

FÜR ANWENDER UNTERWEGS

Mobil-App – Ordivis IT auf dem Android-Telefon

Die Android-App – einrichten, anmelden, melden, scannen, Inventur und Alarme

Produktversion 2026.10.03 · Handbuch-Revision 2.1
Stand 03.10.2026 · Plattform .NET 10 / Windows Server

ID-13 Mobil-App

Mobil-App – Ordavis IT auf dem Android-Telefon

Die **Ordavis-App** bringt Ordavis IT auf das Diensttelefon. Mitarbeitende melden damit eine Störung und verfolgen ihre Vorgänge, ohne einen Rechner zu brauchen. Technik und Service-Desk bearbeiten unterwegs Tickets, scannen Geräte-Etiketten, ordnen NFC-Tags zu und zählen bei der Inventur. Wer Bereitschaft hat, bekommt Alarme aufs Telefon und beantwortet sie dort.

Dieses Dokument beschreibt die App vollständig: wie sie auf das Telefon kommt, wie sie sich mit Ihrem Server verbindet, was jeder Reiter kann, was ohne Netz geht und was nicht, wie Benachrichtigungen und Alarme ankommen und wie die App sich aktualisiert.

Auf einen Blick: Die App gibt es **nur für Android** (ab Android 6.0), nicht für iPhone. Sie kommt **nicht aus dem Play Store**, sondern als Datei vom Hersteller. Sie spricht mit **Ihrem** Ordavis-Server; ein Google-Konto braucht sie nicht. Nur die Push-Benachrichtigungen setzen die Google-Play-Dienste voraus (Abschnitt 12).

INHALT**1 Was die App ist**

- 1.1 Aufbau der App
- 1.2 Was die App nicht kann

2 Voraussetzungen und Rechte

- 2.1 Das Telefon
- 2.2 Server und Netz
- 2.3 Rechte

3 Installieren

- 3.1 Woher die App kommt
- 3.2 Auf einem einzelnen Telefon installieren
- 3.3 Über eine Geräteverwaltung (MDM) verteilen

4 Mit dem Server verbinden

- 4.1 Serveradresse eintragen
- 4.2 Wie die App die Adresse ergänzt
- 4.3 Eigenes Serverzertifikat: Fingerabdruck bestätigen
- 4.4 Mehrere Server: Verbindungen merken und umschalten

5 Anmelden, angemeldet bleiben, abmelden

- 5.1 Anmelden
- 5.2 Was bei der Anmeldung geschieht
- 5.3 Wie lange Sie angemeldet bleiben
- 5.4 Gemarkte Anmeldung biometrisch schützen
- 5.5 Abmelden
- 5.6 Anmeldung am Arbeitsplatz per App freigeben

6 Reiter Start**7 Reiter Tickets**

- 7.1 Vorgänge finden
- 7.2 Ticket übernehmen
- 7.3 Status setzen und lösen
- 7.4 Interne Notiz schreiben
- 7.5 Vorgang melden
- 7.6 Leistung aus dem Katalog bestellen

8 Reiter Geräte

- 8.1 Gerät suchen und Steckbrief öffnen
- 8.2 Trefferliste als CSV weitergeben
- 8.3 Wareneingang buchen
- 8.4 NFC-Tag zuordnen
- 8.5 NFC-Zuordnung lösen

9 Reiter Scannen

- 9.1 Etiketten scannen
- 9.2 Was die App mit einem Code macht
- 9.3 Inventur

10 Weitere Kacheln der Startseite

- 10.1 Netze
- 10.2 Wissen und Kennzahlen
- 10.3 Handbücher und Checklisten für den Notfall mitnehmen
- 10.4 Checkliste abarbeiten
- 10.5 Sicherungsprüfung abschließen

11 Ohne Netz arbeiten

- 11.1 Was ohne Netz geht
- 11.2 Liegegebliebenes senden
- 11.3 Abgelehnte und kollidierende Handlungen

12 Benachrichtigungen und Alarme

- 12.1 Was aufs Telefon kommt
- 12.2 Push für ein Ereignis einschalten
- 12.3 Das Telefon für Alarme vorbereiten
- 12.4 Einen Alarm beantworten
- 12.5 Ruhezeit einstellen

13 Aktualisierung und Mindestfassung

- 13.1 Hinweis beim Start und Pflichtband
- 13.2 Von Hand aktualisieren

14 Sicherheit und Datenschutz

- 14.1 Meine Geräte: ein Gerät abmelden
- 14.2 Ein Gerät im Windows-Client abmelden
- 14.3 Lokale Daten löschen
- 14.4 Was auf dem Telefon liegt

15 Referenz: die Einstellungsseite der App

16 Fehlerbehebung

17 Beispiele aus der Praxis

- 17.1 Beispiel: Inventur im Bauhof Musterstadt
- 17.2 Beispiel: Ein Ticket unterwegs lösen
- 17.3 Beispiel: Ein neues Diensttelefon für die Bereitschaft einrichten

18 Häufige Fragen

Verwandte Themen

1 Was die App ist

Die App heißt auf dem Telefon **Ordavis IT**. Sie ist kein Fernzugriff auf den Windows-Client und keine Kopie des Portals, sondern eine eigene Oberfläche für die Aufgaben, die man unterwegs erledigt. Sie arbeitet mit denselben Daten und denselben Rechten wie Client und Portal: Was Sie dort nicht dürfen, dürfen Sie in der App auch nicht.

1.1 Aufbau der App

Startbild. Beim Öffnen läuft für etwa fünf Sekunden ein Startbild mit Ton. Antippen überspringt es. Sind in Android die Animationen abgeschaltet, bleibt das Bild stehen und der Ton entfällt; er entfällt auch, wenn die Medienlautstärke auf null steht oder gerade Musik läuft.

Untere Leiste. Vier Reiter führen zu den Hauptseiten:

Reiter	Wofür	Erscheint nur mit
<i>Start</i>	Begrüßung, Zähler, Schnellzugriff, Warteschlange	– (immer)
<i>Tickets</i>	eigene Vorgänge und die der Gruppe	<code>tickets.self.read</code> oder <code>tickets.read</code>
<i>Geräte</i>	Gerätebestand durchsuchen, Steckbrief	<code>cmdb.ci.read</code>
<i>Scannen</i>	Kamera und NFC für Etiketten	<code>cmdb.ci.read</code>

Kopfzeile. Oben auf jeder Hauptseite steht das **Zahnrad** – es öffnet die *Einstellungen*. Daneben zeigt ein **farbiger Punkt** den Verbindungsstand: grün verbunden, gelb oder rot gestört.

Melden. Auf *Start*, *Tickets* und *Geräte* schwebt unten die Schaltfläche *Melden*. Sie öffnet das Formular für eine neue Meldung (Abschnitt 7.5). Ohne das Recht `tickets.create` fehlt sie.

Schnellzugriff. Die Startseite trägt Kacheln für alles, was keinen eigenen Reiter hat – Inventur, Netze, Wissen, Kennzahlen, Handbücher, Checklisten, Sicherungsprüfungen, Meine Alarme und den Katalog. Welche erscheinen, hängt an Ihren Rechten (Abschnitt 2.3).

1.2 Was die App nicht kann

Damit Sie nicht vergeblich suchen – diese Dinge gibt es in der App **nicht**:

Gesucht	Wo es stattdessen geht
ein neues Gerät (CI) anlegen	Windows-Client oder Portal (ID-21)
dem Melder antworten – die App schreibt nur interne Notizen	Windows-Client oder Portal (ID-11)
eine Liste der Benachrichtigungen (Glocke)	Windows-Client oder Portal (ID-31)
festlegen, welche Ereignisse aufs Telefon kommen	nur im Windows-Client (Abschnitt 12.2)
die eigene Ruhezeit für Alarme einstellen	nur im Windows-Client (Abschnitt 12.5)
eine Inventur abschließen und auswerten	Windows-Client, Portal zum Ansehen (Abschnitt 9.3)
Geräte ohne Netz suchen	– (Abschnitt 11.1)
Etiketten drucken	Windows-Client (ID-21)
die Verbindung per QR-Code koppeln	– die Adresse wird eingetragen oder per Geräteverwaltung vorgegeben
sich selbst per App-Freigabe anmelden	– in der App gelten Kennwort und Einmalcode (Abschnitt 5.6)
ein iPhone	– die App gibt es nur für Android

2 Voraussetzungen und Rechte

2.1 Das Telefon

Was	Voraussetzung
Android	ab 6.0
Biometrischer Schutz der gemerkten Anmeldung	ab Android 11 , mit eingerichtetem Fingerabdruck, Gesicht oder einer Gerätesperre
Push-Benachrichtigungen und Alarme	Google-Play-Dienste auf dem Gerät, Benachrichtigungen für die App erlaubt (ab Android 13 fragt Android danach)
Scannen	Kamera, Freigabe <i>Kamera</i> für die App
NFC-Tags	NFC-Hardware; ohne sie blendet die App alles zu NFC aus
Speicher	Die App-Datei misst rund 40 MB; beim Aktualisieren kommt die nächste Fassung noch einmal dazu.

