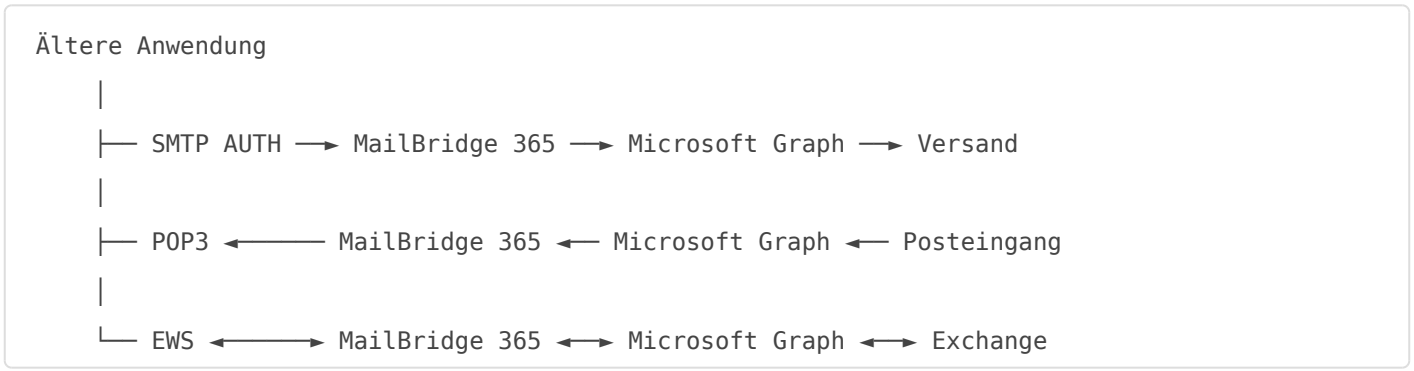
MailBridge 365 – Technische Gesamtdokumentation

Version 3.19.1 · Stand 16. September 2026

Technische Gesamtdokumentation für Installation, Betrieb, SMTP, POP3, Webclient, Journal sowie EWS- und Graph-Synchronisation.

Überblick

MailBridge 365 verbindet ältere Anwendungen und Mailprogramme mit Microsoft 365. Die angebundene Anwendung kann weiterhin klassisches SMTP AUTH für den Versand, POP3 für den Abruf oder einen kompatiblen Teil von Exchange Web Services verwenden. Die Kommunikation mit Microsoft 365 erfolgt sicher über OAuth2 und Microsoft Graph.



Es wird keine SMTP- oder POP3-Anmeldung mit einem Microsoft-365-Kennwort durchgeführt. Der Connector verwendet stattdessen eine eigene Anwendung in Microsoft Entra ID.

Ende von EWS in Exchange Online

Microsoft beginnt am **1. Oktober 2026** mit der stufenweisen Sperre von Exchange Web Services in Exchange Online. Ab **1. April 2027** ist EWS dort vollständig und dauerhaft abgeschaltet. Microsoft sieht über diesen Termin hinaus keine Ausnahmen vor. Die Änderung betrifft Microsoft 365 und Exchange Online; EWS in einem lokalen Exchange Server ist nach aktueller Ankündigung nicht betroffen.

Zeitpunkt	Bedeutung
Bis September 2026	EWS-Abhängigkeiten erfassen, verwendete Vorgänge prüfen und die Umstellung testen
Ab 1. Oktober 2026	Microsoft beginnt, EWS mandantenweise zu sperren; ohne vorbereitete Übergangsfreigabe können bestehende Anwendungen unterbrochen werden
Übergangsphase	`EWSEnabled` und `EWSAllowedAppIDs` können genehmigte EWS-Anwendungen vorübergehend weiter zulassen; sie ersetzen keine Migration

Zeitpunkt	Bedeutung
Ab 1. April 2027	EWS ist in Exchange Online vollständig und dauerhaft abgeschaltet

Microsoft bezeichnet die Graph-Abdeckung für die große Mehrheit typischer EWS-Szenarien als nahezu vollständig. Es gibt jedoch **keinen veröffentlichten Termin, an dem jede einzelne EWS-Funktion vollständig oder identisch in Microsoft Graph nachgebildet sein soll**. Sonderfunktionen und Hybridfälle müssen deshalb anhand der tatsächlich verwendeten Anwendung geprüft werden.

MailBridge 365 stellt den EWS-Endpunkt ausschließlich lokal für kompatible Bestandsanwendungen bereit. Gegenüber Exchange Online verwendet der Connector OAuth2 und Microsoft Graph und ruft dort kein EWS auf. Deshalb benötigt MailBridge 365 selbst keine Freigabe über `EWSAllowedAppIDs`. Andere Anwendungen, die weiterhin direkt per EWS auf Exchange Online zugreifen, müssen unabhängig davon geprüft und gegebenenfalls für die Übergangsphase freigegeben werden.

Offizielle Microsoft-Informationen:

- Zeitplan zur EWS-Abschaltung in Exchange Online
- EWSAllowedAppIDs für die Übergangsphase
- Migration von EWS zu Microsoft Graph
- Zuordnung von EWS-Vorgängen zu Graph

Leistungsumfang

- SMTP AUTH mit `AUTH LOGIN` und `AUTH PLAIN`
- POP3-Zugriff auf Microsoft-365-Postfächer
- OAuth2-Anmeldung über Microsoft Entra ID
- Versand und Abruf über Microsoft Graph
- Lokaler EWS-zu-Graph-Proxy für bestehende ERP-Anbindungen
- Exchange-Ordnerhierarchie mit stabilen Graph-Ordnerkennungen
- Optionaler lesender Abgleich von Kalenderterminen und Kontakten
- Optionaler EWS-Modus nur für Versand und **Gesendete Elemente**
- Optionale Vermeidung doppelter Versandkopien im Ordner **Gesendete Elemente**
- Globale Vorgaben für die manuelle und automatische Neuanlage von Benutzern
- Dynamisches Absendepostfach anhand der `From:`-Adresse
- Ablage versendeter Nachrichten im richtigen Ordner **Gesendete Elemente**
- Versand großer Nachrichten und Anhänge
- Persistente Warteschlange mit automatischen Wiederholungsversuchen
- Rückgabe dauerhaft unzustellbarer Ausgangsmails über POP3
- Eigene POP3-/SMTP-Benutzer mit individuellem Kennwort und Kontosperre
- Ein lokales, dublettenfreies Journalpostfach für ein- und ausgehende Mails

- Optionale E-Mail-Automatisierung mit Steuerzeichen, INI-Ausgabe und nachgelagerter Aktion
- Optionales STARTTLS für SMTP und POP3
- Freigabe nach Client-IP, Absenderadresse, Absenderdomain und POP3-Postfach
- Verschlüsselte Speicherung von Kennwort und Client Secret
- Windows-Dienst für den unbeaufsichtigten Betrieb
- Grafische Oberfläche für Konfiguration, Status und Live-Protokoll
- Lokaler HTTPS-Webclient zur Postfachprüfung und optionalen Nachrichtenlöschung
- Persistente SQLite-Indizes und Graph-DeltaLinks für große Postfächer
- Einstellbare globale Stichtage für E-Mails und Termine
- Separates EWS-/Graph-Diagnoseprotokoll mit mehreren Detailstufen

Voraussetzungen

- Unterstütztes Windows-Client- oder Windows-Server-Betriebssystem
- .NET Framework 4.8
- Microsoft-365-Mandant mit Exchange Online
- Berechtigung zum Erstellen einer App-Registrierung in Microsoft Entra ID
- Administratorzustimmung für die benötigten Microsoft-Graph-Berechtigungen
- Lokale Windows-Administratorrechte für die Dienstinstallation
- Ausgehender HTTPS-Zugriff auf Port 443
- Zugriff auf folgende Ziele:

```
login.microsoftonline.com
graph.microsoft.com
outlook.office.com
```

`outlook.office.com` wird insbesondere für von Microsoft Graph bereitgestellte Upload-Adressen bei großen Anhängen benötigt.

Vorbereitung in Microsoft 365

App-Registrierung anlegen

1. Öffnen Sie das **Microsoft Entra Admin Center**.
2. Wechseln Sie zu **Identität → Anwendungen → App-Registrierungen**.
3. Erstellen Sie eine neue, nur für den eigenen Mandanten vorgesehene Anwendung.
4. Verwenden Sie beispielsweise den Namen `MailBridge 365`.
5. Notieren Sie die **Anwendungs-ID (Client-ID)**.
6. Notieren Sie die **Verzeichnis-ID (Tenant-ID)**.
7. Öffnen Sie **Zertifikate und Geheimnisse**.
8. Erstellen Sie ein neues Client Secret.
9. Notieren Sie sofort den angezeigten Secret-Wert.

Der Secret-Wert kann im Microsoft-Portal später nicht erneut angezeigt werden. Hinterlegen Sie außerdem einen internen Termin zur rechtzeitigen Erneuerung vor dem Ablaufdatum.

Microsoft-Graph-Berechtigungen vergeben

Fügen Sie unter **API-Berechtigungen** folgende **Microsoft Graph-Anwendungsberechtigungen** hinzu:

Berechtigung	Verwendung
`Mail.Send`	Nachrichten aus einem Microsoft-365-Postfach versenden
`Mail.ReadWrite`	POP3-Abruf sowie Erstellen und Senden großer Nachrichten
`User.Read.All`	Anzeigename und sekundäre SMTP-, SIP-, X500- und weitere Proxyadressen für EWS `ResolveNames`
`Calendars.Read`	Optional: Kalendertermine über den EWS-Proxy lesen
`Contacts.Read`	Optional: Kontakte über den EWS-Proxy lesen

Erteilen Sie anschließend die **Administratorzustimmung für den Mandanten**. Ohne Administratorzustimmung kann der Connector nicht auf die Postfächer zugreifen.

Microsoft-Dokumentation zu Graph-Berechtigungen

Zugriff auf Postfächer begrenzen

Die Graph-Anwendungsberechtigungen können standardmäßig Zugriff auf alle Postfächer des Mandanten ermöglichen. Für einen möglichst kleinen Berechtigungsumfang empfiehlt sich **Role Based Access Control for Applications in Exchange Online**.

Microsoft-Dokumentation zu Application RBAC

Die Einrichtung von Exchange Application RBAC sollte durch die zuständige Microsoft-365-Administration erfolgen. Wichtig ist, dass die für SMTP und POP3 benötigten Postfächer vollständig im gewählten Bereich enthalten sind.

> **Sicherheitshinweis:** Berechtigungen aus Microsoft Entra ID und Exchange Application RBAC können additiv wirken. Lassen Sie die endgültige Berechtigungskonfiguration durch die Microsoft-365-Administration prüfen.

Installation

Programmdateien bereitstellen

1. Kopieren Sie den vollständig gelieferten Programmordner an seinen endgültigen Speicherort.
2. Verwenden Sie einen eigenen Ordner, beispielsweise:

```
C:\MailBridge365
```

3. Verschieben oder löschen Sie diesen Ordner nach der Dienstinstallation nicht.
4. Starten Sie `MailBridge365.exe` für die erstmalige Einrichtung mit **Als Administrator ausführen**.

Die Dienstinstallation verwendet genau die EXE am aktuellen Speicherort. Eine zusätzliche Kopie der Anwendung wird nicht angelegt.

