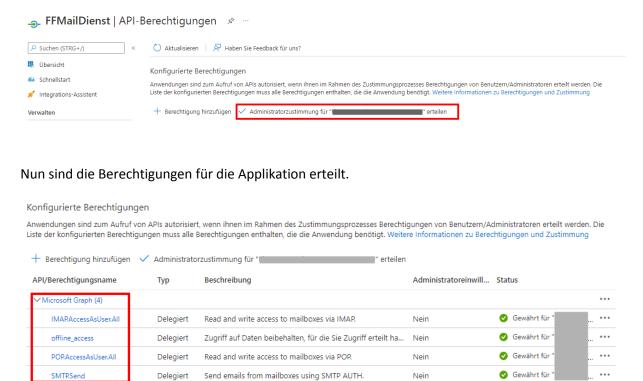
Und anschließend 'Delegierte Berechtigungen' als Art der Berechtigung ..



Folgende Berechtigungen sollten mindestens gesetzt werden:

- IMAP.AccessAsUser.All
- o POP.AccessAsUser.All
- o SMTP.Send
- Offline_Access

Nachdem die Berechtigungen hinzugefügt wurden, müssen für diese nun noch Zustimmungen erteilt werden. Hierzu klicken wir die Schaltfläche *Administratorzustimmung für "Dienstname" erteilen*.



3 Berechtigungen für SMTP Versand überprüfen

Der Maildienst versendet E-Mails per SMTP. Damit dies weiterhin auch mit Exchange Online Konten funktioniert, müssen einige Hürden genommen werden, die Microsoft hier leider aufgestellt hat.

Eine genauere Beschreibung finden Sie zB. hier:

https://docs.microsoft.com/de-de/exchange/clients-and-mobile-in-exchange-online/authenticated-client-smtp-submission

3.1 Organisationsweite Aktivierung SMTP Versand

Dies geschieht im Wesentlichen durch Aktivierung des SMTP-Protokolls, welches entweder für die ganze Organisation oder auch kontospezifisch erfolgen kann.

Leider ist die aktuelle Einstellung für die Organisation nicht ohne weiteres ersichtlich, es ist aber sehr wahrscheinlich, dass diese Einstellung bereits deaktiviert wurde.

Um das SMTP-Protokoll für die Organisation zu aktivieren, müssen Sie in der "Exchange-Online Powershell" den folgenden Befehl eingeben:

Set-TransportConfig -SmtpClientAuthenticationDisabled \$false

Wenn Sie in Ihrer Authentifizierungsrichtlinie die Standardauthentifizierung für SMTP <u>nicht</u> deaktiviert haben, dürfte diese Aktion bereits ausreichen, um mit allen verknüpften Konten E-Mails über den Maildienst zu versenden. Anderenfalls sollten Sie die Richtlinie evtl. anpassen.

3.2 Kontospezifische Aktivierung SMTP Versand

Möchten Sie das SMTP Protokoll *nicht* organisationsweit aktivieren, haben Sie noch die Möglichkeit das Protokoll für bestimmte Konten freizuschalten.

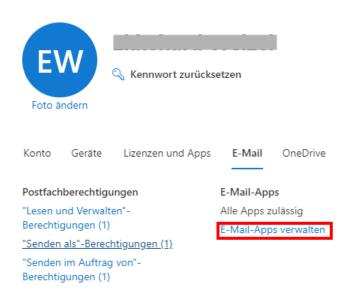
Gehen Sie hierfür in das "Microsoft 365 admin center".

https://portal.azure.com

Wählen Sie jeweils in der Benutzer-Auswahlliste die Benutzer aus, die über den Maildienst E-Mails empfangen bzw. senden möchten. Gehen Sie dann auf den Reiter ,E-Mail' ..

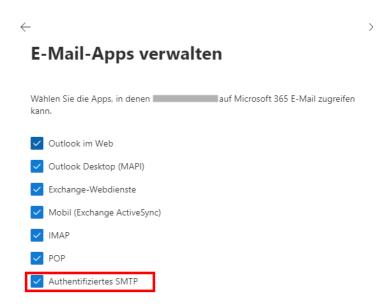


Wählen Sie dort ,E-Mail-Apps verwalten'



Wählen Sie die für diesen Benutzer benötigten Apps – 'Authentifiziertes SMTP' wird dann benötigt, wenn Sie über das Postfach per 'moderne Authentifizierung' E-Mails versenden möchten.

