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	9
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'.

_	Benutzer			
٩	Suche	~	+ Zuweisungen hinzufügen $ imes $ Zuweisungen entfernen $$ O Aktualisieren	l A
8	Übersicht		Administratorrollen	
	Überwachungsprotokolle		Administratorrollen können verwendet werden, um Zugriff auf Azure AD und ande	ere Mici
Э	Anmeldeprotokolle		P Nach Name oder Beschreibung suchen ⁺ ∀ Filter hinzufügen	
Þ	Diagnose und Problembehandlung		Rolle	↑↓
			🗌 🍰 Globaler Administrator	
Ver	walten			
2,	Zugewiesene Rollen			

2.1 Anmelden im Azure Portal

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

Nach erfolgreicher Anmeldung wechseln wir in die Active Directory Verwaltung.

=	Microsoft Azure	,P Search resources, services, and docs (G+/)	E & 4 & 0 & 2
		Start with an Azure free trial Manage Azure Active Directory Access student benefits Get 3000 free credit board Azure products and services. Manage access sets mult policies, and enhance security Get free software, Azure Active Directory. Get the software Azure Active Directory. Get the software Azure Active Directory. Get the software Azure Active Directory. Tools for Teaching after you verify you academic student security. Start Learn more 0 ⁴ Yew Learn more 0 ⁴ Explore Learn more 0 ⁴	y anus
		Azure services	
		Image: Create a quicktart Virtual App Services Storage SQL databases Azure Cosmos Kubernetes Function App More services Create a quicktart Creater Creater App Services Storage SQL databases Azure Cosmos Kubernetes Function App More services	→ + services
		Resources	
		Recent Favorite	
		Name Type Last Viewed	

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.

Microsoft Azure	P Search resources, services, and docs (G+/)		5 6 4 🚳 7	
Home >				
Azure Active Directory	Overview			×
0	🏾 🕂 🖞 🖉 Manage tenants 🔀 What's new 🛛 🗔 Preview features 🛛 🖗 Got feedback? 🗸			
 Overview 				~
Preview features	Microsoft Entra has a simpler, integrated experience for managing all your Identity and Access Management needs. Try the ne	w Microsoft Entra admin center (Preview))		
X Diagnose and solve problems	Learn more 🖸			^
Manage				
💄 Users	My feed			
🐣 Groups		A Arrest 4D Connect		
External Identities	4a98e292-a0ed-4e15-a2ca-28fe45b930e9	O Not enabled		
Roles and administrators	Global administrator and 7 other roles Secure score updates can take up to 48 hours.	Sync has never run		
Administrative units	View profile View secure score	Go to Azure AD Connect		
Enterprise applications				
Devices	Feature highlights			
App registrations				
Identity Governance	Access reviews Authentication methods	Azure AD Domain Services		
Application proxy	A Make sure only the right people have continued access. Configure your users in the authentication methods policy to enable passwordless authentication.	 Lift-and-shift legacy applications run premises into Azure. 	ning on-	
 Custom security attributes (Preview) 				
🔓 Licenses				
Azure AD Connect	Specify the list of tenants that their users are			
🐖 Custom domain names	permitted to access.			
Mobility (MDM and MAM)				
Password reset	Oulde actions			
Company branding	Quick actions			
User settings				
Properties	Add user Add aroun Add enterprise Add antication			
https://portal.azure.com/#view/Microsoft AAD	D IAM/ActiveDirectoryMenuBlade/~/RegisteredApps application registration			

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

Dashboard > >			
Anwendung registrieren			
* Name			
Der dem Benutzer gezeigte Anzeigename für diese Anwendung. (Dieser kann später geändert werden.)			
ffMailDienst 🗸			
Unterstützte Kontotypen			
Wer kann diese Anwendung verwenden oder auf diese API zugreifen?			
● Nur Konten in diesem Organisationsverzeichnis (nur " 🖬 🗤 🗤 🗤 🗤 💭 🖉 🖉 – einzelner Mandant)			
🔿 Konten in einem beliebigen Organisationsverzeichnis (beliebiges Azure AD-Verzeichnis – mehrinstanzenfähig)			
Konten in einem beliebigen Organisationsverzeichnis (beliebiges Azure AD-Verzeichnis – mehrinstanzenfähig) und persönliche Microsoft-Konten (z. B. Skype, Xbox)			
O Nur persönliche Microsoft-Konten			
Entscheidungshilfe			
Umleitungs-URI (optional)			
Die Authentifizierungsantwort wird nach erfolgreicher Authentifizierung des Benutzers an diesen URI zurückgegeben. Die Angabe ist zum jetzigen Zeitpunkt optional und kann später geändert werden. Für die meisten Authentifizierungsszenarien ist jedoch ein Wert erforderlich.			
Plattform auswählen V Beispiel: https://example.com/auth			

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

Registrieren

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.

