

MICROSOFT 365 | TECHNISCHE EINRICHTUNG

SMTP Auth 365 Connector

App-Registrierung, Microsoft-Graph-Berechtigungen und sichere Übergabe für die Installation am Windows Server

Ziel dieser Anleitung

Nach Abschluss kann der Connector ohne Benutzeranmeldung über OAuth2 auf die freigegebenen Exchange-Online-Postfächer zugreifen. Eine eigene Übergabeseite fasst alle Daten für den ausführenden Windows-Techniker zusammen.

Für Microsoft-365-, Entra- und Exchange-Administratoren



1

Auftrag und Voraussetzungen

Der Connector ist ein lokaler Windows-Dienst. Er meldet sich als eigene Anwendung an Microsoft Entra ID an und verwendet Microsoft Graph. Es meldet sich dabei kein Microsoft-365-Benutzer interaktiv an.

Microsoft 365

Aktiver Microsoft-365-Tenant mit Exchange Online und mindestens einem produktiven Postfach.

Administrator

Konto mit Berechtigung für App-Registrierungen und tenantweite Administratorzustimmung.

Windows Server

Ausgehendes HTTPS (TCP 443), funktionierende DNS-Auflösung und korrekte Systemzeit.

Sichere Übergabe

Tenant-ID und Client-ID dürfen dokumentiert werden. Der Secret-Wert wird getrennt und geschützt übergeben.

Vor Beginn festlegen

- ☐ Welche Absenderpostfächer dürfen über den Connector senden?
- ☐ Welche Postfächer dürfen über POP3 oder Webclient gelesen werden?
- ☐ Darf der Connector Nachrichten als gelesen markieren oder aus Exchange löschen?
- ☐ Soll der App-Zugriff später mit Exchange Application RBAC auf bestimmte Postfächer beschränkt werden?
- ☐ Wer ist für die rechtzeitige Erneuerung des Client Secrets verantwortlich?

Benötigte Microsoft-Graph-Anwendungsberechtigungen

Mail.Send für den Versand sowie Mail.ReadWrite für Abruf, Gelesen-Markierung und Löschung. Es sind ausdrücklich Anwendungsberechtigungen, keine delegierten Berechtigungen.

Keine Umleitungs-URI erforderlich

Der Connector verwendet den OAuth2 Client-Credentials-Flow ohne Benutzeranmeldung. Im Abschnitt Authentication / Authentifizierung muss deshalb keine Redirect URI eingetragen werden.

2

App in Microsoft Entra ID registrieren

Portal: <https://entra.microsoft.com>. Die Portalbezeichnungen können je nach Sprache als Deutsch oder Englisch erscheinen.

Navigation

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

- Richtigen Tenant prüfen
Oben rechts kontrollieren, dass der produktive Kunden-Tenant ausgewählt ist. Eine App kann später nicht in einen anderen Tenant verschoben werden.
- Neue Registrierung starten
Auf Neue Registrierung klicken.
- Name vergeben
Empfehlung: SMTP Auth 365 Connector - <Kundenname>
- Kontotyp festlegen
Nur Konten in diesem Organisationsverzeichnis / Single tenant auswählen.
- Umleitungs-URI leer lassen
Für diesen Dienst ist keine Web-, SPA- oder Public-Client-Umleitungsadresse erforderlich.
- Registrieren
Nach dem Speichern öffnet sich die Übersichtsseite der App.

Werte sofort notieren

Feld	Einzutragender Wert / Hinweis
Directory (tenant) ID	Mandanten-ID / Tenant-ID als GUID. Nicht mit der primären Domain verwechseln.
Application (client) ID	Anwendungs-ID / Client-ID als GUID. Nicht die Object-ID verwenden.
Display name	Vergebener App-Name, damit die Registrierung später eindeutig gefunden wird.

Nicht verwechseln

Für die Windows-Konfiguration werden Directory (tenant) ID und Application (client) ID benötigt. Die Objekt-ID der App oder des Enterprise-Application-Service-Principals ist dafür nicht geeignet.

3

Microsoft-Graph-Berechtigungen vergeben

Die App arbeitet als Hintergrunddienst ohne angemeldeten Benutzer. Deshalb müssen beide Rechte unter Application permissions / Anwendungsberechtigungen hinzugefügt werden.