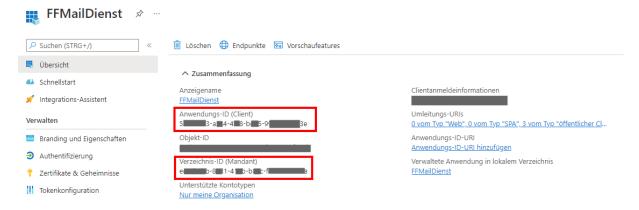
Laut Microsoft überschreibt diese Einstellung die organisationsweite Einstellung für dieses eine Konto.



4 Ermitteln der benötigten IDs

Zur Konfiguration der oAuth Anmeldung im Maildienst benötigen wir 3 Werte aus der Registrierung. Die Mandanten bzw. Tenant ID, die Anwendungs- oder Client-ID sowie den Wert des geheimen Clientschlüssels.

Beide erstgenannten IDs finden wir in der Übersicht für die registrierte Anwendung die zuvor eingerichtet wurde:



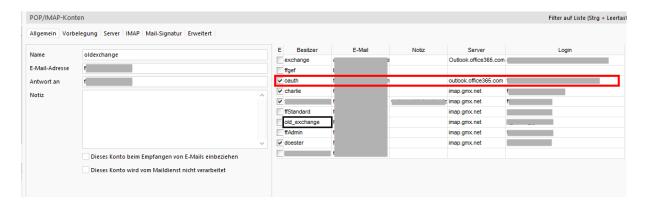
Die Übersicht finden wir in der Verwaltung des Azure Active Directories (s.o.) und dort auf der linken Seite unter dem Punkt App-Registrierungen.

Den geheimen Clientschlüssel hatten wir nach der Erzeugung an einem sicheren Ort zwischengespeichert.

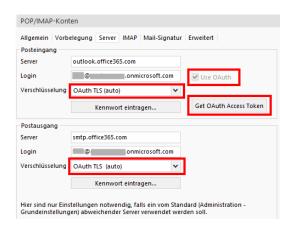
5 Administration - OAuth Konfiguration Performer Mail

Die Konfiguration beginnt im Konto eines Flowfact Performer Benutzers, der auf sein Office365 Konto mittels moderner Authentifizierung zugreifen möchte.

Dies ist im Prinzip für jedes Konto durchzuführen, über welches Mails empfangen bzw. versendet werden soll. Zur Erleichterung bieten wir Funktionen an mit der erforderliche Daten zum Teil auf alle gleichartigen Konten verteilt werden können. Eine Beschreibung dieser Funktionalität erfolgt weiter unten.



Im Bereich Server konfigurieren Sie die Verschlüsselung. Stellen Sie jeweils den Eintrag mit 'OAuth' ein



Speichern Sie Ihre Änderungen.

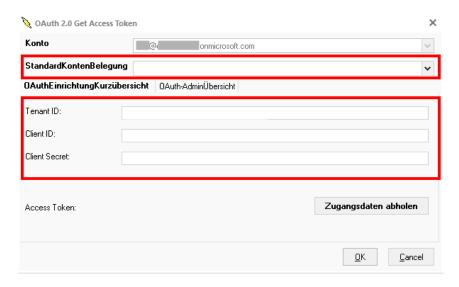
Diese Eingaben führen Sie bitte für alle Konten aus, die ebenfalls ein Office365 Konto nutzen möchten. Also jeweils:

- Konto im Kontenfenster auswählen
- Server und Login überprüfen und ggfls einstellen
- Verschlüsselung für den Empfang und Versand jeweils den 'OAuth' Eintrag wählen
- Und letztendlich speichern

Wir kommen zurück zu unserem anfänglich bearbeiteten Konto:

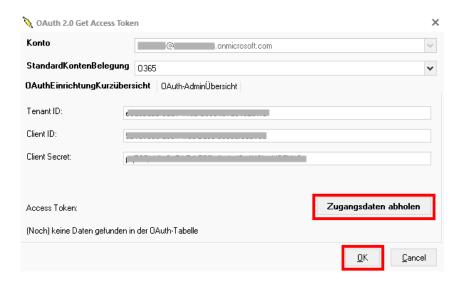
Um weitere Daten für die OAuth Konfiguration eingeben zu können, öffnen wir nun die OAuth - Eingabeform über den Button

