MailBridge 365 – Microsoft-365-Einrichtung

ERPAUSTRIA
Business solutions]

Dokumentversion 1.4 · Stand 16. September 2026

Technikerunterlage für App-Registrierung, Microsoft-Graph-Berechtigungen, EWS-Proxy und sichere Datenübergabe für die Installation am Windows Server.

Ziel dieser Anleitung

MailBridge 365 ist ein lokaler Windows-Dienst. Er stellt bestehenden Anwendungen SMTP AUTH, POP3, einen HTTPS-Webclient und einen EWS-kompatiblen Endpunkt zur Verfügung. Der EWS-Proxy übersetzt unterstützte EWS-Anfragen intern auf Microsoft Graph. Gegenüber Microsoft 365 meldet sich der Dienst ohne interaktive Benutzeranmeldung über OAuth2 an.

Nach Abschluss dieser Anleitung sind:

- eine eigene Anwendung im richtigen Microsoft-Entra-Tenant registriert,
- die benötigten Microsoft-Graph-Anwendungsberechtigungen eingerichtet,
- die tenantweite Administratorzustimmung erteilt,
- ein Client Secret erstellt und sicher übergeben,
- die verwendeten Postfächer und Funktionen dokumentiert,
- EWS-, Graph-, Cache- und Synchronisationseinstellungen festgelegt,
- alle Informationen für die Installation am Windows Server vorhanden.

> **Wichtig:** Der Connector benötigt keine persönlichen Microsoft-365-Benutzerkennwörter. Tenant-ID, Client-ID und Client-Secret-Wert gehören zur registrierten Anwendung.

Aktueller Microsoft-Zeitplan für EWS

Microsoft beginnt am **1. Oktober 2026** mit der stufenweisen Sperre von EWS in Exchange Online. Am **1. April 2027** wird EWS in Exchange Online vollständig und dauerhaft abgeschaltet. Die Übergangseinstellungen `EWSEnabled` und `EWSAllowedAppIDs` können bestehende direkte EWS-Anwendungen nur vorübergehend weiter zulassen und ersetzen keine Migration.

MailBridge 365 verwendet EWS nicht für die Verbindung zu Microsoft 365. Der EWS-kompatible Endpunkt befindet sich ausschließlich lokal zwischen der Bestandsanwendung und MailBridge 365. Die Verbindung von MailBridge 365 zu Exchange Online erfolgt über OAuth2 und Microsoft Graph. Für MailBridge 365 selbst muss daher keine App-ID in `EWSAllowedAppIDs` eingetragen werden.

Andere Anwendungen im Kunden-Tenant, die weiterhin direkt per EWS auf Exchange Online zugreifen, müssen separat ermittelt und bewertet werden. Microsoft hat keinen allgemeinen Termin veröffentlicht, an dem jede einzelne EWS-Funktion vollständig oder identisch in Graph verfügbar sein soll. Der Funktionsumfang muss deshalb für jede Bestandsanwendung getestet werden.

- Microsoft-Zeitplan zur EWS-Abschaltung
- EWSAllowedAppIDs für die Übergangsphase
- Microsoft-Leitfaden zur EWS-Graph-Migration

Inhaltsübersicht

1. Auftrag und Voraussetzungen
2. App in Microsoft Entra ID registrieren
3. Microsoft-Graph-Berechtigungen vergeben
4. Administratorzustimmung erteilen
5. Client Secret erstellen und sichern
6. Postfachzugriff sinnvoll begrenzen
7. Datenübergabe an den Windows-Techniker
8. Vorbereitung und Einrichtung am Windows Server
9. Abnahme und Funktionstest
10. Fehlerzuordnung
11. Secret-Erneuerung
12. Offizielle Microsoft-Quellen

---

1. Auftrag und Voraussetzungen

Funktionsweise

```
Bestehende Anwendung
        |
        | SMTP AUTH / POP3 / EWS / HTTPS-Webclient
```

```
        v
MailBridge 365 auf dem Windows Server
        |
        | OAuth2 Client Credentials / HTTPS
        v
Microsoft Entra ID und Microsoft Graph
        |
        v
Exchange Online
```

Der Connector arbeitet als Hintergrunddienst mit einer eigenen Anwendungsidentität. Es findet keine interaktive Microsoft-365-Benutzeranmeldung statt. Deshalb werden **Anwendungsberechtigungen** benötigt.

Voraussetzungen in Microsoft 365

- Aktiver Microsoft-365-Tenant mit Exchange Online
- Mindestens ein verwendbares Benutzer-, Shared- oder Funktionspostfach
- Konto mit Berechtigung zum Erstellen einer App-Registrierung
- Konto mit Berechtigung zum Erteilen einer tenantweiten Administratorzustimmung
- Festgelegte Microsoft-365- und Exchange-Ansprechperson

Wenn die Schaltfläche für die Administratorzustimmung deaktiviert ist, muss ein entsprechend berechtigter Microsoft-Entra-Administrator den betreffenden Schritt durchführen.

Voraussetzungen am Windows Server

- Unterstütztes Windows-System mit .NET Framework 4.8
- Lokale Administratorrechte für Installation und Dienstverwaltung
- Funktionierende DNS-Auflösung und korrekte Systemzeit
- Ausgehendes HTTPS über TCP-Port 443
- Erreichbarkeit von `login.microsoftonline.com` und `graph.microsoft.com`
- Bei großen Nachrichten gegebenenfalls Erreichbarkeit von durch Graph bereitgestellten Upload-Endpunkten unter `outlook.office.com`
- Fester Programm- und Datenpfad
- Schreibrechte des Windows-Dienstkontos im Datenpfad
- Festgelegte lokale SMTP-, POP3-, EWS-Proxy- und Webclient-Ports

Vor Beginn festlegen

- ☐ Welche Postfächer dürfen Nachrichten versenden?
- ☐ Welche Postfächer dürfen über POP3 oder den Webclient gelesen werden?
- ☐ Welche ERP-Systeme verwenden den EWS-Proxy und welche Postfächer fragen sie ab?

