

Technische und betriebliche Dokumentation der Windows-Anwendung ERPPrintPilot mit Schwerpunkt auf Dateisynchronisation, Azure-Konfiguration, Sicherheit und Fehleranalyse.

Wichtigste Aussage zur Microsoft Konfiguration

Die vorliegende ERPPrintPilot-Version authentifiziert sich mit dem Zugriffsschlüssel des Azure Storage Accounts. Für diesen Betriebsmodus werden keine Microsoft Entra App Registration, keine Microsoft-Graph-Berechtigungen und kein Azure Key Vault benötigt.

Für die Inbetriebnahme sind erforderlich:

- Azure-Abonnement
- Azure Storage Account
- privater Blob-Container
- Name und Zugriffsschlüssel des Storage Accounts
- Netzwerkzugriff vom Windows-Rechner zum Blob-Endpunkt
- lokale Arbeits- und Archivordner
- gotomaxx PDF-Mailer mit gültigem Druckprofil

Für den sicheren Dauerbetrieb wird eine spätere Umstellung auf Microsoft Entra ID und Azure RBAC empfohlen. Diese Umstellung erfordert eine dafür freigegebene ERPPrintPilot-Version und kann nicht allein über das Azure-Portal aktiviert werden.

Systemübersicht

Bereich	Ausführung
Anwendung	Windows-Desktop-Anwendung
Laufzeit	.NET Framework 4.8
Cloudspeicher	Microsoft Azure Blob Storage
Druckkomponente	gotomaxx PDF-Mailer 6
Lokale Daten	Arbeitsordner, Archive und gotomaxx-Protokolldatenbank
Verzeichnisdienst	optionales lokales Active Directory für E-Mail-Adressen

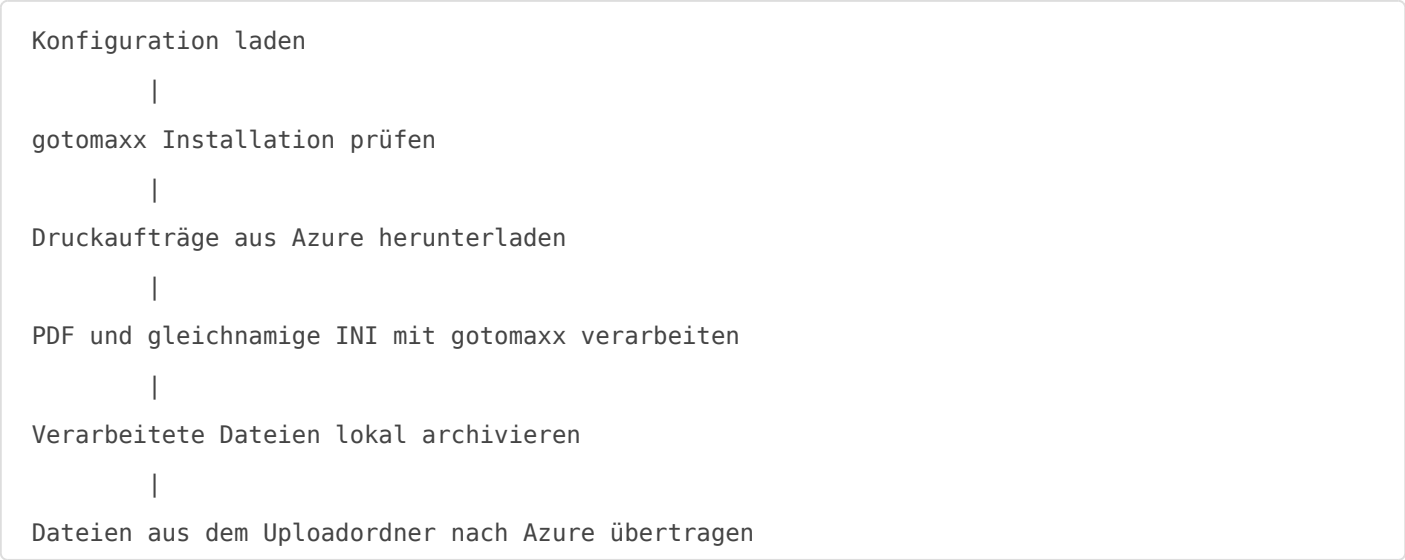
ERPPrintPilot muss unter einem festgelegten Windows-Konto betrieben werden. Lokal geschützte Zugangsdaten und Zugriffstoken sind an den Rechner beziehungsweise das Benutzerkonto

gebunden.