,Get OAuth Access Token':



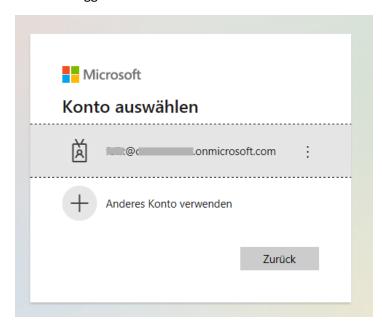
Stellen Sie hier zunächst als Standard-Kontenbelegung "O365" ein und unter dem Reiter OAuthEinrichtungKurzübersicht die bei der Azure – App Registrierung ermittelten Werte für Tenant Id (Mandanten ID), Client ID sowie den Wert des ClientSecrets.

Speichern Sie Ihre Eingaben und öffnen Sie die Form erneut ...

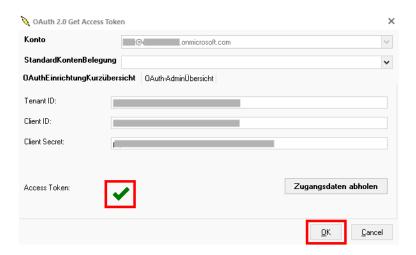


Nachdem Sie gespeichert haben, rufen Sie Ihr Access Token ab (Zugangsdaten abrufen).

Beachten Sie, dass alle Felder gefüllt sind bevor Sie den Access-Code abrufen. Wenn alles korrekt konfiguriert wurde, werden sie auf die Microsoft Seite geleitet, wo Sie sich mit dem zugehörigen Konto einloggen müssen



Wählen Sie das Konto aus und melden Sie sich mit dem entsprechenden Passwort in Ihrem O365 Account an.



Sofern die Anmeldung erfolgreich war, erhalten Sie ein 'Access-Token' (grüner Haken). Speichern Sie dieses mit 'OK' ab.

In der Konten Ansicht können Sie jetzt für das gewählte Konto unter IMAP die im Account verfügbaren Ordner abrufen und ggfls. zuordnen...

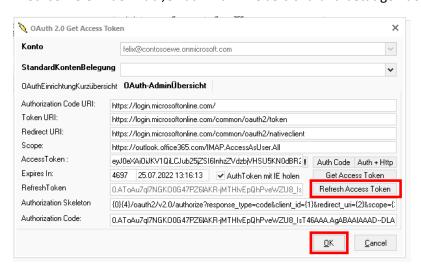


Öffnen Sie den Posteingang des gewählten Kontos. Es erscheint folgende Meldung:

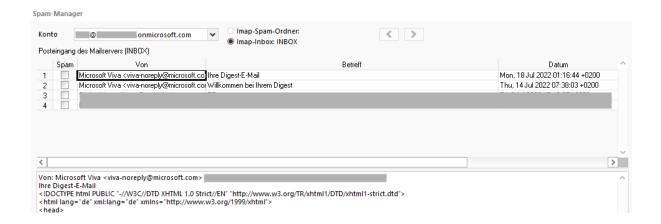


Nach ,ok' erscheint wieder die OAuth Eingabeform.

Wechseln Sie in den Tab ,OAuth- Admin Übersicht' und betätigen dort ,Refresh Access Token'.



Jetzt sollen die E-Mails in dem Postfach angezeigt werden – die Einrichtung ist abgeschlossen.



Die Einrichtung für das erste Konto ist hiermit abgeschlossen.

5.1 Administration - Datenverteilung auf gleichartige Konten

Die Abfrage des Autorisierung-Tokens und die damit verbundene Freigabe des Verfahrens auf Microsoftseite muss leider für jeden einzelnen Benutzer einzeln durchgeführt werden. Dies bedeutet jeder einzelne Anwender muss sich über die Microsoft Seite anfänglich in seinem O365 Account anmelden.

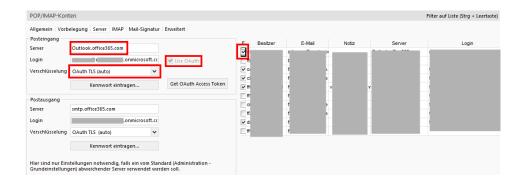
ACHTUNG: Führt der Administrator die Anmeldungen für mehrere Benutzer nacheinander aus, so scheint die Anmeldung zwar erfolgreich zu sein, allerdings wird die Anmeldung aufgrund von WebBrowser-Caching jeweils auf dem ersten Konto ausgeführt. Es wird deshalb empfohlen, dass sich jeder einzelne Benutzer getrennt auf seinem System registriert.