Der technische Windows-Dienstname lautet `MailBridge365`. In der Windows-Diensteverwaltung wird er als **SMTP, POP3 und EWS MailBridge 365** angezeigt. Erkennt die Anwendung noch eine Installation unter dem früheren Dienstnamen, bietet die Oberfläche die automatische Umstellung an. Dabei wird der alte Dienst beendet und entfernt; Programmdateien, Einstellungen, Daten und Warteschlange bleiben bestehen.

Vorhandene Installation kopieren oder verschieben

Kennwörter und Client Secret sind nicht in der EXE oder ihrer Konfigurationsdatei enthalten. Sie liegen standardmäßig in folgenden verschlüsselten Dateien:

```
<Datenpfad>\Secrets\smtp-password.bin
<Datenpfad>\Secrets\oauth-client-secret.bin
<Datenpfad>\Secrets\ews-client-password.bin
```

Wird nur die EXE mit ihrer Konfigurationsdatei, aber ohne die Datenunterordner kopiert, müssen das gemeinsame SMTP/POP3-Kennwort und das OAuth-Client-Secret am neuen Speicherort erneut eingegeben werden. Dasselbe gilt nach einer Änderung des Datenpfads, wenn am neuen Ziel noch keine verschlüsselte Datei vorhanden ist.

Die Oberfläche prüft dies vor dem Speichern und nennt den fehlenden Zielpfad. Bereits ausgefüllte Einstellungen bleiben dabei zur Korrektur erhalten.

Die Verschlüsselung ist an den Windows-Computer gebunden. Beim Umzug auf einen anderen Computer müssen die beiden Geheimnisse daher auch dann neu eingegeben werden, wenn die verschlüsselten Dateien mitkopiert wurden.

Verhalten beim ersten Start

Beim ersten Start öffnet sich die grafische Oberfläche. Da noch keine Zugangsdaten hinterlegt sind, kann die lokale Instanz zunächst einen Konfigurationsfehler anzeigen. Bestätigen Sie diese Meldung und tragen Sie anschließend unter **Einstellungen** die benötigten Werte ein.

Die Oberfläche besteht aus drei Bereichen:

- **Übersicht:** Status der lokalen Instanz und des Windows-Dienstes sowie die verwendeten Endpunkte und Pfade; außerdem Lizenzverwaltung und LiveUpdate
- **Einstellungen:** Konfiguration von Allgemein, POP3, SMTP, EWS-Proxy, Microsoft Graph, EWS-/Graph-Log, Webclient und Mail-Automatisierung
- **Live-Protokoll:** Laufende Diagnosemeldungen mit farblicher Kennzeichnung

Lizenzierung und LiveUpdate

Bei jedem Programmstart wird die Lizenz über das PHXFramework geprüft. Bei einem normalen interaktiven Start kann dabei der Lizenzdialog angezeigt werden. Beim Start als Windows-Dienst oder mit `--nogui` erfolgt dieselbe Prüfung ohne Dialogfenster. Den aktuellen Zustand zeigt die untere Statusleiste als **Lizenz: gültig** oder **Lizenz: Demo / nicht gültig** an.

Über **Übersicht → Lizenz verwalten** kann der Lizenzdialog auch während des Betriebs geöffnet werden. Nach dem Schließen wird die Lizenz erneut geprüft und die Statusanzeige aktualisiert.

Bei einer ungültigen Lizenz bleibt der Connector grundsätzlich betriebsfähig, ist jedoch auf **ein normales Benutzerpostfach** beschränkt. Das automatisch vorhandene Journalpostfach zählt nicht als normales Benutzerpostfach, seine Journalfunktion wird bei ungültiger Lizenz aber automatisch deaktiviert und kann nicht aktiviert werden. Ein weiteres manuell angelegtes oder über EWS angefragtes Postfach wird abgewiesen. Bereits gespeicherte zusätzliche Konten werden nicht gelöscht. Der Lizenzstatus und lizenzbedingte Ablehnungen werden im PHX-Lizenzprotokoll sowie im normalen Connector-Protokoll festgehalten.

Über **Übersicht → LiveUpdate** wird die Aktualisierungsfunktion des PHXFrameworks gestartet. Sobald ein Update bestätigt und vorbereitet wurde, beendet die Oberfläche die lokale Connector-Instanz und stoppt den installierten Windows-Dienst. Danach wird das Programm geschlossen, damit der Updater die Programmdateien ersetzen kann. Falls der Dienst mangels Berechtigung nicht gestoppt werden kann, muss die Oberfläche als Administrator gestartet werden. Kundeneinstellungen liegen getrennt in `MailBridge365.settings.config` und werden durch den Austausch der erzeugten `EXE.config` nicht überschrieben.

Konfiguration

Registerkarte Allgemein

Feld	Beschreibung	Empfehlung
Datenpfad	Ablageort für Warteschlange, Protokolle, POP3-Status und Geheimnisse	Leer lassen, um den Programmordner zu verwenden
Warteschlange prüfen	Abstand zwischen zwei Prüfungen der Versandwarteschlange	`10` Sekunden

Feld	Beschreibung	Empfehlung
Maximale Versandversuche	Höchstzahl der Versuche vor dem Verschieben nach `DeadLetter`	`50`
Verbindungs-Timeout	Maximale Dauer einer Verbindung zu Microsoft 365	`30` Sekunden
Maximale Wartezeit beim Beenden	Zeit für aktive SMTP-/POP3-Sitzungen zum sauberen Abschluss	`30` Sekunden
Ausführliche Debugprotokollierung	Schreibt zusätzliche Diagnoseinformationen	Nur zur Fehlersuche aktivieren

Programmdateien und Betriebsdaten sind zwei getrennte Bereiche. Der gelieferte Programmordner enthält die Anwendung und alle benötigten Laufzeitdateien:

```
<Programmordner>
├── MailBridge365.exe
├── MailBridge365.exe.config
├── MailBridge365.settings.config
├── PHXFramework.dll
├── weitere mitgelieferte DLL-Dateien
└── runtimes
    ├── win-x64\native\e_sqlite3.dll
    └── win-x86\native\e_sqlite3.dll
```

> **Wichtig:** Für Installation und Update muss immer der vollständig gelieferte Programmordner verwendet werden. Das alleinige Kopieren oder Umbenennen der EXE reicht nicht aus. `MailBridge365.settings.config` enthält die Kundeneinstellungen und muss bei einem Update erhalten bleiben.

Der in der Konfiguration angegebene **Datenpfad** enthält die veränderlichen Betriebsdaten. Ist das Feld leer, ist der Datenpfad identisch mit dem Programmordner; die folgenden Ordner liegen dann direkt neben der EXE. Für einen Windows-Dienst ist ein eigener beschreibbarer Datenpfad meist übersichtlicher:

```
<Datenpfad>
├── Queue
│   ├── Incoming\<Auftrags-ID>\message.eml + envelope.xml
│   ├── Pending\<Auftrags-ID>\message.eml + envelope.xml
│   └── DeadLetter\<Auftrags-ID>\message.eml + envelope.xml
├── State
│   ├── connector-state.db
```

```
│   ├── Pop3                        (nur Altbestand/Migration)
│   └── EwsReplay                   (lokale Wiederholungsstände)
├── Mailboxes
│   ├── <lesbares Postfach>-<Kurz-ID>
│   │   ├── Cache
│   │   │   ├── Mail
│   │   │   │   ├── Inbox
│   │   │   │   ├── SentItems
│   │   │   │   └── Folders\<Ordner-ID>
│   │   │   ├── Calendar\index.xml
│   │   │   └── Contacts\index.xml
│   │   └── Drafts
│   └── _Journal
│       ├── Incoming
│       └── Messages\<00>\<00>\<Nachrichten-ID>.eml
├── Users
│   ├── pop3-users.xml
│   └── Secrets\<Benutzer-ID>.bin
├── Secrets
│   ├── smtp-password.bin
│   ├── oauth-client-secret.bin
│   └── ews-client-password.bin
├── Certificates
│   ├── MailBridge365-selfsigned.pfx
│   └── MailBridge365-selfsigned-password.bin
├── Log
│   ├── MailBridge365-<Datum>.log
│   └── MailBridge365-EWS-Graph-<Datum>.log
└── Actions
    └── Pending
```

Die Postfachordner bestehen aus einem lesbaren Teil der Mailadresse und einer kurzen eindeutigen Kennung. Dadurch bleibt die Zuordnung für Administratoren erkennbar, ohne dass ungewöhnliche Zeichen oder gleichartige Adressen zu ungültigen beziehungsweise kollidierenden Windows-Pfaden führen.

Ein abweichender lokaler Pfad oder UNC-Pfad kann angegeben werden. Das Konto des Windows-Dienstes benötigt dort die erforderlichen Zugriffsrechte. Bei einem UNC-Pfad benötigt das Computerkonto des Connector-Computers, beispielsweise `FIRMA\MAILSERVER$`, passende Freigabe- und NTFS-Rechte am Zielserver. Außerdem müssen Netzwerkverbindung und Namensauflösung bereits beim Start des Windows-Dienstes verfügbar sein. Ein lokaler Datenpfad ist für einen

besonders ausfallsicheren Betrieb vorzuziehen.

Registerkarte EWS-Proxy

Der EWS-Proxy stellt für bestehende Anwendungen einen lokalen, TLS-geschützten Teilumfang von Exchange Web Services bereit. Intern werden die Anforderungen mit Microsoft Graph und der vorhandenen Versandwarteschlange verarbeitet.

Feld	Beschreibung	Empfehlung
EWS-Graph-Proxy aktivieren	Startet den lokalen EWS-Endpunkt	Erst nach vollständiger Konfiguration aktivieren
EWS-Adresse	Lokale Bindeadresse	`127.0.0.1` auf demselben Server, sonst eine gezielt erreichbare Serveradresse
EWS-HTTPS-Port	TCP-Port des lokalen Endpunkts	`8444`
Erlaubte EWS-Client-IP-Adressen	Positivliste der zugelassenen Quelladressen	Nur die Server der angebundenen Anwendung eintragen
Gemeinsames EWS-Clientkennwort	Optionales Kennwort für alle EWS-Benutzer; wird zuerst geprüft	Für ERP-Legacy-Anbindungen ein eigenes langes Kennwort vergeben
Microsoft-Bearer-Token interner Clients akzeptieren	Akzeptiert das vom unveränderten ERP gesendete Bearer-Token ohne zweite Tokenprüfung	Nur zusammen mit einer engen EWS-Client-IP-Positivliste verwenden
Max. Einträge je EWS-Antwort	Seitengröße für E-Mails; bei Terminen und Kontakten zugleich deren Cachegrenze	`1000`
MIME-Cache maximal	Maximale Gesamtgröße vollständig geladener E-Mails	`10240 MB`
MIME-Cache Aufbewahrung	Zeitliche Bereinigung der vollständigen E-Mail-Dateien; `0` deaktiviert sie	`30 Tage`
Cache aktualisieren	Mindestabstand zwischen zwei Graph-Synchronisationen	`30` Sekunden
EWS-Löschungen an Exchange weitergeben	Erlaubt `DeleteItem` über Graph	Standardmäßig deaktiviert lassen
Termine und Kontakte synchronisieren	Stellt Kalendertermine und Kontakte über den EWS-Proxy lesend bereit	Erst nach Vergabe von `Calendars.Read` und `Contacts.Read` aktivieren

Globale Synchronisations-Stichtage

Die beiden Felder befinden sich unter **Einstellungen > Microsoft Graph**:

Feld	Beschreibung	Beispiel

E-Mails bereitstellen ab	Begrenzt E-Mails global für POP3, Webclient und EWS	`14.09.2026 08:00`
Termine bereitstellen ab	Begrenzt Kalendertermine global; zukünftige Vorkommen älter angelegter Serien bleiben enthalten	`14.09.2026 00:00`

Die Eingabe gilt in der lokalen Zeitzone des Windows-Servers. Ein leeres Feld bedeutet **unbegrenzt**. Der E-Mail-Stichtag wird direkt an Microsoft Graph übergeben und bleibt Bestandteil des DeltaLinks. Dadurch werden ältere Mailinhalte weder vorab heruntergeladen noch später über den Connector bereitgestellt. MIME-Dateien werden unverändert nur bei einem tatsächlichen Abruf geladen.

