Ordivis Belegung

ADMINISTRATION

Konten, Rollen und Anmeldung

Ersteinrichtung, die drei Anmeldemodi, Konten der Verwaltung und die Anmeldung der Antragsteller

ALPHA · Fassung 0.9.0

Handbuch-Fassung 1.0 · Stand 29.08.2026

Grams IT · Produktreihe Ordivis · .NET 10 · PostgreSQL · Exchange

ID-41 Identität

© 2026 Grams IT. Ordivis Belegung™ ist ein Erzeugnis der Produktreihe Ordivis. Alle Rechte vorbehalten.

Konten, Rollen und Anmeldung

Achtung: Alpha-Fassung. Ordivis Belegung steht in der Fassung 0.9.0 und ist eine **Alpha-Fassung**. Die Anwendung wird laufend weitergebaut: **Masken, Menüwege, Bezeichnungen, Konfigurationsschlüssel und Abläufe können sich jederzeit und ohne Vorankündigung ändern** — und mit ihnen die Angaben in diesem Handbuch. Dieses Kapitel beschreibt den Stand vom 29.08.2026. Weicht die Anwendung von einer Beschreibung ab, gilt die Anwendung und nicht dieses Blatt; melden Sie die Abweichung. Für den Echtbetrieb ist diese Fassung **nicht freigegeben**.

Es gibt in diesem System **zwei getrennte Anmeldungen**, und sie haben miteinander nichts zu tun:

	Verwaltungsbereich (`/pflege`)	Antragsteller (`/mein-konto`)
Wer	Sachbearbeitung, Verwaltung, Administration	Bürgerinnen, Vereine
Wie	Benutzername + Kennwort **oder** Windows	Link an die eigene Adresse, **kein Kennwort**
Wer legt an	die **Administration**	die Person selbst
Einzustellen	`Sicherheit:Modus`	**nichts**
Sitzung	10 Stunden, gleitend	12 Stunden, gleitend

INHALT

1 · Die drei Rollen

Rolle	Darf
Sachbearbeitung	Vorgänge bearbeiten und entscheiden
Verwaltung	Stammdaten, Zeiten, Entgelte, Trauorte und Schlüssel pflegen
Administration	alles — einschließlich der Konten und der Exchange-Anbindung. **Schließt die beiden anderen ein**, es sind also keine weiteren Haken nötig

© 2026 Grams IT — Ordivis Belegung™

Die vollständige Zuordnung von Seiten und Handlungen zu Rollen steht in **ID-44**.

2 · Modus `Konten` — lokale Konten (Vorgabe)

Benutzername und Kennwort, hier gepflegt. **Kein Active Directory nötig** — und das ist der Grund für diesen Weg: Ein Einrichtungsverantwortlicher ohne AD-Konto (Hausmeister, Ortsvorsteher) bekommt damit einen Zugang, den es sonst nicht gäbe.

Kennwortlänge	mindestens **12 Zeichen**, keine Zeichenklassen
Sperre	nach **5** Fehlversuchen für **15 Minuten**
Sitzung	HttpOnly-Cookie `ordivis.verwaltung`, **10 Stunden**, gleitend
Erstkennwort	ist beim ersten Anmelden zu ändern
Kennwort vergessen	setzt ein Administrator zurück. **Kein Weg über die E-Mail-Adresse**

Länge statt Zeichenklassen ist Absicht (BSI, NIST SP 800-63B): „mindestens ein Sonderzeichen" erzeugt `Kennw0rt!` und sonst nichts. Zwölf Zeichen sind ein Satz, und ein Satz lässt sich merken.
Warum es keinen Weg über die E-Mail-Adresse gibt: Er wäre ein zweites Anmeldeverfahren neben diesem, mit allem, was daran hängt — Postfach, Zustellbarkeit, Marken, Fristen. Für eine Handvoll Konten in einem Haus ist das die falsche Rechnung.