☐ Soll EWS alle Nachrichten oder nur **Gesendete Elemente** bereitstellen?

☐ Sollen vom ERP versendete Nachrichten bei der Rücksynchronisation aus **Gesendete Elemente** unterdrückt werden, um Dubletten im ERP zu vermeiden?

☐ Werden Termine und Kontakte lesend benötigt?

☐ Ab welchem Datum und welcher Uhrzeit dürfen Mails beziehungsweise Termine bereitgestellt werden?

☐ Sollen abgerufene Nachrichten in Exchange als gelesen markiert werden?

☐ Dürfen Nachrichten nach erfolgreichem POP3-Abruf gelöscht werden?

☐ Darf ein POP3-Client mit `DELE` Nachrichten in Exchange löschen?

☐ Soll das lokale Journalpostfach aktiviert werden?

☐ Soll Exchange den App-Zugriff serverseitig auf bestimmte Postfächer begrenzen?

☐ Wer ist für die Erneuerung des Client Secrets verantwortlich?

Benötigte Microsoft-Graph-Rechte

Berechtigung	Typ	Verwendung
`Mail.Send`	Application / Anwendung	Versand aus den freigegebenen Exchange-Online-Postfächern
`Mail.ReadWrite`	Application / Anwendung	Abruf, Gelesen-Markierung, Löschung und Entwurfsverarbeitung großer Nachrichten
`User.Read.All`	Application / Anwendung	Anzeigename und sekundäre SMTP-, SIP-, X500- und weitere Proxyadressen für EWS `ResolveNames`
`Calendars.Read`	Application / Anwendung	Optional: lesender Terminabgleich über den EWS-Proxy
`Contacts.Read`	Application / Anwendung	Optional: lesender Kontaktabgleich über den EWS-Proxy

> **Keine Redirect URI erforderlich:** Der Connector verwendet den OAuth2 Client-Credentials-Flow. Unter **Authentication** / **Authentifizierung** muss keine Web-, SPA- oder Public-Client-Umleitungsadresse eingetragen werden.

---

2. App in Microsoft Entra ID registrieren

Microsoft Entra Admin Center öffnen

Öffnen Sie:

https://entra.microsoft.com

Kontrollieren Sie vor der Registrierung oben rechts, dass der **produktive Kunden-Tenant** ausgewählt ist. Eine registrierte Anwendung kann später nicht in einen anderen Tenant verschoben werden.

Navigation

```
Microsoft Entra Admin Center
> Entra ID
> App registrations / App-Registrierungen
> New registration / Neue Registrierung
```

Registrierung durchführen

1. Wählen Sie **New registration / Neue Registrierung**.
2. Vergeben Sie einen eindeutigen Namen, beispielsweise:

   ```
   MailBridge 365 - <Kundenname>
   ```

3. Wählen Sie als unterstützten Kontotyp:

   ```
   Accounts in this organizational directory only
   Nur Konten in diesem Organisationsverzeichnis
   ```

4. Lassen Sie **Redirect URI / Umleitungs-URI** leer.
5. Wählen Sie **Register / Registrieren**.
6. Nach dem Speichern öffnet sich die Übersichtsseite der App.

Werte sofort erfassen

Portalbezeichnung	Benötigter Wert	Hinweis
Directory (tenant) ID	Tenant-ID als GUID	Nicht mit der primären Microsoft-365-Domain verwechseln
Application (client) ID	Client-ID als GUID	Nicht die Object-ID verwenden
Display name	Anzeigename der App	Dient zum späteren Auffinden der Registrierung

> **Nicht verwechseln:** Für den Connector werden die **Directory (tenant) ID** und die **Application (client) ID** benötigt. Die **Object-ID** der App oder des Service

> Principals ist dafür nicht geeignet.

---

3. Microsoft-Graph-Berechtigungen vergeben

Navigation

```
App-Registrierung
> API permissions / API-Berechtigungen
> Add a permission / Berechtigung hinzufügen
```

Rechte hinzufügen

1. Wählen Sie **Microsoft Graph**.
2. Wählen Sie **Application permissions / Anwendungsberechtigungen**.
3. Wählen Sie ausdrücklich **nicht** die delegierten Berechtigungen.
4. Suchen Sie nach `Mail.Send` und markieren Sie diese Berechtigung.
5. Suchen Sie nach `Mail.ReadWrite` und markieren Sie diese Berechtigung.
6. Suchen Sie nach `User.Read.All` und markieren Sie diese Berechtigung.
7. Wenn Termine und Kontakte über den EWS-Proxy synchronisiert werden sollen, markieren Sie zusätzlich `Calendars.Read` und `Contacts.Read`.
8. Bestätigen Sie mit **Add permissions / Berechtigungen hinzufügen**.

Warum werden zwei Rechte benötigt?

`Mail.Send` erlaubt der Anwendung den Versand ohne angemeldeten Benutzer. Das Recht enthält jedoch keinen allgemeinen Lese- oder Änderungszugriff.

`Mail.ReadWrite` erlaubt Lesen, Erstellen, Aktualisieren und Löschen von Nachrichten ohne angemeldeten Benutzer. Es enthält aber keine Versandberechtigung.