Nach einer Änderung des Stichtags beginnt der betroffene Graph-Abgleich mit einem neuen Delta-Stand. Nicht mehr zulässige lokale Metadaten werden still entfernt. Dabei entsteht ausdrücklich **keine EWS-Löschanweisung an das ERP**. Für Termine verwendet der Connector bei gesetztem Stichtag eine Kalenderansicht, die Serientermine in ihrem relevanten Zeitraum auflöst.

E-Mail-Metadaten werden ohne feste Gesamtanzahl in der lokalen SQLite-Datei `<Datenpfad>\State\connector-state.db` geführt. Nach dem Erstabgleich verwendet der Connector je Ordner den von Microsoft Graph gelieferten DeltaLink und ruft nur noch Änderungen ab. Vollständige Mailinhalte werden erst bei Bedarf geladen. Die Größen- und Altersbereinigung des MIME-Dateicaches erzeugt niemals eine EWS-Löschanweisung an das ERP. Löschereignisse entstehen ausschließlich aus einer tatsächlichen Graph-Änderung oder einer ausdrücklich erlaubten Client-Löschung.

Registerkarte EWS-/Graph-Log

Dieser Reiter steuert ein eigenes tägliches Diagnoseprotokoll ausschließlich für die Kommunikation des Connectors mit dem EWS-Client und Microsoft Graph. Das normale Live-Protokoll bleibt davon unabhängig bestehen.

Feld	Beschreibung	Empfehlung
Detailstufe	Legt fest, wie ausführlich EWS- und Graph-Vorgänge in die separate Datei geschrieben werden	Im Normalbetrieb `1 – Standard`, zur Fehlersuche vorübergehend `2 – Detailliert` oder `3 – Protokoll`
Mailinhalte protokollieren	Nimmt bei Detailstufe 3 zusätzlich MIME-/Mailinhalte in das Diagnoseprotokoll auf	Aus Datenschutz- und Speichergründen deaktiviert lassen und nur gezielt kurzzeitig einschalten

Änderungen an diesen Einstellungen werden nach einem Neustart der lokalen Instanz beziehungsweise des Windows-Dienstes wirksam. Über **Live-Protokoll → EWS-/Graph-Log öffnen** lässt sich die Datei des aktuellen Tages direkt öffnen.

Der einzutragende EWS-Endpunkt lautet:

```
https://<Connector-Server>:<EWS-Port>/EWS/Exchange.asmx
```

Das Serverzertifikat wird automatisch erzeugt und im Datenpfad wiederverwendet. Es ist selbstsigniert und muss daher auf dem Computer der angebundenen Anwendung als vertrauenswürdig hinterlegt oder dort ausdrücklich akzeptiert werden. Die EWS-Anmeldung verwendet Benutzername und Kennwort aus der **Benutzerverwaltung**. Das Konto darf nicht gesperrt sein und der Schalter für den Exchange-Online-Abruf muss aktiviert sein. Ein EWS-Benutzer kann nur auf sein eigenes Postfach zugreifen und nur mit seiner eigenen Absenderadresse senden.

Optional kann im Reiter **EWS-Proxy** ein **gemeinsames EWS-Clientkennwort** hinterlegt werden. Der Proxy prüft dieses Kennwort zuerst. Stimmt es nicht, wird als Fallback weiterhin das individuelle Kennwort des angegebenen Benutzers geprüft. Das gemeinsame Kennwort hebt weder Kontosperren noch die benutzerspezifische Ordnerfreigabe auf und wird DPAPI-verschlüsselt gespeichert.

Wenn der ERP-Client sein vorhandenes Microsoft-Tenant-Client-Secret weiterhin zur Tokenbeschaffung verwendet, bleibt dessen Struktur unverändert. Mit **Microsoft-Bearer-Token interner Clients akzeptieren** nimmt der Proxy das daraus entstandene Bearer-Token an, ohne es nochmals kryptografisch zu prüfen. Die Quelladresse muss in der EWS-IP-Positivliste stehen; das in `ExchangeImpersonation` genannte Konto muss vorhanden, entsperrt und für den Exchange-Online-Zugriff aktiviert sein. Diese Option ist nur für abgeschottete interne Netze vorgesehen.

In der Benutzerverwaltung kann zusätzlich **Nur Mailversand und den Ordner „Gesendete Elemente“ synchronisieren** aktiviert werden. Der Schalter hält den Exchange-Online-Zugriff automatisch aktiv, beschränkt den EWS-Nachrichtenabruf aber auf `sentitems`. In dieser Betriebsart werden nur die notwendigen Basisordner an den EWS-Client übermittelt; benutzerdefinierte und versteckte Exchange-Ordner werden nicht angelegt. Posteingang und alle anderen Ordner werden beim Nachrichtenabruf leer beantwortet. Versand über `CreateItem`/`SendItem` bleibt vollständig möglich. Die Einstellung betrifft den EWS-Proxy und ändert nicht eigenständig das Verhalten eines separat verwendeten POP3-Clients.

Mit **Nachrichten aus „Gesendete Elemente“ nicht übertragen** kann zusätzlich auch die Rückübertragung aus `sentitems` vollständig abgeschaltet werden. Der Basisordner bleibt sichtbar, enthält für den Client jedoch keine synchronisierten Nachrichten. Das Erstellen und Versenden neuer Nachrichten über EWS ist davon nicht betroffen. Die Option ist standardmäßig deaktiviert.

Für diesen eingeschränkten Modus steht zusätzlich **Doppelte Mails im Ordner „Gesendete Elemente“ vermeiden** zur Verfügung. Der Connector merkt sich die Kennungen der über seinen EWS-Endpunkt versendeten Nachrichten und unterdrückt deren anschließende Rückübertragung aus Microsoft 365 an denselben EWS-Client. Damit erscheint eine vom ERP versendete Nachricht dort nicht zuerst als lokaler Versand und danach ein zweites Mal als synchronisierte Exchange-Kopie. Die Nachricht bleibt in Microsoft 365 und Outlook unverändert einmal vorhanden und wird weiterhin journalisiert. Nachrichten, die außerhalb des Connectors etwa mit Outlook oder einem Mobilgerät gesendet wurden, werden weiterhin regulär an das ERP übertragen.

Die Dublettenvermeidung wirkt nur zusammen mit **Nur Mailversand und den Ordner „Gesendete Elemente“ synchronisieren**. Sie entfernt keine bereits vorhandenen Dubletten aus

dem ERP. Bei einer absichtlich ausgelösten Bereinigung des lokalen Synchronisationsstands können noch vorhandene Nachrichten erneut angeboten werden.

Ist das adressierte Postfach noch nicht in der Benutzerverwaltung vorhanden, legt der Connector es nach einer erfolgreichen vertrauenswürdigen EWS-Anmeldung automatisch an. Das gilt für das gemeinsame EWS-Clientkennwort und den ausdrücklich freigegebenen internen Bearer-Modus. Zuvor wird der Zugriff auf das Postfach über Microsoft Graph geprüft. Das neue Benutzerkonto übernimmt die unter **Vorgaben für neue Benutzer** gespeicherten Werte für Exchange-Online-Abruf, EWS-Synchronisation, Unterdrückung gesendeter Elemente und Dublettenvermeidung. Ein bestehendes Konto und dessen Einstellungen werden niemals automatisch überschrieben; gesperrte Konten bleiben gesperrt.

Bei aktivierter Option **Termine und Kontakte synchronisieren** ergänzt der Proxy den EWS-Ordnerbaum um Kalender und Kontakte und überträgt deren Inhalte lesend über `SyncFolderItems`, `FindItem` und `GetItem`. Auch spätere Änderungen werden über EWS-Pull-Benachrichtigungen an das ERP gemeldet. Die Daten werden unter `DataPath\Mailboxes\<Postfach-Kennung>\Cache\Calendar` beziehungsweise `Contacts` zwischengespeichert. Dafür benötigt die Entra-App zusätzlich die Anwendungsberechtigungen `Calendars.Read` und `Contacts.Read`. Änderungen durch das ERP sowie Aufgaben werden in dieser Ausbaustufe nicht unterstützt.

Kalendertermine werden bei `GetItem` zusätzlich als iCalendar-Inhalt in `MimeContent` bereitgestellt. Dadurch können auch ältere ERP-Clients, die den Termin nicht ausschließlich aus den strukturierten EWS-Feldern aufbauen, den Kalendereintrag vollständig übernehmen.

Unterstützt werden:

- `GetFolder` und `FindFolder` für den jeweils freigegebenen Mailordner
- `FindItem`, `GetItem` und `GetAttachment` einschließlich MIME-Inhalt
- `CreateItem` mit `SaveOnly`, `SendOnly` und `SendAndSaveCopy`
- `SendItem` für lokal gespeicherte Entwürfe
- `UpdateItem` für gelesen/ungelesen
- `DeleteItem`, sofern ausdrücklich aktiviert
- `SyncFolderItems` mit lokalem Synchronisationsstand
- `SyncFolderHierarchy` für die Ordnererkennung
- `ResolveNames` für die in den ERP-Protokollen verwendete Postfachprüfung
- `Subscribe`, `GetEvents` und `Unsubscribe` für Pull-Subscriptions

Bei `ResolveNames` berücksichtigt der Proxy die Clientanforderung `ReturnFullContactData=true`. Die Antwort enthält dann zusätzlich zum Postfach einen vollständigen EWS-Kontakt mit Anzeigename, bis zu drei sekundären SMTP-, SIP-, X500- oder weiteren Proxyadressen und `ContactSource`. Die primäre SMTP-Adresse bleibt separat im `Mailbox`-Block. Dafür ist die Graph-Anwendungsberechtigung `User.Read.All` mit Administratorzustimmung erforderlich. Kann Graph die Benutzerinformationen nicht lesen, bleibt die Namensauflösung funktionsfähig, liefert jedoch nur die primäre Adresse und protokolliert einen Warnhinweis. Dies ist für ältere ERP-Verbindungstests erforderlich, die eine reine Postfachauflösung trotz `NoError` nicht als erfolgreiche Verbindung anerkennen.

Für den freigegebenen Standardordner verwendet der Proxy die von Microsoft Graph gelieferte unveränderliche Ordner-ID. Dadurch erkennt ein bereits eingerichteter ERP-Client seinen bisherigen Microsoft-365-Ordner auch nach der Umstellung auf den Proxy wieder. Übermittelt der Client beim Abonnieren zusätzlich seine alte vollständige Exchange-Ordnerliste, akzeptiert der Proxy die Anfrage, ignoriert die nicht freigegebenen Ordner und erstellt intern ausschließlich ein Abonnement für den erlaubten Ordner. Die SOAP-Struktur des Clients muss nicht geändert werden.

