

# Konfiguration Authentication Code Flow (delegated) MS Graph API

## Konfiguration in Squeeze

Diese Konfigurationsoberfläche wird ab der Version 2.3.0 bereitgestellt.

Wenn Sie diese Authentifizierungsmethode nutzen möchten, stellen Sie sicher, dass der Interne Job **refresh-tokens** aktiviert ist. Dies ist weiter unten im Artikel dokumentiert.

## Emailkonten anlegen



Dokumentenklasse

Eingangsrechnungend



Protokoll

Microsoft Graph API Delegated



Postfach \*

r[REDACTED]@dexpro.de

Client Secret \*

[REDACTED]



Client ID \*

[REDACTED]

Tenant ID \*

[REDACTED]

Posteingang \*

TestOAuth

Verarbeitet \*

Bearbeitet

Fehler \*

Error

Abbrechen

Speichern

---

Wie man nun erkennt, kann man in der Konfigurations-Oberfläche unter Protokoll zwei Arten der Anbindung zu Microsoft(MS) Graph API wählen:

Protokoll

Microsoft Graph API Delegated

IMAP

EWS

Microsoft Graph API

Microsoft Graph API Delegated

Deaktiviert

Für den delegierten Autorisierungsprozess wählen wir **Microsoft Graph API Delegated**. Im nächsten Schritt füllen wir die Felder Client ID, Client Secret die Tenant ID und die restlichen Felder.

## Ordner - Konfiguration

Bei der Ordnerkonfiguration müssen Sie drei Ordner angeben

Posteingang \*

Posteingang

Verarbeitet \*

Verarbeitet

Fehler \*

Fehler

### 1. **Posteingang**

Dieser Ordner wird regelmäßig überprüft, um die enthaltenen Emails zu importieren.

### 2. **Verarbeitet**

In diesen Ordner werden die erfolgreich importierten Emails verschoben.

### 3. **Fehler**

In diesen Ordner werden die Emails abgelegt, die nicht importiert werden konnten (z.B. fehlende Anlagen)

Bei der Definition der Ordner achten Sie bitte darauf, dass die Namen der Ordner eindeutig sein müssen, da die Ordner in der Verzeichnisstruktur des Postfachs gesucht werden. Ist ein konfigurierter Ordner nicht eindeutig kann es dies dazu führen, dass ein anderer

Ordner genutzt wird, als der gewünschte.

## Konfiguration in Entra ID (vormals Azure Active Directory)

Weitere notwendige Schritte für ein reibungslosen Ablauf sind die Einrichtung einer Entra ID Application

mit einem Client Secret. Die Globale Registrierung eines Mail-Dienstes der "Dexpro" im Entra ID-Directory des Kunden, wird vorerst nicht angeboten.

Zudem muss darauf geachtet werden dass die Applikation folgende Scopes besitzt.

### Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission    ✓ Grant admin consent for DEXPRO Solutions GmbH

API / Permissions name	Type	Description	Admin consent requ...	Status
▼ Microsoft Graph (5)				
Mail.ReadWrite	Delegated	Read and write access to user mail	No	...
Mail.ReadWrite.Shared	Delegated	Read and write user and shared mail	No	...
MailboxSettings.ReadWrite	Delegated	Read and write user mailbox settings	No	...
offline_access	Delegated	Maintain access to data you have given it access to	No	...
User.Read	Delegated	Sign in and read user profile	No	...

Anders als in den Permission für den Client Credential Flow ist jegliche Permission hier beschränkt auf den autorisierenden User.

**Merke:** Wenn auf ein Shared-Mailbox Postfach zugegriffen werden soll, muss das Shared-Mailbox Postfach unter Postfach eingetragen werden und die Application Permission Mail.Read.Write.Shared muss konfiguriert werden.

Denken Sie daran, dass die Shared-Mailbox auch Ihrer Email-Aktivierten Sicherheitsgruppe hinzugefügt wird, wenn Sie eine eingerichtet haben.

