06 – Mailtransport, Melder und Firmenportal-Anmeldung

Kommunikation und Anmeldung einrichten

Versand über den Server

Unter **E-Mail & Versand** den Transport auswählen und eine Testmail an ein kontrolliertes Postfach senden.

Transport	Benötigte Angaben	Abnahme
SMTP	Server, Port, TLS-Verfahren, gegebenenfalls Benutzer/Kennwort, Absender, Antwortadresse	Anmeldung und Versand prüfen; etwa Port 587 mit STARTTLS nach Vorgabe des Mailservers
Microsoft 365 / Graph	Mandanten-ID, App-/Client-ID, Clientschlüssel, Absenderpostfach; App-Anwendungsberechtigung Mail.Send mit Administratorzustimmung	App darf als das vorgesehene Postfach senden; gegebenenfalls Postfachbeschränkungen beachten

Bei pf-Absendern muss der Transport auch für diese Adresse berechtigt sein. Eine Vorlage allein erteilt keine Sendeberechtigung. Im Graph-Transport können gesendete Mails im Absenderpostfach abgelegt werden. Ein Standard-BCC für jede Servermail ist in den Versandeinstellungen möglich. Keine Kennwörter oder Clientschlüssel in Belegsteuerzeichen oder in das Betriebsprotokoll schreiben.

Autoversand und ausdrückliche Versandentscheidung

Für den normalen Autoversand gelten aktivierter Mailtransport, globaler Autoversandschalter, Status Bereit (optional Warnungen) und die eingestellte Wartezeit, standardmäßig 5 Minuten. Die Prüfung erfolgt ungefähr alle 30 Sekunden. Ohne bisherigen Versandversuch, mit Empfänger oder geplantem Partner-Versandweg und ohne Fehler kann ein Vorgang berücksichtigt werden. Normale MAPI-E-Mails werden nie automatisch versendet.

Wichtig sind die neuen Ausnahmen: Die Versandentscheidungen **direkt** und **wennok** aus Steuerzeichen oder Regeln können den global ausgeschalteten Autoversand übersteuern. Wennok verlangt Bereit, direkt berücksichtigt weiterhin Prüfstatus und die global zulässigen Warnungen. Freigabe, Outlook und gotomaxx laufen nicht über den normalen Autoversand. Beim MAPI-

Direktweg kann sofortiges Senden erfolgen. Benutzer mit Outlook-Freigabe sind nur beim Standardweg vom globalen Autoversand ausgenommen; ein ausdrücklicher Direktweg ist gesondert zu prüfen.

Vor Aktivierung oder Regeländerung Normal-, Warnungs- und Fehlerfall mit kontrolliertem Empfänger testen. Im Vorgang den effektiv gewählten Weg beachten.

Benutzer und Sichtbarkeit

Aktive Benutzer mit Anmeldename/E-Mail, ERP-Bedienernummer und gegebenenfalls Druckbenutzernamen pflegen. Je Benutzer **Versenden**, **Admin** und **Outlook** nach Aufgabe freigeben. Sicht kann auf eigene Belege, eigene plus ausgewählte Kollegen oder alle Belege begrenzt werden. Administratoren sehen alles. Nicht zugeordnete Belege sind bei eingeschränkter Sicht nicht automatisch sichtbar.

Belegpost Melder

1. Belegpost-Melder.exe am Arbeitsplatz bereitstellen. Für den Download im Portal muss sie beim Portalpaket vorhanden sein.
2. Mit dem vorgesehenen Benutzer im Portal anmelden und **Melder verbinden** wählen.
3. Den Kopplungslink öffnen oder den Code im Melder eingeben.
4. Gewünschtes Verhalten einstellen: Hinweis, Portal öffnen oder – bei Freigabe – Outlook.
5. Einen Beleg mit der eigenen pb-Bedienernummer drucken und die Zuordnung kontrollieren.

Jeder PC erhält einen eigenen Zugang und kann im Portal getrennt werden. Der Melder läuft im Infobereich und kann mit Windows starten. Die Kopplung enthält auch den Zertifikats-Fingerabdruck. Für die normale Portalanzeige trotzdem ein zum Servernamen passendes, vertrauenswürdiges HTTPS-Zertifikat bereitstellen.

