

How to do Webmail: OAuth 2.0

Stand: Version 7.1.2, Mai 2024



Inhalt

1	EINLEITUNG	3
2	ANLEGEN EINES MAILKONTOS MIT OAUTH 2.0-PROTOKOLL IM BM	4
2.1	OAuth 2.0 Endpunkt-URL	6
2.2	OAuth 2.0 Client-ID	7
2.3	OAuth 2.0 Client Secret	
2.4	OAuth 2.0 Scope	
2.5	Andere Einstellungen für MS Mailkonten im bm	
2.6	Bekannte Probleme mit MS Mailkonten	19



1 Einleitung

Seit einigen Jahren hat Microsoft begonnen, den Zugriff auf die bei ihnen gehosteten Mailkonten durch ein zusätzliches Autorisierungsprotokoll zu schützen. Es handelt sich dabei um das so genannte "OAuth 2.0" (Open Authorization). Seit 2023 ist dieses Verfahren verpflichtend für den Zugriff auf diese Konten (Office 365, Outlook, GMail).

Aus diesem Grund wurde der business manager (bm) dahingehend erweitert, dass er auch das OAuth 2.0-Protokoll unterstützt. Bei den bisherigen Mailkonten ist es lediglich erforderlich, im bm die notwendigen Zugangsdaten und Einstellungen (Mailadresse, Name des Mailkontos, Passwort, Pop- und SMTP-Server, POP- und SMTP-Ports) zu tätigen.

Im Gegensatz zu den bisherigen Mailservern, sind bei den MS-Mailkonten zusätzliche Einstellungen und weitere Schritte erforderlich, um das Mailkonto im bm einzutragen. Hierzu gehört auch, dass man auf der Administrationsseite des Mailservers tätig werden muss. Die genauen Schritte werden im Folgenden beschrieben. Einige weitere Einstellungen eines MS Mailkontos werden hier danach kurz aufgeführt.



2 Anlegen eines Mailkontos mit OAuth 2.0-Protokoll im bm

Beim Anlegen und Bearbeiten eines Mailkontos (Modul "Webmail", "Optionen", Karte "Benutzerkonten") gibt es nun im business manager (bm) die Option "OAuth 2.0 aktivieren".

Speichern Abbrechen		
Neues Benutzerkonto		
Präfix)
eMail-Adresse		
Standard		
POP Server Konfiguration		
POP3 Server		
POP3 Port (Standard: 110)		
Benutzerkonto		
Kennwort		
OAuth 2.0 aktivieren		
Sichere Verbindung	~	
SMTP Server Konfiguration		
SMTP Server		

Diese Option ist standardmäßig dekativiert und muss für alle Konten, die das OAuth 2.0-Protokoll verwenden, ausgewählt werden. Wird diese Option ausgewählt, so erscheinen weitere Felder, die ausgefüllt werden müssen.



POP3 Server		
POP3 Port (Standard: 110)		
Benutzerkonto		
Kennwort		
OAuth 2.0 aktivieren		
OAuth 2.0 Endpunkt-URL		
OAuth 2.0 Client-ID		
OAuth 2.0 Client Secret		
OAuth 2.0 Scope		
	V	

Um die richtigen Werte eintragen zu können, benötigen Sie den Zugriff auf Ihr Azure-Konto von Microsoft:

• Rufen Sie in Ihrem Webbrowser das Azure-Portal auf und melden sich mit Ihrer Mailadresse und Ihrem Kennwort an: **portal.azure.com**

Microsoft Azure	Microsoft Azure				
Microsoft Anmelden Mt Microsoft Azure fortfahren -Mail, Telefon oder Skype Kein Konto? Erstellen Sie jetzt eins! Sie können nicht auf Ihr Konto zugreifen? Murück Weiter	Microsoft Cennwort eingeben Cennwort vergessen Kennwort vergessen Anmelden				

Folgende Einstellungen müssen nun im bm getätigt werden.



2.1 OAuth 2.0 Endpunkt-URL

Dies ist eine Standard-URL, die zum Erwerb von Zugriffstoken verwendet wird. Jeder Server stellt seine eigene URL bereit.