👯 FFMailDienst	\$					
₽ Suchen (STRG+/)	~	📋 Löschen 🕀 Endpunk	te 💀 Vorschaufeatures			
ubersicht		A Zucommonfossung				
Schnellstart		Anzeigename	: FFMailDienst		Clientanmeldeinformatio	Zertifikat, Geheimnis hinzufügen

Erzeugen Sie einen neuen geheimen Clientschlüssel.

💡 FFMailDienst Ze	ertif	ikate & Geheimnisse 🛷 …	\times
₽ Suchen (STRG+/)	~	R Haben Sie Feedback für uns?	
📕 Übersicht		Anhand von Anmeldeinformationen können vertrauliche Anwendunoen sich beim Authentifizierunosdienst identifizieren, wenn sie Token (über ein HTTPS-Schema) an ei	nem
i Schnellstart		adressierbaren Webspeicherort erhalten. Für eine höhere Sicherheitsstufe wird empfohlen, ein Zertifikat (anstelle eines Clientgeheimnisses) als Anmeldeinformation zu verwenden.	
🚀 Integrations-Assistent			
Verwalten		1 Anwendungsregistrierungszertifikate. Geheimnisse und Verbundanmeldeinformationen finden Sie auf den Registerkarten unten.	\times
🧮 Branding und Eigenschaften			
Authentifizierung		Zertifikate (0) Geheime Clientschlüssel (0) Verbundanmeldeinformationen (0)	
📍 Zertifikate & Geheimnisse			
Tokenkonfiguration		Eine geheime Zeichenfolge, die von der Anwendung beim Anfordern eines Tokens als Identitätsnachweis verwendet wird. Wird auch als Anwendungskennwort bezeichr	iet.
- API-Berechtigungen		+ Neuer geheimer Clientschlüssel	

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

Geheimen Clientschlüs	sel hinzufügen	×
Beschreibung	ClientSecret Maildienst	
Gültig bis	24 Monate	\sim

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

ClientSecret Maildienst 22.7	.7.2024 ubc8Q~AKaRHacjUwre74tKgi5	54Mzv_nli 🗅 ca701446-2557-41c5-83c0-9b3a433cb4b4 🗅 🣋
------------------------------	-----------------------------------	--

Gehen Sie wieder in die Übersicht der Registrierung

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

🚯 FFMailDienst 🖈		×
Suchen (STRG+/)	« 间 Löschen 🌐 Endpunkte 💀 Vorschaufeatures	
📕 Übersicht		
n Schnellstart	Zusammentassung	
🚀 Integrations-Assistent	Anzeigename FFMailDienst	
Verwalten	Anwendungs-ID (Client) 5 1111168 -a 14-4 3-b 1 5-9 116 f clie 3e	Umleitungs-URIs - <u>URI hinzufügen</u>
🔤 Branding und Eigenschaften	Objekt-ID	Anwendungs-ID-URI
Authentifizierung	e nder die die die die die die die die die die	Anwendungs-ID-URI hinzufügen
📍 Zertifikate & Geheimnisse	e minib b-8 1 1-4 1 b-b 1 c-f 1 and fa	FFMailDienst
Tokenkonfiguration	Unterstützte Kontotypen Nur meine Organisation	

Dies führt uns in die Authentifizierungskonfiguration der Anwendungsregistrierung.

2.3 Einstellen der Umleitungs URI

In der Authentifizierungskonfiguration klicken wir zunächst auf Plattform hinzufügen.

