Ordivis

TECHNISCHE REFERENZ

Rollen- & Rechte-Matrix (RBAC)

RBAC – Rollen, Berechtigungen und vollständige Rechte-Matrix

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

ID-44 Rollen & Rechte

Rollen- & Rechte-Matrix (RBAC)

Technisches Referenzdokument für Fachpersonal (Administratoren, Auditoren, Sicherheitsverantwortliche). Es dokumentiert das rollenbasierte Berechtigungsmodell von Ordivis Platform vollständig: das Berechtigungskonzept, alle **Systemrollen**, den **Berechtigungskatalog** sowie die exakte Zuordnung Rolle → Berechtigungen.

> **Hinweis:** Grundlagen zur Bedienung der Benutzerverwaltung (Benutzer anlegen, MFA, Kennwort) stehen im Modul-Dokument **ID-41**. Dieses Dokument ist die technische Referenz zum Rechtemodell.

INHALT

1 Berechtigungskonzept
- 1.1 SuperAdmin und die Plattform-Ebene

2 Systemrollen

3 Berechtigungskatalog
- 3.1 CMDB (cmdb)
- 3.2 Ticketing / Service Desk (ticketing)
- 3.2a Prozessdokumentation (process)
- 3.3 Wissensdatenbank (knowledge)
- 3.4 IPAM (ipam)
- 3.5 Change (change)
- 3.6 Identität (identity)
- 3.7 System, Audit, Reporting, Lizenz
- 3.8 Verträge, Discovery, Workflow, DR
- 3.9 Informationssicherheit (security)
- 3.10 Business Continuity (bcm)
- 3.11 Datenschutz (datenschutz)
- 3.12 Checklisten (checklist)
- 3.13 Handbücher (handbook)
- 3.14 Organisation und Geschäftsverteilungsplan (gvp)
- 3.15 Plattform-Betrieb (platform)
- 3.16 Maschinen-Zugänge (Integrations-Token)

4 Rolle → Berechtigungen (exakte Zuordnung)

5 Besondere Hinweise
- 5.1 Funktionstrennung (Vier-Augen-Prinzip)
- 5.2 Nach dem Update: einmalige Neuanmeldung erforderlich

6 Bedienung in der Anwendung
- 6.1 Berechtigungsmatrix (Rollen × Berechtigungen)
- 6.2 Mandanten-Verwaltung (nur SuperAdmin / Plattform-Administrator)
- 6.3 Mandanten-Umschalter
- 6.4 DSGVO-Betroffenenrechte

Verwandte Themen

1 Berechtigungskonzept

- **Modell:** Role-Based Access Control (RBAC). Berechtigungen (*Permissions*) hängen an **Rollen**, Rollen an **Benutzern**. Ein Benutzer kann mehrere Rollen besitzen; die effektiven Rechte sind die **Vereinigung** aller Rollenrechte.
- **Token:** Nach der Anmeldung enthält das JWT ausschließlich `permission`**-Claims** – keine Rollennamen. Client und Portal steuern Sichtbarkeit anhand dieser Claims.
- **Durchsetzung (Server):** Jeder geschützte Endpunkt trägt `[RequiresPermission("<key>")]`. Fehlt das Recht, antwortet die API mit **HTTP 403**.
- **Schlüsselschema:** `<modul>.<objekt>.<aktion>` (z. B. `cmdb.ci.update`). Lesen endet meist auf `.read`, verwalten auf `.manage`.
- **Prinzip der minimalen Rechte:** Eine Rolle trägt nur die tatsächlich benötigten Rechte. Wie eine Rolle zusammengestellt wird, steht in Abschnitt 6.1.

1.1 SuperAdmin und die Plattform-Ebene

Ordivis Platform unterscheidet zwei Ebenen:

- **Mandanten-Ebene** – der normale Betrieb *innerhalb* eines Mandanten (CMDB, Ticketing, IPAM …). Hier arbeiten die operativen Rollen, allen voran der **IT-Administrator** (`ItAdmin`).
- **Plattform-Ebene** – die mandantenübergreifende Verwaltung *der Mandanten selbst* (Mandant anlegen, archivieren, löschen, Hierarchie, mandantenübergreifende Zugriffe).

