Ordivis

TEIL I · TECHNIK

Systemvoraussetzungen & Architektur

Architektur, Komponenten und Voraussetzungen für Betrieb und Client

Produktversion 2026.08.19 · Handbuch-Revision 1.0
Stand 19.08.2026 · Plattform .NET 10 / Windows Server

ID-02 Architektur

Systemvoraussetzungen & Architektur

Dieses Dokument beschreibt den technischen Aufbau von Ordivis Platform und die Voraussetzungen für Server und Arbeitsplätze. Es richtet sich an **IT-Betrieb** und **Administratoren**. Die konkreten Installationsschritte stehen im Betriebshandbuch (ID-50).

INHALT

1 Architektur im Überblick

Ordivis Platform läuft **nativ auf Windows Server** – **ohne Docker/Container**. Die Plattform besteht aus mehreren Komponenten, die als **Windows-Dienste** betrieben werden:

Komponente	Aufgabe	Betriebsart
Ordivis API	Zentrale Geschäftslogik, REST-Schnittstelle, Authentifizierung, RBAC	Windows-Dienst (Kestrel/HTTPS)
Discovery-Collector	Netzwerk-Inventarisierung und Scans in einem **entfernten Netz** – optional, eigenes Installationspaket	Windows-Dienst auf dem Rechner im Zielnetz
Web-Portal	Blazor-Web-Portal – Selbstbedienung für Endbenutzer **und** vollwertiger Arbeitsplatz für Agenten, Fachanwender und Administratoren (Port 8080)	Windows-Dienst
PostgreSQL	Datenhaltung (relationale Datenbank)	Nativer Dienst
WinUI-Client	Desktop-Arbeitsoberfläche (unpackaged)	Desktop-App je Arbeitsplatz

Abbildung 1 zeigt, wie diese Komponenten zusammenhängen und in welche Richtung die Verbindungen aufgebaut werden.

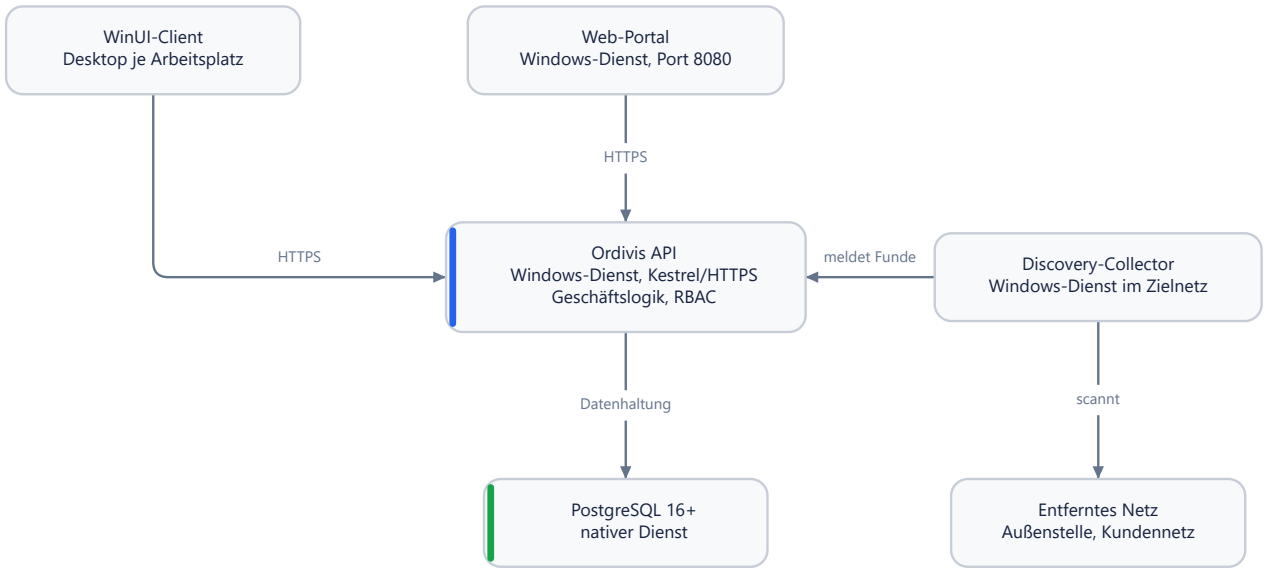

Abb. 1 – Komponenten und ihre Verbindungen. Der Collector im entfernten Netz ruft in der Zentrale an, nicht umgekehrt.