Navigation

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

- Microsoft Graph wählen
- Application permissions wählen
Nicht Delegated permissions / Delegierte Berechtigungen auswählen.
- Mail.Send suchen und markieren
Erlaubt der Anwendung den Versand ohne angemeldeten Benutzer.
- Mail.ReadWrite suchen und markieren
Erlaubt Lesen, Erstellen, Aktualisieren und Löschen von E-Mails. Dieses Recht enthält keinen Versand, daher wird Mail.Send zusätzlich benötigt.
- Add permissions / Berechtigungen hinzufügen bestätigen

Erforderliches Recht	Verwendung im Connector
Microsoft Graph - Mail.Send	Typ: Application. Zweck: Versand als freigegebenes Benutzer- oder Funktionspostfach.
Microsoft Graph - Mail.ReadWrite	Typ: Application. Zweck: POP3/Webclient-Abruf, Gelesen-Markierung, Löschen und Entwurfsverarbeitung großer Nachrichten.

Standardrecht User.Read entfernen

Falls nach der Registrierung noch User.Read - Delegated eingetragen ist, kann es entfernt werden. Der Connector verwendet keine delegierte Benutzeranmeldung und benötigt dieses Recht nicht.

Wirkung ohne Exchange-Einschränkung

Mail.Send und Mail.ReadWrite als Anwendungsberechtigungen gelten nach der Administratorzustimmung grundsätzlich tenantweit. Der Connector selbst verwendet nur konfigurierte Postfächer; für eine serverseitig erzwungene Einschränkung siehe Schritt 6.

4

Administratorzustimmung erteilen

Das bloße Hinzufügen der Rechte genügt nicht. Anwendungsberechtigungen werden erst nach einer tenantweiten Administratorzustimmung wirksam.

Navigation

App-Registrierung > API permissions / API-Berechtigungen

- Grant admin consent for <Tenant> anklicken
Deutsch: Administratorzustimmung für <Tenant> erteilen.
- Sicherheitsdialog kontrollieren
Nur Microsoft Graph Mail.Send und Mail.ReadWrite freigeben. Unerwartete zusätzliche Rechte vor der Bestätigung klären.
- Bestätigen und Ansicht aktualisieren
- Status prüfen
Bei beiden Rechten muss Granted for <Tenant> / Gewährt für <Tenant> mit grünem Status erscheinen.

Wenn die Schaltfläche deaktiviert ist

Das verwendete Konto darf keine tenantweite Zustimmung erteilen. Ein entsprechend berechtigter Microsoft-Entra-Administrator muss diesen Schritt durchführen. Eine Benutzerzustimmung reicht nicht aus.

Sollzustand

Eintrag	Erwarteter Status
Mail.Send	Microsoft Graph Application Granted for <Tenant>
Mail.ReadWrite	Microsoft Graph Application Granted for <Tenant>
Delegierte Rechte	Keine für den Connector erforderlich.

Nach späteren Berechtigungsänderungen

Wenn Rechte ergänzt oder geändert werden, muss die Administratorzustimmung erneut erteilt werden. Erst danach erscheinen die geänderten Anwendungsrechte in neu ausgestellten Zugriffstokens.

5

Client Secret erstellen und sichern

Der aktuelle Connector authentifiziert sich mit einem Client Secret. Der Wert wird auf dem Windows Server per DPAPI für das lokale System verschlüsselt gespeichert.

Navigation

App-Registrierung > Certificates & secrets / Zertifikate & Geheimnisse > Client secrets > New client secret

- Beschreibung eingeben
Empfehlung: SMTP Auth 365 Connector - Windows Server <SERVERNAME>
- Ablaufzeit wählen
Microsoft begrenzt Client Secrets auf maximal 24 Monate und empfiehlt eine Laufzeit unter 12 Monaten. Betriebsverantwortung und Rotation vor Ablauf festlegen.
- Add / Hinzufügen anklicken
- Value / Wert sofort kopieren
Der Secret-Wert wird nach Verlassen der Seite nicht erneut angezeigt.
- Ablaufdatum dokumentieren
Mindestens 30 Tage vor Ablauf einen Termin für die Erneuerung einplanen.

