



FÜR DEN SYSTEMADMINISTRATOR

Ordivis Bauhof Administratorhandbuch

**Installation, Betrieb, Zugänge, Aktualisierung und Schnittstelle des Fachverfahrens
für den kommunalen Bauhof**

Produktfassung 2026.09.04.1843 · Handbuchfassung 1.0

Stand 04.09.2026 · Hersteller Grams IT

Plattform .NET 10 · Windows Server 2022/2025 · PostgreSQL

Band A · OB-02 · OB-40 ... OB-60

Ordvis Bauhof — Administratorhandbuch

ALPHA-FASSUNG — BITTE ZUERST LESEN

Ordvis Bauhof befindet sich im **Alphastand**. Das Produkt ist nicht freigegeben, nicht abgenommen und in keiner Kommune im Wirkbetrieb.

Inhalte, Bildschirme, Bezeichnungen, Schnittstellen und Abläufe können sich jederzeit und ohne Ankündigung ändern — auch so, dass in diesem Handbuch beschriebene Wege danach anders verlaufen oder ganz entfallen.

Dieses Handbuch ist deshalb **keine Leistungsbeschreibung und keine Zusage**. Es beschreibt den Stand am Tag des Satzes; verbindlich ist allein, was vertraglich vereinbart wird.

Jedes Dokument trägt im Kopf einen **Stand** — *gebaut, teilweise* oder *geplant*. Er sagt Ihnen, wie viel von dem, was Sie lesen, es heute wirklich gibt.

Die Dokumente dieses Bandes

Code	Dokument	Zielgruppe	Stand
OB-00 Übersicht	Ordvis Bauhof — Handbuch-Übersicht	Gesamtdokumentation	Beschreibt Vorhandenes
OB-01 Einführung	Einführung und Grundlagen	Grundlagen	Beschreibt Vorhandenes
OB-02 Architektur	Systemvoraussetzungen und Architektur	Für den Systemadministrator	Beschreibt Vorhandenes
OB-40 Administration	Administrationshandbuch	Für den Systemadministrator	Beschreibt Vorhandenes
OB-41 Zugang	Benutzer, Rollen und Zugang	Für den Systemadministrator	Beschreibt Vorhandenes
OB-42 Geräte	Ausgabestationen und Fahrzeuggeräte	Für den Systemadministrator	Beschreibt Vorhandenes
OB-44 Rechtematrix	Rollen- und Rechtematrix	Für Administration und Revision	Beschreibt Vorhandenes
OB-50 Installation	Installation und Server	Für den Systemadministrator	Beschreibt Vorhandenes
OB-51 Aktualisierung	Aktualisierung, Sicherung, Wiederanlauf	Für den Systemadministrator	Teilweise gebaut
OB-52 Konfiguration	Konfigurationsreferenz	Für den Systemadministrator	Beschreibt Vorhandenes

Code	Dokument	Zielgruppe	Stand
OB-54 Betrieb	Wachen, Betriebsprotokoll und Störungsbilder	Für den Systemadministrator	Beschreibt Vorhandenes
OB-60 Schnittstelle	Schnittstellen-Referenz	Für Entwicklung und Integration	Beschreibt Vorhandenes
OB-90 Glossar	Glossar und Rechtsgrundlagen	Anhang	Beschreibt Vorhandenes

Ordavis Bauhof — Handbuch-Übersicht

OB-00 Übersicht Alpha-Hinweis, Lesewege, Dokumentenkarte und Impressum

Beschreibt Vorhandenes

Willkommen zur Dokumentation von **Ordavis Bauhof**, dem Fachverfahren für den kommunalen Baubetriebshof: Betriebsmittel führen, Prüffristen überwachen, Straßenausstattung erfassen und kontrollieren, Anordnungen vollziehen, Werkstatt und Lager bewirtschaften, Winterdienst nachweisen.

Ordavis Bauhof ist ein Produkt der Dachmarke **Ordavis** von **Grams IT**. Gliederung und Darstellung folgen dem Handbuchwerk der Ordavis Plattform — ein Haus, das beide betreibt, soll nicht zwei Lesegewohnheiten brauchen.

INHALT

⚠️ ⚠️ Alpha-Fassung — lesen Sie das zuerst

Der Stand jedes Dokuments

Die beiden Bände

Wo Sie anfangen

Dokumentenkarte

Grundlagen — in beiden Bänden

Administratorhandbuch

Verwaltungshandbuch

Was dieses Werk (noch) nicht enthält

Konventionen

★ ★ ★ Woher ein Begriff kommt, steht dabei

Impressum

Nachweise Dritter

Kein Rechtsrat

Verwandte Themen

⚠️ ⚠️ Alpha-Fassung — lesen Sie das zuerst

Ordavis Bauhof befindet sich im Alphastand. Das Produkt ist nicht freigegeben, nicht abgenommen und in keiner Kommune im Wirkbetrieb.

Achtung: Anwendung und Inhalte können sich jederzeit ändern. Bildschirme, Bezeichnungen, Menüwege, Schnittstellen, Datenfelder und Abläufe stehen unter Vorbehalt — auch so, dass ein in diesem Handbuch beschriebener Weg danach anders verläuft oder ganz entfällt. Eine Ankündigung dafür gibt es im Alphastand nicht.

Wichtig: Dieses Handbuch ist keine Leistungsbeschreibung und keine Zusage. Es beschreibt den Stand am Tag des Satzes. Verbindlich ist allein, was vertraglich vereinbart wird.

☆☆☆ Der Grund für diese Deutlichkeit ist nicht Bescheidenheit, sondern Haftung. Ein Handbuch wird im kommunalen Vergabewesen als Leistungsbeschreibung gelesen. Ein Kapitel über eine Maske, die es nicht gibt, ist dann keine Vorwegnahme, sondern eine Zusage — und die steht später einer Abnahme gegenüber.

Der Stand jedes Dokuments

Damit die Alpha-Warnung nicht als pauschaler Vorbehalt über allem schwebt und damit nichts sagt, trägt jedes Dokument im Kopf einen Stand:

Stand	Was Sie erwarten dürfen
gebaut	Beschreibt Vorhandenes. Am Programm nachgesehen, nicht aus dem Konzept abgeleitet.
teilweise	Der beschriebene Teil ist da; welcher Teil fehlt, steht im Dokument.
geplant	Noch nichts davon gebaut. Das Dokument nennt das Arbeitspaket und beschreibt keine Bedienung.

Ein Prüfskript (`build/pruefe_handbuch.py`) setzt das durch: Ein Dokument mit dem Stand `geplant` , das eine Bedienung im Indikativ beschreibt („Sie klicken auf ...“), lässt den Lauf scheitern. Ein Dokument mit dem Stand `teilweise` , das nirgends sagt, was fehlt, ebenso.

⚠ Ohne diesen Wächter wäre die Regel ein Vorsatz. Genau so entstehen Handbücher, die mehr versprechen als das Programm hält — nicht aus Absicht, sondern weil beim Schreiben niemand nachsieht.

Die beiden Bände

Dieses Handbuchwerk erscheint in **zwei Bänden**, weil es zwei Publika hat, die nichts voneinander brauchen.

Band	Für wen	Was darin steht
Administratorhandbuch	Systemadministration, IT-Betrieb	Architektur, Installation, Konfiguration, Zugänge, Aktualisierung, Sicherung, Hintergrunddienste, Störungsbilder, Schnittstelle
Verwaltungshandbuch	Verwaltung, Sachbearbeitung, Betriebsleitung	Anmeldung und Aufbau des Portals, Bestand, Prüffristen, Anordnungen, Werkstatt, Lager, Winterdienst, Nachweise, Datenschutz

☆☆ **Drei Dokumente stehen in beiden Bänden** — diese Übersicht, die Einführung und das Glossar. Sie sind dort jeweils **vollständig abgedruckt** und nicht als Verweis: Der Administrator bekommt seinen Band als eine Datei, und ein Glossar, das im anderen liegt, ist für ihn keines.

Wo Sie anfangen

Sie müssen dieses Werk nicht am Stück lesen. Suchen Sie Ihre **Rolle** — die Tabelle nennt die Dokumente, die für Ihre Aufgaben zählen.

Rolle	Was Sie tun	Ihr Einstieg	Weiterführend
Systemadministrator	Installieren, konfigurieren, betreiben	OB-50	OB-40, OB-52, OB-54
IT-Betrieb	Aktualisieren, sichern, wiederanlaufen	OB-51	OB-02, OB-54
Zugangsverwaltung	Benutzer, Rollen, Kennwörter, Stationen	OB-41	OB-42, OB-44
Verwaltung / Sachbearbeitung	Anordnungen, Vollzug, Nachweise, Fristen	OB-14	OB-24, OB-22, OB-27
Betriebsleitung	Bestand, Rückstand, Auswertung	OB-25	OB-23, OB-27, OB-30
Werkstatt / Lager	Fahrzeuge, Prüffristen, Material, Ausgabe	OB-25	OB-28, OB-22
Einsatzleitung	Tagesarbeit, Disposition, Winterdienst	OB-23	OB-26
Datenschutzbeauftragte	Verarbeitung, Rechtsgrundlage, Betroffenenrechte	OB-32	OB-33, OB-41
Personalrat	Beschäftigtendatenschutz, Auswertungssperren	OB-33	OB-32
Revision / Prüfung	Nachweise, Berechtigungen, Protokolle	OB-27	OB-44, OB-32
Entwicklung / Integration	Schnittstelle, Datenübernahme, Export	OB-60	OB-02

Dokumentenkarte

Die Karte listet **alle** Dokumente dieses Werks.

Grundlagen — in beiden Bänden

Code	Dokument	Zielgruppe	Stand
OB-00	Handbuch-Übersicht, Alpha-Hinweis und Impressum	Alle	gebaut
OB-01	Einführung und Grundlagen	Alle	gebaut
OB-90	Glossar und Rechtsgrundlagen	Alle	gebaut

Administratorhandbuch

Code	Dokument	Zielgruppe	Stand
OB-02	Systemvoraussetzungen und Architektur	Betrieb / Admin	gebaut
OB-40	Administrationshandbuch — der Betrieb im Überblick	Administrator	gebaut
OB-41	Benutzer, Rollen und Zugang	Administrator	gebaut

Code	Dokument	Zielgruppe	Stand
OB-42	Ausgabestationen und Fahrzeuggeräte	Administrator	gebaut
OB-44	Rollen- und Rechtematrix	Revision / Admin	gebaut
OB-50	Installation und Server	IT-Betrieb	gebaut
OB-51	Aktualisierung, Sicherung, Wiederanlauf	IT-Betrieb	teilweise
OB-52	Konfigurationsreferenz	IT-Betrieb	gebaut
OB-54	Wachen, Betriebsprotokoll und Störungsbilder	IT-Betrieb	gebaut
OB-60	Schnittstellen-Referenz	Entwicklung	gebaut

Verwaltungshandbuch

Code	Dokument	Zielgruppe	Stand
OB-14	Das Portal — Anmeldung, Aufbau, Bedienung	Verwaltung	gebaut
OB-20	Modul Straßenkataster	Fachanwender	teilweise
OB-22	Modul Kontrolle und Prüffristen	Verwaltung / Werkstatt	teilweise
OB-23	Disposition und Arbeitsvorrat	Einsatzleitung	teilweise
OB-24	Anordnungen und Vollzugsmeldungen	Verwaltung	gebaut
OB-25	Fuhrpark, Werkstatt und Lager	Betriebsleitung / Werkstatt	teilweise
OB-26	Modul Winterdienst	Einsatzleitung / Verwaltung	teilweise
OB-27	Nachweise und Berichte	Verwaltung / Revision	teilweise
OB-28	Werkzeug- und Materialausgabe	Lager	gebaut
OB-30	Personenstamm und Besetzung des Tages	Verwaltung / Einsatzleitung	gebaut
OB-31	Befähigung und Berechtigung	Verwaltung / Leitung	gebaut
OB-32	Datenschutz	DSB / Verwaltung	teilweise
OB-33	Beschäftigtendatenschutz und Mitbestimmung	Personalrat / Leitung	teilweise

Was dieses Werk (noch) nicht enthält

★ **Genannt statt verschwiegen.** Wer nichts findet, weiß sonst nicht, ob es das Kapitel nicht gibt oder ob das Handbuch es vergessen hat.

Thema	Warum kein Dokument
Außendienst-App (Aufzeichnung, Beleg, Etikett)	Eigenes Dokument OB-10, gehört in einen dritten Band für den Außendienst. Es ist nicht Teil der beiden hier gesetzten Bände.
Lizenzierung und Aktivierung	Es gibt kein Lizenzsystem. Ordvis Bauhof prüft weder Lizenzschlüssel noch Aktivierung. Ein Kapitel darüber beschrieb nichts.

Thema	Warum kein Dokument
Mandantenfähigkeit	Eine Installation, ein Bauhof (<code>ENT-11</code>). Der Anspruch <code>tenant_id</code> steht im Anmelde-Token, wird aber nirgends ausgewertet.
Datenbank-Referenz (Tabellen und Spalten)	Das Schema entsteht im Alphastand aus dem Modell (<code>EnsureCreated</code>) und ändert sich mit jeder Fassung. Eine Referenz darauf wäre am Tag nach dem Satz falsch.

Konventionen

Zeichen	Bedeutung
Fett	Beschriftung auf dem Bildschirm
<code>Schreibmaschine</code>	Eingabe, Dateiname, Pfad, Endpunkt, Kennung eines Arbeitspakets
⚠	Hinweis, dessen Missachtung Daten, Nachweise oder Betrieb kostet
★	Entwurfsentscheidung mit Begründung
<code>FUH-05</code>	Kennung eines Arbeitspakets aus der Projektplanung — sie erlaubt es, im Support genau zu benennen, worüber gesprochen wird
Ⓢ	Hausbegriff von Ordvis — siehe unten

Sprache. Das Programm spricht Deutsch, und das Handbuch auch. Wo ein englischer Fachbegriff unvermeidlich ist, steht er einmal in Klammern und danach nicht mehr.

★ ★ ★ Woher ein Begriff kommt, steht dabei

Dieses Werk benutzt Wörter aus drei ganz verschiedenen Quellen — und **das sieht man einem Wort nicht an**. Deshalb sind sie gekennzeichnet:

Herkunft	Kennzeichen	Beispiele	Was das für Sie heißt
Allgemeinsprache	keines	Auftrag, Frist, Lager	Nichts weiter.
Fachbegriff der Branche	keines, aber im Glossar erklärt	Hauptuntersuchung, UVV, Verkehrssicherungspflicht, Urschrift, Peilung, Wiedervorlage	Sie können ihn nachschlagen — in Vorschriften, Fachliteratur, bei Ihrem Unfallversicherungsträger.
Hausbegriff von Ordvis	Ⓢ	Ⓢ Wache, Ⓢ Fachdienst, Ⓢ Übersteuerung, Ⓢ Rückfallregel, Ⓢ Arbeitsplatz	⚠ Sie können ihn nicht nachschlagen. Er gilt nur hier. Was er bedeutet, steht bei seiner ersten Nennung und im Glossar (OB-90).

★ ★ ★ Der Grund für diese Unterscheidung ist eine **verlorene Stunde, nicht Ordnungsliebe**. Ein Hausbegriff, der wie ein Fachbegriff aussieht, schickt den Leser in die falsche Literatur: Wer „Wache“ für

einen Begriff aus dem Arbeitsschutz hält, sucht ihn in der DGUV-Vorschrift 70 — und findet dort nichts, ohne zu erfahren, dass es dort auch nichts zu finden gibt.

⚠ **Ein Hausbegriff wird erklärt, nicht ersetzt.** Er steht so im Betriebsprotokoll, in der Konfiguration und auf dem Bildschirm; ein anderes Wort im Handbuch zwänge Sie bei jedem Nachschlagen zum Übersetzen.

Merksatz für den Hersteller: **Jeder unübliche Begriff wird an drei Stellen geklärt** — bei der ersten Nennung im Text, im Glossar mit seinem Herkunftskennzeichen, und dort, wo er dem Anwender auf dem Bildschirm zuerst begegnet.

Bildschirmnamen. Kursiv oder fett gesetzte Begriffe sind wortgleich die Beschriftungen im Programm. ⚠ Im Alphastand ändern sich diese Beschriftungen; im Zweifel gilt, was auf dem Bildschirm steht.

Impressum

Produkt	Ordvis Bauhof
Dachmarke	Ordvis
Hersteller	Grams IT
Produktfassung	siehe Titelseite und Fußzeile dieses Bandes
Handbuchfassung	siehe Titelseite
Anschrift, Vertretung, Kontakt	siehe ordvis.eu/impressum.html
Dokumentation im Netz	ordvis.eu/dokumentation.html
Meldung von Schwachstellen	ordvis.eu/produktsicherheit.html

Nachweise Dritter

⚠ **Der Kartenunterbau** ist basemap.de des Bundesamts für Kartographie und Geodäsie. Die von der Lizenz verlangte Namensnennung lautet © **basemap.de / BKG** (www.bkg.bund.de) und steht an jeder Karte im Programm.

Die Erzeugung von PDF-Dokumenten (Vollzugsmeldung, Schichtnachweis, Tagesliste, Schadensakte) verwendet **QuestPDF** unter der Community-Lizenz.

Kein Rechtsrat

Die in diesem Werk genannten Rechtsgrundlagen — § 29 StVZO, DGUV Vorschrift 70, § 14 BetrSichV, § 45 StVO, § 74 HPVG, DSGVO — sind eine **fachliche Einordnung**. Intervalle, Prüferqualifikation, Nachweis- und Aufbewahrungspflichten sind vor dem Wirksamwerden mit dem Unfallversicherungsträger, der Rechtsaufsicht, der Kämmerei und einer fachkundigen Stelle abzugleichen. Das gilt im Alphastand ganz besonders.

Verwandte Themen

- **OB-01 · Einführung und Grundlagen** — warum es Ordvis Bauhof gibt und nach welchen Leitideen es gebaut wird
- **OB-90 · Glossar und Rechtsgrundlagen** — jeder Begriff, der in diesem Werk anders gebraucht wird als umgangssprachlich

Einführung und Grundlagen

OB-01 Einführung Was Ordvis Bauhof ist, wofür es gedacht ist und nach welchen Leitideen es gebaut wird

Beschreibt Vorhandenes

Ein kommunaler Bauhof hält eine Stadt in Betrieb. Er räumt Schnee, stellt Schilder auf, mäht Grün, prüft Spielgeräte, repariert, was kaputtgeht, und rückt aus, wenn ein Ast auf der Fahrbahn liegt. Wie er das tut, steht selten an einer Stelle. Es steht in Köpfen, auf einem Kalender im Meisterbüro, in Ordnern hinter der Tür und in einer Tabelle, die eine einzelne Person pflegt.

Das trägt, solange niemand fragt. Gefragt wird nach einem Sturz auf dem Gehweg, nach einer Beschwerde, vor einer Prüfung durch die Aufsicht — oder an dem Tag, an dem die Person krank ist, die es weiß. Dann fehlt nicht die Arbeit; die wurde geleistet. Es fehlt der **Beleg**, dass sie geleistet wurde, und zwar rechtzeitig und von jemandem, der es durfte.

Ordvis Bauhof schließt genau diese Lücke. Es führt den Bestand, die Fristen, die Aufträge und die Personen in **einem** Verfahren und schreibt dabei mit, was geschehen ist. Dieses Dokument erklärt die Leitideen, aus denen alles Weitere folgt — und es sagt ebenso deutlich, was Ordvis Bauhof ausdrücklich **nicht** sein will.

INHALT

1 Die Frage, aus der dieses Produkt entstanden ist

2 Was Ordvis Bauhof ist

2.1 Was es ausdrücklich nicht ist

3 Die drei Oberflächen

3.1 ★ ★ ★ Die Hausregel

4 Die Leitideen

4.1 Ein Nachweis ist etwas anderes als eine Notiz

4.2 Eine Messreihe ist kein Feld

4.3 Ein Bestand ist die Summe der Bewegungen

4.4 Eine Beziehung hat eine Zeit

4.5 Was von selbst geschieht, geschieht auch, wenn niemand hinsieht

4.6 Eine ehrliche Grenze schützt vor einer enttäuschten Erwartung

5 Die Cluster — die Ordnung hinter den Arbeitspaketen

6 Verhältnis zur Ordvis Plattform

7 Was Sie zum Weiterlesen brauchen

Verwandte Themen

1 Die Frage, aus der dieses Produkt entstanden ist

Stellen Sie sich vor, ein Jahr nach einem Unfall fragt ein Gericht: „Wann ist diese Straße das letzte Mal kontrolliert worden, von wem, und was wurde dabei festgestellt?“

In vielen Bauhöfen steht die Antwort auf einem Zettel im Fahrzeug, in einem Ordner im Regal oder in der Erinnerung eines Kollegen, der seit zwei Jahren im Ruhestand ist. Dieselbe Frage stellt sich in Varianten den

ganzen Betrieb entlang:

- Wann war der Unimog zuletzt bei der Hauptuntersuchung — und wo ist der Nachweis?
- Welcher Streuer hing am 14. Januar an welchem Fahrzeug?
- Wieviel Splitt liegt noch in Halle 2, und stimmt das mit dem, was gebucht wurde?
- Wer darf die Motorsäge führen, und ist seine Unterweisung noch gültig?
- Ist die Anordnung vom März vollzogen, und wer hat den Vollzug gemeldet?

Ordvis Bauhof ist der Versuch, diese Fragen **belegbar** zu beantworten — nicht dem Gedächtnis nach, sondern aus einem Bestand, der beim Arbeiten nebenbei entsteht.

2 Was Ordvis Bauhof ist

Ordvis Bauhof ist ein **Fachverfahren für den kommunalen Baubetriebshof**. Es führt drei Dinge zusammen, die in der Praxis meist in getrennten Listen liegen:

Gegenstand	Was geführt wird
Betriebsmittel	Fahrzeuge, Anbaugeräte, Maschinen, Kleingeräte — mit Zählerständen, Prüffristen, Schäden und Akte
Straßenausstattung	Verkehrszeichen, Ausstattung und Anlagen im öffentlichen Raum — mit Zustand, Kontrollpflicht und Historie
Arbeit	Anordnungen, Aufträge, Kontrollgänge, Werkstattaufträge, Materialentnahmen, Winterdiensteinsätze

Der Zusammenhang ist der eigentliche Gehalt: Eine **Anordnung** erzeugt einen **Auftrag**, der Auftrag verändert den **Bestand**, der Bestand erzeugt eine **Kontrollpflicht**, die Kontrolle erzeugt einen **Mangel**, der Mangel erzeugt den nächsten Auftrag. Wer nur eine dieser Stationen führt, führt eine Liste; wer den Kreis führt, hat einen Nachweis.

2.1 Was es ausdrücklich nicht ist

☆☆ Ordvis Bauhof ist kein IT-Verwaltungssystem und sieht auch nicht so aus. Das Menü enthält keine Netzwerk-Erkennung, keine IP-Adressverwaltung, keine Notfallplanung. Eine kommunale Installation, in der solche Einträge stehen, verliert das Vertrauen der Anwender in der ersten Schulungsstunde — und der Bauhof hat recht damit.

Es ist außerdem kein **Zeitwirtschaftssystem**. Was hier erfasst wird, ist **Auftragszeit** für die Kosten- und Leistungsrechnung, nicht Arbeitszeit; die liegt beim Personalwesen in dessen eigenem Verfahren. Die Grenze ist keine Feinheit — mehr dazu in OB-33 (Verwaltungshandbuch).

3 Die drei Oberflächen

Oberfläche	Technik	Für wen
Portal	Blazor Server, im Browser	Verwaltung, Betriebsleitung, alle, die einen Arbeitsplatz haben
Arbeitsplatz	WinUI 3, Windows-Programm	Bauhofleitung, Werkstattmeister, Lagerverwalter, Kämmerei
Außendienst-App	Android, im Fahrzeug	Fahrer, Kontrolleure

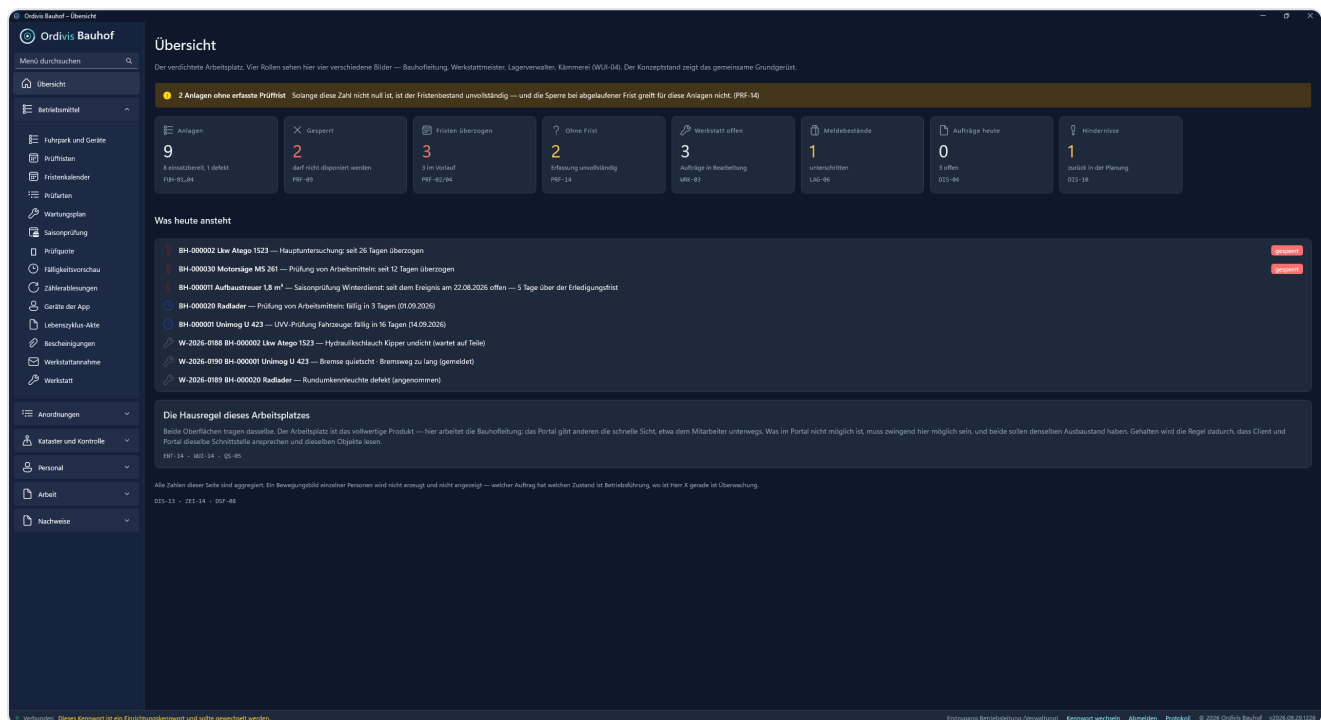


Abbildung 1 — Der Arbeitsplatz nach dem Anmelden: acht Kennzahlen zum Bestand, darunter „Was heute ansteht“ mit den überzogenen Prüfungen und den offenen Werkstattmeldungen. Die rot hinterlegten Zahlen verlangen eine Entscheidung, die übrigen sind Auskunft.

3.1 ★★ Die Hausregel

Merksatz: Was der Arbeitsplatz kann, muss das Portal auch können. Der Arbeitsplatz darf schneller sein, nicht mächtiger.

Jede Fachlogik, die nur im Windows-Programm existiert, ist eine Funktion, die es für Anwender mit Hilfsmitteln nicht gibt — Barrierefreiheit nach BITV 2.0 ist über das Portal erreichbar, nicht über ein Desktop-Programm.

Technisch gehalten wird die Regel dadurch, dass **Portal und Arbeitsplatz dieselbe Schnittstelle ansprechen und dieselben Objekte lesen**. Keiner von beiden rechnet selbst. Die Prüfung vor der Auslieferung (WUI-14) hält beide Menübäume noch einmal ausdrücklich gegeneinander.

⚠️ **Das Gefälle darf nur in eine Richtung bestehen.** Heute führt das Portal *mehr* Einträge als der Arbeitsplatz — Anbaugeräte, Disposition, den Planstand. Das ist die zulässige Richtung. Umgekehrt wäre es ein Befund.

4 Die Leitideen

Sechs Entscheidungen ziehen sich durch das ganze Produkt. Wer sie kennt, versteht die meisten Einzelheiten, ohne sie nachschlagen zu müssen.

4.1 Ein Nachweis ist etwas anderes als eine Notiz

Ein Nachweis trägt **wer, wann, wo** und **womit**. Deshalb steht an einem Kontrollgang der Name des Kontrolleurs, an einem Beleg der Fehlerradius der Ortung, an einer Prüfung die hinterlegte Bescheinigung.

⚠️ Eine Frist ohne hinterlegten Beleg ist im Schadensfall wertlos.

4.2 Eine Messreihe ist kein Feld

Ein Betriebsstundenzähler ist keine Zahl, sondern eine Reihe von Ablesungen mit Ableser, Zeitpunkt und Quelle. Beim **Zählertausch** beginnt die Anzeige neu, der Betriebsstundenstand nicht. Ein einzelnes Feld könnte das nicht abbilden — und niemand würde bemerken, dass es falsch ist.

4.3 Ein Bestand ist die Summe der Bewegungen

Der Lagerbestand wird **nicht** als Feld fortgeschrieben, sondern aus allen Buchungen gerechnet. Ein fortgeschriebenes Feld ist nach dem ersten Abbruch mitten in einer Buchung falsch, und niemand kann sagen, seit wann.

4.4 Eine Beziehung hat eine Zeit

Die Frage lautet nicht „*welcher Streuer hängt am Unimog*“, sondern „*welcher Streuer hing am 14. Januar am Unimog*“. Montagen tragen deshalb einen Zeitraum, nicht nur einen Zustand.

4.5 Was von selbst geschieht, geschieht auch, wenn niemand hinsieht

Fristen, Bestandsuntergrenzen, ausbleibende Ablesungen und überfällige Kontrollen werden täglich selbsttätig geprüft. Der Alltag hat genau eine Bedingung, die als erste ausfällt: dass jemand in eine Übersicht sieht.

Hinweis: **Wache** ☹ — so heißen in Ordvis Bauhof die acht Abläufe, die das tun. Der Begriff ist ein **Hausbegriff**: Er stammt aus dem Programm, nicht aus der Fachsprache des Bauhofs. Sie werden ihn in keiner DGUV-Vorschrift und in keinem Verwaltungshandbuch finden — wohl aber wörtlich im Betriebsprotokoll („*Fristenwache (PRF-05) läuft täglich um 06:30*“), im Konfigurationsabschnitt **Lueckenwache** und auf der Portalseite **Eskalation**. Deshalb steht er auch hier so; ein anderes Wort im Handbuch zwänge Sie beim Nachschlagen zum Übersetzen.

Eine **Wache** ist: ein Ablauf im Fachdienst, der **einmal täglich zu fester Uhrzeit** eine fachliche Frage prüft und seinen Befund ins Betriebsprotokoll schreibt. Sie lässt sich **ab- und anschalten** und ihre Uhrzeit setzen; mehr nicht.

⚠ **Nicht zu verwechseln** mit den *geplanten Aufgaben* der Ordvis Plattform: Dort gibt es dafür eine Maske mit Liste, Schalter und „Jetzt ausführen“. Ordvis Bauhof hat das nicht — hier wird über die Konfigurationsdatei und einen Dienstneustart gesteuert. Und **nicht** mit den *Windows-Diensten* `Ordvis.Bauhof.API` und `.Portal` : Die Wachen laufen **innerhalb** des Fachdienstes.