Die Ersteinrichtung

💻 **Verwaltung:** `/pflege/einrichtung` · 🔑 der **Einrichtungsschlüssel**

Beim ersten Start gibt es noch kein Konto. Dann steht die Ersteinrichtung offen — geschützt nicht durch eine Anmeldung, die es noch nicht geben kann, sondern durch einen **Einrichtungsschlüssel**. Die Anwendung erzeugt ihn beim Start und legt ihn an **zwei** Stellen ab:

```
warn: Ordivis.Belegung.Api.Sicherheit.Ersteinrichtung[1710]
      ERSTEINRICHTUNG: Es gibt noch kein Verwaltungskonto. Legen Sie es unter
      /pflege/einrichtung an. Der Einrichtungsschlüssel lautet <…> und steht
      auch in <Pfad>\einrichtung.schluessel.
```

🔒 Pflichtreihenfolge

1. Lesen Sie den Schlüssel aus dem Protokoll oder aus `einrichtung.schluessel`.
2. Rufen Sie `/pflege/einrichtung` auf.
3. Legen Sie das erste Konto an — **es ist Administrator**.
4. Prüfen Sie, dass `einrichtung.schluessel` **verschwunden** ist.

✅ **Ergebnis:** `GET /verwaltung/einrichtung` meldet `"noetig": false`, und der Weg ist für immer zu.

© 2026 Grams IT — Ordivis Belegung™

An beide Stellen kommt nur heran, wer ohnehin auf dem Server ist — der Ausweis der Ersteinrichtung ist der **Zugriff auf die Maschine**.

Achtung: Sobald das erste Konto steht, wird die Datei gelöscht. Eine Datei, die liegen bliebe, wäre ein zweiter Hauptschlüssel, von dem niemand mehr weiß. Prüfen Sie das (ID-55).

Das erste Konto ist Administrator. Alles andere wäre eine Installation, in der niemand Konten anlegen kann.

Voraussetzung bei schreibgeschütztem Anwendungsverzeichnis:
`Sicherheit:Einrichtungsverzeichnis` auf ein beschreibbares Verzeichnis setzen — unter systemd das Zustandsverzeichnis der Einheit:
`Sicherheit__Einrichtungsverzeichnis=/var/lib/ordivis-belegung`
Das ist bei einer ordentlich abgesicherten Installation der Normalfall, nicht die Ausnahme: `ProtectSystem=strict` macht `/opt` schreibgeschützt. Die Anwendung startet auch ohne diese Angabe — der Schlüssel steht dann nur im Protokoll und **gilt nur bis zum nächsten Dienstneustart**.

Ein Konto anlegen

💻 **Nur im Verwaltungsbereich:** *Pflege* ▸ *Konten* · 🔑 Rolle **Administration** — Es gibt bewusst **keine Selbstregistrierung**: In einer Verwaltung entscheidet nicht die Person, ob sie Zugang bekommt.

1. *Konto anlegen* ▸ Benutzername, **Anzeigename**, Rollen.
2. Vergeben Sie ein **Erstkennwort** — mindestens zwölf Zeichen. Es steht absichtlich lesbar in der Maske: Sie müssen es weitergeben können.
3. Übergeben Sie es **persönlich**, nicht per E-Mail.

✅ **Ergebnis:** In der Spalte *Stand* steht `Erstkennwort`, bis die Person es geändert hat. **So lange kennen Sie das Kennwort dieser Person** — und das ist der Grund für den Zwang.

Der Anzeigename steht im Verlauf jeder Entscheidung, nicht der Benutzername. Dort ist „a.muster" eine Kennung und keine Auskunft — schreiben Sie ihn aus.

Wenn jemand das Haus verlässt

Achtung: Außer Betrieb nehmen, nicht löschen. Der Name steht im Verlauf jeder Entscheidung, die die Person getroffen hat; ein gelöschtes Konto machte daraus Einträge ohne Person.

Ein Konto außer Betrieb kann sich nicht mehr anmelden — sein Name im Verlauf bleibt lesbar.

Zwei Dinge lässt die Anwendung nicht zu, und beide aus demselben Grund:

© 2026 Grams IT — Ordivis Belegung™

- **Das eigene Konto außer Betrieb nehmen.** Der schnellste Weg, sich auszusperren — und er sieht bis zum nächsten Anmelden nach nichts aus.
- **Dem letzten Administrator die Rolle nehmen.** Danach könnte niemand mehr Konten verwalten, auch nicht das Konto selbst.

3 · Modus `Windows` — Negotiate/Kerberos gegen das AD

Kein zweites Verzeichnis, kein zweites Kennwort. Die Sachbearbeitung ist am Arbeitsplatz ohnehin angemeldet, und ein eigener Benutzerbestand wäre eine zweite Stelle, an der jemand vergessen wird, wenn er das Haus verlässt.