Ebenfalls ein maßgebender Unterschied zum Client Credential Flow ist hier die Verwendung einer **Redirect URI**.

Diese Redirect URI wird in der Entra ID unter der Applikation im Reiter Authentication angelegt:

[Got feedback?](#)[Overview](#)[Quickstart](#)[Integration assistant](#)**Manage**[Branding & properties](#)**Authentication**[Certificates & secrets](#)[Token configuration](#)[API permissions](#)[Expose an API](#)[App roles](#)[Owners](#)

### Platform configurations

Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URLs, specific authentication settings, or fields specific to the platform.

[+ Add a platform](#)

#### Web

##### Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. The redirect URI you send in the request to the login server should match one listed here. [Learn more about Redirect URIs and their restrictions](#)

[Add URI](#)

Hier ihr vollwertiger qualifizierter Domainname

### Schema Redirect URI:

`https://Ihr.vollwertiger.DomainName/api/v2/importers/email/authenticate/end`

**Merke:** Ein Squeeze Mandant benötigt immer eine Entra ID Applikation mit einer Redirect URI. Das bedeutet Sie müssen für jeden Mandanten eine Applikation anlegen.

## Autorisierungsprozess Authentication Code Flow

hat man nun seine Application in Entra ID konfiguriert und alle notwendigen Daten in die Konfigurationsoberfläche getippt kann man nun seine Konfiguration abspeichern.

1CE963E6-03D5-4702-8B72-D1197111

04131616-778C-40E7-B916-798D1CE64

Posteingang \*

TestOAuth

Verarbeitet \*

Bearbeitet

Fehler \*

Error

✕ Abbrechen

✓ Speichern

Nun öffnet sich ein weiteres Dialog Feld :













### Warnung



⚠ Die Authentifizierung muss separat gestartet werden, sonst kann keine Verbindung zu dem Microsoft Konto hergestellt werden.

✓ OK

Das System hat Ihre Konfiguration gespeichert, den Prozess der Authentifizierung müssen Sie jedoch separat über einen Button in der Email Konfiguration starten. Hierfür wählen Sie bitte den folgenden Button:

schlüsselung	Zertifikat prüfen	Benutzer	Passwort	Client ID	Tenant ID	Posteingang	Verarbeitet	Fehler	
						TestOAuth	Bearbeitet	Error	   
						Inbox	Bearbeitet	Error	   
						Posteingang	Verarbeitet	Fehler	   
						TestOAuth	Bearbeitet	Error	   
						TestOAuth	Bearbeitet	Error	   
						test	test	test	   

Nach einem Klick auf diesen Button werden Sie nun zur Oberfläche von Microsoft weitergeleitet. Dort beginnt der Authentifizierungsprozess befolgen Sie die Anweisungen von Microsoft:

Geben Sie ihre Email-Adresse an.



## Anmelden

[Sie können nicht auf Ihr Konto zugreifen?](#)

Weiter



Anmeldeoptionen

Geben Sie Ihr Passwort ein:

# DEXPRO



## Kennwort eingeben

.....

[Kennwort vergessen](#)

Anmelden

Je nach Unternehmen werden Sie ebenfalls aufgefordert eine 2-Faktor-Authentifizierung durchzuführen.:



# DEXPRO

## Überprüfen Ihrer Identität



SMS an +XX XXXXXXXXXX



Anrufen unter +XX XXXXXXXXXX

### Weitere Informationen

Sind Ihre Überprüfungsmethoden aktuell? Überprüfen sie unter <https://aka.ms/mfasetup>

Abbrechen

Sobald Sie Authentifiziert sind, werden die Berechtigungen abgefragt und Sie werden aufgefordert diese Berechtigungen zu bestätigen. Nach Ihrer Bestätigung leitet Microsoft umgehend zurück zur Squeeze-Oberfläche.