Die vollständige Liste der acht steht in OB-54 (Administratorhandbuch).

⚠ Diese Wachen **melden ins Betriebsprotokoll und verschicken nichts**. Ein Dienst, der Post verschickt, braucht Postfach, Zugangsdaten und Empfängerliste — und die sind genau dann falsch, wenn es darauf ankommt. Die Versandwege sind ein eigenes, noch offenes Arbeitspaket (`PEX-10`).

4.6 Eine ehrliche Grenze schützt vor einer enttäuschten Erwartung

Das Portal enthält im Alphastand die Seite **Was fehlt noch** (`/plan`). Sie nennt, was in diesem Stand umgesetzt ist und was nicht — und warum das Fehlende wichtig ist. Sie entfällt im Kundenstand.

5 Die Cluster — die Ordnung hinter den Arbeitspaketen

Alle Kennungen in diesem Handbuch (`FUH-05` , `PRF-09` , `WIN-11` ...) folgen einer festen Ordnung. Sie ist im Support nützlich: Statt „das mit den Fristen“ lässt sich `PRF-04` sagen.

Kürzel	Cluster
ENT	Grundsatzentscheidungen des Produkts
FUH	Fuhrpark und Geräte
PRF	Prüffristen und Wartung
WRK	Werkstatt und Schadensmanagement
LAG	Lager und Materialwirtschaft
DIS	Disposition und Einsatzplanung
ZEI	Zeiterfassung und Kosten-Leistungs-Rechnung
WIN	Winterdienst und Straßenreinigung
INV	Bewegliches Inventar und Aufbauten

Kürzel	Cluster
KTR / KLA	Kataster und Kontrolle
ITS	Anordnungen und Prozesskreis
NAW	Nachweise und Berichte
DSF	Datenschutz und Beschäftigtendatenschutz
BET	Betrieb, Installation, Koexistenz, Zugang
PEX	Übernahme aus der Ordvis Plattform
WUI	Windows-Arbeitsplatz
MOB	Außendienst-App
BUE	Bürgermeldungen (<i>optional</i>)
CV	Bilderkennung

6 Verhältnis zur Ordvis Plattform

Ordvis Bauhof ist ein **eigenes Produkt mit eigener Datenbank und getrennter Installation** (ENT-11). Es ist **kein Modul** der Ordvis Plattform.

Gleichzeitig erbt es von ihr: Datenmodell-Muster, Anmeldeverfahren, Kennwortverfahren, Aktualisierungsweg, Darstellungsregeln. Ein Unimog ist im übernommenen Modell ein Konfigurationsobjekt mit einer Klasse, genau wie ein Verkehrszeichen.

Drei Dinge kann dieses geerbte Modell nicht, und alle drei sind in Ordvis Bauhof eigens gebaut:

Lücke	Warum ein Attribut es nicht kann
Zählerstand (FUH-05)	Eine Messreihe mit Ableser, Zeitpunkt und Quelle ist kein Wert.
Zeitbezogene Beziehung (FUH-07)	Eine Beziehung beantwortet nur die Gegenwart; gefragt ist ein Stichtag.
Bestandsmenge (LAG-01)	Ein Kubikmeter Splitt hat keine Identität; der Bestand ist die Summe der Bewegungen.

⚠ Wer beide Produkte auf einem Server betreibt, findet in OB-02 und OB-50 (Administratorhandbuch) die fünf Dinge, die sich unterscheiden **müssen** — Dienstname, Port, Verzeichnis, Datenbank, Datenbankrolle.

7 Was Sie zum Weiterlesen brauchen

Sie wollen ...	Lesen Sie	Band
das System installieren	OB-50	Administratorhandbuch
verstehen, was auf dem Server läuft	OB-02	Administratorhandbuch
Benutzer und Kennwörter verwalten	OB-41	Administratorhandbuch
mit dem Portal arbeiten	OB-14	Verwaltungshandbuch
Prüffristen führen	OB-22	Verwaltungshandbuch
eine Anordnung vollziehen	OB-24	Verwaltungshandbuch
einen Nachweis für Gremien erzeugen	OB-27	Verwaltungshandbuch
einen Begriff nachschlagen	OB-90	beide Bände

★ **Die Spalte Band ist keine Zierde.** Sie halten **einen** der beiden Bände in der Hand. Was im anderen steht, finden Sie dort — und nicht durch Blättern in diesem.

Verwandte Themen

- **OB-24 · Anordnungen und Vollzugsmeldungen** (Verwaltungshandbuch) — der Prozesskreis aus Anordnung, Auftrag, Ausführung und Nachweis in ganzer Länge
- **OB-14 · Das Portal — Anmeldung und Aufbau** (Verwaltungshandbuch) — das Portal: anmelden, sich zurechtfinden, Listen bedienen
- **OB-02 · Systemvoraussetzungen und Architektur** (Administratorhandbuch) — was auf dem Server läuft und wie die Teile zusammenhängen
- **OB-90 · Glossar und Rechtsgrundlagen** — Begriffe, Abkürzungen und die Rechtsgrundlagen, auf die sich das Verfahren stützt

Systemvoraussetzungen und Architektur

OB-02 Architektur Was auf dem Server läuft, was es braucht und wie die Teile zusammenhängen

Beschreibt Vorhandenes

„Was muss ich denn aufstellen?“ ist die erste Frage der Systemadministration, und sie hat selten eine Ein-Wort-Antwort. Ordvis Bauhof ist kein Programm, das man auf einen Rechner legt, sondern ein Fachdienst mit einer Datenbank, auf den drei sehr verschiedene Oberflächen zugreifen: ein Windows-Arbeitsplatz, ein Portal im Browser und eine App im Fahrzeug.

Das hat einen Grund, und der ist keine Geschmacksfrage. Ein Werkstattmeister arbeitet stundenlang an einer Liste und braucht dabei den Vorgang daneben; eine Sachbearbeiterin öffnet zweimal am Tag eine Auskunft; ein Fahrer hat eine Hand frei und Handschuhe an. Dieselbe Oberfläche für alle drei wäre für alle drei die falsche.

Dieses Dokument beschreibt, welche Teile es gibt, was jedes davon tut, worüber sie miteinander reden und was der Server dafür mitbringen muss. Wer lieber Handgriffe als Zusammenhänge liest, findet dieselbe Anlage im Installationskapitel Schritt für Schritt.

INHALT

1 Der Aufbau in einem Bild

2 Die Teile im Einzelnen

3 Systemvoraussetzungen

3.1 Server

3.2 Arbeitsplatz

3.3 Netz

4 ⚠️ ⚠️ Koexistenz mit der Ordvis Plattform

4.1 Die Falle mit den maschinenweiten Umgebungsvariablen

5 Das Datenmodell in Stichworten

5.1 ⚠️ Das Schema entsteht aus dem Modell — die wichtigste Grenze des Alphastands

6 Wo Daten liegen

7 Was dieser Stand nicht kann

Verwandte Themen

1 Der Aufbau in einem Bild

Ordvis Bauhof besteht aus **zwei Windows-Diensten**, einer **Datenbank** und **zwei Bedienoberflächen**. Alles läuft im Haus; es gibt keinen Anteil in einer Wolke.

Alles im Haus — es gibt keinen Anteil in einer Wolke.

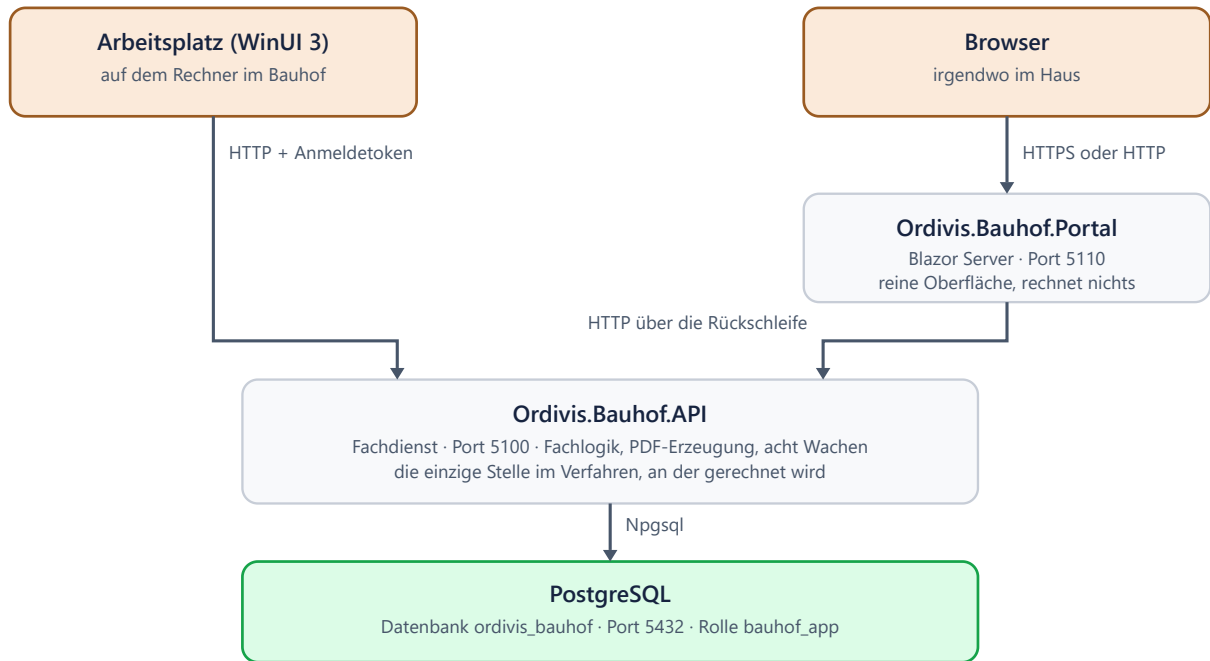


Abbildung 2 — Der Aufbau. Zwei Oberflächen, ein Fachdienst, eine Datenbank — und nur der Fachdienst rechnet.

☆☆ Der Fachdienst ist die einzige Stelle, an der gerechnet wird. Portal und Arbeitsplatz rufen dieselben Endpunkte auf und lesen dieselben Objekte. Das ist der technische Ort der Hausregel aus OB-01: Was der Arbeitsplatz kann, muss das Portal auch können.

2 Die Teile im Einzelnen

Baustein	Was er ist	Wo er läuft
<code>Ordavis.Bauhof.API</code>	Fachdienst: REST-Schnittstelle, EF Core auf PostgreSQL, alle Fachrechnungen, alle Wachen	Windows-Dienst, Port 5100
<code>Ordavis.Bauhof.Portale</code>	Webportal, Blazor Server mit MudBlazor	Windows-Dienst, Port 5110
<code>Ordavis.Bauhof.Client</code>	Arbeitsplatz, WinUI 3	Auf dem Arbeitsplatzrechner
<code>Ordavis.Bauhof.Shared</code>	Domänenmodell und Übertragungsobjekte — ohne Datenbank- und Oberflächenbezug	Bibliothek in allen dreien
<code>Ordavis.Bauhof.Ausgabe</code>	PDF-Erzeugung (Vollzugsmeldung, Schichtnachweis, Tagesliste, Schadensakte)	Bibliothek im Fachdienst
PostgreSQL	Datenhaltung	Vorhandener Server, eigene Datenbank

☆ `Shared` hat bewusst keinen Datenbankbezug. Die Fachrechnungen (Fristenrechner, Verfügbarkeitsprüfung, Bestandsrechnung) sind damit ohne laufende Datenbank prüfbar — dasselbe

Muster wie beim Ordavis Winterdienst-Protokoll.

3 Systemvoraussetzungen

3.1 Server

	Mindestens	Empfohlen
Betriebssystem	Windows Server 2022	Windows Server 2025
Prozessor	4 Kerne	8 Kerne
Arbeitsspeicher	8 GB	16 GB
Plattenplatz Programm	1 GB	2 GB
Plattenplatz Daten	10 GB	wächst mit Belegen und Winterdienstprotokollen
Laufzeitumgebung	.NET 10 (im Verteilstand enthalten)	—
Datenbank	PostgreSQL 15	PostgreSQL 16 oder neuer
Rechte für die Installation	lokaler Administrator	—

⚠ **Windows 11 geht auch.** Für Erprobung, Schulung und kleine Gemeinden ist ein Windows-11-Rechner ein zulässiges Ziel; die Dienste laufen dort unverändert. Für den Wirkbetrieb ist ein Server die richtige Wahl — schon wegen der Sicherung.

3.2 Arbeitsplatz

Portal	Aktueller Browser (Edge, Chrome, Firefox). ⚠ Blazor Server hält eine stehende Verbindung — eine unterbrochene Leitung meldet sich als Verbindungsverlust in der Seite.
Arbeitsplatzprogramm	Windows 11, x64. Windows App SDK wird mitgeliefert.
Bildschirm	1920 × 1080 oder größer. Die Fachlisten sind breit.

3.3 Netz

Von	Nach	Port	Wofür
Arbeitsplatzrechner	Server	5110/TCP	Portal im Browser
Arbeitsplatzprogramm	Server	5100/TCP	Fachdienst
Portal (auf dem Server)	Fachdienst (auf dem Server)	5100 über localhost	Rückschleife
Fachdienst	PostgreSQL	5432/TCP	Datenbank

Von	Nach	Port	Wofür
Portal	<code>basemap.de</code> (BKG)	443/TCP	Kartenhintergrund

⚠ **Der Fachdienst wird vom Installer NICHT in der Firewall geöffnet.** Solange nur das Portal auf demselben Rechner ihn anspricht, hat er im Netz nichts zu suchen. Wer das Arbeitsplatzprogramm auf anderen Rechnern einsetzt, öffnet 5100 ausdrücklich — siehe OB-50, Abschnitt zur Firewall.

★ **Der Kartenhintergrund wird serverseitig geholt.** Die Karte steht damit auch dann, wenn der Arbeitsplatz in der Gemeinde keinen eigenen Weg ins Netz hat. Bleibt der Hintergrund aus, bleibt die gefahrene Linie: Sie ist der Nachweis, die Karte ist die Lesehilfe.

4 ⚠ ⚠ Koexistenz mit der Ordvis Platform

Auf demselben Rechner läuft in aller Regel bereits die **Ordvis Platform**. Ordvis Bauhof ist nach `ENT-11` ein eigenes Produkt mit eigener Datenbank und getrennter Installation. **Fünf Dinge müssen sich unterscheiden**, und `deploy\setup.ps1` prüft alle fünf, *bevor* es etwas tut:

	Ordvis Platform	Ordvis Bauhof
Dienste	<code>InfraDesk.API</code> , <code>InfraDesk.Portal</code>	<code>Ordvis.Bauhof.API</code> , <code>Ordvis.Bauhof.Portal</code>
Ports	5000 / 5001, 8080 / 443	5100, 5110
Verzeichnis	<code>...\Ordvis Platform</code>	<code>...\Ordvis Bauhof</code>
Datenbank	<code>infradesk</code>	<code>ordvis_bauhof</code>
Datenbankrolle	<code>infradesk_app</code>	<code>bauhof_app</code>
Installer-Anwendungskennung	eigene	eigene

Der PostgreSQL-Server wird **geteilt**, die Datenbank **nicht**. Ein zweiter Datenbankserver auf demselben Rechner kostete Arbeitsspeicher, eine zweite Sicherungsstrecke und eine zweite Stelle, an der jemand ein Kennwort pflegen muss.

Achtung: Die **geteilte Anwendungskennung** wäre der schlimmste denkbare Fehler des Setups. Windows hielte beide Produkte für dieselbe Anwendung, und eine Deinstallation von Ordvis Bauhof nähme die Ordvis Platform mit. Sie ist deshalb ausdrücklich eine andere.

4.1 Die Falle mit den maschinenweiten Umgebungsvariablen

★★★ **Befund vom 27.08.2026, und der Grund für eine Besonderheit im Fachdienst.**

Auf dem Entwicklungsrechner standen `Identity__Jwt__Secret` , `__Issuer` und `__Audience` als **maschinenweite** Umgebungsvariablen — gesetzt für die Ordvis Platform. ASP.NET Core liest

Umgebungsvariablen **zuletzt** und damit stärker als jede `appsettings.json`. Der Fachdienst von Ordvis Bauhof stellte deshalb Token mit dem Geheimnis, dem Aussteller und dem Empfänger der Plattform aus.

Achtung: Auf einem gemeinsamen Server ist das eine offene Tür. Beide Installationen hätten dasselbe Geheimnis — ein Token der Ordvis Plattform öffnete den Bauhof-Fachdienst und umgekehrt. Genau die Grenze, die `ENT-11` zieht, wäre an der Anmeldung nicht vorhanden.

Und es fällt **nicht** auf: Der Dienst startet, die Anmeldung funktioniert, und die Prüfung auf ein fehlendes Geheimnis ist zufrieden — die Nachbarvariable hat es ja gefüllt.

Die Abhilfe ist eng gefasst. Der Fachdienst liest **nur den Abschnitt Identity** aus einer eigenen Sicht, die ausschließlich die `appsettings`-Dateien *dieser* Installation kennt. Alles andere bleibt normal konfigurierbar. Zusätzlich liest diese Sicht Umgebungsvariablen mit dem Präfix `ORDIVIS_BAUHOF_` (also `ORDIVIS_BAUHOF_Identity__Jwt__Secret`) — der Unterschied ist der Präfix und damit die **Absicht**: Wer ihn schreibt, meint dieses Produkt.

⚠ Findet der Dienst beim Start unpräfixierte `Identity__Jwt__*`-Variablen, **warnt er im Betriebsprotokoll und startet trotzdem**. Die Variablen gehören dem Nachbarn; ein Bauhof-Dienst, der ihretwegen nicht startet, zwingt zu einer Änderung, die die Ordvis Plattform stilllegt.

5 Das Datenmodell in Stichworten

Ordvis Bauhof führt zwei Bestände nebeneinander, die sich ein Muster teilen, aber nichts voneinander wissen müssen:

Bestand	Was darin liegt	Klassen
Anlagen	Betriebsmittel des Bauhofs	Fahrzeug, Anbaugerät, Maschine, Kleingerät
Kataster	Ausstattung im öffentlichen Raum	Straßenausstattung nach Objektklassen

Dazu die Bewegungsdaten: Prüffristen und Prüfprotokolle, Ablesungen, Montagen, Schäden und Werkstattaufträge, Lagerartikel und Buchungen, Kontrollgänge und Mängel, Anordnungen und Vollzugsmeldungen, Winterdienstprotokolle und Einsätze, Ausleihen, Befähigungen.

5.1 ⚠ Das Schema entsteht aus dem Modell — die wichtigste Grenze des Alphastands

Der Fachdienst legt sein Schema beim Start mit `EnsureCreated` an. Das ist für einen ersten Stand richtig und für ein Kundenprodukt falsch:

Achtung: `EnsureCreated` kann eine bestehende Datenbank nicht fortschreiben. Kommen im Modell Spalten oder Tabellen dazu, läuft der neue Fachdienst gegen ein Schema, das sie nicht hat. Er startet, meldet nichts — und der erste Zugriff scheitert zur Laufzeit mit `column does not exist`.

Für den Alphastand gibt es dafür zwei Wege, und beide stehen in OB-51:

1. `deploy\schema-abgleich.ps1` — **additiv**, lässt den Bestand stehen. Der Regelweg.

2. `deploy\setup.ps1 -DatenbankVerwerfen` — wirft den Bestand weg. Nur für Erprobung.

⚠ **Umbenennungen und Typänderungen kann auch der Abgleich nicht.** Dafür treten vor der ersten Installation in einer Kommune EF-Migrationen an diese Stelle (`PEX-18`).

6 Wo Daten liegen

Was	Wo
Fachdaten	PostgreSQL, Datenbank <code>ordivis_bauhof</code>
Belege und Bescheinigungen	in der Datenbank
Programm	<code>C:\Program Files\Ordivis Bauhof</code> (wählbar)
Konfiguration	<code>...\Ordivis Bauhof\api\appsettings.Production.json</code> und <code>...\portal\appsettings.Production.json</code>
Betriebsprotokoll	Windows-Ereignisanzeige und Konsolenausgabe des Dienstes
Eingang der Winterdienstprotokolle	wählbarer Ordner (<code>Postfach:Ordner</code>), mit Unterordnern <code>angenommen</code> und <code>abweisung</code>

★ **Die Postfachannahme löscht nie.** Angenommenes geht nach `angenommen`, Abgewiesenes nach `abweisung`. Wenn die Annahme selbst kaputt ist, ist die Datei dort das Einzige, was noch da ist.

7 Was dieser Stand nicht kann

Damit niemand die Architektur für mehr hält, als sie ist:

Fehlt	Auswirkung	Kommt mit
Mandantenfähigkeit	Eine Installation trägt genau einen Bauhof.	<code>ENT-11</code> — bewusst nicht vorgesehen
Rechtemodell mit Berechtigungen	Es gibt drei Rollen, keine Rechtematrix. Siehe OB-44.	<code>PEX-09</code>
OIDC / SAML / Active Directory	Anmeldung nur mit lokaler Kennung und Kennwort.	<code>PEX-09</code>
Zwei-Faktor-Anmeldung	—	<code>PEX-09</code>
Aktualisierungstoken	Ein Token gilt acht Stunden und wird nicht erneuert.	<code>PEX-09</code>
Anmeldesperre nach Fehlversuchen	Es gibt keine Zählung von Fehlversuchen.	<code>PEX-09</code>
HTTPS an den Diensten selbst	Die Dienste sprechen HTTP. Verschlüsselung gehört vor sie.	OB-50, Abschnitt 8

Fehlt	Auswirkung	Kommt mit
Datenbankmigrationen	Siehe 5.1.	PEX-18
E-Mail-Versand	Die Wachen melden ins Protokoll und verschicken nichts.	PEX-10

⚠ **Diese Liste ist Teil des Alphastands** und ändert sich mit ihm. Sie ist der Stand am Tag des Satzes dieses Handbuchs.

Verwandte Themen

- **OB-50 · Installation und Server** — dieselbe Architektur als Handgriffsfolge — vom leeren Server bis zur ersten Anmeldung
- **OB-52 · Konfigurationsreferenz** — jeder Wert in den appsettings-Dateien, sein Vorgabewert und seine Wirkung
- **OB-54 · Wachen, Protokoll und Störungsbilder** — die acht Wachen, das Betriebsprotokoll und die häufigsten Störungsbilder
- **OB-60 · Schnittstellen-Referenz** — die REST-Schnittstelle, über die Portal, Arbeitsplatz und App auf den Fachdienst gehen

Administrationshandbuch

OB-40 Administration Der laufende Betrieb im Überblick – Dienste, Kennzahlen, Aufgaben im Jahreslauf

Beschreibt Vorhandenes

Dieses Dokument ist der Einstieg für alle, die Ordvis Bauhof **betreiben**. Es beschreibt, was läuft, was zu tun ist und in welcher Reihenfolge — und verweist für die Einzelheiten auf die übrigen Dokumente dieses Bandes.

INHALT

1 Was Sie täglich, wöchentlich und jährlich tun

2 Die beiden Dienste

2.1 Anhalten und Starten

2.2 Was in den Diensten steckt

3 Die drei Auskünfte über den Zustand

3.1 Gesundheit

3.2 Fassung

3.3 Kennzahlen

4 Die Konfiguration in Kürze

5 Platzbedarf und Wachstum

6 Was ein Administrator im Programm selbst tut

7 Grenzen, die ein Administrator kennen muss

Verwandte Themen

1 Was Sie täglich, wöchentlich und jährlich tun

Takt	Aufgabe	Wo beschrieben
täglich	Betriebsprotokoll auf Befunde der Wachen ansehen	OB-54
täglich	Prüfen, ob die Datensicherung gelaufen ist	OB-51
wöchentlich	Gesundheitsprüfung und Fassungsstand beider Dienste vergleichen	Abschnitt 3
wöchentlich	Neue und gesperrte Benutzer durchsehen	OB-41
monatlich	Plattenplatz der Datenbank und des Postfachordners ansehen	Abschnitt 5
je Fassung	Aktualisierung einspielen: Schema zuerst, dann Programm	OB-51
jährlich	Wiederherstellung einmal wirklich proben	OB-51
jährlich	Stationsschlüssel und Fahrzeuggeräte durchsehen	OB-42

Achtung: Die Datensicherung richtet der Installer nicht ein. Ordvis Bauhof legt eine Datenbank an und füllt sie; für Sicherung und Wiederherstellung ist die Datenbankverwaltung der Kommune zuständig. Wer das übersieht, betreibt ein Nachweisverfahren ohne Nachweisschutz.

2 Die beiden Dienste

	Fachdienst	Webportal
Dienstname	Ordvis.Bauhof.API	Ordvis.Bauhof.Portal
Anzeigenname	Ordvis Bauhof — Fachdienst	Ordvis Bauhof — Webportal
Programm	...\api\Ordvis.Bauhof.Api.exe	...\portal\Ordvis.Bauhof.Web.exe
Port	5100 (nur lokal geöffnet)	5110 (Firewall: Domäne, Privat)
Start	automatisch	automatisch
Neustart nach Absturz	3× (5 s, 10 s, 30 s), dann Ruhe	dito

2.1 Anhalten und Starten

```
# Reihenfolge beim Anhalten: erst das Portal, dann der Fachdienst.
Stop-Service Ordvis.Bauhof.Portal
Stop-Service Ordvis.Bauhof.API

# Beim Starten umgekehrt.
Start-Service Ordvis.Bauhof.API
Start-Service Ordvis.Bauhof.Portal
```

★ Die Reihenfolge ist kein Zeremoniell. Startet das Portal vor dem Fachdienst, zeigen die ersten Seitenaufrufe Fehlermeldungen — die Anwender melden das als Störung, obwohl nach zwanzig Sekunden alles läuft.

⚠ Das Portal braucht beim Anhalten **rund vierzehn Sekunden**, bis der Prozess wirklich weg ist: Blazor Server räumt seine Verbindungen ab. `Stop-Service` kehrt vorher zurück. Wer sofort danach Dateien austauscht, scheitert an gehaltenen Dateien.

2.2 Was in den Diensten steckt

Der Fachdienst trägt **alles**: die Fachlogik, die Datenbankanbindung, die PDF-Erzeugung und **acht Wachen**. Das Portal ist eine reine Oberfläche und rechnet nichts.

Hinweis: **Wache** ⓘ ist ein **Hausbegriff von Ordvis** — kein Fachbegriff des Bauhofs und nirgends nachschlagbar. Gemeint ist ein Ablauf innerhalb des Fachdienstes, der einmal täglich zu fester Uhrzeit eine fachliche Frage prüft und seinen Befund ins Betriebsprotokoll schreibt. Das Wort steht wörtlich im Protokoll und im Konfigurationsabschnitt **Lueckenwache**, deshalb wird es hier verwendet. Vollständig erklärt in OB-01 (Abschnitt 4.5), aufgelistet in OB-54.

Daraus folgt eine nützliche Regel für die Störungssuche:

Merksatz: Fehlt eine **Zahl**, liegt es am Fachdienst. Fehlt eine **Seite**, liegt es am Portal.

3 Die drei Auskünfte über den Zustand

3.1 Gesundheit

```
GET http://localhost:5100/gesundheit
```

Antwortet **200** mit „bereit“ oder **503**. **Ohne Anmeldung erreichbar** — und das ist Absicht: Die Betriebsüberwachung fragt ihn im Takt ab, und der Installer wartet beim Einrichten darauf. Beides geschieht, bevor es einen Benutzer gibt. Er gibt keinen Datensatz, keinen Namen und keine Zahl preis.

3.2 Fassung

```
GET http://localhost:5100/api/version
```

Ebenfalls **ohne Anmeldung**, und zwar aus einem konkreten Grund: Die Statusleiste beider Oberflächen ruft ihn alle zwanzig Sekunden — **auch vor der Anmeldung**. Läuft ein Arbeitsplatz gegen einen Fachdienst anderer Fassung, ist genau das die Ursache der fehlschlagenden Anmeldung. Hinter der Anmeldung wäre das nicht zu sehen.

Wichtig: Nach jeder Teilaktualisierung diese beiden Fassungen vergleichen. Ein Portal, das gegen einen älteren Fachdienst läuft, ist der häufigste Fehler nach einem unvollständigen Update — und er sieht wie ein Anmeldeproblem aus.

3.3 Kennzahlen

```
GET http://localhost:5100/api/kennzahlen (Anmeldung erforderlich)
```

Dieselben Zahlen zeigt das Portal auf der **Übersicht**. Für die Betriebsüberwachung sind zwei davon Warnwerte:

Kennzahl	Wenn sie steigt
Überzogene Prüffristen	Rechtspflichten laufen aus — fachlich, nicht technisch. Siehe OB-22 (Verwaltungshandbuch).
Anlagen ohne erfasste Frist	Der Bestand ist unvollständig gepflegt. Ein Fahrzeug ohne Frist wird von keiner Wache gemeldet.

4 Die Konfiguration in Kürze

Zwei Dateien, beide im Installationsverzeichnis:

Datei	Was darin steht
<code>api\appsettings.Production.json</code>	Datenbank, Port, Anmeldegeheimnis, Postfach, Lückenwache
<code>portal\appsettings.Production.json</code>	Port, Adresse des Fachdienstes

Vollständige Beschreibung aller Werte: **OB-52**.

Achtung: Nach jeder Änderung an einer dieser Dateien muss der zugehörige Dienst **neu gestartet** werden. Die Dateien werden beim Start gelesen und danach nicht mehr (`reloadOnChange: false`) — eine Änderung ohne Neustart wirkt nicht, meldet das aber auch nicht.

5 Platzbedarf und Wachstum

Was wächst	Wodurch	Was tun
Datenbank	Belege, Bescheinigungen, Winterdienstprotokolle, Fahrtpunkte	Größe monatlich ansehen; Fahrtpunkte sind der größte Posten
Postfachordner	Eingehende Winterdienstprotokolle	angenommen regelmäßig archivieren — nicht löschen, solange die Aufbewahrungsfrist läuft
Ereignisprotokoll	Meldungen der Wachen	Windows-Vorgabe reicht; bei Bedarf Größe der Anwendungsprotokolle erhöhen

⚠ **Der Ordner `abweisung` ist ein Warnsignal, kein Ablagefach.** Was dort liegt, ist angekommen und **nicht** übernommen worden. Ein Ordner, der leise wächst, ist derselbe Verlust wie ein ausgefallener Eingang. Siehe OB-54.

6 Was ein Administrator im Programm selbst tut

Ordvis Bauhof hat **keine eigene Verwaltungsoberfläche** und ausdrücklich keinen Einstellungsbereich im Portal. Was administriert wird, geschieht an drei Stellen:

Aufgabe	Wo
Benutzer, Kennwörter, Rollen	Kommandozeile und Datenbank — siehe OB-41
Ausgabestationen und Ausweismarken	Portal, Seite Ausgabestation — siehe OB-42
Fahrzeuggeräte der Winterdienst-App	Portal, Seite Geräte der App — siehe OB-42
Prüfarten, Gerätetypen, Lagerorte, Artikel	Portal, Fachseiten — siehe Verwaltungshandbuch

★ **Das ist kein Versäumnis, sondern der Stand.** Ein vollständiges Rechte- und Benutzerverwaltungsmodul bringt die Ordvis Plattform mit (**PEX-09**); ein zweites, halbes Modell hier wäre die sichere Quelle für Abweichungen, die niemand bemerkt.

