



---

## **How to do Webmail: OAuth 2.0**

Stand: Version 7.1.2, Mai 2024

---

## Inhalt

<b>1</b>	<b>EINLEITUNG .....</b>	<b>3</b>
<b>2</b>	<b>ANLEGEN EINES MAILKONTOS MIT OAUTH 2.0-PROTOKOLL IM BM .....</b>	<b>4</b>
2.1	OAuth 2.0 Endpunkt-URL .....	6
2.2	OAuth 2.0 Client-ID .....	7
2.3	OAuth 2.0 Client Secret.....	11
2.4	OAuth 2.0 Scope .....	18
2.5	Andere Einstellungen für MS Mailkonten im bm.....	18
2.6	Bekannte Probleme mit MS Mailkonten.....	19

---

## 1 Einleitung

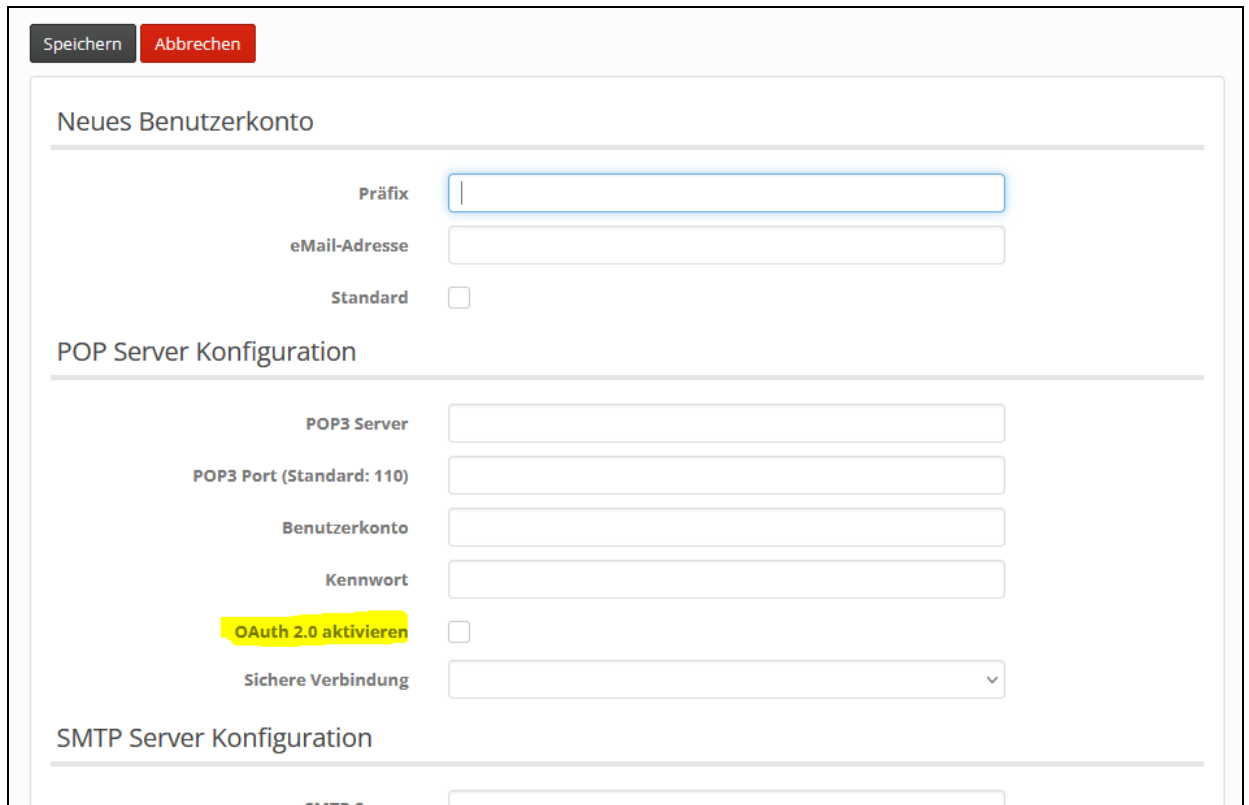
Seit einigen Jahren hat Microsoft begonnen, den Zugriff auf die bei ihnen gehosteten Mailkonten durch ein zusätzliches Autorisierungsprotokoll zu schützen. Es handelt sich dabei um das so genannte „OAuth 2.0“ (Open Authorization). Seit 2023 ist dieses Verfahren verpflichtend für den Zugriff auf diese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



The screenshot shows the 'Neues Benutzerkonto' configuration form. At the top, there are two buttons: 'Speichern' (dark grey) and 'Abbrechen' (red). The form is divided into three sections:

- Neues Benutzerkonto:** Contains fields for 'Präfix' (highlighted with a blue border), 'eMail-Adresse', and a 'Standard' checkbox.
- POP Server Konfiguration:** Contains fields for 'POP3 Server', 'POP3 Port (Standard: 110)', 'Benutzerkonto', 'Kennwort', and a highlighted 'OAuth 2.0 aktivieren' checkbox. Below these is a 'Sichere Verbindung' dropdown menu.
- SMTP Server Konfiguration:** Contains a partially visible 'SMTP Server' field.

Diese Option ist standardmäßig deaktiviert 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.

### POP Server Konfiguration

---

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

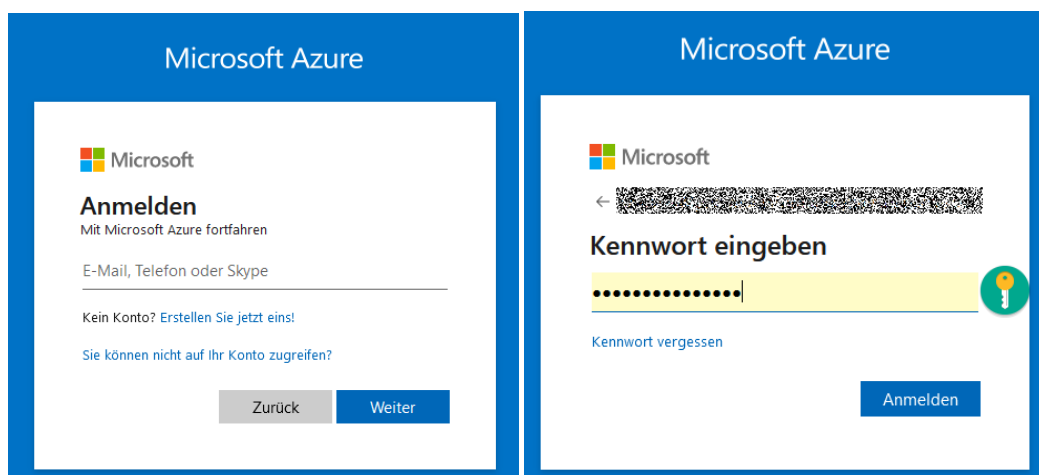
Sichere Verbindung

---

### SMTP Server Konfiguration

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**



Folgende Einstellungen müssen nun im bm getätigt werden.