Die Oberfläche wird Ihnen nun anzeigen ob Squeeze nun Autorisiert ist oder ob ein Fehler aufgetreten ist:

### Erfolg



Graph Api is connected successfully

Mail ID: 13

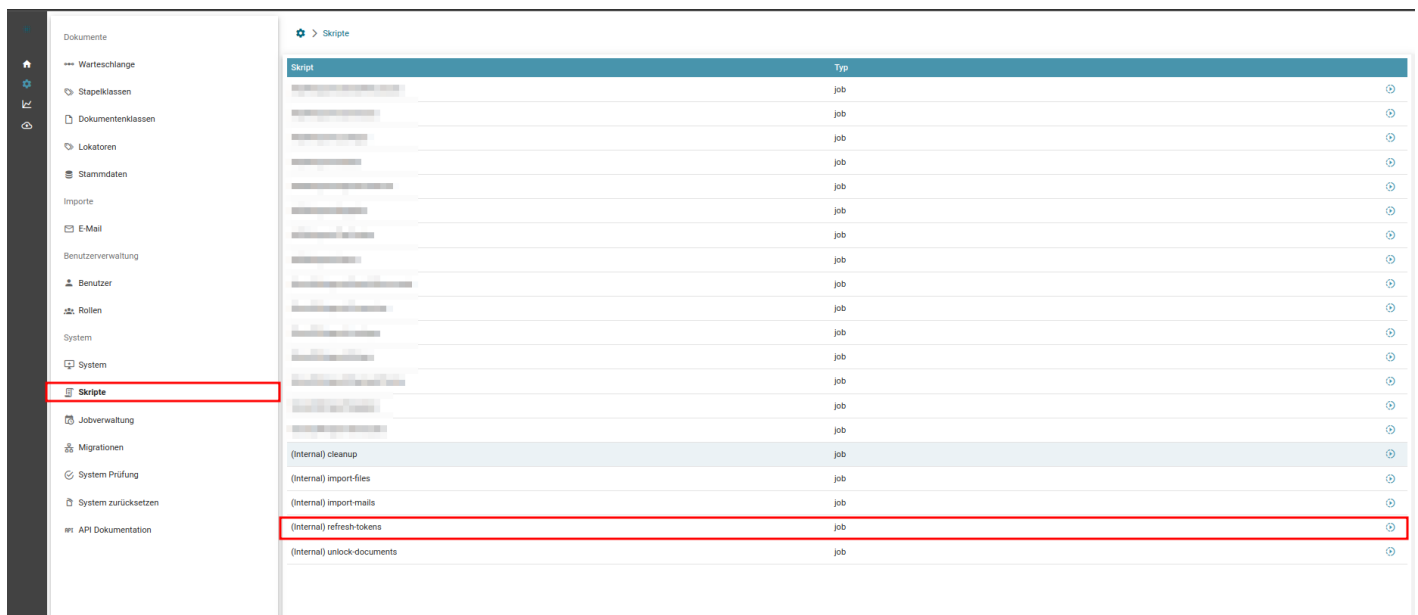
✓ OK

Nun können Sie die Mail Verbindung testen indem Sie den Mail Verbindungstest Button in der Oberfläche bedienen.

## Job-Konfiguration

Die Verwendung dieses Authentifizierungsverfahrens erfordert, dass ein separater Job aktiviert ist, welcher im Hintergrund die Zugriffsdaten für die Graph API aktuell hält.

Hierfür finden wir in der Administration unter "Skripte" das neue Skript mit den Namen **refresh-tokens**:



Skript	Typ
[redacted]	job
[redacted]	job
[redacted]	job
[redacted]	job
[redacted]	job
[redacted]	job
[redacted]	job
[redacted]	job
[redacted]	job
[redacted]	job
[redacted]	job
[redacted]	job
[redacted]	job
[redacted]	job
[redacted]	job
[redacted]	job
(Internal) cleanup	job
(Internal) import-files	job
(Internal) import-mails	job
(Internal) refresh-tokens	job
(Internal) unlock-documents	job

Dieses Skript kann man zu jedem Zeitpunkt manuell ausführen.