Entscheidend: VALUE, nicht SECRET ID

Der Windows-Techniker benötigt den Inhalt der Spalte Value / Wert. Die Spalte Secret ID ist nur eine Kennung und funktioniert nicht als Kennwort.

Sichere Übermittlung

Den Secret-Wert nicht zusammen mit Tenant-ID und Client-ID in einer normalen E-Mail versenden. Empfohlen sind ein Passwortmanager, ein zeitlich begrenzter Secret-Link oder eine getrennte Übermittlung über einen zweiten Kanal. Nach der lokalen Eingabe keine Klartextkopie auf dem Server ablegen.

Hinweis zur Microsoft-Empfehlung

Microsoft bevorzugt für Produktionssysteme Zertifikate oder föderierte Identitäten. Diese Connector-Version verwendet derzeit ein Client Secret; deshalb sind kurze Laufzeit, geschützte Übergabe und geplante Rotation besonders wichtig.

6

Postfachzugriff sinnvoll begrenzen

Dieser Schritt ist eine Sicherheitsentscheidung des Kunden. Die Entra-Anwendungsberechtigungen allein erlauben grundsätzlich Zugriff auf alle Exchange-Online-Postfächer.

Basisbetrieb

Der Connector begrenzt seine Nutzung auf die in seiner Benutzer- und Absenderverwaltung eingetragenen Adressen. Das ist die schnellste Inbetriebnahme.

Erhöhte Absicherung

Exchange Online erzwingt zusätzlich, dass die App technisch nur auf definierte Postfächer zugreifen darf.

Empfohlene Vorgehensweise

- Für neue Einschränkungen Role Based Access Control for Applications (Application RBAC) in Exchange Online verwenden.
- Die Exchange-Rollen Application Mail.Send und Application Mail.ReadWrite nur dem benötigten Empfängerbereich zuweisen.
- Den Bereich anhand einer gepflegten Postfachgruppe oder eines passenden Exchange-Recipient-Filters definieren.
- Mindestens ein erlaubtes und ein nicht erlaubtes Postfach testen.

Keine neuen Legacy-Policies anlegen

Microsoft kennzeichnet Application Access Policies inzwischen als Legacy und empfiehlt Application RBAC. Bereits vorhandene Policies können den Zugriff weiterhin beeinflussen und sollten bei HTTP 403 mitgeprüft werden.

Für die Einschränkung bereitzustellen

Feld	Einzutragender Wert / Hinweis
Application (client) ID	_____
Erlaubte Postfächer	Als vollständige SMTP-Adressen; Funktions- und Shared-Mailboxes ausdrücklich aufnehmen.
Nicht erlaubtes Testpostfach	Eine Adresse außerhalb des Scopes für den Negativtest.
Exchange-Administrator	Name und Kontakt der ausführenden Person.

Wichtig für große Nachrichten

Da große Nachrichten über Entwurf und Upload-Sitzung verarbeitet werden, benötigt jedes Versandpostfach sowohl Mail.Send als auch Mail.ReadWrite im wirksamen Exchange-Scope.

7

Datenübergabe an den Windows-Techniker

Diese Seite kann ausgefüllt übergeben werden. Der Client-Secret-Wert wird getrennt davon über einen sicheren Übertragungsweg bereitgestellt.

Feld	Einzutragender Wert / Hinweis
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	Mail.Send: ☐ gewährt Mail.ReadWrite: ☐ gewährt
Exchange Application RBAC	☐ nicht gewünscht ☐ eingerichtet ☐ separat beauftragt
Microsoft-365-Ansprechpartner	Name: Kontakt:

Postfächer und gewünschte Funktion

Feld	Einzutragender Wert / Hinweis
Versandpostfächer	
POP3-/Webclient-Postfächer	
Exchange-Abruf	☐ aktiv ☐ nicht benötigt
Nach RETR als gelesen	☐ ja ☐ nein
Automatisch nach Abruf löschen	☐ ja ☐ nein
POP3-DELE an Exchange	☐ erlauben ☐ nicht erlauben
Journalpostfach	☐ aktivieren ☐ zunächst deaktiviert lassen

Nicht in die Übergabeunterlage eintragen

Keine Microsoft-365-Benutzerkennwörter, keine OAuth-Tokens und keinen Client-Secret-Wert im Klartext in diesem PDF speichern. Für den Connector werden keine persönlichen Microsoft-365-Kennwörter benötigt.