`Calendars.Read` und `Contacts.Read` werden ausschließlich benötigt, wenn in der Connector-Konfiguration **Termine und Kontakte synchronisieren** aktiviert wird. Der Zugriff ist in dieser Ausbaustufe lesend.

Der Connector benötigt `Mail.ReadWrite` zusätzlich für:

- POP3- und Webclient-Abruf,
- Markieren als gelesen,
- Löschen von Exchange-Nachrichten,

- Erstellen und Verarbeiten von Entwürfen bei großen Nachrichten,
- Upload-Sitzungen für große Anhänge.

Nicht benötigtes Standardrecht entfernen

Falls nach der Registrierung noch `User.Read` vom Typ **Delegated / Delegiert** eingetragen ist, kann dieses Recht entfernt werden. Der Connector verwendet keine delegierte Benutzeranmeldung und benötigt es nicht.

> **Sicherheitswirkung:** Nach der Administratorzustimmung gelten die vergebenen Anwendungsberechtigungen grundsätzlich tenantweit. Der Connector verwendet nur die lokal konfigurierten Postfächer. Für eine zusätzlich durch Exchange erzwungene Begrenzung siehe Abschnitt 6.

---

4. Administratorzustimmung erteilen

Das bloße Hinzufügen der Berechtigungen reicht nicht aus. Anwendungsberechtigungen werden erst nach der tenantweiten Administratorzustimmung wirksam.

Navigation

```
App-Registrierung
> API permissions / API-Berechtigungen
```

Zustimmung durchführen

1. Wählen Sie **Grant admin consent for** `<Tenant>` beziehungsweise **Administratorzustimmung für** `<Tenant>` **erteilen**.
2. Kontrollieren Sie den Sicherheitsdialog.
3. Erwartet werden `Mail.Send`, `Mail.ReadWrite` und `User.Read.All` sowie bei aktiviertem Termin-/Kontaktabgleich zusätzlich `Calendars.Read` und `Contacts.Read`.
4. Klären Sie unerwartete zusätzliche Rechte, bevor Sie zustimmen.
5. Bestätigen Sie die Zustimmung.
6. Aktualisieren Sie die Ansicht.
7. Prüfen Sie bei beiden Rechten den grünen Status **Granted for** `<Tenant>` **/ Gewährt für** `<Tenant>`.

Erwarteter Sollzustand

Eintrag	Typ	Status

Microsoft Graph `Mail.Send`	Application	Granted for `<Tenant>`
Microsoft Graph `Mail.ReadWrite`	Application	Granted for `<Tenant>`
Microsoft Graph `User.Read.All`	Application	Granted for `<Tenant>`
Microsoft Graph `Calendars.Read`	Application	Optional, bei Terminabgleich: Granted for `<Tenant>`
Microsoft Graph `Contacts.Read`	Application	Optional, bei Kontaktabgleich: Granted for `<Tenant>`
Delegierte Rechte	Nicht benötigt	Keine erforderlich

> **Wenn die Schaltfläche deaktiviert ist:** Das verwendete Konto darf keine tenantweite Zustimmung erteilen. Eine Benutzerzustimmung reicht nicht aus. Ein berechtigter Entra-Administrator muss den Schritt durchführen.

> **Bei späteren Änderungen:** Werden die API-Berechtigungen geändert, muss die Administratorzustimmung erneut erteilt werden. Erst danach erscheinen die geänderten Rechte in neu ausgestellten Zugriffstokens.

---

5. Client Secret erstellen und sichern

Der aktuelle Connector authentifiziert sich mit einem Client Secret. Dieses wird bei der Einrichtung am Windows Server per DPAPI für den lokalen Computer verschlüsselt gespeichert.

Navigation

```
App-Registrierung
> Certificates & secrets / Zertifikate & Geheimnisse
> Client secrets
> New client secret / Neuer geheimer Clientschlüssel
```

Secret erstellen

1. Tragen Sie eine nachvollziehbare Beschreibung ein, beispielsweise:

   ```
   MailBridge 365 - Windows Server <SERVERNAME>
   ```

2. Legen Sie die Laufzeit fest.

3. Microsoft begrenzt Client Secrets auf maximal 24 Monate und empfiehlt eine Laufzeit unter 12 Monaten.
4. Wählen Sie **Add / Hinzufügen**.
5. Kopieren Sie unmittelbar den Inhalt der Spalte **Value / Wert**.
6. Dokumentieren Sie das Ablaufdatum.
7. Planen Sie mindestens 30 Tage vor Ablauf einen Termin zur Erneuerung ein.

> **Entscheidend - VALUE, nicht SECRET ID:** Der Windows-Techniker benötigt den Inhalt der Spalte **Value / Wert**. Die **Secret ID** ist nur eine Kennung und kann nicht als Kennwort verwendet werden.

Der Secret-Wert wird nach dem Verlassen der Seite nicht erneut angezeigt. Geht der Wert verloren, muss ein neues Secret erstellt werden.

Sichere Übermittlung

Der Secret-Wert darf nicht zusammen mit Tenant-ID und Client-ID in einer normalen E-Mail versendet werden.

Geeignete Übertragungswege sind beispielsweise:

- freigegebener Eintrag in einem Passwortmanager,
- zeitlich begrenzter Secret-Link,
- getrennte Übermittlung über einen zweiten Kommunikationskanal,
- direkte Eingabe durch den berechtigten Administrator am Windows Server.

Nach der Eingabe darf keine Klartextkopie in einer Textdatei, E-Mail oder ungeschützten Dokumentation auf dem Server verbleiben.

> **Hinweis zur Microsoft-Empfehlung:** Microsoft bevorzugt für Produktionssysteme Zertifikate oder föderierte Identitäten. Diese Connector-Version verwendet derzeit ein Client Secret. Kurze Laufzeit, geschützte Übertragung und geplante Rotation sind deshalb besonders wichtig.