Vorlage für die Token-Endpunkt-URL von Microsoft:

https://login.microsoftonline.com/{Mandanten-ID}/oauth2/v2.0/token

Um die Mandanten-ID zu finden, wählen Sie in Ihrem Azure-Konto den Eintrag "Microsoft Entra ID aus.



Nun öffnet sich eine Seite mit der Karte "Übersicht". Dort finden Sie den Eintrag für die Mandanten-ID.



≡ Micr	osoft Azure			𝒫 Nach Ressourcen,	Diensten und Dokumer	nten suchen (G+/)
Home >		📲 👘 🛛 Über	sicht …			
	<	🖕 🕂 Hinzufügen 🗸 🦸	🖇 Mandanten verwalten 🛛 Neuigkeiten	Vorschaufeatures	Haben Sie F	eedback für uns? 🗸
i Übersicht						
💀 Vorschau	features	 Azure Active Direc 	tory ist jetzt Microsoft Entra ID. Weitere Info	mationen 🖸		
🗙 Diagnose Problemb	und behandlung	Übersicht Überwac	hung Eigenschaften Empfehlunge	n Lernprogramme		
Verwalten		🔎 Ihren Mandanten	durchsuchen			
🚨 Benutzer		Basisinformationen				
🎒 Gruppen						
🏮 External I	dentities	Name			Benutzer	2
👃 Rollen un	d Administratoren	Mandanten-ID		<u>.</u> D	Gruppen	0
🚨 Verwaltur	igseinheiten	Primäre Domäne			Anwendungen	4
Partner fü Administr	ir delegierten ator	Lizenz	Microsoft Entra ID Free		Geräte	0
👢 Unterneh	mensanwendungen	Warnungen				

Diese ID könnte z.B. "6b29fc40-ca47-1067-b31d-00dd010662da" lauten. Kopieren Sie sie in den oben aufgeführten Link und diesen Link (also z.B. https://login.microsoftonline.com/6b29fc40-ca47-1067-b31d-00dd010662da /oauth2/v2.0/token) in das Feld "OAuth 2.0 Endpunkt-URL" im bm.

2.2 OAuth 2.0 Client-ID

ID eines Clients. Ein Client stellt eine Anwendung dar, die Anfragen an den Server stellt und Zugriffstokens erwirbt.

Um die Client-ID zu finden, muss zunächst in Ihrem Azure-Konto eine Applikation registriert werden. Hierzu wählen Sie wie zuvor in dem Azure-Konto den Eintrag "Mircosoft Entra ID" aus.





Wählen Sie dort im Menü am linken Rand die Funktion "App-Registrierungen" und dort die Funktion "Neue Registrierung" aus.



≡ Microsoft Azure	
Home > App-Registrierungen >	
Anwendung registrieren	
* Name	
Der dem Benutzer gezeigte Anzeigename für diese Anwendung. (Dieser kann später geändert werden.)	
bm_mail	~
Unterstützte Kontotypen	
Wer kann diese Anwendung verwenden oder auf diese API zugreifen?	
 Nur Konten in diesem Organisationsverzeichnis (nur "pirAMide Informatik GmbH" – einzelner Mandant) 	
🔘 Konten in einem beliebigen Organisationsverzeichnis (beliebiger Microsoft Entra ID-Mandant – mandantenfähig	j)
 Konten in einem beliebigen Organisationsverzeichnis (beliebiger Microsoft Entra ID-Mandant – mandantenfähig Microsoft-Konten (z. B. Skype, Xbox) 	ı) und persönliche
O Nur persönliche Microsoft-Konten	
Entscheidungshilfe	
Umleitungs-Uki (optional)	
Die Authentifizierungsantwort wird nach erfolgreicher Authentifizierung des Benutzers an diesen URI zuruckgegeben. jetzigen Zeitpunkt optional und kann später geändert werden. Für die meisten Authentifizierungsszenarien ist jedoch erforderlich.	Die Angabe ist zum ein Wert
Plattform auswählen V Beispiel: https://example.com/auth	
Registrieren Sie eine App, an der Sie gerade arbeiten. Integrieren Sie Katalog-Apps und andere Apps von außerhalb) Ihrer Organisation, indem Sie si
Indem Sie den Vorgang fortsetzen, stimmen Sie den Microsoft-Plattformrichtlinien zu. 🗗	
Registrieren	

In dem sich nun öffnenden Fenster tragen Sie einen beliebigen Namen für den bm ein z.B. "bm_mail" und klicken auf die Schaltfläche "Registrieren". Sie gelangen nun zurück zur Übersicht der registrierten Applikationen.