2.2 Server und Netz

- Die Adresse der Schnittstelle (API) Ihres Ordavis-Servers, mit Schema und Port – zum Beispiel `https://ordavis.musterstadt.local:5001`. Das ist **nicht** die Adresse des Portals. Ihre IT-Abteilung nennt sie Ihnen.
- Ein Weg vom Telefon zum Server: im WLAN des Hauses oder unterwegs über ein VPN. Ohne diesen Weg meldet die App, dass der Server nicht erreichbar ist.
- Für Updates einen Weg ins Internet: Die App holt neue Fassungen beim Hersteller (`update.ordavis.eu`), nicht bei Ihrem Server (Abschnitt 13).
- Für Push: Ihr Server muss online aktiviert sein; Einzelheiten zur Zustellung stehen in ID-40.

2.3 Rechte

Die App blendet nur ein, wofür Sie das Recht haben. Durchgesetzt werden die Rechte vom Server – eine Schaltfläche, die Sie nicht sehen, würde der Server ohnehin abweisen.

Recht	Was es in der App freischaltet
<code>tickets.create</code>	Schaltfläche <i>Melden</i> , <i>Vorgang melden</i> am Gerät
<code>tickets.self.read</code>	Reiter <i>Tickets</i> mit den eigenen Vorgängen, Zähler „ <i>offen bei mir</i> “
<code>tickets.read</code>	Reiter <i>Tickets</i> mit den Vorgängen der Gruppe, Zähler „ <i>offen im Team</i> “
<code>tickets.assign</code>	<i>Mir zuweisen</i> im Ticket
<code>tickets.update</code>	<i>Status setzen</i> und <i>Notiz</i> im Ticket
<code>cmdb.ci.read</code>	Reiter <i>Geräte</i> und <i>Scannen</i> , Steckbrief
<code>cmdb.ci.update</code>	Kachel <i>Inventur</i> , <i>Wareneingang buchen</i> , <i>Tag zuordnen und beschreiben</i>
<code>audit.read</code>	Abschnitt <i>Historie</i> im Steckbrief
<code>ipam.prefix.read</code>	Kachel <i>Netze</i> (Bereiche durchsuchen)
<code>ipam.ip.read</code>	<i>Adresse nachschlagen</i> , <i>Nächste freie Adresse</i>
<code>knowledge.read.internal</code>	Kachel <i>Wissen</i>
<code>reporting.read</code>	Kachel <i>Kennzahlen</i>
<code>handbook.read</code>	Kachel <i>Handbücher</i>
<code>checklist.read</code>	Kachel <i>Checklisten</i>
<code>checklist.run.execute.self</code>	Prüfpunkte einer zugewiesenen Checkliste abhaken
<code>backup.read</code>	Kachel <i>Sicherungsprüfungen</i>
<code>backup.verify</code>	Eine Sicherungsprüfung <i>Abschließen</i>
<code>ticketing.service_catalog.read</code>	Kachel <i>Katalog</i> (zusammen mit <code>tickets.create</code>)

Die Kachel *Meine Alarme* braucht kein Recht: Der Server zeigt jedem nur die Alarme, in deren Empfängerkreis er steht. Sie setzt aber voraus, dass das Modul Notfallmanagement eingeschaltet ist.

Beispiel Rolle *Enduser*: Eine Mitarbeiterin mit der mitgelieferten Rolle *Enduser* sieht die Reiter *Start* und *Tickets*, die Schaltfläche *Melden* und die Kacheln *Checklisten*, *Katalog* und *Meine Alarme*. *Geräte*, *Scannen* und *Wissen* sieht sie nicht – die Rolle trägt nur das Leserecht für **öffentliche** Wissensartikel, und die liest man im Portal. Den vollständigen Rechtekatalog enthält ID-44.

3 Installieren

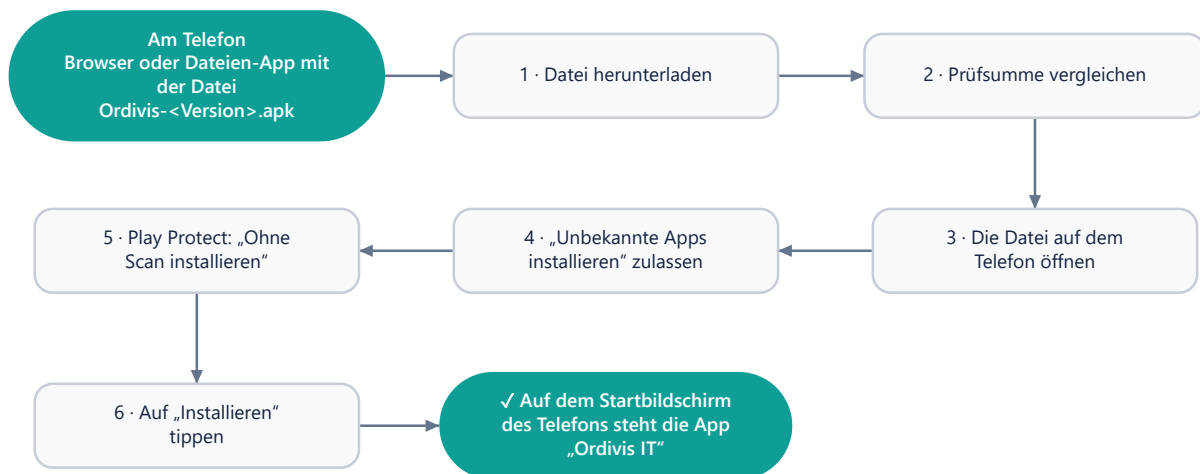
3.1 Woher die App kommt

Die App wird als fertiges Android-Paket (**APK**) ausgeliefert, mit der Paketkennung `eu.ordavis.plattform`. Sie liegt im **Kundenbereich** des Herstellers, neben jeder Datei ihre **SHA-256-Prüfsumme** (`.sha256`). Damit belegen Sie vor dem Verteilen, dass Sie dieselbe Datei in der Hand haben, die der Hersteller gebaut hat.

Hinweis: Windows-Client und Portal bieten **keinen** Download der App an. Den Bezug regelt Ihre IT-Abteilung – auf verwalteten Geräten über die Geräteverwaltung (Abschnitt 3.3), auf einzelnen Geräten über eine Datei, die Ihre IT bereitstellt.

3.2 Auf einem einzelnen Telefon installieren

 **Am Telefon:** Browser oder Dateien-App mit der Datei `Ordavis-<Version>.apk` ·  Bedienung des Telefons, kein Ordavis-Recht



Klickweg – Auf einem einzelnen Telefon installieren

 **Pflichtreihenfolge** – erst prüfen, dann installieren.

1. Laden Sie die Datei herunter. Meldet Chrome „Die Datei könnte schädlich sein“, tippen Sie auf *Trotzdem herunterladen*.
2. Vergleichen Sie die Prüfsumme der Datei mit dem Wert aus der `.sha256`-Datei, etwa am Rechner mit `Get-FileHash <datei> -Algorithm SHA256`.
3. Öffnen Sie die Datei auf dem Telefon.
4. Schalten Sie unter *Unbekannte Apps installieren* die Freigabe für den Browser oder die Dateien-App ein, wenn Android danach fragt.

5. Tippen Sie bei der Meldung von Play Protect auf *Weitere Details* und dann auf *Ohne Scan installieren*.

6. Tippen Sie auf *Installieren*.

✓ **Ergebnis:** Auf dem Startbildschirm des Telefons steht die App **Ordavis IT**. Beim ersten Öffnen zeigt sie „Willkommen bei Ordavis IT“ – weiter geht es mit Abschnitt 4.

Hinweis: Die Warnungen von Chrome und Play Protect erscheinen bei **jeder** App, die nicht aus dem Play Store kommt. Sie sagen nichts über diese App aus. Die Prüfsumme sagt es: Stimmt sie, ist es die Datei des Herstellers. Die App ist mit dem Schlüssel des Herstellers signiert; Android nimmt später kein Update an, das diesen Schlüssel nicht trägt.

3.3 Über eine Geräteverwaltung (MDM) verteilen

Auf verwalteten Telefonen verteilt Ihre Geräteverwaltung (MDM) das Paket wie jede hauseigene App, etwa über *Managed Google Play* oder als hochgeladenes APK. Dabei lässt sich die **Verbindung zentral vorgeben**, sodass auf dem Telefon nichts eingetippt werden muss. Die App bringt dafür eine *Managed Configuration* mit; die Felder erscheinen in der MDM-Konsole unter diesen Namen:

Feld in der MDM-Konsole	Schlüssel	Bedeutung
Eigene Serveradresse zulassen	<code>allowCustom</code>	Ja/Nein, Vorgabe Nein . Mit <i>Ja</i> darf die Person neben der Liste eine eigene Adresse eintragen – gedacht als Notausgang, wenn eine falsche Vorgabe alle aussperrt.
Ordavis-Installationen	<code>connections</code>	Liste der Server, zwischen denen auf der Anmeldeseite gewechselt wird. Der erste Eintrag gilt beim ersten Start.
Kennung	<code>id</code>	Kurze, gleichbleibende Kennung, zum Beispiel <code>hv</code> . Sie hält die Auswahl fest, auch wenn sich die Adresse ändert.
Anzeigenname	<code>name</code>	So erscheint die Installation auf der Anmeldeseite, zum Beispiel <i>Hauptverwaltung</i> .
API-Adresse	<code>apiBaseUrl</code>	Vollständige Adresse mit Schema und Port, zum Beispiel <code>https://ordavis.musterstadt.local:5001</code> .
Fingerabdruck des Serverzertifikats (SHA-256)	<code>certificateFingerprint</code>	Nur für ein eigenes Serverzertifikat ohne Zertifizierungsstelle (Abschnitt 4.3); gilt nur für diese eine Installation.