Der modulare Aufbau folgt einer **Clean-Architecture** je Modul (Domain, Application, Infrastructure, Api). Alle Module teilen sich eine Datenbank; die Trennung erfolgt logisch über Mandanten und Berechtigungen.

2 Software-Plattform

- **Laufzeit:** .NET 10 (alle Server-Komponenten und der Client).
- **Datenbank:** PostgreSQL 16 oder neuer (empfohlen 18).
- **Betriebssystem Server:** Windows Server 2022 / 2025.
- **Client-Betriebssystem:** Windows 11 (empfohlen). Windows 10 (ab 19041) ist technisch lauffähig, wird aber **nicht empfohlen** (siehe EOL-Hinweis unten).

3 Voraussetzungen – Server

Ressource	Minimum	Empfohlen
CPU	4 Kerne	8 Kerne
Arbeitsspeicher	8 GB	16 GB+
Datenträger	50 GB SSD	100 GB+ SSD (getrennt für DB)
Netzwerk	1 GbE, fester Hostname (FQDN)	1 GbE, DNS + gültiges TLS-Zertifikat
Zusätzlich	VC++-Runtime (für PostgreSQL-Installer)	Interne Root-CA im Vertrauensspeicher

Voraussetzung: Der PostgreSQL-Installer benötigt die Option `--install_runtimes 1`, sonst scheitert die Installation auf frischen Servern an fehlender VC++-Runtime.

Wichtig – statische MAC-Adresse (Lizenzbindung): Die Produktaktivierung bindet die Lizenz an einen Hardware-Fingerprint, der u. a. die MAC-Adresse der primären Netzwerkkarte einbezieht. In **virtuellen Maschinen** muss die MAC-Adresse der primären vNIC daher **statisch** konfiguriert sein (feste/„static" MAC in Hyper-V, VMware, Proxmox o. ä.). Eine **dynamische MAC**, die sich beim Neustart oder bei einer Migration ändert, führt sonst zu einer fälschlichen Aktivierungssperre („Manipulation erkannt"). Reine Host-Adapter (Hyper-V Default Switch, VPN/TAP, WSL/Docker-Bridges) werden nicht herangezogen und dürfen wechseln. Details siehe ID-43.

4 Voraussetzungen – Arbeitsplatz (Client)

Ressource	Wert
Betriebssystem	**Windows 11** (empfohlen); Windows 10 (19041+) technisch lauffähig, aber EOL
Arbeitsspeicher	4 GB+
Bildschirm	1440×900 oder höher empfohlen
Netzwerk	HTTPS-Erreichbarkeit der API
Zusätzlich	WebView2-Runtime (für grafische BPMN-Darstellung)

Das Self-Service-Portal benötigt am Endbenutzer-Arbeitsplatz nur einen **aktuellen Browser** (Edge, Chrome, Firefox) – keine Installation.

Achtung – Betriebssystem-Lebenszyklus (EOL): Betriebssysteme haben ein Support-Ende (End of Life). **Windows 10 hat am 14. Oktober 2025 sein End-of-Support erreicht** und erhält keine Sicherheitsupdates mehr. Ordivis Platform läuft technisch weiterhin auf Windows 10, der Einsatz wird jedoch **ausdrücklich nicht empfohlen**. Betreiben Sie Clients auf **Windows 11**.

Hinweis: Prüfen Sie auch für **Server** und **PostgreSQL** regelmäßig den Support-Zeitraum. Setzen Sie nur Versionen ein, die noch Sicherheitsupdates erhalten (z. B. Windows Server 2022/2025, aktuell gepflegte PostgreSQL-Hauptversionen). EOL-Systeme sind ein Sicherheits- und Compliance-Risiko.

5 Netzwerk & Ports

Von	Nach	Port	Zweck
Client / Portal	API	443 (HTTPS)	REST-Zugriff
Browser	Portal	8080 (HTTPS)	Self-Service
API	PostgreSQL	5432	Datenbank
API	Mail-Server	587 (STARTTLS) / 993 (IMAPS)	Versand / Eingang

Von	Nach	Port	Zweck
API	Zielsysteme	135/445 (WMI), 22 (SSH), 161 (SNMP), 389/636 (LDAP)	Discovery-Scan (serverseitig)
Discovery-Collector	Zielsysteme im Standortnetz	135/445 (WMI), 22 (SSH), 161 (SNMP), 389/636 (LDAP)	Discovery-Scan vor Ort
Discovery-Collector	API	443 (HTTPS)	Funde melden – die Verbindung geht **immer vom Standort aus**

> **Es gibt keinen eigenen Scan-Dienst auf dem Server.** Die serverseitigen Scans laufen im API-Dienst mit; die Verbindungen zu den Zielsystemen gehen also vom API-Host aus. Ein eigener Windows-Dienst existiert nur für entfernte Netze, die der Server nicht erreicht: der **Discovery-Collector** mit eigenem Installationspaket (siehe ID-50). Er nimmt keine eingehenden Verbindungen an.