7 Grenzen, die ein Administrator kennen muss

Grenze	Auswirkung im Betrieb
Kein E-Mail-Versand	Alle Wachen melden ins Betriebsprotokoll. Wer nicht hineinsieht, erfährt nichts.
Keine Anmeldesperre nach Fehlversuchen	Kennwortraten wird nicht gebremst. Der Fachdienst gehört deshalb nicht ins offene Netz.
Kein Aktualisierungstoken	Nach acht Stunden ist neu anzumelden. Das trifft die Frühschicht am Nachmittag.
Kein HTTPS an den Diensten	TLS gehört davor. Siehe OB-50, Abschnitt 8.
EnsureCreated statt Migrationen	Eine neue Fassung ändert das Schema nicht von selbst. Siehe OB-51.
Eine Installation, ein Bauhof	Keine Mandantentrennung.

⚠ Diese Liste beschreibt den **Alphastand** und ändert sich mit ihm.

Verwandte Themen

- **OB-50 · Installation und Server** — die Erstinstallation, auf der dieser Betrieb aufsetzt
- **OB-51 · Aktualisierung, Sicherung, Wiederanlauf** — eine neue Fassung einspielen, sichern und wiederanlaufen
- **OB-52 · Konfigurationsreferenz** — jeder Konfigurationswert, sein Vorgabewert und seine Wirkung
- **OB-54 · Wachen, Protokoll und Störungsbilder** — die Wachen, das Betriebsprotokoll und die häufigsten Störungsbilder

Benutzer, Rollen und Zugang

OB-41 Zugang Anmeldung, Kennwörter, Rollen, Sperren – und was dieser Stand ausdrücklich nicht kann

Beschreibt Vorhandenes

Zugang ist das Erste, was eingerichtet wird, und das Letzte, worüber jemand nachdenkt. Am Tag der Installation legt die Systemadministration ein paar Kennungen an, verteilt Erstkennwörter und wendet sich den Fachfragen zu. Zwei Jahre später ist niemand mehr sicher, wer alles ein Konto hat, welches davon noch gebraucht wird und wessen Kennwort seit dem ersten Tag unverändert ist.

Dieses Kapitel beschreibt deshalb nicht nur, wie ein Benutzer angelegt wird, sondern auch, was dabei entsteht: eine Kennung, ein Kennworthash, eine Rolle und ein Token mit einer Laufzeit. Wer diese vier Dinge auseinanderhält, versteht die meisten Störungsbilder rund um die Anmeldung ohne weiteres Nachsehen.

Und es sagt in aller Deutlichkeit, was dieser Stand **nicht** kann. Ordavis Bauhof hat im Alphastand kein feingliedriges Rechtemodell; die Rolle steuert vier klar benannte Dinge und nicht den Zugang zu Fachseiten. Wer das für ein Versehen hält, richtet den Betrieb falsch ein.

INHALT

- 1 Wie die Anmeldung funktioniert
- 2 ★★ Der Fachdienst ist vorgabeweise geschlossen
 - 2.1 Die vier Wege, die ohne Anmeldung offenstehen
 - 2.2 Die zweite Hälfte der Regel
- 3 Die drei Rollen
- 4 Einen Benutzer anlegen
 - 4.1 Der Weg über die Datenbank
 - 4.2 Rolle ändern
- 5 Sperren statt löschen
- 6 Kennwort wechseln
 - 6.1 Fälliger Wechsel
- 7 Was die Anmeldung nach außen preisgibt — und was nicht
- 8 Das Anmeldegeheimnis
 - 8.1 Das Geheimnis wechseln
 - 8.2 ⚠️ Die Nachbarschaftswarnung
- 9 Was in den Token steht
- 10 Was dieser Stand nicht kann
- Verwandte Themen

1 Wie die Anmeldung funktioniert

Ordavis Bauhof hat eine **eigene Benutzerverwaltung** mit lokalen Kennungen und Kennwörtern. Sie ist bewusst schmal gehalten und als **Zwischenstufe** gebaut: Alles, was nach außen sichtbar ist, entspricht dem Verfahren der Ordavis Plattform, damit ein späterer Austausch des Ausstellers (**PEX-09**) Fleißarbeit bleibt und kein Umbau wird.

Verfahren	JSON Web Token als Bearer -Kopfzeile
Kennwortverfahren	Argon2 (Isopoh.Cryptography.Argon2 2.0.0) — wortgleich zur Ordvis Platform
Gültigkeit eines Tokens	480 Minuten (acht Stunden)
Erneuerung	keine. Es gibt keine Aktualisierungstoken.
Kürzestes Kennwort	12 Zeichen
Zeichenklassenregel	keine

★ **Zwölf Zeichen und keine Sonderzeichenpflicht.** Erzwungene Sonderzeichen erzeugen nachweislich **Sommer2026!** — Länge trägt mehr.

★ **Acht Stunden und nicht dreißig Minuten.** Es gibt hier keine Erneuerung; eine kurze Lebensdauer ohne Erneuerung hieße, den Vorarbeiter mitten in der Schicht abzumelden. Eine Schicht ist das fachliche Maß.

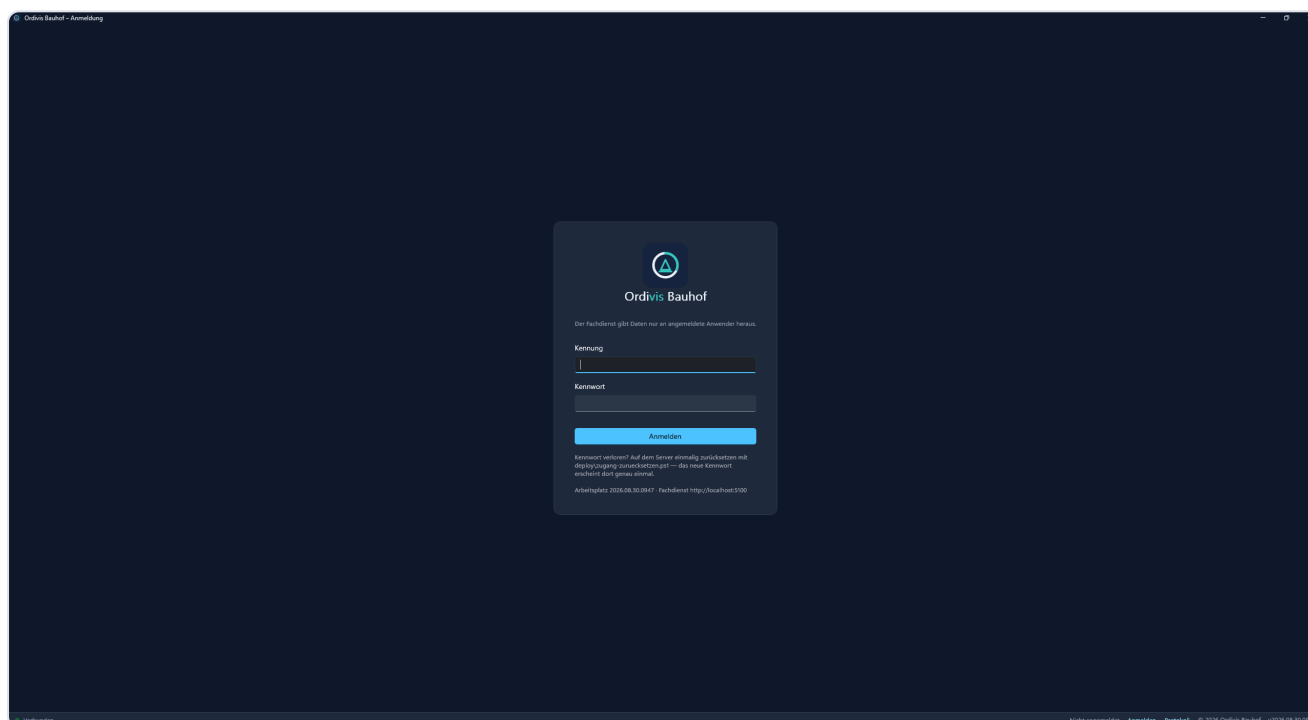


Abbildung 3 — Die Anmeldung des Arbeitsplatzes. Unten stehen zwei Angaben, die im Störfall die ersten sind, nach denen man fragt: die Fassung des Programms und die Adresse des Fachdienstes. Darüber der Weg zurück, wenn niemand mehr das Erstkennwort hat — er steht hier und nicht in einer Anleitung, weil genau an dieser Stelle danach gefragt wird.

2 ★ ★ ★ Der Fachdienst ist vorgabeweise geschlossen

Eine **Rückfallregel** verlangt an **jedem** Endpunkt einen angemeldeten Benutzer — auch an einem, der morgen dazukommt und an den niemand gedacht hat.

Merksatz: Der Unterschied zu „an jeden Endpunkt einen Vermerk schreiben“ ist die **Richtung des Vergessens**. Dort führt ein vergessener Vermerk zu einem offenen Endpunkt, hier zu einem geschlossenen. Nur die eine Richtung ist die harmlose.

2.1 Die vier Wege, die ohne Anmeldung offenstehen

Diese Liste ist vollständig, und ein Prüflauf hält sie gegen den Quelltext des Fachdienstes: Ein fünfter offener Weg ohne Begründung lässt die Prüfung fehlschlagen.

Weg	Warum offen
<code>/gesundheit</code>	Betriebsüberwachung und Installer fragen ihn, bevor es einen Benutzer gibt. Er gibt „bereit“ oder 503 zurück und sonst nichts.
<code>/api/version</code>	Die Statusleiste beider Oberflächen ruft ihn alle 20 Sekunden, auch vor der Anmeldung. Ein Fassungsunterschied ist genau die Ursache einer fehlschlagenden Anmeldung — hinter der Anmeldung wäre er nicht zu sehen.
<code>/api/anmeldung</code>	Die Anmeldung selbst. Ein Endpunkt, der eine Anmeldung verlangt, um sich anmelden zu können, ist eine Tür, die sich nur von innen öffnen lässt.
<code>/api/kiosk/anmeldung</code>	Die Anmeldung einer Ausgabestation . ⚠️ Offen heißt nicht ungeprüft: Der Aufruf verlangt einen Stationsschlüssel, der mit demselben Argon2-Verfahren geprüft wird wie ein Kennwort. Siehe OB-42.

2.2 Die zweite Hälfte der Regel

Ein Kiosktoken ist ein **gültiges** Token. Es erfüllt „angemeldet“ und käme damit überallhin — an die Zeitauswertung, an Personendaten, an die Aufträge. Ein Schlüssel, der an einem Gerät an der Lagertür klebt, wäre dann ein Generalschlüssel.

Deshalb weist die Rückfallregel jeden Aufruf zurück, der den Kioskanspruch trägt. Nur die beiden Kioskendpunkte verlangen ihn ausdrücklich.

3 Die drei Rollen

Rolle	Wert	Wer das ist	Was sie bedeutet
Mitarbeiter	0	Der Regelfall im Bauhof	Sieht die eigenen Daten.
Leitung	1	Einsatzleitung, Vorarbeiter	Sieht die eigene Kolonne.
Verwaltung	2	Betriebsleitung, Verwaltung	Darf auswerten.

Wichtig: Das ist keine Rechtematrix. Die Rolle wandert in das Anmeldetoken und wird heute für die **Auswertungssperre der Zeitauswertung** (ZEI-14) ausgewertet — und für nichts sonst. Ein Benutzer mit der Rolle *Mitarbeiter* kann alle übrigen Fachseiten aufrufen.

Warum das Feld trotzdem schon da ist: Ein Rollenfeld nachträglich einzuführen hieße, jedes ausgestellte Token ungültig zu machen.

⚠ **Was das für den Betrieb heißt:** Der Zugang zum Portal ist im Alphastand eine **Alles-oder-nichts-**Entscheidung. Wer eine Kennung bekommt, kann fachlich alles sehen. Die vollständige Rechtematrix und ihre Grenzen stehen in **OB-44**.

4 Einen Benutzer anlegen

Achtung: Im Alphastand gibt es **keine Oberfläche zur Benutzerverwaltung**. Benutzer werden über die Datenbank angelegt. Das ist eine bekannte Lücke und kein Versehen — sie schließt sich mit **PEX-09**.

4.1 Der Weg über die Datenbank

Der Kennwortprüfwert muss ein **Argon2-Wert im Format der Ordvis Platform** sein. Ein Klartextkennwort in dieser Spalte ergibt einen Benutzer, der sich nie anmelden kann — die Prüfung wirft bei einem undeutbaren Prüfwert und wird als „Kennwort falsch“ behandelt.

Der praktikable Weg im Alphastand hat zwei Schritte:

1. **Zeile anlegen** — mit einem beliebigen, undeutbaren Prüfwert:

```
INSERT INTO "Benutzer"
  ("Id", "Kennung", "Anzeigename", "Kennwortpruefwert", "Rolle",
   "Gesperrt", "KennwortwechselFaellig", "Angelegt")
VALUES
  (gen_random_uuid(), 'm.mueller', 'Martina Müller', '', 2,
   false, true, now());
```

2. **Kennwort setzen** — über den Rücksetzbefehl des Fachdienstes:

```
& "C:\Program Files\Ordvis Bauhof\api\Ordvis.Bauhof.Api.exe" zugang-zuruecksetzen
m.mueller
```

Der Befehl erzeugt ein Zufallskennwort, weist es **genau einmal** im Betriebsprotokoll aus und verlangt den Wechsel beim nächsten Anmelden.

⚠ **Die Kennung wird kleingeschrieben abgelegt.** **M.Mueller** und **m.mueller** sind derselbe Mensch. Tragen Sie sie klein ein — die Normalisierung im Programm greift beim Anmelden, nicht beim **INSERT**.

4.2 Rolle ändern

```
UPDATE "Benutzer" SET "Rolle" = 2 WHERE "Kennung" = 'm.mueller';
```

⚠ **Die Änderung wirkt erst beim nächsten Anmelden.** Die Rolle steht im Token, und das gilt bis zu acht Stunden.

5 Sperren statt löschen

```
UPDATE "Benutzer" SET "Gesperrt" = true WHERE "Kennung" = 'm.mueller';
```

Achtung: **Löschen Sie keinen Benutzer.** Seine Zeitbuchungen, Vermerke, Kontrollgänge und Vollzugsmeldungen bleiben — und müssen einen Namen behalten. Ein Nachweis, dem nachträglich der Urheber abhandenkommt, ist wertlos.

⚠ Eine Sperre wirkt **beim nächsten Anmelden**, nicht sofort: Ein bereits ausgestelltes Token bleibt bis zu acht Stunden gültig. Wer eine Sperre sofort durchsetzen muss, wechselt zusätzlich das Anmeldegeheimnis — das meldet allerdings **alle** ab.

6 Kennwort wechseln

Anwender wechseln ihr Kennwort in der Oberfläche. Der Fachdienst verlangt dabei **immer das bisherige Kennwort** — auch dann, wenn der Wechsel fällig ist.

★ Ein Token allein darf kein Kennwort setzen können. Sonst genügt ein liegengelassener, angemeldeter Bildschirm, um den Zugang zu übernehmen.

Abgewiesen wird ein neues Kennwort, wenn es

- kürzer als 12 Zeichen ist oder
- mit dem bisherigen übereinstimmt.

6.1 Fälliger Wechsel

Ein Benutzer mit `KennwortwechselFaellig = true` kann sich anmelden; die Anmeldung sagt den fälligen Wechsel mit.

★ Wer den Wechsel erzwingt, indem er die Anmeldung abweist, bekommt einen Benutzer, der nicht hineinkommt und nicht weiß, warum.

7 Was die Anmeldung nach außen preisgibt — und was nicht

Achtung: **Alle Fehlschläge nennen denselben Satz:** „Kennung oder Kennwort stimmen nicht.“ Unbekannte Kennung, falsches Kennwort und gesperrter Zugang sind von außen nicht zu unterscheiden. Wer hier „Benutzer unbekannt“ gegen „Kennwort falsch“ stellt, verrät jedem Fragenden, welche Kennungen es gibt.

Im **Betriebsprotokoll** steht der Unterschied — dort gehört er hin:

```
Anmeldung abgewiesen: Kennung m.mueller ist unbekannt.  
Anmeldung abgewiesen: falsches Kennwort für m.mueller.  
Anmeldung abgewiesen: m.mueller ist gesperrt.  
Anmeldung: m.mueller (Verwaltung).
```

★ ★ Auch bei unbekannter Kennung wird gerechnet. Ohne diesen Leerlauf antwortete eine unbekannte Kennung in Mikrosekunden und eine bekannte in rund 100 Millisekunden — der Unterschied ist messbar und zählt die Benutzerliste auf.

★ Die **Sperre** wird erst **nach** dem Kennwort geprüft. Sonst verriete ein anderer Antwortzeitpunkt, dass es die Kennung gibt.

8 Das Anmeldegeheimnis

Wo	<code>api\appsettings.Production.json</code> , Abschnitt <code>Identity:Jwt:Secret</code>
Woher	vom Installer erzeugt, 48 Byte aus dem kryptographischen Zufallsgenerator, Base64
Mindestlänge	32 Byte (256 Bit) — HMAC-SHA256 verlangt das
Bei Aktualisierung	wird übernommen , nicht neu erzeugt

Achtung: Ohne Geheimnis startet der Fachdienst nicht. Das ist Absicht: Ein Dienst, der ohne Geheimnis hochfährt, nimmt Anmeldungen entgegen und stellt Token aus, die jeder selbst ausstellen kann.

Die Länge wird **beim Start** geprüft. Ein zu kurzes Geheimnis ließe die Anmeldung sonst erst beim **ersten Ausstellen** scheitern — also nach der Installation und nicht beim Start.

8.1 Das Geheimnis wechseln

```
Stop-Service Ordvis.Bauhof.API  
# Identity:Jwt:Secret in api\appsettings.Production.json ersetzen (mind. 32 Byte, Base64)  
Start-Service Ordvis.Bauhof.API
```

⚠ Damit sind alle angemeldeten Anwender abgemeldet — sofort und ohne Meldung. Tun Sie das außerhalb der Arbeitszeit, oder wenn ein Zugang zu sperren ist und acht Stunden zu lange sind.

8.2 ⚠ ⚠ Die Nachbarschaftswarnung

Findet der Fachdienst beim Start maschinenweite Umgebungsvariablen `Identity__Jwt__Secret`, `__Issuer` oder `__Audience`, warnt er im Betriebsprotokoll:

```
BET-14/BET-13 – Im Umfeld dieses Dienstes stehen Anmeldevariablen einer ANDEREN  
Ordvis-Installation: ... Ordvis Bauhof ignoriert sie und liest seine Anmeldeeinstellungen  
ausschliesslich aus den appsettings-Dateien dieser Installation.
```

Er ignoriert sie und startet. Warum keine Abbruchmeldung: Die Variablen gehören der Ordvis Plattform — ein Bauhof-Dienst, der ihretwegen nicht startet, zwingt zu einer Änderung, die den Nachbarn stilllegt.

Zu prüfen bleibt trotzdem, ob dort ein maschinenweites Geheimnis liegt. Es muss je Installation verschieden sein. Hintergrund in OB-02, Abschnitt 4.1.

9 Was in den Token steht

Anspruch	Inhalt	Anmerkung
<code>sub</code>	Kennung des Benutzers (GUID)	
<code>email</code>	die Anmeldekennung	⚠ nicht zwingend eine Adresse — der Bauhof meldet sich mit <code>m.mueller</code> an. Der Anspruch heißt trotzdem <code>email</code> , weil die Ordvis Plattform ihn so liest.
<code>name</code>	Anzeigename	
<code>tenant_id</code>	leer (00000000-...)	Der Fachdienst ist nicht mandantenfähig. Der Anspruch ist da, weil die Plattform ihn erwartet, und leer, weil hier alles andere gelogen wäre.
<code>jti</code>	Kennung des Tokens	
<code>rolle</code>	0, 1 oder 2	für die Auswertungssperre
<code>kiosk</code>	Name der Station	nur in Stationstoken, siehe OB-42

⚠ **Keine Kulanz auf der Uhr.** Die Prüfung läuft mit `clockSkew = 0`. Die übliche Vorgabe von fünf Minuten hieße, dass ein abgelaufenes Token noch fünf Minuten trägt — bei einer Sperre ist das die falsche Richtung. **Die Uhren von Server und Arbeitsplatz müssen stimmen.**

10 Was dieser Stand nicht kann

Fehlt	Folge im Betrieb	Kommt mit
Rechtemodell mit Berechtigungen	Wer eine Kennung hat, sieht fachlich alles.	<code>PEX-09</code>
Active Directory, OIDC, SAML	Jede Kennung wird hier gepflegt.	<code>PEX-09</code>
Zwei-Faktor-Anmeldung	—	<code>PEX-09</code>
Aktualisierungstoken	Abmeldung nach acht Stunden.	<code>PEX-09</code>
Anmeldesperre nach Fehlversuchen	Kennwortraten wird nicht gebremst. Der Fachdienst gehört deshalb nicht ins offene Netz.	<code>PEX-09</code>
Anmeldehistorie	Nur <code>LetzteAnmeldung</code> je Benutzer; der Verlauf steht im Betriebsprotokoll.	<code>PEX-09</code>

Fehlt	Folge im Betrieb	Kommt mit
Oberfläche für die Benutzerverwaltung	Anlegen und Sperren über die Datenbank.	PEX-09
Mandantenfähigkeit	Eine Installation, ein Bauhof.	ENT-11 — bewusst nicht vorgesehen

Merksatz: Was hier steht, ist **ein Schloss an der Tür** — nicht mehr, und genau das war der offene Punkt. Bis zum 26.08.2026 enthielt der Fachdienst keine einzige Zeile zum Thema Anmeldung: Jeder Aufruf gegen Port 5100 wurde ausgeführt, von jedem, der den Rechner erreichte.

Verwandte Themen

- **OB-44 · Rollen- und Rechtematrix** — was die drei Rollen tatsächlich bewirken, und was sie ausdrücklich nicht bewirken
- **OB-42 · Ausgabestationen und Fahrzeuggeräte** — Geräte, die sich anmelden: Ausgabestationen und Fahrzeuggeräte
- **OB-14 · Das Portal — Anmeldung und Aufbau** (Verwaltungshandbuch) — wie sich die Anmeldung dem Anwender im Portal darstellt
- **OB-32 · Datenschutz** (Verwaltungshandbuch) — welche personenbezogenen Daten am Benutzerkonto hängen

Ausgabestationen und Fahrzeuggeräte

OB-42 Geräte Geräte, die sich anmelden – Ausgabestationen an der Lagertür und Fahrzeuggeräte der Winterdienst-App

Beschreibt Vorhandenes

Zwei Arten von **Geräten** haben in Ordvis Bauhof einen eigenen Zugang: die **Ausgabestation** an der Lagertür und das **Fahrzeuggerät**, auf dem die Winterdienst-App läuft. Beide werden vom Administrator eingerichtet, und bei beiden hängt am Verfahren mehr, als es zunächst aussieht.

INHALT

1 Die Ausgabestation an der Lagertür

- 1.1 Warum es sie gibt
- 1.2 ★★ Die Unterscheidung, auf der alles ruht
- 1.3 Eine Station einrichten
- 1.4 Ausweismarken pflegen
- 1.5 Eine Station stilllegen
- 1.6 Was der Administrator im Auge behält

2 Fahrzeuggeräte der Winterdienst-App

- 2.1 Das Problem, das die Geräteleiste löst
- 2.2 Ein Gerät anmelden
- 2.3 ★★ Was die Anmeldung rückwirkend tut
- 2.4 Die vier Befunde am Eingang
- 2.5 Ein Gerät stilllegen
- 2.6 Die Geräteübersicht
- 2.7 Aufbewahrung

3 Die Verteilung der Außendienst-App

Verwandte Themen

1 Die Ausgabestation an der Lagertür

1.1 Warum es sie gibt

★★ Eine Ausgabe, die einen Lagerverwalter voraussetzt, findet außerhalb dessen Dienstzeit nicht statt — und damit ist der Bestand falsch, sobald jemand Überstunden macht. Um 6:30 Uhr tippt niemand mit Arbeitshandschuhen ein Kennwort.

Die Station ist die Antwort darauf: ein Bildschirm an der Lagertür, an dem Werkzeug ohne Anmeldung ausgegeben und zurückgenommen wird.

1.2 ★★ Die Unterscheidung, auf der alles ruht

Die Station meldet sich an	mit einem eigenen Stationsschlüssel . Das ist eine echte Anmeldung, nur von einem Gerät und nicht von einem Menschen.
-----------------------------------	--

Der Mensch weist sich aus	mit einer Marke , einem Ausweis, einer Nummer. Das ist <i>Identifikation</i> und keine <i>Authentifizierung</i> : Eine Marke kann verliehen, verloren und nachgemacht werden.
---------------------------	--

Merksatz: Der Kiosk ist ein Erfassungsweg und kein Anmeldeweg. Er hält fest, wer *sagt*, dass er etwas mitnimmt — und das ist erheblich mehr als nichts. Nichts ist genau das, was man bekommt, wenn es die Station nicht gibt.

⚠️ ⚠️ **Daraus folgt die härteste Regel:** Ein Stationsschlüssel darf **ausschließlich** Werkzeug ausgeben und zurücknehmen. Ein Kiosktoken, mit dem sich die Zeitauswertung lesen ließe, wäre ein Kennwort, das an der Wand klebt. Technisch durchgesetzt wird das über den Anspruch **kiosk** — siehe OB-41, Abschnitt 2.2.

1.3 Eine Station einrichten

Im Portal unter **Ausgabestation** (**/kiosk**). Sie brauchen:

Angabe	Regel
Name	Pflicht. Er steht später in jeder Buchung — wählen Sie ihn so, dass man die Tür daran erkennt („Lagerhalle Nord“).
Standort	freiwillig
Stationsschlüssel	mindestens 16 Zeichen

Achtung: Der Stationsschlüssel wird einmal vergeben und dann jahrelang nicht gewechselt. Ein kurzer Schlüssel ist hier schlimmer als bei einem Kennwort, nicht besser. Sechzehn Zeichen sind die untere Grenze, nicht die Empfehlung.

Der Schlüssel wird mit **demselden Argon2-Verfahren** abgelegt wie ein Benutzerkennwort — nicht als einfacher Vergleichswert. Ein Stationsschlüssel ist ein Geheimnis, auch wenn er an einem Gerät klebt.

⚠️ **Notieren Sie den Schlüssel beim Anlegen.** Er lässt sich später nicht auslesen; es gibt nur den Weg über einen neuen.

1.4 Ausweismarken pflegen

Eine Marke löst eine Nummer in einen Namen auf, damit an der Station ein Mensch und nicht eine Ziffernfolge auf dem Bildschirm steht.

Wichtig: Eine Marke ist kein Konto. Sie hat kein Kennwort, keine Rolle und keinen Zugang zum Fachdienst.

⚠️ ⚠️ **Eine unbekannte Marke wird nicht abgewiesen.** Sie wird als Nummer festgehalten, und die Übersicht zählt sie. Wer die Ausgabe verweigert, weil eine Marke noch nicht eingetragen ist, hat um 6:30 Uhr keinen sauberen Bestand, sondern ein Gerät, das **ohne jeden Eintrag** mitgeht — genau der Zustand, den die Station beseitigen soll.

★ Für den Administrator heißt das: **Die Liste der unbekannten Marken ist eine Arbeitsliste.** Sie regelmäßig durchzugehen und die Marken nachzutragen ist Pflege, nicht Fehlerbehebung.

1.5 Eine Station stilllegen

Achtung: Stillgelegt, nicht gelöscht. Eine Station, die aus dem Bestand verschwindet, nimmt die Frage mit, wer im letzten Winter an der Lagertür gebucht hat.

Eine stillgelegte Station kann sich nicht mehr anmelden; ihre bisherigen Buchungen bleiben mit ihrem Namen stehen.

1.6 Was der Administrator im Auge behält

Was	Warum
LetzteVerwendung je Station	Eine Station, die seit Wochen nichts gebucht hat, ist entweder abgeschaltet oder wird umgangen. Beides gehört geklärt.
Anteil unbekannter Marken	Steigt er, fehlen Einträge — der Bestand wird ungenauer, ohne dass etwas ausfällt.
Offene Ausleihen	Werkzeug, das nie zurückgebucht wurde. Siehe OB-28 (Verwaltungshandbuch).

2 Fahrzeuggeräte der Winterdienst-App

2.1 Das Problem, das die Geräteliste löst

Die Winterdienst-App **signiert** ihre Protokolle; der private Schlüssel liegt im Sicherheitselement des Telefons. Damit ist die eine Hälfte der Frage beantwortet:

Merksatz: Eine gültige Signatur sagt, dass die Datei **unverändert** ist — nicht, **von wem** sie stammt.

Die zweite Hälfte beantwortet die **Geräteliste**: Ein öffentlicher Schlüssel wird **angemeldet**, und erst danach gilt ein damit signiertes Protokoll als von einem bekannten Gerät stammend.

⚠ ⚠ Ein Schlüssel wird **angemeldet** und **nie** beim ersten Protokoll **übernommen**. Eine Liste, die sich selbst füllt, beantwortet „*von wem stammt die Datei*“ mit „*von dem, der sie geschickt hat*“.

2.2 Ein Gerät anmelden

Im Portal unter **Geräte der App** (`/protokollgeraete`). Anzugeben sind der öffentliche Schlüssel des Geräts sowie Fahrzeug und Bezeichnung, damit später erkennbar ist, welches Gerät gemeint ist.

Wer ein Gerät anmeldet, steht mit seinem Namen daran — der Fachdienst nimmt den Anzeigenamen aus dem Anmeldetoken.

2.3 ★ ★ ★ Was die Anmeldung rückwirkend tut

Protokolle, die als „Gerät unbekannt“ eingegangen sind, werden nach der Anmeldung des Schlüssels auf „unverändert“ gehoben.

Achtung: Nur dieser eine Übergang. Eine verfälschte Datei bleibt verfälscht, und eine ohne Signatur bekommt keine. Die Anmeldung eines Geräts ändert nichts an dem, was damals ankam.

2.4 Die vier Befunde am Eingang

Befund	Bedeutung	Wird das Protokoll angenommen?
unverändert	Signatur gültig, Gerät bekannt	ja
Gerät unbekannt	Signatur gültig, Schlüssel nicht angemeldet	ja, mit Vermerk
ohne Signatur	keine Begleitdatei vorhanden	ja, mit Vermerk
verfälscht	Signatur passt nicht zur Datei	ja, mit Vermerk

★ ★ Die Prüfung verhindert nichts. Ein abgewiesenes Protokoll ist kein Nachweis, und die Lücke im Bestand wäre schlimmer als eine Zeile mit dem Vermerk „ohne Signatur“. Der Befund steht am Protokoll und ist auswertbar; entschieden wird von einem Menschen.

2.5 Ein Gerät stilllegen

Verlangt einen Grund von mindestens fünf Zeichen.

★ Ein stillgelegtes Gerät ohne Begründung ist von einem Versehen nicht zu unterscheiden — und wird beim nächsten Zweifel wieder angemeldet.

Achtung: Ein stillgelegtes Gerät bleibt bekannt. An seinem Schlüssel hängen Protokolle, und ein Nachweis, dem nachträglich der Absender abhandenkommt, ist wertlos. Die Stilllegung wirkt **nach vorn**, nicht rückwärts.

2.6 Die Geräteübersicht

Die Seite zeigt je Gerät, wie viele Protokolle eingegangen sind und wie viele davon welchen Befund tragen. Zwei Zahlen sind für den Administrator die wichtigen:

Zahl	Was sie bedeutet
Protokolle mit Gerät unbekannt	Ein Schlüssel ist nicht angemeldet. Nachholen — die Protokolle werden dann rückwirkend gehoben.
Protokolle ohne Signatur	Auf dem Gerät läuft eine App-Fassung, die nicht signiert, oder die Begleitdatei geht auf dem Postweg verloren. Beides gehört geklärt.