Outlook-Übergabe

Der Administrator aktiviert **Outlook** für den Benutzer. Beim Melder-Weg muss der gekoppelte Melder laufen; für den eingerichteten RDS-Direktweg gelten die Voraussetzungen der MAPI-/Outlook-Seite. Bevorzugt wird das klassische Outlook: Die fertig gestaltete Mail mit Empfängern, Betreff, Text und Anlagen wird als Entwurf geöffnet. Als Rückfall dient eine EML-Datei, deren Öffnen vom installierten Mailprogramm abhängt.

„In Outlook“ bestätigt zunächst die Entwurfsübergabe. Der Anwender prüft und sendet in Outlook. Inzwischen gibt es einen Versandstatusabgleich: Der Windows-Melder sucht beim laufenden klassischen Outlook nach dem zugeordneten Element in Gesendete Elemente und meldet einen gefundenen Versand zurück. Bleibt die Bestätigung aus, erscheint nach der eingestellten Frist ein eigener Status. Der Mac-Abgleich verwendet Betreff/Zeit und ist weniger eindeutig. Kein Abgleich ist eine Zustell- oder Lesebestätigung. Die tatsächlich gewählte Absenderadresse im Entwurf kontrollieren; ein gewünschter Absender setzt ein verfügbares und berechtigtes Konto voraus. Details enthält die neue MAPI-/Outlook-Seite.

Microsoft-Anmeldung

Für direkte Benutzeranmeldung die Entra-App unter **Anmeldung** konfigurieren. Die Umleitungsadresse lautet bei Standardport beispielsweise `https://belegpost.kunde.example:5444/signin-oidc`. Adresse, Hostname und Port müssen zur tatsächlichen Installation passen. Microsoft-Anmeldung innerhalb eines eingebetteten Rahmens ist nicht der vorgesehene Weg; dafür die Firmenportal-Übergabe verwenden.

Anmeldung aus dem Firmenportal übergeben

Diese Übergabe betrifft ausschließlich die Anmeldung und überträgt keinen Beleg.

1. Unter **Anmeldung → Einbindung ins Firmenportal** die Übergabe aktivieren.
2. Die genaue Herkunft des Firmenportals festlegen, zum Beispiel `https://portal.kunde.example:5443`.
3. Gemeinsamen Schlüssel erzeugen und geschützt im Firmenportal hinterlegen. Keinen echten Schlüssel in dieser Dokumentation ablegen.
4. Speichern und das Portal geplant neu starten, damit die Cookie-Einstellungen für Einbettung wirksam werden.
5. Festlegen, ob unbekannte, bestätigte Benutzer automatisch angelegt werden dürfen. Diese erhalten zunächst Sicht auf eigene Belege.

Das Firmenportal erzeugt pro Aufruf ein neues signiertes JWT mit folgenden Parametern:

Parameter	Vorgabe
alg	HS256
iss	Firmenportal
aud	Belegpost

Parameter	Vorgabe
email	E-Mail/UPN des angemeldeten Benutzers; alternativ upn oder preferred_username
name	Anzeigename, optional
jti	Eindeutige ID je Aufruf; nicht wiederverwenden
iat / exp	Unix-Zeit in Sekunden; Lebensdauer höchstens 5 Minuten, empfohlen 2 Minuten
Signatur	HMAC-SHA256 mit dem UTF-8-Text des gemeinsamen Schlüssels

Aufrufmuster, ohne echtes Token:

```
https://belegpost.kunde.example:5444/auth/firmenportal?token=<NEUES-JWT>&ziel=%2F%23%2Fvorgaenge%3Ff%3Dmeine
```

`ziel` ist URL-kodiert und bezeichnet einen lokalen Portalpfad. Beispiele vor Kodierung: `/#/vorgaenge?f=meine`, `/#/vorgaenge?f=offen` oder `/#/vorgang?id=<Vorgangs-ID>`. HTTPS und vertrauenswürdige Zertifikate für beide Portale verwenden. Bei abgelehnter Übergabe Signaturschlüssel, Benutzerzuordnung, Serverzeit, Tokenablauf und neue jti kontrollieren. Kein bereits verbrauchtes Token erneut öffnen.

Anmeldearten: Microsoft, Windows und Active Directory

Unter **Anmeldung → Anmeldeart** wird zwischen Microsoft/Entra, automatischer Windows-Anmeldung und Anmeldung mit Windows-/AD-Benutzername und Kennwort gewählt. Die Windows-Automatik verwendet Kerberos/NTLM und benötigt eine passende Browser-/Domänenkonfiguration. Bei Änderungen der Anmeldeart beziehungsweise der Entra-Konfiguration den erforderlichen Dienstneustart geplant durchführen.