Zuständigkeiten

Rolle	Aufgabe
Azure-Administrator	Storage Account, Container, Netzwerkzugriff und Zugriffsschlüssel bereitstellen
Windows-Administrator	Laufzeit, Dienstkonto, Ordnerrechte und geplanten Task einrichten
gotomaxx-Techniker	PDF-Mailer, Druckprofil, Steuerdateien und Archivpfad konfigurieren
Applikationsbetreuer	ERPPrintPilot konfigurieren, testen und überwachen

Gesamtablauf



Die Synchronisation wird nur ausgeführt, wenn das konfigurierte gotomaxx-Verzeichnis vorhanden ist. Fehlt die gotomaxx-Installation oder ist der Pfad falsch, werden weder Download noch Upload gestartet.

Startparameter

Parameter	Wirkung
/H	vollständigen Workflow unbeaufsichtigt ausführen und danach beenden
/P	Archive bereinigen und danach beenden

Parameter	Wirkung
/S	Sendeprotokoll erzeugen und danach beenden
/BWPROT	zusätzliche BWProt-Analyse aktivieren
/VON=	Beginn des Berichtszeitraums
/BIS=	Ende des Berichtszeitraums

Synchronisation

Download und Upload verwenden denselben Blob-Container. Die Trennung erfolgt über unterschiedliche Prefixe, die in Azure wie virtuelle Ordner erscheinen.

Richtung	Quelle	Ziel	Standardprefix
Download	Azure Blob Storage	lokaler Arbeitsordner	print/
Upload	lokaler Uploadordner	Azure Blob Storage	scan/

Authentifizierung

ERPPrintPilot erzeugt aus dem Storage-Account-Key eine kurzlebige Zugriffsfreigabe für den Container. Diese umfasst Lesen, Auflisten, Schreiben, Erstellen und Löschen. Der Zugriffstoken wird lokal geschützt gespeichert und bei Ablauf erneuert. Die reguläre Laufzeit beträgt in der vorliegenden Version ungefähr eine Stunde.

Der Storage-Account-Key besitzt weitreichende Berechtigungen und ist wie ein privilegiertes Kennwort zu behandeln. Er darf nicht in BookStack, Tickets, E-Mails oder allgemein lesbaren Dateien dokumentiert werden.

Download

- Der allgemeine Azure-Datenabgleich muss aktiviert sein.
- ERPPrintPilot liest Blobs unterhalb des konfigurierten Download-Prefixes.
- Es werden nur Dateien mit den Endungen `.pdf` und `.ini` heruntergeladen.
- Unterordner des Blob-Pfads werden im lokalen Arbeitsordner beibehalten.
- Die spätere PDF-Suche erfolgt rekursiv.
- Zu jeder PDF wird im gleichen Ordner eine gleichnamige INI-Datei erwartet.
- Authentifizierungsfehler führen zu einer Erneuerung des Zugriffstokens.
- Zeitüberschreitungen, Drosselungen und vorübergehende Azure-Fehler werden kurzzeitig wiederholt.

Wenn `Delete remote files after download` aktiv ist, löscht ERPPrintPilot den Azure-Blob unmittelbar nach dem erfolgreichen Download. Der Druck ist zu diesem Zeitpunkt noch nicht abgeschlossen. Remote-Löschen sollte daher erst nach einem getesteten Wiederanlaufverfahren aktiviert werden.

Druckverarbeitung

1. ERPPrintPilot sucht im lokalen Arbeitsordner nach PDF-Dateien.
2. Zu `auftrag.pdf` muss im selben Ordner `auftrag.ini` vorhanden sein.
3. ERPPrintPilot ergänzt bei Bedarf die Auftragssteuerung.
4. PDF und Steuerdatei werden an gotomaxx übergeben.
5. Der Verarbeitungserfolg wird über das gotomaxx-Archiv und die Protokolldaten geprüft.
6. Erfolgreich verarbeitete Dateien werden entfernt oder archiviert.

Upload

- Der allgemeine Azure-Datenabgleich und der separate Upload müssen aktiviert sein.
- Der lokale Uploadordner muss vorhanden sein.
- Alle Dateien und Unterordner werden rekursiv verarbeitet; es besteht kein Dateitypfilter.
- Unterordner werden im Zielprefix beibehalten.
- Bereits vorhandene Blobs werden überschrieben.
- Bei konfiguriertem Archiv werden erfolgreich hochgeladene Dateien dorthin verschoben.

Der lokale Uploadpfad muss nach dem Speichern und nach einem Neustart ausdrücklich kontrolliert werden. Bleibt der Wert nicht erhalten, darf der Upload nicht produktiv freigegeben werden. Gleichnamige Dateien aus unterschiedlichen Unterordnern können außerdem im flach geführten Uploadarchiv kollidieren.