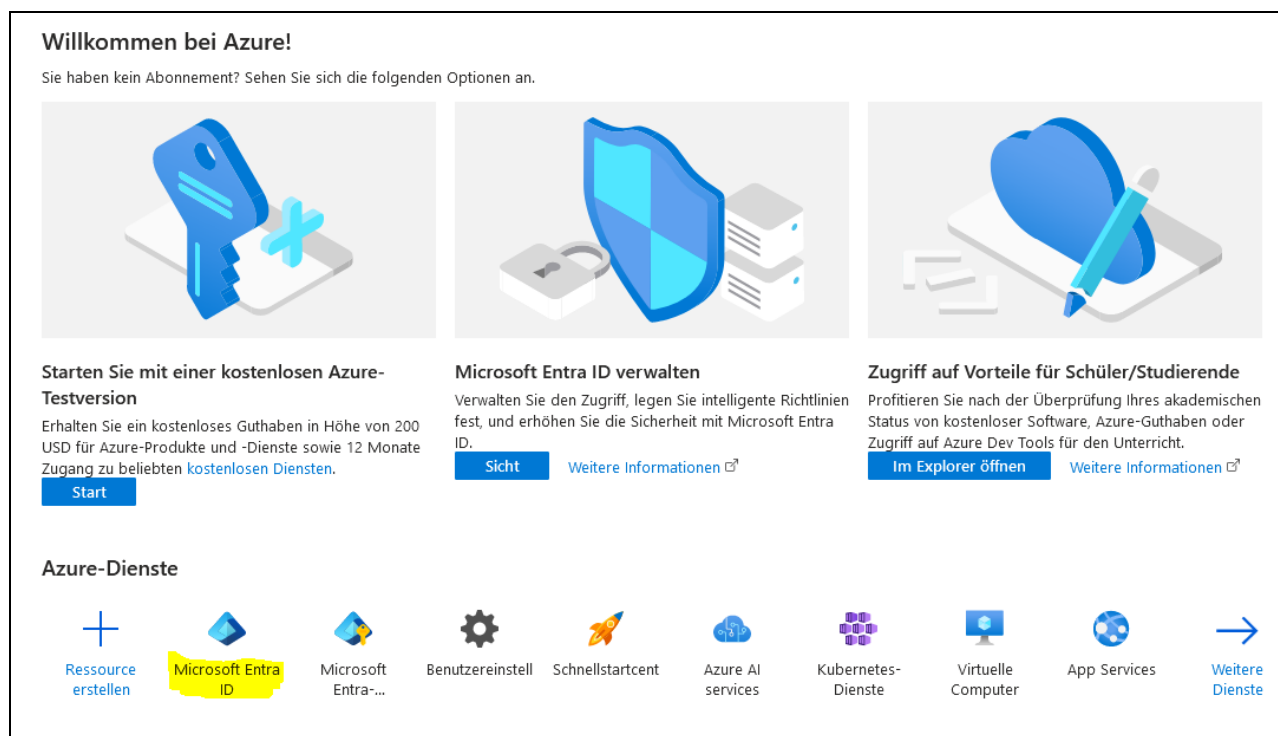
## 2.1 OAuth 2.0 Endpunkt-URL

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

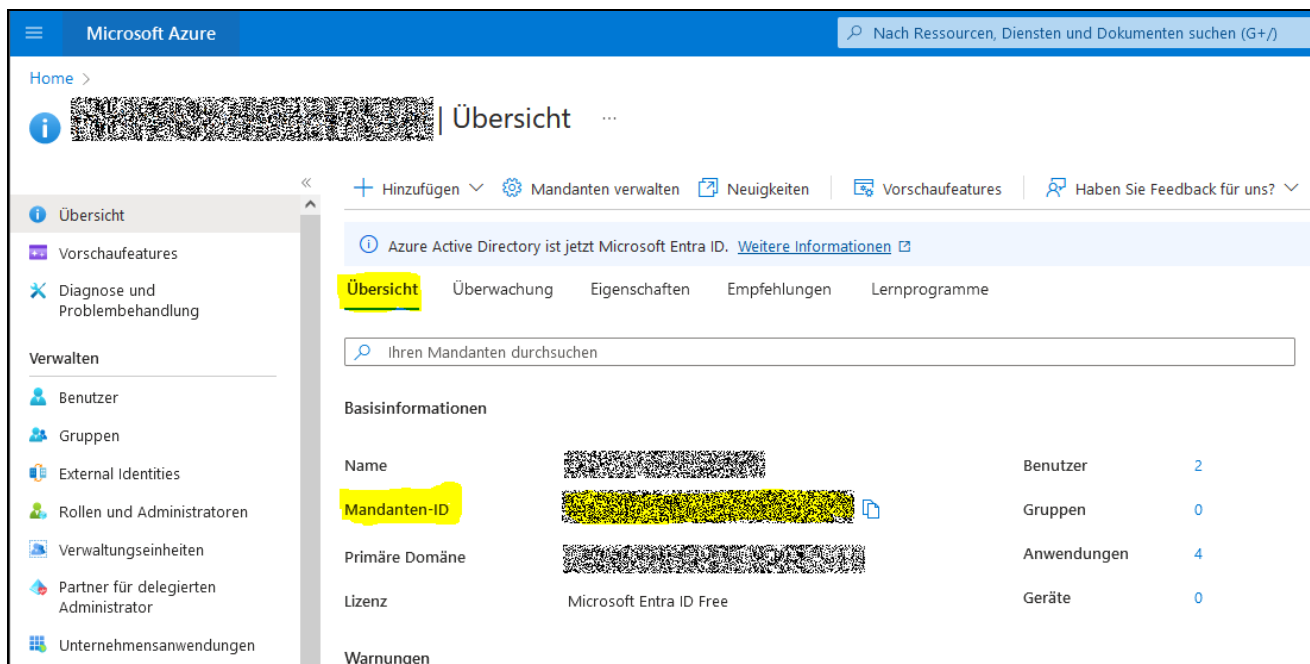
Vorlage für die Token-Endpunkt-URL von Microsoft:

`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.



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.

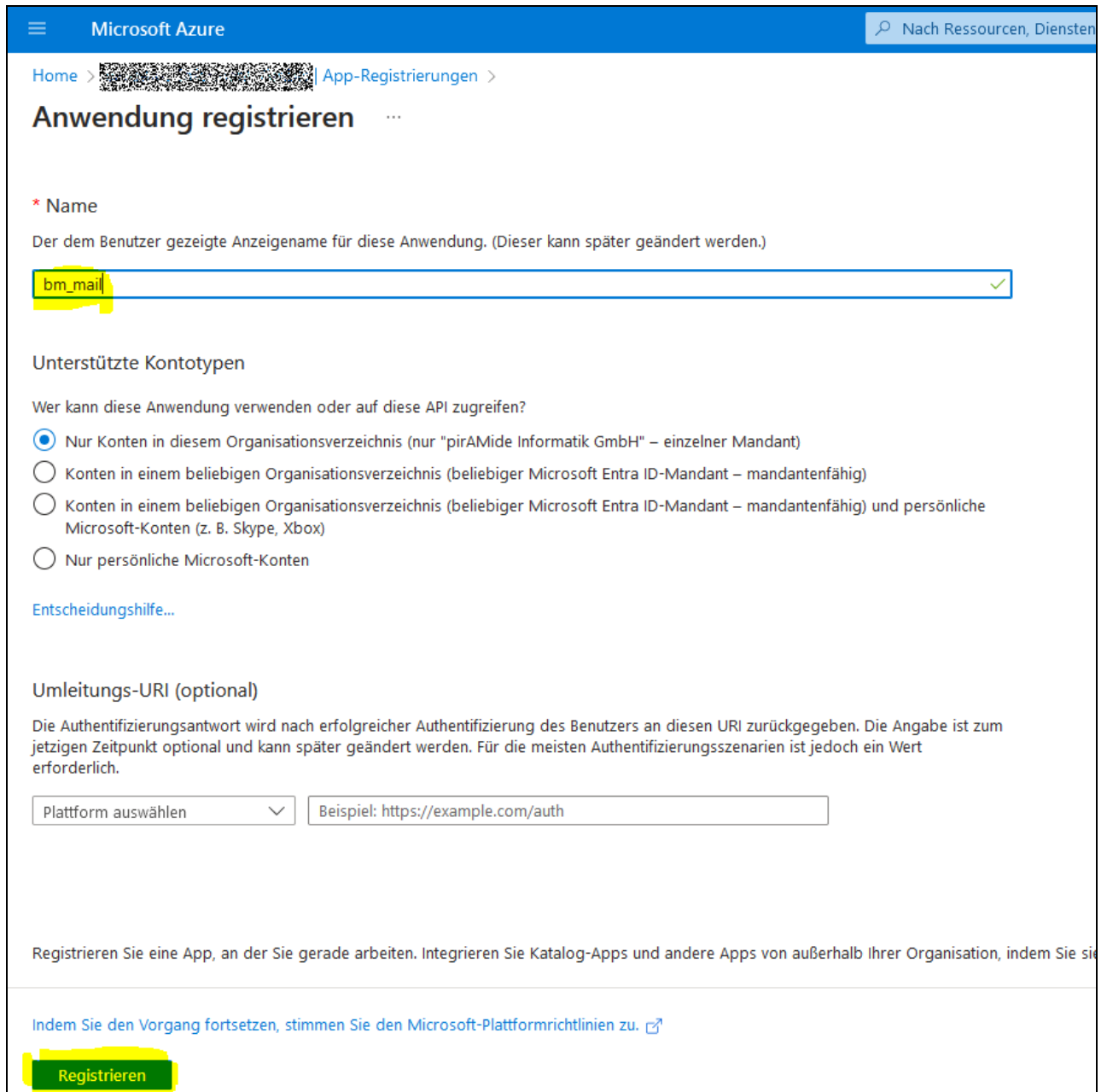
## 2.2 OAuth 2.0 Client-ID

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 „Microsoft Entra ID“ aus.







Microsoft Azure

Nach Ressourcen, Diensten

Home > [redacted] > 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)
- Konten in einem beliebigen Organisationsverzeichnis (beliebiger Microsoft Entra ID-Mandant – mandantenfähig) und persönliche Microsoft-Konten (z. B. Skype, Xbox)
- 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.