● FFMailDienst Auther	entifizierung 🖈 …
₽ Suchen (STRG+/) «	校 Haben Sie Feedback für uns?
ubersicht Übersicht	Plattformkonfigurationen
🗳 Schnellstart	hattomkomgaratoren
🚀 Integrations-Assistent	Abhängig von der Zielplattform oder dem Zielgerät für diese Anwendung ist möglicherweise eine zusätzliche Konfiguration erforderlich. Beispielsweise kann es erforderlich sein, Umleitungs-URIs, bestimmte Authentifizierungseinstellungen oder plattformspezifische Felder festzulegen.
Verwalten	
Branding und Eigenschaften	+ Plattform hinzufügen

Wir wählen den Eintrag für Mobilgerät- und Desktopanwendungen:

Plattformen konfigurieren				
Webanwendungen				
Web Hiermit wird eine Webserveranwendung erstellt, gehostet und bereitgestelltNET, Java,	Single-Page-Webanwendung Hiermit konfigurieren Sie Browserclientanwendungen und progressive Webanwendungen.			
Mobilgerät- und Desktopanwendunger	n			
iOS/macOS	Android			
Objective-C, Swift, Xamarin	Java, Kotlin, Xamarin			
Mobilgerät- und Desktopanwendungen				
Windows, UWP, Konsole, IoT-Geräte & Geräte für Zugangsbeschränkungen, iOS (klassisch) + Android				

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

 Mobilgerät- und Desktopanwendungen 	Schnellstart	Dokumente	Î
Umleitungs-URIs			
Die URIs, die wir als Ziele akzeptieren, wenn wir nach der erfolgreichen Benutzerauthentifizierung Authentifizierungsantworten (URI, den Sie in der Anforderung an den Anmeldeserver senden, muss mit dem hier aufgeführten übereinstimmen. Wird auch als Informationen zu Umleitungs-URIs und den zugehörigen Einschränkungen 🗗	Token) zurückgel Antwort-URLs b	ben. Der Umleitu ezeichnet. Weite	ngs- re
https://login.live.com/oauth20_desktop.srf (LiveSDK)			
msal5b1e1333-a5c4-4f08-bde5-9953cfc8b13e://auth (Nur MSAL)			
URI hinzufügen			

Nun können wir die Konfiguration speichern.

Erweiterte Einstellungen

Öffentliche Clientflows zulassen 🛈

Folgende Mobilgerät- und Desktopflows aktivieren:

Ja Nein

- App erfasst Klartextkennwort (Flow f
 ür Kennwortanmeldeinformationen des Ressourcenbesitzers) Weitere Informationen
 [™]
- Keine Tastatur (Gerätecodeflow) Weitere Informationen 🗹
- SSO f
 ür in die Dom
 äne eingebundene Windows-Ger
 äte (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

	erechtigungen 🖈 …	×
✓ Suchen (STRG+/) «	🕐 Aktualisieren 🔰 🔊 Haben Sie Feedback für uns?	
\rm Übersicht	Konfigurierte Berechtigungen	
i Schnellstart	Anwendungen sind zum Aufruf von APIs autorisiert, wenn ihnen im Rahmen des Zustimmungsprozesses Berechtigungen von Benutzern/Administrato	ren
🚀 Integrations-Assistent	erteilt werden. Die Liste der konfigurierten Berechtigungen muss alle Berechtigungen enthalten, die die Anwendung benötigt. Weitere Informationen : Berechtigungen und Zustimmung	zu
Verwalten	+ Rerechtigung hinzufügen	
🚍 Branding und Figenschaften	entellen	

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

API-Berechtigungen anfordern

Hiermit wählen Sie eine API aus.

Microsoft-APIs Von meiner Organisation verwendete APIs Eigene APIs

Häufig verwendete Microsoft-APIs



Microsoft Graph

Nutzen Sie die gewaltige Datenmenge in Office 365, Enterprise Mobility + Security und Windows 10. Greifen Sie auf Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planer und vieles mehr über einen einzigen Endpunkt zu.

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



Folgende Berechtigungen sollten mindestens gesetzt werden:

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

 \geq

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

FFMailDienst API-Berechtigungen 🖈 ····				
✓ Suchen (STRG+/) «	🖒 Aktualisieren 🔰 🞘 Haben Sie Feedback für uns?			
ubersicht	Konfigurierte Berechtigungen			
n Schnellstart	Anwendungen sind zum Aufruf von APIs autorisiert, wenn ihnen im Rahmen des Zustimmungsprozesses Berechtigungen von Benutzern/Administratoren erteilt werden. Die			
💉 Integrations-Assistent	Liste der könfigurierten Berechtigungen muss alle Berechtigungen enthalten, die die Anwendung benötigt. Weitere Informationen zu Berechtigungen und Zustimmung			
Verwalten	+ Berechtigung hinzufügen 🗸 Administratorzustimmung für "time in tereilen "erteilen			

Nun sind die Berechtigungen für die Applikation erteilt.