Rangfolge. Die App nimmt die Verbindung aus der ersten Quelle, die etwas vorgibt:

1. die Managed Configuration der Geräteverwaltung,
2. die mit der App ausgelieferte `appsettings.json` (Abschnitt `Api` mit `BaseUrl`, `AllowCustom` und `Connections`) – nur bei einem eigenen Bau der App von Bedeutung,
3. die Adresse, die die Person selbst eingetragen hat.

Gibt die Geräteverwaltung eine Liste vor, zeigt die Seite *Serveradresse* „Die Verbindungen gibt der Administrator vor.“ und darunter, woher die Vorgabe kommt. Die Adresse lässt sich dann nicht ändern; *Speichern und verbinden* prüft nur noch die Verbindung. Ab **zwei** Einträgen erscheint auf der Anmeldeseite das Feld *INSTALLATION*.

Hinweis: Wie die Selbstaktualisierung der App (Abschnitt 13) mit einer Verteilung über die Geräteverwaltung zusammenspielt, regelt die App nicht: Sie bietet ein Update an, sobald der Hersteller eine neue Fassung veröffentlicht – auch wenn Ihre Geräteverwaltung noch die alte verteilt. Stimmen Sie die beiden Wege in Ihrem Betrieb ab.

4 Mit dem Server verbinden

Bevor sich jemand anmelden kann, muss die App wissen, mit welchem Server sie spricht. Auf verwalteten Geräten ist das schon geschehen (Abschnitt 3.3); sonst tragen Sie die Adresse einmal ein. Abbildung 1 zeigt den Weg vom ersten Start bis zur Anmeldung.

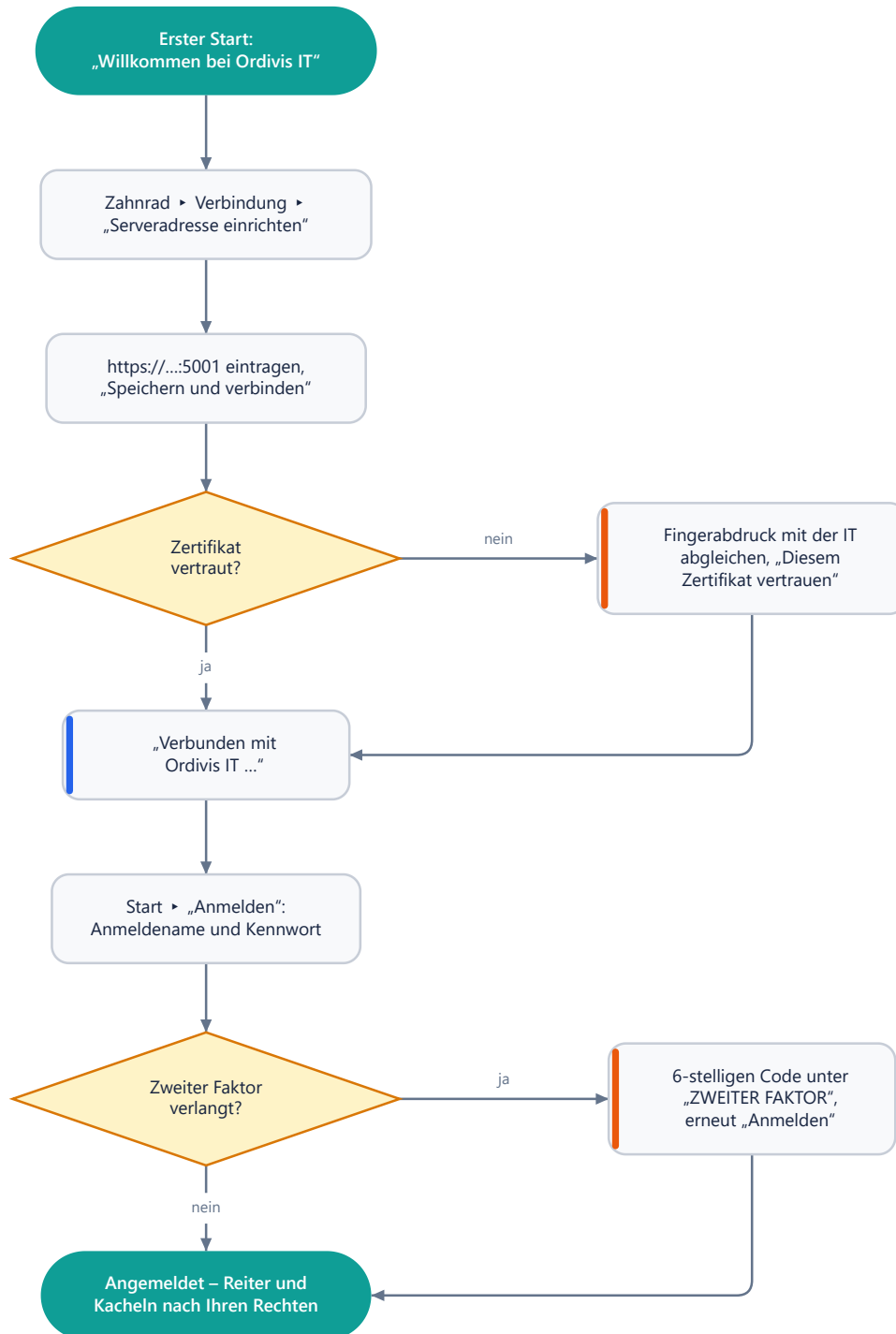
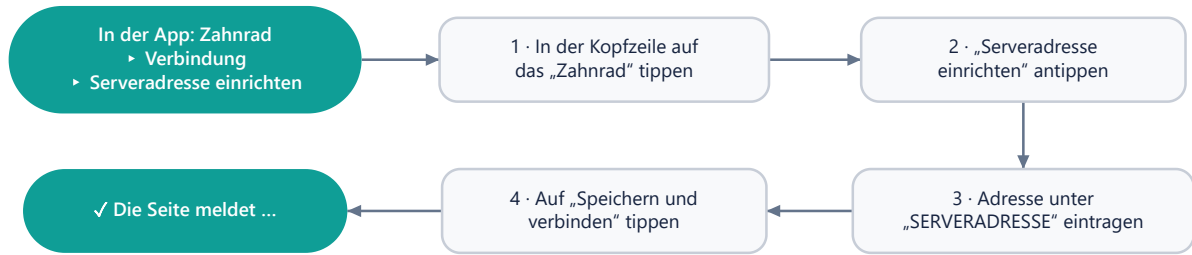


Abb. 1 – Erste Einrichtung: Serveradresse, Zertifikat und Anmeldung.

4.1 Serveradresse eintragen

 **In der App:** Zahnrad ▶ Verbindung ▶ Serveradresse einrichten ·  kein Recht nötig – die Adresse gehört zum Telefon, nicht zum Konto

Voraussetzung: Sie kennen die Adresse der Ordavis-Schnittstelle, mit `https://` und Port.



Klickweg – Serveradresse eintragen

1. Tippen Sie in der Kopfzeile auf das *Zahnrad*.
2. Tippen Sie im Abschnitt *Verbindung* auf *Serveradresse einrichten* (ist schon eine Adresse eingetragen, heißt die Schaltfläche *Serveradresse ändern*).
3. Tragen Sie unter *SERVERADRESSE* die vollständige Adresse ein, zum Beispiel `https://ordavis.musterstadt.local:5001`.
4. Tippen Sie auf *Speichern und verbinden*.

✓ **Ergebnis:** Die Seite meldet „Verbunden mit Ordavis IT 2026.10.01.1643 (Stand ...)“ – mit der Fassung Ihres Servers. Der Punkt in der Kopfzeile wird grün, und auf der Startseite steht die Schaltfläche *Anmelden*.

Meldet die App stattdessen „Das Serverzertifikat ist nicht vertrauenswürdig. Sein Fingerabdruck: ...“, geht es in Abschnitt 4.3 weiter. Alle übrigen Meldungen erklärt Abschnitt 16.