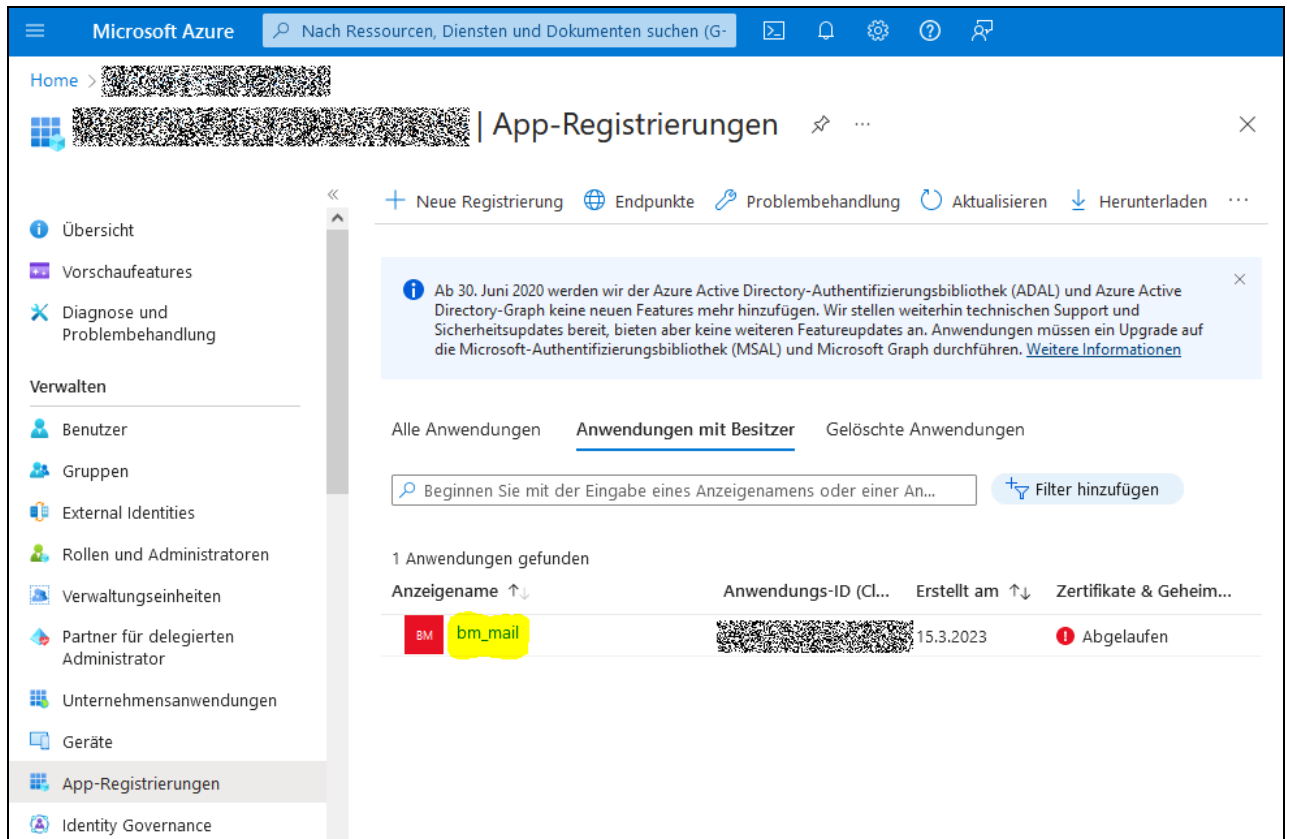
Plattform auswählen ▼ Beispiel: https://example.com/auth

Registrieren Sie eine App, an der Sie gerade arbeiten. Integrieren Sie Katalog-Apps und andere Apps von außerhalb Ihrer Organisation, indem Sie sie

[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 | App-Registrierungen

Ab 30. Juni 2020 werden wir der Azure Active Directory-Authentifizierungsbibliothek (ADAL) und Azure Active 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. [Weitere Informationen](#)

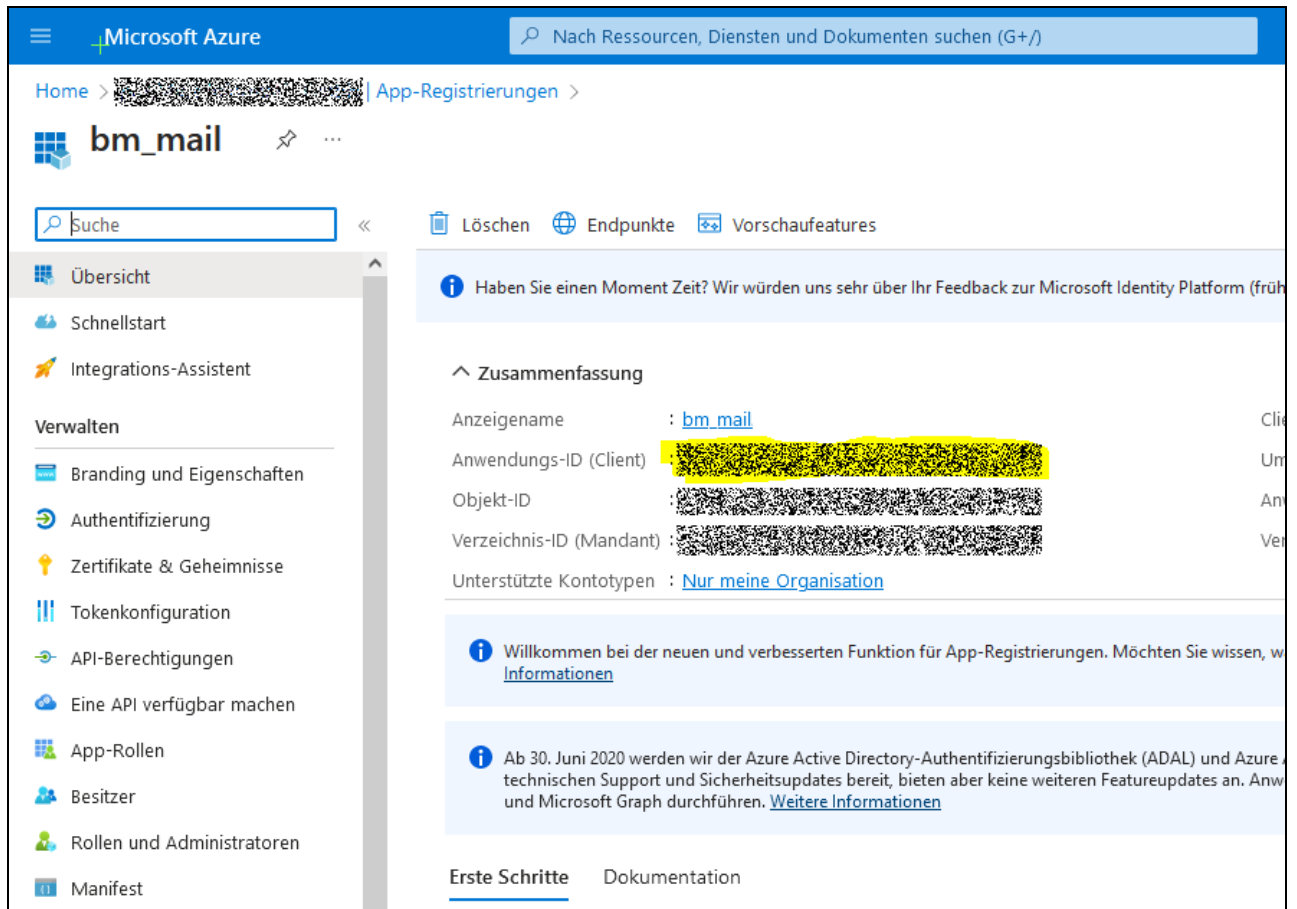
Alle Anwendungen | **Anwendungen mit Besitzer** | Gelöschte Anwendungen

Beginnen Sie mit der Eingabe eines Anzeigenamens oder einer An... [Filter hinzufügen](#)

1 Anwendungen gefunden

Anzeigename	Anwendungs-ID (Cl...	Erstellt am	Zertifikate & Geheim...
 <b>bm_mail</b>	[Redacted]	15.3.2023	 Abgelaufen

Klicken Sie nun auf den Namen der gerade registrierten Applikation (z.B. „bm\_mail“).



The screenshot shows the Microsoft Azure portal interface. At the top, there's a search bar and navigation links. The main content area displays the details for an application named 'bm\_mail'. The 'Anwendungs-ID (Client)' field is highlighted in yellow. The left sidebar contains a navigation menu with options like 'Übersicht', 'Schnellstart', 'Integrations-Assistent', and 'Verwalten'. The right pane shows a summary of the application's properties, including its name, ID, and supported account types.