Konfigurierte Berechtigungen

Anwendungen sind zum Aufruf von APIs autorisiert, wenn ihnen im Rahmen des Zustimmungsprozesses Berechtigungen von Benutzern/Administratoren erteilt werden. Die Liste der konfigurierten Berechtigungen muss alle Berechtigungen enthalten, die die Anwendung benötigt. Weitere Informationen zu Berechtigungen und Zustimmung

+ Berechtigung hinzufügen	 Administrator 	zustimmung für "			
API/Berechtigungsname	Тур	Beschreibung	Administratoreinwill	Status	
∽ Microsoft Graph (4)					***
IMARAccessAsUser.All	Delegiert	Read and write access to mailboxes via IMAP.	Nein	📀 Gewährt für "	***
offline_access	Delegiert	Zugriff auf Daten beibehalten, für die Sie Zugriff erteilt ha	Nein	📀 Gewährt für "	•••
POP.AccessAsUser.All	Delegiert	Read and write access to mailboxes via POP.	Nein	📀 Gewährt für "	•••
SMTRSend	Delegiert	Send emails from mailboxes using SMTP AUTH.	Nein	🕑 Gewährt für "	••••

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/authenticatedclient-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.

POP/IMAP-Konte	POP/IMAP-Konten Filter auf Liste (Strg + Leertas)					
Allgemein Vorbe	legung Server IMAP Mail-Signatur Erweitert					
Name E-Mail-Adresse	oldexchange f	E Besitzer exchange	E-Mail	Notiz	Server Outlook.office365.com	Login
Antwort an Notiz		v oauth v charlie ffStandard ffAdmin ffAdmin	f f f f	• • • • • • •	outlook.office365.com imap.gmx.net imap.gmx.net imap.gmx.net imap.gmx.net imap.gmx.net	
	Dieses Konto beim Empfangen von E-Mails einbeziehen Dieses Konto wird vom Maildienst nicht verarbeitet	C doester	1		imap.gmx.net	

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

POP/IMAP-Kont	en	
Allgemein Vorb	elegung Server IMAP Mail-Signatur	Erweitert
Server	outlook.office365.com	
Login	@onmicrosoft.com	🖌 Use OAuth
Verschlüsselung	OAuth TLS (auto) 💙	
	Kennwort eintragen	Get OAuth Access Token
Postausgang		
rostaasgang		
Server	smtp.office365.com	
Server	smtp.office365.com	
Server Login Verschlüsselung	smtp.office365.com © OAuth TLS (auto)	
Server Login Verschlüsselung	smtp.office365.com Count rLS (auto) Kennwort eintragen	

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':

OAuth 2.0 Get Access	loken	×
Konto	@ onmicrosoft.com	~
StandardKontenBelegu	ng	~
OAuthEinrichtungKurzü	bersicht OAuth-AdminÜbersicht	
Tenant ID:		
Client ID:		
Client Secret:		
Access Token:	Z	Zugangsdaten abholen
		<u>D</u> K <u>C</u> ancel

Stellen Sie hier zunächst als Standard-Kontenbelegung ,0365' 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 ...

Auth 2.0 Get Access To	oken	×
Konto	@ .onmicrosoft.com	~
StandardKontenBelegur	9 0365	*
OAuthEinrichtungKurzüb	ersicht OAuth-AdminÜbersicht	
Tenant ID:	έ	
Client ID:		
Client Secret:	P	
Access Token:		Zugangsdaten abholen
(Noch) keine Daten gefunde	n in der UAuth-I abelle	
		<u>D</u> K <u>C</u> ancel

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

Mi	icrosoft			
Kont	to auswä	ihlen		
à	1@c	.onmicro	osoft.com	:
+	Anderes Ko	nto verwenden		
			Zurück	
			Lunder	
	Kont	Microsoft Konto auswa Anderes Ko	Microsoft Konto auswählen	Microsoft Konto auswählen

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

OAuth 2.0 Get Access	Token	×
Konto	@(.onmicrosoft.com	~
StandardKontenBelegu	ing	*
OAuthEinrichtungKurzü	ibersicht OAuth-AdminÜbersicht	
Tenant ID:		
Client ID:		
Client Secret:	۱.	
Access Token:	✓	Zugangsdaten abholen
		<u>Q</u> K <u>C</u> ancel

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...