4.2 Wie die App die Adresse ergänzt

Die App speichert jede Adresse in der Form `schema://rechner:port`. Fehlt etwas, ergänzt sie es nach dieser Regel:

Sie tragen ein	Die App speichert	Warum
<code>https://ordavis.musterstadt.local:5001</code>	unverändert	vollständig
<code>ordavis.musterstadt.local</code>	<code>https://ordavis.musterstadt.local:443</code>	ohne Schema und ohne Port: https
<code>server:5000</code>	<code>http://server:5000</code>	ohne Schema, aber mit Port: http
<code>https://ordavis.musterstadt.local:5001/portal</code>	<code>https://ordavis.musterstadt.local:5001</code>	Pfad und Zusätze fallen weg

Achtung: Schreiben Sie das Schema immer aus. Wer `ordavis.musterstadt.local:5001` ohne `https://` einträgt, bekommt `http://...:5001` – an diesem Port antwortet der Server aber mit HTTPS, und die Verbindung scheitert. Der Hilfetext unter dem Feld sagt noch „Ohne http:// oder https:// wird http angenommen.“ – das gilt nur, wenn ein Port dabeisteht.

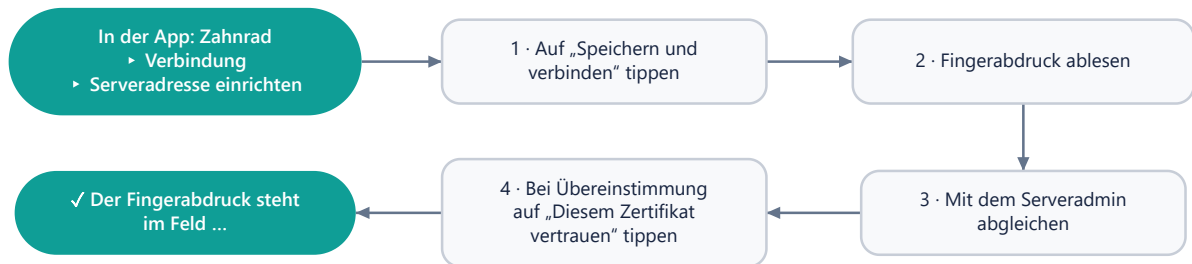
Achtung: unverschlüsselte Verbindung. Bei einer `http://`-Adresse zeigt die App auf der Seite *Serveradresse* und auf der Anmeldeseite ein gelbes Band: Kennwort und Daten gehen im Klartext über das Netz. Diese Fassung verbindet noch; laut Ankündigung lässt die nächste Fassung der App nur noch `https://` zu. Lassen Sie den Server auf HTTPS umstellen (ID-50, Abschnitt 7) und passen Sie die Adresse an.

4.3 Eigenes Serverzertifikat: Fingerabdruck bestätigen

Läuft Ihr Server mit einem Zertifikat, das Android nicht kennt – etwa selbst ausgestellt oder von einer internen Zertifizierungsstelle, die nicht auf dem Telefon hinterlegt ist –, lehnt die App die Verbindung zunächst ab und zeigt den **Fingerabdruck** des Zertifikats. Vertrauen Sie ihm erst, wenn er mit dem Wert Ihres Serveradministrators übereinstimmt.

⚙️ In der App: *Zahnrad* ▶ *Verbindung* ▶ *Serveradresse einrichten* · 🔑 kein Recht nötig

Voraussetzung: Die Adresse beginnt mit `https://`. Die Karte für den Fingerabdruck erscheint nur bei HTTPS.



Klickweg – Eigenes Serverzertifikat: Fingerabdruck bestätigen

🔒 **Pflichtreihenfolge** – erst abgleichen, dann vertrauen.

1. Tippen Sie auf *Speichern und verbinden*.
2. Lesen Sie den Fingerabdruck aus der Meldung „Das Serverzertifikat ist nicht vertrauenswürdig. Sein Fingerabdruck: ...“ vollständig ab.
3. Vergleichen Sie ihn Zeichen für Zeichen mit dem Fingerabdruck, den Ihnen der Serveradministrator nennt.
4. Tippen Sie bei Übereinstimmung auf *Diesem Zertifikat vertrauen*.

✅ **Ergebnis:** Der Fingerabdruck steht im Feld *Fingerabdruck des Serverzertifikats (SHA-256, optional)*, die App verbindet sich und meldet „Verbunden mit Ordvis IT ...“. Ab jetzt nimmt sie für diese Verbindung genau dieses Zertifikat an – und kein anderes.

Kennen Sie den Fingerabdruck schon vorher, tragen Sie ihn gleich in das Feld ein, bevor Sie auf *Speichern und verbinden* tippen. Erlaubt sind 64 Hexadezimalzeichen, mit oder ohne Doppelpunkte. Den Wert am Server ermitteln beschreibt ID-50, Abschnitt 7.2.

Achtung: Stimmen die Werte **nicht** überein, vertrauen Sie dem Zertifikat nicht. Dann antwortet unter der Adresse ein anderes Gerät als Ihr Server. Wird das Serverzertifikat erneuert, ändert sich der Fingerabdruck – die App lehnt dann wieder ab, und der Abgleich ist neu zu machen.

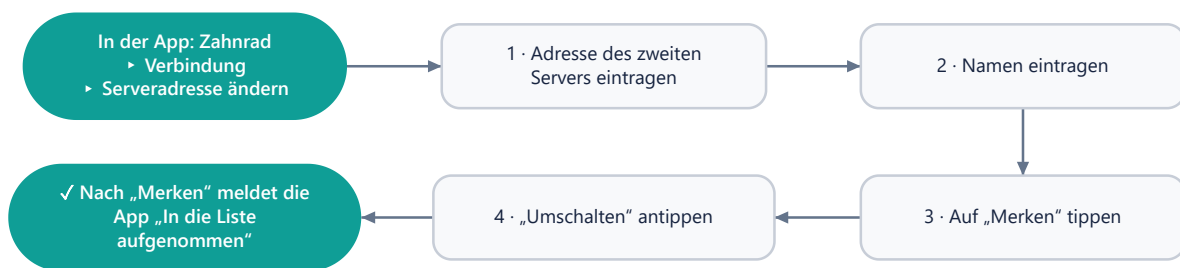
Hinweis: Einen Schalter „Zertifikatfehler übergehen“ gibt es nicht. Stammt das Zertifikat von einer Zertifizierungsstelle, der Android vertraut – etwa einer öffentlichen –, ist kein Fingerabdruck nötig.

4.4 Mehrere Server: Verbindungen merken und umschalten

Wer mit mehreren getrennten Ordavis-Installationen arbeitet – etwa Hauptverwaltung und Testsystem –, kann bis zu **zwölf** Verbindungen in der App merken und mit einem Griff umschalten. Jede Verbindung hat ihre **eigene Anmeldung** und ihren **eigenen Offline-Bestand**; beim Umschalten geht nichts verloren.

 **In der App:** *Zahnrad* ▶ *Verbindung* ▶ *Serveradresse ändern* ·  kein Recht nötig

Voraussetzung: Die Geräteverwaltung gibt keine Liste vor, oder sie lässt eine eigene Adresse zu (Abschnitt 3.3). Sonst fehlen die Felder zum Merken.



Klickweg – Mehrere Server: Verbindungen merken und umschalten

1. Tragen Sie unter *SERVERADRESSE* die Adresse des zweiten Servers ein, zum Beispiel `https://test.musterstadt.local:5001`.
2. Tragen Sie unter *Name* (*frei lassen für die Adresse*) einen Namen ein, zum Beispiel `Testsystem`.
3. Tippen Sie auf *Merken*.
4. Tippen Sie unter *Gemerkte Verbindungen* beim gewünschten Eintrag auf *Umschalten*.

✓ **Ergebnis:** Nach *Merken* meldet die App „In die Liste aufgenommen.“; nach *Umschalten* arbeitet sie mit dem gewählten Server. Sind zwei oder mehr Verbindungen bekannt, steht auf der Anmeldeseite das Feld *INSTALLATION* zur Auswahl.

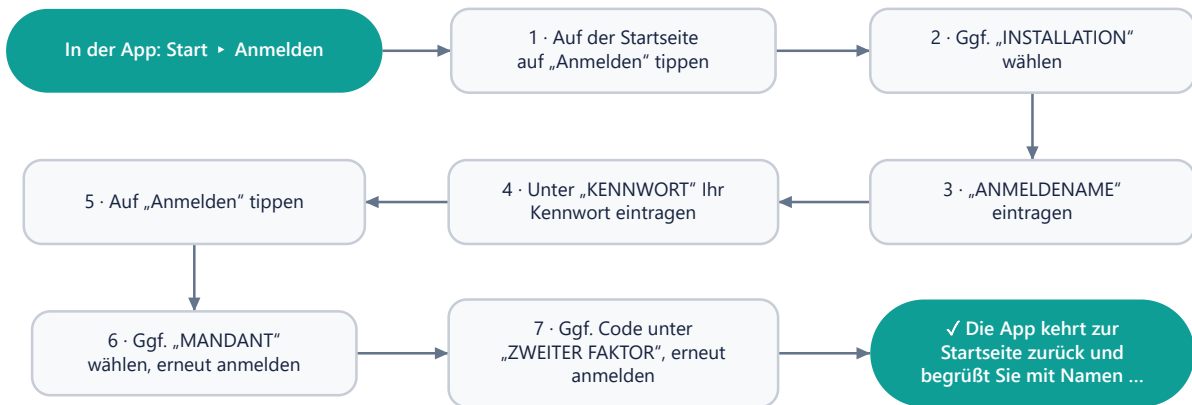
Merken legt eine Adresse nur in die Liste, *Speichern und verbinden* schaltet sofort auf sie um. *Entfernen* löscht einen Eintrag aus der Liste – nicht aber die Verbindung, mit der die App gerade arbeitet; dafür erst umschalten.