---

6. Postfachzugriff sinnvoll begrenzen

Basisbetrieb

Der Connector begrenzt seine Verwendung auf die in der Absender- und Benutzerverwaltung eingetragenen Mailadressen. Dies ermöglicht eine schnelle Inbetriebnahme.

Die Entra-Anwendungsberechtigungen erlauben technisch grundsätzlich Zugriff auf die entsprechenden Daten aller Exchange-Online-Postfächer des Tenants, solange Exchange keine zusätzliche Einschränkung erzwingt.

Erhöhte Absicherung mit Exchange Application RBAC

Für eine serverseitig erzwungene Beschränkung sollte bei neuen Installationen **Role Based Access Control for Applications / Application RBAC** in Exchange Online verwendet werden.

Empfohlene Vorgehensweise:

1. Zulässigen Empfängerbereich in Exchange Online definieren.
2. Die Exchange-Anwendungsrolle **Application Mail.Send** auf diesen Bereich begrenzen.
3. Die Exchange-Anwendungsrolle **Application Mail.ReadWrite** auf denselben benötigten Bereich begrenzen.
4. Alle Benutzer-, Shared- und Funktionspostfächer aufnehmen, die der Connector verwenden soll.
5. Mindestens ein erlaubtes Postfach testen.
6. Mindestens ein Postfach außerhalb des Bereichs als Negativtest verwenden.

> **Wichtig für große Nachrichten:** Jedes Versandpostfach benötigt im wirksamen Exchange-Scope sowohl `Mail.Send` als auch `Mail.ReadWrite`, weil große Nachrichten über Entwurf und Upload-Sitzung verarbeitet werden.

Legacy Application Access Policies

Microsoft kennzeichnet **Application Access Policies** inzwischen als Legacy und empfiehlt für neue Einschränkungen Application RBAC. Bereits vorhandene Legacy-Policies können den Zugriff weiterhin beeinflussen und müssen insbesondere bei HTTP 403 geprüft werden.

Für die Einrichtung der Einschränkung werden benötigt:

Angabe	Wert
Application (client) ID	_____
Erlaubte Postfächer	_____
Weiteres erlaubtes Postfach	_____
Nicht erlaubtes Testpostfach	_____
Zuständiger Exchange-Administrator	_____

7. Datenübergabe an den Windows-Techniker

Diese Liste kann ausgefüllt an den ausführenden Windows-Techniker übergeben werden. Der Client-Secret-Wert wird getrennt davon über einen sicheren Übertragungsweg bereitgestellt.

Microsoft-365- und Entra-Daten

Feld	Einzutragender Wert
Kunde / Tenant	_____
Primäre Microsoft-365-Domain	_____
Directory (tenant) ID	_____
Application (client) ID	_____
App-Anzeigename	_____
Client Secret - Value	Separat und sicher übergeben: [ ] erledigt
Secret gültig bis	_____
Erinnerung zur Rotation	[ ] angelegt
Admin Consent für `Mail.Send`	[ ] gewährt
Admin Consent für `Mail.ReadWrite`	[ ] gewährt
Admin Consent für `User.Read.All`	[ ] gewährt
Termin-/Kontaktabgleich	[ ] nicht benötigt [ ] aktiviert
Admin Consent für `Calendars.Read`	[ ] nicht benötigt [ ] gewährt
Admin Consent für `Contacts.Read`	[ ] nicht benötigt [ ] gewährt
Exchange Application RBAC	[ ] nicht gewünscht [ ] eingerichtet [ ] separat beauftragt
Microsoft-365-Ansprechpartner	_____
Kontakt	_____

Postfächer und Funktionen

Feld	Einzutragender Wert
Versandpostfächer	_____
Weitere Versandpostfächer	_____
POP3-/Webclient-Postfächer	_____
Weitere Abrufpostfächer	_____

Feld	Einzutragender Wert
EWS-Postfächer	_____
EWS-Betriebsart	[ ] vollständiger Mailabgleich [ ] nur Versand und Gesendete Elemente
Eigene Versandkopien erneut ans ERP übertragen	[ ] ja [ ] nein, Dubletten vermeiden
Termine über EWS/Graph	[ ] nicht benötigt [ ] lesend bereitstellen
Kontakte über EWS/Graph	[ ] nicht benötigt [ ] lesend bereitstellen
Mails bereitstellen ab	_____ Datum/Uhrzeit
Termine bereitstellen ab	_____ Datum/Uhrzeit
Exchange-Abruf	[ ] aktiv [ ] nicht benötigt
Nach `RETR` als gelesen markieren	[ ] ja [ ] nein
Automatisch nach Abruf löschen	[ ] ja [ ] nein
POP3-`DELE` an Exchange weitergeben	[ ] erlauben [ ] nicht erlauben
Journalpostfach	[ ] aktivieren [ ] zunächst deaktiviert lassen

Server- und Netzwerkdaten

Feld	Einzutragender Wert
Windows-Servername	_____
Installationspfad	_____
Datenpfad	_____
Dienstkonto	_____
SMTP-Adresse und Port	_____
POP3-Adresse und Port	_____
EWS-Proxy-Adresse und Port	_____
Webclient-Adresse und Port	_____
Gemeinsames lokales EWS-Kennwort	Separat und sicher übergeben: [ ] erledigt
Zulässige EWS-Client-IP-Adressen	_____
Erlaubte Client-IP-Adressen	_____
Proxy erforderlich	[ ] nein [ ] ja: _____

> **Nicht eintragen:** Keine Microsoft-365-Benutzerkennwörter, keine OAuth-Tokens und keinen Client-Secret-Wert im Klartext in diese BookStack-Seite eintragen. Für den Connector werden keine persönlichen Microsoft-365-

> Kennwörter benötigt.