2.7 Aufbewahrung

```
GET /api/winterdienst/aufbewahrung?stichtag=...
```

Die Auskunft nennt, **was löschreif wäre** — und mehr sagt sie nicht.

Achtung: Es wird nichts von selbst gelöscht, und es gibt bewusst keinen Löschweg. Ein Winterdienstprotokoll ist ein Entlastungsbeweis; eine Frist, die von selbst zuschlägt, trifft irgendwann genau das Protokoll, um das gerade gestritten wird.

3 Die Verteilung der Außendienst-App

Verteilt wird über die **Geräteverwaltung der Kommune**, nicht über den Play Store.

Achtung: Die **Signatur des App-Pakets ist eine unveränderliche Größe**. Android ersetzt eine App nur durch eine, die mit **demselben Schlüssel** signiert ist. Geht die erste Verteilung mit dem falschen Schlüssel hinaus und kommt später eine richtig signierte, verweigert Android das Update — jedes Gerät muss dann deinstalliert und neu installiert werden. Dabei geht der App-Ordner verloren, und in ihm liegen die noch nicht übertragenen Aufnahmen.

⚠ Klären Sie **vor** der ersten Verteilung mit dem Hersteller, mit welchem Schlüssel das Paket signiert ist. Ein debug-signiertes Paket installiert sich, läuft und sieht in jeder Hinsicht richtig aus — der Fehler zeigt sich erst beim ersten Update.

⚠ Die zweite unveränderliche Größe ist die **Anwendungskennung** des Pakets. Auch sie lässt sich nach der ersten Verteilung nicht mehr ändern, ohne jedes Gerät anzufassen.

Verwandte Themen

- **OB-41 · Benutzer, Rollen und Zugang** — Anmeldung und Token der Personen — das Gegenstück zum Gerätetoken
- **OB-44 · Rollen- und Rechtematrix** — die Kiosksperre: was ein Stationstoken darf und was nicht
- **OB-28 · Werkzeug- und Materialausgabe** (Verwaltungshandbuch) — die Ausgabe an der Lagertür aus Sicht des Anwenders
- **OB-26 · Winterdienst** (Verwaltungshandbuch) — der Winterdienst, dessen Protokoll das Fahrzeuggerät aufzeichnet

Rollen- und Rechtematrix

OB-44 Rechtematrix Was die drei Rollen wirklich bewirken – und die vier Sperren, die es tatsächlich gibt

Beschreibt Vorhandenes

Eine Rechtematrix beantwortet üblicherweise die Frage, wer welche Maske öffnen darf. Dieses Dokument beantwortet sie auch — die Antwort fällt nur kürzer aus, als jeder erwartet, der schon einmal eine solche Matrix gelesen hat.

Das ist der Grund, aus dem dieses Kapitel überhaupt eigenständig ist. Ein Handbuch, das an dieser Stelle schweigt, wird als Zusage gelesen: Man unterstellt ein Rechtemodell, weil jedes andere Fachverfahren eines hat, richtet den Betrieb entsprechend ein und merkt erst in der Revision, dass die angenommene Trennwand nie existiert hat.

Dieses Dokument sagt deshalb zuerst, was die drei Rollen **nicht** tun, dann die vier Wirkungen, die sie tatsächlich haben, und schließlich die vier Sperren, die es wirklich gibt — sie hängen nämlich gar nicht an Rollen, sondern an Sachverhalten. Das ist die belastbarere Konstruktion, und es ist auch die, die man kennen muss.

INHALT

- 1 ⚠️ ⚠️ Lesen Sie zuerst das hier
- 2 Die drei Rollen
- 3 Was die Rolle tatsächlich bewirkt
 - 3.1 ★★ ★ Melden darf jeder
 - 3.2 ★★ ★ Recht und Filter sind nicht dasselbe
 - 3.3 ⚠️ Auch die eigene bestätigte Buchung nicht
- 4 Die vier Sperren, die es wirklich gibt
 - 4.1 Die Auswertungssperre nach Person
 - 4.2 Die Kiosksperre
 - 4.3 Die Betriebssperre bei abgelaufener Frist
 - 4.4 Die Freigabesperre in der Werkstatt
- 5 Die Zugänge im Überblick
- 6 Was für eine Prüfung sonst noch wichtig ist
- 7 Empfehlung für den Betrieb im Alphastand
- Verwandte Themen

1 ⚠️ ⚠️ Lesen Sie zuerst das hier

Dieses Dokument heißt **Rechtematrix** und ist eine — nur eine sehr kurze. Der Grund gehört an den Anfang und nicht in eine Fußnote:

Achtung: Ordvis Bauhof hat im Alphastand kein Rechtemodell. Es gibt drei Rollen, und sie steuern vier klar benannte Dinge. Sie steuern **nicht**, welche Fachseiten und welche Endpunkte jemand aufrufen darf. Wer eine gültige Kennung hat, kommt fachlich überall hin.

Das ist kein Versehen, sondern eine bewusste Zwischenstufe: Ein zweites, halbes Rechtemodell neben dem der Ordavis Plattform (PEX-09) wäre die sichere Quelle für Abweichungen, die niemand bemerkt. Hintergrund in OB-41.

Für die Revision heißt das: Die Zugangsbeschränkung liegt im Alphastand **außerhalb** der Anwendung — bei der Vergabe von Kennungen und beim Netzzugang. Sie ist nicht innerhalb der Anwendung fein einstellbar.

2 Die drei Rollen

Rolle	Wert	Wer
Mitarbeiter	0	Der Regelfall im Bauhof — sieht die eigenen Daten
Leitung	1	Einsatzleitung, Vorarbeiter — sehen ihre Kolonne
Verwaltung	2	Betriebsleitung und Verwaltung — dürfen auswerten

Die Rolle steht in der Datenbank am Benutzer und wandert beim Anmelden als Anspruch **rolle** ins Token.

⚠ Eine Rollenänderung wirkt erst beim nächsten Anmelden — das Token gilt bis zu acht Stunden.

3 Was die Rolle tatsächlich bewirkt

Nr.	Wirkung	Wo	Mitarbeiter	Leitung	Verwaltung
1	Kontrollgangeliste in der Außendienst-App sehen	App	nur eigene zugewiesene	alle	alle
2	Auftragsliste in der Außendienst-App sehen	App	nur eigene zugewiesene	alle	alle
3	Bestätigte Zeitbuchung korrigieren	Zeiterfassung	nein — auch nicht die eigene	ja, protokolliert	ja, protokolliert
4	Anzeige der Rolle in der Oberfläche	Portal, Arbeitsplatz	ja	ja	ja

Und das ist die vollständige Liste.

3.1 ★★ ★ Melden darf jeder

Ein **Mangel** kann von jeder Rolle gemeldet werden, und das mit Absicht: Ein Mangel, den jemand sieht und nicht melden kann, weil seine Rolle es nicht vorsieht, wird nicht gemeldet — und die Mängel, die niemand meldet, sind die, die man später sucht.

3.2 ★ ★ ★ Recht und Filter sind nicht dasselbe

Merksatz: Was jemand nicht darf, wird nicht gezeigt. Was ihm nicht zugewiesen wurde, wird gezählt.

Der Mitarbeiter sieht in der App **seine** Kontrollgänge — die übrigen sind nicht *verboten*, sondern *nicht seine*. Deshalb sieht er auch, **dass es andere gibt**. Der Unterschied wird ständig verwechselt, und die Verwechslung erzeugt entweder eine Sperre, die wie ein Fehler aussieht, oder eine Liste, in der man das Eigene nicht findet.

3.3 ⚠ Auch die eigene bestätigte Buchung nicht

Ein Mitarbeiter darf seine **bestätigte** Zeitbuchung nicht korrigieren.

★ Wer den eigenen Tag nach der Bestätigung still nachbessern darf, hat mit der Bestätigung nichts bestätigt — sie kostet dann einen Griff und sagt nichts aus. Eine **unbestätigte** Buchung darf jeder ändern; dabei entsteht kein Korrektur eintrag, weil sie geändert und nicht korrigiert wird.

4 Die vier Sperren, die es wirklich gibt

Die eigentlichen Schutzwirkungen in Ordvis Bauhof hängen **nicht** an Rollen. Sie hängen an Sachverhalten — und das ist die belastbarere Konstruktion.

4.1 Die Auswertungssperre nach Person

```
GET /api/zeit/person/{person}
```

Antwortet **403**, wenn keine der beiden Bedingungen erfüllt ist:

Zulässiger Grund	Bedingung
Selbstauskunft	Der Abrufer fragt nach sich selbst.
Freigabe	Es liegt eine Auswertungsfreigabe vor, die diese Person und den heutigen Tag trägt.

Achtung: Jeder Abruf steht im Protokoll — auch der abgewiesene. Das ist der eigentliche Schutz: nicht die Sperre allein, sondern ihre Nachvollziehbarkeit.

★ **403 und nicht 404.** Der Weg existiert, und die Person auch. Ein 404 wäre eine Notlüge und wäre durchschaubar — die Sperre soll erklärt werden, nicht versteckt.

Eine **Freigabe** braucht Anlass, **zwei Namen** und einen Zeitraum. Mehr dazu in OB-33 (Verwaltungshandbuch).

★ Die **zusammengefasste** Auswertung (`/api/zeit/auswertung`) ist für jeden Angemeldeten zugänglich: Sie enthält keine personenbezogene Aussage — dafür sorgt die Mindestbesetzung.

4.2 Die Kiosksperre

Ein Stationstoken trägt den Anspruch `kiosk`. Die Rückfallregel des Fachdienstes **weist jeden Aufruf zurück**, der diesen Anspruch trägt; nur die beiden Kioskendpunkte verlangen ihn ausdrücklich.

Weg	Stationstoken	Benutzertoken
POST <code>/api/kiosk/ausgabe</code>	ja	nein
POST <code>/api/kiosk/rueckgabe</code>	ja	nein
alles andere	nein	ja

Damit öffnet der Schlüssel an der Lagertür genau zwei Türen und nicht das Haus.

4.3 Die Betriebssperre bei abgelaufener Frist

Ein Betriebsmittel mit **überzogener** Prüffrist ist gesperrt. Das ist keine Berechtigungsfrage, sondern eine Sachlage — und sie gilt für jede Rolle gleich.

Aufgehoben wird sie nur durch eine **befristete Übersteuerung** mit Begründung, und die steht danach in der Akte. Mehr dazu in OB-22 (Verwaltungshandbuch).

4.4 Die Freigabesperre in der Werkstatt

Ein Fahrzeug wird aus der Werkstatt nur freigegeben, wenn ein **Beleg** vorliegt **und** kein weiterer Schaden mehr sperrt. Auch das ist eine Sachlage und keine Rolle. Mehr dazu in OB-25 (Verwaltungshandbuch).

5 Die Zugänge im Überblick

Zugangsart	Was sie öffnet	Wie sie sich ausweist
Benutzerkennung	alle Fachwege des Portals und des Arbeitsplatzes	Kennung + Kennwort (Argon2), Token 8 h
Stationsschlüssel	ausschließlich Ausgabe und Rücknahme von Werkzeug	Stationsname + Schlüssel (Argon2), Token 8 h, Anspruch <code>kiosk</code>
Ausweismarke	nichts — sie ist kein Zugang	eine Nummer. Identifikation, keine Authentifizierung.
Gerätesignatur	nichts — sie ist kein Zugang	öffentlicher Schlüssel, angemeldet. Sie beantwortet die Herkunft eines Protokolls.

6 Was für eine Prüfung sonst noch wichtig ist

Frage der Revision	Antwort im Alphastand
Werden Zugriffe protokolliert?	Teilweise. Anmeldungen, personenscharfe Zeitabrufe, Eskalationen, Beschaffungsvorgänge und Auswertungsfreigaben stehen im Protokoll. Ein allgemeines Zugriffsprotokoll über alle Lesevorgänge gibt es nicht.
Gibt es eine Vier-Augen-Regel?	Ja, bei der Auswertungsfreigabe (zwei Namen). Sonst nicht.
Lassen sich Nachweise nachträglich ändern?	Vollzugsmeldungen und Prüfprotokolle werden abgeschlossen und tragen danach ihren Abschlusszeitpunkt. Korrekturen erzeugen Einträge. Winterdienstprotokolle liegen zusätzlich als Urschrift vor.
Kann jemand einen Nachweis rückdatieren?	Zeitpunkte kommen von der Serveruhr , nie aus einem Eingabefeld.
Wird etwas automatisch gelöscht?	Nein. Es gibt bewusst keinen automatischen Löschweg — auch nicht für abgelaufene Aufbewahrungsfristen.
Trennt das System Mandanten?	Nein. Eine Installation, ein Bauhof.

7 Empfehlung für den Betrieb im Alphastand

Solange es kein feines Rechtemodell gibt, liegt der Schutz außerhalb der Anwendung. Drei Maßnahmen tragen am meisten:

1. **Kennungen sparsam vergeben.** Wer eine hat, sieht fachlich alles.
2. **Den Fachdienst nicht ins offene Netz stellen.** Es gibt keine Anmeldesperre nach Fehlversuchen.
3. **Das Portal hinter TLS und, wenn möglich, hinter das Hausnetz legen.** Siehe OB-50, Abschnitt 8.

⚠ Und die Erwartung im Haus entsprechend setzen: Eine Zusage „nur die Werkstatt sieht die Werkstattdaten“ lässt sich im Alphastand **nicht** einlösen.

Verwandte Themen

- **OB-41 · Benutzer, Rollen und Zugang** — woher Kennung, Rolle und Token kommen und wie sie verwaltet werden
- **OB-32 · Datenschutz** (Verwaltungshandbuch) — die Verarbeitung, auf die sich die Auswertungssperre bezieht
- **OB-33 · Beschäftigtendatenschutz und Mitbestimmung** (Verwaltungshandbuch) — die Auswertungsfreigabe: Anlass, zwei Namen, Zeitraum

Installation und Server

0B-50 Installation Vom leeren Server bis zur ersten Anmeldung – Schritt für Schritt

Beschreibt Vorhandenes

Vor Ihnen steht ein leerer Server, und am Ende dieses Kapitels meldet sich jemand am Portal an. Dazwischen liegen eine Datenbank, ein Dienst, ein Webserver, ein Zertifikat und eine Handvoll Werte, die zueinander passen müssen.

Die Reihenfolge ist dabei nicht beliebig, und die Stellen, an denen eine Installation erfahrungsgemäß hängenbleibt, sind wenige und immer dieselben: die Rechte des Datenbankbenutzers, die Bindung des Dienstes an eine Adresse, das Zertifikat und die erste Anmeldung. Dieses Dokument führt der Reihe nach hindurch und sagt an jeder dieser Stellen, woran man erkennt, dass der Schritt wirklich gelungen ist.

★ **Geprüft wird am Erzeugnis und nicht am Rückgabewert.** Ein Dienst, der startet, ist kein Dienst, der antwortet; eine angelegte Datenbank ist kein nutzbares Schema. Jeder Abschnitt endet deshalb mit einer Probe, die man selbst ausführen kann.

INHALT

1 Bevor Sie beginnen

- 1.1 Was Sie brauchen
- 1.2 Die fünf Unterscheidungsmerkmale
- 1.3 Die Voraussetzungsliste im Setup

2 Der Probelauf zuerst

3 Die Installation

4 Was der Installer der Reihe nach tut

- Schritt 1 · Voraussetzungen
- Schritt 2 · Koexistenz mit der Ordvis Plattform
- Schritt 3 · Verbindung zum PostgreSQL-Server
- Schritt 4 · Datenbank und Rolle anlegen
- Schritt 5 · Dateien kopieren
- Schritt 6 · Konfiguration schreiben
- Schritt 7 · Dienste einrichten
- Schritt 8 · Firewall
- Schritt 9 · Prüfung

5 Der erste Zugang

- 5.1 Wenn das Erstkennwort verloren ist

6 Nach der Installation: die Aufräumarbeiten

7 Deinstallation

8 Verschlüsselung: drei Betriebsarten

- 8.1 Der Umkehrstellvertreter
- 8.2 Eigenes Zertifikat am Dienst
- 8.3 Der Ablauf ist eine Frist
- 8.4 ⚠ Zwei Ordvis-Produkte auf einem Server

9 Wenn es nicht läuft

Verwandte Themen

1 Bevor Sie beginnen

1.1 Was Sie brauchen

Ein Windows-Server 2022/2025 oder Windows 11	mit lokalen Administratorrechten
Einen vorhandenen PostgreSQL-Server	Ordvis Bauhof bringt keinen mit und richtet keinen ein
Ein Datenbankkonto mit CREATEROLE und CREATEDB	oder eine vorab angelegte Rolle und Datenbank
Den Verteilstand	Ordner dist mit den Unterordnern api , portal und — falls gewünscht — client
Windows PowerShell 5.1	gehört zu Windows — PowerShell 7 wird nicht gebraucht
psql im Suchpfad	kommt mit dem PostgreSQL-Server
Nur bei eigenem HTTPS: ein Zertifikat	im Windows-Speicher LocalMachine\My , als PFX oder als PEM-Paar — vor der Installation bereitgelegt

⚠️ ⚠️ **Befund vom Pilotserver Fuldata1, 01.09.2026 — und der Grund, warum die Zeile über PowerShell so ausdrücklich dasteht:** Hier stand einmal „PowerShell 7 oder neuer“. Das Setup ruft **setup.ps1** aber mit **powershell.exe** auf, und das ist **immer** Windows PowerShell 5.1. Das Skript verlangte 7 — und lief deshalb **gar nicht**. Zurück blieb eine Installation aus Dateien: keine Datenbank, keine Konfiguration, **keine Dienste** — und die Meldung „erfolgreich abgeschlossen“.

Seit dem 01.09.2026 kommt **setup.ps1** mit 5.1 aus. **PowerShell 7 nachzuinstallieren hilft nicht und ist nicht nötig.**

Wichtig: Der PostgreSQL-Server wird **geteilt**, die Datenbank **nicht**. Läuft auf dem Rechner bereits die Ordvis Plattform, nutzt Ordvis Bauhof denselben Datenbankserver — mit einer **eigenen** Datenbank und einer **eigenen** Rolle. Ein zweiter Datenbankserver kostete Arbeitsspeicher, eine zweite Sicherungstrecke und eine zweite Stelle, an der jemand ein Kennwort pflegen muss.

1.2 Die fünf Unterscheidungsmerkmale

Der Installer prüft, **bevor er etwas tut**, dass sich Ordvis Bauhof in fünf Dingen von einer vorhandenen Ordvis Plattform unterscheidet:

Dienstname · Port · Installationsverzeichnis · Datenbank · Datenbankrolle

⚠️ Und in einem sechsten, das nur der Installer setzen kann: der **Anwendungskennung** des Setups. Wäre sie geteilt, hielte Windows beide Produkte für dieselbe Anwendung — und eine Deinstallation von Ordvis Bauhof nähme die Ordvis Plattform mit.

1.3 Die Voraussetzungsliste im Setup

Bevor der Installer etwas kopiert, zeigt er eine **abgehakte Liste** dessen, was er geprüft hat:

```
[x] Administratorrechte
[x] Windows PowerShell 5.1      PowerShell 7 wird NICHT gebraucht
[x] Zielverzeichnis            kein Verzeichnis der Ordvis Platform
[x] Port 5100 (Fachdienst)      frei
[x] Port 5110 (Webportal)       frei
[x] PostgreSQL-Clientwerkzeug   D:\Program Files\PostgreSQL\18\bin\psql.exe
[x] Verbindung zum PostgreSQL-Server localhost:5432 als 'postgres'
[x] Rechte des Datenbankkontos  darf Rolle und Datenbank anlegen
[x] Datenbank 'ordvis_bauhof'   wird neu angelegt
```

Was fehlt, hält das Setup an. Das ist Absicht: Ein Setup, das trotz fehlender Voraussetzungen durchläuft, hinterlässt eine Installation, die es gar nicht gibt — und meldet Erfolg dafür. Genau das war der Befund vom 01.09.2026.

★ ★ **Reicht das Konto nicht, fragt das Setup nach einem anderen.** Der Regelfall auf einem Rechner mit der Ordvis Platform: Deren Anwendungsrolle `infradesk_app` darf **kein** `CREATEROLE` — und das ist richtig so, eine Anwendungsrolle soll das nicht können. Unter der Liste erscheinen dann vier Felder für ein Konto, das eine Datenbank anlegen darf (in aller Regel `postgres`). „Erneut prüfen“ prüft mit diesem Konto.

⚠ Das Kennwort wird **nicht gespeichert**. Es geht über eine Datei im Temp-Ordner an `setup.ps1` — nicht über die Befehlszeile, denn die ist auf dem Rechner für jeden Prozess sichtbar — und wird direkt nach dem Aufruf gelöscht.

★ **Und der Arbeitsplatz-Installer hat seine eigene Liste.** Er braucht keine Datenbank; er braucht einen Fachdienst, der unter der eingetragenen Adresse antwortet. Er prüft genau das und vergleicht die Fassungen. Der Grund: Steht dort eine falsche Adresse, **startet der Arbeitsplatz trotzdem** und zeigt leere Listen — und der Anwender meldet ein kaputtes Programm, während in Wahrheit ein Buchstabe fehlt.

Die stille Verteilung (`/SILENT` mit `/SERVER=`) sieht diese Seite nicht und wird von ihr auch nicht aufgehalten.

2 Der Probelauf zuerst

Empfehlung: Beginnen Sie **immer** mit dem Probelauf. Er prüft Voraussetzungen, Nachbarschaft, Datenbankverbindung und Rechte — und ändert nichts.

```
.\deploy\setup.ps1 -WhatIf
```

★ Die Abfrage steht an **jeder** schreibenden Stelle: Datenbank, Rolle, Dateien, Dienste, Firewall. Erfahrungswert vom 25.08.2026: Der Vermerk am Skriptkopf *sieht aus* wie eine Zusicherung für das ganze

Skript und ist keine.

3 Die Installation

```
.\deploy\setup.ps1
```

Ohne weitere Angaben installiert das Skript mit diesen Vorgaben:

Schalter	Vorgabe	Bedeutung
-InstallDir	C:\Program Files\Ordivis Bauhof	Zielverzeichnis
-ApiPort	5100	HTTP-Port des Fachdienstes
-PortalPort	5110	HTTP-Port des Webportals
-DbName	ordivis_bauhof	Name der neuen Datenbank
-DbUser	bauhof_app	Name der neuen Datenbankrolle
-DbPassword	(leer)	leer = wird zufällig erzeugt und in die Konfiguration geschrieben
-PgSuperConnection	(leer)	leer = die Serverangaben der vorhandenen Ordivis Platform werden übernommen
-PgSuperConnectionDatei	(leer)	dasselbe, aber aus einer Datei gelesen — ⚠️ so ruft das Setup an , denn in der Zeichenfolge steht ein Kennwort, und eine Befehlszeile ist auf dem Rechner für jeden Prozess sichtbar
-DistDir	<Skriptverzeichnis>\dist	Verzeichnis mit den fertigen Dateien
-Unattended	aus	keine Rückfragen
-DatenbankVerwerfen	aus	⚠️ verwirft die Datenbank und baut sie neu auf

Beispiel für eine gesteuerte Installation:

```
.\deploy\setup.ps1 `
  -InstallDir "D:\Program Files\Ordivis Bauhof" `
  -ApiPort 5100 -PortalPort 5110 `
  -DbName ordivis_bauhof -DbUser bauhof_app `
  -PgSuperConnection
"Host=localhost;Port=5432;Username=postgres;Password=...;Database=postgres" `
  -Unattended
```

Achtung: `-Unattended` allein genügt nicht, wenn das Skript aus einer nicht-interaktiven Sitzung heraus läuft (Inno-Setup, geplante Aufgabe, Fernwartung). Das Skript setzt deshalb zusätzlich `$ConfirmPreference` selbst zurück. Wer es aus eigenen Skripten aufruft, sollte den Schalter trotzdem immer mitgeben.

4 Was der Installer der Reihe nach tut

Schritt 1 · Voraussetzungen

Administratorrechte, PowerShell-Fassung, `psql`, Verteilstand.

★ Jeder Lauf schreibt ein Protokoll nach `%ProgramData%\Ordavis Bauhof\setup-protokolle`. Das gilt besonders für den unbeaufsichtigten Lauf aus dem Setup heraus: Der läuft unsichtbar, und ohne Protokoll bliebe von einem Fehlschlag nichts zurück, woran man ihn erkennen könnte. Schlägt die Einrichtung fehl, nennt das Setup diesen Pfad in der Fehlermeldung — zusammen mit dem Befehl, mit dem sich die Einrichtung **ohne Neuinstallation** wiederholen lässt.

Schritt 2 · Koexistenz mit der Ordavis Plattform

Die fünf Merkmale aus Abschnitt 1.2. Findet der Installer eine Ordavis Plattform, prüft er, dass Dienstnamen, Ports, Verzeichnis, Datenbank und Rolle sich unterscheiden — und **fasst deren Dienste nicht an**.

Unangetastet bleiben: `InfraDesk.API`, `InfraDesk.Portal`, `InfraDesk.PublishAgent`, `InfraDesk.Discovery.Collector`, `postgresql-ordavis`.

Schritt 3 · Verbindung zum PostgreSQL-Server

Ohne `-PgSuperConnection` liest der Installer die **maschinenweite** Umgebungsvariable `ConnectionStrings__InfraDesk` der vorhandenen Ordavis Plattform und übernimmt daraus **Host und Port** sowie das dortige Konto. Das Kennwort wird gelesen, aber nirgends ausgegeben und nirgends abgelegt.

Achtung: Die Anwendungsrolle der Ordavis Plattform reicht nicht. `infradesk_app` hat weder `CREATEROLE` noch `CREATEDB` — gutes Handwerk auf deren Seite, eine Anwendungsrolle soll das nicht können. Das Skript prüft die Rechte **vor dem ersten Schreibvorgang** und bricht mit einer verständlichen Meldung ab, statt eine halb angelegte Datenbank zu hinterlassen.

Abhilfe, wenn die Rechte fehlen — eine von beiden:

```
# (a) mit einem privilegierten Konto installieren
.\deploy\setup.ps1 -PgSuperConnection
"Host=localhost;Port=5432;Username=postgres;Password=..."
```

```
-- (b) Rolle und Datenbank vorab von der Datenbankverwaltung anlegen lassen
CREATE ROLE bauhof_app LOGIN PASSWORD '...';
CREATE DATABASE ordavis_bauhof OWNER bauhof_app;
```

und dann mit `-DbUser` / `-DbName` / `-DbPassword` übergeben.

Schritt 4 · Datenbank und Rolle anlegen

Legt Rolle und Datenbank an, sofern sie fehlen. Vorhandenes wird **nicht** überschrieben — es sei denn, `-DatenbankVerwerfen` ist gesetzt.

Achtung: `-DatenbankVerwerfen` **wirft den Bestand weg**. Ohne `-Unattended` fragt das Skript zur Bestätigung nach dem Datenbanknamen. Für eine Aktualisierung ist dieser Schalter **nicht** der Weg — dafür gibt es `schema-abgleich.ps1` (siehe OB-51).

Schritt 5 · Dateien kopieren

Die Dienste werden angehalten, die Zielverzeichnisse **geleert** und der Verteilstand kopiert.

★ Das Leeren ist Absicht: Ein bloßes Überschreiben lässt Dateien liegen, die es im neuen Stand nicht mehr gibt — und die werden weiter ausgeliefert. Das ist der Fehlertyp „*ich hab's geändert und es zeigt trotzdem das Alte*“.

Wichtig: Von Hand abgelegte Dateien im Programmverzeichnis überleben eine Aktualisierung **nicht**. Die Konfiguration ist davon nicht betroffen — sie wird in Schritt 6 neu geschrieben.

⚠ Angehalten wird auf das **Prozessende**, nicht auf die Meldung der Dienststeuerung. Beim Portal liegen dazwischen rund vierzehn Sekunden, in denen Blazor Server seine Verbindungen abräumt; ein Lösversuch in dieser Zeit scheitert reproduzierbar an `clrjit.dll`.

Schritt 6 · Konfiguration schreiben

Geschrieben werden `api\appsettings.Production.json` und `portal\appsettings.Production.json` mit Verbindungszeichenfolge, Ports und dem Anmeldegeheimnis.

Achtung: Das Anmeldegeheimnis wird je Installation erzeugt — 48 Byte aus dem kryptographischen Zufallsgenerator. Ein eingebautes Geheimnis wäre in jeder Installation dasselbe und beim ersten Kunden bekannt; jeder könnte sich damit für jede andere Installation ein gültiges Token ausstellen.

⚠ Bei einer Aktualisierung wird das vorhandene Geheimnis übernommen. Ein neues meldete jeden angemeldeten Anwender ab — mitten im Betrieb, ohne Grund und ohne Meldung.

Schritt 7 · Dienste einrichten

Dienst	Anzeigename	Programm
<code>Ordvis.Bauhof.API</code>	Ordvis Bauhof — Fachdienst	<code>...\api\Ordvis.Bauhof.Api.exe</code>
<code>Ordvis.Bauhof.Portal</code>	Ordvis Bauhof — Webportal	<code>...\portal\Ordvis.Bauhof.Web.exe</code>

Beide starten automatisch. Nach einem Absturz startet Windows sie **dreimal** neu (nach 5, 10 und 30 Sekunden) und lässt sie danach in Ruhe.

★ Kein endloser Neustart: Ein Dienst, der sich ununterbrochen neu startet, füllt das Ereignisprotokoll und verdeckt damit die Ursache.

Schritt 8 · Firewall

Geöffnet wird **nur der Portal-Port** (5110), und zwar für die Profile *Domäne* und *Privat*.

Wichtig: Der Fachdienst auf 5100 bleibt bewusst geschlossen. Das Portal spricht ihn über die Rückschleife an. Wer das Arbeitsplatzprogramm auf anderen Rechnern einsetzt, öffnet ihn ausdrücklich:

```
New-NetFirewallRule -DisplayName "Ordavis Bauhof Fachdienst" -Direction Inbound `
  -Action Allow -Protocol TCP -LocalPort 5100 -Profile Domain
```

⚠ ⚠ Bei eigenem HTTPS werden **ZWEI** Ports geöffnet und nicht einer — 5110 und 5111. Der HTTP-Port bleibt gebunden: Er ist die Quelle der Umleitung. Wer nur den HTTPS-Port öffnet, bekommt eine Umleitung, die niemanden erreicht.

⚠ In der Vorgabe spricht der Fachdienst **HTTP**, nicht HTTPS. Öffnen Sie ihn nur in einem Netz, in dem das vertretbar ist — oder stellen Sie einen Umkehrstellvertreter davor (Abschnitt 8).

Schritt 9 · Prüfung

Der Installer wartet auf beide Dienste und meldet erst dann Erfolg:

```
http://localhost:5100/gesundheit      → 200
http://localhost:5110/                → 200
```

Schlägt eine der beiden Proben fehl, endet das Skript mit Rückgabewert 1 und nennt, was zu prüfen ist.

5 Der erste Zugang

Beim allerersten Start legt der Fachdienst **einen** Benutzer an — und **nur**, wenn die Benutzertabelle leer ist.

Kennung	<code>verwaltung</code> (oder was in <code>Identity:Ersteinrichtung:Kennung</code> steht)
Anzeigenname	Erstzugang Betriebsleitung
Rolle	Verwaltung
Kennwort	zufällig erzeugt und genau einmal im Betriebsprotokoll ausgewiesen

Die Meldung sieht so aus und steht als **Warnung** im Protokoll, damit sie zwischen den Startmeldungen nicht untergeht:

BET-14 – ERSTZUGANG ANGELEGT. Dieses Kennwort erscheint NUR HIER.

Kennung: verwaltung

Kennwort: ... 20 Zeichen ...