Der **erste, bei der Installation eingerichtete Benutzer** ist der **SuperAdmin**. Er ist bewusst **speziell** und von den gewöhnlichen IT-Systemadministratoren einer IT-Abteilung zu unterscheiden: nur er (bzw. Rollen, denen er die Plattform-Rechte ausdrücklich delegiert) darf neue Mandanten anlegen oder löschen. Technisch trägt der SuperAdmin die Rolle **SystemAdmin** (alle Rechte inklusive der Plattform-Berechtigungen `tenant.*`).

Für die **Vertretung** kann der SuperAdmin einzelnen Benutzern die Rolle **Plattform-Administrator** geben – diese erlaubt ausschließlich die Mandanten-Verwaltung (`tenant.manage` , `tenant.rollup.read`), **nicht** die volle Systemmacht. Ein gewöhnlicher **IT-Administrator** (`ItAdmin`) besitzt **keine** `tenant.*` -Rechte und kann daher keine fremden Mandanten provisionieren oder löschen.

2 Systemrollen

Ordivis Platform liefert 13 vordefinierte **Systemrollen** aus (bei jedem Start konvergent nachgezogen). Eigene Rollen lassen sich zusätzlich anlegen und mit beliebigen Berechtigungen bestücken.

Rolle	Bezeichnung	Kurzbeschreibung
SystemAdmin	System Administrator	Voller Systemzugriff (**alle** Rechte) – die Rolle des **SuperAdmins** (s. 1.1)
PlatformAdmin	Plattform-Administrator	Mandanten anlegen/archivieren/löschen + Roll-up (Vertretung des SuperAdmins, **keine** volle Systemmacht)

Rolle	Bezeichnung	Kurzbeschreibung
ItAdmin	IT-Administrator	Vollzugriff auf alle operativen Module (Ausnahmen s. u.)
SdAgentL1	Service-Desk-Agent (L1)	Tickets bearbeiten, CMDB lesen, KB pflegen
SdAgentL2	Service-Desk-Agent (L2/L3)	Erweiterte Ticket-/CI-/Change-/Workflow-Rechte
CmdbAdmin	CMDB-Administrator	CMDB-Klassen und -Strukturen verwalten
NetworkAdmin	Netzwerk-Administrator	IPAM vollständig verwalten
ChangeManager	Change Manager	Change Requests freigeben/umsetzen
Enduser	Endbenutzer (Self-Service)	Eigene Tickets, Servicekatalog, öffentliche KB
CIO	CIO	Strategische Übersicht, Dashboards, lesend
DSB	Datenschutzbeauftragter	Audit-Log, DSGVO-relevante Leserechte
ISB	Informationssicherheitsbeauftragter	Vollzugriff ISMS/IT-Grundschutz, genehmigt Risiken
BCMB	BCM-Beauftragter	Vollzugriff Business Continuity Management

3 Berechtigungskatalog

Der Katalog umfasst **140 Berechtigungen**, gruppiert nach Modul. `key` ist der technische Wert im JWT und in `[RequiresPermission]`.

3.1 CMDB (`cmdb`)

key	Beschreibung
cmdb.ci.read	CI-Datensätze lesen
cmdb.ci.create	Neue CIs anlegen
cmdb.ci.update	CIs bearbeiten
cmdb.ci.delete	CIs löschen
cmdb.ci.lifecycle.manage	CI-Lifecycle-Status ändern
cmdb.class.manage	CMDB-Klassen definieren
cmdb.relation.manage	CI-Beziehungen verwalten
cmdb.import	Massen-Import
cmdb.export	Export von CI-Listen
cmdb.baseline.manage	Baselines verwalten

3.2 Ticketing / Service Desk (`ticketing`)

key	Beschreibung
tickets.read	Tickets der eigenen Support-Gruppe(n) lesen
tickets.read.all	Tickets ALLER Support-Gruppen lesen (kein Gruppen-Filter)
tickets.self.read	Nur eigene Tickets lesen
tickets.create	Tickets erstellen
tickets.update	Tickets bearbeiten
tickets.assign	Tickets zuweisen
tickets.close	Tickets schließen
tickets.delete	Tickets löschen
tickets.escalate	Tickets eskalieren
tickets.approve	Service-Request-Freigaben entscheiden
tickets.export	Ticket-Listen exportieren
tickets.sla.manage	SLA-Profile konfigurieren
ticketing.category.manage	Ticket-Kategorien verwalten
ticketing.config.manage	**Neu:** Service-Desk-Konfiguration verwalten – Routing-Regeln, Automatisierungsregeln, Genehmigungsstufen, Support-Gruppen, Wartungsfenster, Textbausteine und Vorlagen
contacts.manage	Lokale Kontakte (externe Melder) verwalten
ticketing.csat.submit	Zufriedenheit (CSAT) abgeben
ticketing.service_catalog.read	Service-Katalog ansehen/bestellen
ticketing.service_catalog.manage	Service-Katalog (Artikel/Kategorien) verwalten