---

8. Vorbereitung und Einrichtung am Windows Server

Programm- und Datenordner festlegen

Der **Installationspfad** bezeichnet den vollständig gelieferten Programmordner. Er enthält `MailBridge365.exe`, `MailBridge365.exe.config`, die benötigten DLL-Dateien sowie den Ordner `runtimes` mit den nativen SQLite-Komponenten. Die Kundeneinstellungen liegen daneben in `MailBridge365.settings.config`.

Der **Datenpfad** enthält dagegen alle veränderlichen Betriebsdaten:

```
<Datenpfad>
├── Queue          Versandwarteschlange und DeadLetter
├── State          SQLite-Datenbank und Synchronisationsstände
├── Mailboxes      postfachbezogener Mail-, Termin- und Kontaktcache
├── Users          Benutzerverwaltung und Benutzerkennwörter
├── Secrets        gemeinsame Kennwörter und OAuth-Client-Secret
├── Certificates   automatisch erzeugte lokale TLS-Zertifikate
├── Log            normales sowie getrenntes EWS-/Graph-Protokoll
└── Actions        Ausgaben der E-Mail-Automatisierung
```

Bleibt das Feld **Datenpfad** leer, verwendet MailBridge 365 den Programmordner auch als Datenpfad. Die genannten Datenordner entstehen dann direkt neben der EXE. Für einen Windows-Dienst ist ein eigener, lokal beschreibbarer Datenpfad meist übersichtlicher. Das Dienstkonto benötigt dort Änderungsrechte. Bei einem UNC-Pfad sind zusätzlich passende Freigabe- und NTFS-Rechte sowie eine bereits beim Dienststart verfügbare Netzwerkverbindung erforderlich.

> **Nicht nur die EXE kopieren:** Zum Programm gehören auch die DLL-Dateien und der Ordner `runtimes`. Bei Updates muss `MailBridge365.settings.config` erhalten bleiben. Geheimnisse unter `<Datenpfad>\Secrets` und `<Datenpfad>\Users\Secrets` sind per Windows DPAPI an den Computer gebunden und müssen nach einem Serverwechsel neu gespeichert werden.

Netzwerk prüfen

- [ ] `login.microsoftonline.com` ist per HTTPS erreichbar.
- [ ] `graph.microsoft.com` ist per HTTPS erreichbar.
- [ ] Erforderliche Graph-/Outlook-Upload-Endpunkte sind erreichbar.
- [ ] DNS-Auflösung funktioniert unter dem späteren Dienstkonto.
- [ ] Datum, Uhrzeit und Zeitzone des Servers stimmen.
- [ ] Proxy oder SSL-Inspection blockiert die Microsoft-Endpunkte nicht.
- [ ] Lokale Ports sind nur für berechtigte Quellsysteme geöffnet.

Microsoft-Graph-Felder im Connector

Connector-Feld	Wert oder Quelle
`TenantId`	Directory (tenant) ID aus der Entra-App
`ClientId`	Application (client) ID aus der Entra-App
Client Secret	Inhalt der Spalte Value / Wert; lokal eingeben
`GraphBaseUrl`	`https://graph.microsoft.com/v1.0`
`OAuthScope`	`https://graph.microsoft.com/.default`
Parallele Graph-Anfragen je Postfach	Standard `2`
Wiederholungen bei Graph-Drosselung	Standard `3`
Mails bereitstellen ab	Globale Untergrenze mit Datum und Uhrzeit; ältere Elemente werden nicht angeboten
Termine bereitstellen ab	Globale Untergrenze mit Datum und Uhrzeit; ältere Termine werden nicht angeboten

Der Connector berücksichtigt bei HTTP `429`, `503` und `504` den von Microsoft gelieferten `Retry-After`-Wert und wiederholt die Anfrage automatisch.

Für den laufenden Abgleich verwendet der Connector Microsoft-Graph-DeltaLinks. Ordner- und Elementmetadaten werden in einer lokalen SQLite-Datenbank gespeichert; vollständige MIME-Inhalte werden erst bei Bedarf geladen. Dadurch muss nicht bei jedem Abruf das gesamte Postfach heruntergeladen werden. Eine reine Cache-Bereinigung erzeugt keine Löschanweisung an das ERP-System.

Benötigte lokale Komponenten aktivieren

Die Protokolle können unabhängig voneinander aktiviert werden. Nicht benötigte Listener sollten ausgeschaltet bleiben.

Komponente	Einstellung	Verhalten

SMTP	**SMTP aktivieren**	Startet den lokalen SMTP-Eingang. Ist SMTP deaktiviert, werden fehlende SMTP-Adresse, Port, Benutzername, Kennwort und Absenderfreigaben nicht als Konfigurationsfehler behandelt
POP3	**POP3 aktivieren**	Startet den lokalen POP3-Endpunkt für Benutzerpostfächer, lokale Unzustellbarkeiten und das Journal
EWS	**EWS-Graph-Proxy aktivieren**	Startet den lokalen HTTPS-Endpunkt `/EWS/Exchange.asmx`
Webclient	**HTTPS-Webclient aktivieren**	Startet die lokale Browseroberfläche zur Postfach- und Journalprüfung

Das Deaktivieren von SMTP beendet nur den SMTP-Listener. Der EWS-Versand, POP3, Webclient, Graph-Abgleich und die Verarbeitung bereits vorhandener Warteschlangeneinträge bleiben entsprechend ihrer eigenen Einstellungen aktiv.