Beim ersten Anmelden zu wechseln.

Achtung: Dieses Kennwort gibt es genau einmal zu lesen. Schreiben Sie es ab, bevor Sie das Fenster schließen. Wer den Start nicht gesehen hat, kommt über `EinrichtenAsync` nicht mehr hinein — die Funktion legt nur in eine leere Benutzertabelle an.

☆☆☆ Es gibt kein eingebautes `admin/admin`. Ein solcher Zugang wäre bequem und stünde binnen einer Woche in jeder Installation.

5.1 Wenn das Erstkennwort verloren ist

```
& "C:\Program Files\Ordivis Bauhof\api\Ordivis.Bauhof.Api.exe" zugang-zuruecksetzen  
verwaltung
```

Der Befehl setzt ein neues Zufallskennwort, weist es im Protokoll aus, verlangt den Wechsel beim nächsten Anmelden — und beendet sich, ohne den Netzdienst zu öffnen.

⚠ ⚠ Dieser Weg läuft über die Kommandozeile und ausdrücklich nicht über einen Endpunkt. Ein Endpunkt zum Zurücksetzen wäre — gleich wie abgesichert — eine Tür im Netz neben der verschlossenen. Wer den Befehl ausführt, steht ohnehin schon am Server: Er hat die Verbindungszeichenfolge, das Anmeldegeheimnis und die Datenbank.

⚠ Ist die Kennung unbekannt, **nennt** der Befehl die vorhandenen Kennungen. Das ist anders als bei der Anmeldung und mit Absicht: Die gleichlautende Abweisung dort schützt vor dem Erraten von Kennungen **aus dem Netz** — hier steht der Ausführende am Server.

6 Nach der Installation: die Aufräumarbeiten

Zu tun	Warum
Erstkennwort wechseln	Es ist ein Einrichtungskennwort und als solches gekennzeichnet.
<code>Identity:Ersteinrichtung:Kennwort</code> aus der Datei entfernen, falls gesetzt	Es steht sonst im Klartext auf der Platte.
Weitere Benutzer anlegen	Siehe OB-41.
Datensicherung einrichten	Siehe OB-51. Der Installer richtet keine ein.
Umkehrstellvertreter mit TLS davorstellen	Siehe Abschnitt 8.

Zu tun	Warum
Prüfen, ob maschinenweite <code>Identity__Jwt__*</code> -Variablen existieren	Siehe OB-02, Abschnitt 4.1.

7 Deinstallation

Über *Apps und Features* (Inno-Setup) oder von Hand:

```
Stop-Service Ordavis.Bauhof.Portal, Ordavis.Bauhof.API
sc.exe delete Ordavis.Bauhof.Portal
sc.exe delete Ordavis.Bauhof.API
Remove-NetFirewallRule -DisplayName "Ordavis Bauhof Portal"
Remove-Item "C:\Program Files\Ordavis Bauhof" -Recurse -Force
```

Achtung: Die Datenbank bleibt stehen. Das ist Absicht — sie enthält Nachweise. Wer sie wirklich verwerfen will, tut das ausdrücklich:

```
DROP DATABASE ordavis_bauhof;
DROP ROLE bauhof_app;
```

8 Verschlüsselung: drei Betriebsarten

— — — Ohne Verschlüsselung gehen Anmeldedaten und der Sitzungsschlüssel im Klartext über das Hausnetz. Der Sitzungsschlüssel ist dabei das Schwerere: Wer ihn aufschnappt, ist acht Stunden lang angemeldet, ohne je ein Kennwort gesehen zu haben. Ein Produkt, das Beschäftigtendaten so trägt, ist in einer Gemeinde nicht betreibbar.

Ordavis Bauhof kennt drei Betriebsarten. Sie stehen in `Hosting:HttpsMode` und werden vom Installationsprogramm gesetzt (`-Uebertragung`).

Betriebsart	Wer verschlüsselt	Was Sie brauchen
<code>ReverseProxy</code> (Vorgabe)	ein vorgelagerter Stellvertreter	IIS, nginx oder eine Appliance — siehe 8.1
<code>Certificate</code>	der Dienst selbst	ein Zertifikat — siehe 8.2
<code>Acme</code>	—	noch nicht gebaut; der Dienst sagt es beim Start und läuft auf HTTP weiter

⚠ ⚠ Die Vorgabe ist `ReverseProxy`, und das heißt nicht „sicher“. Sie ist das Verhalten heutiger Installationen. Der Grund ist ein anderer: Eine Vorgabe, die eine bestehende Anlage beim Update auf einen Port umbindet, den niemand freigegeben hat, macht den Dienst **unerreichbar** — er läuft, und trotzdem kommt niemand mehr hinein. Wer keinen Stellvertreter hat, stellt auf `Certificate` um.

⚠ **Die Betriebsart wird beim Start gelesen.** Sie ist die einzige Einstellung, die einen Neustart beider Dienste braucht.

★ Was gerade läuft, steht in beiden Oberflächen unter **Einstellungen** → **Übertragung & Zertifikat** — samt Ablaufdatum des Zertifikats und dem Hinweis, wenn die Konfiguration vom laufenden Stand abweicht.

8.1 Der Umkehrstellvertreter

Üblicherweise IIS mit *Application Request Routing*, ein nginx oder eine vorhandene Anwendungsschicht der Kommune.

Nach außen	<code>https://bauhof.gemeinde.de</code> (443)
Weiterleitung an	<code>http://localhost:5110</code>
Fachdienst	bleibt hinter dem Stellvertreter, nicht öffentlich

⚠ **Blazor Server braucht WebSockets.** Ein Stellvertreter ohne WebSocket-Durchreichung liefert eine Seite, die aussieht, als sei sie geladen — und auf keinen Klick reagiert. Das ist der häufigste Fehler bei dieser Art Installation.

⚠ Setzen Sie außerdem die üblichen Weitergabekopfzeilen (`X-Forwarded-For` , `X-Forwarded-Proto`), damit im Protokoll die richtige Herkunft steht.

8.2 Eigenes Zertifikat am Dienst

Der Regelfall in einer Kommune ist ein Zertifikat der eigenen Verwaltung oder des Landesdienstleisters. Es kommt als PFX oder liegt bereits im Speicher des Servers.

Genau eine Quelle wird eingetragen. Zwei sind ein Fehler und keine Auswahl — eine stillschweigende Rangfolge machte daraus einen Zufall.

Weg	Aufruf des Installationsprogramms
Windows-Speicher (empfohlen)	<code>-Uebertragung Certificate -Fingerabdruck "AB12..."</code>
PFX-Datei	<code>-Uebertragung Certificate -PfxDatei "D:\tls\bauhof.pfx" - PfxKennwort "..."</code>
PEM-Paar	<code>-Uebertragung Certificate -PemZertifikat "... .crt" -PemSchluessel "... .key"</code>

★ ★ **Der Fingerabdruck ist der bessere Weg.** Ein Zertifikat im Windows-Speicher wird von der Verwaltung erneuert, **ohne dass jemand eine Datei tauscht** — und es überlebt ein Update des Bauhofs. Den Fingerabdruck liefert der Zertifikatsdialog von Windows; Leerzeichen daraus stören nicht, sie werden abgeschnitten.

⊖ **Legen Sie eine PFX-Datei nicht ins Programmverzeichnis.** Das Installationsprogramm leert es bei jedem Update. Die Datei wäre danach weg, der Dienst lief ohne TLS weiter — und auffallen würde es erst,

wenn der Browser warnt. Das Installationsprogramm **weist einen solchen Pfad ab**.

⚠ **Das Zertifikat muss einen privaten Schlüssel haben.** Ohne ihn weist es aus und verschlüsselt nicht; das Installationsprogramm prüft es und sagt es. Bei einem Zertifikat aus dem Windows-Speicher heißt eine solche Meldung meist, dass der Dienstbenutzer den Schlüssel nicht lesen darf.

★ **Das PFX-Kennwort steht verschlüsselt in der Konfiguration** (Präfix `DPAPI:`). Der Grund wiegt schwerer als bei anderen Kennwörtern: Wer es hat, hat den privaten Schlüssel des Servers — damit lässt sich der Dienst nicht nur mitlesen, sondern **nachmachen**. Einzelheiten und der Weg von Hand stehen in **OB-52**, Abschnitt 2.1.

⚠ **Beim Umzug neu eintragen.** Die Verschlüsselung ist an das Dienstkonto gebunden; auf einem anderen Server ist sie nicht lesbar.

8.3 Der Ablauf ist eine Frist

Das Programm meldet ihn **30 Tage vorher**, ab 7 Tagen als Warnung — täglich um 06:05 im Betriebsprotokoll und in beiden Oberflächen. Der Grund für den langen Vorlauf: Ein Zertifikat der Verwaltung wird **beantragt** und nicht erzeugt, und das dauert in einer Kommune Wochen.

Einzelheiten in **OB-54**, Abschnitt 3.1.

8.4 ⚠ Zwei Ordvis-Produkte auf einem Server

Läuft daneben Ordvis IT, brauchen beide **zwei Portpaare und zwei Zertifikatszuordnungen**. Deshalb ist der HTTPS-Port des Bauhof-Portals **5111 und nicht 443**: Den 443 belegt das Portal von Ordvis IT bereits.

Ein **gemeinsames** Zertifikat für beide wäre kein Fehler — aber eine gemeinsame **Entscheidung**, und die entsteht nicht von selbst. Das Programm sagt den Satz beim Start, sobald TLS am Dienst läuft.

9 Wenn es nicht läuft

Bild	Wahrscheinliche Ursache	Was tun
Der Dienst startet und beendet sich sofort	Keine Verbindungszeichenfolge oder kein Anmeldegeheimnis	Ereignisanzeige lesen — beides meldet sich mit Klartext.
The <code>ConnectionString</code> property has not been initialized	<code>ConnectionStrings:Bauhof</code> ist leer	<code>appsettings.Production.json</code> prüfen.
Anmeldung schlägt nach einer Teilaktualisierung fehl	Portal und Fachdienst haben verschiedene Fassungen	<code>http://localhost:5100/api/version</code> aufrufen — der Weg ist bewusst ohne Anmeldung erreichbar.
Portal ohne Formatierung, Serifenschrift, blaue Verweise	Statische Dateien fehlen	Nur im Entwicklungslauf zu erwarten; im Verteilstand liegt alles unter <code>wwwroot</code> .

Bild	Wahrscheinliche Ursache	Was tun
<code>column does not exist</code> beim ersten Zugriff	Schema ist älter als das Modell	<code>schema-abgleich.ps1</code> — siehe OB-51.
Setup bricht in Schritt 4 mit SQL-Fehler ab	Rechte fehlen	Siehe Schritt 3.

Mehr dazu in OB-54.

Verwandte Themen

- **OB-02 · Systemvoraussetzungen und Architektur** — was Sie da eigentlich aufstellen — die Architektur hinter den Handgriffen
- **OB-52 · Konfigurationsreferenz** — die Werte, die Sie beim Einrichten setzen, mit Vorgabewert und Wirkung
- **OB-51 · Aktualisierung, Sicherung, Wiederanlauf** — der zweite Tag: eine neue Fassung einspielen und das Schema nachziehen
- **OB-40 · Administrationshandbuch** — der laufende Betrieb, sobald die erste Anmeldung steht

Aktualisierung, Sicherung, Wiederanlauf

OB-51 Aktualisierung Eine neue Fassung einspielen, das Schema nachziehen, sichern und wiederanlaufen

Teilweise gebaut

Achtung: Stand dieses Dokuments. Der Aktualisierungsweg ist gebaut und erprobt. Seit dem 31.08.2026 liegt er **als Dienst in der Installation** (**BET-02** Stufe 2) und braucht dort weder das .NET-SDK noch den Entwicklungsstand — Abschnitt 4.6. Der Weg über `update.ps1` bleibt daneben bestehen und ist für den **Server** weiterhin der richtige. Eine **Datensicherung richtet Ordvis Bauhof nicht ein**; sie ist Sache der Datenbankverwaltung. Beides ist unten ausdrücklich benannt.

Die Erstinstallation macht man einmal, die Aktualisierung viele Male — und sie ist der gefährlichere Vorgang. Bei der Installation ist nichts da, was kaputtgehen könnte. Bei der Aktualisierung liegen Daten aus dem laufenden Betrieb auf der Platte, und das Schema, das sie lesbar macht, ändert sich mit.

Der häufigste Fehler dabei ist kein technischer. Er besteht darin, die Sicherung als Schritt zu behandeln, den man macht, wenn Zeit ist — und die Wiederherstellung als etwas, das man erst im Ernstfall zum ersten Mal ausprobiert. Eine Sicherung, aus der noch nie jemand zurückgeholt hat, ist eine Vermutung.

Dieses Dokument beschreibt die Aktualisierung in der Reihenfolge, in der sie gefahrlos ist, was beim Schemaabgleich geschieht und woran man sieht, dass er durchgelaufen ist. Dazu die Sicherung — was hineingeht, was regelmäßig vergessen wird — und den Wiederanlauf als Übung, nicht als Notfall.

INHALT

1 ★ ★ ★ Die Reihenfolge ist der ganze Inhalt dieses Kapitels

2 Warum ein Schemaabgleich überhaupt nötig ist

3 Der Schemaabgleich

3.1 Wie er arbeitet

3.2 ⚠ ⚠ Was der Abgleich nicht kann

4 Die Aktualisierung des Programms

4.1 Wie sie arbeitet

4.2 ⚠ ⚠ Drei Dinge trennen das von der Ordvis Plattform

4.3 Die Sicherung gegen das falsche Ziel

4.4 Was die Aktualisierung nicht tut

4.5 Nach der Aktualisierung

4.6 Der Aktualisierungsdienst

5 Datensicherung

5.1 Was zu sichern ist

5.2 Ein einfacher Sicherungslauf

5.3 ★ ★ ★ Eine Sicherung, die nie zurückgespielt wurde, ist eine Vermutung

6 Wiederanlauf

6.1 Nach einem Neustart des Servers

6.2 Nach einem Datenverlust

6.3 Nach dem Verlust der Konfiguration

6.4 Wenn niemand mehr hineinkommt

7 Was in diesem Stand noch fehlt

Verwandte Themen

1 ★ ★ ★ Die Reihenfolge ist der ganze Inhalt dieses Kapitels

Erst das Schema, dann die Binärdateien.

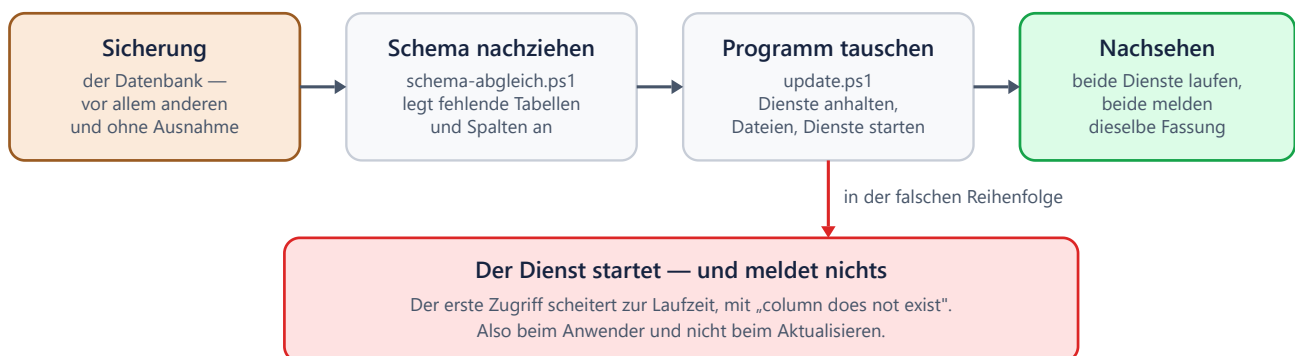


Abbildung 4 — Die Reihenfolge einer Aktualisierung. Der untere Weg ist der, den man nimmt, wenn man sie für Zeremoniell hält.

Erst das Schema, dann die Binärdateien. Andersherum läuft der neue Dienst eine Weile gegen ein altes Schema — er startet, meldet nichts, und der erste Zugriff scheitert zur Laufzeit.

⚠ Und davor, immer: **eine Sicherung der Datenbank.**

★ Das Bild beginnt auf dem **Server**. Die Fassung selbst entsteht davor und anderswo: `deploy\build-dist.ps1` packt sie auf dem Entwicklungsrechner, und `update.ps1` nimmt sie später aus `deploy\updates`. Wer beides am selben Ort vermutet, sucht das Paket auf der falschen Maschine.

2 Warum ein Schemaabgleich überhaupt nötig ist

Der Fachdienst legt sein Schema mit `EnsureCreated` an. Das legt ein Schema **nur in einer leeren Datenbank** an; eine bestehende schreibt es **nicht** fort.

Achtung: Kommen mit einer neuen Fassung Tabellen oder Spalten dazu, **startet der Dienst trotzdem und meldet nichts**. Der erste Zugriff scheitert dann mit `column does not exist` oder `relation ... does not exist` — also beim Anwender und nicht beim Aktualisieren.

Befund vom 26.08.2026: Genau so fehlten einer Datenbank fünf Tabellen des Winterdienstclusters.

⚠ `setup.ps1 -DatenbankVerwerfen` ist nicht der Weg. Er wirft den Bestand weg. Für eine Erprobungsinstallation ist er zulässig, für eine mit Nachweisen nicht.

3 Der Schemaabgleich

```
.\deploy\schema-abgleich.ps1 -NurZeigen      # nur vergleichen und berichten
.\deploy\schema-abgleich.ps1                # das Fehlende einspielen
```

3.1 Wie er arbeitet

★ Das **Soll** wird **nicht geraten, sondern gebaut**. Der Fachdienst wird einmal gegen eine **Wegwerf-Datenbank** gestartet; dort baut `EnsureCreated` das Schema aus dem Modell. Das ist die einzige Quelle, die garantiert stimmt — jsonb-Wandler, Wertevergleicher, ausgenommene Eigenschaften und Indizes ließen sich von Hand nicht richtig raten.

Dann wird auf **zwei Ebenen** verglichen:

1. fehlende **Tabellen**
2. fehlende **Spalten** in bestehenden Tabellen — ⚠ das ist der Teil, den man übersieht

Eingespielt wird nur das Fehlende.

Schalter	Wirkung
<code>-NurZeigen</code>	vergleicht und berichtet, ändert nichts
<code>-InstallDir</code>	Installation, deren Datenbank abgeglichen wird
<code>-Verbindung</code>	Zielverbindung von Hand statt aus der Konfiguration
<code>-Fachdienst</code>	Die <code>.exe</code> , deren Modell das Soll ist. Vorgabe: der letzte Bau

Schalter	Wirkung
<code>-OhneSicherung</code>	überspringt die Sicherung vor dem Einspielen

⚠️ `-Fachdienst` zeigt auf den neuen Stand, nicht auf den laufenden. Das Schema muss zu der Fassung passen, die eingespielt werden soll — nicht zu der, die noch läuft.

3.2 ⚠️ ⚠️ Was der Abgleich nicht kann

Achtung: Es ist ein Werkzeug und kein Ersatz für Migrationen. Er erkennt fehlende Tabellen und Spalten. Er erkennt nicht:

- eine **Umbenennung** — die sieht von hier aus wie eine gelöschte plus eine neue Spalte
- eine **Typänderung** mit Datenumzug
- und er **löscht nichts**. Löschen ist nie additiv, und was in der Zieldatenbank zu viel ist, gehört vor eine menschliche Entscheidung.

Nicht-leere Tabelle plus neue Pflichtspalte ohne Vorgabewert wird ausdrücklich **nicht** eingespielt: Postgres verlangt dafür einen Wert für die bestehenden Zeilen, und den zu erfinden ist eine fachliche Entscheidung — in einem Nachweisprodukt erst recht. Das Skript nennt die Spalte, legt die Anweisung als **Vorschlag** ab und endet mit Rückgabewert 2.

⚠️ Rückgabewert 2 ist kein Fehler und kein Erfolg. Er heißt: *Hier muss jemand entscheiden*. Wer ihn in einer Automatik als Erfolg wertet, spielt die Fassung mit unvollständigem Schema ein.

4 Die Aktualisierung des Programms

```
.\deploy\update.ps1 -WhatIf      # zeigt, was geschähe
.\deploy\update.ps1             # spielt die neueste Fassung aus deploy\updates ein
```

4.1 Wie sie arbeitet

Ein signiertes Freigabemanifest je Fassung, eine inhaltsadressierte Ablage — und das Delta wird am Ziel **gerechnet**: Es wird nur geholt, was sich tatsächlich unterscheidet.

```
Ablage\<fassung>\manifest.json    signiertes Manifest (ES256-JWS)
Ablage\blobs\<sha256>             die Dateien, inhaltsadressiert
```

Schalter	Wirkung
<code>-InstallDir</code>	Ziel der Aktualisierung
<code>-Ablage</code>	Verzeichnis mit Manifest und Blobs. Vorgabe: <code>deploy\updates</code>
<code>-Fassung</code>	eine bestimmte Fassung statt der neuesten
<code>-Von</code>	Bezug aus dem Netz; die Ablage dient dann als Zwischenspeicher

Schalter	Wirkung
-Kanal	stabil oder pilot
-NurZeigen	vergleicht und berichtet

Ablauf in fünf Schritten: Voraussetzungen → Abgleich → Dienste anhalten → Dateien tauschen → Dienste starten und prüfen.

4.2 ⚠️ ⚠️ Drei Dinge trennen das von der Ordvis Platform

Warum die Trennung bleiben muss	
Eigener Schlüssel	Beide Produkte teilen sich den Signierer, aber nicht die Vollmacht. Mit einem gemeinsamen Schlüssel ließe sich ein Platform-Release als Bauhof-Update einspielen und umgekehrt.
Eigene Ablage	Der Veröffentlichungsdienst der Platform beobachtet deren Webseitenbaum, spiegelt ihn nach außen und räumt dort auf. Bauhof-Dateien in diesem Baum gingen entweder öffentlich ins Netz oder würden gelöscht.
Eigene Dienste	Angehalten und gestartet werden ausschließlich <code>Ordvis.Bauhof.API</code> und <code>Ordvis.Bauhof.Portal</code> .

4.3 Die Sicherung gegen das falsche Ziel

Das Skript prüft, ob das Zielverzeichnis der Ordvis Platform gehört, und bricht dann ab.

★ **Diese Prüfung steht doppelt** — im Skript und im Werkzeug. Ein vertippter Pfad, der auf die Platform zeigt, tauschte dort Dateien aus und löschte alles, was nicht im Bauhof-Manifest steht. Das ist der eine Fehler, der auf einem gemeinsamen Server nicht passieren darf.

4.4 Was die Aktualisierung nicht tut

Achtung: Sie sichert die Datenbank nicht, und sie gleicht das Schema nicht ab. Beides ist ein eigener Schritt und gehört davor.

⚠️ Von Hand abgelegte Dateien im Programmverzeichnis überleben die Aktualisierung nicht. Die Zielverzeichnisse werden geleert — sonst blieben Dateien liegen, die es im neuen Stand nicht mehr gibt, und würden weiter ausgeliefert.

⚠️ Die **Konfiguration** ist davon nicht betroffen: `appsettings.Production.json` wird neu geschrieben, und das **Anmeldegeheimnis** wird **übernommen**. Ein neues meldete jeden angemeldeten Anwender ab — mitten im Betrieb, ohne Grund und ohne Meldung.

4.5 Nach der Aktualisierung

```
# 1. Beide Dienste laufen?  
Get-Service Ordvis.Bauhof.API, Ordvis.Bauhof.Portal  
  
# 2. Der Fachdienst antwortet?  
Invoke-WebRequest http://localhost:5100/gesundheit -UseBasicParsing  
  
# 3. Und mit welcher Fassung?  
Invoke-RestMethod http://localhost:5100/api/version
```

Wichtig: Vergleichen Sie die Fassung mit der des Arbeitsplatzprogramms. Ein Arbeitsplatz, der gegen einen Fachdienst anderer Fassung läuft, meldet sich mit einem Anmeldefehler — und genau deshalb ist `/api/version` ohne Anmeldung erreichbar.

⚠ **Das Arbeitsplatzprogramm wird nicht mit aktualisiert**, wenn es auf anderen Rechnern installiert ist. Es liegt zwar im Installationsverzeichnis unter `client\`, wird von dort aber nur verteilt.

4.6 Der Aktualisierungsdienst

Seit `BET-02` Stufe 2 liegt der Aktualisierungsweg **mit in der Installation:** `{Installationsordner}\aktualisierung`. Er läuft als Windows-Dienst `Ordvis.Bauhof.Aktualisierung`, sieht **alle vier Stunden** nach und spielt ein, was er einspielen darf.

☆☆☆ **Warum es ihn gibt.** Der Weg über `update.ps1` ruft ein Werkzeug aus dem Entwicklungsstand auf und setzt damit das .NET-SDK und ein Git-Submodul voraus. Auf einem Rechner der Gemeinde gibt es beides nicht. Und: Der Arbeitsplatz liegt unter `%ProgramFiles%` — eine laufende Anwendung kann ihre eigenen Dateien nicht ersetzen, und ein Sachbearbeiter ohne lokale Administratorrechte darf dort ohnehin nicht schreiben. Der Dienst läuft als lokales System und darf es.

⚠ ⚠ **Er fasst voreingestellt NUR den Arbeitsplatz an**, und der Grund steht nicht in der Aktualisierung, sondern in der **Datenbank**: Eine neuere Fassung des Fachdienstes kann ein Schema voraussetzen, das erst der Schemaabgleich herstellt (Abschnitt 3). Ein Dienst, der das selbstständig überginge, ließe den Fachdienst gegen ein altes Schema starten — er meldet nichts, und der erste Zugriff scheitert im Betrieb. **Der Server bleibt beim Weg über `update.ps1`.**

Einstellung	Bedeutung
Bezugsquelle	Woher die Fassungen kommen. Vorgabe <code>https://update.ordvis.eu/v1/bauhof</code> ; eine Netzwerkfreigabe ist zulässig
Kanal	<code>stabil</code> oder <code>pilot</code>
PruefintervallMinuten	Vorgabe 240
Komponenten	Vorgabe <code>["client"]</code> — siehe die Warnung oben
Eingeschaltet	<code>false</code> zieht ihn aus dem Verkehr, ohne ihn zu deinstallieren

Die Datei dafür ist `aktualisierung\appsettings.Production.json`. Sie überlebt jede Aktualisierung — dieselbe Regel wie bei der Konfiguration des Fachdienstes.

VON HAND ANSTOSSEN

```
# zeigt, was geschähe – ändert nichts
& "$env:ProgramFiles\Ordivis
Bauhof\aktualisierung\Ordivis.Bauhof.Aktualisierungsdienst.exe" --zeigen

# ein Durchgang, dann Schluss. Rückgabewert 0 = in Ordnung, 1 = fehlgeschlagen
& "$env:ProgramFiles\Ordivis
Bauhof\aktualisierung\Ordivis.Bauhof.Aktualisierungsdienst.exe" --einmal
```

WORAN MAN SIEHT, WAS ER GETAN HAT

★ Ein Dienst läuft in Sitzung 0 und **kann nichts anzeigen**. Er hinterlegt deshalb zweierlei:

Ort	Inhalt
<code>%ProgramData%\Ordivis Bauhof\aktualisierung.json</code>	Der Zustand: installierte und angebotene Fassung, letzter Lauf, letzter Fehler. Der Arbeitsplatz zeigt ihn unter <i>Systemstatus</i>.
<code>%ProgramData%\Ordivis Bauhof\Protokolle\aktualisierung-JJJJMMTT.log</code>	Was genau getauscht wurde. Eine Datei je Tag, Aufbewahrung 30 Tage

⚠ **Der Arbeitsplatz wird nie weggenommen.** Läuft er, während für ihn etwas bereitliegt, wartet der Dienst — und schaltet auf einen kürzeren Takt um. Im *Systemstatus* steht dann: „*Fassung X liegt bereit. Sie wird eingespielt, sobald dieser Arbeitsplatz geschlossen ist.*“

⚠ **Schnappschuss und Rücknahme.** Vor jedem Tausch wird weggelegt, was überschrieben oder gelöscht wird. Geht etwas schief, wird zurückgespielt; misslingt auch das, steht es **namentlich** im Protokoll und der Stand von vorher bleibt unter `.ordivis-schnappschuss` liegen.

5 Datensicherung

Achtung: Ordivis Bauhof richtet keine Datensicherung ein und führt keine durch. Wer das übersieht, betreibt ein Nachweisverfahren ohne Nachweisschutz.

5.1 Was zu sichern ist

Was	Wie oft	Anmerkung
Datenbank <code>ordivis_bauhof</code>	täglich	Enthält alles Fachliche, auch Belege und Bescheinigungen
<code>api\appsettings.Production.json</code>	bei jeder Änderung	⚠ enthält zwei Geheimnisse

Was	Wie oft	Anmerkung
portal\appsettings.Production.json	bei jeder Änderung	
Postfachordner mit <code>angenommen</code>	täglich	Die eingegangenen Protokolldateien im Urzustand
Programmverzeichnis	nicht nötig	Es entsteht aus dem Verteilstand neu

5.2 Ein einfacher Sicherungslauf

```
$tag = Get-Date -Format 'yyyy-MM-dd'
$env:PGPASSWORD = '...'
& pg_dump -h localhost -p 5432 -U bauhof_app -Fc -f "D:\Sicherung\bauhof-$tag.dump"
ordivis_bauhof
```

⚠️ `-Fc` (das eigene Format) und nicht reines SQL: Es lässt sich selektiv zurückspielen und ist erheblich kleiner.

⚠️ Das Kennwort gehört **nicht** in ein Skript, das breiter lesbar ist als die Datenbank selbst. Nutzen Sie eine `.pgpass` -Datei oder die Sicherungslösung des Hauses.

5.3 ★ ★ ★ Eine Sicherung, die nie zurückgespielt wurde, ist eine Vermutung

Merksatz: Proben Sie die Wiederherstellung **einmal im Jahr**, auf einem anderen Rechner und mit einer echten Datei aus dem Bestand.

Was dabei zu prüfen ist:

1. Lässt sich die Datei überhaupt einlesen?
2. Startet der Fachdienst gegen die zurückgespielte Datenbank?
3. Sind die Winterdienstprotokolle des letzten Winters da — **mit ihrer Urschrift?**
4. Meldet sich ein Benutzer an?

6 Wiederanlauf

6.1 Nach einem Neustart des Servers

Beide Dienste starten automatisch. **Nichts zu tun** — außer:

⚠️ **Ein Neustart überspringt die Wachen dieses Tages**, deren Uhrzeit bereits vorbei ist. Wer morgens um sieben neu startet, hat an diesem Tag keine Fristenmeldung. Für geplante Neustarts ist der Nachmittag die bessere Wahl. Siehe OB-54.

6.2 Nach einem Datenverlust

```
# 1. Dienste anhalten
Stop-Service Ordavis.Bauhof.Portal, Ordavis.Bauhof.API

# 2. Datenbank neu anlegen und zurückspielen
& psql -h localhost -U postgres -c "DROP DATABASE ordavis_bauhof;"
& psql -h localhost -U postgres -c "CREATE DATABASE ordavis_bauhof OWNER bauhof_app;"
& pg_restore -h localhost -U postgres -d ordavis_bauhof "D:\Sicherung\bauhof-2026-08-28.dump"

# 3. Dienste starten
Start-Service Ordavis.Bauhof.API
Start-Service Ordavis.Bauhof.Portal
```

⚠️ Prüfen Sie danach die Eigentümerschaft der Tabellen. Ein Rückspielen als `postgres` kann die Tabellen dieser Rolle zuordnen; der Fachdienst meldet dann `permission denied for table`:

```
SELECT tablename, tableowner FROM pg_tables WHERE schemaname = 'public';
-- Erwartet: bauhof_app
```

6.3 Nach dem Verlust der Konfiguration

Ohne `appsettings.Production.json` startet der Fachdienst nicht. Zwei Werte sind zu ersetzen:

Wert	Folge, wenn er neu ist
<code>ConnectionStrings:Bauhof</code>	keine — nur richtig eintragen
<code>Identity:Jwt:Secret</code>	⚠️ alle angemeldeten Anwender werden abgemeldet. Fachlich bleibt alles erhalten, Kennwörter gelten weiter

★ Das Anmeldegeheimnis verschlüsselt **keine Daten** — es signiert Token. Ein neues Geheimnis kostet Sitzungen, keine Nachweise.

