

E-Mail über Microsoft 365

Microsoft hat die Anmeldung mit Benutzer und Kennwort für SMTP abgeschaltet. Für Postfächer in Microsoft 365 führt deshalb einer der beiden folgenden Wege zum Ziel. Beide brauchen einmalig eine **App-Registrierung** im Azure-Portal.

Welchen Weg wählen

	OAuth	App-Only
Versand als	ein angemeldetes Benutzerkonto	die Anwendung selbst
Anmeldung	einmalig im Browser	keine
Absender	das angemeldete Postfach	ein frei angegebenes Postfach
Nötige Rechte	Delegiert: SMTP.Send, offline_access	Anwendung: Mail.Send

Für einen Server, der jahrelang unbeaufsichtigt läuft, ist **App-Only** der robustere Weg: Es hängt kein Benutzerkonto daran, das gesperrt werden oder das Kennwort wechseln könnte.

App-Only mit Mail.Send als Anwendungsberechtigung erlaubt der Registrierung, als **jedes** Postfach der Organisation zu senden. Wer das eng ziehen will, beschränkt die Registrierung in Exchange Online über eine Anwendungszugriffsrichtlinie auf das eine Absenderpostfach. Das gehört mit der Microsoft-365-Administration abgestimmt.

Weg 1 — OAuth

E-Mail

?

STANDARD

M365-OAUTH

Tenant ID

Redirect URI

/api/settings/oauth/redirect

Client ID

Client Secret

Empfänger

Betreff

Interval

VERBINDEN

1. App registrieren

Im Azure-Portal eine neue App-Registrierung anlegen, mit einem eindeutigen Namen. Als **Umleitungs-URI** wird die Adresse dieser FINN.ghost-Installation eingetragen, endend auf `/api/mail/oauth/redirect`:

`https://finn.kunde.de:8083/api/mail/oauth/redirect`

[Home](#) > [App-Registrierungen](#) >

Anwendung registrieren

* Name

Der dem Benutzer gezeigte Anzeigename für diese Anwendung. (Dieser kann später geändert werden.)

FINN.ghost ✓

Unterstützte Kontotypen

Wer kann diese Anwendung verwenden oder auf diese API zugreifen?

- ☒ Nur Konten in diesem Organisationsverzeichnis (nur "DAKO-IT 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.

Web

`https://192.168.2.35:8083/api/settings/oauth/redirect` ✓

Registrieren Sie eine App, an der Sie gerade arbeiten. Integrieren Sie Katalog-Apps und andere Apps von außerhalb Ihrer Organisation, indem Sie sie aus [Unternehmensanwendungen](#) hinzufügen.

Die Umleitungs-URI muss **zeichengenau** mit der Adresse übereinstimmen, unter der FINN.ghost erreichbar ist — samt Port. Weicht sie ab, bricht Microsoft die Anmeldung mit einer Meldung zur Redirect-URI ab. Das ist der häufigste Stolperstein.

In älteren Fassungen dieser Anleitung endete die Adresse auf `/api/settings/oauth/redirect`. Das gilt nicht mehr — der Pfad lautet `/api/mail/oauth/redirect`.

2. Clientschlüssel erstellen

Unter **Zertifikate & Geheimnisse** einen neuen Clientschlüssel anlegen und den **Wert** sofort notieren.

Haben Sie Feedback für uns?

- Übersicht
- Schnellstart
- Integrations-Assistent
- Diagnose und Problembehandlung
- Verwalten
 - Branding und Eigenschaften
 - Authentifizierung
 - Zertifikate & Geheimnisse**
 - Tokenkonfiguration
 - API-Berechtigungen
 - Eine API verfügbar machen
 - App-Rollen
 - Besitzer
 - Rollen und Administratoren
 - Manifest
- Support + Problembehandlung

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
ClientSecret	2.11.2025	mXq8Q~95Q1r-JVbb5D5G_0avETfKvPt...	b274505b-4e72-4328-a261-6a102e3897...

Der Wert wird nur einmal angezeigt. Wer ihn nicht notiert, muss einen neuen Schlüssel anlegen. Clientschlüssel laufen außerdem ab — das Ablaufdatum gehört notiert, sonst bleibt der Mailversand irgendwann ohne Vorwarnung stehen.

3. Berechtigungen setzen

Unter **API-Berechtigungen** zwei delegierte Berechtigungen von **Microsoft Graph** hinzufügen und die Zustimmung erteilen:

Berechtigung	Wofür
SMTP.Send	Mails über SMTP AUTH senden
offline_access	Zugriff behalten, ohne erneute Anmeldung

Suche

Aktualisieren

Haben Sie Feedback für uns?

Übersicht

Schnellstart

Integrations-Assistent

Diagnose und Problembehandlung

Verwalten

Branding und Eigenschaften

Authentifizierung

Zertifikate & Geheimnisse

Tokenkonfiguration

API-Berechtigungen

Eine API verfügbar machen

App-Rollen

Besitzer

Rollen und Administratoren

Manifest

Support + Problembehandlung

Die Administratoreinwilligung wurde für die angeforderten Berechtigungen erfolgreich erteilt.

Durch das Erteilen einer mandantenweiten Einwilligung können Berechtigungen widerrufen werden, die bereits mandantenweit für diese Anwendung erteilt wurden. Berechtigungen, die

In der Spalte "Administratoreinwilligung erforderlich." wird der Standardwert für eine Organisation angezeigt. Die Benutzereinwilligung kann jedoch pro Berechtigung, Benutzer oder App

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

Administratorzustimmung für "DAKO-IT GmbH" erteilen

API/Berechtigungsname	Typ	Beschreibung	Administratoreinwill...	Status
Microsoft Graph (3)				
offline_access	Delegiert	Zugriff auf Daten beibehalten, für die Sie Zugriff erteilt ha...	Nein	Gewährt für "DAKO-IT G..."
SMTP.Send	Delegiert	Send emails from mailboxes using SMTP AUTH.	Nein	Gewährt für "DAKO-IT G..."
User.Read	Delegiert	Anmelden und Benutzerprofil lesen	Nein	Gewährt für "DAKO-IT G..."

