Ordivis

MODUL · IDENTITÄT & RBAC

Modul Identität, Benutzer & Rollen (RBAC)

Benutzer anlegen, Rollen zuweisen, MFA, Passwörter, Rechtematrix

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

ID-41 Identität

Modul Identität, Benutzer & Rollen (RBAC)

Nicht jeder in einer Organisation soll alles dürfen. Die Auszubildende im ersten Monat braucht andere Möglichkeiten als die Administratorin, und die Buchhaltung hat in der IT-Dokumentation wenig verloren. Würde man jeder Person ihre Rechte einzeln zuteilen, wäre das bei mehr als einer Handvoll Leuten kaum noch zu überblicken und fehleranfällig obendrein.

Deshalb arbeitet Ordivis Platform *rollenbasiert*, im Fachjargon RBAC für „Role-Based Access Control“. Der Gedanke ist einfach: Berechtigungen (Rechte) werden nicht direkt an Personen vergeben, sondern an Rollen wie „Agent“, „Administrator“ oder „Nur-Lesen“. Eine Person bekommt eine oder mehrere Rollen und erbt damit genau deren Rechte. Ändert sich der Zuschnitt einer Rolle, wirkt das sofort für alle, die sie haben. Dieses Modul verwaltet die drei Bausteine dahinter: die Konten (Benutzer), die Rollen und die Rechte.

INHALT

1 Grundprinzip: permission-basiert

Das Anmelde-Token (JWT) enthält ausschließlich `permission`**-Claims** – keine Rollennamen. Die Sichtbarkeit von Menüpunkten und Aktionen richtet sich nach diesen Rechten. Serverseitig sichert `[RequiresPermission]` jeden Endpunkt ab.

2 Lokalen Benutzer anlegen

💻 **Client:** *Fußbereich ▸ Einstellungen ▸ Benutzerverwaltung ▸ Neuer Benutzer* · 🌐 **Portal:** *Verwaltung ▸ Benutzer und Rollen* · 🔑 `identity.users.manage`

🔒 **Pflichtreihenfolge** — der Benutzer wird **passwortlos** angelegt und kann sich damit nicht anmelden. Schritt 4 gehört zwingend dazu; ohne ihn ist der Vorgang nicht abgeschlossen, sondern halb erledigt.

1. Öffnen Sie die Benutzerverwaltung und klicken Sie auf *Neuer Benutzer*.
2. Erfassen Sie *Login*, *Anzeigename*, *E-Mail* und den *Mandanten*.
3. Weisen Sie die *Rollen* zu – sie entscheiden, was die Person sieht und darf (ID-44).
4. Speichern Sie und vergeben Sie anschließend über *Passwort zurücksetzen* ein **erstes Kennwort**.
5. Geben Sie das Kennwort auf einem anderen Weg als per E-Mail an die Person weiter.

✅ **Ergebnis:** Die Person kann sich anmelden und ihr Kennwort danach selbst ändern (ID-10, Abschnitt 3).

> **Wichtig:** Ein neu angelegter Benutzer kann sich erst anmelden, nachdem ein Administrator ein **Kennwort zurückgesetzt** (vergeben) hat. Das ist der häufigste Grund für die Meldung, die Anmeldung funktioniere nicht.

3 Stammdaten & Status pflegen

- **Ändern:** Anzeigename, **Vorname**, **Nachname**, **Funktion/Titel**, E-Mail, Abteilung, Telefon. Vor- und Nachname speisen u. a. die E-Mail-Signatur des Service Desks (Nachname dort aus Datenschutzgründen gekürzt).
- **Aktivieren/Deaktivieren:** sperrt bzw. reaktiviert den Zugang.
- **Passwort zurücksetzen:** vergibt ein neues Kennwort.
- **MFA zurücksetzen:** entfernt den zweiten Faktor (Neu-Einrichtung nötig).
- **Sessions:** aktive Anmeldungen einsehen/beenden.