Der EWS-Systemordner `publicfoldersroot` wird für die Kompatibilität mit der ERP-Ordnerverwaltung angeboten. Ein vollständiger inhaltlicher Abgleich echter Exchange-Online-Public-Folder-Postfächer über Microsoft Graph ist jedoch nicht Bestandteil dieser Version.

Nicht enthalten sind schreibende Kalender-/Kontaktoperationen, Aufgaben, Regeln, vollständiger Public-Folder-Inhaltsabgleich, Stellvertretungen, Streaming-/Push-Abonnements und sonstige EWS-Spezialbereiche. Der EWS-Proxy ist deshalb eine Kompatibilitätsschicht für typische Mailzugriffe und keine vollständige Exchange-Server-Nachbildung.

EWS-Nachrichten werden je Benutzerpostfach unter `DataPath\Mailboxes\<Postfach-Kennung>\Cache\Mail` gespeichert. Posteingang, Gesendete Elemente und weitere Ordner besitzen darunter getrennte Verzeichnisse. Nachrichten liegen als einzelne `.eml`-Dateien im jeweiligen Ordner und erhalten keinen eigenen Unterordner. Die unveränderliche Graph-ID ist eindeutig indiziert. Wiederholte `FindItem`-, `GetItem`- oder `SyncFolderItems`-Aufrufe legen dieselbe Nachricht daher nicht mehrfach ab. Innerhalb des Aktualisierungsintervalls werden Anfragen direkt aus dem lokalen Cache beantwortet. Ist Graph vorübergehend nicht erreichbar, bleibt der bereits vorhandene Cache lesbar; der Fehler wird im Protokoll ausgewiesen.

Beim Versand meldet der Connector Erfolg, nachdem die Nachricht dauerhaft in seiner lokalen Warteschlange gespeichert wurde. Die anschließende Graph-Zustellung erfolgt durch die bestehende Warteschlangenverarbeitung und ist im Live-Protokoll nachvollziehbar. Dadurch gehen angenommene Nachrichten bei einem vorübergehenden Graph- oder Netzwerkfehler nicht verloren.

Kann eine über EWS angenommene Nachricht auch nach den konfigurierten Wiederholungsversuchen nicht an Microsoft Graph übergeben werden, stellt der Connector sie dem ursprünglichen EWS-Benutzer als lokale Nachricht im **Posteingang** bereit. Der Betreff beginnt mit `Unzustellbar:`, der Header `X-MailBridge365-Delivery-Error` enthält den technischen Fehler. Dies gilt auch für Benutzer mit **Nur Mailversand und Gesendete Elemente synchronisieren**: Normale Posteingangsmails werden in diesem Modus weiterhin nicht übertragen, lokale Unzustellbarkeiten jedoch schon.

Die Rückmeldung besitzt eine stabile EWS-ID und wird nach erfolgreichem `GetItem` nicht erneut als neues Synchronisationsereignis gemeldet. Sie bleibt im lokalen Posteingang sichtbar, bis sie über EWS gelöscht wird oder durch einen anderen freigegebenen Zugriff wie POP3 oder Webclient aus `DeadLetter` entfernt wurde. Die Funktion **Lokalen Synchronisationsstand bereinigen** setzt auch diesen Rückgabestand zurück und bietet noch vorhandene Unzustellbarkeiten erneut an.

Für einen ersten Funktionstest liegt `Test-EwsProxy.ps1` bei. Beispiel:

```
.\Test-EwsProxy.ps1 -Server 127.0.0.1 -Port 8444 `
  -User benutzer@firma.at -Password "LokalesKennwort"
```

Registerkarte SMTP

Feld	Beschreibung	Beispiel
SMTP aktivieren	Startet den lokalen SMTP-Eingang. Bei deaktivierter Option werden fehlende SMTP-Adresse, Port, Benutzername, Kennwort und Absenderfreigaben nicht beanstandet	Nur aktivieren, wenn Anwendungen per SMTP senden sollen
SMTP-Adresse	Lokale IP-Adresse, auf der SMTP angenommen wird	`127.0.0.1`
SMTP-Port	Port für die ältere Anwendung	`2525`
Erlaubte Client-IP-Adressen	Geräte, die den Connector verwenden dürfen	`127.0.0.1,::1`
SMTP-Benutzername	Gemeinsamer lokaler Benutzername	`alte-anwendung`
Gemeinsames SMTP/POP3-Kennwort	Gemeinsames lokales Kennwort	Sicheres, eigenes Kennwort
SMTP STARTTLS erzwingen	Erfordert eine verschlüsselte Verbindung vor der Anmeldung	Für LAN-Zugriffe aktivieren
TLS-Zertifikat-Thumbprint	Fingerabdruck des Windows-Zertifikats	Nur bei STARTTLS erforderlich
Ungültige/selbstsignierte TLS-Zertifikate zulassen	Verwendet auch ein abgelaufenes, selbstsigniertes oder nicht vertrauenswürdiges Zertifikat	Nur für Tests oder kontrollierte interne Netze
Fehlendes TLS-Zertifikat automatisch erstellen	Erstellt ohne eingetragenen Thumbprint einmalig ein selbstsigniertes Notfallzertifikat	Nur als interne Notlösung verwenden
Erlaubte Absender	Vollständige Adressen erlaubter Absendepostfächer	`rechnung@firma.at`
Erlaubte Absender-Domains	Alternative Freigabe einer vollständigen Domain	`firma.at`
Maximale Nachrichtengröße	Grenze der kompletten SMTP-/MIME-Nachricht in Byte	`26214400`
Maximale Empfänger	Höchstzahl der Empfänger pro Nachricht	`100`

Mehrere Werte werden mit Komma oder Semikolon getrennt.

Ist **SMTP aktivieren** ausgeschaltet, startet kein SMTP-Listener. POP3, EWS-Proxy, Webclient, Journal und die Verarbeitung bereits vorhandener Warteschlangeneinträge können unabhängig davon weiterlaufen. Für bestehende Konfigurationen ist SMTP nach dem Update standardmäßig weiterhin aktiviert.

> **Wichtig:** Sobald mindestens eine vollständige Adresse unter **Erlaubte Absender** eingetragen ist, wird ausschließlich diese Adressliste verwendet. Die Domainfreigabe dient nur als Alternative, wenn die Adressliste leer ist.

Registerkarte POP3

Feld	Beschreibung	Empfehlung
POP3 aktivieren	Schaltet den POP3-Endpunkt ein	Nur bei benötigtem Mailabruf aktivieren
POP3-Adresse	Lokale IP-Adresse, auf der POP3 angenommen wird	`127.0.0.1`
POP3-Port	Port für den alten Mailclient	`2110`
Erlaubte POP3-Postfächer	Vollständige Adressen einzelner Postfächer	`eingang@firma.at`
Erlaubte POP3-Domains	Erlaubt alle Postfächer einer Domain	`firma.at`
POP3 STLS erzwingen	Erfordert Verschlüsselung vor der Anmeldung	Für LAN-Zugriffe aktivieren
Maximale Nachrichten	Höchstzahl der noch nicht übertragenen Nachrichten pro Anmeldung	`1000`
Maximale POP3-Mailgröße	Maximale MIME-Größe einer Nachricht in Byte	`52428800`
Nach RETR als gelesen markieren	Markiert vollständig abgerufene Nachrichten in Outlook als gelesen	Nach Bedarf
Übertragene Nachrichten bei QUIT löschen	Löscht erfolgreich übertragene Nachrichten nach sauberem Sitzungsende	Nur nach bewusster Entscheidung aktivieren
POP3-DELE in Exchange zulassen	Gibt ein ausdrückliches `DELE` des Clients bei sauberem `QUIT` an Exchange weiter	Nur aktivieren, wenn der Mailclient löschen darf

Der POP3-Benutzername ist immer die vollständige Mailadresse des gewünschten Postfachs. Für nicht verwaltete, über die Freigabelisten erlaubte Postfächer wird das gemeinsame lokale SMTP/POP3-Kennwort verwendet. Das persönliche Microsoft-365-Kennwort ist dafür nicht erforderlich.

Über **Benutzerverwaltung** auf der Registerkarte **Übersicht** können zusätzlich eigene Konten angelegt werden. Für ein dort vorhandenes Konto ist bei POP3 immer dessen individuelles Kennwort erforderlich. Das gemeinsame Kennwort wird für dieses Konto nicht mehr akzeptiert. Nicht eigens angelegte Postfächer können weiterhin über die Postfach- oder Domainfreigabe und das gemeinsame Kennwort verwendet werden.

Für jedes verwaltete Konto stehen folgende Optionen zur Verfügung:

Option	Bedeutung
Benutzer / Mailadresse	Vollständige Mailadresse und POP3-Benutzername
Kennwort	Lokales Kennwort für POP3 und SMTP AUTH; kein Microsoft-365-Kennwort
Exchange-Online-Abruf	Erlaubt für dieses Konto den Microsoft-Graph-Abruf durch POP3 und EWS
EWS-Synchronisation	Optional: Nur Mailversand und den Ordner „Gesendete Elemente“ synchronisieren; andere EWS-Ordner bleiben leer
Übertragung unterdrücken	Optional: Nachrichten aus „Gesendete Elemente“ nicht an ERP oder EWS-Mailclient übertragen; der Versand bleibt möglich
Doppelte gesendete Mails	Verhindert im eingeschränkten EWS-Modus, dass eine über den Connector versendete Nachricht anschließend als zweite Versandkopie aus Microsoft 365 an das ERP zurückgegeben wird
Lokalen Synchronisationsstand bereinigen	Einmalige Vormerkung: Beim nächsten POP3- oder EWS-Abruf werden die lokalen Übertragungsstände dieses Benutzers zurückgesetzt
Journalpostfach	Kennzeichnet das einmalige, rein lokale Archivpostfach
Journalfunktion	Aktiviert die Übernahme ein- und ausgehender Mailkopien
Konto gesperrt	Verhindert SMTP-, POP3-, Webclient- und EWS-Zugriffe dieses Kontos

Vorgaben für neue Benutzer

Oberhalb der Benutzerliste befindet sich der getrennte Bereich **Vorgaben für neue Benutzer**. Dort können folgende Startwerte festgelegt werden:

- **Exchange-Online-Abruf aktivieren**
- **Nur Mailversand und den Ordner „Gesendete Elemente“ synchronisieren**
- **Nachrichten aus „Gesendete Elemente“ nicht übertragen**
- **Doppelte Mails im Ordner „Gesendete Elemente“ vermeiden**

Mit **Vorgaben speichern** werden diese Werte dauerhaft gespeichert. Sie gelten ab diesem Zeitpunkt sowohl für die manuelle Neuanlage über **Neu** als auch für Benutzer, die nach einer erfolgreichen vertrauenswürdigen EWS-Anmeldung automatisch angelegt werden. Vorhandene Benutzer werden durch eine Änderung der Vorgaben ausdrücklich nicht verändert.

Die abhängigen Optionen werden automatisch konsistent gehalten: Ohne Exchange-Online-Abruf kann der Modus für Gesendete Elemente nicht aktiviert werden; ohne diesen Modus ist auch die Übertragungsunterdrückung nicht aktiv. Wenn gar keine gesendeten Elemente übertragen werden, ist die zusätzliche Dublettenvermeidung nicht erforderlich und wird deaktiviert. Die Vorgaben und Benutzerkonten liegen gemeinsam in `<Datenpfad>\Users\pop3-users.xml`; eine manuelle Bearbeitung

der XML-Datei ist nicht erforderlich.