Wichtig (seit 2026.07.14.1845): Die Steuerungsobjekte des Service Desks – SLA-Profile, Routing, Automatisierungsregeln, Genehmigungsstufen, Support-Gruppen, Wartungsfenster und Textbausteine – ließen sich zuvor mit dem reinen Leserecht `tickets.read` ändern. Sie verlangen jetzt `ticketing.config.manage` bzw. `tickets.sla.manage` . Diese Rechte besitzen der **Service-Desk-Agent (L2)** sowie IT- und System-Administratoren; ein **L1-Agent** kann die Konfiguration nun nicht mehr verändern (die zugehörigen Schaltflächen sind für ihn ausgeblendet).

3.2a Prozessdokumentation (`process`)

key	Beschreibung
process.manage	**Neu:** Prozessdokumentation pflegen – Steckbrief, RACI, KPI, Datenobjekte, BPMN-Entwurf

key	Beschreibung
process.approve	**Neu:** Prozessdefinition freigeben bzw. verwerfen (IKS-Kontrolle)

Funktionstrennung: Pflege und Freigabe sind bewusst **getrennte** Rechte. Der **CMDB-Administrator** pflegt die Prozessdokumentation (`process.manage`), die Freigabe (`process.approve`) liegt bei der Leitungsebene (**CIO**). Damit ist die Freigabe einer Prozessdefinition eine eigenständige Kontrollhandlung im Sinne des internen Kontrollsystems (ISO 9001, ISO 27001 A.5.37) und nicht mehr durch jeden CMDB-Leser vollziehbar.

3.3 Wissensdatenbank (`knowledge`)

key	Beschreibung
knowledge.read.public	Öffentliche KB-Artikel lesen
knowledge.read.internal	Interne KB-Artikel lesen
knowledge.author	KB-Artikel erstellen/bearbeiten
knowledge.review	KB-Artikel prüfen (Review-Gate)
knowledge.publish	KB-Artikel veröffentlichen/zurückziehen
knowledge.admin	KB-Artikel löschen/verwalten

3.4 IPAM (`ipam`)

key	Beschreibung
ipam.prefix.read	Subnetze lesen
ipam.prefix.manage	Subnetze verwalten
ipam.ip.read	IP-Adressen lesen
ipam.ip.assign	IPs reservieren/zuweisen
ipam.ip.free	IPs freigeben
ipam.ip.confirm	Unbestätigte IPs bestätigen
ipam.vrf.manage	VRFs verwalten
ipam.dhcp.manage	DHCP-Konfiguration verwalten
ipam.dhcp.import	Windows-DHCP-Server importieren
ipam.scan.trigger	IP-Scan auslösen
ipam.export	IP-Listen exportieren

3.5 Change (`change`)

key	Beschreibung
change.read	Change Requests lesen
change.create	Change Requests erstellen
change.approve	Change Requests genehmigen
change.reject	Change Requests ablehnen
change.implement	Change als umgesetzt markieren
change.emergency	Emergency Changes erstellen

3.6 Identität (`identity`)

key	Beschreibung
identity.users.read	Benutzerliste lesen
identity.users.manage	Benutzer verwalten
identity.roles.read	Rollenkonfiguration lesen
identity.roles.manage	Rollen verwalten
identity.permissions.manage	Berechtigungen konfigurieren
identity.mfa.enforce	MFA-Pflicht setzen
identity.sessions.manage	Aktive Sessions verwalten