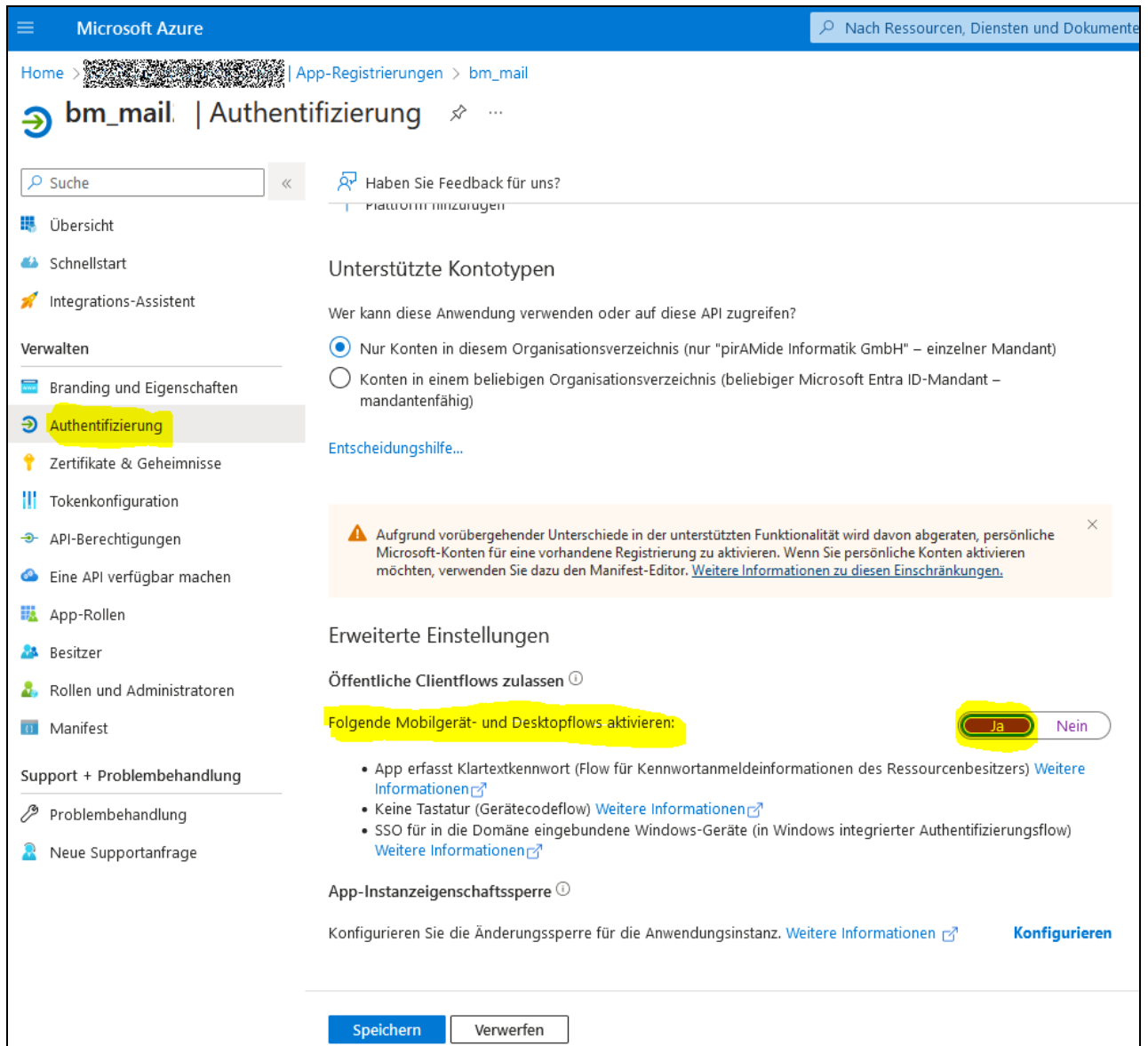
Auf der sich öffnenden Seite finden Sie ein Feld „Anwendungs-ID (Client) ID“. Kopieren Sie den entsprechenden Eintrag und tragen ihn im bm im Feld „OAuth 2.0 Client-ID“ ein.

### 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.



Microsoft Azure

Home > [redacted] > App-Registrierungen > bm\_mail

**bm\_mail** | Authentifizierung

Suche

Haben Sie Feedback für uns?  
Plattformhinzufragen

Übersicht  
Schnellstart  
Integrations-Assistent

Verwalten

Branding und Eigenschaften  
**Authentifizierung**  
Zertifikate & Geheimnisse  
Tokenkonfiguration  
API-Berechtigungen  
Eine API verfügbar machen  
App-Rollen  
Besitzer  
Rollen und Administratoren  
Manifest

Support + Problembehandlung  
Problembehandlung  
Neue Supportanfrage

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)

Entscheidungshilfe...

**⚠** Aufgrund vorübergehender Unterschiede in der unterstützten Funktionalität wird davon abgeraten, persönliche Microsoft-Konten für eine vorhandene Registrierung zu aktivieren. Wenn Sie persönliche Konten aktivieren möchten, verwenden Sie dazu den Manifest-Editor. [Weitere Informationen zu diesen Einschränkungen.](#)

Erweiterte Einstellungen

Öffentliche Clientflows zulassen ⓘ

Folgende Mobilgerät- und Desktopflows aktivieren: **Ja** Nein

- App erfasst Klartextkennwort (Flow für Kennwortanmeldeinformationen des Ressourcenbesitzers) [Weitere Informationen](#)
- Keine Tastatur (Gerätecodeflow) [Weitere Informationen](#)
- SSO für in die Domäne eingebundene Windows-Geräte (in Windows integrierter Authentifizierungsflow) [Weitere Informationen](#)

App-Instanzeigenschaftssperre ⓘ

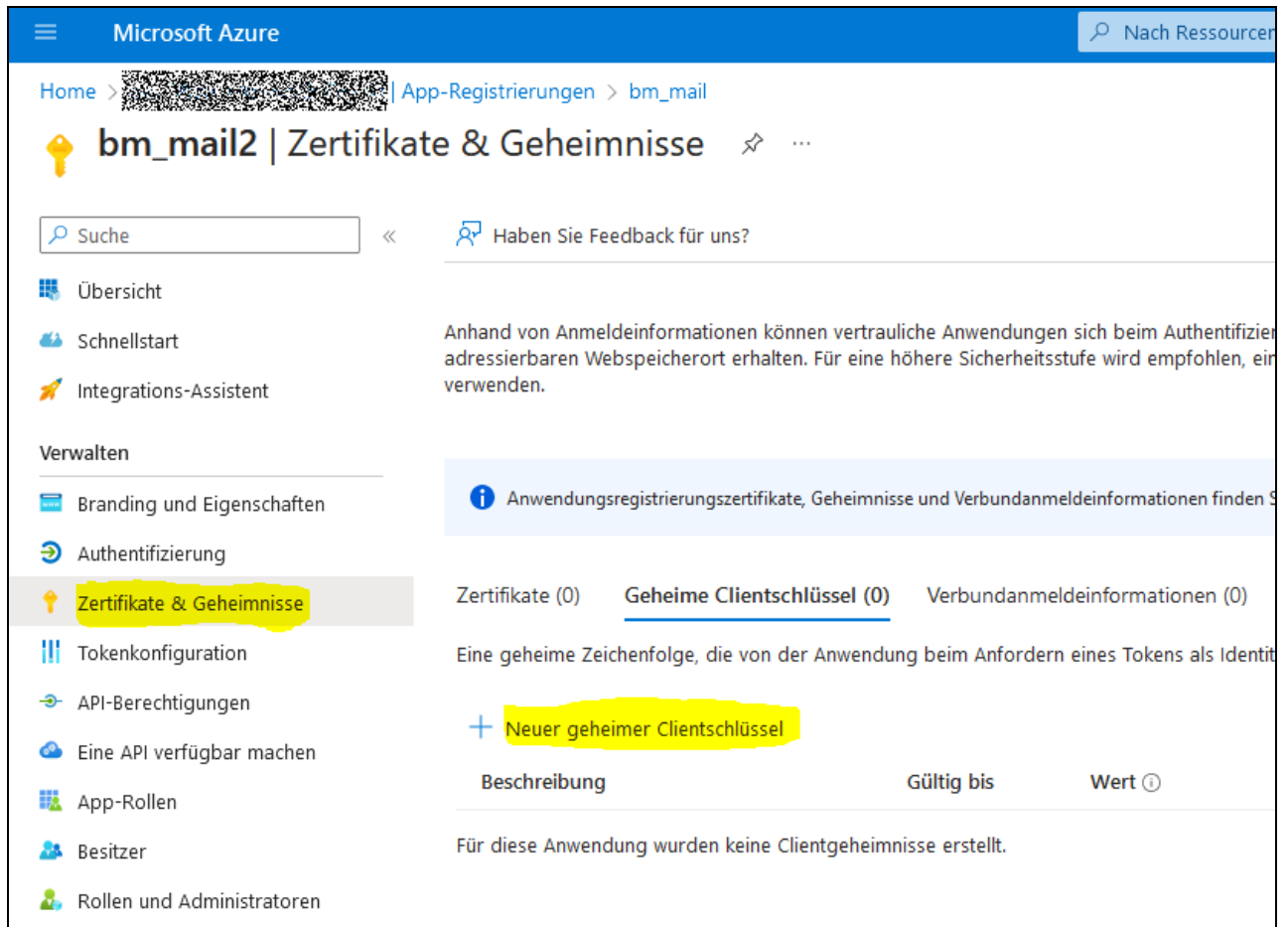
Konfigurieren Sie die Änderungssperre für die Anwendungsinstanz. [Weitere Informationen](#) **Konfigurieren**