≡ Microsoft Azure 🔎 №	ach Ressourcen, Diensten und Dokumenten suchen (G- 🖸 💭 🏳 🐯 🕜 📈
Home > 4. Conf. State Conf.	
	App-Registrierungen ≈ ··· ×
	🔍 🕂 Neue Registrierung 🌐 Endpunkte 🧷 Problembehandlung 💍 Aktualisieren 🞍 Herunterladen \cdots
🕕 Übersicht	
Vorschaufeatures	1 Ab 30. Juni 2020 werden wir der Azure Active Directory-Authentifizierungsbibliothek (ADAL) und Azure Active
Diagnose und Problembehandlung	Directory-Graph keine neuen Features mehr hinzufügen. Wir stellen weiterhin technischen Support und Sicherheitsupdates bereit, bieten aber keine weiteren Featureupdates an. Anwendungen müssen ein Upgrade auf die Microsoft-Authentifizierungsbibliothek (MSAL) und Microsoft Graph durchführen. <u>Weitere Informationen</u>
Verwalten	
🚨 Benutzer	Alle Anwendungen Anwendungen mit Besitzer Gelöschte Anwendungen
🎎 Gruppen	
🏮 External Identities	
🎄 Rollen und Administratoren	1 Anwendungen gefunden
Verwaltungseinheiten	Anzeigename \uparrow_{\downarrow} Anwendungs-ID (ClErstellt am \uparrow_{\downarrow} Zertifikate & Geheim
Partner für delegierten Administrator	bm_mail 15.3.2023 I Abgelaufen
📕 Unternehmensanwendungen	
🖳 Geräte	
👯 App-Registrierungen	
Identity Governance	

Klicken Sie nun auf den Namen der gerade registrierten Applikation (z.B. "bm_mail").



\equiv +Microsoft Azure	${\cal P}$ Nach Ressourcen, Diensten und Dokumenten suchen (G+/)	
Home > And Appendix A	p-Registrierungen >	
<mark>, </mark>	📋 Löschen 🌐 Endpunkte 💀 Vorschaufeatures	
🕷 Übersicht 🔨	i Haben Sie einen Moment Zeit? Wir würden uns sehr über Ihr Feedback zur Microsoft Identity Platform (früh
i Schnellstart		
🚀 Integrations-Assistent	^ Zusammenfassung	
Verwalten	Anzeigename : <u>bm_mail</u>	Cli
🔤 Branding und Eigenschaften	Anwendungs-ID (Client)	Un
Authentifizierung	Objekt-ID :	An
📍 Zertifikate & Geheimnisse	Verzeichnis-ID (Mandant)	Vei
Tokenkonfiguration		
- API-Berechtigungen	Willkommen bei der neuen und verbesserten Funktion für App-Registrierungen. Möchten Sie wisse	n, w
eine API verfügbar machen		
🌇 App-Rollen	1 Ab 30. Juni 2020 werden wir der Azure Active Directory-Authentifizierungsbibliothek (ADAL) und Az	ure
🔉 Besitzer	technischen Support und Sicherheitsupdates bereit, bieten aber keine weiteren Featureupdates an. A und Microsoft Graph durchführen. <u>Weitere Informationen</u>	4nw
🚨 Rollen und Administratoren		
🔲 Manifest	Erste Schritte Dokumentation	

Auf der sich öffnenden Seite finden Sie ein Feld "Anwendungs-ID (Client) ID". Kopieren Sie den entsprechenden Eintrag und tragen ihn im bm im Feld "OAuth 2.0 Client-ID" ein.