Vorbereitung und Einrichtung am Windows Server

Mit den übergebenen Daten kann die Connector-Konfiguration abgeschlossen und geprüft werden.

Servervoraussetzungen

- [] Unterstütztes Windows-System mit .NET Framework 4.8 und lokalen Administratorrechten.
- [] Ausgehendes TCP 443 zu login.microsoftonline.com und graph.microsoft.com; für Graph bereitgestellte Upload-Endpunkte gegebenenfalls auch unter outlook.office.com.
- [] DNS-Auflösung, Systemzeit und TLS-Verbindung funktionieren; Proxy oder SSL-Inspection blockiert die Microsoft-Endpunkte nicht.
- [] Fester Programm- und Datenpfad mit Schreibrechten für das Windows-Dienstkonto.
- [] Lokale SMTP-, POP3- und Webclient-Ports sind festgelegt und in der Firewall nur für berechtigte Quellsysteme geöffnet.

Im Connector einzutragen

Connector-Feld	Wert / Quelle
TenantId	Directory (tenant) ID aus Schritt 2
ClientId	Application (client) ID aus Schritt 2
Client Secret	Value / Wert aus Schritt 5; lokal eingeben und verschlüsselt speichern
GraphBaseUrl	https://graph.microsoft.com/v1.0
OAuthScope	https://graph.microsoft.com/.default
Graph-Anfragen je Postfach	Standard 2; nur nach technischer Begründung ändern
Drosselungswiederholungen	Standard 3; Retry-After von Microsoft wird beachtet

Secret-Speicherung

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

Abnahme, Fehlerprüfung und Quellen

Die Inbetriebnahme gilt erst nach erfolgreichem Versand und - sofern verwendet - erfolgreichem Abruf als abgeschlossen.

Abnahmeprotokoll

- [] OAuth2-Token wurde erfolgreich angefordert; im Protokoll steht kein 401 oder invalid_client.
- [] Testmail wurde aus einem erlaubten Postfach versendet und liegt in Gesendete Elemente.
- [] POP3/Webclient zeigt Nachrichten eines erlaubten Postfachs an, falls diese Funktion aktiviert ist.
- [] Gelesen-Markierung und Löschung wurden entsprechend der Kundenentscheidung geprüft.
- [] Bei eingerichtetem Application RBAC funktioniert ein erlaubtes Postfach und ein nicht erlaubtes wird abgewiesen.
- [] Secret-Ablaufdatum und verantwortliche Person sind dokumentiert.

Schnelle Fehlerzuordnung

Symptom	Prüfung
AADSTS7000215 / invalid_client	Meist falscher Secret-Wert, Secret-ID statt Value oder abgelaufenes Secret.
HTTP 401	Tenant-ID, Client-ID, Secret und Token-Endpunkt prüfen.
HTTP 403	Admin Consent, Berechtigungstyp Application sowie Exchange Application RBAC oder vorhandene Legacy-Policies prüfen.
HTTP 429 / 503 / 504	Microsoft-Drosselung oder temporäre Störung. Der Connector berücksichtigt Retry-After und wiederholt automatisch.
Nur große Mails fehlerhaft	Mail.ReadWrite im wirksamen Scope sowie Zugriff auf Graph-/Outlook-Upload-Endpunkte prüfen.

Offizielle Microsoft-Quellen

App registrieren: learn.microsoft.com/.../quickstart-register-app
 Graph-Anwendungszugriff ohne Benutzer: learn.microsoft.com/.../graph/auth-v2-service
 Client Credentials verwalten: learn.microsoft.com/.../how-to-add-credentials
 Graph-Berechtigungsreferenz: learn.microsoft.com/.../graph/permissions-reference
 Exchange Application RBAC: learn.microsoft.com/.../exchange/permissions-exo/application-rbac

Dokumentationsstand

Gepüft am 11. September 2026. Microsoft kann Portalbezeichnungen, Rollen und Grenzwerte ändern. Bei Abweichungen haben die verlinkten Microsoft-Learn-Seiten und die Richtlinien des Kunden-Tenants Vorrang.