**Speichern** Verwerfen

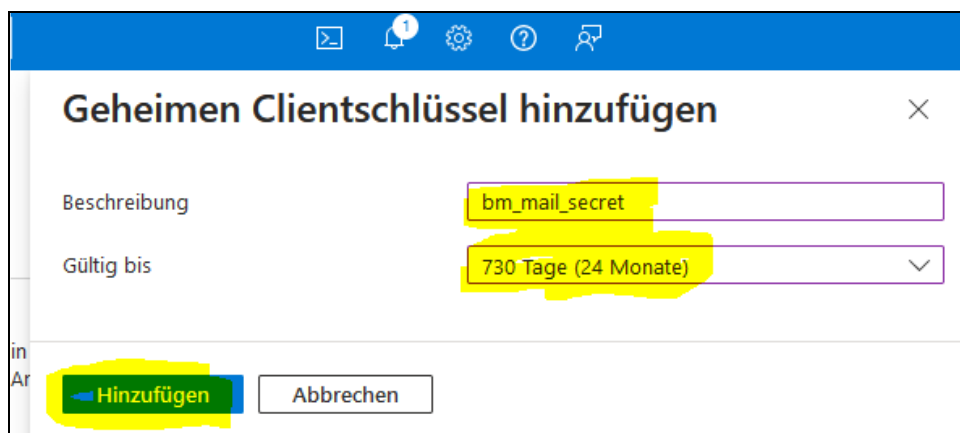
Das Feld „OAuth 2.0 Client Secret“ bleibt in diesem Fall leer.

## b) Nicht öffentlich / privat

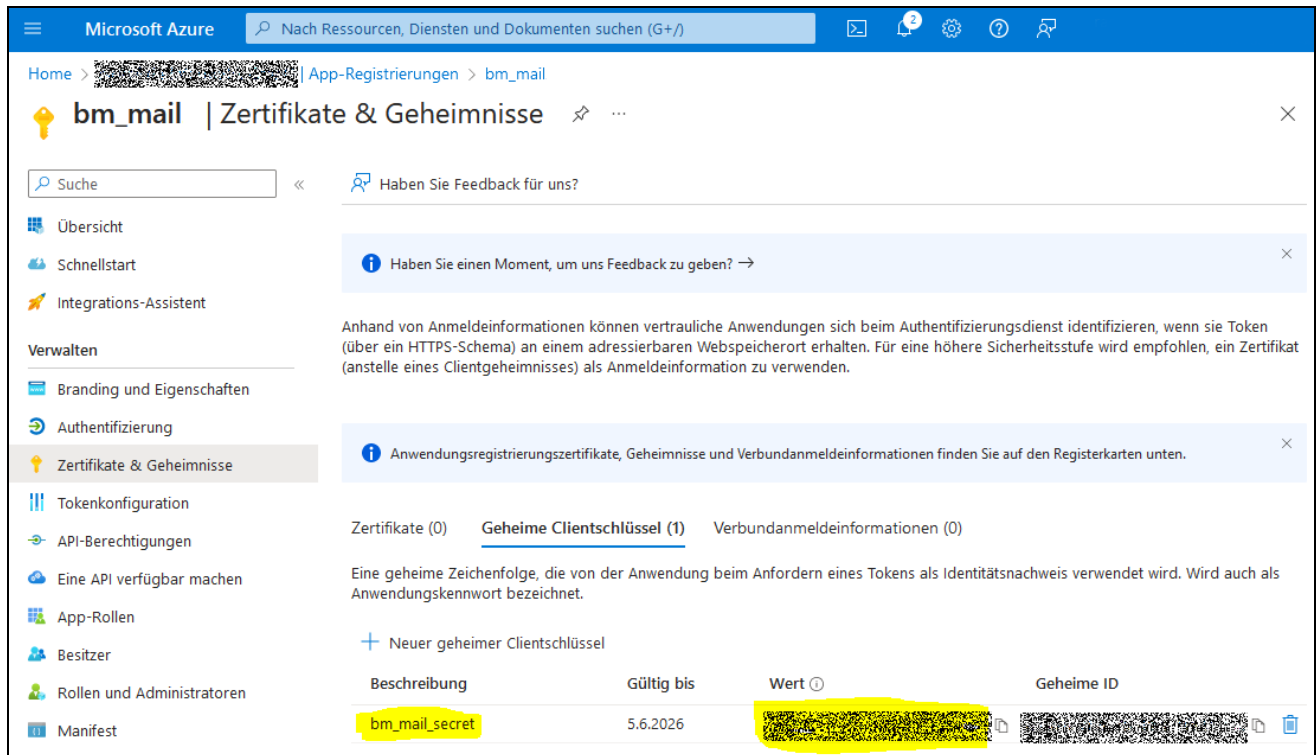
Soll der Client nicht öffentlich sein, so lassen Sie obige Einstellung „Folgende Mobilgerät- und Desktopflows aktivieren“ auf „Nein“. In diesem Fall müssen wir stattdessen einen Client Secret definieren. Klicken Sie hierfür im Menü am linken Rand auf die Funktion „Zertifikate & Geheimnisse“ und dann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



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



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.



Microsoft Azure | Nach Ressourcen, Diensten und Dokumenten suchen (G+/)

Home > [redacted] | App-Registrierungen > bm\_mail

## bm\_mail | Zertifikate & Geheimnisse

Suche << Haben Sie Feedback für uns?

Übersicht  
Schnellstart  
Integrations-Assistent

Verwalten

- Branding und Eigenschaften
- Authentifizierung
- Zertifikate & Geheimnisse**
- Tokenkonfiguration
- API-Berechtigungen
- Eine API verfügbar machen
- App-Rollen
- Besitzer
- Rollen und Administratoren
- Manifest

Haben Sie einen Moment, um uns Feedback zu geben? →

Anhand von Anmeldeinformationen können vertrauliche Anwendungen sich beim Authentifizierungsdienst identifizieren, wenn sie Token (über ein HTTPS-Schema) an einem adressierbaren Webspeicherort erhalten. Für eine höhere Sicherheitsstufe wird empfohlen, ein Zertifikat (anstelle eines Clientgeheimnisses) als Anmeldeinformation zu verwenden.

Anwendungsregistrierungszertifikate, Geheimnisse und Verbundanmeldeinformationen finden Sie auf den Registerkarten unten.

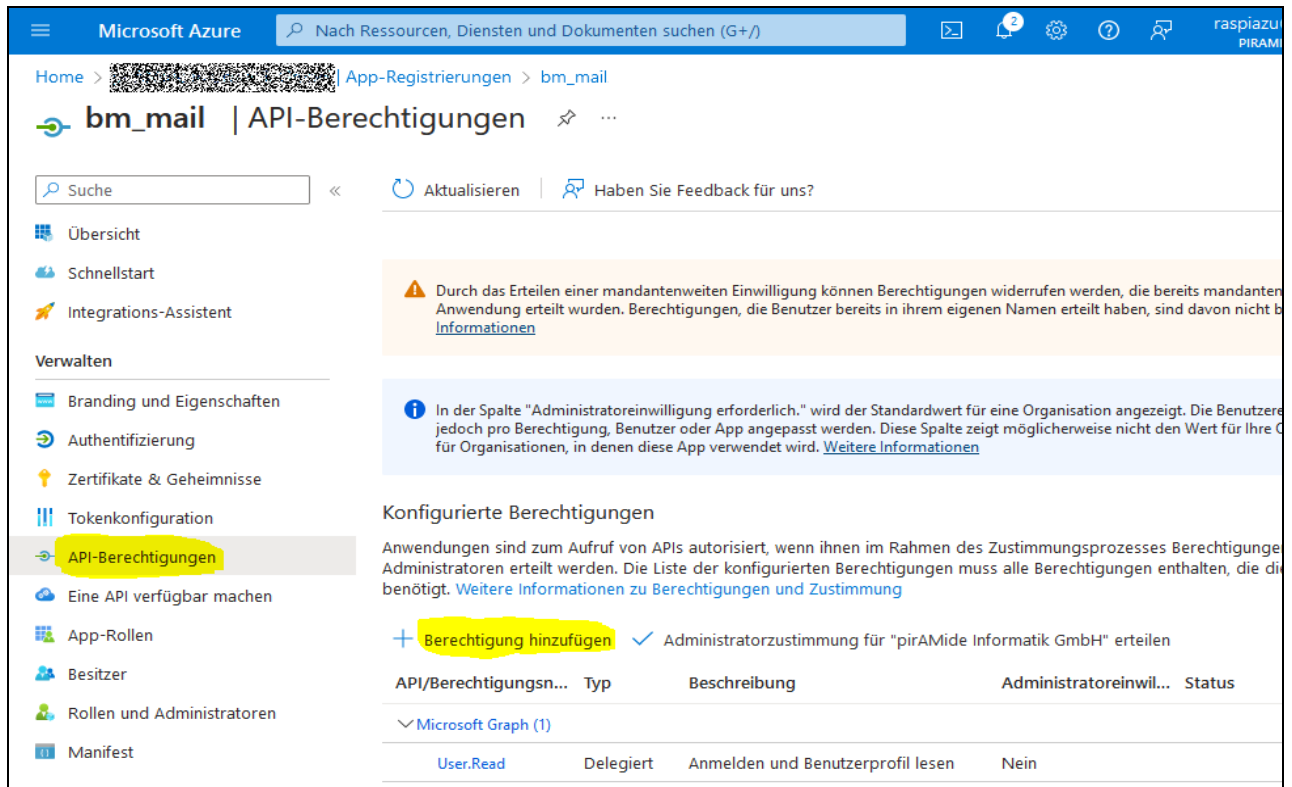
Zertifikate (0) **Geheime Clientschlüssel (1)** Verbundanmeldeinformationen (0)