2.3 OAuth 2.0 Client Secret

Ein Client kann öffentlich oder privat sein. Wenn es öffentlich ist, ist kein Passwort/Geheimnis erforderlich. Wenn es privat ist, müssen wir ein Secret angeben. Wir empfehlen, den Client als "privat" festzulegen.

a) Öffentlich

Im Menü am linken Rand klicken Sie dann auf "Authentifizierung", ändern unter "Folgende Mobilgerät- und Desktopflows aktivieren" die Einstellung auf "Ja" und speichern dann diese Änderung.





Das Feld "OAuth 2.0 Client Secret" bleibt in diesem Fall leer.

b) Nicht öffentlich / privat

Soll der Client nicht öffentlich sein, so lassen Sie obige Einstellung "Folgende Mobilgerät- und Desktopflows aktivieren" auf "Nein". In diesem Fall müssen wir stattdessen einen Client Secret definieren. Klicken Sie hierfür im Menü am linken Rand auf die Funktion "Zertifikate & Geheimnisse" und dann auf die Funktion "Neuer geheimer Clientschlüssel".



				𝒫 Nach Ressourcer					
Home > 0	Home > App-Registrierungen > bm_mail								
🔶 bm_mail2 Zertifikate & Geheimnisse 🛷 …									
✓ Suche «	🔗 Haben Sie F	eedback für uns?							
🐺 Übersicht									
📣 Schnellstart	Anhand von Anme adressierbaren W	eldeinformationen können vertraul Vebspeicherort erhalten. Für eine h	iche Anwendungen öhere Sicherheitsst	sich beim Authentifizier					
🚀 Integrations-Assistent	verwenden.								
Verwalten									
😑 Branding und Eigenschaften	1 Anwendung	gsregistrierungszertifikate, Geheimniss	e und Verbundanme	ldeinformationen finden S					
Authentifizierung									
📍 Zertifikate & Geheimnisse	Zertifikate (0)	Geheime Clientschlüssel (0)	Verbundanmel	deinformationen (0)					
Tokenkonfiguration	Eine geheime Ze	ichenfolge, die von der Anwendur	ig beim Anfordern	eines Tokens als Identit					
- API-Berechtigungen		eimer Clientschlüssel							
🔷 Eine API verfügbar machen	Desekasikus		citile bis	West O					
u App-Rollen	Beschreibung)	Guitig bis	wert ()					
🚑 Besitzer	Für diese Anwen	dung wurden keine Clientgeheimn	isse erstellt.						
🕹 Rollen und Administratoren									

Geben Sie nun einen Namen für den Clientschlüssel, wählen Sie die Gültigkeitsdauer aus und klicken auf "Hinzufügen".

	D 🖓	\$ 0 R
	Geheimen Clientschlü	issel hinzufügen $ imes$
	Beschreibung	bm_mail_secret
	Gültig bis	730 Tage (24 Monaté)
in Ar	- Hinzufügen Abbrechen	

Sie gelangen nun zurück zur Übersicht der angelegten Clientschlüssel. Kopieren Sie den Wert des Felds "Wert" und tragen ihn im bm in das Feld "OAuth 2.0 Client Secret" ein.