POP/IMAP-Konten						Filter auf List	te (Strg + Leertaste)
Allgemein Vorbele	gung Server IMAP Mail-Signatur Erw	eitert					
Bitte rufen Sie zuers Ordner für den Post	t die IMAP-Ordner ab, um dann die entspre eingang und den Spamordner aus zu wähle IMAP-Ordner abrufen	chenden m.	E Besitzer	E-Mail	Notiz	Server outlook.office36	Login @< o
IMAP-Posteingang Spamordner Gesendet-Ordner	INBOX	✓ 2✓✓			vorher		
Erledigt-Ordner Gelöschte-Ordner	Noile, dia in litrom IMAR "Caléschia, Orden	v v					
dem Abruf unwiderr durch FLOWFACT no Mails aus dem Poste dem Gesendete-Ord	uffich vom E-Mail-Server gelöscht. Diese E-N bch durch Ihren E-Mail-Provider wiederherg ingang, dem Spamordner und ner des Servers nach	Aails können weder estellt werden. Tag(en) entfernen					
	IMAP-Postfach öffnen	3					

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'.

OAuth 2.0 Get Access	Token				×
Konto	feli	x@contosoewe.onmicros	oft.com		~
StandardKontenBelegu	ung				~
0AuthEinrichtungKurzüber:	sicht 04	Auth-AdminÜbersicht			
Authorization Code URI:	https:/	/login.microsoftonline.cor	n/		
Token URI:	https:/	/login.microsoftonline.com	n/common/oauth2/token		
Redirect URI:	https:/	/login.microsoftonline.com	n/common/oauth2/nativeclient		
Scope:	https:/	/outlook.office365.com/l	MAP.AccessAsUser.All		
AccessToken :	eyJ0e≯	KAiOiJKV1QiLCJub25jZSI	6InhzZVdzbjVHSU5KN0dBR2 I	Auth Code	Auth + Http
Expires In:	4697	25.07.2022 13:16:13	✓ AuthToken mit IE holen	Get Acce	ess Token
RefreshToken	0.ATo4	Au7ql7NGK00G47PZ6lA	KR-jMTHIvEpQhPveWZU8_Is	Refresh Ac	cess Token
Authorization Skeleton	{0}{4}/	/oauth2/v2.0/authorize?r	esponse_type=code&client_id={1	}&redirect_uri=	{2}&scope={:
Authorization Code:	0.ATo/	Au7ql7NGK00G47PZ6IA	KR-jMTHIvEpQhPveWZU8_IsT4I	6444.AgABA4	AIAAADDLA
				<u>0</u> K	<u>C</u> ancel

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

Spam	Manag	ler					
Kont	0	@onmicrosoft.com	 Imap-Spam-Ordner: Imap-Inbox: INBOX 		< >		
Post	eingang	des Mailservers (INBOX)					
	Spam	Von		Betreff		Datum	~
1		Microsoft Viva <viva-noreply@microsoft.co< td=""><td>) Ihre Digest-E-Mail</td><td></td><td></td><td>Mon, 18 Jul 2022 01:16:44 +0200</td><td></td></viva-noreply@microsoft.co<>) Ihre Digest-E-Mail			Mon, 18 Jul 2022 01:16:44 +0200	
2		Microsoft Viva <viva-noreply@microsoft.co< td=""><td>Willkommen bei Ihrem Digest</td><td></td><td></td><td>Thu, 14 Jul 2022 07:38:03 +0200</td><td></td></viva-noreply@microsoft.co<>	Willkommen bei Ihrem Digest			Thu, 14 Jul 2022 07:38:03 +0200	
3							
4							
							~
<							>
Van	Minor						
Ihre	Digest-	E-Mail					^
D0</td <td>OCTYPE</td> <td>html PUBLIC "-//W3C//DTD XHTML 1.0 St</td> <td>rict//EN" "http://www.w3.org/TR/</td> <td>/xhtml1/DTD/xhtml1-st</td> <td>rict.dtd"></td> <td></td> <td></td>	OCTYPE	html PUBLIC "-//W3C//DTD XHTML 1.0 St	rict//EN" "http://www.w3.org/TR/	/xhtml1/DTD/xhtml1-st	rict.dtd">		
<htr< td=""><td>nl lang:</td><td>="de" xml:lang="de" xmlns="http://www</td><td>.w3.org/1999/xhtml"></td><td></td><td></td><td></td><td></td></htr<>	nl lang:	="de" xml:lang="de" xmlns="http://www	.w3.org/1999/xhtml">				
<ne< td=""><td>ad></td><td></td><td></td><td></td><td></td><td></td><td></td></ne<>	ad>						

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.