4 Benutzername & Kennwort

Der **Benutzername** ist **case-insensitiv** (Anmeldung unabhängig von Groß-/Kleinschreibung), das **Kennwort** ist case-sensitiv. Abbildung 1 zeigt die Anmeldung im Ganzen – einschließlich Sperre (Abschnitt 4.1) und zweitem Faktor (Abschnitt 6).

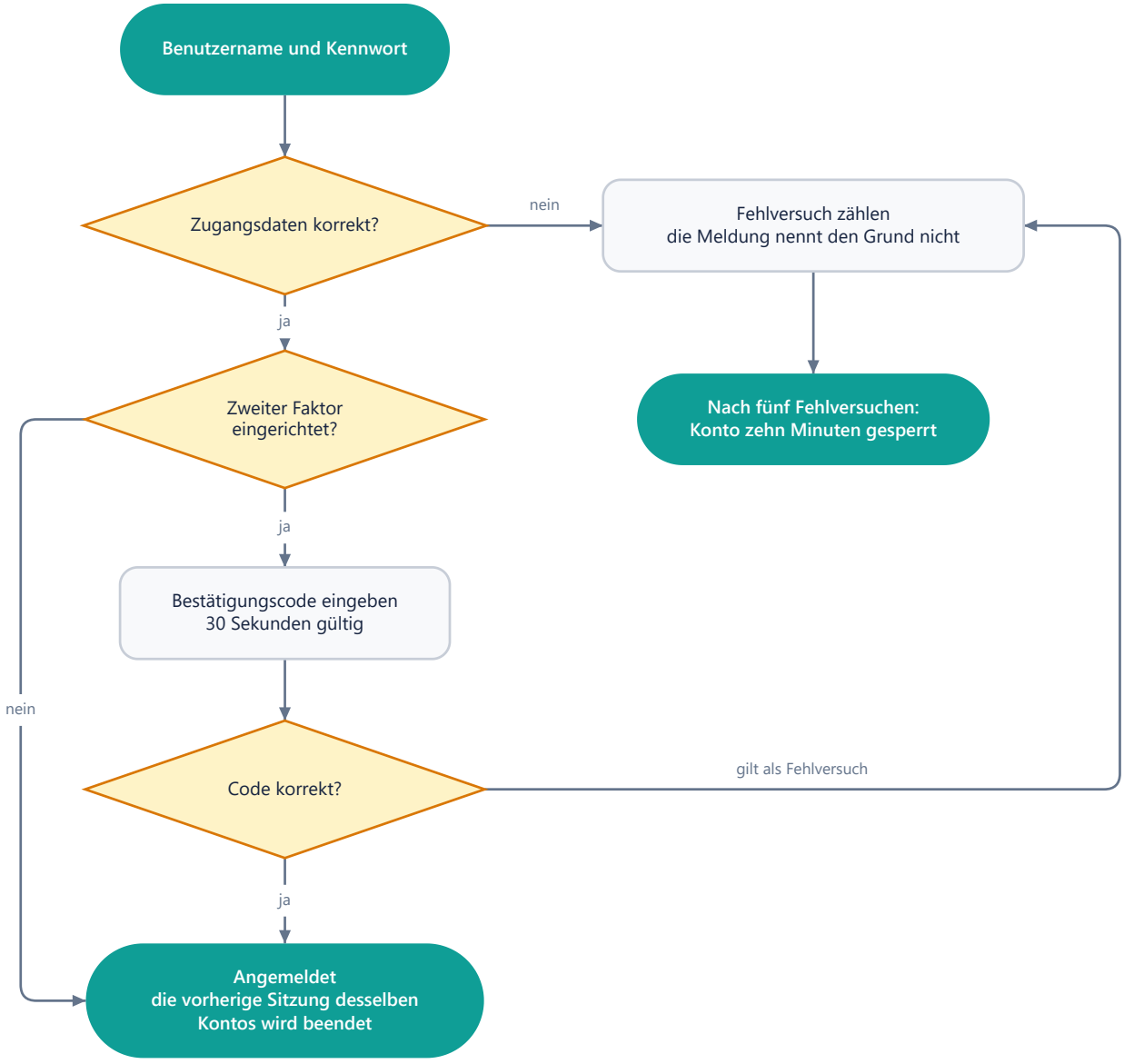

Abb. 1 – Anmeldung mit Kennwort und zweitem Faktor. Ein falscher Bestätigungscode läuft in dieselbe Sperre wie ein falsches Kennwort.