\equiv Microsoft Azure P Nach F	Ressourcen, Diensten und Dokumenten	suchen (G+/)	D	L ² &)	<i>ম</i>	
Home > App-Registrierungen > bm_mail							
pm_mail Zertifikate & Geheimnisse							×
✓ Suche «	🖗 Haben Sie Feedback für uns?						
🤻 Übersicht							
i Schnellstart	🚺 Haben Sie einen Moment, um un	s Feedback zu geben? —	÷				×
💉 Integrations-Assistent	Anhand van Anmaldainfarmatianan k	önnen vertrauliche Anv	uandungan sish hai	m Authorit	fiziorungu	-dienst identifizieren wenn sie Tek	
Verwalten	(über ein HTTPS-Schema) an einem a	dressierbaren Webspe	eicherort erhalten. F	ür eine höl	here Sich	erheitsstufe wird empfohlen, ein Ze	ertifikat
Branding und Eigenschaften	(anstelle ernes Clientgeneimnisses) al	s Anmeldeinformation	zu verwenden.				
Authentifizierung							×
📍 Zertifikate & Geheimnisse	Anwendungsregistrierungszertifik	kate, Geheimnisse und Ve	rbundanmeldeinform	iationen fin	den Sie au	f den Registerkarten unten.	
Tokenkonfiguration	Zertificate (0) Coheirer Client						
- API-Berechtigungen	Zertifikate (0) Geneime Clients	schlussel (1) Verb	undanmeldeinform	ationen (U))		
Eine API verfügbar machen	Eine geheime Zeichenfolge, die von Anwendungskennwort bezeichnet.	der Anwendung beim	Anfordern eines To	kens als Id	lentitätsna	achweis verwendet wird. Wird auch	i als
🌇 App-Rollen	- -						
🔉 Besitzer	+ Neuer geheimer Clientschlüsse	2					
🎝 Rollen und Administratoren	Beschreibung	Gültig bis	Wert 🛈			Geheime ID	
III Manifest	bm_mail_secret	5.6.2026					D İ

Nun müssen noch einige Berechtigungen erteilt werden. Hierfür klicken Sie in Ihrer Azure-Verwaltung im Menü am linken Rand auf die Funktion "API-Berechtigungen" und dann auf die Funktion "Berechtigung hinzufügen".



E Microsoft Azure P Nach R	essourcen, Diensten und Dokumenten suchen (G+/)	Þ	Ç2	٢	?	ন্দ	raspiazu PIRAMI		
Home > 2000 And 2000 And 2000 Ap	p-Registrierungen > bm_mail								
<mark></mark>	⊸ bm_mail API-Berechtigungen 🖉 …								
₽ Suche «	💍 Aktualisieren 🕂 Haben Sie Feedback für uns?								
📕 Übersicht									
SchnellstartIntegrations-Assistent	Durch das Erteilen einer mandantenweiten Einwilligung können Be Anwendung erteilt wurden. Berechtigungen, die Benutzer bereits in Informationen	rechtigungen n ihrem eiger	n widerr nen Nam	ufen w ien erte	erden, d eilt habe	lie bereit: n, sind d	s mandanten lavon nicht b		
Verwalten									
🚍 Branding und Eigenschaften	1 In der Spalte "Administratoreinwilligung erforderlich." wird der Sta	ndardwert fü	r eine O	rganisa	tion ang	gezeigt. [)ie Benutzere		
Authentifizierung	jedoch pro Berechtigung, Benutzer oder App angepasst werden. Di für Organisationen, in denen diese App verwendet wird. <u>Weitere In</u>	ese Spalte ze formationen	igt mög	licherw	eise nic	ht den W	/ert für Ihre C		
📍 Zertifikate & Geheimnisse									
Tokenkonfiguration	Konfigurierte Berechtigungen								
- API-Berechtigungen	Anwendungen sind zum Aufruf von APIs autorisiert, wenn ihnen im F Administratoren erteilt werden. Die Liste der konfigurierten Berecht	Rahmen des igungen mu	: Zustim Iss alle I	mung: Berech	sproze: itigung	sses Ber en entha	echtigunge alten, die di		
🙆 Eine API verfügbar machen	benötigt. Weitere Informationen zu Berechtigungen und Zustimmun	9							
👪 App-Rollen	🕂 🕂 🕂 Herechtigung hinzufügen	pirAMide Ir	nformat	ik Gml	bH" ert	eilen			
🤷 Besitzer	API/Berechtigungsn Typ Beschreibung		Adm	inistra	atorein	wil S	tatus		
🎄 Rollen und Administratoren	✓ Microsoft Graph (1)								
Manifest	User.Read Delegiert Anmelden und Benutzerpro	fil lesen	Nein						

In der sich nun rechts öffnenden Seite wählen Sie zunächst den Block "Microsoft Graph" aus.

