



DISPONIC®

DISPONIC

E-Mail-Versand über Microsoft 365 (OAuth)

Hinweise für Kunden

Stand: 09.10.2026

Inhaltsverzeichnis

1	WICHTIGER HINWEIS	1
2	WORUM ES GEHT	2
3	VORAUSSETZUNGEN	2
4	WAS DISPONIC BENÖTIGT	3
5	ECKPUNKTE DER EINRICHTUNG IN MICROSOFT 365	3
6	EINTRAGUNG IN DISPONIC	4
7	FUNKTIONSTEST	5
8	UNTERSTÜTZUNG DURCH DEN DISPONIC-SUPPORT	5
9	MICROSOFT-DOKUMENTATION	6

1 WICHTIGER HINWEIS

Dieses Dokument gibt Orientierung, ersetzt aber keine Einrichtungsanleitung. Die Konfiguration von Microsoft 365, Microsoft Entra ID und Exchange Online liegt vollständig in der Verantwortung des Kunden.

- Die Einrichtung darf nur durch Personen mit fundiertem Fachwissen zu Microsoft 365, Entra ID und Exchange Online erfolgen. Fehlt dieses Wissen, ziehen Sie bitte einen qualifizierten IT-Dienstleister hinzu.
- Maßgeblich ist stets die aktuelle Dokumentation von Microsoft (siehe Abschnitt „Microsoft-Dokumentation“). Portale, Menüpfade und Rollenbezeichnungen ändern sich häufig.
- Die Bite AG übernimmt keine Gewähr für Vollständigkeit oder Aktualität der Hinweise und keine Haftung für Einstellungen in der IT-Umgebung des Kunden.
- Sicherheitsentscheidungen (z. B. Umfang der Versandberechtigung) trifft der Kunde bzw. dessen IT-Sicherheit.

2 WORUM ES GEHT

Bei aktivem OAuth versendet DISPONIC E-Mails nicht über einen SMTP-Server, sondern über Microsoft Graph. DISPONIC meldet sich dabei als Anwendung (nicht als Benutzer) bei Microsoft Entra ID an und sendet aus einem festgelegten Exchange-Online-Postfach.

Merkmal	Angabe
DISPONIC	ab Version 6.6 (Oberfläche ab 7.x abweichend)
Microsoft	Microsoft 365 / Exchange Online, weltweite Cloud
Verfahren	OAuth 2.0 Client Credentials über Microsoft Graph
Nicht gemeint	SMTP AUTH mit OAuth, Anmeldung eines Benutzers

SMTP-Server, Port, SSL, Benutzername und Kennwort werden für diesen Versandweg nicht genutzt, auch wenn die Felder in DISPONIC sichtbar sind.

3 VORAUSSETZUNGEN

- Microsoft-Entra-Mandant mit Exchange Online.
- Ein echtes Exchange-Online-Postfach als Absender, idealerweise eine dedizierte Adresse (z. B. noreply@ihre-firma.de). Verwenden Sie die primäre SMTP-Adresse, keinen Alias und keine Verteilerliste.
- Administratorrechte für App-Registrierung und Administratoreinwilligung; für eine Einschränkung auf bestimmte Postfächer zusätzlich Exchange-Online-Administrationsrechte.
- Ausgehender HTTPS-Zugriff (TCP 443) vom DISPONIC-Server auf login.microsoftonline.com und graph.microsoft.com.
- Ein sicherer Weg, das Client-Secret direkt in DISPONIC einzutragen.



4 WAS DISPONIC BENÖTIGT

DISPONIC braucht genau vier Werte aus Ihrer Microsoft-365-Umgebung. |

DISPONIC-Feld	Bedeutung in Microsoft 365	Typische Verwechslung
Tenant	Verzeichnis-ID (Mandanten-ID) als GUID	Nicht die Domäne angeben
Client ID	Anwendungs-ID (Client-ID) der App-Registrierung	Nicht die Objekt-ID
Secret	Wert des Client-Secrets	Nicht die Geheimnis-ID (Secret-ID)
Absender	Primäre SMTP-Adresse eines Exchange-Online-Postfachs	Kein Alias, keine Gruppe

5 ECKPUNKTE DER EINRICHTUNG IN MICROSOFT 365

Die folgenden Punkte zeigen, was eingerichtet werden muss. Wie es im Detail umgesetzt wird, entnimmt Ihre Microsoft-365-Administration der verlinkten Microsoft-Dokumentation.