4.1 Sperre nach Fehlversuchen

Nach **fünf** aufeinanderfolgenden Fehlversuchen wird das Konto für **zehn Minuten** gesperrt; danach ist eine Anmeldung wieder möglich, ohne dass jemand eingreifen muss. Ein erfolgreicher Versuch setzt den Zähler zurück. Beide Werte sind in der Serverkonfiguration einstellbar (`Login:BruteForceMaxAttempts`, `Login:BruteForceLockMinutes`).

Eine Administratorin oder ein Administrator muss eine solche Sperre nicht aufheben. Wer nicht warten möchte, kann über **Passwort zurücksetzen** ein neues Kennwort vergeben.

> Die Anmeldemaske nennt bei falschen Zugangsdaten bewusst **nicht**, ob es das Konto überhaupt gibt – und antwortet in beiden Fällen gleich schnell. Andernfalls ließe sich von außen herausfinden, welche Benutzernamen existieren. Jeder Fehlversuch und jede ausgelöste Sperre stehen im Windows-Sicherheits- protokoll (siehe Administrationshandbuch) und lassen sich damit an ein SIEM anbinden.

4.2 Nur eine Anmeldung gleichzeitig

Eine neue Anmeldung **beendet die vorherige Sitzung desselben Kontos**. Wer sich am zweiten Gerät anmeldet, wird am ersten beim nächsten Zugriff abgemeldet. Das ist beabsichtigt: Ein Konto, das an mehreren Orten gleichzeitig offen ist, lässt sich im Nachhinein keiner Person mehr zuordnen.

Die Sitzung selbst läuft nach **zwölf Stunden ohne Zugriff** ab; das kurzlebige Zugriffstoken wird währenddessen alle **15 Minuten** im Hintergrund erneuert (`Identity:Jwt:RefreshTokenExpiryHours`, `Identity:Jwt:AccessTokenExpiryMinutes`). Die zwölf Stunden sind eine Frist der Ruhe, keine Höchstdauer: Jede Erneuerung setzt sie neu, ein geöffneter Client hält die Sitzung also offen. Sie läuft ab, wenn zwölf Stunden lang kein Zugriff erfolgt — Anwendung geschlossen, Rechner aus oder im Ruhezustand. Aktive Sitzungen lassen sich in der Benutzerverwaltung einsehen und gezielt beenden (Abschnitt 3).

Auf dem Server einstellen. Beide Werte stehen als Maschinen-Umgebungsvariable (`Identity__Jwt__RefreshTokenExpiryHours` , `Identity__Jwt__AccessTokenExpiryMinutes`) und werden vom Installer gesetzt. Sie haben Vorrang vor `appsettings.Production.json` — und sind zugleich der einzige Weg, der eine bestehende Installation erreicht, denn Updates lassen `appsettings*.json` bewusst unangetastet. Nach einer Änderung den Dienst `InfraDesk.API` neu starten.

Das Web-Portal hat eine eigene, deutlich kürzere Frist. Es bringt eine zweite Uhr mit — die Laufzeit seines Anmelde-Cookies, einstellbar über `Session:LifetimeMinutes` (Vorgabe **30 Minuten**). Sie gilt unabhängig von den zwölf Stunden oben: Wer im Portal arbeitet, wird nach einer halben Stunde ohne Zugriff zur Anmeldung geschickt. Das ist Absicht — das Portal steht Endanwendern offen und läuft auch an gemeinsam genutzten Rechnern. Siehe Betriebshandbuch, Abschnitt 3.5.

Warum wurde ich abgemeldet? Das Portal unterscheidet die beiden Fälle seit `2026.08.07.2104` und benennt sie auch so: *„Diese Sitzung wurde beendet"* steht für eine Anmeldung an anderer Stelle (oder eine gezielt beendete Sitzung), *„Ihre Anmeldung ist abgelaufen"* für das Ende der zwölf Stunden. Vorher meldete die Schnittstelle beides mit demselben Text, und das Portal sprach immer von „abgelaufen" – was beim häufigeren Fall, der Zweitanmeldung, in die Irre führte. Für die Fehlersuche steht der Grund zusätzlich im Protokoll des Portaldienstes.