\equiv Microsoft Azure P Nach F								
Home > API-Berechtigungen anfordern								
v – .	Hiermit wählen Sie eine API aus.							
	Microsoft-APIs Von meiner Organisation verwendete APIs Eigene APIs							
 Übersicht Schnellstart Integrations-Assistent 	Häufig verwendete Microsoft-APIs							
Verwalten	Nutzen Sie die enormen Datenmengen in Office 365, Enterprise Mobility + Security und Windows 10. Nicrosoft Entra ID, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner und vi einen einzelnen Endpunkt zu.							
🧮 Branding und Eigenschaften	Branding und Eigenschaften							
Authentifizierung								
📍 Zertifikate & Geheimnisse								
Tokenkonfiguration	Azure Service Management	Intune				Office 365 N		
API-Berechtigungen	Programmgesteuerter Zugriff auf den Großteil der Funktionen, die über das Azwe Portal zur Verfügung stehen	Programmgesteuerter Intune-Daten	Zugriff auf		Abruf Benut Richt	en von Inform zer-, Administ inienaktionen		

Nun wählen Sie den Block "Deligierte Berechtigungen" aus.





Es öffnet sich eine Liste mit Berechtigungen. Wählen Sie unter "POP" die Option "POP.AccessAsUser.All" aus.

\equiv Microsoft Azure \checkmark Nach	Ressourcen, Diensten und Dokumenten suchen (G+/)	
Home > A A A A A A A A A A A A A A A A A A	API-Berechtigungen anfordern	
✓ Suche «	> Policy	
Ubersicht	V POP (1)	
Schnellstart		
💉 Integrations-Assistent	Read and write access to mailboxes via POP.	
Verwalten	> Presence	

Wähen Sie zusätzlich unter "SMTP" die Option "SMTP.Send" aus und betätigen Sie die Schaltfläche am unteren Rand "Berechtigungen hinzufügen".



≡ Microsoft Azure 🔎 Nac	h Ressourcen, Diensten und Dokumenten suchen (G+/)	۶.	¢ 🖇
Home > 2000 America Americ America America Ame	API-Berechtigungen anfordern Sites		
Suche Ubersicht Schnellstart	SMTP (1) SMTP.Send ① Send emails from mailboxes using SMTP AUTH.		
Integrations-Assistent	> SpiffeTrustDomain		
Branding und Eigenschaften	SubjectRightsRequest		
Zertifikate & Geheimnisse Tokenkonfiguration	SynchronizationData-User		
- API-Berechtigungen			
 Eine API verfügbar machen App-Rollen 	Berechtigungen hinzufügen Verwerfen		

Sie gelangen nun zurück zur Übersicht der Berechtigungen. Betätigen Sie hier den Link "Administratorzustimmung für … erteilen".



■ Microsoft Azure P Nach Re	essourcen, Diensten und D	okumenten	suchen (G+/)	>_	J	٢	?	~	
Home > A A A A A A A A A A A A A A A A A A									
 bm_mail API-Berechtigungen 🛷 …									
- 🔎 Suche «	🖔 Aktualisieren 🛛	२ २ Haben Si	e Feedback für uns?						
ÜbersichtSchnellstart	Sie bearbeiten Berechtigungen für Ihre Anwendung. Benutzer müssen auch dann ihre Einwilligung erteilen, wenn sie dies getan haben.								
 Integrations-Assistent Verwalten 	Durch das Erteilen einer mandantenweiten Einwilligung können Berechtigungen widerrufen werden, die bereits mandant Anwendung erteilt wurden. Berechtigungen, die Benutzer bereits in ihrem eigenen Namen erteilt haben, sind davon nich betroffen. Weitere Informationen								
🧮 Branding und Eigenschaften	🖬 Branding und Eigenschaften								
Authentifizierung Zertifikate & Geheimnisse Tokenkonfiguration	In der Spalte "Administratoreinwilligung erforderlich." wird der Standardwert f ür eine Organisation angezeigt. Die Benutz kann jedoch pro Berechtigung, Benutzer oder App angepasst werden. Diese Spalte zeigt m öglicherweise nicht den Wert f Organisation oder f ür Organisationen, in denen diese App verwendet wird. <u>Weitere Informationen</u>								
 → API-Berechtigungen 	Konfigurierte Berechtigungen								
 Eine API verfügbar machen App-Rollen 	Anwendungen sind zum Aufruf von APIs autorisiert, wenn ihnen im Rahmen des Zustimmungsprozesses Berechtigung Administratoren erteilt werden. Die Liste der konfigurierten Berechtigungen muss alle Berechtigungen enthalten, die benötigt. Weitere Informationen zu Berechtigungen und Zustimmung								
🎥 Besitzer	+ Berechtigung hinzu	fügen 🗸	Administratorzustimmung für "🌺	38) A	Rea		erte	ilen	
🍰 Rollen und Administratoren	API/Berechtigungs	Тур	Beschreibung		Admini	strato	reinwil	Status	
0 Manifest	∽Microsoft Graph (3)								
Support + Problembehandlung	POP.AccessAsUser	Delegiert	Read and write access to mailb	oxe	Nein				
Problembehandlung	SMTP.Send	Delegiert	Send emails from mailboxes us	ing	Nein				
Neue Supportanfrage	User.Read	Delegiert	Anmelden und Benutzerprofil le	sen	Nein				