Schlüssel	Rolle
`Sicherheit:GruppeSachbearbeitung`	Vorgänge entscheiden
`Sicherheit:GruppeVerwaltung`	Stammdaten und Zeitregeln pflegen
`Sicherheit:GruppeAdministration`	alles — und die beiden Rollen oben automatisch mit

Die Gruppennamen dürfen **kurz** stehen (`FB4-Gebaeudemanagement`); verglichen wird auf Endung, weil Windows sie als `INTERN\FB4-Gebaeudemanagement` liefert.

> **Achtung: `Windows` ohne eine einzige Gruppe verhindert den Start.** Anmeldung ohne Berechtigung wäre eine Namensliste — jedes Konto im Haus käme herein, und der einzige Unterschied zu „offen" bestünde darin, dass der Name im Verlauf steht.
>
> **Im Modus `Windows` gewinnt der angemeldete Name.** Er steht im Vorgangsverlauf statt des Feldes aus der Eingabemaske — ein Verlauf, in den jeder einen beliebigen Namen schreiben kann, belegt nichts.

4 · Modus `Offen` — ohne Anmeldung

Wer die Adresse kennt, kommt herein.

> **Achtung: Nur für automatische Prüfungen und für eine Vorführung im Hausnetz.** Niemals ins offene Netz. Die Startmeldung sagt es, und die Seite `/pflege` zeigt einen Hinweis.

`Offen` ist eine Angabe, die jemand **eintragen** muss, und keine, die man stehenlässt: Mit lokalen Konten braucht es keine Domäne mehr, sondern nur die Ersteinrichtung.

5 · Die Anmeldung der Antragsteller

Es gibt dafür keinen Konfigurationsschlüssel. Der Weg ist immer da und hängt nur an zwei Dingen, die ohnehin gesetzt sind: `Traeger:OeffentlicheAdresse` und einem funktionierenden Nachrichtenversand.

© 2026 Grams IT — Ordivis Belegung™

Anmeldelink gültig	**15 Minuten**
Verwendbar	**einmal**; ein neuerer entwertet die älteren
Höchstens ein Link	je Konto und **Minute**
Sitzung	HttpOnly-Cookie, 12 Stunden, gleitend

In der Datenbank steht der Anmeldelink nicht, sondern nur sein Abdruck (SHA-256). Wer die Tabelle lesen kann — eine Sicherung, ein Ausdruck für die Fehlersuche —, bekommt daraus keinen funktionierenden Link.

Achtung: Drei Dinge für die Prüfliste.

1. Die Anmeldung läuft **nur, wo die Anwendung antwortet**. Der öffentliche Teil draußen besteht aus Dateien und einem PHP-Skript und kennt keine Sitzung.
2. Das Sitzungscookie ist außerhalb der Entwicklung als `Secure` gekennzeichnet: **Ohne HTTPS geht die Anmeldung im Betrieb nicht** — und das ist gewollt.
3. Der Anmeldedienst braucht einen **Postausgang**. Ohne ihn ist er gar nicht angemeldet, und die Kontoendpunkte antworten mit **503** und einem Satz, der das sagt.

Was das Konto kann, steht in ID-13 §5.

Nutzerkonto Bund/Land (BundID, Servicekonto Hessen)

Ein zusätzlicher Anmeldeweg, kein Ersatz. Ohne Eintrag ist der Weg aus: kein Anmeldeweg, kein Endpunkt, kein Knopf. Eine Installation, die nichts hinterlegt hat, ist nicht falsch konfiguriert — sie benutzt den Weg nicht.

Bei der Registrierung anzugeben ist der Rückweg:

```
https://buchung.ihre-kommune.de/konto/nutzerkonto/rueckweg
```

`email` **ist Pflicht und keine Kür.** Ohne Adresse lässt sich ein Konto weder anlegen noch zuordnen, und der Anmeldeweg endet mit einer Absage, deren Grund nur im Protokoll steht.

DAS VERTRAUENSNIVEAU — DIE ANGABE, AUF DIE ES ANKOMMT

Ein BundID-Konto lässt sich mit **Benutzername und Kennwort**, mit einem **ELSTER-Zertifikat** oder mit dem **Online-Ausweis** benutzen. Das sind drei sehr verschiedene Dinge, und der Anbieter sagt in jedem Fall, welches es war.