Eine geheime Zeichenfolge, die von der Anwendung beim Anfordern eines Tokens als Identitätsnachweis verwendet wird. Wird auch als Anwendungskennwort bezeichnet.

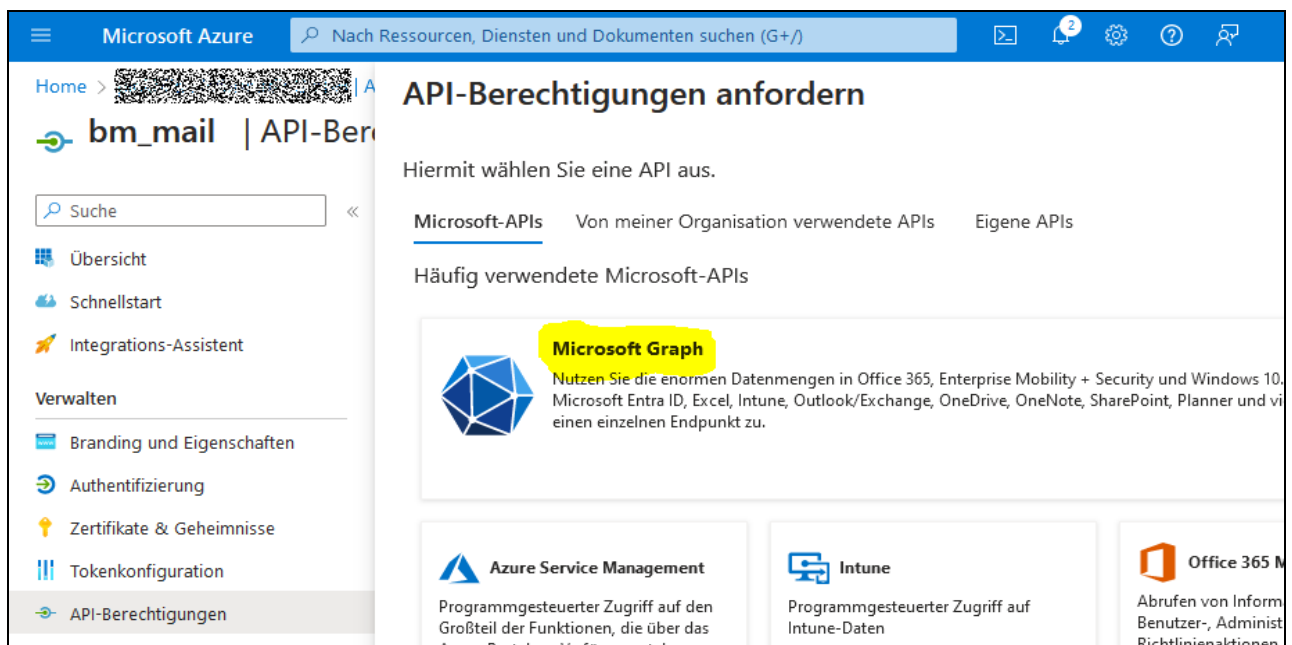
+ Neuer geheimer Clientschlüssel

Beschreibung	Gültig bis	Wert	Geheime ID
bm_mail_secret	5.6.2026	[redacted]	[redacted]

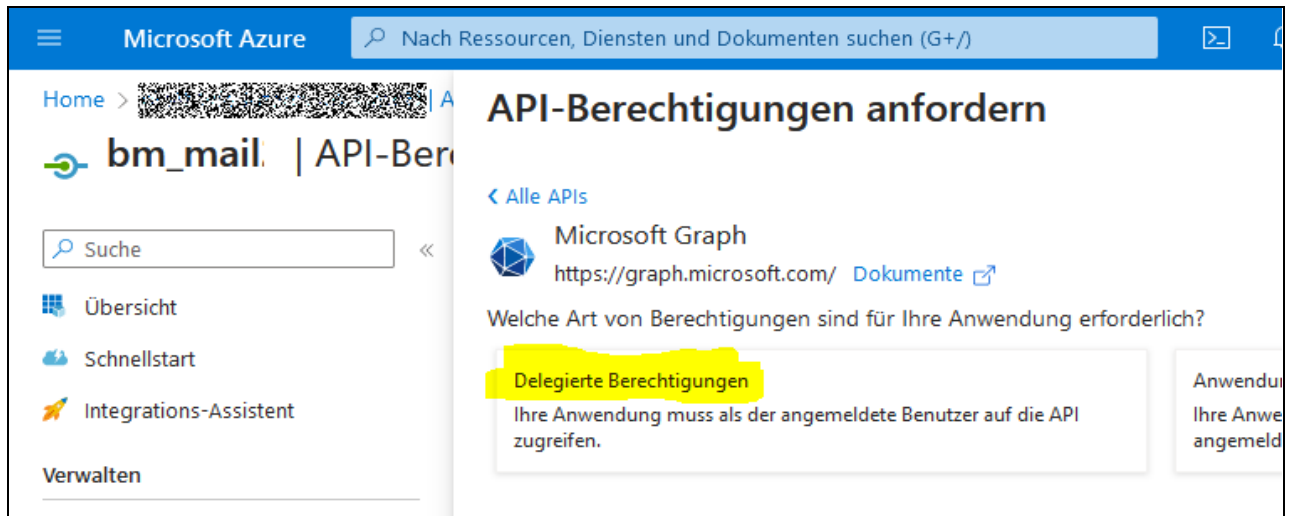
Nun müssen noch einige Berechtigungen erteilt werden. Hierfür klicken Sie in Ihrer Azure-Verwaltung im Menü am linken Rand auf die Funktion „API-Berechtigungen“ und dann auf die Funktion „Berechtigung hinzufügen“.



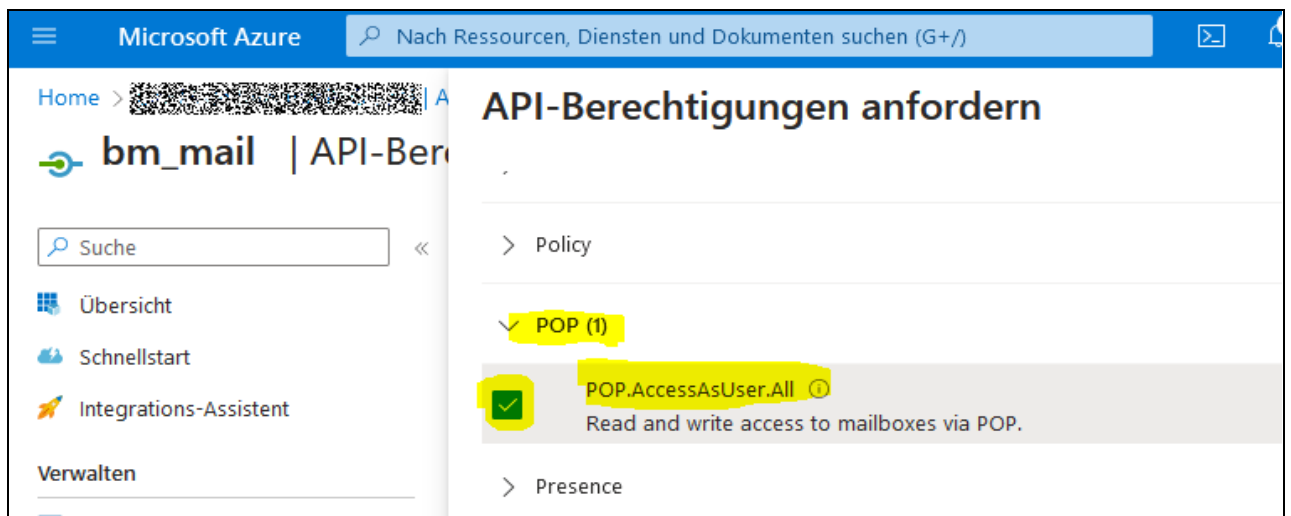
In der sich nun rechts öffnenden Seite wählen Sie zunächst den Block „Microsoft Graph“ aus.