2.4 OAuth 2.0 Scope

Dieser Parameter definiert, welche Berechtigungen ein Zugriffstoken haben wird. OAuth 2.0 bietet eine differenzierte Kontrolle über Berechtigungen und wir müssen einen Bereich angeben, der es uns ermöglicht, eine Verbindung zu POP3/SMTP-Servern herzustellen. Für Office 365 und Outlook-Mailkonten tragen Sie hier ein:

https://outlook.office365.com/.default

2.5 Andere Einstellungen für MS Mailkonten im bm

Für Microsoft-Mailkonten gelten außerdem folgende Einstellungen im bm:

- Benutzerkonto: gleich Mailadresse
- POP3 Server: Outlook.office365.com
- POP3 Port: 995



- POP3 Sichere Verbindung: STARTTLS
- SMTP Server: Smtp.office365.com
- SMTP Port: 587
- SMTP Sichere Verbindung: STARTTLS

2.6 Bekannte Probleme mit MS Mailkonten

a) Es kann sein, dass in einem MS-Mailkonto das SMTP-Protokoll deaktiviert ist. Um dies zu ändern:

	Exchange Admin Cente	r				🔎 Suchen (Vorschau)
=			Start > Ei	instellungen		
ŵ	Startseite		_			
8	Empfänger	~	Einst	ellungen		
	E-Mail-Fluss	~				
R	Rollen	\sim				
5	Migration					
J.	Mobiltelefon	\sim		Name	Beschreib	ung
~	Berichte	\sim	=	Listenansichtseinstellung	Wählen S	e die normale Ansicht oder die kompakte Ansicht als bevorzugte Listenansichtseinstellung aus.
Q	Erkenntnisse			Nachrichtenfluss	Verwalten	der Einstellungen Ihrer Organisation zum Senden und Empfangen von Nachrichten
Ē	Öffentliche Ordner		$\overline{1}$	Hybrideinrichtung	Verbinder	und verwalten Sie sowohl Ihre lokalen als auch Ihre Exchange Online-Organisationen.
格	Organisation	^				
	Teilen					
ت <mark>ې</mark>	Einstellungen					
	Weitere Features					

- Rufen Sie das Exchange Admin Center auf: https://admin.exchange.microsoft.com/#/settings
- Wählen Sie im Menü am linken Rand die Funktion "Einstellungen"
- Wählen Sie im sich öffnenden Fenster den Link "Nachrichtenfluss"