6.4 Wenn niemand mehr hineinkommt

```
& "C:\Program Files\Ordavis Bauhof\api\Ordavis.Bauhof.Api.exe" zugang-zuruecksetzen
verwaltung
```

Siehe OB-41.

7 Was in diesem Stand noch fehlt

Fehlt	Auswirkung	Paket
Eigenständiges Aktualisierungswerkzeug in der Installation	Die Aktualisierung läuft heute über <code>dotnet run</code> aus dem Entwicklungsstand und setzt das .NET-SDK voraus. Für eine Kundeninstallation taugt das nicht.	<code>BET-02</code> , zweite Stufe

Fehlt	Auswirkung	Paket
Datenbankmigrationen	Umbenennungen und Typänderungen sind Handarbeit.	PEX-18
Automatische Datensicherung	Sache der Datenbankverwaltung.	—
Sicherungsprüfung im Produkt	Es gibt keine Anzeige „letzte Sicherung war am ...“.	—
Aktualisierung des Arbeitsplatzprogramms auf entfernten Rechnern	Verteilung über die Softwareverteilung der Kommune.	—

Verwandte Themen

- **OB-50 · Installation und Server** — die Erstinstallation und die Verzeichnisse, auf die sich die Sicherung bezieht
- **OB-52 · Konfigurationsreferenz** — die Konfigurationswerte, die eine neue Fassung verlangen kann
- **OB-54 · Wachen, Protokoll und Störungsbilder** — was nach einem Wiederanlauf im Protokoll stehen muss, damit er gelungen ist
- **OB-40 · Administrationshandbuch** — die Aufgaben im Jahreslauf, in denen die Sicherung wiederkehrt

Konfigurationsreferenz

OB-52 Konfiguration Jeder Wert in den appsettings-Dateien, sein Vorgabewert und seine Wirkung

Beschreibt Vorhandenes

Dieses Dokument liest niemand von vorn. Man kommt hierher mit einer Frage: Was bewirkt dieser Wert, welchen hat er, wenn ich ihn nicht setze, und was passiert, wenn ich ihn falsch setze?

Es ist deshalb als Nachschlagewerk gebaut — je Abschnitt der Konfigurationsdatei eine Tabelle mit Name, Vorgabewert und Wirkung. Wo ein Wert eine Falle enthält, steht sie daneben und nicht in einem eigenen Kapitel; wer den Wert nachschlägt, muss die Falle im selben Blick sehen.

⚠ Ein Wert ohne Vorgabewert ist ein Pflichtwert. Fehlt er, startet der Dienst nicht — was freundlicher ist, als es klingt: Der Dienst, der mit einer halben Konfiguration startet, fällt später auf und an einer Stelle, die mit der Ursache nichts zu tun hat.

INHALT

1 Die Dateien und ihre Rangfolge

1.1 ⚠ ⚠ Der Sonderweg für den Abschnitt Identity

2 Der Fachdienst — api\appsettings.Production.json

2.1 Hosting — Ports und Transportverschlüsselung

2.2 ConnectionStrings

2.3 Identity:Jwt

2.4 Identity:Ersteinrichtung

2.5 Postfach — die Annahme der Winterdienstprotokolle

2.6 Die Wachen

2.7 Lizenz — die Produktlizenz

2.8 Logging

2.9 Sicherung — wo die Datensicherung liegt

3 Das Portal — portal\appsettings.Production.json

4 Umgebungsvariablen

5 Beispiel einer vollständigen Produktionskonfiguration

Verwandte Themen

1 Die Dateien und ihre Rangfolge

Ordvis Bauhof liest seine Einstellungen aus JSON-Dateien im jeweiligen Programmverzeichnis.

Rang	Quelle	Wer schreibt sie
1 (schwächster)	appsettings.json	mitgeliefert, nicht ändern
2	appsettings.Production.json	der Installer
3 (stärkster)	Umgebungsvariablen mit dem Präfix <code>ORDIVIS_BAUHOF_</code>	von Hand, nur im Ausnahmefall

Achtung: Ändern Sie `appsettings.json` nicht. Sie wird bei jeder Aktualisierung ersetzt — das Zielverzeichnis wird beim Kopieren geleert. Alles Eigene gehört in `appsettings.Production.json`.

Achtung: Nach jeder Änderung den Dienst neu starten. Die Dateien werden beim Start gelesen und danach nicht mehr. Eine Änderung ohne Neustart wirkt nicht — und meldet das auch nicht.

1.1 ⚠️ Der Sonderweg für den Abschnitt `Identity`

Der Abschnitt `Identity` wird aus einer **eigenen Sicht** gelesen, die ausschließlich die `appsettings`-Dateien dieser Installation und Umgebungsvariablen mit dem Präfix `ORDIVIS_BAUHOF_` kennt.

Der Grund steht in OB-02, Abschnitt 4.1: Maschinenweite Variablen `Identity__Jwt__Secret` der Ordvis Plattform überschrieben sonst die Einstellungen dieses Produkts — und beide Installationen hätten dasselbe Anmeldegeheimnis.

Alles andere (`Hosting`, `ConnectionStrings`, `Postfach`, die Wachen) bleibt normal über Umgebungsvariablen konfigurierbar.

2 Der Fachdienst — `api\appsettings.Production.json`

2.1 `Hosting` — Ports und Transportverschlüsselung

Schlüssel	Vorgabe	Bedeutung
<code>Hosting:HttpPort</code>	<code>5100</code>	HTTP-Port. ⚠️ Die Ordvis Plattform belegt 5000/5001.
<code>Hosting:HttpsMode</code>	<code>ReverseProxy</code>	Betriebsart: <code>ReverseProxy</code> , <code>Certificate</code> oder <code>Acme</code>
<code>Hosting:HttpsPort</code>	<code>5101</code>	HTTPS-Port. Nur bei <code>Certificate</code> und <code>Acme</code> gebunden.
<code>Hosting:Domain</code>	<i>(leer)</i>	Öffentlicher Name des Dienstes (<code>bauhof.gemeinde.de</code>)
<code>Hosting:LoopbackOnly</code>	<code>false</code>	Nur an 127.0.0.1 binden statt an alle Adressen
<code>Hosting:RedirectHttpToHttps</code>	<code>true</code>	HTTP auf HTTPS umleiten, sobald HTTPS läuft
<code>Hosting:CertificateStoreThumbprint</code>	<i>(leer)</i>	SHA-1-Fingerabdruck im Windows-Speicher <code>LocalMachine\My</code>
<code>Hosting:CertificatePfxPath</code>	<i>(leer)</i>	Pfad zu einer PFX-/PKCS#12-Datei
<code>Hosting:CertificatePfxPassword</code>	<i>(leer)</i>	Kennwort der PFX-Datei, verschlüsselt — siehe unten
<code>Hosting:CertificatePemPath</code>	<i>(leer)</i>	PEM-Zertifikat

Schlüssel	Vorgabe	Bedeutung
Hosting:CertificatePemKeyPath	(leer)	Privater Schlüssel zum PEM-Zertifikat

DIE DREI BETRIEBSARTEN

Wert	Was der Dienst tut	Was er voraussetzt
ReverseProxy	Spricht nur HTTP	Einen vorgelagerten Proxy (IIS, nginx, Appliance), der TLS übernimmt
Certificate	Spricht selbst HTTPS	Ein Zertifikat — aus dem Windows-Speicher, als PFX oder als PEM-Paar
Acme	Bezüge sein Zertifikat selbst	Noch nicht gebaut. Der Dienst sagt es beim Start und läuft auf HTTP weiter.

⚠️ ⚠️ Die Vorgabe ist **ReverseProxy**, und das heißt nicht „sicher“. Sie ist das Verhalten heutiger Installationen: Ohne vorgelagerten Proxy geht **alles unverschlüsselt über das Hausnetz** — Anmeldedaten und der Sitzungsschlüssel eingeschlossen. Wer keinen Proxy hat, stellt auf **Certificate** um.

⚠️ Der HTTP-Port bleibt immer gebunden, auch wenn HTTPS läuft. Er ist die Quelle der Umleitung und der Weg, auf dem Let's Encrypt später seine Rückfrage stellt.

⚠️ Die Betriebsart wird beim Start gelesen. Sie ist der einzige Bereich, der einen Neustart braucht — die übrigen Einstellungen liest der Dienst im Betrieb nach. Der Grund liegt nicht im Programm: Ein Netzwerk-Endpunkt lässt sich nicht umbinden, während er benutzt wird.

WOHER DAS ZERTIFIKAT KOMMT

Genau **eine** Quelle wird eingetragen. Zwei sind ein Fehler und keine Auswahl: Eine stillschweigende Rangfolge machte daraus einen Zufall — beim nächsten Erneuern tauscht jemand die Datei, und in Betrieb bleibt das Zertifikat aus dem Speicher. Der Dienst weist beides ab und nennt den Grund.

★ ★ Der Fingerabdruck ist der bessere Weg. Ein Zertifikat im Windows-Speicher wird von der Verwaltung erneuert, **ohne dass jemand eine Datei tauscht** — und es überlebt ein Update des Bauhofs.

– Eine PFX-Datei gehört nicht ins Programmverzeichnis. Das Installationsprogramm leert es bei jedem Update. Die Datei wäre danach weg, der Dienst lief ohne TLS weiter, und auffallen würde es erst, wenn der Browser warnt. Das Installationsprogramm weist einen solchen Pfad deshalb ab.

– DAS PFX-KENNWORT STEHT VERSCHLÜSSELT IN DER DATEI

Es beginnt mit **DPAPI:** und ist mit Windows-Bordmitteln verschlüsselt. Der Grund wiegt schwerer als bei anderen Kennwörtern: **Wer das PFX-Kennwort hat, hat den privaten Schlüssel des Servers** — damit lässt sich der Dienst nicht nur mitlesen, sondern nachmachen.

Das Installationsprogramm verschlüsselt es. Von Hand geht es so:

```
Ordvis.Bauhof.Api.exe geheimnis-schuetzen "MeinKennwort"
```

Die Ausgabe wird unverändert in **Hosting:CertificatePfxPassword** eingetragen.

⚠️ ⚠️ **Der Aufruf muss unter dem Dienstkonto laufen.** Die Verschlüsselung ist an das Konto gebunden, das sie erzeugt hat — ein als Administrator verschlüsselter Wert ist für den Dienst nicht lesbar, und das fällt erst beim nächsten Start auf, mit einer Meldung über ein falsches PFX-Kennwort.

⚠️ **Dasselbe gilt beim Umzug.** Wird der Dienst auf ein anderes Konto umgestellt oder die Konfiguration auf einen anderen Server kopiert, ist das Kennwort dort nicht mehr lesbar und neu einzutragen.

★ Ein Wert **ohne** das Präfix wird unverändert gelesen. Eine bestehende Installation, die ihr Kennwort noch im Klartext trägt, verliert durch ein Update nicht ihr TLS.

2.2 ConnectionStrings

Schlüssel	Vorgabe	Bedeutung
ConnectionStrings:Bauhof	(<i>leer</i>)	Npgsql-Verbindungszeichenfolge

```
"ConnectionStrings": {
  "Bauhof":
  "Host=localhost;Port=5432;Database=ordivis_bauhof;Username=bauhof_app;Password=..."
}
```

Achtung: Ohne Verbindungszeichenfolge startet der Dienst nicht. Er wirft beim Start eine Meldung mit Klartext. Das ist Absicht: Ein Fehlstart mit Meldung ist besser als ein Betrieb mit falscher Annahme.

⚠️ Geprüft wird auf **leer oder nur Leerzeichen**, nicht auf `null`. Die mitgelieferte `appsettings.json` trägt eine **leere Zeichenfolge** — ein Nullausweich griffe nie, und Npgsql meldete erst beim ersten Zugriff `The ConnectionString property has not been initialized`.

2.3 Identity:Jwt

Schlüssel	Vorgabe	Bedeutung
Identity:Jwt:Issuer	Ordivis.Bauhof	Aussteller. Trägt den Produktnamen, damit ein Token im Protokoll zuzuordnen ist.
Identity:Jwt:Audience	Ordivis.Bauhof	Empfänger. Beide Oberflächen sprechen denselben Fachdienst an.
Identity:Jwt:Secret	(<i>leer</i>)	Pflicht. Mindestens 32 Byte. Vom Installer erzeugt.
Identity:Jwt:AccessTokenExpiryMinutes	480	Lebensdauer eines Tokens in Minuten

Achtung: Hier steht bewusst kein Vorgabewert für `Secret`. Ein eingebautes Geheimnis ist dasselbe wie kein Geheimnis: Es steht im Quelltext, in jeder Installation, und ist beim ersten Kunden bekannt.

⚠ Die **Länge** wird beim Start geprüft. Ohne diese Prüfung scheiterte erst die *erste Anmeldung* nach der Installation — also nicht beim Start und ohne Bezug zur Ursache.

⚠ Wer **Issuer** oder **Audience** ändert, macht **alle ausgestellten Token ungültig**. Es gibt keinen Grund, sie zu ändern.

2.4 Identity:Ersteinrichtung

Schlüssel	Vorgabe	Bedeutung
Identity:Ersteinrichtung:Kennung	verwaltung	Kennung des Erstzugangs
Identity:Ersteinrichtung:Kennwort	(leer)	leer = zufälliges Kennwort, einmal im Protokoll ausgewiesen

Wirkt **nur**, wenn die Benutzertabelle leer ist. Sie schreibt nie über Vorhandenes.

Achtung: Nach der Einrichtung gehört **Kennwort** wieder heraus. Es steht sonst im Klartext in einer Datei auf der Platte. Auch ein hier gesetztes Kennwort gilt als Einrichtungskennwort und verlangt den Wechsel beim ersten Anmelden — was der Installer geschrieben hat, ist kein Geheimnis.

2.5 Postfach — die Annahme der Winterdienstprotokolle

Schlüssel	Vorgabe	Bedeutung
Postfach:Ordner	(leer)	Überwacher Ordner. Leer = der Annahmedienst läuft nicht.
Postfach:TaktSekunden	60	Abstand zwischen zwei Durchläufen
Postfach:RuhezeitSekunden	10	Wie lange eine Datei unverändert sein muss, bevor sie angefasst wird

★ ★ Hier steht bewusst kein Postfachzugang mit Kennwort. Die ausgelieferten Apps senden ihre Protokolle als Anhang; eine Regel im Mailprogramm oder auf dem Mailserver legt den Anhang in diesem Ordner ab. Ein Dienst, der keine Zugangsdaten hat, kann sie auch nicht verlieren.

★ Die **Ruhezeit** ist kein Zierrat: Eine Datei, die gerade geschrieben wird, ist unvollständig — und eine unvollständig gelesene Signatur ist eine verfälschte.

⚠ Der Dienst löscht nie. Angenommenes geht nach `<Ordner>\angenommen`, Abgewiesenes nach `<Ordner>\abweisung`. Wenn die Annahme selbst kaputt ist, ist die Datei dort das Einzige, was noch da ist.

Ist kein Ordner gesetzt, **beendet sich der Dienst sofort und meldet das** — er ist damit auf jeder Installation gefahrlos eingeschaltet.

2.6 Die Wachen

Alle Wachen haben denselben Aufbau: ein Schalter, eine Uhrzeit, und der Lauf schreibt ins Betriebsprotokoll. Die vollständige Beschreibung, was jede Wache prüft, steht in **OB-54**.

Abschnitt	Aktiv	Uhrzeit	Weitere Werte
Zertifikatswache	true	06:05	—
Turnuswache	true	05:15	Vorlaufstage (leer = 14)
Beschaffungswache	true	06:00	—
(Ablesewache)	fest an	06:15	nicht einstellbar
(Befähigungswache)	fest an	06:15	nicht einstellbar
Fristenwache	true	06:30	—
(Hochrechnungswache)	fest an	06:45	nicht einstellbar
Kontrollwache	true	07:00	Erinnerung und Meldeschwelle in Tagen
Lueckenwache	true	10:00	RueckblickTage (Vorgabe 14)

```
"Lueckenwache": { "Aktiv": true, "Uhrzeit": "10:00", "RueckblickTage": 14 },
"Fristenwache": { "Aktiv": true, "Uhrzeit": "06:30" },
"Kontrollwache": { "Aktiv": true, "Uhrzeit": "07:00" },
"Beschaffungswache": { "Aktiv": true, "Uhrzeit": "06:00" },
"Turnuswache": { "Aktiv": true, "Uhrzeit": "05:15", "Vorlaufstage": null }
```

☆☆☆ DIE TURNUSWACHE IST DIE EINE, DIE ARBEIT ERZEUGT

Alle übrigen Wachen **melden** — sie schreiben Befunde ins Betriebsprotokoll. Die Turnuswache (DIS-05) **legt Aufträge an**: Aus der Pflegeklasse einer Fläche (Gänge je Saison, Saisonfenster) entstehen Mähaufräge im Voraus. Das ist zulässig, weil der Auftrag selbst die Meldung ist — er steht in der Tagesliste, und dort gehört er hin. Was sie **nicht** tut, ist disponieren: Welche Kolonne mäht, entscheidet ein Mensch.

☆☆ Sie läuft als erste, und 05:15 ist gewählt und nicht geraten. Sie liegt hinter dem Fensterschluss der Datensicherung (05:00, siehe *Aktualisierung, Sicherung, Wiederanlauf*): Die Sicherung gehört die Nacht, und ein Turnuslauf, der in sie hineinläuft, streitet mit ihr um dieselbe Datenbank. Und sie liegt vor allen übrigen Wachen und vor dem Arbeitstag — alles, was den Tag ansieht, soll die Aufträge schon sehen.

⚠ **Vorlaufstage** bestimmt, wie weit im Voraus geplant wird. Leer heißt 14 Tage: lang genug, dass eine Kolonne disponiert werden kann, kurz genug, dass die Tagesliste nicht mit Arbeit gefüllt ist, die noch niemanden angeht.

⚠ ⚠ Sie erzeugt nichts doppelt und nichts rückdatiert. Ein Gang, für den schon ein Auftrag steht, entsteht nicht noch einmal. Und ein Gang, der in der Vergangenheit liegt und nie geplant wurde, wird **genannt und nicht angelegt**: Er ist nicht ausgefallen — er hat nie existiert. Ein rückdatierter Auftrag im Zustand „geplant“ behauptete dagegen, die Arbeit sei eingeteilt gewesen und liegengeblieben. Steht diese Zahl bei einer laufenden Installation im Protokoll, ist die Planung zu lange nicht gelaufen.

⚠ **Außerhalb des Saisonfensters entsteht kein Auftrag** (GRN-04). Das ist der Normalfall im Winter und kein Versäumnis: Ein Turnus, der das ganze Jahr lief, füllte den Rückstand mit Mähaufrägen für

gefrorenen Boden — und ein Arbeitsvorrat, der Unsinn enthält, wird nicht mehr gelesen. Das Fenster steht je Pflegeklasse und ist dort einstellbar.

⚠️ Eine **unlesbare Uhrzeit** lässt den Dienst nicht scheitern. Sie ist ein Konfigurationsfehler und darf keinen Ausfall erzeugen: Die Wache meldet den falschen Wert und läuft mit ihrer Vorgabe weiter. **Sehen Sie deshalb nach einer Änderung ins Protokoll** — dort steht, welche Uhrzeit wirklich gilt.

⚠️ Eine **ausgeschaltete Wache** meldet das **einmal beim Start**. Wer eine Meldung vermisst, findet dort die Antwort.

2.7 Lizenz — die Produktlizenz

Schlüssel	Vorgabe	Bedeutung
Lizenz:Datei	%ProgramData%\Ordvis Bauhof\lizenz.lic	Pfad zur Lizenzdatei
Lizenz:Token	(<i>leer</i>)	Die Lizenz unmittelbar als Text — geht der Datei vor

Ordvis Bauhof und Ordvis Platform sind **getrennte Produkte mit getrennten Lizenzen**. Beide prüfen gegen denselben Signaturschlüssel der Ordvis-Lizenzstelle; unterschieden werden sie allein über das Produktkennzeichen, das mitsigniert in der Lizenz steht. **Eine Platform-Lizenz schaltet den Bauhof nicht frei** — und umgekehrt. Wer beide Produkte einsetzt, wie es auf einem gemeinsamen Server vorkommt, braucht deshalb zwei Lizenzdateien an zwei Orten.

Was der Dienst beim Start ins Protokoll schreibt, und das ist die Stelle, an der Sie nachsehen:

```
info: Lizenz (C:\ProgramData\Ordvis Bauhof\lizenz.lic): Lizenziert für Gemeinde  
Fuldata1,  
gültig bis 01.09.2027.
```

Was passiert, wenn die Lizenz nicht trägt

Zustand	Lesen	Ändern
Gültig	ja	ja
Abgelaufen, Nachfrist (30 Tage)	ja	ja — mit Hinweis
Abgelaufen, Nachfrist vorbei	ja	nein (HTTP 402)
Ungültig — beschädigt, gefälscht oder für ein anderes Ordvis-Produkt	ja	nein (HTTP 402)
Keine Lizenzdatei vorhanden	ja	ja — siehe unten

★ **Lesen bleibt in jedem Fall offen, und das ist Absicht.** Eine abgelaufene Lizenz darf den Betrieb anhalten, aber sie darf Sie nicht von Ihren eigenen Daten abschneiden: Gerade wer nicht verlängert, muss den Bestand einsehen, ausdrucken und ausleiten können. Ebenso offen bleiben die Anmeldung, die Anmeldung einer Ausgabestation, `/gesundheits` und `/api/version` — sonst führte die Sperre in eine Tür, die sich nur von innen öffnen lässt.

⚠️ **Eine fehlende Lizenzdatei sperrt heute nichts.** Der Grund ist einfach: Es gibt derzeit keinen Weg, eine Bauhof-Lizenz einzuspielen, und ausgestellt werden kann sie ebenfalls noch nicht. Eine Sperre ohne Ausweg wäre ein Ausfall und kein Schutz. Das ändert sich, sobald beides vorhanden ist; das Handbuch wird an dieser Stelle nachgezogen.

2.8 Logging

Schlüssel	Vorgabe
Logging:LogLevel:Default	Information
Logging:LogLevel:Microsoft.AspNetCore	Warning
Logging:LogLevel:Microsoft.EntityFrameworkCore.Database.Command	Warning

⚠️ Die letzte Zeile ist wichtig: Auf `Information` protokolliert EF Core **jede** SQL-Anweisung. Das ist zur Fehlersuche nützlich und im Dauerbetrieb ein Plattenfresser.

2.9 Sicherung — wo die Datensicherung liegt

Schlüssel	Vorgabe	Bedeutung
Sicherung:Ablage	(<i>leer</i>)	Ordner, in den <code>sicherung.ps1</code> seine Läufe schreibt. Leer = der Fachdienst kann über die Sicherung nichts sagen.

⊖ ⊖ **Der Fachdienst sichert nicht.** Er *liest* nur, was die geplante Aufgabe hinterlassen hat — je Lauf ein Ordner mit einer Beschreibung (`lauf.json`). Der Lauf gehört der Aufgabenplanung, **weil er auch dann laufen muss, wenn der Fachdienst steht.** Eingerichtet wird er mit `sicherung-einrichten.ps1`; siehe *Aktualisierung, Sicherung, Wiederanlauf*.

⚠️ ⚠️ **Kein Vorgabewert, und das ist Absicht.** Ein geratener Pfad, unter dem nichts liegt, ergäbe die Meldung „keine Sicherung gefunden“ — und das ist eine **ganz andere Aussage** als „hier ist nicht eingerichtet, wohin gesichert wird“. Die erste beschuldigt den Lauf, die zweite die Einrichtung, und wer die erste liest, sucht am falschen Ende.

WAS DER SYSTEMSTATUS DARAUS MACHT

Ist der Schlüssel gesetzt, erscheint auf der Seite *Systemstatus* der Abschnitt **Datensicherung**. Er beantwortet vier Fragen, und zwar an derselben Stelle:

Meldung	Was sie heißt
Zuletzt erfolgreich gesichert am ...	Mit dem Alter daneben, sobald es mehr als einen Tag ist — „vor fünf Tagen“ ist eine Aussage darüber, wie viel Arbeit im Ernstfall weg wäre
Fehlende Tage	Einzeln aufgezählt. Ein fehlender Lauf und ein Tag ohne Änderungen sehen in der Ablage gleich aus — gezählt werden deshalb die Tage, an denen etwas stehen <i>müsste</i>
Lauf ohne Ende	Er läuft noch, oder er ist gestorben, ohne es zu sagen. In der Ablage sieht beides gleich aus, und das zweite ist der Fall, auf den es ankommt

Meldung	Was sie heißt
Bildstand liegt auseinander	Die Datenbank verweist auf Bilddateien. Wer beides zu verschiedenen Zeiten sichert, spielt einen Stand zurück, dessen Verweise ins Leere zeigen — und das sieht nicht wie ein Fehler aus, sondern wie fehlende Bilder

☆☆☆ Eine Anlage ohne Sicherung meldet „gestört“ und nicht „ruht“. Beim Postfach ist das Fehlen der Normalfall — Protokolle kommen dann eben über das Portal. Eine Anlage ohne Sicherung hat keinen zweiten Weg: **Was fehlt, fehlt endgültig**. Deshalb steht dort „gestört“, auch wenn niemand etwas kaputtgemacht hat.

☆☆☆ Und ein Satz steht immer da, auch wenn alles grün ist: Eine Sicherung, die nie zurückgespielt wurde, ist keine Sicherung, sondern eine Datei. Der Probelauf gehört auf eine **leere** Maschine und endet damit, dass sich jemand an der wiederhergestellten Installation anmeldet — ein Rückspielen neben die laufende Installation findet alles vor, was fehlen könnte (Verzeichnisse, Rechte, Zeichensätze, Datenbankbenutzer) und beweist nur, dass die Datei lesbar ist.

⚠ Die Rückschau umfasst **14 Tage** und endet **gestern**: Die heutige Nacht war noch nicht, und einen Lauf zu vermissen, den es noch gar nicht geben kann, hieße jeden Vormittag eine Störung zu melden.

3 Das Portal — `portal\appsettings.Production.json`

Schlüssel	Vorgabe	Bedeutung
<code>Hosting:HttpPort</code>	<code>5110</code>	HTTP-Port. ⚠ Die Ordvis Plattform belegt 8080/443.
<code>Hosting:HttpsMode</code>	<code>ReverseProxy</code>	Wie beim Fachdienst — dieselben drei Betriebsarten
<code>Hosting:HttpsPort</code>	<code>5111</code>	HTTPS-Port des Portals
<code>Api:BaseUrl</code>	<code>http://localhost:5100</code>	Adresse des Fachdienstes
<code>Logging:LogLevel:Default</code>	<code>Information</code>	
<code>AllowedHosts</code>	<code>*</code>	

☆ Der Fachdienst wird über die Rückschleife angesprochen. Er ist im Netz nicht geöffnet; solange keine mobile Anwendung angebunden ist, hat er dort nichts zu suchen.

⚠ Wer `Api:BaseUrl` auf einen anderen Rechner zeigen lässt, muss den Fachdienst dort in der Firewall öffnen — **und bedenken, dass die Verbindung dann unverschlüsselt über das Netz geht**.

⚠ ⚠ Der HTTPS-Port des Portals ist 5111 und nicht 443. Auf einem Server, der Ordvis IT mitführt, belegt deren Portal den 443 bereits. Wer 443 will, trägt ihn ein — dann steht die Entscheidung wenigstens irgendwo.

☆ Der Weg vom Portal zum Fachdienst bleibt HTTP über die Rückschleife, auch wenn nach außen HTTPS läuft. Über 127.0.0.1 verlässt nichts den Rechner, und ein Zertifikat dafür müsste auf `localhost` lauten — eine zweite, gänzlich eigene Beschaffung.

Der Zeitablauf für Aufrufe an den Fachdienst liegt fest bei **15 Sekunden** und ist nicht einstellbar. Ebenso der Abruf des Kartenhintergrunds: ★ Ein hängender Kartendienst darf die Ansicht nicht blockieren — ohne Hintergrund bleibt die gefahrene Linie, und die ist der Nachweis.

4 Umgebungsvariablen

Alle Werte lassen sich auch als Umgebungsvariable setzen; die Abschnittstrennung ist ein doppelter Unterstrich.

```
# Für den Abschnitt Identity ist der Präfix PFLICHT:
[Environment]::SetEnvironmentVariable(
    'ORDIVIS_BAUHOF_Identity__Jwt__Secret', '...', 'Machine')

# Für alles andere geht auch die schmucklose Form:
[Environment]::SetEnvironmentVariable('Postfach__Ordner', 'D:\Bauhof\Eingang', 'Machine')
```

Wichtig: Setzen Sie niemals unpräfixierte `Identity__Jwt__*` -Variablen maschinenweit. Sie gälten für **jede** ASP.NET-Core-Anwendung auf diesem Rechner — auch für die Ordvis Platform. Genau daraus entstand der Befund vom 27.08.2026.

5 Beispiel einer vollständigen Produktionskonfiguration

```
{
  "Hosting": { "HttpPort": 5100 },
  "ConnectionStrings": {
    "Bauhof":
"Host=localhost;Port=5432;Database=ordivis_bauhof;Username=bauhof_app;Password=..."
  },
  "Identity": {
    "Jwt": {
      "Issuer": "Ordivis.Bauhof",
      "Audience": "Ordivis.Bauhof",
      "Secret": "...mindestens 32 Byte, Base64...",
      "AccessTokenExpiryMinutes": 480
    }
  },
  "Postfach": { "Ordner": "D:\\Bauhof\\Protokolleingang", "TaktSekunden": 60,
"RuhezeitSekunden": 10 },
  "Lueckenwache": { "Aktiv": true, "Uhrzeit": "10:00", "RueckblickTage": 14 },
  "Fristenwache": { "Aktiv": true, "Uhrzeit": "06:30" },
  "Kontrollwache": { "Aktiv": true, "Uhrzeit": "07:00" },
  "Beschaffungswache": { "Aktiv": true, "Uhrzeit": "06:00" },
  "Logging": {
    "LogLevel": {
      "Default": "Information",
      "Microsoft.AspNetCore": "Warning",
      "Microsoft.EntityFrameworkCore.Database.Command": "Warning"
    }
  },
  "AllowedHosts": "*"
}
```

⚠ Diese Datei enthält zwei Geheimnisse — das Datenbankkennwort und das Anmeldegeheimnis. Sie gehört in die Zugriffsrechte des Programmverzeichnisses und **nicht** in eine Dateisicherung, die breiter zugänglich ist als der Server selbst.