3.7 System, Audit, Reporting, Lizenz

key	Modul	Beschreibung
system.config.read	system	Systemkonfiguration lesen
system.config.manage	system	Systemkonfiguration ändern (= „**Administrator**“)
system.backup.manage	system	Backups verwalten
system.security.manage	system	Sicherheitseinstellungen
reporting.read	reporting	Berichte lesen
reporting.create	reporting	Berichte erstellen – **und** die Vorschau freier SQL-Abfragen (freies SQL läuft an den Modul-Berechtigungen vorbei, siehe Kapitel *Reports & SQL-Abfragen*)
reporting.manage	reporting	Alle Berichte verwalten
reporting.dashboard.manage	reporting	Dashboard-Widgets konfigurieren
audit.read	audit	Audit-Log lesen

key	Modul	Beschreibung
audit.export	audit	Audit-Log als CSV ausgeben (zusätzlich zu `audit.read`; ohne dieses Recht wird der Abruf abgewiesen)
licensing.read	licensing	Lizenzdaten lesen
licensing.manage	licensing	Lizenzen verwalten
activation.manage	activation	Produktaktivierung / Lizenz verwalten
notifications.mailbox.admin	notifications	E-Mail-Postfächer (Versand + Ticket) verwalten
notifications.messenger.admin	notifications	Messenger-Verbindungen (Mattermost, Webhook) verwalten
discovery.action1.admin	discovery	Action1-Anbindung verwalten (Zugang, Organisation, Datenquellen)
tenant.manage	platform	**Plattform:** Mandanten anlegen/archivieren/löschen/Hierarchie (nur SuperAdmin / Plattform-Administrator)
tenant.rollup.read	platform	**Plattform:** mandantenübergreifendes Roll-up-Aggregat lesen
tenant.grant.manage	platform	**Plattform:** mandantenübergreifende Zugriffs-Grants verwalten (nur SuperAdmin)
privacy.manage	privacy	DSGVO-Betroffenenrechte (Auskunft/Löschung) + Verarbeitungsverzeichnis (DSB)

Die `tenant.*`-Berechtigungen bilden die **Plattform-Ebene** (s. 1.1). Sie sind bewusst von der mandantenweiten `system.config.manage` getrennt: Ein IT-Administrator besitzt Letztere, aber **keine** `tenant.*`-Rechte und kann somit keine fremden Mandanten verwalten.

3.8 Verträge, Discovery, Workflow, DR

key	Modul	Beschreibung
contracts.read	contracts	Verträge und Lieferanten lesen
contracts.manage	contracts	Verträge/Lieferanten/Verpflichtungen verwalten
discovery.read	discovery	Discovery-/Scan-Daten lesen
discovery.manage	discovery	Scans auslösen, Anmeldedaten/Anhänge verwalten
discovery.collector.manage	discovery	Discovery-Collector anlegen, anmelden, sperren
discovery.result.review	discovery	Gefundene Clients prüfen und als CI übernehmen
workflow.read	workflow	Workflows und Aufgaben lesen
workflow.manage	workflow	Workflows starten und Aufgaben bearbeiten
dr.read	dr	Notfall-/DR-Pläne lesen

key	Modul	Beschreibung
dr.manage	dr	Notfall-/DR-Pläne und Testergebnisse verwalten

3.9 Informationssicherheit (`security`)

key	Beschreibung
security.catalog.manage	Sicherheitskataloge (BSI/ISO) importieren/verwalten
security.scope.manage	Informationsverbund/Geltungsbereich verwalten
security.assessment.manage	Schutzbedarfsfeststellung verwalten
security.modelling.manage	Modellierung (Baustein-Zuweisung) verwalten
security.audit.manage	IT-Grundschutz-Checks/Audits verwalten
security.check.write	Prüfergebnisse erfassen
security.check.read	ISMS-Daten/Prüfergebnisse lesen
security.risk.manage	Risikoanalysen verwalten
security.risk.accept	Risiken freigeben/akzeptieren
security.report.generate	ISMS-Berichte erzeugen
security.report.read	ISMS-Berichte/Dashboards lesen
security.measures.own.write	Eigene zugewiesene Maßnahmen bearbeiten

