Konfigurationsbeschreibung für die Microsoft 365-Einrichtung

ERPAUSTRIA
Business solutions]

> **Technikerunterlage**
> App-Registrierung, Microsoft-Graph-Berechtigungen und sichere Datenübergabe für die Installation am Windows Server.
> **Stand:** 11. September 2026 | **Dokumentversion:** 1.0

> SMTP_Auth_365_Connector_Microsoft_365_Einrichtung.pdf

Ziel dieser Anleitung

Der SMTP Auth 365 Connector ist ein lokaler Windows-Dienst. Er ermöglicht bestehenden Anwendungen den Versand per SMTP AUTH sowie bei Bedarf den Abruf per POP3 oder HTTPS-Webclient. Gegenüber Microsoft 365 meldet sich der Dienst ohne interaktive Benutzeranmeldung über OAuth2 und Microsoft Graph an.

Nach Abschluss dieser Anleitung sind:

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

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

Inhaltsübersicht

---

1. Auftrag und Voraussetzungen

Funktionsweise

```
Bestehende Anwendung
        |
        | SMTP AUTH / POP3
        v
SMTP Auth 365 Connector auf dem Windows Server
        |
        | OAuth2 Client Credentials / HTTPS
        v
Microsoft Entra ID und Microsoft Graph
        |
        v
Exchange Online
```

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

Voraussetzungen in Microsoft 365

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

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

Voraussetzungen am Windows Server

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

Vor Beginn festlegen

- ☐ Welche Postfächer dürfen Nachrichten versenden?
- ☐ Welche Postfächer dürfen über POP3 oder den Webclient gelesen werden?
- ☐ Sollen abgerufene Nachrichten in Exchange als gelesen markiert werden?
- ☐ Dürfen Nachrichten nach erfolgreichem POP3-Abruf gelöscht werden?
- ☐ Darf ein POP3-Client mit `DELE` Nachrichten in Exchange löschen?
- ☐ Soll das lokale Journalpostfach aktiviert werden?
- ☐ Soll Exchange den App-Zugriff serverseitig auf bestimmte Postfächer begrenzen?
- ☐ Wer ist für die Erneuerung des Client Secrets verantwortlich?

Benötigte Microsoft-Graph-Rechte

Berechtigung	Typ	Verwendung
`Mail.Send`	Application / Anwendung	Versand aus den freigegebenen Exchange-Online-Postfächern
`Mail.ReadWrite`	Application / Anwendung	Abruf, Gelesen-Markierung, Löschung und Entwurfsverarbeitung großer Nachrichten

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

---

2. App in Microsoft Entra ID registrieren

Microsoft Entra Admin Center öffnen

Öffnen Sie:

https://entra.microsoft.com

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

Navigation

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

Registrierung durchführen

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

   ```
   SMTP Auth 365 Connector - <Kundenname>
   ```

3. Wählen Sie als unterstützten Kontotyp:

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

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

Werte sofort erfassen

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

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

---

3. Microsoft-Graph-Berechtigungen vergeben

Navigation

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

Rechte hinzufügen

1. Wählen Sie **Microsoft Graph**.
2. Wählen Sie **Application permissions / Anwendungsberechtigungen**.
3. Wählen Sie ausdrücklich **nicht** die delegierten Berechtigungen.
4. Suchen Sie nach `Mail.Send` und markieren Sie diese Berechtigung.
5. Suchen Sie nach `Mail.ReadWrite` und markieren Sie diese Berechtigung.
6. Bestätigen Sie mit **Add permissions / Berechtigungen hinzufügen**.

Warum werden zwei Rechte benötigt?

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

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

Der Connector benötigt `Mail.ReadWrite` zusätzlich für:

- POP3- und Webclient-Abruf,
- Markieren als gelesen,
- Löschen von Exchange-Nachrichten,
- Erstellen und Verarbeiten von Entwürfen bei großen Nachrichten,
- Upload-Sitzungen für große Anhänge.

Nicht benötigtes Standardrecht entfernen

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

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

---

4. Administratorzustimmung erteilen

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

Navigation

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

Zustimmung durchführen

1. Wählen Sie **Grant admin consent for `<Tenant>`** beziehungsweise **Administratorzustimmung für `<Tenant>` erteilen**.
2. Kontrollieren Sie den Sicherheitsdialog.

3. Erwartet werden ausschließlich die benötigten Microsoft-Graph-Rechte `Mail.Send` und `Mail.ReadWrite`.
4. Klären Sie unerwartete zusätzliche Rechte, bevor Sie zustimmen.
5. Bestätigen Sie die Zustimmung.
6. Aktualisieren Sie die Ansicht.
7. Prüfen Sie bei beiden Rechten den grünen Status **Granted for `<Tenant>` / Gewährt für `<Tenant>`**.

