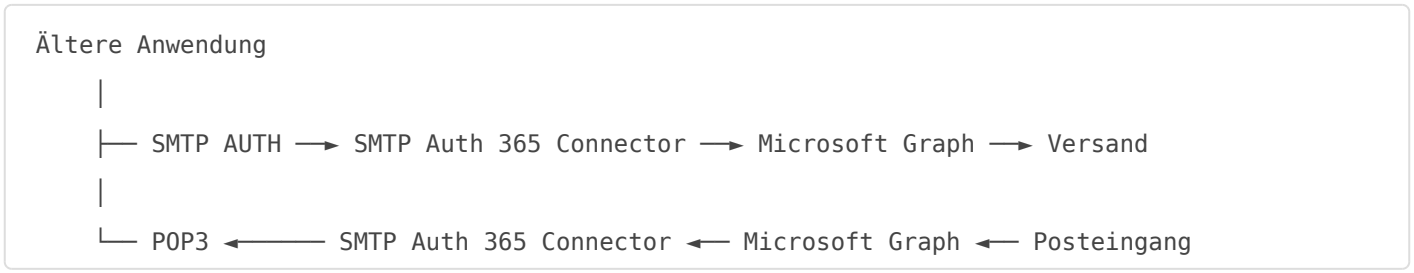
Allgemeine Dokumentation – SMTP-/POP3-Anbindung für Microsoft 365

Überblick

SMTP Auth 365 Connector verbindet ältere Anwendungen und Mailprogramme mit Microsoft 365. Die angebundene Anwendung kann weiterhin klassisches SMTP AUTH für den Versand und POP3 für den Abruf 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.

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
- 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
- Optionale Mail-Steuerfelder mit 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

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 `SMTP Auth 365 Connector`.
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

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:\SMTPAuth365Connector
```

3. Verschieben oder löschen Sie diesen Ordner nach der Dienstinstallation nicht.
4. Starten Sie `SMTPAuth365Connector.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.

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
```

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 oder eines eigenen Secret-Dateipfads, 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
- **Einstellungen:** Konfiguration von Allgemein, POP3, SMTP, Microsoft Graph und Mail-Steuerfeldern
- **Live-Protokoll:** Laufende Diagnosemeldungen mit farblicher Kennzeichnung

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
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

Bei leerem Datenpfad verwendet die Anwendung folgende Ordner:

```
<Programmordner>
├── Logs
├── Pop3State
├── Queue
├── Secrets
├── Users
└── Actions
```

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 SMTP

Feld	Beschreibung	Beispiel
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`

Feld	Beschreibung	Beispiel
Gemeinsames SMTP/POP3-Kennwort	Gemeinsames lokales Kennwort	Sicheres, eigenes Kennwort
Kennwortdatei	Optionaler abweichender Speicherort	Leer lassen
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.

> **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`

Feld	Beschreibung	Empfehlung
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

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 **POP3-/SMTP-Benutzer verwalten** 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	Lädt den Posteingang zusätzlich über Microsoft Graph
Konto gesperrt	Verhindert POP3- und SMTP-Anmeldungen dieses Kontos

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

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.

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-Steuerfelder

Feld	Beschreibung
Mail-Steuerfelder auswerten	Aktiviert oder deaktiviert die Funktion global
Eingehende E-Mails (POP3) prüfen	Wertet Steuerfelder beim Abruf einer Nachricht über POP3 aus
Ausgehende E-Mails (SMTP) prüfen	Wertet Steuerfelder beim Versand einer Nachricht über SMTP aus
Erkannte Steuerfelder 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 Steuerfelder erfolgt nur, wenn mindestens ein gültiges Steuerfeld erkannt und in eine INI-Datei übernommen wurde. Anlagen werden nicht verändert.

Steuerfelder 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
Secret-Datei	Optionaler abweichender Speicherort	Leer lassen
Graph-Basisadresse	Microsoft-Graph-Endpunkt	`https://graph.microsoft.com/v1.0`
OAuth-Scope	OAuth2-Berechtigungsbereich	`https://graph.microsoft.com/.default`

Kennwort und Client Secret werden verschlüsselt für den lokalen Computer gespeichert. Nach dem Speichern zeigt die Oberfläche `********` an. Dies bedeutet, dass bereits ein Wert vorhanden ist. Der Platzhalter wird nicht als Kennwort gespeichert.

Einstellungen speichern

1. Tragen Sie alle erforderlichen Werte ein.
2. Wählen Sie **Speichern**.
3. Die Anwendung schreibt die Eingaben dauerhaft in `SMTPAuth365Connector.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 `SMTPAuth365Connector.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`.

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-SMTPAuth365Connector-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 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.
- Ein Verbindungsabbruch vor `QUIT` führt im Löschmodus nicht zur Löschung.
- `RSET` hebt Löschvormerkungen der aktuellen Sitzung auf.

Der lokale Übertragungsstatus befindet sich standardmäßig unter:

```
<Programmordner>\Pop3State
```

Löschen Sie diesen Ordner 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.

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.

> **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>\Logs
```

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

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

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
- 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
```

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.

Verschlüsselte Kennwort- oder Secret-Datei wurde nicht gefunden

Öffnen Sie die Einstellungen und geben Sie je nach Meldung das gemeinsame SMTP/POP3-Kennwort oder das OAuth-Client-Secret erneut ein. Kontrollieren Sie außerdem den in der Meldung angegebenen Daten- beziehungsweise Secret-Pfad. 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 `SMTPAuth365Connector.settings.config` weiterhin neben der EXE vorhanden?
- Besitzt `NETWORK SERVICE` Zugriff auf Programm- und Datenpfad?
- 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` und `Mail.ReadWrite` 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.

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:

```
SMTPAuth365Connector.settings.config
<Datenpfad>\Queue
<Datenpfad>\Pop3State
<Datenpfad>\Secrets
<Datenpfad>\Users
<Datenpfad>\Actions
```

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 `SMTPAuth365Connector.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 #15
Created 2026-09-02 15:47:34 CEST by Martin Dauwa
Updated 2026-09-11 16:11:21 CEST by Martin Dauwa