3.10 Business Continuity (`bcm`)

key	Beschreibung
bcm.scope.manage	BCM-Geltungsbereich/Verbund verwalten
bcm.process.manage	BCM-Prozess-Overlay verwalten
bcm.bia.manage	Business Impact Analyse (BIA) verwalten
bcm.resource.link	Ressourcen (CI/Vendor/Person) verknüpfen
bcm.risk.read	BCM-Risiko-/Gap-Daten lesen
bcm.org.manage	Bewältigungsorganisation (AAO/BAO) verwalten
bcm.plan.manage	Notfallpläne/Checklisten verwalten
bcm.plan.read	Notfallpläne/Checklisten lesen (Portal)
bcm.exercise.manage	Übungen/Tests verwalten
bcm.capa.manage	Korrektur-/Verbesserungsmaßnahmen (CAPA) verwalten
bcm.report.generate	BCM-Berichte erzeugen

key	Beschreibung
bcm.report.read	BCM-Berichte/Dashboards lesen
bcm.crisis.operate	Krisenmodus/BAO-Aktivierung bedienen

3.11 Datenschutz (`datenschutz`)

Das Verzeichnis der Verarbeitungstätigkeiten (VVT) trennt bewusst zwischen **eigenen** und **allen** Verfahren: `datenschutz.vvt.read` zeigt die Verfahren des eigenen Bereichs, erst `datenschutz.vvt.read.all` das gesamte Verzeichnis – dieses Recht gehört der oder dem Datenschutzbeauftragten und dem Betriebsrat, nicht jeder fachlich beteiligten Person.

key	Beschreibung
datenschutz.vvt.read	Verzeichnis lesen (Standard-Umfang: eigene Verfahren)
datenschutz.vvt.read.all	Gesamtes Verzeichnis lesen (DSB/Betriebsrat)
datenschutz.vvt.edit	Verarbeitungstätigkeiten anlegen/ändern
datenschutz.vvt.approve	Verarbeitungstätigkeiten freigeben (DSB)
datenschutz.vvt.export	Behördenkonformen Export erzeugen
datenschutz.catalog.manage	Kataloge (Betroffene/Datenkategorien) verwalten
datenschutz.breach.read	Datenschutzverletzungen lesen (Art. 33/34 DSGVO)
datenschutz.breach.report	Datenschutzverletzung melden/erfassen
datenschutz.breach.manage	Datenschutzverletzungen bewerten/melden/abschließen (DSB)

3.12 Checklisten (`checklist`)

`checklist.run.execute.self` ist bewusst eng: Damit arbeitet jemand **die ihm zugewiesene** Durchführung ab, ohne fremde Durchführungen zu sehen oder starten zu können.

key	Beschreibung
checklist.read	Checklisten und Durchführungen lesen
checklist.template.manage	Checklisten-Vorlagen pflegen
checklist.run.manage	Durchführungen starten/zuweisen/abbrechen
checklist.run.execute.self	Eigene zugewiesene Checkliste abarbeiten

3.13 Handbücher (`handbook`)

key	Beschreibung
handbook.read	Handbücher lesen (Betrieb/Notfall/Wiederanlauf)
handbook.manage	Handbücher pflegen/generieren (Kapitel, Bausteine, Versionierung)

key	Beschreibung
handbook.approve	Handbuch freigeben (Entwurf → freigegebener Stand)

3.14 Organisation und Geschäftsverteilungsplan (`gvp`)

key	Beschreibung
gvp.read	Produktkatalog, Ablauf-/Aufbauorganisation und Geschäftsverteilungsplan lesen
gvp.manage	Katalogpflege, Übernahme, Zuständigkeiten und GVP-Fassungen verwalten

3.15 Plattform-Betrieb (`platform`)

Wie die `tenant.*`-Rechte gehören diese der **Plattform-Ebene** (s. 1.1) und nicht in die Rolle eines mandantenbezogenen Administrators.

key	Beschreibung
platform.monitor	Plattform-Überwachung lesen (PostgreSQL, Sitzungen, Betriebskennzahlen der Mandanten)
platform.hosting.manage	HTTPS/Transportsicherheit konfigurieren (Zertifikat, ACME, Reverse-Proxy)
platform.eventlog.manage	Windows-Sicherheitsprotokoll (Ereignisanzeige) konfigurieren
platform.integrationtoken.manage	Integrations-Token (Maschinen-Zugang) ausstellen und widerrufen
system.backup.restore	Datenbank aus einer Sicherung wiederherstellen (**destruktiv**)

> `system.backup.restore` überschreibt den laufenden Datenbestand. Es gehört keiner Rolle, die im Tagesgeschäft benutzt wird, sondern wird für den Wiederherstellungsfall gezielt vergeben.