Microsoft Azure für den aktuellen Betrieb einrichten

Erforderliche Ressourcen

Ressource	Erforderlich	Zweck
Azure-Abonnement	Ja	Bereitstellung und Abrechnung
Ressourcengruppe	empfohlen	gemeinsame Verwaltung
Azure Storage Account	Ja	Speicherung der Dateien
privater Blob-Container	Ja	Container für <code>print/</code> und <code>scan/</code>

Ressource	Erforderlich	Zweck
Storage-Account-Key	Ja	Authentifizierung der aktuellen Programmversion
Entra App Registration	Nein	im aktuellen Betriebsmodus nicht verwendet
Azure Key Vault	Nein	im aktuellen Betriebsmodus nicht verwendet
Microsoft Graph	Nein	wird nicht benötigt

Storage Account und Container

1. Im Azure-Portal einen Storage Account vom Typ General Purpose v2 anlegen.
2. Sichere Übertragung über HTTPS aktiv lassen und mindestens TLS 1.2 verwenden.
3. Eine zur erwarteten Last passende Standardredundanz wählen.
4. Unter **Data storage > Containers** einen Container anlegen.
5. Den anonymen Zugriff deaktiviert lassen.
6. Für `print/` und `scan/` müssen keine echten Ordner angelegt werden. Sie entstehen mit den Blob-Namen.

Shared Key und Zugriffsschlüssel

Unter **Security and networking > Access keys** wird der Wert von Key1 oder Key2 benötigt. In ERPPrintPilot wird nur der Schlüsselwert hinterlegt, nicht die vollständige Connection String.

Für die vorliegende Programmversion muss **Allow storage account key access** beziehungsweise **AllowSharedKeyAccess** aktiviert bleiben. Wird Shared Key deaktiviert, funktioniert die Synchronisation nicht mehr.

Netzwerkzugriff

Der Windows-Rechner benötigt ausgehend TCP 443 zu:

```
https://<storage-account>.blob.core.windows.net
```

Netzwerkvariante	Verwendung	Konfiguration
Zugriff aus allen Netzen	nur für einen kurzen Funktionstest	öffentlichen Zugriff vorübergehend erlauben
ausgewählte Netzwerke	typischer On-Premises-Betrieb	öffentliche Ausgangs-IP des Standorts freigeben
Private Endpoint	abgeschottete Netze	Private DNS sowie Routing über VPN oder ExpressRoute bereitstellen

Ein gültiger Account Key oder Zugriffstoken umgeht die Storage-Firewall nicht. Ist das Quellnetz nicht erlaubt, antwortet Azure weiterhin mit 403.

ERPPrintPilot konfigurieren

Azure Storage

Einstellung	Empfehlung für Ersttest	Bedeutung
Datenabgleich aktiv	True	Azure-Dateitransfer einschalten
Storage Account	kundenspezifischer Name	Name ohne DNS-Suffix
Account Key	geheimer Schlüsselwert	Zugriffsschlüssel des Storage Accounts
Container Name	kundenspezifischer Name	privater Blob-Container
Local path	C:\ProgramData\ERPPrintPilot\Data	Ziel des Downloads und Quelle der Druckverarbeitung
Remote path	print/	Prefix der Druckaufträge
Delete remote files after download	False	Azure-Datei nach Download löschen
Token expires in X minutes	Standard belassen	angezeigter Wert entspricht nicht zwingend der tatsächlichen Laufzeit

Die Felder `Tenant ID`, `Client ID`, `Client Secret` und `Vault Name` bleiben im aktuellen Betriebsmodus leer.

Azure Storage Upload

Einstellung	Empfehlung für Ersttest	Bedeutung
Datenabgleich aktiv	False	Upload erst nach erfolgreichem Downloadtest aktivieren
Local path	C:\ProgramData\ERPPrintPilot\Data.Upload	Quelle aller Uploaddateien
Remote path	scan/	Zielprefix im Container
Path to Archive-Folder	C:\ProgramData\ERPPrintPilot\Upload.Archiv	Archiv für hochgeladene Dateien

Inbetriebnahme und Abnahme

Vorbereitung

- ☐ dediziertes Windows-Konto festlegen
- ☐ .NET Framework 4.8 prüfen
- ☐ gotomaxx PDF-Mailer installieren und Druckprofil einrichten
- ☐ freigegebenes ERPPrintPilot-Paket installieren
- ☐ lokale Arbeits-, Upload- und Archivordner anlegen
- ☐ NTFS-Berechtigungen auf Dienstkonto und Administratoren begrenzen
- ☐ Azure Storage Account und privaten Container anlegen
- ☐ Netzwerkerreichbarkeit des Blob-Endpunkts prüfen
- ☐ ERPPrintPilot-Einstellungen eintragen
- ☐ geplanten Task unter dem vorgesehenen Windows-Konto anlegen