5.1 Dünner Client – standortübergreifend, VPN, weltweit

Der Windows-Client ist ein **dünner Client**: Er spricht **ausschließlich** die REST-API an (HTTP/HTTPS) und verbindet sich **nie** direkt mit der Datenbank – er kann es technisch gar nicht (der Client enthält keinen Datenbanktreiber). Auch datenbanknahe Anzeigen holt er über die API.

Für den Betrieb folgt daraus:

- **Nur der API-Port** muss von den Arbeitsplätzen erreichbar sein. **PostgreSQL (5432) kann auf den Server bzw. localhost beschränkt bleiben** – die Datenbank ist aus dem Client-Netz gar nicht erreichbar (Sicherheitsgewinn).
- Der Client ist damit **standortübergreifend** einsetzbar: über **VPN**, zwischen mehreren Standorten, bei Bedarf **weltweit** – vorausgesetzt, die API wird **sicher veröffentlicht** (natives HTTPS/TLS, siehe Betriebshandbuch ID-50, Abschnitt „HTTPS einrichten") **oder** der Zugang läuft über ein **VPN**.
- Die eine API-Adresse (`http(s)://server:port`) wird im Client unter *Verbindungseinstellungen* bzw. bei der Installation gesetzt (Betriebshandbuch, Abschnitt 7.2).

> **Sicherheitshinweis:** Eine ins Internet veröffentlichte API immer mit HTTPS und starker Authentifizierung betreiben. Wo das nicht gewährleistet ist, den Zugang auf ein VPN beschränken.

6 Datensicherheit auf einen Blick

- **Verschlüsselung:** TLS für alle Verbindungen; Zugangsdaten für Discovery werden AES-256-verschlüsselt im Credential-Vault gespeichert.
- **Authentifizierung:** JWT-basiert; Berechtigungen werden als `permission`-Claims transportiert.
- **AD/LDAP-Anbindung:** immer **read-only** – Ordivis Platform schreibt niemals ins Active Directory.
- **Mandantentrennung:** serverseitige Query-Filter je Mandant.
- **Kein Direktzugriff auf die Datenbank:** Der Client spricht ausschließlich die API an; PostgreSQL ist aus dem Client-Netz nicht erreichbar, und der Client trägt **keine** Datenbank-Zugangsdaten (nichts, das am

Arbeitsplatz gestohlen oder ausgelesen werden könnte). Jeder Datenzugriff wird API-seitig durch Authentifizierung, RBAC, Mandantentrennung, Validierung und Audit vermittelt – ein Vorbeischleusen an diesen Kontrollen, wie es direkter Datenbankzugriff erlauben würde, ist ausgeschlossen. Das entspricht den Grundsätzen der Netzsegmentierung und der minimalen Rechte (ISO 27001 / BSI-Grundschutz). Die Absicherung konzentriert sich damit auf die API: Diese ist folglich mit **HTTPS und starker Authentifizierung** zu betreiben bzw. der Zugang über **VPN** zu führen (siehe 5.1).

Details zu Härtung, Zertifikaten und Sicherung finden Sie im Betriebshandbuch (ID-50) sowie im ISMS-Modul (ID-28).

7 Editionen & Lizenzierung

Der Funktionsumfang kann durch die **Produktlizenz** begrenzt sein (z. B. Anzahl Administratoren oder Mandanten). Die Testphase umfasst 30 Tage mit vollem Funktionsumfang. Einzelheiten zur Aktivierung siehe ID-43.

Verwandte Themen

- **ID-50 – Betriebshandbuch – Installation & Serverbetrieb** – Installation, Update und Sicherung Schritt für Schritt
- **ID-51 – Datenbank-Leistung & Dimensionierung** – Dimensionierung und Verbindungspools nach Kundengröße
- **ID-42 – Modul Mandantenfähigkeit** – wie mehrere Organisationen in einer Installation getrennt werden
- **ID-28 – Modul Informationssicherheit (ISMS)** – Schutzbedarf und Härtung