3.16 Maschinen-Zugänge (Integrations-Token)

Diese Berechtigungen stehen im Katalog, gehören aber **nicht in eine Benutzerrolle**. Sie werden ausschließlich von **Integrations-Token** getragen (externe Werkzeuge, Discovery-Collector). Die zugehörigen Endpunkte akzeptieren nur das Token-Verfahren – ein angemeldeter Benutzer erreicht sie auch mit dem passenden Recht nicht.

key	Beschreibung
ipam.scan.ingest	Scan-Ergebnisse externer Agenten einspeisen
cmdb.ingest	Geräte und Zertifikate externer Agenten als Funde einliefern
security.finding.ingest	Schwachstellenbefunde externer Agenten einliefern
discovery.collector.report	Collector meldet Auftrag, Lebenszeichen und Funde

`discovery.collector.report` lässt sich **nicht von Hand ausstellen**: Diesen Token vergibt ausschließlich das Enrollment eines Collectors, gebunden an genau einen Collector.

4 Rolle → Berechtigungen (exakte Zuordnung)

Die folgende Auflistung entspricht der ausgelieferten Seed-Konfiguration. Sie ist die verbindliche Matrix je Rolle.

SystemAdmin – **alle** Berechtigungen (uneingeschränkt).

IT-Administrator (ItAdmin) – **alle Berechtigungen außer** `system.backup.manage` und `identity.permissions.manage`. (Kann also Benutzer/Rollen verwalten, aber nicht das Berechtigungsschema selbst ändern und keine Backups steuern.)

CMDB-Administrator (CmdbAdmin) `cmdb.ci.read`, `cmdb.ci.create`, `cmdb.ci.update`, `cmdb.ci.delete`, `cmdb.ci.lifecycle.manage`, `cmdb.class.manage`, `cmdb.relation.manage`, `cmdb.import`, `cmdb.export`, `cmdb.baseline.manage`, `reporting.read`, `reporting.create`, `licensing.read`, `contracts.read`, `discovery.read`, `dr.read`.

Service-Desk-Agent L1 (SdAgentL1) `tickets.read`, `tickets.create`, `tickets.update`, `tickets.close`, `tickets.escalate`, `ticketing.csat.submit`, `contacts.manage`, `ticketing.service_catalog.read`, `cmdb.ci.read`, `reporting.read`, `knowledge.read.public`, `knowledge.read.internal`, `knowledge.author`.

Service-Desk-Agent L2/L3 (SdAgentL2) – L1 plus: `tickets.assign`, `tickets.delete`, `tickets.export`, `notifications.mailbox.admin`, `ticketing.service_catalog.manage`, `cmdb.ci.update`, `cmdb.relation.manage`, `change.read`, `change.create`, `reporting.create`, `workflow.read`, `workflow.manage`, `knowledge.review`, `knowledge.publish`.

Netzwerk-Administrator (NetworkAdmin) `ipam.prefix.read`, `ipam.prefix.manage`, `ipam.ip.read`, `ipam.ip.assign`, `ipam.ip.free`, `ipam.vrf.manage`, `ipam.dhcp.manage`, `ipam.dhcp.import`, `ipam.scan.trigger`, `ipam.ip.confirm`, `ipam.export`, `cmdb.ci.read`, `cmdb.ci.create`, `reporting.read`, `discovery.read`, `discovery.manage`, `discovery.collector.manage`, `discovery.result.review`.

Change Manager (ChangeManager) `change.read`, `change.create`, `change.approve`, `change.reject`, `change.implement`, `change.emergency`, `cmdb.ci.read`, `tickets.read`, `reporting.read`, `licensing.read`, `contracts.read`, `workflow.read`, `workflow.manage`, `dr.read`, `dr.manage`.

CIO (strategisch, überwiegend lesend) `reporting.read`, `reporting.create`, `reporting.manage`, `cmdb.ci.read`, `tickets.read`, `tickets.read.all`, `ipam.prefix.read`, `ipam.ip.read`, `audit.read`, `licensing.read`, `contracts.read`, `workflow.read`, `dr.read`, `security.report.read`, `security.check.read`, `knowledge.read.public`, `knowledge.read.internal`, `bcm.report.read`, `bcm.plan.read`.