1. **App-Registrierung** in Microsoft Entra ID anlegen: nur ein Mandant (Single Tenant), keine Umleitungs-URL erforderlich.
2. **Client-Secret** erzeugen. Der Wert wird nur einmal angezeigt. Microsoft begrenzt die Laufzeit auf höchstens 24 Monate; legen Sie Ablaufdatum und Verantwortlichen für die Erneuerung fest. DISPONIC unterstützt Client-Secrets, keine Zertifikate.
3. **Versandberechtigung** erteilen. Benötigt wird ausschließlich die Microsoft-Graph-Anwendungsberechtigung Mail.Send. Dabei gibt es zwei Wege:

Variante	Wirkung	Hinweis
Tenantweit (Mail.Send mit Administratoreinwilligung in Entra ID)	App darf grundsätzlich als jedes Postfach im Mandanten senden	Einfach, aber weitreichend; nur bei bewusster Entscheidung des Kunden
Eingeschränkt über Exchange Online RBAC for Applications (empfohlen)	App darf nur aus festgelegten Postfächern senden	Erfordert Exchange Online PowerShell; Nachfolger der Application Access Policies



Wichtig bei der eingeschränkten Variante:

- Die tenantweite Mail.Send-Berechtigung darf in Entra ID **nicht** zusätzlich erteilt sein. Beide Berechtigungen wirken additiv; die tenantweite hebt die Einschränkung sonst auf.
- Die Zuweisung in Exchange erfolgt auf den Dienstprinzipal der Unternehmensanwendung. Dessen Objekt-ID unterscheidet sich von der Objekt-ID der App-Registrierung.
- Erlaubte Postfächer werden typischerweise über eine E-Mail-aktivierte Sicherheitsgruppe festgelegt; verschachtelte Gruppen werden nicht berücksichtigt.
- Microsoft stellt mit Test-ServicePrincipalAuthorization eine Prüfmöglichkeit bereit. Änderungen können im Betrieb verzögert wirksam werden.

6 EINTRAGUNG IN DISPONIC

- **Version 6.x:** In den E-Mail-Einstellungen „OAuth verwenden“ aktivieren und Client ID, Tenant und Secret eintragen. In jedem relevanten Versandbereich die zugelassene Absenderadresse hinterlegen.
- **Ab Version 7.x:** Die OAuth-Daten stehen in den SMTP-Server-Einstellungen. Einen Eintrag anlegen (z. B. „Microsoft 365 OAuth“), OAuth aktivieren und die drei Werte eintragen. Diesen Eintrag in den E-Mail-Einstellungen der Versandbereiche auswählen und dort den zugelassenen Absender hinterlegen.

Der Eintrag heißt weiterhin „SMTP-Server“, obwohl der Versand technisch über Microsoft Graph läuft. Adresse, Port und SSL spielen dabei keine Rolle.



7 FUNKTIONSTEST

Senden Sie nach dem Speichern eine Test-E-Mail an eine interne Adresse, genau mit dem in Microsoft 365 zugelassenen Absender.

- ☐ Secret: Wert eingetragen, nicht die Secret-ID
- ☐ Tenant-ID und Client-ID sind GUIDs und stammen aus derselben App-Registrierung
- ☐ Absender ist ein vorhandenes, für die App zugelassenes Postfach
- ☐ Test-E-Mail ist intern angekommen (Absender, Betreff, Anhänge geprüft)
- ☐ Bei eingeschränkter Variante: nicht zugelassenes Postfach wird abgelehnt
- ☐ Ablaufdatum des Secrets und Verantwortlicher für die Erneuerung dokumentiert

Nimmt Microsoft Graph eine Nachricht an, ist sie noch nicht zwingend zugestellt. Bei fehlender Zustellung prüfen Sie Nachrichtenablaufverfolgung, Quarantäne und Empfängersystem. Beim Erneuern des Secrets das neue zuerst testen, dann das alte entfernen.

8 UNTERSTÜTZUNG DURCH DEN DISPONIC-SUPPORT

Der DISPONIC-Support unterstützt bei der Konfiguration innerhalb von DISPONIC, nicht bei der Einrichtung Ihrer Microsoft-365-Umgebung. Administratorkennwörter benötigen wir nicht. Für eine Fehleranalyse helfen uns:

- DISPONIC-Version
- Tenant-ID und Client-ID
- konfigurierte Absenderadresse
- gewählte Berechtigungsvariante (tenantweit oder eingeschränkt)
- Zeitpunkt des Tests und vollständiger Fehlertext

Den Secret-Wert bitte nie per E-Mail oder Ticket senden, sondern direkt in DISPONIC eintragen oder nur über einen freigegebenen sicheren Weg übergeben.



9 MICROSOFT-DOKUMENTATION

Maßgeblich für die Einrichtung in Microsoft 365 sind diese Seiten in ihrer jeweils aktuellen Fassung:

- [Anwendung bei der Microsoft Identity Platform registrieren](#)
- [OAuth 2.0 Client-Credentials-Flow](#)
- [Microsoft Graph: user sendMail](#)
- [Microsoft Graph Berechtigungsreferenz](#)
- [Exchange Online RBAC for Applications](#)
- [Microsoft-365-URLs und IP-Adressbereiche](#)