Sie müssen für dieses Skript einen Job einrichten, der häufig genug ausgeführt wird, um ein Ablaufen der Zugriffsdaten zu verhindern. Im Standard sind Refresh-Token von Microsoft 1 Tag lang gültig, es sollte also mehrmals am Tag versucht werden die Zugriffsdaten zu aktualisieren.

Bei geringerer Gültigkeit als 12 Std. muss per Projekt Change Request die Erneuerung eines Tokens auf eine passende kürzere Zeit von einem Consultant angepasst werden.

Wir empfehlen den Job jede Stunde auszuführen:

Cron-Ausdruck für den Job: **\*/50 \* \* \* \***

Wie Jobs zu konfigurieren sind, ist hier dokumentiert:

- [Artikel über Job Ausführungen in Squeeze](#)
- [Artikel über Job Steuerungen](#)

# Fragen und Antworten

Was passiert wenn der Job ausfällt ?	Ist der Job durch unvorhersehbare Gründe nicht gelaufen so müssen Sie sich neu Authentifizieren mit dem Authentifizierung-Button in der Email-Konfiguration
Kann ich einfach meine Postfach in der Konfiguration ändern und muss ich danach was tun ?	Sobald Sie die Konfiguration ändern oder abspeichern, weist die Anwendung Sie darauf hin, ein neuen Authentifizierungsprozess einzuleiten. Lehnen Sie dieses Aufforderung ab, haben Sie immer noch die Möglichkeit den Authentifizierungsbutton zu betätigen.
Kann ich meine Entra ID Applikation für mehrere Squeeze Mandanten nutzen ?	<p>Nein, die Verwendung einer Entra ID Applikation für mehrere Mandanten ist nicht Möglich, solange die Mandanten unter anderen Domänen erreichbar sind.</p> <p><b>Beispiel:</b></p> <p><u>1 Mandant:</u> test.mandant.squeeze.one</p> <p><u>2 Mandant:</u> test2.mandant.squeeze.one</p> <p>In diesem Beispiel kann man keine Application verwenden, da wir pro Application nur einen Mandanten ansprechen können. Ein Authentifizierung bei Microsoft würde ggf. immer nur auf einen Mandanten laufen.</p> <div>Du hast die Möglichkeit mehrere Postfächer mit der selben Applikation zu nutzen, dort gibt es keine Begrenzungen.</div>

Meine Zugriff durch die AzureTokens laufen ständig ab, obwohl ich den Job richtig konfiguriert habe.

Es kann vorkommen, dass die Server Zeit und die konfigurierte Zeit der Squeeze Applikation sich unterscheiden.

**Beispiel:**

Server Zeit: CEST (UTC +2)

Squeeze Zeit: UTC (UTC +0)

In diesem Fall werden die Tokens, die erzeugt wurden, in CEST abgespeichert. Wenn in diesem Fall die Squeeze Applikation nun prüft, ob ein Token erneuert werden muss, dann wird diese in diesem Fall den Token als noch nicht abgelaufen ansehen, da der Token in der Annahme von Squeeze gültig ist.

Das liegt daran, dass Squeeze den Token in der Vergangenheit mit UTC (+0) prüft aber der Token wurde mit CEST (+2) ausgestellt. Der Token ist demnach schon abgelaufen, da die Squeeze Applikation in der zeitlichen Vergangenheit hängt.

Das Problem wurde mit der Version 2.5 behoben.

Sollten Sie diese Version noch nicht besitzen, versuchen Sie die Serverzeit mit der Applikationszeit zu synchronisieren.

Dazu kann die Zeitzone in der php.ini gesetzt werden.

Siehe:

<https://www.php.net/manual/en/datetime.configuration.php>

Revision #22

Created 7 November 2022 13:33:33 by Vahdettin Balum

Updated 7 March 2025 12:57:35 by Simon Pust