Ordivis

TECHNISCHE REFERENZ

API-Referenz

REST-API – Authentifizierung, Konventionen, Endpunkte und Nutzung

Produktversion 2026.08.19 · Handbuch-Revision 1.0

Stand 19.08.2026 · Plattform .NET 10 / Windows Server

ID-60 API-Referenz

API-Referenz

Technisches Referenzdokument für Fachpersonal (Entwickler, Integratoren, Automatisierung). Es beschreibt die REST-API von Ordivis Platform: Authentifizierung, Autorisierung, Konventionen, Fehlerbehandlung und die verfügbaren Endpunkt-Bereiche. Das Rechtemodell ist in **ID-44** vertieft.

INHALT

1 Überblick

- **Stil:** REST über HTTPS, JSON als Austauschformat.
- **Basis-URL:** `https://<host>/` (Standard-Port 443). Alle fachlichen Endpunkte liegen unter `/api/v1/...`.
- **Versionierung:** URL-basiert (`/api/v1`). Neue, inkompatible Versionen erhalten einen neuen Pfad (`/api/v2`). Innerhalb einer Major-Version bleiben Endpunkte abwärtskompatibel.
- **Interaktive Dokumentation:** Die API stellt **OpenAPI/Swagger** bereit (Swagger-UI unter `/swagger`). Dort finden Sie die exakten Request-/Response-Schemata jedes Endpunkts.

> **Hinweis:** Dieses Dokument beschreibt Struktur und Nutzung. Die **maschinenlesbare, stets aktuelle** Schnittstellenbeschreibung ist die OpenAPI-Spezifikation der jeweils installierten Version.

2 Authentifizierung

Ordivis Platform verwendet **JWT (Bearer-Token)**.

2.1 Anmeldung

`POST /api/v1/auth/central-login`

Request-Body:

```
{
  "login": "christian.grams",
  "password": "GeheimesKennwort",
  "tenantId": null
}
```

Response (`LoginResult`):

```
{
  "accessToken": "eyJhbGciOiJI ... ",
  "refreshToken": "b3f1 ... ",
  "expiresAt": "2026-07-11T12:30:00+00:00",
  "tenantId": "1e2d ... ",
  "tenantName": "Musterstadt",
  "requiresTenantSelection": false,
  "tenants": []
}
```

- Der **Benutzername** ist case-insensitiv, das **Kennwort** case-sensitiv.
- Gehört der Benutzer zu **mehreren Mandanten** und wurde keiner gewählt, ist `requiresTenantSelection = true` und `tenants` enthält die Auswahl. Wiederholen Sie den Login mit gesetztem `tenantId`.

2.2 Token verwenden

Senden Sie den Access-Token bei jedem Aufruf im Header:

```
Authorization: Bearer <accessToken>
```

Der Token enthält die **`permission`-Claims** des Benutzers (siehe ID-44) sowie den Mandantenkontext.

2.3 Erneuern & Mandant wechseln

- **Erneuern:** Mit dem `refreshToken` einen neuen Access-Token anfordern (Refresh-Endpunkt der Auth-Ressource), bevor `expiresAt` erreicht ist.
- **Mandant wechseln:** `POST /api/v1/auth/switch-tenant` stellt für Benutzer mit mehreren Mandanten einen Token für den Zielmandanten aus (erfordert entsprechendes Recht, siehe ID-42).

2.4 Maschinen-Zugang (Integrations-Token)

Externe Werkzeuge und der Discovery-Collector melden sich **nicht** mit einem Benutzer-Login an, sondern mit einem **Integrations-Token** – einem widerrufbaren Maschinen-Zugang, der zu genau einem Mandanten gehört. Er reist im selben Header:

```
Authorization: Bearer ifd_<zufälliger Wert>
```

Unterschiede zum Benutzer-Token, die im Betrieb zählen:

- Ein Integrations-Token **läuft nicht ab** (sofern kein Ablaufdatum gesetzt wurde) und braucht kein Refresh – ein Dienst am Standort soll nach einem Stromausfall von selbst wiederkommen.
- Er trägt **nur die Einspeise-Rechte**, die bei seiner Ausstellung festgelegt wurden. Neue Rechte wachsen einem bestehenden Token **nicht** zu; für eine erweiterte Fläche wird ein neuer ausgestellt.
- Die Ingest-Endpunkte akzeptieren **ausschließlich** dieses Verfahren. Ein angemeldeter Benutzer erreicht sie auch mit dem passenden Recht nicht – und umgekehrt kommt ein Integrations-Token nicht an die Fachendpunkte der Oberfläche. Die beiden Flächen sind getrennt, nicht abgestuft.

Ausstellung und Widerruf beschreibt das Betriebshandbuch (**ID-50**, Abschnitt 7.4).