Beim Bearbeiten eines Kontos zeigen acht Sternchen an, dass bereits ein Kennwort gespeichert ist. Bleibt dieser Platzhalter unverändert, wird das bisherige Kennwort beibehalten.

Die Bereinigung wird beim nächsten Abruf automatisch ausgeführt und anschließend im Benutzerkonto wieder deaktiviert. Noch in Exchange vorhandene Nachrichten werden erneut angeboten. Dabei wird keine Nachricht in Microsoft 365 gelöscht oder verändert; im ERP können durch den gewünschten erneuten Import Duplikate entstehen. Für das rein lokale Journalpostfach steht diese Funktion nicht zur Verfügung, da bereits per POP3 gelöschte Journaldateien nicht aus Exchange wiederhergestellt werden können.

Ein verwaltetes Konto darf sein eigenes Postfach auch als SMTP-Absender verwenden. Die bisherigen gemeinsamen SMTP-Zugangsdaten und Absenderfreigaben bleiben parallel bestehen. Änderungen in der Benutzerverwaltung werden von einer laufenden Instanz automatisch übernommen. SMTP, POP3 und das Live-Protokoll werden beim Öffnen oder Schließen der Benutzerverwaltung nicht gestoppt. Eine Änderung gilt für die nächste Anmeldung; eine bereits authentifizierte Verbindung läuft regulär bis zu ihrem Ende weiter.

Beim ersten Öffnen wird `journal@localhost` automatisch als deaktiviertes Journalpostfach angelegt. Es darf genau ein Journalpostfach geben. Seine Adresse kann beim Bearbeiten geändert werden. Vor der erstmaligen Aktivierung muss ein neues lokales Kennwort für das Archivsystem vergeben werden. Das Journalpostfach kann nicht für SMTP AUTH verwendet werden und greift nicht auf Exchange Online zu. Das Archivsystem meldet sich mit der Journaladresse am lokalen POP3-Endpunkt an. Abgeholte Journalnachrichten werden nur nach einem ausdrücklichen `DELE` und einem sauberen `QUIT` lokal entfernt.

Ausgehende SMTP- und EWS-Nachrichten werden vor dem Graph-Versand abgelegt. Eingehende Nachrichten werden beim POP3-, EWS- oder Webclient-Abgleich übernommen. Beim EWS-Abgleich werden sowohl der Posteingang als auch Gesendete Elemente berücksichtigt. Die vollständigen MIME-Dateien werden im Hintergrund geladen; das Öffnen einer einzelnen Nachricht ist daher nicht erforderlich. Stabile Graph-UIDLs und die MIME-Message-ID verhindern, dass dieselbe Nachricht über mehrere Zugriffswege doppelt journalisiert wird. Jede Journalnachricht wird als einzelne `.eml`-Datei unter `<Datenpfad>\Mailboxes\_Journal\Messages` gespeichert. Der dauerhafte SQLite-Index `<Datenpfad>\State\connector-state.db` bleibt auch nach dem Löschen einer Journalnachricht erhalten. Ein wiederholter Abruf derselben Quellmail erzeugt daher keinen neuen Journaleintrag.

Beim erstmaligen Wechsel von einer Version vor 3.18.18 auf Version 3.18.18 oder neuer werden ältere Cache-, Journal- und Synchronisationsdaten nicht in die neue Ordnerstruktur übernommen. Die Programmkonfiguration, Benutzerverwaltung und verschlüsselten Geheimnisse bleiben erhalten. Microsoft-365-Inhalte werden beim nächsten Zugriff neu abgeglichen; in einer produktiven Installation ist deshalb vor der Umstellung eine gesonderte Migrationsplanung erforderlich.

Ein Postfach ist erlaubt, wenn entweder seine vollständige Adresse oder seine Domain freigegeben ist. Eine Domain wird ohne `@` eingetragen. Die Freigabe von `firma.at` schließt `tochter.firma.at`

nicht automatisch ein.

> **Sicherheitshinweis:** Eine Domainfreigabe erlaubt jedem berechtigten Client, mit dem gemeinsamen Kennwort auf alle Postfächer dieser Domain zuzugreifen, soweit auch die Microsoft-365-App Zugriff besitzt. Einzelne Postfachfreigaben sind daher vorzuziehen.

Registerkarte Mail-Automatisierung

Feld	Beschreibung
E-Mail-Steuerzeichen auswerten	Aktiviert oder deaktiviert die Funktion global
Eingehende E-Mails (POP3) prüfen	Wertet Steuerzeichen beim Abruf einer Nachricht über POP3 aus
Ausgehende E-Mails (SMTP) prüfen	Wertet Steuerzeichen beim Versand einer Nachricht über SMTP aus
Erkannte Steuerzeichen aus der E-Mail entfernen	Entfernt erkannte `[[NAME=WERT]]`-Felder nach der Auswertung aus Betreff sowie Text- und HTML-Inhalt
Ausgabeordner für INI-Dateien	Zielordner; leer verwendet `<Datenpfad>\Actions\Pending`
Nachgelagertes Programm	Optionales Programm, das nach dem Erstellen einer INI-Datei gestartet wird

Die globale Option muss aktiviert sein. Anschließend können Eingangs- und Ausgangsprüfung unabhängig voneinander ein- oder ausgeschaltet werden. Die Entfernung der Steuerzeichen erfolgt nur, wenn mindestens ein gültiges Steuerzeichen erkannt und in eine INI-Datei übernommen wurde. Anlagen werden nicht verändert.

Steuerzeichen können im Betreff oder Nachrichtentext in folgender Form stehen:

```
[[AUFTRAG=4711]]
[[KUNDENNUMMER=10025]]
[[AKTION=LieferscheinDrucken]]
```

Ein Name beginnt mit einem Buchstaben und darf anschließend Buchstaben, Zahlen, Punkt, Bindestrich und Unterstrich enthalten. Jede in einer aktivierten Richtung verarbeitete Mail mit mindestens einem erkannten Steuerfeld erzeugt eine eigene UTF-8-kodierte INI-Datei:

```
[Message]
QueueId=7d7e5f...
Direction=Ausgang
CreatedUtc=2026-09-03T10:15:30.0000000Z
Sender=versand@firma.at
```

```
Recipients=empfaenger@firma.at
Subject=Auftrag 4711
MessageId=<beispiel@firma.at>
MimeDate=2026-09-03T12:15:00.0000000+02:00
ControlCount=3

[Variables]
AUFTRAG=4711
KUNDENNUMMER=10025
AKTION=LieferscheinDrucken
```

`Direction` enthält je nach Verarbeitungsweg den Wert `Eingang` oder `Ausgang`. Bei `Eingang` wird die Nachricht beim POP3-Abruf geprüft. Bei `Ausgang` erfolgt die Prüfung bei der SMTP-Annahme vor der Ablage in der Versandwarteschlange.

Ist ein nachgelagertes Programm hinterlegt, wird es nach erfolgreicher INI-Erstellung gestartet. Als erstes Argument erhält es den vollständigen Pfad der INI-Datei. Werte aus der Mail werden nicht als Befehlszeile ausgeführt. Bei einem eigenen Ausgabeordner muss das Konto des Windows-Dienstes dort Änderungsrechte besitzen.

> **Sicherheitshinweis:** Inhalte eingehender Mails sind nicht vertrauenswürdig. Das nachgelagerte Programm muss erlaubte Aktionen und Werte selbst prüfen. Es sollte eine INI-Datei erst nach erfolgreicher Verarbeitung entfernen oder in einen eigenen Archivordner verschieben.

Registerkarte Microsoft Graph

Feld	Beschreibung	Wert
Tenant-ID	Verzeichnis-ID aus der App-Registrierung	Mandantenspezifische GUID
Client-ID	Anwendungs-ID aus der App-Registrierung	Anwendungsspezifische GUID
Client Secret	Secret-Wert aus Microsoft Entra ID	Vertraulich behandeln
Graph-Basisadresse	Microsoft-Graph-Endpunkt	`https://graph.microsoft.com/v1.0`
OAuth-Scope	OAuth2-Berechtigungsbereich	`https://graph.microsoft.com/.default`
Parallele Graph-Anfragen je Postfach	Gemeinsame Obergrenze für Versand, POP3 und Webclient	`2` (zulässig: 1 bis 4)
Wiederholungen bei Graph-Drosselung	Anzahl direkter Wiederholungen bei HTTP 429, 503 und 504	`3` (zulässig: 0 bis 10)

Kennwort und Client Secret werden automatisch unter `DataPath\Secrets` verschlüsselt für den lokalen Computer gespeichert. Ein eigener Dateipfad ist nicht erforderlich. Nach dem Speichern zeigt die Oberfläche `********` an. Dies bedeutet, dass bereits ein Wert vorhanden ist. Der Platzhalter wird nicht als Kennwort gespeichert.

Registerkarte Webclient

Feld	Beschreibung	Empfehlung
HTTPS-Webclient aktivieren	Startet die lokale Weboberfläche	Nur bei Bedarf aktivieren
Webclient-Adresse	IP-Adresse des HTTPS-Endpunkts	`127.0.0.1`, für LAN-Zugriff `0.0.0.0`
HTTPS-Port	Frei wählbarer TCP-Port	`8443`
Nachrichten im Webclient löschen erlauben	Zeigt die endgültige Löschfunktion an	Nur für berechtigte Benutzer aktivieren

Nach einem Dienstneustart ist der Webclient beispielsweise unter `https://127.0.0.1:8443` erreichbar. Bei einer LAN-Freigabe muss zusätzlich die Client-IP in **Erlaubte Client-IP-Adressen** enthalten und der Port in der Windows-Firewall freigegeben sein.

Das TLS-Zertifikat wird automatisch unter `<Datenpfad>\Certificates` erzeugt und bei späteren Starts wiederverwendet. Es muss kein Thumbprint konfiguriert werden. Weil es selbstsigniert ist, meldet ein Browser das Zertifikat zunächst als nicht vertrauenswürdig. Für eine warnungsfreie interne Verwendung kann das erzeugte Zertifikat auf den zugreifenden Geräten durch die Administration als vertrauenswürdig verteilt werden.

Die Anmeldung erfolgt mit einer Mailadresse und dem zugehörigen Kennwort aus der Benutzerverwaltung. Normale Benutzer sehen ausschließlich ihr eigenes Exchange-Postfach und lokale Unzustellbarkeiten. Das Journalpostfach wird mit dem aktivierten Journalbenutzer geöffnet. Der Webclient verwendet sichere Sitzungscookies, CSRF-Schutz und beendet inaktive Sitzungen nach 30 Minuten. HTML-Mailinhalte werden nicht als aktiver Fremdcode ausgeführt, sondern HTML-kodiert als Text angezeigt.

Ist die Löschfunktion freigegeben, werden Exchange-Nachrichten sofort über Microsoft Graph gelöscht. Journal- und Dead-Letter-Nachrichten werden lokal entfernt. Die Löschung wird protokolliert.

Einstellungen speichern

1. Tragen Sie alle erforderlichen Werte ein.
2. Wählen Sie **Speichern**.
3. Die Anwendung schreibt die Eingaben dauerhaft in `MailBridge365.settings.config`.
4. Anschließend wird die vollständige Konfiguration geprüft.
5. Fehler bei dieser Prüfung werden als Warnung angezeigt, setzen die gespeicherten Eingaben jedoch nicht zurück.
6. Korrigieren Sie den genannten Wert und speichern Sie erneut.