Der Arbeitsplatz-Client folgt seit `2026.08.08.1302` **.** Zuvor räumte er die beendete Sitzung stillschweigend weg: Das Fenster blieb offen, und jede Seite scheiterte einzeln mit ihrer eigenen Meldung („… konnte nicht geladen werden: Unauthorized"). Jetzt kehrt er zur Anmeldemaske zurück und nennt denselben Grund wie das Portal.

⚠️ Zu beachten: Das **Zugriffstoken** bleibt nach dem Widerruf noch bis zu 15 Minuten gültig. Die Abmeldung am ersten Gerät wird deshalb nicht sofort sichtbar, sondern erst beim nächsten Erneuern.

Eine Störung meldet nicht ab. Antwortet die Schnittstelle beim Erneuern mit einer Überlastung (429), einem Serverfehler oder gar nicht, bleibt die Anmeldung bestehen und der nächste Versuch erneuert erneut. Nur ein **zurückgewiesenes** Erneuerungs-Token beendet die Sitzung. Andernfalls würde eine kurze Lastspitze die halbe Belegschaft aus der Arbeit werfen.

5 Rollen & Rechtematrix

💻 **Client:** *Fußbereich ▸ Einstellungen ▸ Benutzerverwaltung* · 🌐 **Portal:** *Verwaltung ▸ Benutzer und Rollen* · 🔑 `identity.roles.manage`

Auf der Benutzer-Detailseite werden **Rollen** über Spalten mit Haken zugewiesen. Eine **Rollen-Matrix** zeigt, welche Rolle welche Rechte besitzt.

So weisen Sie einem Benutzer eine Rolle zu:

1. Öffnen Sie die Benutzerverwaltung und suchen Sie den Benutzer.
2. Setzen Sie in seiner Zeile den Haken in der Spalte der gewünschten Rolle.
3. Speichern Sie.

✅ **Ergebnis:** Die Rolle greift, sobald sich der Benutzer **neu anmeldet** – die Rechte stehen im Token, und das wird bei der Anmeldung ausgestellt (ID-44, Abschnitt 5.2).

> **Wichtig:** Vergeben Sie Rechte nach dem Prinzip der **minimalen Berechtigung**. Mehrere Rollen addieren sich; die effektiven Rechte sind ihre Vereinigung, nie ihr Durchschnitt.

Abbildung 2 zeigt die Zuweisung als angehakte Spalten.