Windows-Konten dem richtigen Portalbenutzer über dessen Druck-Benutzer zuordnen. Bei aktivierter automatischer Benutzeranlage können unbekannte Konten aus AD-/lokalen Kontodaten beziehungsweise der Microsoft-Anmeldung angelegt werden. Danach Sicht, Mandanten, ERP-Bedienernummer und Versandrechte prüfen; die automatische Anlage erteilt keine Administratorrolle.

Administratoren werden über die Windows-Automatik nicht automatisch angemeldet. Über **Administration …** im Benutzermenü zur manuellen Anmeldung wechseln. Auch localhost beziehungsweise eine ausdrücklich manuell geöffnete Anmeldung startet keine stille Windows-Anmeldung.

Bei der AD-Kennwortanmeldung wird das Kennwort gegen Windows/AD geprüft und nicht als Portal-Kennwort gespeichert. Nach jeweils fünf Fehlversuchen greift eine einminütige Sperre. „Nicht freigeschaltet“ betrifft die Portalzuordnung beziehungsweise Aktivierung; „AD nicht erreichbar“ die Kontoprüfung.

Die Option **Firefox am Server automatisch einrichten** trägt die Portaladressen in die Firefox-Authentifizierungsrichtlinie am Server ein. Bestehende andere Richtlinien bleiben erhalten. Firefox anschließend neu starten und unter `about:policies` prüfen. Die Einrichtung betrifft nicht automatisch alle entfernten Arbeitsplatzbrowser.

Microsoft 365 für Outlook im Web einrichten (24.11.2026)

Unter **MAPI-Mails → Mailprogramm für „In Outlook senden“** eine globale Vorgabe wählen; in der Benutzerverwaltung kann sie unter „MAPI-Mails und Melder“ überschrieben werden. Vorrang: Benutzer → globale Vorgabe → Outlook. Diese Auswahl ist von der MAPI-Entscheidung Outlook/Portal/Direkt und vom Öffnungsort Melder/RDS-Sitzung getrennt.

Für **Outlook im Web (Microsoft 365)** müssen Mandanten-ID, Client-ID und geschützter Clientschlüssel unter E-Mail eingerichtet sein. Die App benötigt zusätzlich **Mail.ReadWrite als Anwendungsberechtigung mit Administratorzustimmung** für die betroffenen Postfächer. Mail.Send allein deckt das Anlegen und Prüfen dieser Entwürfe nicht ab. Eventuelle Postfachbeschränkungen müssen die Benutzerpostfächer einschließen.

Beim Benutzer die E-Mail-Adresse seines tatsächlichen Microsoft-365-Postfachs hinterlegen. In diesem Postfach wird der Entwurf mit Text, Gestaltung und Anlagen angelegt. Standardabsender ist das Benutzerpostfach; eine explizite abweichende Absenderadresse benötigt die entsprechenden Microsoft-365-Rechte. Der allgemeine BCC für Serverversand wird diesem Web-Entwurf nicht zusätzlich angefügt; vorgangsbezogenes BCC bleibt bestehen.

Abnahme: kontrollierten Beleg öffnen, Aktion „Freigeben & in Outlook im Web senden“ wählen, richtigen Browser-/Postfachbenutzer, Absender, Empfänger, Text und Anlagen prüfen und erst dann selbst senden. Die Aktion im Portal benötigt keinen Melder. Nicht wiederholt auslösen, wenn nur der Browser-Tab fehlt: zunächst im Entwurfsordner nachsehen, ob der Entwurf bereits angelegt wurde.

Belegpost sucht ungefähr alle zwei Minuten serverseitig nach der zugeordneten Nachricht in Gesendete Elemente. Bestätigter Versand führt zu 110 beziehungsweise bei erneutem Versand zu 120. Ohne auffindbare Nachricht ist die Übergabe kein Versandnachweis. Meldungen „Postfach nicht gefunden“ durch Benutzeradresse/Exchange-Postfach prüfen; „Zugriff verweigert“ durch App-Rechte, Administratorzustimmung und Postfachfreigabe.

Created 2026-11-14 08:52:08 CET by Access MCP API
Updated 2026-11-24 10:47:07 CET by Access MCP API