Um die Anmeldung möglichst komfortabel vorzubereiten, haben wir eine Funktion integriert mit der wir die notwendigen Daten zur (Client-Id, Client-Secret, Tenant-ID) auf die Konten der potentiellen Benutzer verteilen.

Als Konto kommt hierbei infrage, welches die folgenden Bedingungen erfüllt:

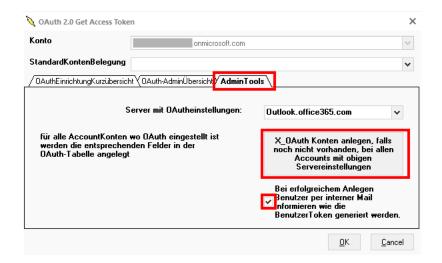
- Aktives Konto
- Server = ,outlook.office365.com^{*}
- Verschlüsselung: ,OAuth' eingestellt
- Noch kein Eintrag in der X OAuth Tabelle vorhanden

Beispielhaft wäre der erste Eintrag in dieser Konten-Liste betroffen.



Um die Daten von dem ersten fertig konfigurierten Konto auf die anderen, potentiell geeigneten Konten zu verteilen rufen Sie wieder in dem fertigen Konto die OAuth Eingabeform und wählen dort den Tab ,Admin Tools'.

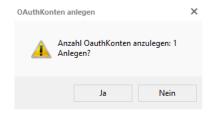
Stellen Sie dort den Server ein für den Sie die Daten verteilen möchten und setzten Sie den Haken für die Benachrichtigung der Benutzer von geänderten Konten. Führen Sie die Verteilung aus indem Sie die große Schaltfläche anklicken.



Information wie viele passende Konten gefunden wurden.



Nachfrage ob die Daten kopiert werden sollen ...



Bestätigung dass Daten angelegt wurden.



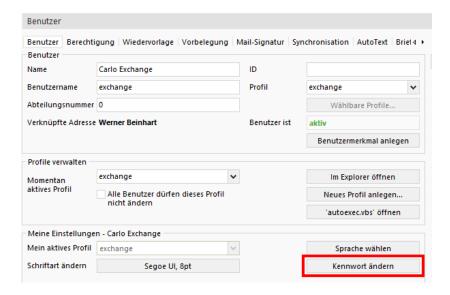
Jetzt sollten alle verfügbaren Daten auf gleichartige Konten übertragen worden sein.

6 Benutzer - OAuth Konfiguration Performer Mail

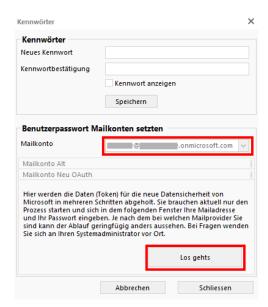
Nachdem die Administration die OAuth Anmeldung auf Exchange Online und Performer vorbereitet hat erhält der Anwender eine interne Nachricht in seiner Wiedervorlage in der die Aktionen für den Anwender beschrieben sind.



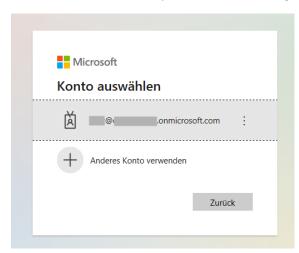
Wie beschrieben geht der Anwender in sein Benutzerkonto und wählt hier "Kennwort ändern".



Stellen Sie hier das O365 Konto ein, für das die OAuth Autorisierung aktiviert werden soll und 'los geht's'



Melden Sie sich in Ihrem persönlichen Exchange Online Konto an



7 Abschluß

Damit Ihre Änderungen wirksam werden, starten Sie den Maildienst neu.

Viel Erfolg!



8 Epilog

Hiermit danken wir ausdrücklich Microsoft für die ganzen Fallstricke, Ärgernisse, Kundensupport und Kosten, aber was nimmt man nicht alles in Kauf für ein wenig mehr an 'Sicherheit'.

Danke!