Die dauerhafte Einstellungsdatei liegt neben der EXE und wird nicht aus der Programmvorlage neu erzeugt. Dadurch bleiben Einstellungen bei einem erneuten Build oder einem Update im selben Programmordner erhalten. Eine vorhandene `MailBridge365.settings.config` darf beim Aktualisieren nicht gelöscht oder durch eine leere Datei ersetzt werden.

Läuft der Windows-Dienst bereits, übernimmt er Änderungen erst nach einem Neustart über **Übersicht → Dienst neu starten**.

Netzwerkbetrieb und TLS

Anwendung und Connector auf demselben Computer

Verwenden Sie vorzugsweise:

```
Adresse: 127.0.0.1
Erlaubte Client-IP-Adressen: 127.0.0.1,::1
```

Damit sind SMTP und POP3 nur lokal erreichbar.

Zugriff aus dem lokalen Netzwerk

Für den Zugriff von einem anderen Computer:

1. Stellen Sie die gewünschte Listen-Adresse auf `0.0.0.0` oder auf eine konkrete lokale IP-Adresse.
2. Tragen Sie ausschließlich die benötigten Client-IP-Adressen ein.
3. Erstellen Sie passende eingehende Regeln in der Windows-Firewall.
4. Aktivieren Sie STARTTLS beziehungsweise STLS.
5. Hinterlegen Sie den Thumbprint eines geeigneten Zertifikats.

Das Zertifikat muss einschließlich privatem Schlüssel im Zertifikatsspeicher `Lokaler Computer\Persönlich` vorhanden sein. Das Dienstkonto `NETWORK SERVICE` benötigt Leserechte auf den privaten Schlüssel.

Ein abgelaufenes, selbstsigniertes oder anderweitig nicht vertrauenswürdiges Zertifikat wird nur verwendet, wenn **Ungültige/selbstsignierte TLS-Zertifikate zulassen** aktiviert ist. Diese Einstellung hebt ausschließlich die Prüfung im Connector auf. Der SMTP- oder POP3-Client muss das Zertifikat ebenfalls akzeptieren beziehungsweise dessen Aussteller als vertrauenswürdig kennen. Für ein manuell ausgewähltes Zertifikat bleibt der Thumbprint erforderlich.

Alternativ kann **Fehlendes TLS-Zertifikat automatisch erstellen** aktiviert werden. Ist kein Thumbprint eingetragen, erzeugt der Connector beim nächsten Start ein selbstsigniertes Zertifikat mit dem Computernamen als Zertifikatsname. Das Zertifikat ist fünf Jahre gültig und wird dauerhaft unter `DataPath\Certificates` gespeichert. Sein zufälliges PFX-Kennwort liegt dort separat und durch Windows DPAPI verschlüsselt. Beim nächsten Start wird dasselbe Zertifikat erneut verwendet. Ein

verwendbares Zertifikat mit eingetragenem Thumbprint hat Vorrang. Kann dieses Zertifikat nicht geladen werden, wird bei aktivierter Notfalloption ebenfalls das automatisch erzeugte Zertifikat benutzt.

Das automatisch erzeugte Zertifikat ermöglicht die TLS-Aushandlung, ersetzt aber kein vertrauenswürdiges Unternehmens- oder öffentliches Zertifikat. Der Client kann es weiterhin wegen des unbekannten Ausstellers oder eines nicht zum Verbindungsnamen passenden Computernamens ablehnen.

Der private Schlüssel wird beim Programmstart in einen Windows-kompatiblen Schlüsselcontainer geladen und während der gesamten Laufzeit gemeinsam für SMTP und POP3 verwendet. Dadurch kann der Windows-TLS-Stack auf den Schlüssel zugreifen, ohne für jede Clientverbindung einen neuen Schlüssel anzulegen.

Unterstützt werden SMTP STARTTLS und POP3 STLS. Implizites SMTPS auf Port 465 und implizites POP3S werden nicht unterstützt.

> **Wichtig:** Stellen Sie die SMTP- und POP3-Ports niemals öffentlich im Internet bereit.

Windows-Dienst einrichten

1. Prüfen Sie zunächst über **Lokalen Proxy starten**, ob die Konfiguration fehlerfrei ist.
2. Beenden Sie eine laufende lokale Instanz bei Bedarf.
3. Wählen Sie unter **Übersicht** die Aktion **Dienst installieren**.
4. Bestätigen Sie die Windows-Administratorabfrage.
5. Warten Sie auf die Meldung, dass der Dienst installiert und gestartet wurde.

Die Installation erfolgt direkt durch die Anwendung. Es werden keine externen Installationsskripte benötigt. Der Dienst startet automatisch mit Windows und läuft unter dem Konto `NETWORK SERVICE`. Die Installation erstellt alle benötigten Datenunterordner und vergibt die Schreibrechte für Warteschlange, Index, Journal, EWS-Cache, Benutzerverwaltung, Protokolle und Zertifikate. Die Aktion **Dienst neu starten** prüft und repariert diese Ordnerrechte erneut.

Wenn der Dienst läuft, startet die Oberfläche keine zweite lokale Instanz auf denselben Ports. Status und Live-Protokoll können trotzdem angezeigt werden.

Kontrolliertes Beenden des Dienstes

Beim Stoppen oder Neustarten beendet der Connector nicht sofort alle Clientverbindungen:

1. SMTP und POP3 nehmen keine neuen Verbindungen mehr an.
2. Bereits aktive Sitzungen dürfen ihre laufende Übertragung und die Abmeldung regulär abschließen.

3. Sobald keine aktiven Clientverbindungen mehr vorhanden sind, wird der Dienst unmittelbar beendet.
4. Sind nach Ablauf der unter **Maximale Wartezeit beim Beenden** eingestellten Zeit weiterhin Verbindungen aktiv, werden diese getrennt und der Dienst wird beendet.

Das Zeitlimit gilt gemeinsam für SMTP und POP3 und kann zwischen 5 und 300 Sekunden eingestellt werden. Der Standardwert beträgt 30 Sekunden. Beginn, Wartezustand und ein gegebenenfalls erreichtes Zeitlimit werden protokolliert.

Alte Anwendung konfigurieren

SMTP-Versand

Einstellung im alten Programm	Wert
SMTP-Server	IP-Adresse oder DNS-Name des Connector-Computers
SMTP-Port	Standardmäßig `2525`
Authentifizierung	SMTP AUTH LOGIN oder PLAIN
Benutzername	Gemeinsamer SMTP-Benutzer oder verwaltete Mailadresse
Kennwort	Gemeinsames Kennwort beziehungsweise individuelles Benutzerkennwort
Verschlüsselung	STARTTLS entsprechend der Connector-Konfiguration

Die Mail muss genau eine gültige `From:`-Adresse enthalten. Diese Adresse bestimmt das Microsoft-365-Absendepostfach und muss im Connector erlaubt sein.

```
From: rechnung@firma.at
→ Versand über das Postfach rechnung@firma.at
→ Ablage in Gesendete Elemente von rechnung@firma.at
```

POP3-Abruf

Einstellung im alten Mailclient	Wert
POP3-Server	IP-Adresse oder DNS-Name des Connector-Computers
POP3-Port	Standardmäßig `2110`
Benutzername	Vollständige Microsoft-365-Mailadresse
Kennwort	Individuelles Benutzerkennwort, andernfalls gemeinsames Kennwort
Verschlüsselung	STLS entsprechend der Connector-Konfiguration

Falls ein alter Client ausschließlich Port 110 unterstützt, kann der POP3-Port auf `110` geändert werden. Prüfen Sie vorher, ob dieser Port bereits verwendet wird und ob für das Binden des Ports ausreichende Rechte vorhanden sind.

Verhalten des POP3-Abrufs

- Zuerst werden lokale, dauerhaft unzustellbare Ausgangsmails des angemeldeten Benutzers geprüft.
- Sind solche lokalen Nachrichten vorhanden, werden in dieser Anmeldung nur diese Nachrichten angeboten. Microsoft 365 wird dabei nicht abgefragt.
- Der Betreff erhält beim Abruf das Präfix `Unzustellbar:` . Der technische Versandfehler wird zusätzlich im Mail-Header `X-MailBridge365-Delivery-Error` mitgegeben.
- Nach vollständigem `RETR` und einem sauberen `QUIT` wird die lokale Nachricht aus `DeadLetter` entfernt. Bei einem Verbindungsabbruch bleibt sie für den nächsten Abruf erhalten.
- Sind keine lokalen unzustellbaren Nachrichten vorhanden und ist der Exchange-Online-Abruf für das Konto aktiv, wird der Posteingang über Microsoft Graph geladen.
- Ist der Exchange-Online-Abruf für das Konto deaktiviert, dient POP3 ausschließlich zur Rückgabe lokaler unzustellbarer Nachrichten.
- Bereits erfolgreich übertragene Nachrichten werden zuerst anhand ihrer UIDL ausgefiltert. Das Nachrichtenlimit wird erst danach angewendet.
- Bei aktivem Journal werden neue Nachrichten bereits beim Öffnen des Postfachs in das lokale Journal übernommen, auch wenn der Client danach nur `LIST` und `UIDL`, aber kein `RETR` sendet.
- Bei einem Limit von `10` werden daher bis zu zehn noch nicht übertragene Nachrichten angeboten. Sind die neuesten Nachrichten bereits übertragen, rücken ältere, noch nicht übertragene Nachrichten nach.
- Pro Postfach ist gleichzeitig nur eine POP3-Sitzung zulässig.
- Neue Nachrichten erscheinen bei der nächsten POP3-Anmeldung.
- `RETR` überträgt den originalen MIME-Inhalt der Nachricht.
- `TOP` liefert nur den gewünschten Teil und gilt nicht als vollständiger Abruf.
- `UIDL` verwendet stabile Nachrichtenkennungen.
- Optional wird eine vollständig abgerufene Nachricht als gelesen markiert.
- Im Modus **nicht löschen** bleiben Nachrichten in Microsoft 365 erhalten und werden nach erfolgreichem Abruf lokal als bereits übertragen vermerkt.
- Im Löschmodus werden Nachrichten erst bei einem sauberen `QUIT` gelöscht.
- Jede erfolgreich mit `RETR` gelieferte Graph-Nachricht wird zusätzlich lokal als übertragen vermerkt. Eine fehlgeschlagene Exchange-Löschung führt deshalb nicht zu einem dauerhaften erneuten Angebot derselben Nachricht.
- Mit **POP3-DELE in Exchange zulassen** wird ein echtes `DELE` des Clients erst bei einem sauberen `QUIT` über Microsoft Graph ausgeführt. Ist die Option aus, lehnt der Connector `DELE` für Exchange-Nachrichten ab.
- Ein Verbindungsabbruch vor `QUIT` führt im Löschmodus nicht zur Löschung.
- `RSET` hebt Löschvormerkungen der aktuellen Sitzung auf.

Der dauerhafte Übertragungsstatus befindet sich in der SQLite-Datenbank unter:

```
<Datenpfad>\State\connector-state.db
```

Löschen Sie diese Datei nicht unbedacht. Andernfalls können bereits übertragene und in Microsoft 365 belassene Nachrichten erneut angeboten werden.

Nachrichtengröße und Anhänge

Die Standardgrenze für die vollständige SMTP-Nachricht beträgt 25 MiB. Dazu gehören Nachrichtentext, MIME-Kopfzeilen, Anhänge und die durch Base64 entstehende Vergrößerung.