5 Anmelden, angemeldet bleiben, abmelden

5.1 Anmelden

 **In der App:** *Start* ▶ *Anmelden* ·  ein aktives Ordavis-Konto

Voraussetzung: Die Serveradresse ist eingerichtet (Abschnitt 4.1).



Klickweg – Anmelden

1. Tippen Sie auf der Startseite auf *Anmelden*.
2. Wählen Sie unter *INSTALLATION* den Server, falls das Feld erscheint.
3. Tragen Sie unter *ANMELDENAME* Ihren Anmeldenamen ein, zum Beispiel `m.muster`.
4. Tragen Sie unter *KENNWORT* Ihr Kennwort ein.
5. Tippen Sie auf *Anmelden*.
6. Wählen Sie unter *MANDANT* den Mandanten, wenn die App „Bitte den Mandanten wählen und erneut anmelden.“ meldet, und tippen Sie erneut auf *Anmelden*.
7. Tragen Sie unter *ZWEITER FAKTOR* den 6-stelligen Code aus Ihrer Authenticator-App ein, wenn die App „Zweiter Faktor nötig — Code aus der Authenticator-App eingeben.“ meldet, und tippen Sie erneut auf *Anmelden*.

✓ **Ergebnis:** Die App kehrt zur Startseite zurück und begrüßt Sie mit Namen und Mandant. Unten erscheinen die Reiter, für die Sie Rechte haben.

Hinweis: Die Felder *MANDANT* und *ZWEITER FAKTOR* erscheinen nur, wenn sie gebraucht werden: *MANDANT* bei mehreren Mandanten zum Anmeldenamen, *ZWEITER FAKTOR* bei einem Konto mit zweitem Faktor. Das Kennwort bleibt dabei stehen, Sie tippen nur noch den Code. Ist der Code falsch oder abgelaufen, leert die App Kennwort und Code; dann beides neu eingeben.

5.2 Was bei der Anmeldung geschieht

Mit der ersten Anmeldung **meldet sich das Telefon beim Server an**. Es erscheint danach in der Liste *Meine Geräte* (Abschnitt 14.1) – mit dem Gerätenamen aus Android oder, wenn keiner gesetzt ist, mit Hersteller und Modell. Bei jeder Anmeldung geschieht außerdem:

- **Benachrichtigungen:** Ab Android 13 fragt das System einmal, ob die App Benachrichtigungen schicken darf. Nur mit dieser Erlaubnis meldet sich die App beim Zustelldienst an (Abschnitt 12).
- **Geräteschlüssel:** Die App legt im Schlüsselspeicher des Telefons einen eigenen Schlüssel an und meldet den öffentlichen Teil beim Server. Er wird für die *Anmeldung per App* gebraucht (Abschnitt 5.6). Scheitert das, meldet die App nichts – die Anmeldung gelingt trotzdem.
- **Gemerkte Anmeldung:** Die App merkt sich die Anmeldung für den nächsten Start (Abschnitt 5.3).

Eine Anmeldung in der App **beendet keine** Sitzung am Arbeitsplatz, und eine Anmeldung am Arbeitsplatz beendet keine in der App. Eine neue Anmeldung auf demselben Telefon ersetzt nur die vorige auf diesem Telefon.

5.3 Wie lange Sie angemeldet bleiben

Was	Dauer	Was danach geschieht
Zugriff der laufenden Sitzung	10 Minuten	verlängert sich von selbst, solange die App genutzt wird
gemerkte Anmeldung	12 Stunden ohne Nutzung	„Die Sitzung ist abgelaufen. Bitte erneut anmelden.“

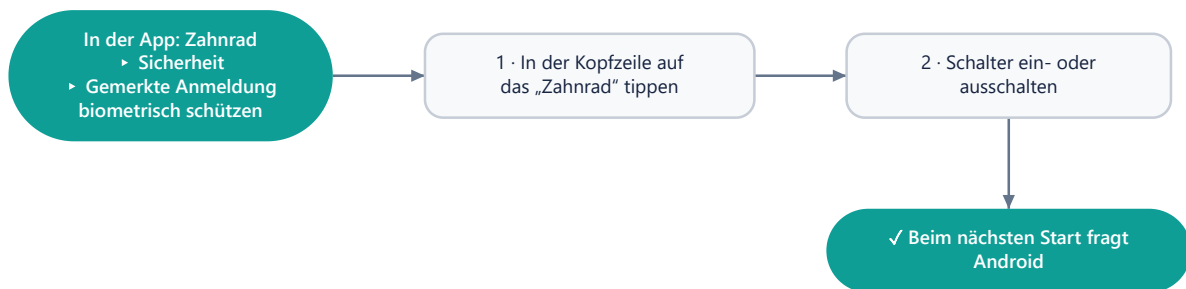
Die Einstellungsseite zeigt unter *SITZUNG* „gültig bis ...“, danach wird automatisch verlängert“. Die Werte setzt der Betrieb am Server (`Identity:Jwt:MobileAccessTokenExpiryMinutes` und `Identity:Jwt:MobileRefreshTokenExpiryHours` , ID-50); für den Arbeitsplatz gelten eigene Werte.

5.4 Gemarkte Anmeldung biometrisch schützen

Ist der Schutz an, setzt die App eine gemerkte Anmeldung beim Start erst fort, wenn Sie mit Fingerabdruck, Gesicht oder der Gerätesperre bestätigen. Er ist **von Haus aus eingeschaltet**. Die Prüfung macht allein Android; die App erfährt nur, ob bestätigt wurde.

⚙️ In der App: *Zahnrad* ▶ *Sicherheit* ▶ *Gemarkte Anmeldung biometrisch schützen* · 🔑 kein Recht nötig

Voraussetzung: Android 11 oder neuer, und auf dem Telefon ist Fingerabdruck, Gesicht oder eine Gerätesperre eingerichtet. Sonst fehlt der Abschnitt mit dem Schalter.



Klickweg – Gemarkte Anmeldung biometrisch schützen

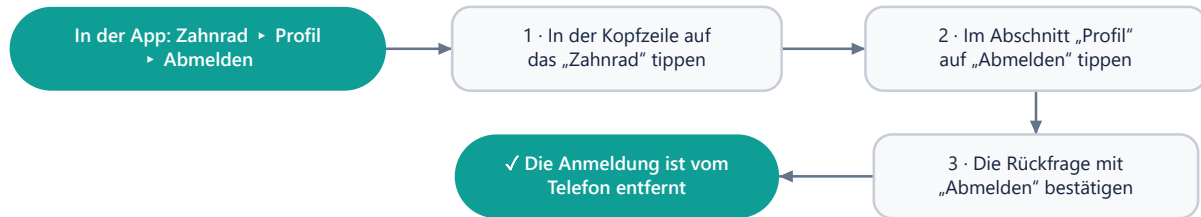
1. Tippen Sie in der Kopfzeile auf das *Zahnrad*.
2. Schalten Sie im Abschnitt *Sicherheit* den Schalter *Gemarkte Anmeldung biometrisch schützen* ein oder aus.

✅ **Ergebnis:** Beim nächsten Start fragt Android – oder eben nicht – vor dem Fortsetzen nach „Ordavis IT entsperren“.

Hinweis: Brechen Sie die Abfrage ab, gilt die gemerkte Anmeldung als gesperrt: Die Startseite meldet „Gemarkte Anmeldung ist gesperrt — App erneut öffnen und bestätigen oder neu anmelden.“ Die App fragt nur einmal je Programmstart. Schließen Sie sie ganz (aus der Liste der zuletzt genutzten Apps wischen) und öffnen Sie sie neu, oder melden Sie sich neu an.

5.5 Abmelden

⚙️ In der App: *Zahnrad* ▶ *Profil* ▶ *Abmelden* · 🔑 kein Recht nötig



Klickweg – Abmelden

1. Tippen Sie in der Kopfzeile auf das *Zahnrad*.
2. Tippen Sie im Abschnitt *Profil* auf *Abmelden*.
3. Bestätigen Sie die Rückfrage mit *Abmelden*.

✓ **Ergebnis:** Die Anmeldung ist vom Telefon entfernt, das Telefon bekommt keine Benachrichtigungen mehr, und der Server hat die Sitzung beendet. Noch nicht gesendete Handlungen bleiben erhalten (Abschnitt 11).