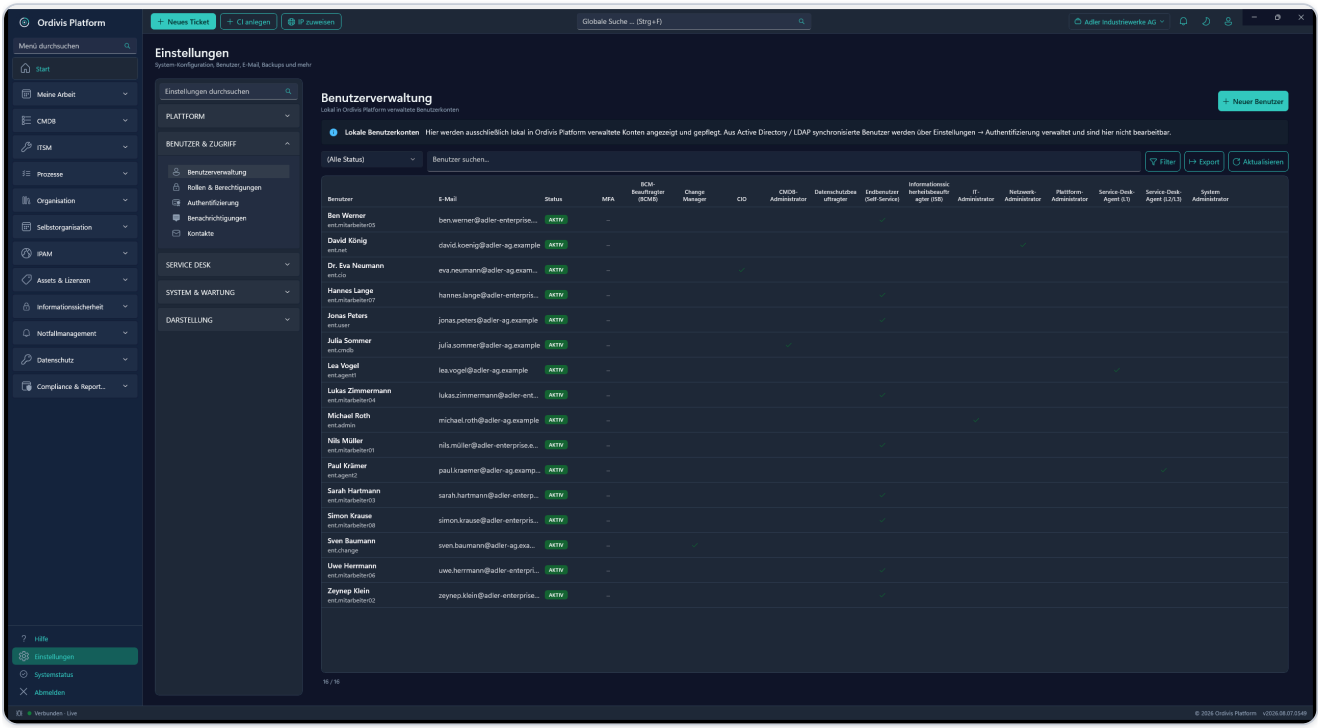

Abb. 2 – Benutzerverwaltung: je Benutzer die zugewiesenen Rollen als angehakte Spalten (Rollen-Matrix).

Beispiele wichtiger Rechte:

Recht	Bedeutung
`system.config.manage`	Administrator (Systemkonfiguration)
`identity.users.manage` / `identity.roles.manage`	Benutzer bzw. Rollen verwalten
`identity.permissions.manage`	Berechtigungen konfigurieren
`tickets.read.all`	alle Tickets (nicht nur Gruppe) sehen
`audit.read` / `audit.export`	Audit-Log lesen / exportieren
`system.security.manage`	Anmeldedaten/Sicherheit verwalten

6 Mehr-Faktor-Authentifizierung (MFA)

MFA ist **freiwillig**: Jeder Benutzer richtet sie für sein eigenes Konto selbst ein – dafür ist kein gesondertes Recht nötig und keines kann sie verhindern. Das **Zurücksetzen fremder** Geräte ist davon getrennt und

verlangt `identity.users.manage`.

6.1 Einrichten (Selbstbedienung)

> 💻 **Nur im Client:** Kopfleiste ▸ **Konto-Menü** (Personen-Symbol) ▸ *Zwei-Faktor-Authentifizierung* · 🔑 kein Recht nötig – jeder richtet seinen eigenen Faktor ein

🔒 **Pflichtreihenfolge — erst der bestätigte Code schaltet den zweiten Faktor scharf.** Brechen Sie den Dialog nach Schritt 1 ab, bleibt Ihr Konto unverändert – ein abgebrochener Versuch sperrt Sie also nicht aus.

1. Der Dialog zeigt einen **QR-Code** und daneben das **Base32-Geheimnis** im Klartext. Scannen Sie den Code mit einer Authenticator-App (Microsoft Authenticator, Google Authenticator, Aegis o. ä.) – oder tippen Sie das Geheimnis manuell ein, wenn Sie nicht scannen können.
2. Geben Sie den in der App angezeigten **6-stelligen Code** ein und bestätigen Sie mit *Aktivieren*.

✅ **Ergebnis:** Ab jetzt fragt die Anmeldung nach dem Kennwort zusätzlich nach dem Code – im Client wie im Portal.

Dasselbe Menü schaltet MFA auch wieder ab; der Eintrag wechselt je nach Stand.