Verwandte Themen

- OB-50 · Installation und Server — wo diese Werte beim Einrichten gesetzt werden
- OB-51 · Aktualisierung, Sicherung, Wiederanlauf — welche Werte eine neue Fassung mitbringt oder verlangt
- OB-02 · Systemvoraussetzungen und Architektur — warum es diese Werte gibt — die Architektur dahinter
- OB-60 · Schnittstellen-Referenz — die Schnittstelle, deren Verhalten ein Teil dieser Werte bestimmt

Wachen, Betriebsprotokoll und Störungsbilder

OB-54 Betrieb Die acht Wachen, das Betriebsprotokoll und was hinter den häufigsten Störungsbildern steckt

Beschreibt Vorhandenes

Es gibt zwei Arten, ein Fachverfahren zu betreiben. In der einen ruft jemand an, weil etwas nicht geht, und die Systemadministration beginnt zu suchen. In der anderen weiß die Systemadministration es vorher.

Der Unterschied zwischen beiden sind ein paar Kennzahlen, die regelmäßig abgefragt werden, und ein Protokoll, in dem etwas Lesbares steht. Ordvis Bauhof bringt dafür acht **Wachen** mit — kleine Prüfungen, die der Dienst über sich selbst durchführt und deren Ergebnis abrufbar ist. Sie beantworten nicht die Frage, ob der Dienst läuft, sondern die weit nützlichere, ob er noch tut, wofür er da ist.

Dieses Dokument beschreibt die acht Wachen und ihre Aussage, den Aufbau des Betriebsprotokolls und die häufigsten Störungsbilder mit ihrer tatsächlichen Ursache. ★ Die Liste der Störungsbilder ist bewusst kurz und stammt aus dem Betrieb: Es sind die, die wirklich vorkommen.

INHALT

1 ★★★★★ Warum es Wachen gibt

- 1.1 ⚠️⚠️ Sie verschicken nichts

2 Der Tagesablauf der Wachen

3 Die Wachen im Einzelnen

- 3.1 Zertifikatswache (06:05)
- 3.1 Beschaffungswache (06:00)
- 3.2 Ablesewache (06:15)
- 3.3 Befähigungswache (06:15)
- 3.4 Fristenwache (06:30)
- 3.5 Hochrechnungswache (06:45)
- 3.6 Kontrollwache (07:00)
- 3.7 Lückenwache (10:00)
- 3.8 Postfachannahme (laufend)

4 Das Betriebsprotokoll

- 4.1 Wo es steht
- 4.2 Welche Meldungen wichtig sind
- 4.3 Was nicht im Protokoll steht

5 Störungsbilder

- 5.1 Der Dienst startet nicht
- 5.2 Anmeldung schlägt fehl
- 5.3 Das Portal zeigt Fehler, obwohl es läuft
- 5.4 Datenbank
- 5.5 Winterdienstprotokolle kommen nicht an
- 5.6 Wachen melden nichts

6 Was Sie melden sollten

Verwandte Themen

1 ★ ★ ★ Warum es Wachen gibt

Ordvis Bauhof zeigt Fälligkeiten, Rückstände, Bestandsuntergrenzen und Lücken auf eigenen Seiten. **Alle diese Seiten setzen voraus, dass jemand sie öffnet.**

Merksatz: Genau das ist im Alltag die Bedingung, die als Erstes ausfällt.

Hinweis: **Wache** ☉ ist ein **Hausbegriff von Ordvis** und kein Fachbegriff des Bauhofs — nachschlagen lässt er sich nirgends. Gemeint ist ein Ablauf **innerhalb des Fachdienstes**, der einmal täglich zu fester Uhrzeit eine fachliche Frage prüft und seinen Befund ins Betriebsprotokoll schreibt. Ab- und anschaltbar, Uhrzeit einstellbar — mehr nicht. Das Wort steht wörtlich im Protokoll („*Fristenwache (PRF-05) läuft täglich um 06:30*“), im Konfigurationsabschnitt **Lueckenwache** und auf der Portalseite **Eskalation**; deshalb wird es erklärt und nicht durch ein anderes ersetzt. Ausführlich in OB-01, Abschnitt 4.5.

⚠ **Nicht** die *geplanten Aufgaben* der Ordvis Plattform — dort gibt es dafür eine Maske mit Liste, Schalter und „Jetzt ausführen“. Hier nicht. Und **nicht** die beiden Windows-Dienste: Die Wachen laufen in einem davon.

Deshalb laufen im Fachdienst **acht Wachen**. Sie sehen selbst nach und schreiben, was sie finden, ins Betriebsprotokoll — und dort, wo es fachlich hingehört, zusätzlich in die Akte des betroffenen Gegenstands.

1.1 ⚠ ⚠ Sie verschicken nichts

Keine dieser Wachen versendet E-Mail, SMS oder eine Benachrichtigung.

★ **Der Grund:** Ein Dienst, der Post verschickt, braucht Postfach, Zugangsdaten und Empfängerliste — drei Dinge, die gepflegt werden müssen und genau dann falsch sind, wenn es darauf ankommt. Der Anschluss an eine Benachrichtigungsstrecke gehört an die Stelle, an der es sie gibt (**PEX-10**). Bis dahin ist ein Eintrag, den man nachlesen kann, ehrlicher als eine Mail, von der niemand weiß, ob sie ankam.

Achtung: Für den Betrieb heißt das: Jemand muss ins Protokoll sehen. Ein Bauhof, der Ordvis Bauhof im Alphastand einsetzt, braucht dafür einen benannten Menschen und einen täglichen Takt — sonst laufen die Wachen ins Leere.

2 Der Tagesablauf der Wachen

Uhrzeit	Wache	Paket	Was sie prüft
06:00	Beschaffungswache	LAG-06	Ist ein Meldebestand unterschritten?
06:15	Ablesewache	FUH-06	Welche Zähler laufen rückwärts, springen ungewöhnlich — oder werden gar nicht abgelesen?

Uhrzeit	Wache	Paket	Was sie prüft
06:15	Befähigungswache	DIS-09	Welche Befähigung läuft aus oder ist abgelaufen?
06:30	Fristenwache	PRF-05	Welche Prüfung ist ins Vorlauffenster getreten oder überzogen?
06:45	Hochrechnungswache	PRF-04	Welche zählergeführte Frist wird absehbar fällig?
07:00	Kontrollwache	KTR-11	Welche Kontrolle ist überfällig?
10:00	Lückenwache	WIN-09	Fehlt zu einem eingeteilten Fahrzeug das Winterdienstprotokoll?
laufend	Postfachannahme	WIN-01	Liegen neue Protokolldateien im überwachten Ordner?

★ Die Reihenfolge ist begründet, nicht zufällig:

Jede Wache setzt voraus, was die vorige geklärt hat.

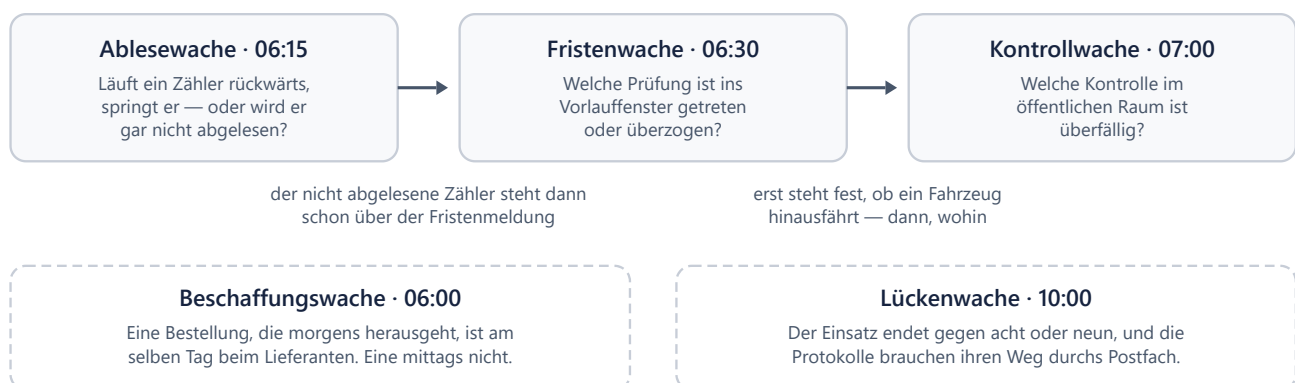


Abbildung 5 — Warum die Wachen in dieser Reihenfolge laufen. Die beiden unteren stehen für sich — ihre Uhrzeit hat einen eigenen Grund.

- **Die Ablesewache läuft vor der Fristenwache.** Meldet die Fristenwache gleich darauf, dass eine zählergeführte Frist *nicht* fällig wird, steht der Grund schon darüber: Der Zähler wurde seit Wochen nicht abgelesen.
- **Die Fristenwache läuft vor der Kontrollwache.** Eine überzogene Hauptuntersuchung entscheidet, ob das Fahrzeug heute überhaupt hinausfährt — die Kontrollgänge entscheiden, wohin.
- **Die Beschaffungswache läuft um sechs.** Eine Bestellung, die morgens herausgeht, ist am selben Tag beim Lieferanten. Eine, die mittags entsteht, ist es nicht.
- **Die Lückenwache läuft erst um zehn.** Ein Winterdiensteinsatz endet gegen acht oder neun, und die Protokolle brauchen ihren Weg durchs Postfach. Um Mitternacht lief die Prüfung über eine Nacht, die noch gar nicht abgeliefert hat — eine Meldung, der man nicht glaubt, ist schlechter als keine.

⚠ Vier der acht Wachen sind **eigene Klassen mit eigenem Schalter und eigener Uhrzeit**, obwohl sie sich einen Zeitgeber teilen könnten. Das ist Absicht: Ein gemeinsamer Zeitgeber spart drei Klassen und kostet die Möglichkeit, das eine ohne das andere abzuschalten.

3 Die Wachen im Einzelnen

3.1 Zertifikatswache (06:05)

Sie sieht täglich nach, ob das TLS-Zertifikat noch trägt — und meldet den Ablauf **mit Vorlauf**.

Abstand zum Ablauf	Was sie meldet
mehr als 30 Tage	nichts
30 bis 8 Tage	einen Hinweis: „läuft am ... ab, in ... Tagen. Ein Ersatz ist zu beantragen“
7 Tage bis zum Ablauftag	eine Warnung: „Ein Ersatz muss JETZT beschafft sein“
abgelaufen	eine Warnung mit der Folge: jeder Aufruf des Portals wird im Browser als unsicher gemeldet

☆☆☆ Ein abgelaufenes Zertifikat ist kein Fehlerzustand des Programms, sondern eine Frist. Es gehört in dieselbe Logik wie jede andere Frist dieses Produkts. Wer es erst merkt, wenn der Browser warnt, hat den Bauhof am Montagmorgen ohne Portal — und dann ruft die Verwaltung an, statt zu arbeiten.

⚠ **Dreißig Tage Vorlauf, und die Zahl hat einen Grund:** Ein Zertifikat der eigenen Verwaltung oder des Landesdienstleisters wird **beantragt** und nicht erzeugt. Zwischen „wir brauchen ein neues“ und „es liegt vor“ liegen in einer Kommune Wochen.

🚫🚫 **Ohne diese Wache fiele der Ablauf durch jedes Raster.** Die Betriebsart wird beim **Start** gelesen; ein Fachdienst, der seit vier Monaten läuft, hat seine einzige Zertifikatsmeldung vor vier Monaten geschrieben.

☆ Sie **lädt neu** und liest nicht den Stand vom Start ab. Wird das Zertifikat im Windows-Speicher von der Verwaltung erneuert, sieht sie es — der Dienst selbst führt bis zum Neustart weiter das alte.

⚠ Im Reverse-Proxy-Betrieb schweigt sie: Dort trägt ein vorgelagerter Proxy das Zertifikat, und über dessen Ablauf weiß dieser Dienst nichts. Eine Wache, die dazu etwas sägte, sägte etwas Erfundenes.

Sie läuft **als erste** — ein ablaufendes Zertifikat betrifft nicht einen Auftrag oder ein Fahrzeug, sondern die Erreichbarkeit des ganzen Portals.

3.1 Beschaffungswache (06:00)

Meldet **einmal** beim Unterschreiten eines Meldebestands und schweigt, solange er unterschritten bleibt. Zurückgesetzt wird erst beim Wiederauffüllen.

☆☆☆ **Der Unterschied zu allen anderen Wachen ist die Hysterese:** Ein Bestand schwankt, eine überfällige Kontrolle nicht. Ohne die Rücksetzung beim Auffüllen schwiege sie beim **zweiten** Absinken — und das ist das, bei dem der Silo wirklich leer wird.

3.2 Ablesewache (06:15)

Drei Prüfungen:

Prüfung	Warum sie zählt
Zähler läuft rückwärts	Deutet auf einen Zählertausch, der nicht erfasst wurde
Ungewöhnlicher Sprung	Ablesefehler oder Zahlendreher
Nie abgelesen	☆☆☆ Ein eigener Zustand und nicht der schlechteste Fall von „lange her“. Wer aus dem Zeitpunkt der letzten Ablesung rechnet, gibt einem Gerät ohne jede Ablesung den besten denkbaren Wert.

⚠ Ein Zähler, den niemand abliest, **sieht aus wie Ordnung**: keine Fehlermeldung, keine rote Zeile, nur eine alte Zahl, mit der weitergerechnet wird.

3.3 Befähigungswache (06:15)

Meldet auslaufende und abgelaufene Befähigungen und Unterweisungen. Siehe OB-31 (Verwaltungshandbuch).

3.4 Fristenwache (06:30)

Meldet jede Prüfung, die ins **Vorlauffenster** getreten ist, wiederholt bei Untätigkeit und meldet an die Leitung bei Überschreitung.

☆☆☆ Die **Staffelung steht nicht in der Wache**. Sie kommt aus dem Vorlauf **je Prüftart** — HU acht Wochen, UVV vier, Ölwechsel zwei — und ist ohne Auslieferung pflegbar. Siehe OB-22 (Verwaltungshandbuch).

3.5 Hochrechnungswache (06:45)

Rechnet aus den Ablesungen hoch, wann eine **zählergeführte** Frist fällig wird.

⚠ ⚠ Sie **nennt keinen Tag, sondern einen Zeitraum** — „in rund 14 Wochen“. Ein Mittelwert aus sieben Ablesungen trägt keine Tagesgenauigkeit, und **wer ein Datum liest, macht danach einen Werkstatttermin**.

☆ Der Grund für diese Wache: Eine Kalenderfrist kündigt sich an; eine Zählerfrist springt von „nicht fällig“ auf „fällig“.

3.6 Kontrollwache (07:00)

Erinnerung nach einer Woche Überzug, Meldung an die Leitung nach vier Wochen. Die Schwellen sind einstellbar.

☆ Sieben Uhr und nicht Mitternacht: Die Meldung soll dort sein, wo die Kolonne sie **vor dem Ausrücken** findet. Um Mitternacht ausgesprochen, wäre sie am Morgen schon eine von gestern.

3.7 Lückenwache (10:00)

Prüft für die letzten **14 Tage**, ob zu jedem eingeteilten Fahrzeug ein Winterdienstprotokoll eingegangen ist.

☆☆☆ **Der gefährlichste Fehler eines Archivs ist die stille Lücke.** Ein fehlendes Protokoll fällt nicht auf — es fällt auf, wenn jemand nach genau dieser Nacht fragt, und dann ist es nicht mehr zu schließen. **Am selben Tag wäre es das gewesen:** Das Gerät hat nicht gesendet, die Datei liegt noch darauf, der Fahrer erinnert sich. Drei Monate später ist die Lücke endgültig.

⚠ **Vierzehn Tage und nicht einer.** Läuft der Dienst über ein Wochenende nicht — Wartung, Neustart, Stromausfall —, fiel die Prüfung sonst für genau die Nächte aus, in denen gefahren wurde.

3.8 Postfachannahme (laufend)

Sieht im Takt von 60 Sekunden im überwachten Ordner nach. Eine Datei wird erst angefasst, wenn sie **10 Sekunden unverändert** ist — eine Datei, die gerade geschrieben wird, ist unvollständig, und eine unvollständig gelesene Signatur ist eine verfälschte.

Ergebnis	Wohin die Datei geht
angenommen	<Ordner>\angenommen
abgewiesen	<Ordner>\abweisung

⚠ **Der Ordner `abweisung` ist ein Warnsignal, kein Ablagefach.** Was dort liegt, ist angekommen und **nicht** übernommen worden. Sehen Sie täglich hinein.

Ohne konfigurierten Ordner beendet sich der Dienst sofort und meldet das — er ist damit auf jeder Installation gefahrlos eingeschaltet.

4 Das Betriebsprotokoll

4.1 Wo es steht

Betriebsart	Wo
Als Windows-Dienst	Ereignisanzeige → Windows-Protokolle → Anwendung, Quelle <code>Ordvis.Bauhof.API</code> bzw. <code>.Portal</code>
Aus der Konsole gestartet	direkt im Fenster

```
# Die letzten 100 Meldungen des Fachdienstes
Get-WinEvent -LogName Application -MaxEvents 500 |
Where-Object ProviderName -like 'Ordvis.Bauhof*' |
Select-Object TimeCreated, LevelDisplayName, Message -First 100
```

4.2 Welche Meldungen wichtig sind

Stufe	Was dort steht
Warnung	Erstzugang mit Kennwort, zurückgesetzter Zugang, Nachbarschaftswarnung, abgewiesene Anmeldungen, unlesbare Uhrzeit einer Wache

Stufe	Was dort steht
Information	Start beider Dienste mit Port und Datenbank, Anmeldungen, Läufe der Wachen und ihre Befunde
Fehler	Fehlende Verbindungszeichenfolge, fehlendes Anmeldegeheimnis, Ausnahmen

★ Zwei Meldungen stehen **absichtlich** als Warnung und mit einem Rahmen aus Gleichheitszeichen: das Erstkennwort und das zurückgesetzte Kennwort. Auf einer Konsole voller Startmeldungen geht eine Information unter — und dieses Kennwort gibt es genau **einmal** zu lesen.

4.3 Was nicht im Protokoll steht

Kennwörter und Prüfwerte	nie, auch nicht vorübergehend
Das Anmeldegeheimnis	nie
Das Datenbankkennwort	wird gelesen, aber nicht ausgegeben
Ein allgemeines Zugriffsprotokoll aller Lesevorgänge	gibt es nicht

5 Störungsbilder

5.1 Der Dienst startet nicht

Meldung	Ursache	Abhilfe
„Keine Datenbankverbindung konfiguriert.“	<code>ConnectionStrings:Bauhof</code> leer	Eintrag in <code>appsettings.Production.json</code> prüfen
„Kein Anmeldegeheimnis konfiguriert.“	<code>Identity:Jwt:Secret</code> leer	Siehe OB-41, Abschnitt 8
„Das Anmeldegeheimnis ... ist zu kurz“	weniger als 32 Byte	längeres Geheimnis setzen
Kein Eintrag, Dienst beendet sich sofort	Arbeitsverzeichnis stimmt nicht	Der Dienst setzt es selbst; tritt nur bei Startversuchen von Hand auf

5.2 Anmeldung schlägt fehl

Bild	Ursache
Alle Anmeldungen scheitern, Protokoll sagt „Kennung ... unbekannt“	Kennung falsch geschrieben — sie wird kleingeschrieben verglichen
Alle Anmeldungen scheitern nach einer Aktualisierung	Anmeldegeheimnis hat sich geändert. ⚠ Der Installer übernimmt es eigentlich — prüfen, ob <code>appsettings.Production.json</code> überschrieben wurde

Bild	Ursache
Token wird sofort abgewiesen	Uhrzeit von Server und Arbeitsplatz weichen ab. Die Prüfung läuft ohne Kulanz (<code>ClockSkew = 0</code>)
Anmeldung scheitert nur im Arbeitsplatzprogramm	Fassungsunterschied. <code>GET /api/version</code> gegen die Fassung des Programms halten
Token öffnet auch die Ordvis Platform (oder umgekehrt)	⚠️ ⚠️ Maschinenweite <code>Identity__Jwt__*</code> -Variablen. Siehe OB-02, Abschnitt 4.1

5.3 Das Portal zeigt Fehler, obwohl es läuft

Bild	Ursache
Jede Fachseite meldet einen Fehler, die Seite selbst lädt	Der Fachdienst läuft nicht. <code>GET /gesundheits</code> prüfen
Seite lädt, reagiert aber auf keinen Klick	WebSockets werden vom Umkehrstellvertreter nicht durchgereicht. Siehe OB-50, Abschnitt 8
Seite ohne Formatierung, Serifenschrift	Statische Dateien fehlen — im Verteilstand nicht zu erwarten
Karte bleibt leer, Linien sind da	Der Kartendienst antwortet nicht. ⭐ Absichtlich kein Fehler: Die Linie ist der Nachweis, die Karte die Lesehilfe

5.4 Datenbank

Bild	Ursache	Abhilfe
<code>column does not exist</code> beim ersten Zugriff	Schema älter als das Modell	<code>schema-abgleich.ps1</code> , siehe OB-51
<code>relation ... does not exist</code>	Tabelle fehlt ganz	dito
Dienst startet, aber jede Liste ist leer	falsche Datenbank in der Verbindungszeichenfolge	Startmeldung lesen — sie nennt Port und Datenbank
<code>permission denied for table</code>	Rolle gehört die Tabelle nicht	Eigentümer prüfen: <code>SELECT tablename, tableowner FROM pg_tables WHERE schemaname='public';</code>

5.5 Winterdienstprotokolle kommen nicht an

Bild	Prüfen
Nichts kommt an	Ist <code>Postfach:Ordner</code> gesetzt? Der Dienst meldet beim Start, wenn nicht.
Dateien bleiben im Eingang liegen	Rechte des Dienstkontos auf den Ordner

Bild	Prüfen
Dateien landen in <code>abweisung</code>	Die Meldung im Protokoll nennt den Grund — meist ein unbekanntes Format
Protokolle tragen „Gerät unbekannt“	Der öffentliche Schlüssel ist nicht angemeldet. Siehe OB-42
Lückenwache meldet Lücken, die keine sind	Läuft sie vor dem Eingang? Uhrzeit prüfen

5.6 Wachen melden nichts

Prüfen	
Steht <code>Aktiv</code> auf <code>false</code> ?	Eine ausgeschaltete Wache meldet das einmal beim Start
Ist die Uhrzeit lesbar?	Eine unlesbare Uhrzeit wird gemeldet, und es gilt die Vorgabe
Lief der Dienst zur fraglichen Uhrzeit?	Ein Neustart um 06:20 überspringt die Beschaffungs- und die Ablesewache dieses Tages

⚠ **Ein Neustart überspringt Wachen.** Jede Wache berechnet beim Start die Zeit bis zu ihrem nächsten Termin. Wer den Dienst morgens um sieben neu startet, hat an diesem Tag keine Fristenmeldung. Für geplante Neustarts ist der Nachmittag die bessere Wahl.

6 Was Sie melden sollten

Findet sich ein Störungsbild hier nicht, gehört es gemeldet — im Alphastand besonders.

Nützlich für die Meldung:

1. Die **Produktfassung** aus `GET /api/version` (oder aus der Fußzeile der Oberfläche)
2. Der **Auszug aus dem Betriebsprotokoll** um den Zeitpunkt herum
3. Was Sie getan haben, was Sie erwartet haben, was geschah
4. Ob die Ordvis Plattform auf demselben Rechner läuft

Meldewege für Schwachstellen: ordvis.eu/produktsicherheit.html

Verwandte Themen

- **OB-40 · Administrationshandbuch** — der Betrieb im Überblick — wann Sie hier überhaupt nachsehen
- **OB-51 · Aktualisierung, Sicherung, Wiederanlauf** — Aktualisierung und Wiederanlauf als häufigste Ursache eines neuen Störungsbildes
- **OB-52 · Konfigurationsreferenz** — die Werte, an denen die Wachen und das Protokoll hängen

Schnittstellen-Referenz

OB-60 Schnittstelle Die REST-Schnittstelle des Fachdienstes – Anmeldung, Konventionen und alle Wege

Beschreibt Vorhandenes

Achtung: Diese Schnittstelle ist im Alphastand nicht stabil. Wege, Felder und Antworten können sich mit jeder Fassung ändern — auch so, dass eine hier beschriebene Anfrage danach anders oder gar nicht mehr beantwortet wird. Wer gegen sie entwickelt, tut das im Wissen darum. Eine Fassungsverwaltung der Schnittstelle (`/v1/`) gibt es **nicht**.

Alles, was Sie in Portal, Arbeitsplatz und App sehen, kommt über dieselbe Schnittstelle. Es gibt keinen zweiten Weg in die Daten und insbesondere keinen, den eine der Oberflächen für sich allein hätte — was diese Referenz zugleich zur vollständigen Beschreibung dessen macht, was das Verfahren kann.

Sie richtet sich an zwei Leser mit sehr verschiedenen Fragen. Der eine baut etwas an: eine Auswertung, eine Übernahme aus einem Altverfahren, eine Anzeige im Rathaus. Der andere sucht einen Fehler und will wissen, was der Aufruf zurückgegeben hat, den die Oberfläche gerade abgesetzt hat.

Dieses Dokument beschreibt zuerst die Konventionen, die für alle Wege gelten — Anmeldung, Token, Fehlerform, Datumsangaben —, und dann die Wege selbst, nach Sachgebieten geordnet. ⚠ Wer nur einen Aufruf sucht, liest trotzdem den Abschnitt über die Anmeldung: Ohne Token antwortet keiner der übrigen Wege.

INHALT

1 Grundlagen

2 Anmelden

2.1 Kennwort wechseln

2.2 Wer bin ich

3 Die vier offenen Wege

4 Antwortkonventionen

5 Die Wege, nach Bereichen

5.1 Dienst und Anmeldung

5.2 Anlagen (Betriebsmittel)

5.3 Prüffristen

5.4 Werkstatt

5.5 Lager und Werkzeug

5.6 Ausgabestation

5.7 Arbeit und Disposition

5.8 Kataster und Kontrolle

5.9 Anordnungen

5.10 Winterdienst

5.11 Geodaten und Adressen

5.12 Personal

5.13 Zeit — ⚠ mit Sperre

5.14 Nachweise

5.15 Betrieb und Auftragsverarbeitung

6 Ein vollständiges Beispiel

7 Was die Schnittstelle nicht hat

Verwandte Themen

1 Grundlagen

Basisadresse	<code>http:// <server>:5100</code>
Datenformat	JSON, UTF-8
Anmeldung	JSON Web Token in der Kopfzeile <code>Authorization: Bearer <token></code>
Fassungsverwaltung	keine
Beschreibungsdatei (OpenAPI)	nicht vorhanden

⚠ **Der Fachdienst spricht HTTP.** Er wird vom Installer nicht in der Firewall geöffnet. Wer ihn im Netz erreichbar macht, stellt TLS davor — siehe OB-50.

⚠ **CORS ist offen** (`AllowAnyOrigin`). Das ist für den Alphastand vertretbar, weil der Dienst nicht im Netz steht. Es ist es nicht mehr, sobald er es tut.

2 Anmelden

```
POST /api/anmeldung
Content-Type: application/json

{ "kennung": "m.mueller", "kennwort": "..." }
```

```
{
  "token": "eyJ...",
  "gueltigBis": "2026-08-28T18:12:44+00:00",
  "anzeigename": "Martina Müller",
  "rolle": "Verwaltung",
  "kennwortwechselFaellig": false
}
```

★ **gueltigBis** ist kein Beiwerk. Ohne diesen Wert müsste jede Oberfläche das Token selbst zerlegen, um zu wissen, wann sie erneuern soll — und ein Zerleger je Oberfläche ist einer zu viel.

⚠ **Es gibt keine Erneuerung.** Nach Ablauf ist neu anzumelden. Behandeln Sie **401** als Aufforderung zur Anmeldung, nicht als Fehler.

⚠ **Alle Fehlschläge nennen denselben Satz.** Unbekannte Kennung, falsches Kennwort und gesperrter Zugang sind nicht zu unterscheiden — siehe OB-41.

2.1 Kennwort wechseln

```
POST /api/anmeldung/kennwort
Authorization: Bearer ...

{ "bisher": "...", "neu": "..." }
```

⚠ **bisher** ist Pflicht, auch bei fälligem Erstwechsel. Ein Token allein darf kein Kennwort setzen können.

2.2 Wer bin ich

```
GET /api/anmeldung/ich
```

3 Die vier offenen Wege

Diese vier Wege brauchen **keine** Anmeldung. Alle anderen brauchen sie — ohne Ausnahme, auch solche, die künftig dazukommen. Begründung in OB-41, Abschnitt 2.

Weg	
GET /gesundheit	„bereit“ oder 503
GET /api/version	Produktfassung

Weg	
POST /api/anmeldung	Anmeldung eines Menschen
POST /api/kiosk/anmeldung	Anmeldung einer Ausgabestation

4 Antwortkonventionen

Kennzahl	Wann
200	Erfolg mit Inhalt
204	Erfolg ohne Inhalt
401	kein oder abgelaufenes Token
403	★ Der Weg existiert und ist gesperrt — etwa die personenscharfe Zeitauswertung
404	Gegenstand nicht vorhanden
422	★ Die Anfrage ist wohlgeformt, es fehlen fachliche Angaben
503	Der Dienst ist nicht bereit

★ ★ **422** und nicht **400** ist die wichtigste dieser Konventionen. Die Antwort trägt dann ein Feld `Maengel` beziehungsweise `Fehlend` — eine Liste mit allen fehlenden Angaben auf einmal:

```
{ "maengel": [
  "Es fehlt die Ausweismarke. Ohne sie hält die Station fest, dass etwas mitgenommen wurde, aber nicht von wem.",
  "Der Stationsschlüssel ist kürzer als 16 Zeichen."
] }
```

★ Wer ein Formular in vier Runden ausfüllen muss, füllt es beim dritten Mal falsch aus.

★ ★ Die Texte sind für Menschen geschrieben und dürfen angezeigt werden. Sie nennen nicht nur *was* fehlt, sondern *warum* es zählt.

