



TEIL II · EINRICHTUNG

Ordivis Service einrichten

Kennwort, Postfächer, Apps und die Reihenfolge, in der es sicher ist

Produktversion 2026.09.07 · Handbuch-Revision 1.0

Stand 07.09.2026 · Plattform .NET 10 / Windows Server

OS-10 Einrichten

Ordavis Service einrichten

Dieses Kapitel führt durch die Erstinbetriebnahme. Es setzt voraus, dass der Dienst installiert ist und läuft; der Aufbau der Anlage steht in *Der Ordavis Stack* (OS-01).

⚠ **Die Reihenfolge in Abschnitt 4 ist keine Empfehlung.** Wer ein Postfach hier einschaltet, bevor er es in der Fachanwendung abschaltet, holt es doppelt ab – und verliert Post.

INHALT

1 Kennwort der Verwaltung

2 Postfächer

2.1 Anmeldung mit OAuth2 (Microsoft 365, Google)

2.2 Bestehende Postfächer aus Ordavis IT übernehmen

3 Apps anbinden

3.1 Nachsehen, ob die Anmeldung wirklich funktioniert

3.2 Ansprüche

4 Die Umschaltung – in dieser Reihenfolge

5 Standardziel und Simulationsbetrieb

1 Kennwort der Verwaltung

```
setx /M Service__AdminPassword "<Kennwort>"
```

Danach **den Dienst neu starten** – eine Umgebungsvariable liest ein laufender Prozess nicht nach.

⚠ **Ohne gesetztes Kennwort ist die Verwaltung nur vom Server selbst erreichbar.** Das ist die sichere Vorgabe, keine Einschränkung: Eine Verwaltung ohne Kennwort im Netz gehört jedem, der sie findet – und über sie lassen sich Postfächer und Zustellziele ändern.

Über unverschlüsseltes HTTP ist sie ebenfalls nur örtlich erreichbar. Aus dem Netz besteht der Dienst auf HTTPS, weil das Kennwort als Kopfzeile über die Leitung geht.

★ **Das Zertifikat legt der Dienst selbst an** – je Installation eines, fünf Jahre gültig, im Speicher `LocalMachine\My`. Es ist nichts zu beantragen und nichts einzutragen. Er hört auf dem Port über dem HTTP-Port: **5310 → 5311**.

2 Postfächer

`Verwaltung` → `Postfächer` → `Neu`. Gebraucht werden Server, Port, Sicherheit, Anmeldeverfahren und die Absenderadresse.

★ **Vor dem Speichern den Verbindungstest benutzen.** Er baut die Verbindung wirklich auf, meldet sich an und öffnet den Ordner **nur lesend** – und schreibt jeden Schritt mit. Ein Postfach, das erst beim ersten Abruf scheitert, scheitert stumm.

2.1 Anmeldung mit OAuth2 (Microsoft 365, Google)

Für Postfächer ohne Kennwortanmeldung führt die Verwaltung durch den **Gerätecode**: Der Dienst zeigt einen Code, der Administrator bestätigt ihn im Browser des Anbieters. Ein Kennwort wird dabei nie eingegeben und nie gespeichert.

⚠ Die Zustimmung läuft ab. Der Dienst erneuert das Token selbsttätig, solange er läuft; nach einer längeren Abschaltung kann eine erneute Bestätigung nötig sein.

2.2 Bestehende Postfächer aus Ordvis IT übernehmen

Postfächer → Aus Ordvis IT übernehmen liest die dort eingerichteten Konten über die Schnittstelle und legt sie hier an. Der Import zeigt zuerst eine **Vorschau**.

⚠ **Übernommene Postfächer sind zunächst abgeschaltet, und das ist Absicht.** Wären sie sofort aktiv, holten zwei Systeme dasselbe Postfach ab – ein Wettlauf, bei dem der Zweite die Mail nie sieht. Erst in Ordvis IT abschalten, dann hier einschalten (Abschnitt 4).

⚠ **Kennwörter werden nicht mit übernommen.** Sie liegen in Ordvis IT verschlüsselt und lassen sich dort nicht auslesen. Sie müssen hier einmal eingetragen werden.

3 Apps anbinden

Eine Fachanwendung meldet sich **selbst** an; sie wird nicht von Hand eingetragen. Was der Administrator tut: das **Bootstrap-Token** setzen, das die *erste* Anmeldung erlaubt.

Verwaltung → Einstellungen → Bootstrap-Token. Speichern genügt – **kein Neustart**, die Erstanmeldung liest den Wert bei jedem Versuch neu.

★ **Ein Token für alle Erstanmeldungen, nicht eines je Anwendung.** Es beglaubigt die erste Anmeldung einer App, die der Dienst noch *nicht* kennt. Für eine bereits registrierte App wird es **nicht** mehr angenommen – sie muss ihr eigenes Token vorlegen. Wer eine zweite Anwendung anbindet, braucht deshalb kein neues Token, sondern dasselbe.