Administratoren sehen den MFA-Stand eines Benutzers in der **Benutzerverwaltung** und können den zweiten Faktor dort **zurücksetzen** (etwa bei einem verlorenen Gerät). Danach ist das Konto wieder ohne zweiten Faktor erreichbar, bis der Benutzer ihn neu einrichtet.

> **Hinweis:** Ordivis Platform unterstützt als zweiten Faktor ausschließlich **TOTP** (zeitbasierte Codes, RFC 6238). FIDO2/Hardware-Schlüssel und E-Mail-Einmalcodes sind derzeit **nicht** verfügbar.

6.2 Anmelden mit dem zweiten Faktor

> 💻 **Client:** Anmeldeformular · 🌐 **Portal:** Anmeldeseite · 🔑 kein Recht nötig

Ist der zweite Faktor scharf, läuft die Anmeldung in **zwei Schritten** – das Kennwort allein genügt nicht mehr.

🔒 **Pflichtreihenfolge** — das Code-Feld erscheint erst, nachdem Kennwort und Benutzername abgeschickt wurden. Vorher gibt es nichts einzutragen.

1. Geben Sie **Benutzername** und **Kennwort** ein und schicken Sie ab.
2. Lesen Sie den **sechsstelligen Code** in Ihrer Authenticator-App ab.
3. Tragen Sie ihn in das Feld *Bestätigungscode* ein.
4. **Im Portal zusätzlich:** Geben Sie Benutzername und Kennwort **erneut** mit ein. Das Portal speichert das Kennwort zwischen den Schritten bewusst nicht zwischen.
5. Schicken Sie ab.

✅ **Ergebnis:** Sie sind angemeldet. Im Client bleiben Kennwort und Mandant nach einem falschen Code stehen; gelöscht wird nur der Code, damit der nächste Versuch ein Klick ist. Die Android-App verhält sich wie der Client.

Der Code ist **30 Sekunden** gültig; die Anwendung akzeptiert zusätzlich den unmittelbar vorangehenden und folgenden Zeitschritt, damit eine leicht abweichende Uhr nicht aussperrt. Ein falscher Code zählt als **Fehlversuch** und läuft in dieselbe Sperre wie ein falsches Kennwort.

> **Hinweis:** Der zweite Faktor tritt **neben** das Kennwort, nicht an seine Stelle. Ein gültiger Code mit falschem Kennwort wird abgewiesen.

6.3 Abschalten verlangt eine Bestätigung

Wer MFA aktiviert hat, muss das Abschalten **erneut bestätigen** – mit dem aktuellen Kennwort **oder** einem gültigen Code aus der Authenticator-App. Ohne Nachweis wird das Abschalten abgelehnt.

Warum: Sonst genügt eine übernommene Sitzung, um den zweiten Faktor still und dauerhaft zu entfernen – der Schutz wäre nur so stark wie das Session-Token.

Beide Wege sind nötig, nicht nur Komfort: Konten aus einem externen Verzeichnis (AD/SAML) haben kein lokales Kennwort und können sich ausschließlich per Code ausweisen.

> **Hinweis:** Solange die Einrichtung **nicht abgeschlossen** ist (kein bestätigtes Gerät), lässt sich der Vorgang ohne Nachweis abbrechen. Es gibt dann noch keinen zweiten Faktor zu schützen – und ein Konto ohne lokales Kennwort käme sonst weder per Kennwort noch per Code an ein Gerät heran, das es nie bestätigt hat.

7 Administrator-Limit (Lizenz)

Die Zahl der **Administratoren** (Benutzer mit `system.config.manage`) kann durch die Produktlizenz begrenzt sein.

> **Achtung:** Ist das Limit erreicht, wird das Anlegen eines Admins bzw. das Zuweisen einer Admin-Rolle mit **HTTP 402** abgelehnt. Siehe ID-43.

8 Verzeichnisbenutzer (AD/LDAP)

Über AD/LDAP synchronisierte Konten (read-only, ID-40) erhalten ihre Rollen ebenfalls hier. Der Sync ändert nie Daten im AD.