© 2026 Grams IT — Ordivis Belegung™

Erst ab *substanziell* zählt eine Anmeldung als „Nutzerkonto Bund/Land". Eine Anmeldung mit Kennwort belegt, dass jemand ein Konto beim Anbieter führt — **nicht, wer er ist**. Das ist derselbe Nachweis wie eine bestätigte E-Mail-Adresse, nur über ein anderes Postfach; das Konto bleibt deshalb auf *E-Mail bestätigt* stehen. Die Verknüpfung entsteht trotzdem — beim nächsten Mal mit dem Ausweis zählt sie.

Achtung: Die Werte des Anbieters stehen INNEN, nicht als Abschnittsname. Sie sind URNs und tragen Doppelpunkte (`http://eidas.europa.eu/LoA/high`), und in der Konfiguration trennt der Doppelpunkt Abschnitte.

`Nutzerkonto__Niveaus__hoch=http://eidas.europa.eu/LoA/high STORK-QAA-Level-4`

Ein Eintrag ersetzt die Vorgabe für genau dieses Niveau, die übrigen bleiben. **Ein Tippfehler im Abschnittsnamen (`substantiel`) verhindert den Start; ein Tippfehler im Wert fällt nirgends auf** — der Wert gilt dann als *unbekannt* und damit als schwächster Fall. Gleichen Sie die Werte bei der Registrierung gegen die Anbindungsdokumentation des Anbieters ab.

WIE EIN KONTO ZUGEORDNET WIRD

1. **Über die Kennung des Anbieters** (`sub`). Sie ist der Schlüssel — wer dort eine neue E-Mail-Adresse hinterlegt, findet seine Anträge weiterhin.
2. **Sonst über die E-Mail-Adresse** — aber nur, wenn der Anbieter sie als **bestätigt** ausweist.
3. **Sonst wird ein neues Konto angelegt.**

Achtung: Schritt 2 ist die sicherheitskritische Stelle. Ohne die Bedingung wäre der ganze Anmeldeweg eine **Kontoübernahme**: Wer sich beim Anbieter mit der Adresse einer anderen Person registriert, ohne sie belegen zu müssen, bekäme deren Anträge. Ein Anbieter, der zu `email_verified` nichts sagt, gilt als *nicht bestätigt*. Ein **neues** Konto anzulegen bleibt harmlos — es gibt nichts zu übernehmen.

Ein Konto gehört zu einem Nutzerkonto. Zwei Menschen an einem Familienpostfach bekommen nicht dieselbe Ablage: Die zweite Kennung wird abgewiesen, und die Anmeldeseite sagt, was zu tun ist.

6 · Der Datenschlüssel

⚙️ **Am Server:** `Sicherheit:Datenschluessel` · 🔑 Schreibzugriff auf die Konfiguration

32 Byte in Base64:

```
openssl rand -base64 32
```

Damit werden hinterlegte Geheimnisse verschlüsselt — heute das Exchange-Kennwort aus der Maske (ID-42).

© 2026 Grams IT — Ordivis Belegung™

Ohne diesen Schlüssel nimmt die Maske kein Kennwort an, und sie sagt es. Ein eingebauter Ersatzschlüssel wäre keine Verschlüsselung, sondern eine Verzierung — er stünde in jedem Auslieferungspaket dieses Erzeugnisses.

Achtung: Sichern Sie ihn. Geht er verloren, ist ein hinterlegtes Kennwort verloren und muss neu eingetragen werden. Die Anwendung kommt dann **ohne Quelle** hoch und sagt es — sie hängt nicht in einer Neustartschleife (ID-53).

Verschlüsselt wird mit AES-GCM, nicht mit AES-CBC: GCM erkennt eine Veränderung am Geheimtext, CBC entschlüsselt sie zu Unsinn und meldet nichts. Bei einem Kennwort wäre der Unterschied eine `401` gegen eine klare Meldung.

Verwandte Themen

- **ID-40** — Administrationshandbuch: die Schlüssel im Überblick
- **ID-42** — Exchange-Anbindung
- **ID-44** — Rollen- und Rechte-Matrix
- **ID-54** — Datenschutz: die Löschung ungenutzter Konten
- **ID-55** — Prüfliste vor der Freischaltung

© 2026 Grams IT — Ordivis Belegung™