Nun wählen Sie den Block „Delegierte Berechtigungen“ aus.

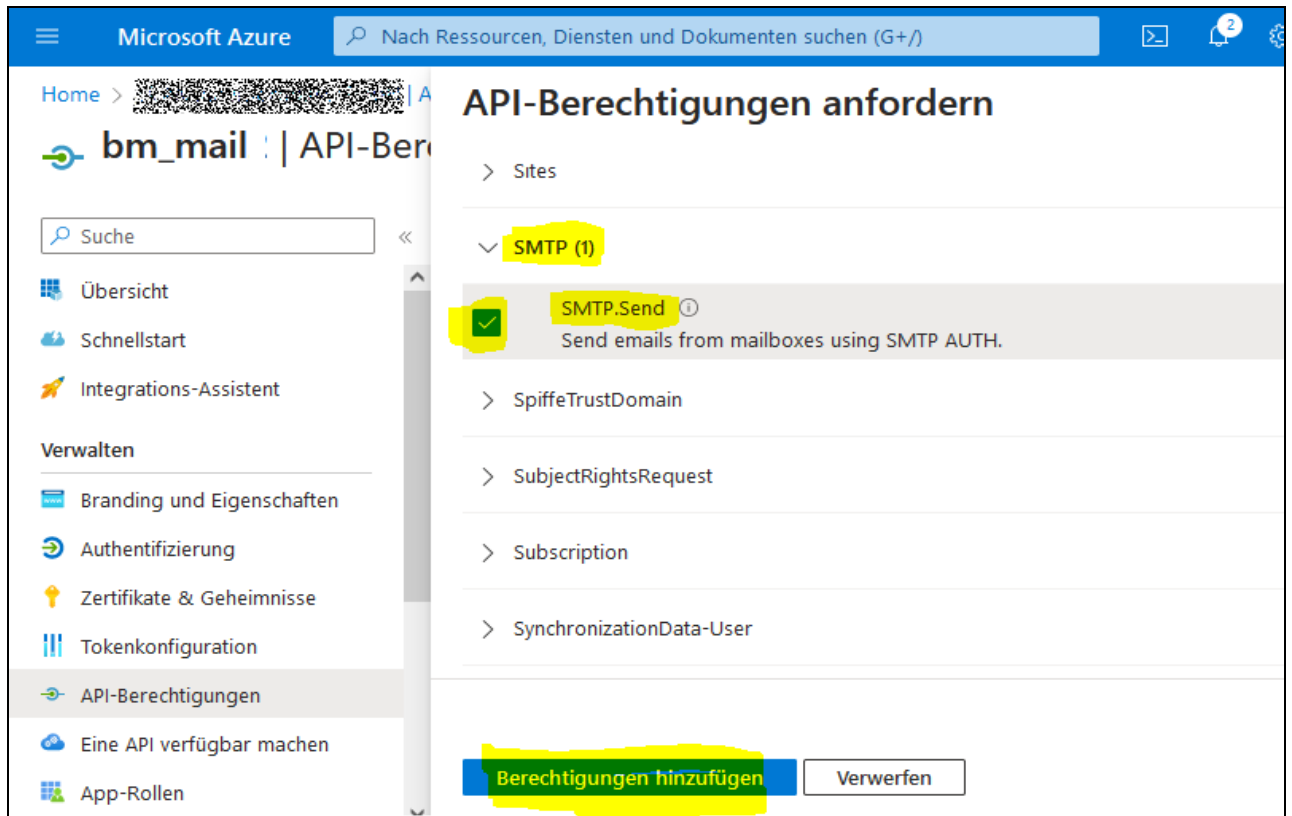


Es öffnet sich eine Liste mit Berechtigungen. Wählen Sie unter „POP“ die Option „POP.AccessAsUser.All“ aus.

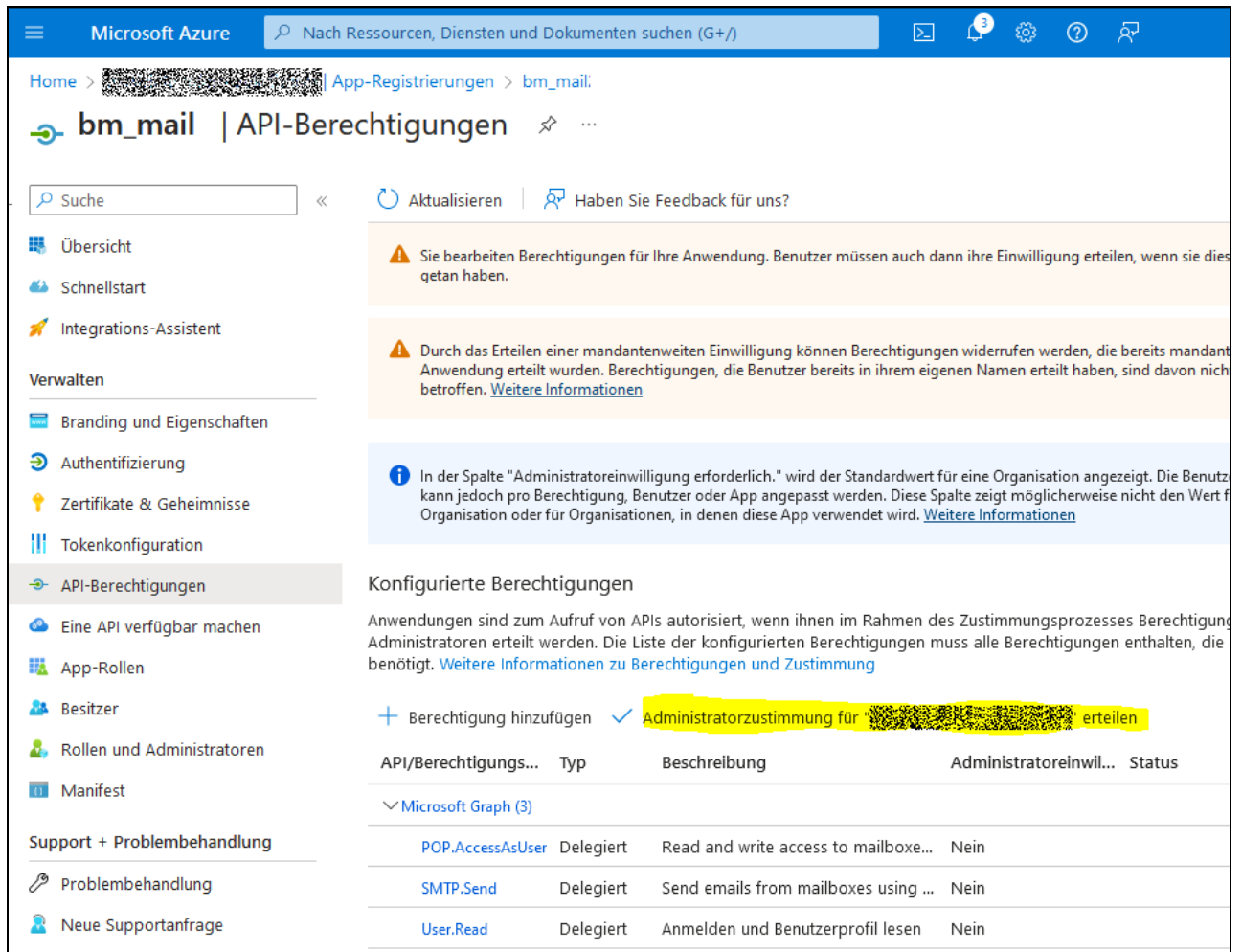


Wählen Sie zusätzlich unter „SMTP“ die Option „SMTP.Send“ aus und betätigen Sie die Schaltfläche am unteren Rand „Berechtigungen hinzufügen“.