POP/IMAP-Konten					Filter auf Liste (Strg + Leertaste)
Allgemein Vorbelegung Server IMAP Mail-Signatur Erweitert					
Posteingang Server Outlook office365 com	E Besitzer	E-Mail	Notiz	Server	Login
Login Use OAuth		t	×		
Verschlüsselung OAuth TLS (auto) 🗸		f	2.		
Kennwort eintragen Get OAuth Access Token	v ff	f	v	v	
Postausgang		1			1
Server smtp.office365.com	E of	f	2		
Login .onmicrosoft.cc	✓ de	f			1
Verschlüsselung OAuth TLS (auto)	E ff	f			
Kennwort eintragen					
Hier sind nur Einstellungen notwendig, falls ein vom Standard (Administration - Grundeinstellungen) abweichender Server verwendet werden soll.					

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 Tools⁴.

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.

Q OAuth 2.0 Get Access Token	×
Konto onmicrosoft.com	*
StandardKontenBelegung / DAuthEinrichtungKurzübersicht \ DAuth-AdminÜbersicht <mark>/ AdminTo</mark>	v
Server mit OAutheinstellungen:	Outlook.office365.com 🗸
für alle AccountKonten wo OAuth eingestellt ist werden die entsprechenden Felder in der OAuth-Tabelle angelegt	X_DAuth Konten anlegen, falls noch nicht vorhanden, bei allen Accounts mit obigen Servereinstellungen
	Bei erfolgreichem Anlegen Senutzer per interner Mail nformieren wie die BenutzerToken generiert werden.
	<u>O</u> K <u>C</u> ancel

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.

Meine Wiedervorlage				
Bis Donnerstag, 4. August 2022 💌	Ab Priorität Nicht wichtig	~		
OAuth-Konto vom MailAdministrat	OAuth-Konto vom MailAdministrator angelegt			
Ihr MailAdministrator hat ein net Bitte gehen Sie im Performer unt Instruktionen unter <benutzerpas< th=""><th>ues OAuth-Mailkonto angele er Administration-Benutzer- iswort Mailkonten setzten> u</th><th>egt. Kennwort ändern und folgen Sie den im dieses für den Mailempfang durch Sie zu aktivi</th><td>ieren</td></benutzerpas<>	ues OAuth-Mailkonto angele er Administration-Benutzer- iswort Mailkonten setzten> u	egt. Kennwort ändern und folgen Sie den im dieses für den Mailempfang durch Sie zu aktivi	ieren	

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

Benutzer				
Benutzer Berechti Benutzer	gung Wiedervorlage Vorbelegung	Mail-Signatur Sy	nchronisation AutoText Briel 4	
Name	Carlo Exchange	ID		
Benutzername	exchange	Profil	exchange 🗸	
Abteilungsnummer	0		Wählbare Profile	
Verknüpfte Adresse Werner Beinhart		Benutzer ist	aktiv	
			Benutzermerkmal anlegen	
Profile verwalten				
Momentan	exchange	*	Im Explorer öffnen Neues Profil anlegen	
aktives Profil	Alle Benutzer dürfen dieses Profil			
	nicht andem		'autoexec.vbs' öffnen	
Meine Einstellunge	n - Carlo Exchange			
Mein aktives Profil	exchange	×	Sprache wählen	
Schriftart ändern	Segoe UI, 8pt		Kennwort ändern	

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

Kennwörter		×
Kennwörter		
Neues Kennwort		
Kennwortbestätigung		
	Kennwort anzeig	en
	Speichern	
Benutzerpasswort N	lailkonten setzten	
Mailkonto	@	onmicrosoft.com 🗸
Mailkonto Alt		
Mailkonto Neu OAuth		
Hier werden die Daten Microsoft in mehreren S Prozess starten und sict und Ihr Passwort einge sind kann der Ablauf gi Sie sich an Ihren System	(Token) für die neue Da Schritten abgeholt. Sie I n in dem folgenden Fer ben. Je nach dem bei w eringfügig anders ausse nadministrator vor Ort.	stensicherheit von brauchen aktuell nur den nster Ihre Mailadresse velchen Mailprovider Sie ehen. Bei Fragen wenden
		Los gehts

Melden Sie sich in Ihrem persönlichen Exchange Online Konto an

Microsoft	
Konto auswählen	
e .onmicro	soft.com
+ Anderes Konto verwenden	
	Zurück
	Zuruck

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!