⚠ **Ein leeres Feld heißt „hier nicht gesetzt“, nicht „abgeschaltet“.** Dann gilt weiter, was in **appsettings.json** unter **Service:BootstrapToken** steht. Beides leer heißt: Es gibt keine Erstanmeldung – eine offene Registrierung wäre ein Weg, sich eine App-Identität zu verschaffen und damit fremde Zustellungen abzugreifen.

⚠ **In der Schlüsselliste unter dem Formular steht der Wert nicht.** Dort erscheint nur, *dass* er gesetzt ist und wie lang er ist. Zum Kopieren steht er im Feld darüber.

– Die Token werden **GENAU EINMAL** ausgegeben – und zwar an die Anwendung, nicht an Sie. Nach der ersten Anmeldung gibt Ordvis Service der Anwendung zwei eigene Token. Sie gehören in deren Konfiguration, und das Bootstrap-Token wird **aus der Konfiguration der Anwendung** entfernt: Es wäre sonst ein zweiter Weg zu dieser App-Identität. Im Dienst bleibt es stehen – dort wird es für die nächste Anwendung gebraucht.

Schreibt die Anwendung ihr Protokoll auf die Konsole und läuft als Windows-Dienst, ist diese Meldung im Moment ihrer Entstehung verloren. **Prüfen Sie deshalb nach der ersten Anmeldung Abschnitt 3.1.**

3.1 Nachsehen, ob die Anmeldung wirklich funktioniert

Verwaltung → Apps , Spalte **Zustand**.

Anzeige	Bedeutung
ok	Letzte Gesundheitsprüfung erfolgreich
Anmeldung scheitert	⚠ Jemand meldet sich unter dieser Kennung mit einem ungültigen Token an – fast immer ein verbrauchtes Bootstrap-Token
Fehler	Die Gesundheitsprüfung erreicht die Anwendung nicht

⚠ »Anmeldung scheitert« wiegt schwerer als »ok«, und die Reihenfolge in der Anzeige ist **Absicht**. Die Gesundheitsprüfung ist ein Anruf *des Dienstes* bei der Anwendung – sie sagt nichts darüber, ob die Anwendung zurückkommt. Sie stand schon einmal stundenlang auf grün, während dieselbe Anwendung sich bei jedem Start vergeblich anmeldete und deshalb nichts melden, keine Ansprüche eintragen und nichts einliefern konnte.

Sind die Token verloren: Apps → Token **erneuern** . Beide werden angezeigt, jedes nur einmal.

⚠ Die Erneuerung tauscht **BEIDE** Token – auch das, an dem die funktionierende Zustellung hängt. Wer nur eines einträgt, bricht die Richtung, die vorher lief.

3.2 Ansprüche

Eine Anwendung meldet bei der Anmeldung, wofür sie zuständig ist: Postfächer, Objekttypen, Betreffpräfixe, Kategorien. Daraus entstehen die Routing-Regeln der Schicht L2.

Anspruch	Wirkung
Postfächer	Meldung aus diesem Postfach → diese Anwendung
Objekttypen	Ein Objekttyp gehört genau einer Anwendung
Betreffpräfixe	⚠ erzeugt Betreff enthält ...
Kategorien	Kategorie → Anwendung

⚠ **Betreffpräfixe sind gefährlicher, als sie aussehen.** Der Anspruch prüft, ob der Betreff die Zeichenkette **enthält** – nicht, ob er damit beginnt. Ein Präfix wie **IT** trifft damit »Mitteilung«, »Bitte um Rückruf« und »Sicherheit«. Im Zweifel leer lassen.

4 Die Umschaltung – in dieser Reihenfolge

Solange die Fachanwendung ihre Post noch selbst abholt, darf Ordvis Service dasselbe Postfach nicht abholen.

1. **In der Fachanwendung** das Empfangs-Postfach deaktivieren. ⚠ Die **SMTP**-Konten bleiben aktiv, wenn die Anwendung ihre Post weiterhin selbst versendet.
2. **Prüfen**, dass dort seither nichts mehr abgeholt wird.
3. **In Ordvis Service** das Postfach einschalten.
4. Eine Testmail schicken und in **Verwaltung → Eingang** nachsehen, dass sie ankommt.
5. In der Fachanwendung nachsehen, dass daraus ein Vorgang wurde.

⚠ **Nie umgekehrt.** Beide gleichzeitig aktiv heißt: Wer zuerst kommt, nimmt die Mail. Der andere sieht sie nie, und es sieht nach einem Fehler in der Anwendung aus.

5 Standardziel und Simulationsbetrieb

Standardziel (`Service:DefaultTargetApp`) ist die Anwendung, an die eine Meldung geht, für die keine Regel greift. Ohne Standardziel bleibt sie liegen.

Simulationsbetrieb (`Service:SimulationOnly`) lässt den Dienst alles tun außer zustellen – er holt ab, routet, protokolliert, stellt aber nichts zu.

★ **Das ist der richtige Zustand für die ersten Tage.** In **Verwaltung → Eingang** lässt sich dann nachsehen, welche Meldung wohin gegangen *wäre*, ohne dass ein Vorgang entsteht.

⚠ **Und der richtige Moment, ihn abzuschalten, ist eine bewusste Entscheidung.** Danach wird jede eingehende Mail zu einem Vorgang.