Geheimnisse speichern

1. Starten Sie die Connector-Oberfläche mit lokalen Administratorrechten.
2. Tragen Sie Tenant-ID und Client-ID ein.
3. Geben Sie den Client-Secret-**Wert** in das dafür vorgesehene Geheimnisfeld ein.
4. Speichern Sie die Konfiguration.
5. Kontrollieren Sie, dass das Geheimnis anschließend als `********` angezeigt wird.
6. Entfernen Sie alle temporären Klartextkopien des Secrets.

Die Anwendung speichert das Client Secret DPAPI-verschlüsselt für den lokalen Computer. Bei einem Serverwechsel oder einem geänderten Datenpfad muss es am neuen Ziel erneut eingegeben werden.

Benutzer und Postfächer einrichten

1. Öffnen Sie die **Benutzerverwaltung** auf der Registerkarte **Übersicht**.
2. Legen Sie im Bereich **Vorgaben für neue Benutzer** fest, ob neue Konten den Exchange-Online-Abruf, den Modus **Nur Mailversand und Gesendete Elemente**, die optionale Unterdrückung gesendeter Elemente und die Dublettenvermeidung erhalten sollen.
3. Wählen Sie **Vorgaben speichern**. Diese Werte gelten nur für anschließend manuell oder automatisch neu angelegte Benutzer; bestehende Konten bleiben unverändert.
4. Legen Sie die benötigten lokalen POP3-/SMTP-Benutzer an.
5. Verwenden Sie vollständige Mailadressen als Benutzernamen.
6. Prüfen Sie die übernommenen Vorgaben für jeden neu angelegten Benutzer.
7. Legen Sie die erlaubten SMTP-Absender fest.
8. Aktivieren Sie Löschfunktionen nur entsprechend der dokumentierten Kundenentscheidung.
9. Vergeben Sie für das Journalpostfach ein eigenes lokales Kennwort.

10. Aktivieren Sie die Journalfunktion erst nach erfolgreichem Funktionstest und wenn sie tatsächlich benötigt wird.

EWS-Proxy für ein ERP-System einrichten

Der EWS-Proxy behält die vom ERP erwartete EWS-Struktur bei und verarbeitet die unterstützten Anfragen intern über Microsoft Graph. Im ERP wird als EWS-Server-URL die lokale HTTPS-Adresse des Connectors eingetragen, beispielsweise:

```
https://<connector-server>:<ews-port>/EWS/Exchange.asmx
```

Einstellung	Bedeutung
EWS-Proxy aktiv	Startet den lokalen HTTPS-Endpunkt
EWS-Port	Frei wählbarer lokaler TCP-Port; in Firewall und ERP identisch konfigurieren
Gemeinsames EWS-Kennwort	Lokales Kennwort für alle ERP-Benutzer; hat Vorrang vor dem jeweiligen Benutzerkennwort
Benutzerkennwort	Fallback, wenn kein gemeinsames EWS-Kennwort gesetzt ist
Zulässige Client-IP-Adressen	Beschränkt den Zugriff auf bekannte interne ERP-Systeme
Exchange-Online-Abruf	Muss für Postfächer aktiv sein, deren Daten über Graph bereitgestellt werden
Nur Mailversand und Gesendete Elemente	Zeigt nur die notwendigen Basisordner und synchronisiert ausschließlich Nachrichten aus **Gesendete Elemente**; Versand bleibt möglich
Nachrichten aus „Gesendete Elemente“ nicht übertragen	Hält auch **Gesendete Elemente** für den Client leer; der EWS-Versand funktioniert weiterhin. Diese Benutzervorgabe ist standardmäßig deaktiviert
Doppelte Mails im Ordner „Gesendete Elemente“ vermeiden	Unterdrückt im eingeschränkten Modus die erneute Rückgabe einer über den Connector versendeten Nachricht an das ERP; externe Versandkopien aus Outlook oder Mobilgeräten bleiben sichtbar
Termine und Kontakte synchronisieren	Optionaler lesender Abgleich; benötigt `Calendars.Read` und `Contacts.Read`

Das lokale EWS-Kennwort ist kein Microsoft-365-Benutzerkennwort. Es ist technisch eine eigene lokale Einstellung; bei Bedarf kann bewusst derselbe Wert wie beim Client Secret eingetragen werden. Das Client Secret im Graph-Feld meldet den Connector bei Microsoft an, das gemeinsame EWS-Kennwort authentifiziert das interne ERP-System am Connector.

Beim ersten erfolgreich validierten EWS-Zugriff kann der Connector ein noch nicht vorhandenes Postfach automatisch in der Benutzerverwaltung anlegen. Das neue Konto übernimmt die zuvor gespeicherten **Vorgaben für neue Benutzer**. Bestehende Benutzer und deren Einstellungen werden dadurch nicht verändert.

Die Dublettenvermeidung gilt nur zusammen mit **Nur Mailversand und Gesendete Elemente**. Sie verändert oder löscht keine Nachricht in Microsoft 365 und bereinigt keine bereits vorhandenen ERP-Dubletten. Die zur Erkennung benötigten Versandkennungen werden lokal unter `<Datenpfad>\State\connector-state.db` gespeichert. Postfachbezogene Cachedateien liegen übersichtlich unter `<Datenpfad>\Mailboxes\<Postfach-Kennung>`; das lokale Journal verwendet `<Datenpfad>\Mailboxes\_Journal`.