Erwarteter Sollzustand

Eintrag	Typ	Status
Microsoft Graph `Mail.Send`	Application	Granted for `<Tenant>`
Microsoft Graph `Mail.ReadWrite`	Application	Granted for `<Tenant>`
Delegierte Rechte	Nicht benötigt	Keine erforderlich

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

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

---

5. Client Secret erstellen und sichern

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

Navigation

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

Secret erstellen

1. Tragen Sie eine nachvollziehbare Beschreibung ein, beispielsweise:

   ```
   SMTP Auth 365 Connector - Windows Server <SERVERNAME>
   ```

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

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

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

Sichere Übermittlung

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

Geeignete Übertragungswege sind beispielsweise:

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

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

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

---

6. Postfachzugriff sinnvoll begrenzen

Basisbetrieb

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

Die Entra-Anwendungsberechtigungen `Mail.Send` und `Mail.ReadWrite` erlauben technisch jedoch grundsätzlich Zugriff auf alle Exchange-Online-Postfächer des Tenants, solange Exchange keine zusätzliche Einschränkung erzwingt.

Erhöhte Absicherung mit Exchange Application RBAC

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

Empfohlene Vorgehensweise:

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

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

Legacy Application Access Policies

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

Für die Einrichtung der Einschränkung werden benötigt:

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

---

7. Datenübergabe an den Windows-Techniker

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

Microsoft-365- und Entra-Daten

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

Postfächer und Funktionen

Feld	Einzutragender Wert
Versandpostfächer	_____
Weitere Versandpostfächer	_____
POP3-/Webclient-Postfächer	_____
Weitere Abrufpostfächer	_____
Exchange-Abruf	[ ] aktiv [ ] nicht benötigt
Nach `RETR` als gelesen markieren	[ ] ja [ ] nein
Automatisch nach Abruf löschen	[ ] ja [ ] nein
POP3-`DELE` an Exchange weitergeben	[ ] erlauben [ ] nicht erlauben
Journalpostfach	[ ] aktivieren [ ] zunächst deaktiviert lassen

Server- und Netzwerkdaten

Feld	Einzutragender Wert
Windows-Servername	_____
Installationspfad	_____
Datenpfad	_____
Dienstkonto	_____
SMTP-Adresse und Port	_____
POP3-Adresse und Port	_____
Webclient-Adresse und Port	_____
Erlaubte Client-IP-Adressen	_____
Proxy erforderlich	[ ] nein [ ] ja: _____

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

---

8. Vorbereitung und Einrichtung am Windows Server

Netzwerk prüfen

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

Microsoft-Graph-Felder im Connector

Connector-Feld	Wert oder Quelle
`TenantId`	Directory (tenant) ID aus der Entra-App
`ClientId`	Application (client) ID aus der Entra-App
Client Secret	Inhalt der Spalte Value / Wert; lokal eingeben
`GraphBaseUrl`	`https://graph.microsoft.com/v1.0`
`OAuthScope`	`https://graph.microsoft.com/.default`
Parallele Graph-Anfragen je Postfach	Standard `2`
Wiederholungen bei Graph-Drosselung	Standard `3`

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

Geheimnisse speichern

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

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

Benutzer und Postfächer einrichten

1. Legen Sie die benötigten lokalen POP3-/SMTP-Benutzer an.
2. Verwenden Sie vollständige Mailadressen als Benutzernamen.
3. Aktivieren Sie den Exchange-Online-Abruf nur bei den dafür vorgesehenen Benutzern.
4. Legen Sie die erlaubten SMTP-Absender fest.
5. Aktivieren Sie Löschfunktionen nur entsprechend der dokumentierten Kundenentscheidung.
6. Vergeben Sie für das Journalpostfach ein eigenes lokales Kennwort.
7. Aktivieren Sie die Journalfunktion erst nach erfolgreichem Funktionstest und wenn sie tatsächlich benötigt wird.

---

9. Abnahme und Funktionstest

OAuth2 und Dienststart

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

SMTP-Versand

- ☐ Eine Testmail wird aus einem erlaubten Postfach versendet.
- ☐ Der Graph-Aufruf endet mit HTTP 202.
- ☐ Die Nachricht liegt im Ordner **Gesendete Elemente** des Absenders.
- ☐ Ein nicht erlaubter Absender wird lokal abgewiesen.
- ☐ Wenn große Nachrichten benötigt werden, wurde zusätzlich eine Nachricht mit großem Anhang getestet.