Download und Druck testen

1. Unter `print/test/` die Dateien `abnahme-001.pdf` und `abnahme-001.ini` mit ungefährlichen Testdaten bereitstellen.
2. Remote-Löschen deaktiviert lassen.
3. ERPPrintPilot interaktiv starten und den Workflow auslösen.
4. Prüfen, ob beide Dateien im lokalen Arbeitsordner vorhanden sind.
5. Verarbeitung und Zielausgabe in gotomaxx kontrollieren.
6. Das gotomaxx-Archiv und die Protokolldaten prüfen.
7. Bestätigen, dass die Azure-Testdateien noch vorhanden sind.

Upload testen

1. Prüfen, ob der Uploadpfad nach Speichern und Neustart unverändert geladen wird.
2. Eine eindeutig benannte Testdatei in den lokalen Uploadordner legen.
3. Upload aktivieren und den Workflow erneut starten.
4. Prüfen, ob die Datei unter `scan/` mit dem erwarteten relativen Pfad vorhanden ist.
5. Bei aktiviertem Archiv prüfen, ob die lokale Datei verschoben wurde.

Freigabekriterien

- Download, Druck und Upload wurden mit Testdaten erfolgreich durchgeführt.
- Fehler sind im ERPPrintPilot-Protokoll oder im zentralen Syslog auffindbar.
- Zugangswerte stehen nicht im Anwendungspaket oder in frei lesbaren Dateien.
- Ein Wiederanlauf nach Programmabbruch wurde getestet.
- Das Betriebskonto kann geschützte Werte nach einem Neustart weiterhin lesen.

- Remote-Löschen wird erst nach Freigabe des Wiederanlaufverfahrens aktiviert.

Fehleranalyse

Symptom	Wahrscheinliche Ursache	Maßnahme
Synchronisation startet nicht	gotomaxx-Pfad fehlt oder ist falsch	gotomaxx-Installationspfad prüfen
403 <code>AuthenticationFailed</code>	falscher Account Key oder ungültiger Zugriffstoken	Account Key prüfen und Einstellungen erneut speichern
403 <code>AuthorizationPermissionMismatch</code>	Zugriffsrechte passen nicht	Authentifizierungsmodus und Containerzugriff prüfen
403 ohne passenden Authentifizierungscode	Storage-Firewall blockiert den Client	öffentliche IP, VNet-Regel, Private Endpoint und DNS prüfen
404	Account, Container oder Datei nicht gefunden	Namen und Prefixe exakt prüfen
408 oder 5xx	temporäre Netz- oder Azure-Störung	Wiederholungen abwarten, danach Netzwerk und Azure-Status prüfen
429	Azure drosselt Anfragen	Ausführungsfrequenz und parallele Instanzen reduzieren
keine Blobs gefunden	falsches oder leeres Prefix	<code>Remote path</code> sowie Groß- und Kleinschreibung prüfen
PDF bleibt liegen	gleichnamige INI fehlt	Dateipaar und Ablageordner prüfen
Uploadpfad fehlt	Pfad wurde nicht übernommen oder Ordner fehlt	Einstellung nach Neustart prüfen und Ordner anlegen
Anwendung bleibt hängen	gotomaxx-Prozess wurde nicht beendet	gotomaxx prüfen und Prozess kontrolliert beenden

Überwachung

Im Regelbetrieb sollten mindestens folgende Werte überwacht werden:

- erfolgreiche und fehlgeschlagene Downloads und Uploads
- Anzahl unbearbeiteter PDF-Dateien im lokalen Arbeitsordner
- Alter der ältesten Datei in `print/`, im Arbeitsordner und in `scan/`
- Fehler 403, 404, 429 und 5xx
- Laufzeit und Abbrüche des gotomaxx-Prozesses
- freier Speicherplatz in Arbeits- und Archivordnern
- Ablaufdaten von Entra-Anmeldeinformationen nach einer späteren Migration