EWS-/Graph-Diagnose und lokale Daten

- Das getrennte EWS-/Graph-Protokoll liegt unter `<Datenpfad>\Log`.
- Die Detailstufe ist einstellbar; Mailinhalte können ausgelassen werden, damit Protokolle klein und datenschutzfreundlicher bleiben.
- Ein lokaler Synchronisationsreset pro Benutzer verwirft den lokalen Zustand. Bereits übertragene Elemente können dadurch erneut bereitgestellt werden, ohne Inhalte in Microsoft 365 zu löschen.
- Cache-Größe und Aufbewahrung begrenzen lokale MIME-Dateien. Metadaten, UIDLs, Seen-Status und DeltaLinks bleiben in SQLite erhalten.
- Bei vielen Postfachinhalten verhindert die Kombination aus DeltaLinks, Metadatenindex und bedarfsgeladenem MIME unnötige Vollabrufe.

> **Lizenzhinweis:** Ist die Lizenzprüfung ungültig, ist nur ein normales Postfach zulässig. Das Journal kann dann nicht aktiviert werden. Weitere manuell oder per EWS angefragte Postfächer werden abgewiesen und im Dateiprotokoll vermerkt.

---

9. Abnahme und Funktionstest

OAuth2 und Dienststart

- [ ] Der Dienst startet ohne Konfigurationsfehler.
- [ ] Ein OAuth2-Token wird erfolgreich angefordert.
- [ ] Im Protokoll steht kein `invalid_client` und kein HTTP 401.
- [ ] Tenant-ID, Client-ID und verwendetes Postfach werden korrekt angezeigt.

SMTP-Versand

- [ ] Eine Testmail wird aus einem erlaubten Postfach versendet.
- [ ] Der Graph-Aufruf endet mit HTTP 202.
- [ ] Die Nachricht liegt im Ordner **Gesendete Elemente** des Absenders.
- [ ] Ein nicht erlaubter Absender wird lokal abgewiesen.

☐ Wenn große Nachrichten benötigt werden, wurde zusätzlich eine Nachricht mit großem Anhang getestet.

POP3 und Webclient

☐ Eine vorhandene Nachricht wird angezeigt.

☐ Die Nachricht kann vollständig abgerufen werden.

☐ Die UIDL bleibt bei wiederholter Anmeldung stabil.

☐ Die Gelesen-Markierung entspricht der Kundenentscheidung.

☐ Die Löschfunktion entspricht der Kundenentscheidung.

☐ Ein POP3-`DELE` wird nur bei aktivierter Berechtigung und sauberem `QUIT` an Exchange weitergegeben.

EWS-Proxy und Graph-Synchronisation

☐ Das ERP erreicht die lokale URL `/EWS/Exchange.asmx` über HTTPS.

☐ Die Anmeldung funktioniert mit dem gemeinsamen EWS-Kennwort oder dem konfigurierten Benutzerkennwort.

☐ Die vollständige Ordnerhierarchie des eigenen Postfachs ist sichtbar.

☐ In der Betriebsart **Nur Mailversand und Gesendete Elemente** werden aus anderen Ordnern keine Nachrichten übertragen.

☐ Senden über EWS funktioniert und die Nachricht erscheint in **Gesendete Elemente**.

☐ Falls die Dublettenvermeidung aktiviert ist, erscheint eine über das ERP versendete Nachricht nach der Exchange-Synchronisation nicht ein zweites Mal im ERP.

☐ Eine außerhalb des Connectors versendete Testnachricht aus Outlook oder einem Mobilgerät wird weiterhin in das ERP synchronisiert.

☐ Falls aktiviert, werden Kalender und Kontakte lesend angezeigt.

☐ Die globalen Untergrenzen für Mails und Termine werden eingehalten.

☐ Ein erneuter Abgleich verwendet den gespeicherten Delta-Zustand und erzeugt keine unnötigen Dubletten.

☐ Das getrennte EWS-/Graph-Protokoll unter `<Datenpfad>\Log` enthält den Test ohne aktivierte Mailinhalte.

Journal

☐ Es existiert nur ein Journalpostfach.

☐ Das Journalpostfach hat ein eigenes lokales Kennwort.

☐ Die Journalfunktion ist nur bei tatsächlichem Bedarf aktiviert.

☐ Eine ein- und eine ausgehende Testnachricht erscheinen jeweils genau einmal.

☐ Das Journalpostfach versendet keine Nachrichten.

☐ SMTP-, POP3-, EWS- und Webclient-Vorgänge werden entsprechend der aktivierten Journalregeln erfasst.

Exchange Application RBAC

☐ Ein erlaubtes Postfach kann verwendet werden.

☐ Ein Postfach außerhalb des Scopes wird abgewiesen.

☐ Versand und Lesezugriff wurden getrennt geprüft.

Abschluss

☐ Secret-Ablaufdatum ist dokumentiert.

☐ Verantwortliche Person für die Rotation ist festgelegt.

☐ Installations- und Datenpfad sind dokumentiert.

☐ Firewall- und Proxy-Freigaben sind dokumentiert.

☐ Kundenspezifische Lösch- und Journalentscheidungen sind dokumentiert.