POP3 und Webclient

- ☐ Eine vorhandene Nachricht wird angezeigt.
- ☐ Die Nachricht kann vollständig abgerufen werden.
- ☐ Die UIDL bleibt bei wiederholter Anmeldung stabil.
- ☐ Die Gelesen-Markierung entspricht der Kundenentscheidung.
- ☐ Die Löschfunktion entspricht der Kundenentscheidung.

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

Journal

☐ Es existiert nur ein Journalpostfach.

☐ Das Journalpostfach hat ein eigenes lokales Kennwort.

☐ Die Journalfunktion ist nur bei tatsächlichem Bedarf aktiviert.

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

☐ Das Journalpostfach versendet keine Nachrichten.

Exchange Application RBAC

☐ Ein erlaubtes Postfach kann verwendet werden.

☐ Ein Postfach außerhalb des Scopes wird abgewiesen.

☐ Versand und Lesezugriff wurden getrennt geprüft.

Abschluss

☐ Secret-Ablaufdatum ist dokumentiert.

☐ Verantwortliche Person für die Rotation ist festgelegt.

☐ Installations- und Datenpfad sind dokumentiert.

☐ Firewall- und Proxy-Freigaben sind dokumentiert.

☐ Kundenspezifische Lösch- und Journalentscheidungen sind dokumentiert.

---

10. Fehlerzuordnung

Symptom	Wahrscheinliche Ursache und Prüfung
`AADSTS7000215` oder `invalid_client`	Falscher Secret-Wert, Secret-ID statt Value, falsche Client-ID oder abgelaufenes Secret
HTTP 401	Tenant-ID, Client-ID, Client Secret und Token-Endpunkt prüfen
HTTP 403	Admin Consent, Typ Application, Exchange Application RBAC und vorhandene Legacy Application Access Policies prüfen

Symptom	Wahrscheinliche Ursache und Prüfung
HTTP 404 beim Postfach	Mailadresse, Exchange-Online-Lizenz und tatsächliche Postfachexistenz prüfen
HTTP 429	Microsoft-Graph-Drosselung; `Retry-After` wird automatisch beachtet
HTTP 503 oder 504	Temporäre Microsoft-Störung; automatische Wiederholung und Protokoll prüfen
Kleine Nachrichten funktionieren, große nicht	`Mail.ReadWrite` im wirksamen Scope sowie Graph-/Outlook-Upload-Endpunkte prüfen
Token funktioniert, bestimmtes Postfach nicht	Exchange Application RBAC oder Legacy Application Access Policy prüfen
Keine POP3-Nachrichten	Exchange-Abruf beim Benutzer, lokale Übertragungs-UIDLs und Postfachinhalt prüfen

Typische Verwechslungen

Falsch	Richtig
Object-ID als Client-ID verwendet	Application (client) ID verwenden
Secret-ID als Kennwort verwendet	Client-Secret-Value verwenden
Delegierte Rechte eingetragen	Application permissions verwenden
Rechte hinzugefügt, aber keine Zustimmung erteilt	Grant admin consent ausführen
Persönliches Microsoft-365-Kennwort eingetragen	Lokales Connector-Kennwort beziehungsweise App-Secret verwenden
Shared-Mailbox nicht im Exchange-Scope	Alle verwendeten Shared-/Funktionspostfächer aufnehmen

---

11. Secret-Erneuerung

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

Empfohlener Ablauf

1. Mindestens 30 Tage vor Ablauf ein neues Client Secret in derselben App-Registrierung erstellen.
2. Den neuen **Value / Wert** sofort sicher erfassen.
3. Wartungsfenster abstimmen.
4. Neues Secret in der Connector-Oberfläche am Windows Server eingeben.
5. Einstellungen speichern und Dienst neu starten.

6. OAuth2-Anmeldung und Testversand prüfen.
7. Falls verwendet, POP3 und Webclient prüfen.
8. Erst nach erfolgreicher Abnahme das alte Secret in Entra ID löschen.
9. Neues Ablaufdatum und nächste Erinnerung dokumentieren.

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

---

12. Offizielle Microsoft-Quellen

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

> **Dokumentationsstand:** Diese Anleitung wurde am 11. September 2026 geprüft. Microsoft kann Portalbezeichnungen, Rollen, Grenzwerte und Empfehlungen ändern. Bei Abweichungen haben die verlinkten Microsoft-Learn-Seiten und die Sicherheitsrichtlinien des Kunden-Tenants Vorrang.

Interne Dokumentation

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

Feld	Eintrag
Nächster Secret-Wechsel spätestens am	_____

Revision #8
Created 2026-09-11 16:00:38 CEST by Martin Dauwa
Updated 2026-09-11 16:12:37 CEST by Martin Dauwa