Endbenutzer (Enduser) `tickets.self.read`, `tickets.create`, `ticketing.csat.submit`, `ticketing.service_catalog.read`, `knowledge.read.public`.

Datenschutzbeauftragter (DSB) `audit.read`, `audit.export`, `reporting.read`, `identity.users.read`.

Informationssicherheitsbeauftragter (ISB) – **alle** `security.*`-Rechte plus `cmdb.ci.read`, `reporting.read`.

BCM-Beauftragter (BCMB) – **alle** `bcm.*`-Rechte plus `cmdb.ci.read`, `cmdb.ci.create`, `cmdb.relation.manage`, `security.check.read`, `dr.read`, `reporting.read`.

5 Besondere Hinweise

- **„Administrator"** im Sinne der Produktlizenz = Benutzer mit `system.config.manage`. Das Administrator-Limit der Lizenz greift beim Zuweisen dieses Rechts (HTTP 402, siehe ID-43).
- **Ticket-Sichtbarkeit:** `tickets.read` ist auf die eigenen **Support-Gruppen** beschränkt; `tickets.read.all` hebt den Gruppen-Filter auf.
- **Konvergenz:** Neue Systemrollen und Berechtigungen werden bei jedem Start additiv nachgezogen; bestehende (Rolle, Recht)-Zuordnungen bleiben unangetastet.
- **Eigene Rollen:** Zusätzliche Rollen sind über `identity.roles.manage` möglich; die Vergabe einzelner Rechte erfolgt über `identity.permissions.manage`.

5.1 Funktionstrennung (Vier-Augen-Prinzip)

Drei Freigaben sind seit **2026.07.14.1845** als feste Regel im System verankert – sie lassen sich auch dann nicht umgehen, wenn eine Person beide Rechte besitzt:

Vorgang	Regel
Änderungsantrag (Change)	Der **Antragsteller** kann seinen eigenen Antrag **nicht** freigeben. Ausnahme: **Notfall-Changes** – dort zählt Geschwindigkeit; die Freigabe wird über die Freigabe-Historie nachvollziehbar dokumentiert (ITIL-Praxis).
Wissensartikel	Öffentliche Artikel müssen von einer **anderen** Person freigegeben werden als dem Autor bzw. Einreicher.
Prozessdefinition	Die Freigabe erfolgt durch eine **andere** Person als den Ersteller; zusätzlich sind Pflege (`process.manage`) und Freigabe (`process.approve`) getrennte Rechte.

Bis zu dieser Version war die Trennung beim Change **nur über die Rollenvergabe** hergestellt: Wer `change.create` **und** `change.approve` besaß, konnte den CAB-Beschluss an sich selbst vorbei durchführen. Das ist nun ausgeschlossen (ISO 27001 A.5.3 „Aufgabentrennung", A.8.32 „Änderungssteuerung").

5.2 Nach dem Update: einmalige Neuanmeldung erforderlich

Die Berechtigungen stehen im Anmelde-Token. Nach dem Update auf **2026.07.14.1845** müssen sich alle Benutzer **einmal neu anmelden**, damit die neuen Rechte (u. a. `ticketing.config.manage`, `process.manage`, `process.approve`) wirksam werden. Ohne Neuanmeldung arbeiten sie weiter mit den Rechten aus ihrem alten Token und erhalten bei den betroffenen Aktionen die Meldung „Keine Berechtigung" (HTTP 403).

6 Bedienung in der Anwendung

6.1 Berechtigungsmatrix (Rollen × Berechtigungen)

> 💻 **Nur im Client:** *Fußbereich ▸ Einstellungen ▸ Rollen & Berechtigungen* · 🔑 `identity.roles.read` zum Ansehen, `identity.permissions.manage` zum Ändern — Das Portal weist Rollen unter *Verwaltung ▸ Benutzer und Rollen* zu, stellt sie aber nicht zusammen.

🔒 **Pflichtreihenfolge — Systemrollen sind schreibgeschützt.** Eine eigene Rolle muss deshalb existieren, bevor Sie Rechte setzen können; die Kontrollkästchen einer Systemrolle bleiben deaktiviert, und ein Hinweisbanner sagt das auch.