8.1 Welche Verzeichnisattribute übernommen werden

Übernommen wird jedes **Textattribut** des Kontos – die benannten Felder (Anzeigename, E-Mail, Abteilung, Telefon, Vorname, Nachname, Funktion) und zusätzlich der vollständige Rohsatz, aus dem sich die Benutzerkonto-CI speist (siehe Kapitel 21b).

Binäre Attribute werden übersprungen – Fotos, Zertifikate, Sicherheitskennungen. Sie tragen keinen lesbaren Text, und ihr Inhalt lässt sich nicht in einem Textfeld ablegen. Fehlt also ein Attribut im Verzeichnisabgleich, das im AD sichtbar ist, ist es mit hoher Wahrscheinlichkeit ein binäres.

8.2 Wie aus AD-Gruppen Rollen werden

In den Systemeinstellungen ordnen Sie AD-Gruppen Rollen zu (ID-40). Jeder Abgleich trägt die passenden Rollen nach.

Die Mitgliedschaft wird über alle Verschachtelungsebenen aufgelöst. Ordnen Sie die Gruppe eines Fachbereichs zu, erhalten auch die Personen ihre Rolle, die nur über eine Fachdienst-Gruppe darin hängen – und ebenso über weitere Zwischenstufen. Das ist der Normalfall in einer gewachsenen Verwaltung: Zugeordnet wird gewöhnlich die obere Gruppe, und darin liegen nicht die Personen, sondern wieder Gruppen. Die Auflösung rechnet der Verzeichnisserver selbst; für Ordivis Platform ist es eine Abfrage je zugeordneter Gruppe, unabhängig von der Zahl der Benutzer.

> **Zuweisen, nicht abgleichen:** Der Lauf **vergibt** Rollen, er nimmt keine weg. Entfernen Sie eine Zuordnung, behalten bereits versorgte Konten ihre Rolle – entziehen müssen Sie sie in der Benutzerverwaltung. So kann ein Fehlgriff in der Zuordnung niemanden aussperren.

Nach dem Ändern einer Zuordnung ist ein Abgleich nötig, damit die Rollen nachgetragen werden; rückwirkend geschieht das nicht von selbst. Wer sofort weiterarbeiten muss, bekommt die Rolle direkt zugewiesen – sie wirkt binnen fünf Minuten.

Was der Lauf meldet. Das Protokoll nennt angelegte und aktualisierte Konten, angetroffene Gruppen und vergebene Rollen. Dabei zählt „Rollen zugewiesen" nur die **neuen** – eine `0` bedeutet also nicht, dass niemand eine Rolle hat, sondern dass sich nichts geändert hat. Gewarnt wird, wenn

- keine Zuordnung hinterlegt ist,
- eine zugeordnete Gruppe bei **keinem** Benutzer angetroffen wurde (umbenannt? verschoben?), oder
- **mehr** Benutzer ohne Rolle dastehen als beim vorigen Lauf.

Der reine Bestand an Konten ohne Rolle ist bewusst **keine** Warnung: Dienst- und Funktionskonten sind zu Recht rollenlos, in größeren Verwaltungen mehrere Hundert. Eine Warnung, die bei jedem Lauf erscheint, wird nicht mehr gelesen – und der eine Lauf, an dem wirklich etwas kippt, ginge darin unter. Den Bestand sehen Sie in der Verzeichnis-Ansicht.

> **Ein Konto ohne Rolle hat kein einziges Recht.** Die Anmeldung gelingt, danach wird jeder Aufruf abgewiesen; im Self-Service-Portal meldet „Meine Vorgänge" nur, dass sich nichts laden lässt. Wer das als Ausfall gemeldet bekommt, prüft zuerst die Rollenzuordnung.

Verwandte Themen

- **ID-44 – Rollen- & Rechte-Matrix** – der vollständige Rechtekatalog
- **ID-40 – Administrationshandbuch** – Ersteinrichtung und Systemeinstellungen

- **ID-42 – Modul Mandantenfähigkeit** – Benutzer in mehreren Mandanten
- **ID-21b – Benutzerkonten in der CMDB** – dieselben Konten als Configuration Item