Na	ichrichtenflusseinstellungen						
Ver Nac	erwalten Sie die Einstellungen Ihrer Organisation zum Senden und Empfangen von achrichten.						
Allo	jemein						
	Deaktivieren Sie die Plus-Adressierung für Ihre Or Weitere Informationen Senden von Aliasnamen aktivieren	ganisation.					
Sic	herheit						
	Deaktivieren des SMTP-AUTH-Protokolls für Ihre (Organisation					
\square	Aktivieren Sie die Verwendung von Legacy-TLS-Cli	ents. Weitere Informationen					
Sch	utz vor einer Allen antworten"-Welle						
~	Schutz vor einer "Allen antworten"-Welle aktivierer	n					
	Mindestanzahl von Empfängern (1000 bis 5000)	2500					
	Mindestanzahl für "Allen antworten" (2 bis 20)	10					
	Mindestanzahl für "Allen antworten" (2 bis 20)	10					
	Mindestanzahl für "Allen antworten" (2 bis 20) Blockdauer (1 bis 24 Stunden)	6					
Nac	Mindestanzahl für "Allen antworten" (2 bis 20) Blockdauer (1 bis 24 Stunden) :hrichtenrückruf	6					
Nad	Mindestanzahl für "Allen antworten" (2 bis 20) Blockdauer (1 bis 24 Stunden) :hrichtenrückruf Cloudbasierten Nachrichtenrückruf aktivieren	6					
Nac V	Mindestanzahl für "Allen antworten" (2 bis 20) Blockdauer (1 bis 24 Stunden) :hrichtenrückruf Cloudbasierten Nachrichtenrückruf aktivieren Ermöglichen Sie Benutzern, vom Empfänger gelese zurückzurufen	10 6					

• Die Option "Deaktivieren des SMTP-Auth-Protokolls für Ihre Organisation" darf NICHT ausgewählt sein. Ggf. ändern Sie diese Einstellung und speichern sie dann.



 b) Wenn die "Sicherheitsstandards" von Microsoft aktiviert sind, wird außerdem das SMTP-Protokoll deaktiviert und wir müssen möglicherweise diese "Sicherheitsstandards" deaktivieren:

≡	Microsoft Azure			ho Nach Ressourcen, Diensten und Dokumenten suchen (G+/)				
Hor	ne > 0.4 and 0.2 and 0.2 and 0.2							
			🛵 🦓 Eigenschaften					
	+	«	Name					
٩	Mandantenübergreifende	^	Name					
	Synchronisierung		Land oder Region	Germany				
4	Microsoft Entra Connect		Speicherort für Daten	EU Model Clause compliant datacenters				
_	Namen der benutzerdefinierten Domänen		Developing the second	Destade				
٢	Mobilität (MDM und WIP)		Benachrichtigungssprache	Deutsch				
•	Zurücksetzen des Kennworts		Mandanten-ID					
	Unternehmensbranding		Technischer Kontakt					
	Reputzereinstellungen			2471/08/27/70.27/22/22/22/29/29/29/27/24/06/				
10	riena de francisco de la composición de		Globaler Datenschutzkontakt					
	Eigenschaften		URL der Datenschutzbestimmungen					
•	Sicherheit							
Übe	rwachung	÷	Zugriffsverwaltung für Azure-Ressourcen					
Э	Anmeldeprotokolle			kann den Zugriff auf alle Azure-Abonnements und Verwal				
	Überwachungsprotokolle		Weitere Informationen 🖸					
ů	Bereitstellungsprotokolle		al 🔵					
*	Integrität							
	Protokollanalyse		Sicherheitsstandards					
*	Diagnoseeinstellungen		Sicherheitsstandards sind grundlegende Mechanismen für die Identitätssicherheit, die von Microsoft empfohlen werden. Sofern aktivier allgemeinen identitätsbezogenen Angriffen geschützt. Weitere Informationen [2]					
	Arbeitsmappen							
αú	Nutzung & Erkenntnisse		A Ihre Organisation ist nicht durch Sicherheit	sstandards geschützt.				
	Fraebnisse von	Sicherheitsstandards verwalten						

- Rufen Sie Ihre Azure-Verwaltung auf (s.o.)
- Wählen Sie Microsoft Extra ID (s.o.)
- Wählen Sie im Menü am linken Rand "Einstellungen"
- Klicken Sie hier unten auf den Link "Sicherheitsstandards verwalten"





• Nun wählen Sie die Einstellung "Deaktiviert" aus und speichern diese Einstellung.