---

10. Fehlerzuordnung

Symptom	Wahrscheinliche Ursache und Prüfung
`AADSTS7000215` oder `invalid_client`	Falscher Secret-Wert, Secret-ID statt Value, falsche Client-ID oder abgelaufenes Secret
HTTP 401	Tenant-ID, Client-ID, Client Secret und Token-Endpunkt prüfen
HTTP 403	Admin Consent, Typ Application, Exchange Application RBAC und vorhandene Legacy Application Access Policies prüfen
HTTP 404 beim Postfach	Mailadresse, Exchange-Online-Lizenz und tatsächliche Postfachexistenz prüfen
HTTP 429	Microsoft-Graph-Drosselung; `Retry-After` wird automatisch beachtet
HTTP 503 oder 504	Temporäre Microsoft-Störung; automatische Wiederholung und Protokoll prüfen
Kleine Nachrichten funktionieren, große nicht	`Mail.ReadWrite` im wirksamen Scope sowie Graph-/Outlook-Upload-Endpunkte prüfen
Token funktioniert, bestimmtes Postfach nicht	Exchange Application RBAC oder Legacy Application Access Policy prüfen

Symptom	Wahrscheinliche Ursache und Prüfung
Keine POP3-Nachrichten	Exchange-Abruf beim Benutzer, lokale Übertragungs-UIDLs und Postfachinhalt prüfen
EWS meldet `Authentication required`	Gemeinsames lokales EWS-Kennwort, Benutzername, Client-IP-Freigabe und EWS-URL prüfen; das Entra-Client-Secret gehört nicht in das ERP-Kennwortfeld
EWS zeigt keine oder unvollständige eigene Ordner	Exchange-Online-Abruf des Benutzers, Graph-Rechte, erste Ordnerabfrage und EWS-/Graph-Protokoll prüfen; ERP-Ordneransicht anschließend neu laden
Nur Gesendete Elemente werden übertragen	Beim Benutzer ist die Betriebsart **Nur Mailversand und Gesendete Elemente** aktiv; dies ist beabsichtigt
Eine ERP-Versandkopie erscheint doppelt in Gesendete Elemente	Beim Benutzer den eingeschränkten EWS-Modus und **Doppelte Mails im Ordner „Gesendete Elemente“ vermeiden** aktivieren; die Einstellung wirkt nur auf künftige Rücksynchronisationen
Neue Benutzer erhalten unerwartete EWS-Einstellungen	In der Benutzerverwaltung die **Vorgaben für neue Benutzer** prüfen; Änderungen daran wirken nicht rückwirkend auf vorhandene Konten
Termine oder Kontakte fehlen	Funktion im Connector sowie `Calendars.Read` beziehungsweise `Contacts.Read` samt Admin Consent prüfen
Ältere Elemente fehlen	Globale Einstellung **Mails bereitstellen ab** beziehungsweise **Termine bereitstellen ab** prüfen
SQLite `unable to open database file`	Schreibrechte des Dienstkontos auf Datenpfad und Datenbankordner sowie erreichbaren lokalen Pfad prüfen
Weiteres EWS-Postfach wird abgewiesen	Lizenzstatus prüfen; bei ungültiger Lizenz ist nur ein normales Postfach zulässig

Typische Verwechslungen

Falsch	Richtig
Object-ID als Client-ID verwendet	Application (client) ID verwenden
Secret-ID als Kennwort verwendet	Client-Secret-Value verwenden
Delegierte Rechte eingetragen	Application permissions verwenden
Rechte hinzugefügt, aber keine Zustimmung erteilt	Grant admin consent ausführen
Persönliches Microsoft-365-Kennwort eingetragen	Am lokalen Protokoll das Connector-Benutzerkennwort oder gemeinsame EWS-Kennwort verwenden; zur Graph-Anmeldung den Client-Secret-Value im Connector hinterlegen
Shared-Mailbox nicht im Exchange-Scope	Alle verwendeten Shared-/Funktionspostfächer aufnehmen

11. Secret-Erneuerung

Ein abgelaufenes Secret führt zu einem vollständigen Ausfall der Microsoft-Graph-Anmeldung. Die Erneuerung muss vor dem Ablauf erfolgen.

Empfohlener Ablauf

1. Mindestens 30 Tage vor Ablauf ein neues Client Secret in derselben App-Registrierung erstellen.
2. Den neuen **Value / Wert** sofort sicher erfassen.
3. Wartungsfenster abstimmen.
4. Neues Secret in der Connector-Oberfläche am Windows Server eingeben.
5. Einstellungen speichern und Dienst neu starten.
6. OAuth2-Anmeldung und Testversand prüfen.
7. Falls verwendet, POP3, Webclient und EWS-Proxy einschließlich Ordnerabgleich prüfen.
8. Erst nach erfolgreicher Abnahme das alte Secret in Entra ID löschen.
9. Neues Ablaufdatum und nächste Erinnerung dokumentieren.

> **Kein unterbrechungsfreier Parallelbetrieb:** Der aktuelle Connector verwendet jeweils ein aktives Client Secret. Deshalb darf das alte Secret erst entfernt werden, nachdem das neue Secret am Server eingetragen und erfolgreich getestet wurde.

---

12. Offizielle Microsoft-Quellen

- App in Microsoft Entra ID registrieren
- Microsoft Graph ohne angemeldeten Benutzer verwenden
- App-Anmeldeinformationen und Client Secrets verwalten
- Microsoft-Graph-Berechtigungsreferenz
- Role Based Access Control for Applications in Exchange Online
- Application Access Policies - Legacy

> **Dokumentationsstand:** Diese Anleitung wurde am 16. September 2026 geprüft. Microsoft kann Portalbezeichnungen, Rollen, Grenzwerte und Empfehlungen ändern. Bei Abweichungen haben die verlinkten Microsoft-Learn-Seiten und die Sicherheitsrichtlinien des Kunden-Tenants Vorrang.

Interne Dokumentation

Feld	Eintrag
Kunde	_____
Ticket / Auftrag	_____
Erstellt durch	_____
Microsoft-365-Konfiguration abgeschlossen am	_____
Windows-Server-Installation abgeschlossen am	_____
Technische Abnahme durch	_____
Nächster Secret-Wechsel spätestens am	_____

Created 2026-09-11 16:00:38 CEST by Martin Dauwa
Updated 2026-09-16 11:37:18 CEST by Martin Dauwa