Der Connector wählt den Versandweg automatisch:

- Kleine Nachrichten werden direkt als MIME-Nachricht versendet.
- Große Nachrichten werden als Entwurf angelegt.
- Große Anhänge werden blockweise über eine Microsoft-Graph-Upload-Sitzung übertragen.
- Nach erfolgreichem Upload wird der Entwurf versendet.
- Bei einem Fehler startet der nächste Warteschlangenversuch den Vorgang neu.

Zusätzlich gelten immer die Größen- und Empfängergrenzen von Exchange Online und des betreffenden Postfachs.

Microsoft-Dokumentation zu großen Anhängen

Warteschlange und Wiederholungsversuche

Eine SMTP-Nachricht wird zunächst dauerhaft in der lokalen Warteschlange gespeichert. Erst danach bestätigt der Connector die Annahme gegenüber der alten Anwendung.

```
<Datenpfad>\Queue
├── Incoming
├── Pending
└── DeadLetter
```

Ordner	Bedeutung
`Incoming`	Nachricht wird gerade übernommen
`Pending`	Nachricht wartet auf Versand oder einen erneuten Versuch
`DeadLetter`	Nachricht konnte dauerhaft nicht versendet werden

Bei vorübergehenden Fehlern versucht der Connector den Versand erneut. Von Microsoft Graph vorgegebene Wartezeiten werden berücksichtigt. Ohne eine solche Vorgabe wird der Abstand

schrittweise erhöht. Unerwartete Fehler werden standardmäßig nach einer Minute erneut versucht.

Zusätzlich schützt eine zentrale Begrenzung alle Graph-Zugriffe durch SMTP, POP3 und Webclient. Standardmäßig werden je Postfach höchstens zwei Anfragen gleichzeitig ausgeführt. Bei HTTP `429` (Drosselung), `503` oder `504` wird die Anfrage bis zu drei Mal direkt wiederholt. Der Connector beachtet dabei den Microsoft-Header `Retry-After`; fehlt er, wird exponentiell mit einem kleinen Zufallsanteil gewartet. Die Wartezeit ist abbrechbar, damit der Dienst sauber beendet werden kann. Jede Wiederholung erscheint mit Postfach, Vorgang, HTTP-Status und Wartezeit im Protokoll.

Nach Erreichen der maximalen Versuchszahl wird die Nachricht nach `DeadLetter` verschoben. Beim nächsten POP3-Abruf des Absenders wird sie als lokale Unzustellbarkeit angeboten. Dabei wird in derselben Sitzung nicht zusätzlich der Microsoft-365-Posteingang abgefragt. Der Ordner und das Protokoll sollten dennoch regelmäßig überwacht werden.

Wurde die Nachricht ursprünglich über EWS angenommen, erscheint dieselbe lokale Unzustellbarkeit außerdem im EWS-Posteingang des Absenders. `FindItem`, `SyncFolderItems` und EWS-Pull-Benachrichtigungen liefern dabei dieselbe stabile lokale Nachrichten-ID; dadurch wird sie nicht bei jeder Abfrage erneut ins ERP übertragen. Erst eine ausdrücklich erlaubte EWS-Löschung entfernt den Eintrag aus `DeadLetter`.

> **Abgrenzung:** Diese lokale Rückmeldung betrifft Fehler, bei denen die Übergabe an Microsoft Graph endgültig scheitert. Nimmt Microsoft 365 die Mail zunächst an und erzeugt erst später einen eigenen Zustellbericht, ist dieser Bericht eine normale Nachricht im Exchange-Online-Posteingang und wird im vollständigen Posteingangsmodus regulär synchronisiert.

> **Hinweis:** In einem seltenen Grenzfall kann eine Nachricht doppelt versendet werden, wenn Microsoft 365 die Nachricht angenommen hat, die Bestätigung den Connector aber nicht mehr erreicht.

Protokollierung

Das Live-Protokoll befindet sich in der Oberfläche unter **Live-Protokoll**. Die Protokolldateien liegen zusätzlich unter:

```
<Datenpfad>\Log
```

Das getrennte EWS-/Graph-Diagnoseprotokoll wird bei aktivierter Detailstufe als folgende Tagesdatei geführt:

```
<Datenpfad>\Log\MailBridge365-EWS-Graph-yyyy-MM-dd.log
```

Das Protokoll enthält unter anderem:

- Start und Ende des Connectors
- Angenommene und abgewiesene Verbindungen
- Versandstatus und Warteschlangen-ID
- POP3-Anmeldungen und Abrufstatus
- OAuth2- und Microsoft-Graph-Fehler
- Wiederholungsversuche und Dead-Letter-Vorgänge
- ungültige Lizenz und die dadurch wirksame Benutzerbegrenzung
- gesperrte oder entsperrte Benutzerkonten
- bewusst deaktivierte oder lizenzbedingt nicht bereitgestellte Postfächer
- automatisch deaktivierte Journalfunktion

Der bereinigte SMTP- und POP3-Dialog wird immer aufgezeichnet. Er ist nicht von der Einstellung **Ausführliche Debugprotokollierung** abhängig. `C:` kennzeichnet Befehle des Clients, `S:` die Antworten des Connectors. Eine kurze Sitzungskennung verbindet zusammengehörige Zeilen auch bei mehreren gleichzeitigen Verbindungen:

Unbekannte Befehle werden mit ihrem tatsächlichen Befehlsnamen protokolliert. Nicht druckbare Binärdaten, beispielsweise ein irrtümlich direkt gesendeter TLS-Handshake, erscheinen als kurze Hex-Darstellung. Nur die Argumente bleiben aus Sicherheitsgründen ausgeblendet.

```
[PROTOCOL] SMTP[a1b2c3d4] C: EHLO altsystem
[PROTOCOL] SMTP[a1b2c3d4] C: AUTH LOGIN <Anmeldedaten ausgeblendet>
[PROTOCOL] SMTP[a1b2c3d4] S: 235 2.7.0 Authentication successful
[PROTOCOL] SMTP[a1b2c3d4] C: <DATA-Inhalt ausgeblendet; 18425 Bytes>

[PROTOCOL] POP3[e5f6a7b8] C: USER postfach@firma.at
[PROTOCOL] POP3[e5f6a7b8] C: PASS <Kennwort ausgeblendet>
[PROTOCOL] POP3[e5f6a7b8] S: +OK 3 messages
[PROTOCOL] SMTP[a1b2c3d4] C: Unbekannter Befehl: XCLIENT; Argumente ausgeblendet
```

Folgende Inhalte werden niemals in das normale Live- und Hauptprotokoll übernommen:

- Kennwörter hinter `PASS`
- Base64-Anmeldedaten von SMTP `AUTH LOGIN` und `AUTH PLAIN`
- OAuth2-Tokens und Client Secrets
- SMTP-Nachrichteninhalt nach `DATA`
- über POP3 übertragener MIME-Nachrichteninhalt
- Argumente unbekannter SMTP- oder POP3-Erweiterungsbefehle

Bei POP3-Kommandos wie `LIST` und `UIDL` werden die normalen Serverzeilen mitgeführt. Bei großen Postfächern können die täglichen Protokolldateien deshalb deutlich wachsen und sollten hinsichtlich Speicherverbrauch überwacht werden.

Der allgemeine Debugmodus ergänzt unabhängig davon weitere technische Diagnoseinformationen im Hauptprotokoll. Kennwörter, Client Secrets, OAuth-Tokens und Nachrichtentexte werden dort ebenfalls nicht protokolliert. Aktivieren Sie den Debugmodus nur während der Fehlersuche und deaktivieren Sie ihn danach wieder.

Getrenntes EWS-/Graph-Diagnoseprotokoll

Für eine gezielte Schnittstellenanalyse stehen vier Detailstufen zur Verfügung:

Stufe	Inhalt
`0 – Aus`	Es wird keine separate EWS-/Graph-Datei geschrieben
`1 – Standard`	Vorgang, betroffenes Postfach, Ergebnis, HTTP-Status und EWS-Antwortcode
`2 – Detailliert`	Zusätzlich Ziel-URLs, Laufzeiten, Datenmengen, Wiederholungen und vollständige Fehlerdetails
`3 – Protokoll`	Zusätzlich bereinigte HTTP- und SOAP-Protokolldaten

Die Option **Mailinhalte protokollieren** wirkt ausschließlich zusammen mit Stufe 3. Ist sie deaktiviert, werden EWS-Felder wie `MIMEContent`, `Body` und `Content` durch einen Platzhalter mit Zeichenanzahl ersetzt. Ist sie aktiviert, können Mailtext, MIME-Daten und Anlageninhalte personenbezogene oder vertrauliche Daten enthalten. Einzelne Mailinhalte werden deshalb auf 64 KiB und komplette Protokolleinträge auf 256 KiB begrenzt. Die Option sollte nur für eine konkrete Fehlersuche und nur so kurz wie erforderlich eingeschaltet werden.

Kennwörter, Client Secrets, OAuth-Tokens und der Wert des HTTP-Headers `Authorization` werden unabhängig von Detailstufe und Inhaltsoption niemals ausgegeben. Die Detailstufe `3 – Protokoll` kann dennoch große Tagesdateien erzeugen; freier Speicherplatz und Aufbewahrung der Dateien sind zu überwachen.

Microsoft-Graph-Aktivitäten

Die wichtigsten Microsoft-Graph-Aktionen werden unabhängig vom Debugmodus mit der Stufe `[GRAPH]` protokolliert. Damit ist erkennbar, ob der Connector gerade sendet, den Posteingang auflistet oder eine Nachricht für POP3 abruft.

Beim Versand enthält das Protokoll unter anderem:

- Queue-ID und verwendetes Absendepostfach
- Anzahl der Empfänger und MIME-Gesamtgröße, jedoch keine Empfängeradressen
- gewählter Versandweg: direkt oder über Entwurf und Upload-Sitzung
- Anzahl und Gesamtgröße der Anhänge, jedoch keine Dateinamen oder Inhalte

- Fortschritt großer Anhänge pro Datenblock
- verkürzte Graph-Nachrichtenkennung und HTTP-Status

Beim POP3-Abruf enthält es unter anderem:

- abgefragtes Postfach und eingestelltes Nachrichtenlimit
- Nummer und Größe jeder abgerufenen Posteingangsseite
- Anzahl geprüfter, bereits übertragener und angebotener Nachrichten
- Beginn und Ende eines MIME-Abrufs einschließlich Byteanzahl
- Markierung als gelesen oder Löschung über Microsoft Graph
- automatische Wiederholungen mit HTTP-Status, Wiederholungsnummer und Wartezeit
- Hinweis, wenn Graph wegen lokaler Unzustellbarkeiten oder einer Benutzereinstellung bewusst nicht abgefragt wird

Auch die Anforderung eines OAuth2-Access-Tokens wird mit HTTP-Status und Gültigkeitsende protokolliert. Das Token selbst, Client Secret, Mailbetreff, Nachrichtentext, Anhanginhalte und Empfängeradressen werden nicht ausgegeben.

```
[GRAPH] Versand startet; Queue-ID=...; Postfach=versand@firma.at; Empfänger=2; MIME-
Bytes=18425
[GRAPH] Direkter Versand beantwortet; Queue-ID=...; Postfach=versand@firma.at; HTTP=202
[GRAPH] POP3-Abruf startet; Postfach=einkauf@firma.at; maximales Angebot=100
[GRAPH] POP3-Abrufliste fertig; Postfach=einkauf@firma.at; geprüft=12; bereits übertragen=9;
angeboten=3
```

Bei aktivierter Dublettenvermeidung bestätigt das detaillierte EWS-Protokoll die Unterdrückung einer eigenen Versandkopie beispielsweise mit:

```
[EWS-DETAIL] Eigene Versandkopie nicht erneut an den EWS-Client übertragen; Postfach=...;
Graph-ID=...; Message-ID=...
```

Funktionstest

SMTP testen

Im Programmordner befindet sich das Testskript `Test-SmtpProxy.ps1`.

```
.\Test-SmtpProxy.ps1 `
    -From "rechnung@firma.at" `
    -To "empfaenger@firma.at"
```

Test mit Anhang:

```
.\Test-SmtpProxy.ps1 `
    -From "rechnung@firma.at" `
    -To "empfaenger@firma.at" `
    -AttachmentPath "C:\Temp\Test.pdf"
```

Kontrollieren Sie anschließend:

1. Die Meldung im Live-Protokoll.
2. Den Eingang beim Empfänger.
3. Den Ordner **Gesendete Elemente** des verwendeten Absendepostfachs.