Sicherheit und Wiederanlauf

Sicherheitsmaßnahmen

- ☐ alle mit Installations- oder Testpaketen gelieferten Kennwörter und Schlüssel vor Produktion ersetzen
- ☐ Zugangswerte nur in den vorgesehenen geschützten Feldern speichern
- ☐ Storage-Account-Keys regelmäßig rotieren
- ☐ das Windows-Betriebskonto nicht für normale Benutzerarbeit verwenden
- ☐ anonymen Containerzugriff deaktiviert lassen
- ☐ Storage-Firewall auf benötigte Standorte oder private Verbindungen begrenzen
- ☐ Arbeits- und Archivordner sichern
- ☐ Azure Blob Soft Delete und Versionierung prüfen
- ☐ zentrale Diagnoseprotokolle und Alarmierung aktivieren

Wiederanlauf nach Abbruch

1. ERPPrintPilot und gotomaxx nicht erneut starten, bevor der Status geprüft wurde.
2. In Azure prüfen, ob der Auftrag noch unter `print/` vorhanden ist.
3. Im lokalen Arbeitsordner nach PDF und gleichnamiger INI suchen.
4. Im gotomaxx-Archiv und in den Protokollen prüfen, ob der Auftrag bereits verarbeitet wurde.
5. Unter `scan/` prüfen, ob Ergebnisdateien bereits hochgeladen wurden.
6. Erst danach entscheiden, ob der Auftrag erneut ausgeführt, nur hochgeladen oder manuell abgeschlossen wird.

Parallele ERPPrintPilot-Instanzen sollten vermieden werden. Arbeits- und Archivordner dürfen während eines laufenden Workflows nicht manuell bereinigt werden.

Empfohlene Zielarchitektur mit Microsoft Entra ID

Für den Dauerbetrieb sollte der Storage-Account-Key von der Windows-Station entfernt werden. Microsoft empfiehlt die Autorisierung von Blobzugriffen über Microsoft Entra ID und Azure RBAC. Falls weiterhin ein SAS benötigt wird, sollte ein User Delegation SAS verwendet werden.

Erforderliche Microsoft Konfiguration

1. Unter **Microsoft Entra ID > App registrations** eine Single-Tenant-App für ERPPrintPilot registrieren.
2. `Application (client) ID` und `Directory (tenant) ID` dokumentieren.
3. Eine vom Hersteller unterstützte Anmeldeinformation konfigurieren. Für Produktion ist ein Zertifikat gegenüber einem Client Secret zu bevorzugen.
4. Dem Service Principal unter **Storage Account > Access control IAM** die Rolle `Storage Blob Data Contributor` auf Storage-Account-Ebene zuweisen.
5. Die neue ERPPrintPilot-Version mit Entra-ID-Zugriff testen.
6. Erst nach erfolgreichem Test Shared Key am Storage Account deaktivieren.

Microsoft-Graph-API-Berechtigungen werden dafür nicht benötigt. Die Storage-Berechtigung wird über Azure RBAC und nicht über die API Permissions der App Registration vergeben.

Azure Key Vault ist nur erforderlich, wenn die eingesetzte ERPPrintPilot-Version Werte nachweislich daraus liest. In diesem Fall benötigt der Service Principal die Rolle `Key Vault Secrets User` und Netzwerkzugriff zum Vault. Ein Key Vault beseitigt nicht automatisch die Notwendigkeit einer sicheren Erstanmeldung.

Begriffe

Begriff	Bedeutung
Blob	Dateiobjekt in Azure Blob Storage
Container	Sammlung von Blobs in einem Storage Account
Prefix	Anfang eines Blob-Namens, der wie ein virtueller Ordner wirkt
Account Key	weitreichender Zugriffsschlüssel eines Storage Accounts
SAS	zeitlich und funktional begrenzte Zugriffsfreigabe
User Delegation SAS	über Microsoft Entra ID autorisierter SAS
Service Principal	technische Identität einer Entra App Registration
Azure RBAC	rollenbasierte Zugriffssteuerung für Azure-Ressourcen und Daten
Private Endpoint	private Netzwerkverbindung zu einem Azure-Dienst

Referenzen

- [Azure Storage SAS Überblick](#)
- [Blobzugriff mit Microsoft Entra ID](#)
- [Azure-Rolle für Blobdaten zuweisen](#)
- [Integrierte Azure Storage Rollen](#)

- [Shared-Key-Autorisierung verhindern](#)
 - [Azure Storage Firewall und Netzwerkzugriff](#)
 - [App in Microsoft Entra ID registrieren](#)
 - [App-Anmeldeinformationen verwalten](#)
 - [Azure RBAC für Key Vault](#)
 - [Key Vault Netzwerkzugriff](#)
-

Revision #2

Created 2026-09-11 08:28:41 CEST by Martin Dauwa

Updated 2026-09-11 08:58:23 CEST by Martin Dauwa