3 Autorisierung

- Jeder geschützte Endpunkt verlangt eine bestimmte **Berechtigung** (`[RequiresPermission("...")]`).
- Fehlt die Berechtigung → **HTTP 403 Forbidden**.
- Ohne (gültigen) Token → **HTTP 401 Unauthorized**.
- Die vollständige Rechte-Referenz steht in **ID-44**.

4 Konventionen

Thema	Regel
Content-Type	`application/json; charset=utf-8` für Request und Response
IDs	GUID (UUID) als String
Datum/Zeit	ISO 8601; Zeitstempel in **UTC** (`+00:00`). Eingehende Werte werden nach UTC normalisiert
Paginierung	Listen über `page` / `pageSize` (bzw. `skip` / `take`) als Query-Parameter; Antwort enthält Gesamtanzahl
Filter/Sortierung	Query-Parameter je Endpunkt (Filterfelder, `sort` / `order`)
Mandantenkontext	ergibt sich aus dem Token; keine Mandanten-ID im Body nötig
Idempotenz	`PUT` / `DELETE` idempotent; `POST` erzeugt neue Ressourcen

Wichtig: Zeitwerte müssen als UTC bzw. mit Offset `+00:00` übergeben werden. Ein Offset ungleich Null wird von der Datenbank (timestamptz) abgelehnt – die API normalisiert clientseitige Werte vor dem Speichern nach UTC.

5 Fehlerbehandlung

HTTP-Status	Bedeutung
200 / 201 / 204	Erfolg (OK / Erstellt / Kein Inhalt)
400	Ungültige Anfrage (z. B. Validierungsfehler, falsches Datumsformat)
401	Nicht authentifiziert (Token fehlt/abgelaufen)
403	Authentifiziert, aber Berechtigung fehlt
402	**Lizenz-/Aktivierungsgrenze** – schreibende Aufrufe bei abgelaufener Lizenz oder Admin-Limit (siehe ID-43)
404	Ressource nicht gefunden
409	Konflikt (z. B. eindeutige Verletzung, veralteter Stand)
422	Nicht verarbeitbar (semantische Validierung)
429	Zu viele Anfragen (Rate-Limit, z. B. E-Mail-Versand)
500	Serverfehler

Fehlerantworten liefern einen strukturierten Body (Problem-Details) mit Kurzbeschreibung.

6 Endpunkt-Bereiche

Die API ist modular geschnitten. Übersicht der Basis-Routen (Details in Swagger):

Bereich	Basis-Route	Zweck
Authentifizierung	`/api/v1/auth`	Login, Token-Refresh, Mandantenwechsel
Ersteinrichtung	`/api/v1/setup`	First-Run-Onboarding
Tickets / Service Desk	`/api/v1/tickets`	Tickets, dazu Unterrouten (s. u.)
Changes	`/api/v1/changes`	Change Requests
Probleme	`/api/v1/problems`	Problem-Management
CMDB	`/api/v1/cmdb`	CIs, `…/inventory`, `…/processes`, `…/label-media` (Etikettenmedien), `…/labels/print` (Druckauftrag je Druckersprache), `…/nfc-tags` (NFC-Zuordnung)
IPAM	`/api/v1/ipam`	Subnetze, IP-Adressen, DHCP
Discovery	`/api/v1/discovery`, `/api/v1/scan-credentials`	Scans, Anmeldedaten, Collector, Client-Inventar

Bereich	Basis-Route	Zweck
Maschinen-Naht (Ingest)	`/api/v1/ipam/ingest`, `/api/v1/discovery/ingest`, `/api/v1/discovery/collector`, `/api/v1/security/ingest`	Aufnahme externer Agenten und Collector (nur Integrations-Token, s. u.)
Assets/Verträge	`/api/v1/contracts`, `/api/v1/vendors`	Verträge, Lieferanten
Wissensdatenbank	`/api/v1/tickets/knowledge`, `/api/v1/portal/knowledge`	KB intern / Portal
Sicherheit (ISMS)	`/api/v1/security`, `/api/v1/security/oscal`, `/api/v1/security/profiles`	BSI/ISO, OSCAL-Export
BCM	`/api/v1/bcm`	Business Continuity
DR-Planung	`/api/v1/drplans`	Notfall-/Wiederanlaufpläne
Workflow	`/api/v1/workflow`	Workflows & Aufgaben
Reporting	`/api/reporting`, `/api/v1/dashboards`	Berichte, Dashboards
Checklisten	`/api/v1/checklists`	Vorlagen und Durchführungen
Handbücher	`/api/v1/handbooks`	Betriebs-/Notfall-/Wiederanlaufhandbücher
Organisation & GVP	`/api/v1/organisation`	Aufbau-/Ablauforganisation, `…/catalog`, `…/gvp`, `…/ozg`, `…/fim`
Datenschutz (VVT)	`/api/v1/datenschutz`	Verarbeitungstätigkeiten, `…/datenpannen`, `…/avv`, `…/kataloge`, `…/export`, `…/dashboard`
Betroffenenrechte	`/api/v1/privacy`	Auskunft, Löschung, Berichtigung (Art. 15–22 DSGVO)
Audit	`/api/v1/audit`	Audit-Log; `…/export` gibt die gefilterten Einträge als CSV aus (`audit.export`)
Benachrichtigungen	`/api/v1/notifications`	In-App-Benachrichtigungen
E-Mail	`/api/v1/mail/accounts`	Postfächer (Versand/Eingang)
Identität	`/api/v1/auth`, `/api/v1/identity/mfa`, `/api/identity/directory`, `/api/identity/access-reviews`	Benutzer, Zwei-Faktor, Verzeichnis, Access Reviews
SSO (SAML)	`/sso/saml`	Anmeldung über einen externen Identitätsanbieter