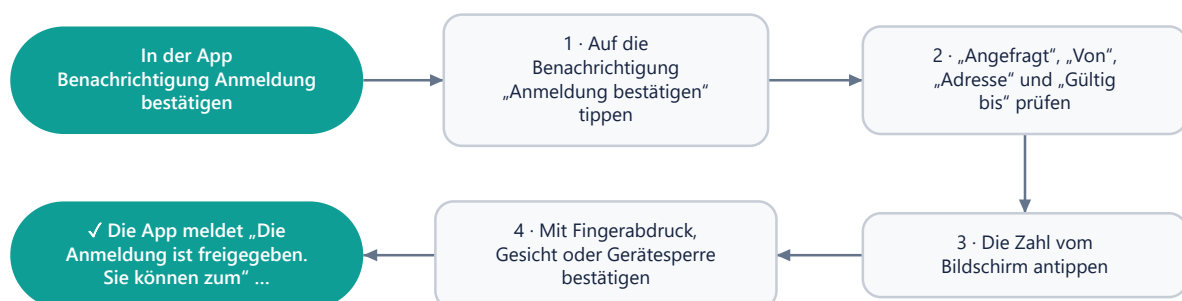
Hinweis: Jede Handlung in der Warteschlange gehört dem Konto, unter dem sie erfasst wurde. Meldet sich nach Ihnen jemand anderes auf demselben Telefon an, sendet die App Ihre liegengeliebenen Handlungen **nicht** unter dessen Namen; sie warten, bis Sie sich wieder anmelden. Auch der Server nimmt eine Handlung nur unter dem Konto an, das sie erfasst hat. Geben Sie ein Telefon weiter, senden Sie vorher alles (Abschnitt 11.2) – oder löschen Sie die lokalen Daten (Abschnitt 14.3), dann sind die Handlungen verloren.

5.6 Anmeldung am Arbeitsplatz per App freigeben

Hat Ihre Verwaltung die **Anmeldung per App** eingeschaltet, bestätigen Sie eine Anmeldung am Windows-Client mit dem Telefon statt mit einem Einmalcode. Der Client zeigt dabei eine Zahl; das Telefon bekommt die Benachrichtigung „Anmeldung bestätigen“.

⚙️ **In der App:** Benachrichtigung *Anmeldung bestätigen* · 🔑 kein Recht nötig – das Telefon muss mit Ihrem Konto angemeldet sein

Voraussetzung: Push-Benachrichtigungen kommen an (Abschnitt 12), und das Telefon zeigt in *Meine Geräte* das Kennzeichen *kann Anmeldung freigeben*.



Klickweg – Anmeldung am Arbeitsplatz per App freigeben

1. Tippen Sie auf die Benachrichtigung *Anmeldung bestätigen*.
2. Prüfen Sie *Angefragt*, *Von*, *Adresse* und *Gültig bis*.

3. Tippen Sie unter den drei Zahlen auf die, die auf dem anfragenden Bildschirm steht.
4. Bestätigen Sie mit Fingerabdruck, Gesicht oder Gerätesperre.

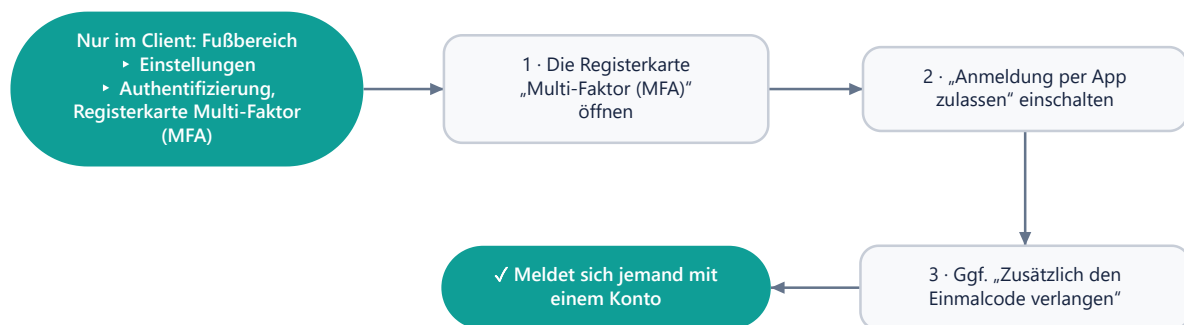
✓ **Ergebnis:** Die App meldet „Die Anmeldung ist freigegeben. Sie können zum Rechner zurückkehren.“; der Windows-Client meldet sich an.

Waren Sie es **nicht**, tippen Sie auf *Ich war das nicht — ablehnen*. Das geht ohne Biometrie; die App rät danach, das Kennwort zu ändern. Eine Anfrage gilt **fünf Minuten**.

Hinweis: Die Anmeldung per App gilt nur für den **Windows-Client**. Portal und App selbst melden sich weiter mit Kennwort und – falls eingerichtet – Einmalcode an. Die App ist auch keine Authenticator-App: Den 6-stelligen Code erzeugt eine andere App.

Eingeschaltet wird die Anmeldung per App im Windows-Client:

🖥️ **Nur im Client:** Fußbereich ▶ Einstellungen ▶ Authentifizierung, Registerkarte Multi-Faktor (MFA) · 🔑
`system.security.manage` — Das Portal bietet diese Einstellung nicht an.



Klickweg – Anmeldung am Arbeitsplatz per App freigeben

1. Öffnen Sie die Registerkarte *Multi-Faktor (MFA)*.
2. Schalten Sie *Anmeldung per App zulassen* ein.
3. Schalten Sie *Zusätzlich den Einmalcode verlangen* ein, wenn trotz Freigabe auch der Einmalcode gelten soll.

✓ **Ergebnis:** Meldet sich jemand mit einem Konto, das ein freigabefähiges Telefon hat, am Windows-Client an, zeigt der Client eine Zahl und wartet auf die Bestätigung am Telefon. Ist kein Telefon erreichbar, gilt das Gewohnte: der Einmalcode, sofern einer eingerichtet ist. Einzelheiten zur Mehrfaktor-Anmeldung stehen in ID-41.

6 Reiter Start

Die Startseite ist die erste Seite nach dem Öffnen. Was dort steht, hängt vom Anmeldestand ab.

Nicht angemeldet. Eine Karte „Willkommen bei Ordavis IT“ mit der Schaltfläche *Anmelden*. Ist noch keine Serveradresse eingerichtet, steht darüber „Bitte zuerst die Adresse des Ordavis-Servers hinterlegen.“ – die Adresse tragen Sie über das Zahnrad ein (Abschnitt 4.1).

Angemeldet, von oben nach unten:

Bereich	Inhalt
Begrüßung	Gruß nach Tageszeit, Ihr Name, <i>Mandant</i>

Bereich	Inhalt
Statusband	Verbindungsstand; „Ein Vorgang von dir hat die vereinbarte Frist überschritten.“, wenn eine Frist gerissen ist
Zähler	„offen bei mir“ und „offen im Team“ – Antippen öffnet den Reiter <i>Tickets</i>
<i>Schnellzugriff</i>	Kacheln nach Ihren Rechten (Abschnitt 2.3)
<i>Noch nicht beim Server</i>	nur wenn etwas in der Warteschlange liegt: <i>Jetzt abgleichen</i> , bei abgelehnten Handlungen <i>Abgelehnte erneut senden</i> und <i>Abgelehnte verwerfen</i> (Abschnitt 11)
<i>Serverstand hat sich geändert</i>	nur bei Konflikten: <i>Eigenen Stand durchsetzen</i> und <i>Serverstand behalten</i> (Abschnitt 11.3)

Die Kacheln im Überblick:

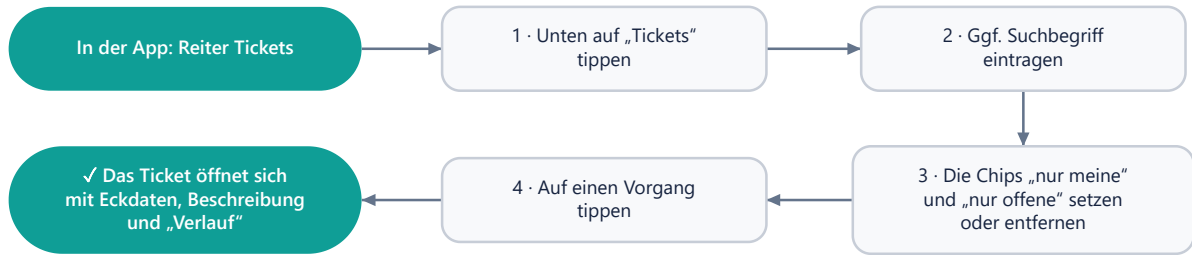
Kachel	Führt zu	Abschnitt
<i>Inventur</i>	Inventurläufe anlegen und Geräte erfassen	9.3
<i>Netze</i>	Bereiche, Belegung, Adresse nachschlagen	10.1
<i>Wissen</i>	Wissensdatenbank	10.2
<i>Kennzahlen</i>	Kennzahlen des Service-Desks	10.2
<i>Handbücher</i>	Betriebs- und Notfallhandbücher, auch ohne Netz	10.3
<i>Checklisten</i>	zugewiesene Checklisten abarbeiten	10.4
<i>Sicherungsprüfungen</i>	eigene offene Prüfungen der Datensicherung	10.5
<i>Meine Alarme</i>	eigene offene Alarme beantworten	12.4
<i>Katalog</i>	Leistung aus dem Service-Katalog bestellen	7.6

Achtung: Die Kachel *Meine Alarme* ist dafür gedacht, immer dazustehen. Tatsächlich erscheint sie nur, wenn wenigstens **eine weitere** Kachel sichtbar ist. Ein Konto, das sonst keine Kachel sieht, findet *Meine Alarme* nicht auf der Startseite. Eine Alarm-Benachrichtigung öffnet die Seite trotzdem (Abschnitt 12.4); antworten können Sie außerdem im Windows-Client und im Portal.