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



## 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

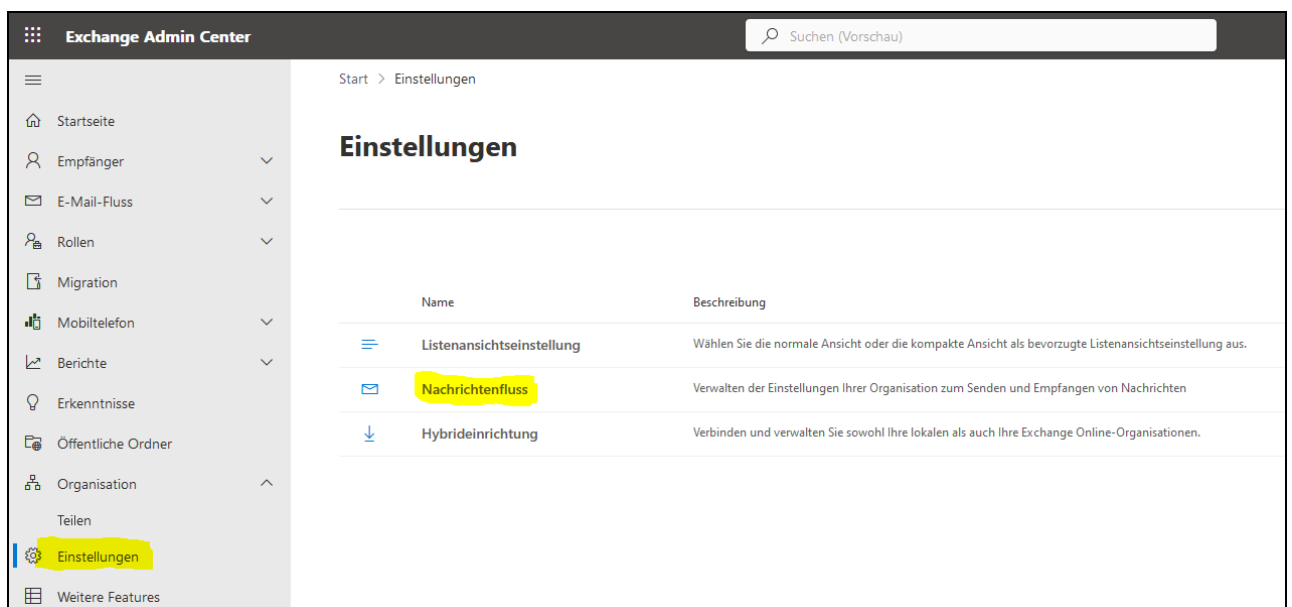
Für Microsoft-Mailkonten gelten außerdem folgende Einstellungen im bm:

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

- POP3 Sichere Verbindung: STARTTLS
- SMTP Server: Smtplib.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:



- 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“

**Nachrichtenflusseinstellungen**

Verwalten Sie die Einstellungen Ihrer Organisation zum Senden und Empfangen von Nachrichten.

**Allgemein**

Deaktivieren Sie die Plus-Adressierung für Ihre Organisation. [Weitere Informationen](#)

Senden von Aliasnamen aktivieren

**Sicherheit**

**Deaktivieren des SMTP-AUTH-Protokolls für Ihre Organisation**

Aktivieren Sie die Verwendung von Legacy-TLS-Clients. [Weitere Informationen](#)

**Schutz vor einer „Allen antworten“-Welle**

Schutz vor einer „Allen antworten“-Welle aktivieren

Mindestanzahl von Empfängern (1000 bis 5000)

Mindestanzahl für „Allen antworten“ (2 bis 20)

Blockdauer (1 bis 24 Stunden)

**Nachrichtenrückruf**

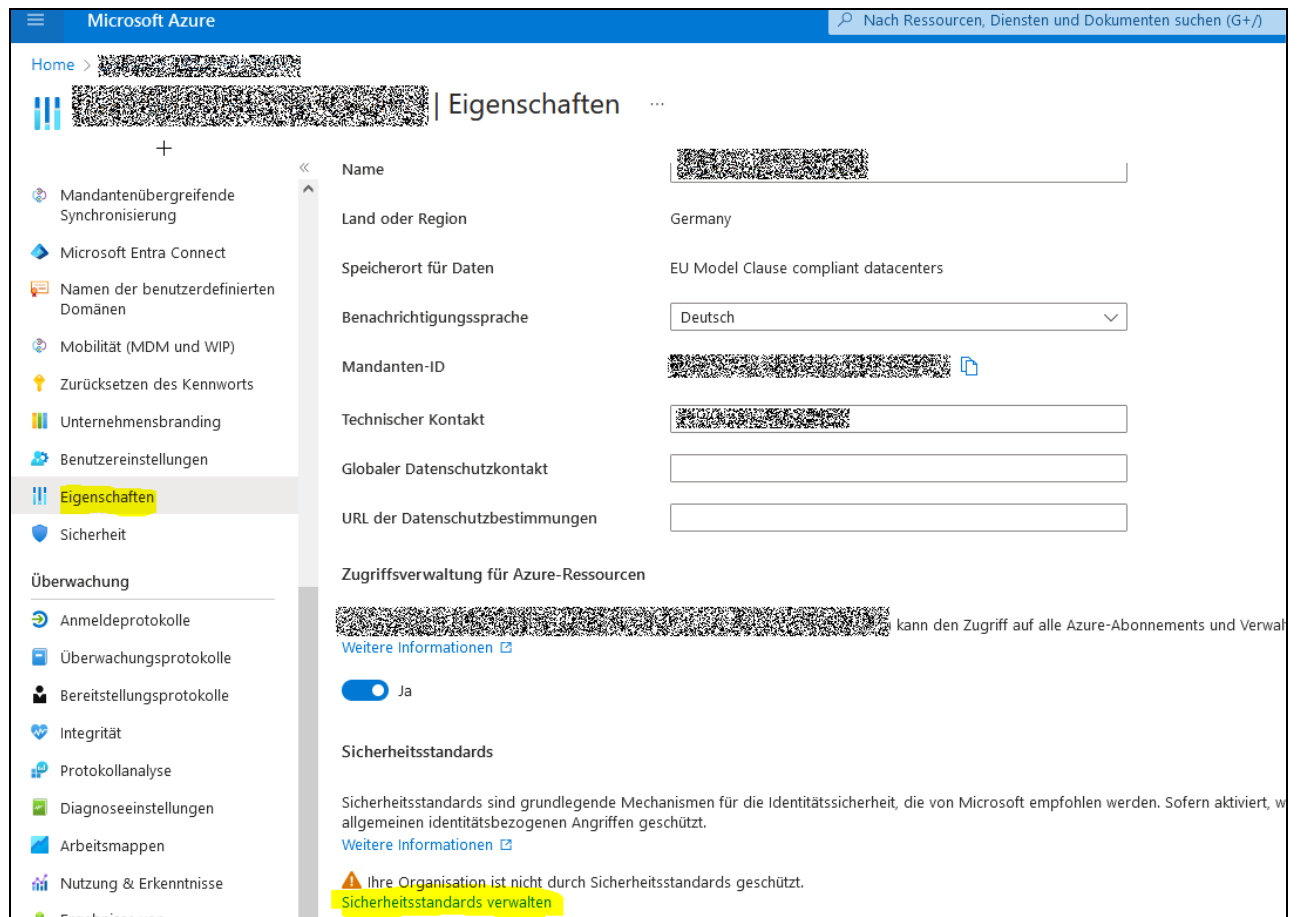
Cloudbasierten Nachrichtenrückruf aktivieren

Ermöglichen Sie Benutzern, vom Empfänger gelesene Nachrichten zurückzurufen

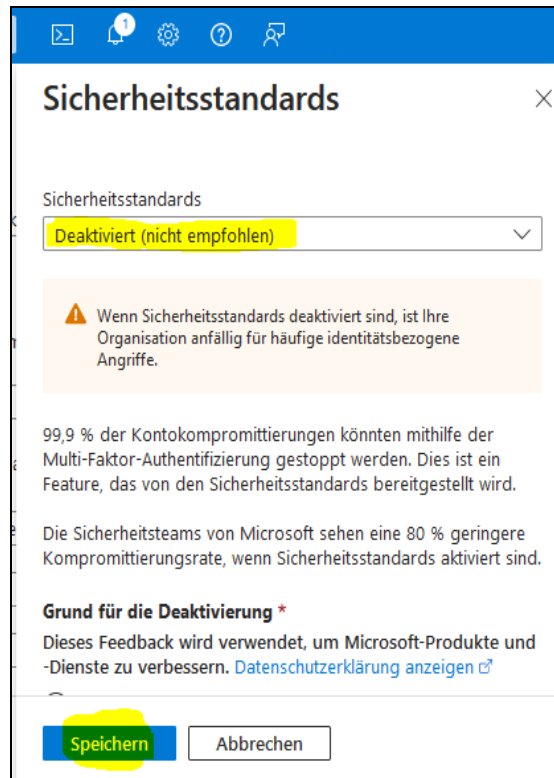
**Speichern**

- 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:



- 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.