Um die genehmigten Berechtigungen für einzelne Apps sowie die Einwilligungseinstellungen Ihres Mandanten anzuzeigen und zu verwalten, testen Sie [Unternehmensanwendung](#).

`User.Read` steht dort in der Regel schon — es wird beim Anlegen der Registrierung mitgegeben und kann bleiben. Wichtig ist der grüne Haken bei *Status*: ohne erteilte Zustimmung greifen die Berechtigungen nicht.

4. Werte übertragen

Aus dem Reiter **Übersicht** der Registrierung:

Feld in Azure	Feld in FINN.ghost
Anwendungs-ID (Client)	Client ID
Verzeichnis-ID (Mandant)	Tenant ID
beim Anlegen hinterlegte Umleitungs-URI	Redirect URI
notierter Wert des Clientschlüssels	Client Secret

E-Mail

?

STANDARD

M365-OAUTH

Tenant ID

Redirect URI

https://192.168.2.35:8083

/api/settings/oauth/redirect

Client ID

6f54d764-cf17-4137-94eb-53537a0eff3d

Client Secret

mXq8Q~95Q1r-JVbb5D5G_0avETfkVdPtWx9HhaYG

Empfänger

info@dako-it.com

Betreff

FINN.ghost

Interval

10

VERBINDEN

5. Verbinden

Nach dem Klick auf **Verbinden** fragt Microsoft nach der Anmeldung. Danach steht die Verbindung, und in der Karte erscheint die Adresse des verbundenen Kontos.

Angemeldet wird das Postfach, aus dem gesendet wird. Es muss ein Postfach in derselben Organisation sein.

Weg 2 — App-Only

E-Mail 

?

STANDARD

M365-OAUTH

M365-APP-ONLY

Tenant ID

Absender-E-Mail

Client ID

Client Secret

Empfänger

Betreff

Interval

VERBINDEN

1. App registrieren

Wie oben eine neue App-Registrierung mit eindeutigem Namen. Eine Umleitungs-URI wird hier **nicht** gebraucht.

Anwendung registrieren ...

* Name

Der dem Benutzer gezeigte Anzeigename für diese Anwendung. (Dieser kann später geändert werden.)

 

Unterstützte Kontotypen

Kontotypen auswählen, die diese Anwendung verwenden oder auf diese API zugreifen können

[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 aus [Unternehmensanwendungen](#) hinzufügen.

2. Clientschlüssel erstellen

Unter **Zertifikate & Geheimnisse**, Wert notieren.

Zertifikate (0)

Geheime Clientschlüssel (0)

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
Für diese Anwendung wurden keine Clientgeheimnisse erstellt.			

3. Berechtigung setzen

Unter **API-Berechtigungen** eine **Anwendungsberechtigung** von Microsoft Graph hinzufügen und die Zustimmung erteilen:

Berechtigung			Typ	
Mail.Send			Anwendung	

Alle der benötigten Berechtigungen muss die Berechtigungen erteilen, die die Anwendung benötigt. Mehrere Berechtigungen erfordern eine Zustimmung.

+

 Berechtigung hinzufügen

✓

 Administratorzustimmung für "DAKO-IT GmbH" erteilen

API/Berechtigungsname	Typ	Beschreibung	Administratoreinwill...	Status
Microsoft Graph (2)				
Mail.Send	Anwendung	Send mail as any user	Ja	⚠ Für "DAKO-IT GmbH" ni...
User.Read	Delegiert	Anmelden und Benutzerprofil lesen	Nein	

Anwendungsberechtigungen brauchen immer die **Administratorzustimmung**. Ohne sie schlägt der Versand mit einer Rechtemeldung fehl, obwohl alle Werte richtig eingetragen sind.

4. Werte übertragen

Feld in Azure	Feld in FINN.ghost
Anwendungs-ID (Client)	Client ID
Verzeichnis-ID (Mandant)	Tenant ID
Wert des Clientschlüssels	Client Secret
—	Absender-E-Mail

STANDARD M365-OAUTH M365-APP-ONLY		
Tenant ID 4232457f-dc03-493d-8193-ae7ebb12913e		Absender-E-Mail l.ruhle@dako-it.com
Client ID 865e8837-4d64-41e9-a6b4-839a69a4c495		Client Secret *****
Empfänger l.ruhle@dako-it.com	Betreff FINN.ghost	Intervall 0

TRENKEN

SPEICHERN

Die **Absender-E-Mail** ist das Postfach, aus dem gesendet wird.

Nach dem Speichern verschickt FINN.ghost eine Testmail an die eingetragenen Empfänger und bestätigt das in der Karte. Kommt sie nicht an, fehlt meist die Administratorzustimmung.

Über **Trennen** wird die Verbindung wieder gelöst.

Wenn der Versand nicht geht

Meldung oder Symptom	Ursache
Fehler zur Redirect-URI beim Verbinden	Umleitungs-URI weicht ab
Anmeldung geht, Versand scheitert	Berechtigung fehlt oder ohne Zustimmung
lief monatelang, jetzt nicht mehr	Clientschlüssel abgelaufen
App-Only meldet fehlende Rechte	Administratorzustimmung nicht erteilt
Absender wird abgelehnt	Postfach gehört nicht zur Organisation

Die Antwort von Microsoft steht im Protokoll. Siehe [Log Informationen](#).

Nächster Schritt

[EU-Auslands-Kontengruppen](#)