Bereich	Basis-Route	Zweck
Mandanten/Plattform	`/api/v1/platform/tenants`, `/api/v1/platform/grants`	Mandanten, Cross-Tenant-Grants
Lizenz/Aktivierung	`/api/v1/licenses`, `/api/v1/activation`	Produktlizenzierung
System	`/api/v1/system`, `/api/v1/settings`, `/api/v1/jobs`, `/api/system/backup`, `/api/system/logging`, `/api/v1/system/ha`	Betrieb & Konfiguration
Darstellung	`/api/v1/branding`	Firmenname und Logo für erzeugte Dokumente (je Mandant)
Wallboard	`/api/v1/wallboard`	Anzeigetafel-Zugang (eigenes Token-Verfahren, keine Anmeldung)
Mobile App	`/api/v1/mobile`	Naht für die Android-App (Inventur, Etiketten, Warteschlange)
Support	`/api/v1/support`	Fehlerbericht aus dem Windows-Client
Suche	`/api/search`	Übergreifende Suche
Anhänge	`/api/v1/attachments`	Datei-Anhänge

Ticket-Unterrouten (Auszug): `sla-profiles`, `routing-rules`, `approval-tiers`, `maintenance-windows`, `canned-responses`, `templates`, `support-groups`, `contacts`, `reporting`, `{ticketId}/knowledge`, `{ticketId}/render`. Daneben stehen `/api/v1/approval-delegations` (Vertretung bei Freigaben) und `/api/v1/ticketing/signatures` (Signaturen unter ausgehenden Mails).

7 Beispiele

7.1 Anmelden (curl)

```
curl -X POST https://host/api/v1/auth/central-login \
  -H "Content-Type: application/json" \
  -d '{"login":"christian.grams","password":"***"}'
```

7.2 Liste abrufen (mit Token)

```
curl https://host/api/v1/tickets?page=1&pageSize=50 \
  -H "Authorization: Bearer <accessToken>"
```

7.3 Ressource erstellen

```
curl -X POST https://host/api/v1/tickets \
  -H "Authorization: Bearer <accessToken>" \
  -H "Content-Type: application/json" \
  -d '{ "title":"Drucker im 2. OG", "urgency":"High", "impact":"Medium", "categoryId":" ... "
```

Achtung: `urgency` und `impact` akzeptieren nur `Low` / `Medium` / `High`. „Kritisch“ ist eine **abgeleitete Priorität**, kein Eingabewert (führt sonst zu HTTP 400).

8 Nutzungshinweise & Betrieb

- **TLS ist Pflicht.** Betreiben Sie Integrationen nie über unverschlüsselte Verbindungen.
- **Least Privilege:** Legen Sie für Automatisierung ein **eigenes Dienstkonto** mit genau den benötigten Rechten an (ID-44), nicht einen Administrator.
- **Rate-Limits:** Insbesondere versendende Aktionen sind ratenbegrenzt (HTTP 429). Implementieren Sie Backoff/Retry.
- **Stabilität:** Verlassen Sie sich auf `/api/v1`; prüfen Sie vor Upgrades die OpenAPI-Diffs.
- **Zeitzonen:** Immer UTC senden und empfangen; lokale Darstellung erst im Client.

Verwandte Themen

- **ID-44 – Rollen- & Rechte-Matrix** – Rechte des technischen Kontos
- **ID-42 – Modul Mandantenfähigkeit** – Mandantenauswahl im Aufruf
- **ID-52 – Datenbank-Referenz** – Datenstruktur hinter den Endpunkten
- **ID-43 – Modul Produktlizenzierung** – lizenzabhängige Limits