7 Reiter Tickets

7.1 Vorgänge finden

 In der App: Reiter *Tickets* ·  `tickets.self.read` (eigene) oder `tickets.read` (Gruppe)



Klickweg – Vorgänge finden

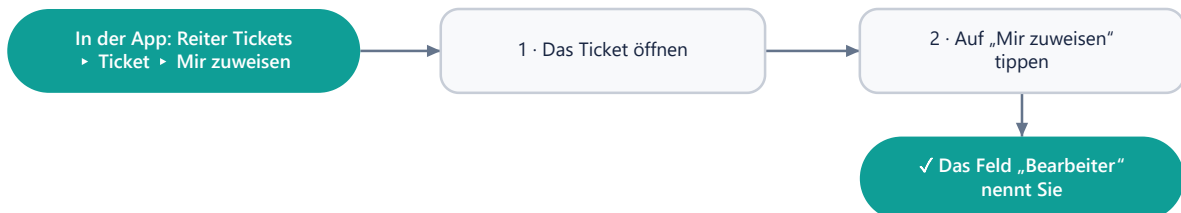
1. Tippen Sie unten auf *Tickets*.
2. Tragen Sie im Suchfeld *Betreff* oder *Ticketnummer* einen Begriff ein und tippen Sie auf die Suchtaste der Tastatur, wenn Sie einen bestimmten Vorgang suchen.
3. Setzen oder entfernen Sie die Chips *nur meine* und *nur offene*.
4. Tippen Sie auf einen Vorgang.

✓ **Ergebnis:** Das Ticket öffnet sich mit Eckdaten, Beschreibung und *Verlauf* – der neueste Eintrag steht oben.

Die Liste zeigt höchstens **50** Treffer; gibt es mehr, steht dort zum Beispiel „50 von 230 — Suche eingrenzen.“. Der Chip *nur meine* erscheint nur, wenn Sie beide Rechte haben; wer nur `tickets.self.read` hat, sieht ohnehin nur die eigenen Vorgänge, wer nur `tickets.read` hat, die der Gruppe.

7.2 Ticket übernehmen

⚙ In der App: Reiter *Tickets* ▶ Ticket ▶ *Mir zuweisen* · 🔑 `tickets.assign`



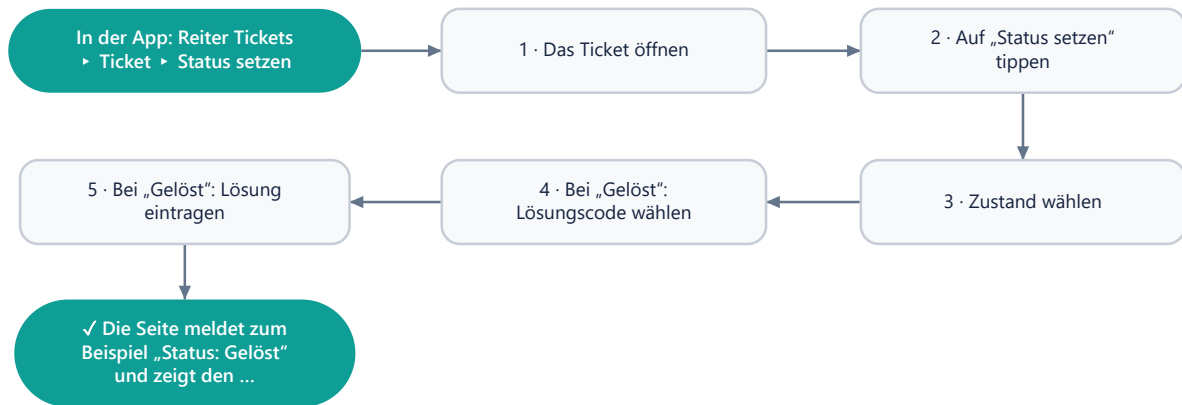
Klickweg – Ticket übernehmen

1. Öffnen Sie das Ticket.
2. Tippen Sie auf *Mir zuweisen*.

✓ **Ergebnis:** Das Feld *Bearbeiter* nennt Sie. Liegt das Ticket schon bei Ihnen, ist *Mir zuweisen* ausgegraut. Ohne Netz merkt die App die Übernahme vor („Übernahme gemerkt“) und sendet sie später.

7.3 Status setzen und lösen

⚙ In der App: Reiter *Tickets* ▶ Ticket ▶ *Status setzen* · 🔑 `tickets.update`



Klickweg – Status setzen und lösen

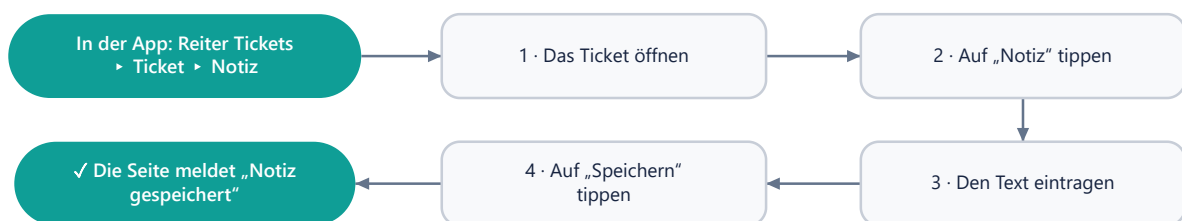
1. Öffnen Sie das Ticket.
2. Tippen Sie auf *Status setzen*.
3. Wählen Sie *In Arbeit*, *Wartet auf Melder*, *Wartet auf Dienstleister*, *Blockiert* oder *Gelöst*.
4. Wählen Sie bei *Gelöst* unter *Lösungscode* den passenden Code.
5. Tragen Sie bei *Gelöst* unter *Was wurde gemacht?* die Lösung ein und tippen Sie auf *Speichern*.

✓ **Ergebnis:** Die Seite meldet zum Beispiel „Status: Gelöst.“ und zeigt den neuen Stand. Ohne Netz steht dort „Kein Netz — Status „Gelöst“ gemerkt. Geht raus, sobald wieder Verbindung besteht.“

Geschlossen lässt sich in der App nicht setzen; das geschieht nach den Regeln des Service-Desks (ID-20). Bei einem Vorgang, dessen meldende Person nach Art. 18 DSGVO eingeschränkt ist, zeigt die App den Hinweis „... Der Vorgang lässt sich lesen, aber nicht ändern.“ und blendet die Schaltflächen aus.

7.4 Interne Notiz schreiben

🔑 In der App: Reiter *Tickets* ▸ Ticket ▸ *Notiz* · 🔑 tickets.update



Klickweg – Interne Notiz schreiben

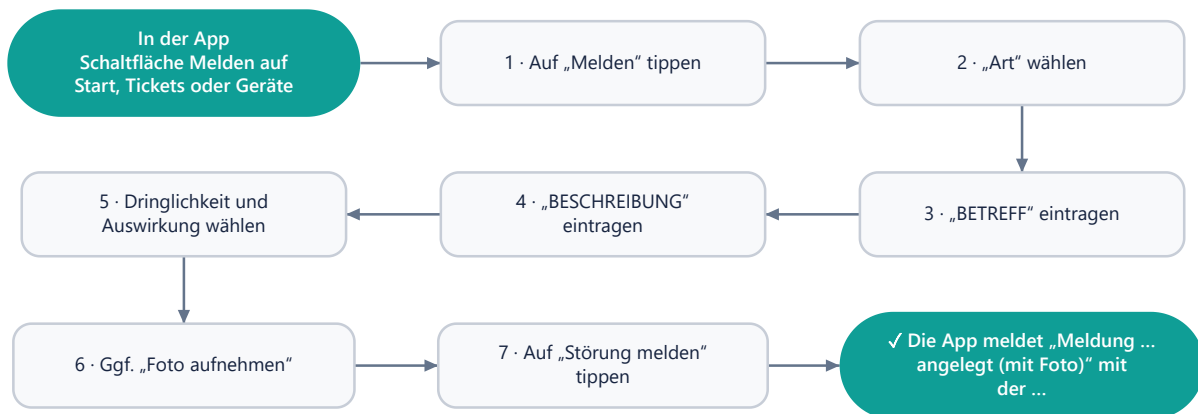
1. Öffnen Sie das Ticket.
2. Tippen Sie auf *Notiz*.
3. Tragen Sie den Text ein, zum Beispiel `Rückruf 14 Uhr vereinbart`.
4. Tippen Sie auf *Speichern*.

✓ **Ergebnis:** Die Seite meldet „Notiz gespeichert.“; im *Verlauf* steht der Eintrag als *Interne Notiz*.

Hinweis: Die Notiz ist **immer intern** – die meldende Person sieht sie nicht. Eine Antwort an den Melder schreiben Sie im Windows-Client oder im Portal (ID-11).