1. Klicken Sie auf *Neue Rolle* und vergeben Sie einen Namen. Die neue Rolle ist sofort ausgewählt und bearbeitbar.
2. Setzen Sie die benötigten Rechte per Kontrollkästchen – die Liste ist **nach Modul gruppiert**.
3. Klicken Sie auf *Speichern*.
4. Weisen Sie die Rolle anschließend den Benutzern zu (ID-41, Abschnitt 2).

✅ **Ergebnis:** Die Rolle steht zur Auswahl. Beachten Sie: Betroffene Benutzer müssen sich **neu anmelden**, damit die Rechte im Token ankommen (Abschnitt 5.2).

Eine bestehende Rolle ansehen: Wählen Sie sie oben aus; die Berechtigungen erscheinen darunter.

Eine eigene Rolle löschen: Klicken Sie auf *Rolle löschen* – nur bei eigenen Rollen und mit Rückfrage.

> **Tipp:** Fangen Sie nicht bei null an. Sehen Sie sich die Systemrolle an, die Ihrem Zweck am nächsten kommt (Abschnitt 4), und bilden Sie deren Rechte in Ihrer eigenen Rolle nach – abzüglich dessen, was die Person wirklich nicht braucht.

6.2 Mandanten-Verwaltung (nur SuperAdmin / Plattform-Administrator)

> 💻 **Client:** *Fußbereich ▸ Einstellungen ▸ Mandanten* · 🌐 **Portal:** *Verwaltung ▸ Mandanten und Module* · 🔑 `tenant.manage`

🔒 **Pflichtreihenfolge — Löschen ist nur nach vorheriger Archivierung möglich.** Das ist keine Schikane, sondern die einzige Stelle, an der ein Irrtum noch auffällt, bevor die Datenbank weg ist.

- **Mandant anlegen:** Kürzel, Name und optional eine Admin-E-Mail angeben. Beim Anlegen wird eine **eigene Datenbank** für den Mandanten bereitgestellt. Voraussetzung dafür ist, dass die Datenbank-Rolle der Anwendung Datenbanken anlegen darf – siehe Betriebshandbuch (ID-50), Abschnitt zur Mandanten-Provisionierung. Fehlt das Recht, meldet das Anlegen einen Fehler („keine Berechtigung, um Datenbank zu erzeugen“).
- **Archivieren** blendet den Mandanten aus dem Betrieb aus (Daten bleiben erhalten).
- **Löschen** entfernt den Mandanten endgültig (Datenbank wird verworfen) und ist nur **nach vorheriger Archivierung** und mit Bestätigung möglich.

> **Lizenz-Grenze:** Beim Anlegen prüft Ordivis Platform die aktive Produktlizenz. Ist die in der Lizenz festgelegte **Höchstzahl an Mandanten** erreicht, wird das Anlegen abgelehnt und ein Hinweis eingeblendet („Die aktive Lizenz erlaubt maximal *X* Mandanten … für eine Erweiterung den Vertrieb kontaktieren"). Eine Lizenz ohne Mandanten-Begrenzung (bzw. die Testphase) hat kein Limit.

6.3 Mandanten-Umschalter

Gehört ein Benutzer zu mehreren Mandanten – der **SuperAdmin** und Plattform-Administratoren erreichen **alle** aktiven Mandanten –, erscheint in der Titelleiste (Gebäude-Symbol) ein **Umschalter**. Ein Klick öffnet die Mandantenliste; die Auswahl wechselt **ohne Neustart** in den Zielmandanten (die Navigation passt sich den dort geltenden Rechten an).

6.4 DSGVO-Betroffenenrechte

Der Datenschutzbeauftragte (Recht `privacy.manage`) kann je Mandant die Betroffenenrechte bedienen: **Datenauskunft** (strukturierter Export aller personenbezogenen Daten einer Person), **Löschung** (Anonymisierung unter Wahrung der Nachweispflichten) sowie das **Verarbeitungsverzeichnis** (Art. 30 DSGVO).

Verwandte Themen

- **ID-41 – Modul Identität, Benutzer & Rollen** – Rollen anlegen und zuweisen
- **ID-42 – Modul Mandantenfähigkeit** – Wirkung der Mandantengrenze auf Rechte
- **ID-27 – Modul Reporting & Dashboards** – warum Auswertungen je Rolle abweichen
- **ID-90 – Anhang – Glossar & Referenzen** – Kurzreferenz der wichtigsten Rechte