5 Die Wege, nach Bereichen

5.1 Dienst und Anmeldung

Weg	
GET	/gesundheit
GET	/api/version
POST	/api/anmeldung

Weg	
POST	/api/anmeldung/kennwort
GET	/api/anmeldung/ich
GET	/api/kennzahlen

5.2 Anlagen (Betriebsmittel)

Weg		Anmerkung
GET	/api/anlagen	Bestand
GET	/api/anlagen/{id}	Akte einer Anlage
POST	/api/anlagen/{id}/ablesung	Zählerablesung
GET	/api/anlagen/{id}/verfuegbarkeit	?person= prüft zusätzlich die Befähigung
POST	/api/anlagen/{id}/ereignis/{kennung}	ereignisgeführte Frist auslösen
POST	/api/anlagen/{id}/schaden	Schadensmeldung
POST	/api/anlagen/{id}/pruefergebnis	Ergebnis einer Prüfung
POST	/api/anlagen/{id}/geraetetyp	Gerätetyp zuordnen
POST	/api/anlagen/sammelaenderung	Sammeländerung
POST	/api/anlagen/uebernahme	Bestandsübernahme
GET	/api/anlagenklassen , /api/anlagenklassen/{kuerzel}	Klassenkatalog
GET	/api/montagen	?stichtag= — ★ die zeitbezogene Beziehung
POST	/api/montagen , /api/montagen/{id}/abbau	
GET · PUT	/api/anlagen/{id}/halterpflichten	Zulassung, Versicherung, Steuer, Plakette, Fahrtenschreiber, ADR — ⚠ je Art genau eine
GET	/api/halterpflichten/fristen	alle ablaufenden Halterpflichten über den ganzen Bestand, mit Empfänger je Art
GET · POST	/api/anlagen/{id}/kosten	die Kostenposten einer Anlage
GET	/api/anlagen/{id}/vollkosten	Kosten je Betriebsstunde — ⚠ nie ohne die Liste der fehlenden Kostenarten
GET	/api/anlagen/{id}/ausfallzeit	die vier Anteile des Stillstands, mit ihren Vorbehalten

5.3 Prüffristen

Weg		Anmerkung
GET	/api/fristen	alle Fristen mit Zustand
POST	/api/fristen	Frist anlegen
POST	/api/fristen/{id}/erledigung	Prüfung als erledigt melden
POST	/api/fristen/{id}/uebersteuerung	befristete Übersteuerung einer Sperre
GET	/api/fristen/vorschau	Hochrechnung zählergeführter Fristen
GET	/api/fristenalarm	was ins Vorlauffenster getreten ist
GET	/api/pruefarten	?auchStillgelegte=true
POST · PUT	/api/pruefarten , /api/pruefarten/{id}	
POST	/api/pruefarten/{id}/stilllegen , /wiederaufnehmen	⚠ stillgelegt, nicht gelöscht
GET	/api/pruefquote	?von=&bis=
GET	/api/ablesungen/faellig	★ „nie abgelesen" ist ein eigener Zustand
GET · POST	/api/pruefkatalog	Katalogpunkte je Prüfert
GET · POST	/api/pruefprotokolle	
POST	/api/pruefprotokolle/{id}/punkte/{punktId}	einzelnen Punkt bewerten
POST	/api/pruefprotokolle/{id}/abschluss	
GET · POST	/api/bescheinigungen	?anlage=
GET	/api/bescheinigungen/{id}/datei	die hinterlegte Datei
GET · POST	/api/geraetetypen , /api/vorlagenpositionen , /api/fristausnahmen	Vorlagen
POST	/api/geraetetypen/{id}/anwenden	Vorlage auf den Bestand anwenden
GET	/api/geraetetypen/{id}/vorlage	die Positionen des Wartungsplans zu einem Gerätetyp
GET · POST	/api/uebernahme , /api/uebernahme/zurueckstellen	Fristenübernahme

5.4 Werkstatt

Weg	
GET	/api/werkstatt (?offen=true), /api/werkstatt/annahme
POST	/api/werkstatt/{id}/annehmen , /einordnen , /zusammenfassen
POST	/api/werkstatt/{id}/freigabe
GET	/api/werkstatt/stillstand — Ausfallzeiten, in vier Anteile zerlegt
GET	/api/wiederholschaeden (?anlage=) — dasselbe Bauteil dreimal in zwölf Monaten

5.5 Lager und Werkzeug

Weg		Anmerkung
GET	/api/lager	Bestand — ★ Summe der Bewegungen, kein fortgeschriebenes Feld
GET · POST	/api/lager/orte , /api/lager/artikel	
GET	/api/lager/artikel/{id}	?lagerort=
POST	/api/lager/buchungen	Zu- und Abgang
POST	/api/lager/buchungen/{id}/gegenbuchung	★ Gegenbuchung statt Änderung
POST	/api/lager/peilung	gemessener Bestand gegen den gebuchten
GET	/api/auftraege/{id}/material	
GET · POST	/api/beschaffung , /api/beschaffung/grenzen	Meldebestände
GET	/api/beschaffung/protokoll	?hoechstens=
GET · POST	/api/werkzeug/ausleihen	?alle=true
POST	/api/werkzeug/ausleihen/{id}/rueckgabe	

5.6 Ausgabestation

Weg		Token
POST	/api/kiosk/anmeldung	offen
POST	/api/kiosk/ausgabe , /api/kiosk/rueckgabe	nur Stationstoken
GET · POST	/api/kiosk/stationen , /api/kiosk/marken	nur Benutzertoken
POST	/api/kiosk/stationen/{id}/stilllegen	nur Benutzertoken

⚠ Ein Stationstoken wird überall sonst zurückgewiesen — siehe OB-42.

5.7 Arbeit und Disposition

Weg	
GET	/api/auftraege (?tag=), /api/rueckstand , /api/tagesuebersicht
POST	/api/auftraege/{id}/dringlichkeit , /hindernis , /abschluss
POST	/api/umplanung
GET · POST	/api/abwesenheiten
GET	/api/eskalation , /api/eskalation/protokoll

5.8 Kataster und Kontrolle

Weg	
GET	/api/kataster (?klasse=&zustand=), /api/kataster/faelligkeit
POST	/api/kataster , /api/kataster/{id}/mangel
GET	/api/kataster/{id}/historie
GET	/api/kontrollgaenge (?zustand=), /api/kontrollgaenge/{id}
POST	/api/kontrollgaenge/plan , /{id}/zuweisung , /{id}/punkte/{punktId} , /{id}/abschluss , /{id}/abbruch
GET	/api/objektklassen , /api/objektklassen/{kuerzel} , /api/objektklassen/maengelkatalog
GET	/api/kontrollplan/arten , /api/kontrollplan/mangelfolge
GET	/api/kataster/strasse — die Objekte an einer Straße
GET	/api/kataster/{id}/standort , /api/kataster/{id}/verlauf — Ort und Ortswechsel

5.9 Anordnungen

Weg	
GET	/api/anordnungen (?zustand=), /api/anordnungen/{id}
POST	/api/anordnungen , /{id}/zustand , /{id}/beauftragen
GET	/api/anordnungen/{id}/vollzug — die Vollzugsmeldung als PDF
GET	/api/anordnungen/fristen , /api/anordnungen/fristen/protokoll
POST	/api/anordnungen/fristen/lauf — stößt den Lauf der Ausführungsfristen an

5.10 Winterdienst

Weg		Anmerkung
GET · POST	/api/winterdienst	?von=&bis=&fahrzeug= · POST nimmt eine Protokolldatei entgegen
GET	/api/winterdienst/{id}/fahrtpunkte , /verbrauch , /urschrift	★ Urschrift = die Datei, wie sie ankam
POST	/api/winterdienst/{id}/vermerk	
GET · POST	/api/winterdienst/einsaetze , /{id}/ende	
GET	/api/winterdienst/einsaetze/{id}/verbrauch , /abgleich	
POST	/api/winterdienst/einsaetze/{id}/abweichungen	
GET	/api/winterdienst/einsaetze/{id}/routen/{kuerzel}/bild	
GET · POST	/api/winterdienst/routen , /routen/datei	Prioritätenplan
GET	/api/winterdienst/luecken (?seit=)	fehlende Protokolle
GET	/api/winterdienst/saison , /saison/bereitschaft	
GET	/api/winterdienst/auskunft	die Auskunft im Schadensfall
GET	/api/winterdienst/aufbewahrung	⚠ nennt nur, was löschreif wäre
GET · POST	/api/protokollgeraete , /{id}/stillegung , /uebersicht	Gerätesignaturen

5.11 Geodaten und Adressen

Weg	
GET	/api/gis/netz , /api/gis/netz.geojson , /api/gis/kataster.geojson , /api/gis/abbildung
POST	/api/gis/netz
GET	/api/koordinaten/utm32 , /api/koordinaten/wgs84
GET · POST	/api/adressen , /api/adressen/suche , /api/adressen/naechste
GET	/api/gis/umkreis — was in einem Umkreis liegt

5.12 Personal

Weg	
GET · POST	/api/befaehigungsarten , /api/befaehigungen (?person=)
POST	/api/anlagen/{id}/befaehigung

5.13 Zeit — ⚠ mit Sperre

Weg		Anmerkung
GET	/api/zeit/auswertung	?von=&bis=&umfang=&mindestbesetzung= — zusammengefasst, für jeden Angemeldeten
GET	/api/zeit/person/{person}	⚠ 403, wenn weder Selbstauskunft noch Freigabe. Jeder Abruf wird protokolliert — auch der abgewiesene
GET · POST	/api/zeit/freigaben	Auswertungsfreigaben
GET	/api/zeit/protokoll	?hoechstens=
GET · POST	/api/zeit/buchungen	Buchungen lesen und anlegen
POST	/api/zeit/buchungen/{id}/anhalten , /{id}/korrektur	⚠ eine bestätigte Buchung korrigiert nur Leitung oder Verwaltung — und es entsteht ein Korrekturereintrag
GET	/api/zeit/korrekturen/offen	Korrekturen, die der betroffenen Person noch mitzuteilen sind
POST	/api/zeit/korrekturen/{id}/mitgeteilt	★ eine Korrektur an fremder Zeit ist erst vollständig, wenn sie mitgeteilt wurde
GET	/api/zeit/tag , /api/zeit/anlage/{id}	der Tag einer Person, die Zeiten an einer Anlage
POST	/api/zeit/tag/abschluss	Tagesabschluss

⚠ ⚠ Diese Wege gibt es, die Zeiterfassung ist aber nicht in Betrieb. Sie steht hinter der Dienstvereinbarung mit der Personalvertretung und der Entscheidung über das Finanzverfahren. Wer sie anspricht, spricht eine Schnittstelle an, deren fachlicher Betrieb noch nicht freigegeben ist — Näheres im Verwaltungshandbuch, OB-33.

5.14 Nachweise

Weg	
GET	/api/berichte/bestand , /api/berichte/kontrollen , /api/berichte/maengel
GET · POST	/api/nachweise — POST stellt eine Fassung aus; ohne Kettenbezug beginnt sie eine neue Kette

Weg	
GET	/api/nachweise/{id} — eine einzelne Fassung
GET	/api/nachweise/kette/{id} — alle Fassungen, mit Prüfung auf Lücken und Doppelungen
GET	/api/nachweise/leistung — der Leistungsnachweis
GET · PUT	/api/briefkopf — der kommunale Briefkopf, den jede PDF-Ausgabe trägt
DELETE	/api/briefkopf/bild — ⚠ ohne Wappen bleibt der Briefkopf leer ; es rückt kein Herstellerzeichen nach

5.15 Betrieb und Auftragsverarbeitung

Weg		Anmerkung
GET · POST	/api/wartungszugriffe	Wartungszugang anfordern und einsehen — namentlich, mit Anlass, höchstens acht Stunden
POST	/api/wartungszugriffe/{id}/freigabe	⚠ eigene Berechtigungsregel. Die Frist läuft ab der Freigabe , nicht ab der Anforderung
GET · POST	/api/stoerungsbestaende	was bei der Störungsbearbeitung an Kopien entstand, mit Ablaufdatum je Art
POST	/api/stoerungsbestaende/{id}/loeschung	★ mit Prüfsumme von außen — der Bestand liegt beim Auftragsverarbeiter. Fehlt sie, wird die Meldung angenommen und sagt es

★ ★ Diese beiden Bereiche sind der technische Unterbau dessen, was das Verwaltungshandbuch in OB-32 aus Sicht des Datenschutzes beschreibt.

6 Ein vollständiges Beispiel

```
# 1. Anmelden
TOKEN=$(curl -s -X POST http://localhost:5100/api/anmeldung \
  -H 'Content-Type: application/json' \
  -d '{"kennung":"verwaltung","kennwort":"..."}' | jq -r .token)

# 2. Bestand lesen
curl -s http://localhost:5100/api/anlagen -H "Authorization: Bearer $TOKEN" | jq '.[0]'

# 3. Anbaugeräte an einem Stichtag
curl -s "http://localhost:5100/api/montagen?stichtag=2026-01-14" \
  -H "Authorization: Bearer $TOKEN" | jq
```

7 Was die Schnittstelle nicht hat

Fehlt	Anmerkung
OpenAPI-Beschreibung	Keine <code>swagger.json</code> , keine Oberfläche zum Ausprobieren
Fassungsverwaltung (<code>/v1/</code>)	Eine Änderung trifft jeden Aufrufer sofort
Seitenweises Lesen	Listen werden vollständig geliefert
Sortier- und Filterparameter außer den genannten	
Ereignisse, Rückrufe, Datenstrom	Es gibt kein Abonnement auf Änderungen
Massenimport-Wege	Bis auf Bestands- und Fristenübernahme sowie Adress- und Netzeinlesen
Durchgängige Mengenbegrenzung	Kein Schutz gegen zu viele Anfragen

⚠ **Die letzte Zeile ist für eine Integration die wichtigste.** Es gibt weder eine Anfragenbegrenzung noch eine Anmeldesperre nach Fehlversuchen. Eine Integration, die in einer Schleife abfragt, kann den Fachdienst belasten, ohne dass etwas eingreift.

Verwandte Themen

- **OB-02 · Systemvoraussetzungen und Architektur** — wer diese Schnittstelle ruft und wo sie in der Architektur steht
- **OB-41 · Benutzer, Rollen und Zugang** — Anmeldung und Token — die Voraussetzung jedes Aufrufs
- **OB-42 · Ausgabestationen und Fahrzeuggeräte** — die Gerätetoken und die Wege, die nur sie öffnen
- **OB-52 · Konfigurationsreferenz** — die Werte, die Adresse, Laufzeit und Grenzen der Schnittstelle setzen

Glossar und Rechtsgrundlagen

OB-90 Glossar Begriffe, Abkürzungen, Rechtsgrundlagen und die Kennungen der Arbeitspakete

Beschreibt Vorhandenes

Ein Handbuch, das Begriffe erklärt, hat sie vorher benutzt. Dieses Verzeichnis ist deshalb kein Anhang im Sinne von „was übrig blieb“, sondern der Ort, an dem nachgeschlagen wird, während man in einem anderen Kapitel liest.

Es führt drei Arten von Einträgen, und die Unterscheidung ist wichtiger, als sie aussieht. **Fachbegriffe** stammen aus dem Bauhofwesen und stehen hier, weil ein Verwaltungsleser sie nicht kennen muss. **Rechtsbegriffe** stammen aus Vorschriften und werden mit ihrer Fundstelle genannt, damit man nachlesen kann statt zu glauben. **Hausbegriffe** hat Ordvis Bauhof selbst geprägt — sie sind als solche gekennzeichnet, denn ein Wort, das nur in diesem Verfahren so gebraucht wird, darf nicht wie ein allgemein üblicher Fachbegriff aussehen.

Dazu die Kennungen der Arbeitspakete, die im Werk als Verweise auftauchen: Sie sagen, welcher Teil des Produkts einen beschriebenen Sachverhalt trägt — und bei einem noch nicht gebauten Teil, worauf er wartet.

INHALT

- 1 Begriffe des Verfahrens
- 2 Technische Begriffe
- 3 Rechtsgrundlagen
 - 3.1 Fahrzeuge und Geräte
 - 3.2 Straße und Verkehr
 - 3.3 Personal und Daten
 - 3.4 Haushalt und Aufbewahrung
- 4 Die Kennungen der Arbeitspakete
- 5 Häufig genannte Pakete
- Verwandte Themen

1 Begriffe des Verfahrens

Hinweis: ☉ **kennzeichnet einen Hausbegriff von Ordvis**. Er gilt nur in diesem Produkt und lässt sich nirgends nachschlagen — Sie finden ihn in keiner Vorschrift und in keinem Verwaltungshandbuch. Begriffe **ohne** dieses Zeichen sind allgemeinsprachlich oder Fachbegriffe der Branche; die lassen sich nachschlagen. Warum diese Unterscheidung getroffen wird, steht in OB-00.

Ablesung

Ein einzelner erfasster Zählerstand mit Ableser, Zeitpunkt und Quelle. ⚠ Ein Zählerstand ist eine **Messreihe**, kein Feld — beim Zählertausch beginnt die Anzeige neu, der Betriebsstundenstand nicht.

Akte ☉

Die Lebenszyklus-Akte einer Anlage: Stammdaten, Zählerstände, Fristen, Schäden, Werkstattaufträge, Montagen, Ereignisse.

Anlage ☉

Ein Betriebsmittel des Bauhofs. Vier Klassen: Fahrzeug, Anbaugerät, Maschine, Kleingerät. Nicht zu verwechseln mit einer *Anlage* im Sinne eines Dokumentanhangs.

Anordnung

Eine verkehrsrechtliche Anordnung nach § 45 StVO. Sie kommt von der Straßenverkehrsbehörde und ist der Eingang in den Prozesskreis.

Arbeitsvorrat

Alle offenen Aufträge mit Alter, Grundlage und — falls vorhanden — Hindernis.

Arbeitsplatz ☉

Das Windows-Programm (`Ordvis.Bauhof.Client`) — die zweite Oberfläche neben dem Portal.

⚠ Nicht der Schreibtisch und nicht der Rechner eines Anwenders. Er darf **schneller** sein als das Portal, nicht **mächtiger** (OB-01).

Auftrag

Die Arbeitseinheit. ★ Es gibt **genau einen** Auftragsbegriff — für Anordnungen, Werkstatt und tägliche Arbeit gleichermaßen.

Auftragszeit

Zeit, die auf einen Auftrag gebucht wird, für die Kosten- und Leistungsrechnung. ⚠ **Nicht Arbeitszeit** — siehe OB-33 (Verwaltungshandbuch).

Ausfallzeit

Die Zeit, in der eine Anlage wegen eines Werkstattauftrags nicht einsatzfähig war. ★ Sie zerfällt in **vier Anteile** — vor der Annahme, auf Teile, bei der Fremdfirma, in Arbeit —, weil die Gesamtzahl allein nicht sagt, woran es lag.

Ausgabestation (Kiosk) ☉

Ein festes Gerät an der Lagertür für die Selbstbedienung. ★ Ein **Erfassungsweg**, kein Anmeldeweg.

Ausweismarke ☉

Eine Nummer, mit der sich jemand an der Ausgabestation ausweist. ⚠ **Kein Konto, kein Kennwort, kein Zugang** — Identifikation, keine Authentifizierung.

Befähigung

Was ein Mensch mitbringen muss, um ein Betriebsmittel zu bedienen: Fahrerlaubnis, Sachkunde, Unterweisung.

Bescheinigung

Der hinterlegte Beleg zu einer Prüfung. ⚠ Eine Frist ohne Bescheinigung ist im Schadensfall wertlos.

Einsatzakte ☉

Die Klammer über eine Winterdienstnacht: Auslösung, Wetterlage, eingeteilte Fahrzeuge, alle Fahrten, Abgleich, Abweichungen, Verbrauch.

Erstbefüllung ☉

Die einmalige Übernahme eines vorhandenen Bestands beim Start — Fahrzeug- und Geräteliste, Fristen, Adressen. ⚠ Nicht zu verwechseln mit dem **Vorführbestand**, den der Fachdienst in eine leere Datenbank legt. Die echte Erstbefüllung (`FUH-16`) ist noch nicht gebaut.

Eskalation

Die automatische Meldung, wenn eine Kontrolle überfällig bleibt — Erinnerung nach einer Woche, Meldung an die Leitung nach vier.

Fachdienst ☉

Der Windows-Dienst `Ordvis.Bauhof.API`. Er trägt die Fachlogik, die Datenbankanbindung und alle acht Wachen.

Frist

Eine Prüfpflicht an einer Anlage. Sie wird fällig **nach Kalender, nach Zählerstand** oder **nach Ereignis**.

Gegenbuchung

Die Korrektur einer Lagerbuchung. ★ Eine falsche Buchung wird **gegengebucht, nicht geändert** — sonst verliert der Bestand die Spur der Korrektur.

Halterpflicht

Eine Pflicht, die den Fahrzeughalter trifft und darüber entscheidet, ob ein Fahrzeug **fahren darf**: Zulassung, Kfz-Haftpflicht, Kfz-Steuer, Feinstaubplakette, Fahrtschreiber, ADR-Ausrüstung. ⚠ Nicht zu verwechseln mit der **Prüffrist**, die sagt, ob es technisch in Ordnung ist. Zwei der sechs sperren den Einsatz, vier nicht.

Hindernis ☉

Der Grund, aus dem ein Auftrag nicht ausgeführt werden kann. ⚠ Kein Abschluss — der Auftrag bleibt offen und das Hindernis erklärt, warum er alt ist.

Kataster

Der Bestand der Ausstattung im öffentlichen Raum — Verkehrszeichen, Anlagen, Ausstattung.

Kontrollgang

Ein geplanter Lauf über fällige Katasterobjekte. ★ **Der Lauf ist der Nachweis**, nicht die einzelne Feststellung.

Meldebestand

Die Untergrenze eines Lagerbestands. ★ Beim Streugut **saisonal** — im November ist ein halb voller Silo ein Alarm, im März nicht.

Montage

Die zeitbezogene Beziehung zwischen Träger und Anbaugerät. ★ Sie beantwortet nicht „*was hängt daran*“, sondern „*was hing am 14. Januar daran*“.

Nachweiskette ☉

Alle Fassungen eines Nachweises in ihrer Reihenfolge. ⚠ Eine Fassungsnummer ohne ihre Vorfassungen belegt nur, dass es sie einmal gab — deshalb prüft die Kette auf Lücken und Doppelungen. Ein **Nachdruck** ist keine neue Fassung.

Peilung

Der gemessene Bestand beim Schüttgut, gehalten gegen den gebuchten.

Portal ☉

Der Windows-Dienst `Ordvis.Bauhof.Portal` — die Weboberfläche.

Prioritätenplan

Die Festlegung, welche Straßen in welcher Priorität geräumt und gestreut werden. ⚠ Ein **Rechtsdokument, kein Fahrplan**.

Protokollgerät ☉

Ein Fahrzeuggerät, dessen öffentlicher Signaturschlüssel angemeldet ist. ⚠ Ein Schlüssel wird **angemeldet** und nie beim ersten Protokoll übernommen.

Prüfart

Ein Stammdatum: Bezeichnung, Rechtsgrundlage, Intervall, Vorlaufzeit, Prüferqualifikation.

Stand ☉ (*eines Handbuchdokuments*)

gebaut , teilweise oder geplant . Siehe OB-00.

Stationsschlüssel ☉

Das Geheimnis, mit dem sich eine Ausgabestation anmeldet. ⚠️ Mindestens 16 Zeichen; er wird einmal vergeben und jahrelang nicht gewechselt.

Störungsbestand ☉

Eine Kopie, die bei der Bearbeitung einer Störung beim Auftragsverarbeiter entsteht — Unterstützungspaket, Protokollauszug, Bildschirmfoto oder Datenbankkopie. Jede trägt ein Ablaufdatum. ⚠️ Der Befund, auf den es ankommt, ist eine Kopie **ohne** Ablaufdatum.

Übersteuerung ☉

Die **befristete** Aufhebung einer Sperre wegen abgelaufener Frist, mit Begründung. ⚠️ Sie läuft ab; eine unbefristete wäre dasselbe wie keine Sperre.

Urschrift

Die Winterdienstprotokolldatei, **wie sie ankam**. ★ Der eigentliche Nachweis; alles andere ist Darstellung.

Vollkosten

Alle Kosten einer Anlage, auf die Betriebsstunde gerechnet — Abschreibung, Kraftstoff, Versicherung, Steuer, Werkstatt eigen und fremd, Ersatzteile, Prüfkosten. ⚠️ Die Zahl wird nie ohne die Liste der Kostenarten ausgegeben, die **fehlen**: Eine Vollkostenzahl mit einer fehlenden Art sieht aus wie eine vollständige.

Vollzugsmeldung

Die Rückmeldung an die anordnende Behörde: Anordnungsbezug, Ausführungsdatum, Beleg.

Vorlaufzeit

Wie früh sich eine Frist meldet. HU acht Wochen, UVV vier, Ölwechsel zwei. ★ Je Prüfer pflegbar, ohne Programmänderung.

Wache ☉

Ein Ablauf **innerhalb des Fachdienstes**, der einmal täglich zu fester Uhrzeit eine fachliche Frage prüft und seinen Befund ins Betriebsprotokoll schreibt. Acht Stück; die Liste steht in OB-54 (Administratorhandbuch). Ab- und anschaltbar, Uhrzeit einstellbar — mehr nicht.

⚠️ **Ein reines Ordvis-Wort**. Es stammt aus dem Programm und nicht aus der Fachsprache des Bauhofs, steht aber wörtlich im Betriebsprotokoll, im Konfigurationsabschnitt **Lueckenwache** und auf der Portalseite **Eskalation** — deshalb wird es erklärt und nicht ersetzt.

⚠️ **Nicht** die *geplanten Aufgaben* der Ordvis Plattform (dort eine Maske mit „Jetzt ausführen“), **nicht** die Windows-Aufgabenplanung und **nicht** die beiden Windows-Dienste.

⚠️ Alle Wachen **melden ins Betriebsprotokoll und verschicken nichts**.

Wartungszugang ☉

Ein befristeter, namentlicher und von der Kommune freigegebener Zugriff des Herstellers auf die Anlage — der Fall, in dem er zum Auftragsverarbeiter wird. ★ Höchstens acht Stunden, und die Frist läuft ab der **Freigabe**, nicht ab der Anforderung.

Wiederholschaden ☉

Dasselbe Bauteil zum dritten Mal innerhalb von zwölf Monaten. ★ Tritt es an mehreren Fahrzeugen **desselben Typs** auf, ist es kein Schaden mehr, sondern ein Konstruktions- oder Bedienungsproblem — mit einer anderen Folge.

Zustandsautomat ☉

Der feste Ablauf, dem der Zustand einer Anlage folgt. ★ Von Hand kommt man am Beleg nicht vorbei.

2 Technische Begriffe

Begriff	Bedeutung
Argon2	Das Verfahren, mit dem Kennwörter und Stationsschlüssel abgelegt werden. Dasselbe wie in der Ordvis Plattform
Blazor Server	Die Technik des Portals. Hält eine stehende Verbindung zum Server
EnsureCreated	Legt das Datenbankschema aus dem Modell an. ⚠ Nur in einer leeren Datenbank — siehe OB-51 (Administratorhandbuch)
GeoJSON	Austauschformat für Geodaten
JWT	JSON Web Token — der Ausweis, den die Anmeldung ausstellt. Gültig acht Stunden
Npgsql	Die Datenbankanbindung an PostgreSQL
PostgreSQL	Die Datenbank. Der Server wird mit der Ordvis Plattform geteilt, die Datenbank nicht
Rückfallregel ☉	Die Regel, die an jedem Endpunkt einen angemeldeten Benutzer verlangt — auch an einem, der morgen dazukommt
UTM Zone 32	Das Koordinatensystem der Vermessung in Deutschland
WGS 84	Das Koordinatensystem der Satellitenortung — Breite und Länge
WinUI 3	Die Technik des Windows-Arbeitsplatzes

3 Rechtsgrundlagen

Achtung: Kein Rechtsrat. Die folgenden Angaben sind eine fachliche Einordnung. Intervalle, Prüferqualifikation, Nachweis- und Aufbewahrungspflichten sind vor dem Wirksamwerden mit dem Unfallversicherungsträger, der Rechtsaufsicht, der Kämmerei und einer fachkundigen Stelle abzugleichen. Im Alphanstand gilt das besonders.

3.1 Fahrzeuge und Geräte

Grundlage	Gegenstand
§ 29 StVZO	Hauptuntersuchung (HU) und Sicherheitsprüfung (SP)

Grundlage	Gegenstand
DGUV Vorschrift 70	Prüfung von Fahrzeugen
§ 14 BetrSichV	Wiederkehrende Prüfung überwachungsbedürftiger Anlagen
DGUV Vorschrift 3	Prüfung elektrischer Betriebsmittel
DGUV Regel 100-500	Arbeitsmittel, u. a. Motorsägen
Herstellervorgaben	Wartungsintervalle

3.2 Straße und Verkehr

Grundlage	Gegenstand
§ 45 StVO	Verkehrsrechtliche Anordnungen
Verkehrssicherungspflicht	Der Maßstab für Kontrolle und Mängelbeseitigung
Landesstraßengesetz	Räum- und Streupflicht; Beschränkung auf verkehrswichtige und gefährliche Stellen und auf das Zumutbare
Kommunale Satzung	Übertragung der Räum- und Streupflicht auf Anlieger, soweit erfolgt

3.3 Personal und Daten

Grundlage	Gegenstand
DSGVO	Verarbeitung personenbezogener Daten, Betroffenenrechte, Verzeichnis nach Art. 30, Folgenabschätzung nach Art. 35
§ 26 BDSG und Landesdatenschutzgesetz	Beschäftigtendatenschutz
§ 74 HPVG (bzw. entsprechende Landesvorschrift)	Mitbestimmung bei technischen Einrichtungen, die zur Überwachung geeignet sind
BITV 2.0	Barrierefreiheit — der Grund für die Hausregel „Was der Arbeitsplatz kann, muss das Portal auch können“

3.4 Haushalt und Aufbewahrung

Grundlage	Gegenstand
Gemeindehaushaltsverordnung	Kosten- und Leistungsrechnung
Kommunalabgabengesetz	Gebührenrelevante Leistungen, z. B. Straßenreinigung
Kommunale Aktenordnung	Aufbewahrungsfristen

4 Die Kennungen der Arbeitspakete

Kennungen wie **PRF-09** stehen an vielen Stellen im Programm und in diesem Handbuch. Sie benennen ein Arbeitspaket der Projektplanung.

Kürzel	Cluster
BET	Betrieb, Installation, Koexistenz, Zugang
BUE	Bürgermeldungen (<i>optional</i>)
CV	Bilderkennung
DIS	Disposition und Einsatzplanung
DSF	Datenschutz und Beschäftigtendatenschutz
ENT	Grundsatzentscheidungen des Produkts
FUH	Fuhrpark und Geräte
INV	Bewegliches Inventar und Aufbauten
ITS	Anordnungen und Prozesskreis
KLA	Objektklassen des Katasters
KTR	Kontrolle
LAG	Lager und Materialwirtschaft
MOB	Außendienst-App
NAW	Nachweise und Berichte
PEX	Übernahme aus der Ordvis Plattform
PRF	Prüffristen und Wartung
STR	Streckenaufnahme
WIN	Winterdienst und Straßenreinigung
WRK	Werkstatt und Schadensmanagement
WUI	Windows-Arbeitsplatz
ZEI	Zeiterfassung und Kosten-Leistungs-Rechnung

★ **Wozu das gut ist:** Statt „das mit den Fristen“ lässt sich **PRF-04** sagen — im Support, in einer Rückmeldung, in einer Frage an den Hersteller.

5 Häufig genannte Pakete

Kennung	Wofür sie in diesem Handbuch steht
BET-02	Aktualisierungsweg
BET-13	Koexistenz mit der Ordvis Plattform
BET-14	Anmeldung und Zugang
ENT-11	Eigenes Produkt, eigene Datenbank, getrennte Installation
ENT-15	Zielverfahren der Kosten- und Leistungsrechnung
ENT-16	Mitbestimmung des Personalrats
FUH-05 / FUH-06	Zählerstand als Messreihe, Ablesewache
FUH-07	Zeitbezogene Beziehung Träger ↔ Anbaugerät
FUH-16	Erstbefüllung aus dem vorhandenen Bestand
ITS-06	Katasterwirkung eines Auftragsabschlusses
ITS-12	Vollzugsmeldung
KTR-11	Kontrollwache
LAG-01	Bestand als Summe der Bewegungen
LAG-06	Meldebestand mit Saisonprofil
LAG-08	Ausgabestation
PEX-09	Übernahme von Identität und Sicherheit aus der Ordvis Plattform
PEX-10	Benachrichtigungsstrecke
PEX-18	Datenbankmigrationen
PRF-05	Fristenwache
PRF-07	Prüfmangel wird zum Werkstattauftrag
PRF-09	Sperre bei abgelaufener Frist
PRF-14	Ausweis der Anlagen ohne erfasste Frist
WIN-09	Lückenwache
WIN-10	Gerätesignatur
WIN-11	Auskunft im Schadensfall
WRK-10	Freigabe nur mit Beleg
WUI-14	Gleichstand von Portal und Arbeitsplatz
ZEI-14	Auswertungssperre nach Person

Verwandte Themen

- **OB-00 · Übersicht, Lesewege und Dokumentenkarte** — die Dokumentenkarte: welches Dokument welche Frage beantwortet
- **OB-01 · Einführung und Grundlagen** — die Leitideen, aus denen die Hausbegriffe entstanden sind