POP3 testen

Im Programmordner befindet sich das Testskript `Test-Pop3Proxy.ps1`.

```
.\Test-Pop3Proxy.ps1 -Mailbox "eingang@firma.at"
```

Das Skript zeigt den Postfachstatus und die UIDL-Liste an. Es ruft keine Nachricht vollständig ab und löscht keine Nachricht.

Fehlerbehebung

Lokale Instanz startet nicht

Prüfen Sie:

- Sind Tenant-ID, Client-ID, Benutzername und erlaubte Absender ausgefüllt?
- Wurden das gemeinsame Kennwort und das Client Secret gespeichert?
- Ist der SMTP- oder POP3-Port bereits durch einen anderen Prozess belegt?
- Ist bei aktiviertem TLS ein gültiger Zertifikat-Thumbprint hinterlegt?
- Erscheint `454 TLS not available`, ist kein verwendbares Zertifikat geladen. Prüfen Sie den Zertifikatsspeicher `Lokaler Computer\Persönlich`, den Thumbprint, den privaten Schlüssel und gegebenenfalls die Option für ungültige/selbstsignierte Zertifikate. Als Notlösung kann die automatische Zertifikatserstellung aktiviert werden.
- Besitzt die Anwendung Zugriff auf den Datenpfad?

Öffnen Sie anschließend das Live-Protokoll und aktivieren Sie bei Bedarf vorübergehend den Debugmodus.

Fehlende NuGet-, PHX- oder SQLite-Laufzeitdatei

Eine erfolgreiche Kompilierung garantiert bei einem klassischen .NET-Framework-Projekt nicht, dass alle indirekten Abhängigkeiten einer referenzierten DLL im Zielordner liegen. Die Konfigurationsdatei des `PHXFramework.dll` wird ebenfalls nicht automatisch in die Konfiguration des Hauptprogramms übernommen. Deshalb müssen immer die EXE-Konfiguration, alle verwalteten

DLLs und der vollständige Ordner `runtimes` ausgeliefert werden.

Der Connector prüft die wichtigsten Dateien vor dem Start der PHX-Lizenzierung. Fehlende Dateien werden gesammelt angezeigt und zusätzlich in `MailBridge365-StartupError.log` protokolliert, sofern der Ordner beschreibbar ist. Bei `Library e_sqlite3 not found` muss insbesondere folgende Datei für einen normalen 64-Bit-Prozess vorhanden sein:

```
runtimes\win-x64\native\e_sqlite3.dll
```

Führen Sie in Visual Studio **NuGet-Pakete wiederherstellen**, anschließend **Projektmappe bereinigen** und **Projektmappe neu erstellen** aus. Der Build bricht nun bereits ab, falls die nativen SQLite-Dateien des Pakets `SQLitePCLRaw.bundle_e_sqlite3` nicht verfügbar sind.

Verschlüsselte Kennwort- oder Secret-Datei wurde nicht gefunden

Öffnen Sie die Einstellungen und geben Sie je nach Meldung das gemeinsame SMTP/POP3-Kennwort, das OAuth-Client-Secret oder das gemeinsame EWS-Kennwort erneut ein. Kontrollieren Sie außerdem den Datenpfad. Die verschlüsselten Dateien werden automatisch im Unterordner `Secrets` abgelegt; der Wert kann nicht aus der Konfigurationsdatei rekonstruiert werden.

Windows-Dienst startet nicht

Prüfen Sie zusätzlich:

- Befindet sich die EXE noch im Ordner, aus dem der Dienst installiert wurde?
- Ist `MailBridge365.settings.config` weiterhin neben der EXE vorhanden?
- Besitzt `NETWORK SERVICE` Zugriff auf Programm- und Datenpfad?
- Besitzt `NETWORK SERVICE` Änderungsrechte auf `<Datenpfad>\State`?
- Ist ein konfigurierter UNC-Pfad beim Systemstart erreichbar?
- Kann der Computer die Microsoft-Endpunkte über HTTPS erreichen?

OAuth2-Anmeldung schlägt fehl

Typische Ursachen sind:

- falsche Tenant-ID
- falsche Client-ID
- abgelaufenes oder falsch eingetragenes Client Secret
- fehlende Administratorzustimmung
- blockierter Zugriff auf `login.microsoftonline.com`

Erstellen Sie bei einem abgelaufenen Secret ein neues Secret in Microsoft Entra ID und speichern Sie den neuen Wert anschließend in der Oberfläche.

Microsoft Graph antwortet mit 403 Forbidden

Prüfen Sie:

- Sind `Mail.Send`, `Mail.ReadWrite` und `User.Read.All` als Anwendungsberechtigungen vorhanden?
- Sind bei aktiviertem Termin-/Kontaktabgleich zusätzlich `Calendars.Read` und `Contacts.Read` als Anwendungsberechtigungen vorhanden?
- Wurde die Administratorzustimmung erteilt?
- Enthält ein verwendeter Exchange-RBAC-Bereich das betroffene Postfach?
- Existiert das Absendepostfach und ist es für den Versand geeignet?

POP3 meldet „mailbox is temporarily unavailable“

Prüfen Sie:

- Ist die vollständige Postfachadresse oder deren Domain erlaubt?
- Kann Microsoft Graph das Postfach öffnen?
- Ist bereits eine andere POP3-Sitzung für dasselbe Postfach aktiv?
- Besitzt die Entra-Anwendung `Mail.ReadWrite` für dieses Postfach?
- Ist das gemeinsame lokale Kennwort korrekt?

Bei einem Konto aus der Benutzerverwaltung prüfen Sie zusätzlich das individuelle Kennwort, den Kontostatus und die Option **Exchange-Online-Abruf**.

Die konkrete Microsoft-Graph-Fehlermeldung steht im Live-Protokoll.

Nachricht bleibt in Pending

Der Connector versucht vorübergehend fehlgeschlagene Nachrichten automatisch erneut zu senden. Prüfen Sie im Protokoll den letzten Fehler und die Warteschlangen-ID. Bei einem dauerhaften Fehler müssen Absenderfreigabe, Microsoft-365-Berechtigungen, Nachrichtengröße und Empfänger geprüft werden.

Nachricht liegt in DeadLetter

Beheben Sie zuerst die im Protokoll angegebene Ursache. Verschieben oder verarbeiten Sie die Dateien im Ordner `DeadLetter` nur nach Rücksprache mit dem zuständigen Support, damit keine Nachricht beschädigt oder doppelt versendet wird.

Nachricht erscheint im ERP doppelt unter Gesendete Elemente

Aktivieren Sie beim betroffenen Benutzer sowohl **Nur Mailversand und den Ordner „Gesendete Elemente“ synchronisieren** als auch **Doppelte Mails im Ordner „Gesendete Elemente“ vermeiden**. Die zweite Option ist nur in dieser Kombination wirksam. Starten Sie danach den Abgleich erneut und kontrollieren Sie bei Bedarf das EWS-/Graph-Protokoll.

Die Einstellung verhindert künftige doppelte Rückübertragungen von Nachrichten, die über den Connector versendet wurden. Sie löscht keine bereits vorhandenen Dubletten aus dem ERP. Versandkopien, die außerhalb des Connectors entstanden sind, werden weiterhin übertragen.

Betrieb und Wartung

- Überwachen Sie regelmäßig das Live-Protokoll und den Ordner `DeadLetter`.
- Kontrollieren Sie den freien Speicherplatz des Datenpfads.
- Sichern Sie Konfiguration, Warteschlange, POP3-Status und Geheimnisdateien.
- Erneuern Sie das Client Secret rechtzeitig vor dessen Ablauf.
- Prüfen Sie nach Änderungen in Microsoft 365 den SMTP- und POP3-Zugriff.
- Halten Sie die Listen erlaubter IP-Adressen und Postfächer möglichst klein.
- Deaktivieren Sie die Debugprotokollierung nach abgeschlossener Fehlersuche.

Datensicherung

Für eine vollständige Sicherung sollten folgende Daten gemeinsam gesichert werden:

```
MailBridge365.settings.config
<Datenpfad>\Queue
<Datenpfad>\Mailboxes
<Datenpfad>\State
<Datenpfad>\Certificates
<Datenpfad>\Secrets
<Datenpfad>\Users
<Datenpfad>\Actions
```

Der Ordner `<Datenpfad>\Log` kann für Nachweis- und Diagnosezwecke zusätzlich gesichert werden, ist für eine technische Wiederherstellung aber nicht erforderlich. Programmdateien werden aus dem zur gesicherten Version passenden Installationspaket wiederhergestellt; die vollständige Laufzeitumgebung einschließlich `runtimes` und der DLL-Dateien muss dabei erhalten bleiben.

Die Geheimnisdateien sind über Windows DPAPI an den lokalen Computer gebunden. Eine reine Kopie auf einen anderen Computer reicht daher nicht aus. Auf einem neuen Computer müssen das gemeinsame Kennwort und das Client Secret erneut über die Oberfläche gespeichert werden.

Deinstallation

1. Starten Sie `MailBridge365.exe` mit Administratorrechten.
2. Öffnen Sie **Übersicht**.
3. Wählen Sie **Dienst deinstallieren**.
4. Bestätigen Sie die Sicherheitsabfrage und die Windows-Administratorabfrage.
5. Prüfen Sie, ob der Dienst als **Nicht installiert** angezeigt wird.

Die Deinstallation entfernt ausschließlich die Registrierung des Windows-Dienstes. Programmdateien, Konfiguration, Warteschlange, POP3-Status, verschlüsselte Geheimnisse und

Protokolle bleiben erhalten und können nach einer abschließenden Datensicherung manuell entfernt werden.

Supportinformationen

Stellen Sie bei einer Supportanfrage möglichst folgende Informationen bereit:

- Zeitpunkt des Fehlers
- betroffene Funktion: SMTP, POP3, OAuth2 oder Dienststart
- verwendetes Absender- beziehungsweise POP3-Postfach
- relevante Meldungen aus dem Live-Protokoll
- aktivierte Netzwerk- und TLS-Einstellungen
- Information, ob der Fehler dauerhaft oder nur zeitweise auftritt

Übermitteln Sie niemals das gemeinsame SMTP/POP3-Kennwort, das Client Secret oder OAuth-Tokens per unverschlüsselter E-Mail.

Revision #21
Created 2026-09-02 15:47:34 CEST by Martin Dauwa
Updated 2026-09-16 11:36:05 CEST by Martin Dauwa