7.5 Vorgang melden

 In der App: Schaltfläche *Melden* auf *Start*, *Tickets* oder *Geräte* ·  `tickets.create`



Klickweg – Vorgang melden

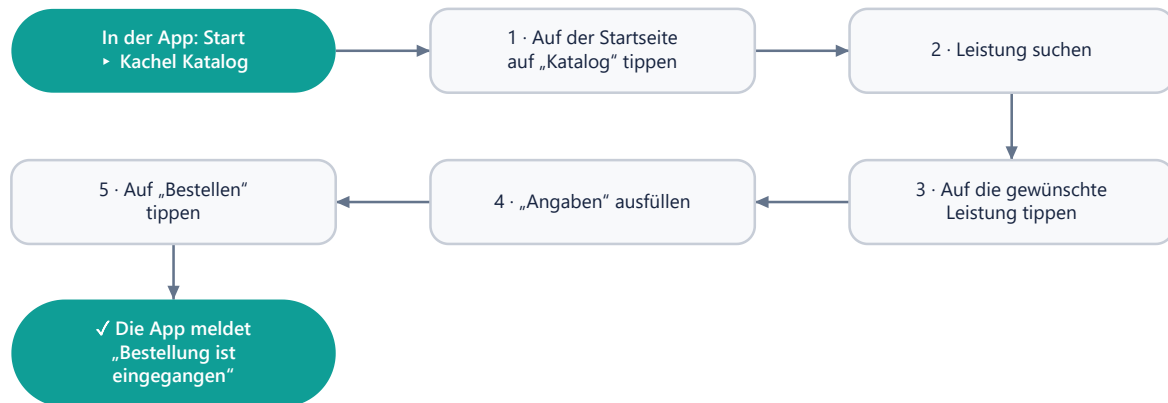
1. Tippen Sie auf *Melden*.
2. Wählen Sie unter *Art* *Störung*, *Anfrage*, *Problem* oder *Änderung*.
3. Tragen Sie unter *BETREFF* kurz ein, was passiert ist.
4. Tragen Sie unter *BESCHREIBUNG* Einzelheiten ein, zum Beispiel die Fehlermeldung.
5. Wählen Sie unter *DRINGLICHKEIT* und *AUSWIRKUNG* jeweils *Niedrig*, *Mittel* oder *Hoch*.
6. Tippen Sie auf *Foto aufnehmen*, wenn ein Bild hilft, und nehmen Sie das Foto auf.
7. Tippen Sie auf *Störung melden* (die Schaltfläche trägt die gewählte Art).

✓ **Ergebnis:** Die App meldet „Meldung ... angelegt (mit Foto).“ mit der Ticketnummer. Ohne Netz meldet sie „Kein Netz — Meldung samt Foto gemerkt. Sie geht raus, sobald wieder Verbindung besteht.“

Vorgaben: *Art* ist *Störung*, *DRINGLICHKEIT* und *AUSWIRKUNG* stehen auf *Mittel*. Nur der *Betreff* ist Pflicht. Das Foto wird vor dem Senden verkleinert (längste Kante 2048 Pixel) und **ohne** Metadaten neu berechnet – auch ein Aufnahmeort fällt weg. Gemeldet aus dem Steckbrief eines Geräts, ist das Gerät als *BETROFFENES GERÄT* eingetragen und der *Betreff* mit „Störung: “ vorbelegt (Abschnitt 8.1).

7.6 Leistung aus dem Katalog bestellen

 In der App: *Start* ▶ *Kachel Katalog* ·  `ticketing.service_catalog.read` und `tickets.create`



Klickweg – Leistung aus dem Katalog bestellen

1. Tippen Sie auf der Startseite auf *Katalog*.
2. Tragen Sie im Feld *Leistung suchen* einen Begriff ein, zum Beispiel **Monitor**.
3. Tippen Sie auf die gewünschte Leistung.
4. Tragen Sie die Pflichtangaben unter *Angaben* ein, bei Bedarf auch *Anmerkungen*.
5. Tippen Sie auf *Bestellen*.

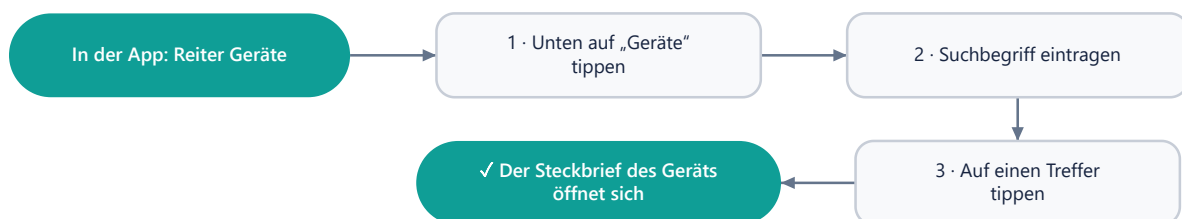
✓ **Ergebnis:** Die App meldet „Bestellung ist eingegangen — Vorgang ...“; *Vorgang öffnen* zeigt den angelegten Service-Vorgang. Steht bei der Leistung *Freigabe nötig*, wird der Vorgang sofort angelegt, aber erst nach der Freigabe bearbeitet.

Der Katalog selbst braucht eine Verbindung. Bricht das Netz erst beim Absenden ab, merkt die App die Bestellung vor („Kein Netz — die Bestellung ist gemerkt und geht raus, sobald wieder Verbindung besteht.“).

8 Reiter Geräte

8.1 Gerät suchen und Steckbrief öffnen

⚙ In der App: Reiter *Geräte* · 🔑 `cmbd.ci.read`



Klickweg – Gerät suchen und Steckbrief öffnen

1. Tippen Sie unten auf *Geräte*.
2. Tragen Sie im Suchfeld *Name, CI-Nummer, Seriennummer* einen Begriff ein und tippen Sie auf die Suchtaste der Tastatur.
3. Tippen Sie auf einen Treffer.

✓ **Ergebnis:** Der Steckbrief des Geräts öffnet sich: Name, Klasse, Lebenszyklus, Stammdaten wie *Seriennummer*, *Hersteller*, *Modell*, *Garantie bis* und *Zuletzt geprüft*, darunter der QR-Code des *ASSET-TAG*.

Ein Teil des Begriffs genügt; die Liste zeigt höchstens 50 Treffer. Im Steckbrief stehen je nach Rechten außerdem *Vorgang melden* (Abschnitt 7.5), *Wareneingang buchen* (Abschnitt 8.3), der Abschnitt *NFC-Tags* (Abschnitt 8.4) und die *Historie* (mit `audit.read`). Der QR-Code des *ASSET-TAG* enthält die CI-Nummer – ein anderes Telefon kann ihn vom Bildschirm scannen.

8.2 Trefferliste als CSV weitergeben

🔧 In der App: Reiter *Geräte* ▶ *Liste teilen (CSV)* · 🔑 `cldb.ci.read`



Klickweg – Trefferliste als CSV weitergeben

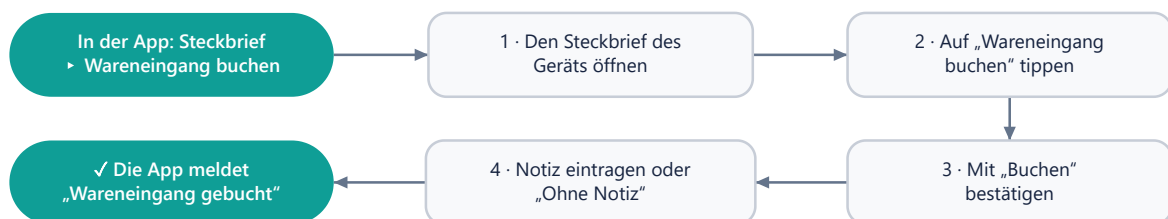
1. Suchen Sie die Geräte, zum Beispiel mit `Latitude`.
2. Tippen Sie auf *Liste teilen (CSV)*.
3. Wählen Sie im Teilen-Menü von Android das Ziel, etwa E-Mail oder Dateien.

✓ **Ergebnis:** Die CSV-Datei (Titel *Geräteliste*) enthält je Treffer eine Zeile mit den Spalten `CI-Nummer;Name;Klasse;Status;Seriennummer` – also nur die angezeigten Treffer, nicht den ganzen Bestand.

8.3 Wareneingang buchen

Kommt ein bestelltes Gerät an, buchen Sie den Wareneingang direkt am Gerät.

🔧 In der App: Steckbrief ▶ *Wareneingang buchen* · 🔑 `cldb.ci.update`



Klickweg – Wareneingang buchen

1. Öffnen Sie den Steckbrief des Geräts, etwa über Scannen oder Suchen.
2. Tippen Sie auf *Wareneingang buchen*.
3. Bestätigen Sie die Frage „...“ als heute eingegangen buchen?“ mit *Buchen*.
4. Tragen Sie unter *Notiz (optional)* zum Beispiel die Lieferschein-Nummer ein und tippen Sie auf *Speichern* – oder tippen Sie auf *Ohne Notiz*.

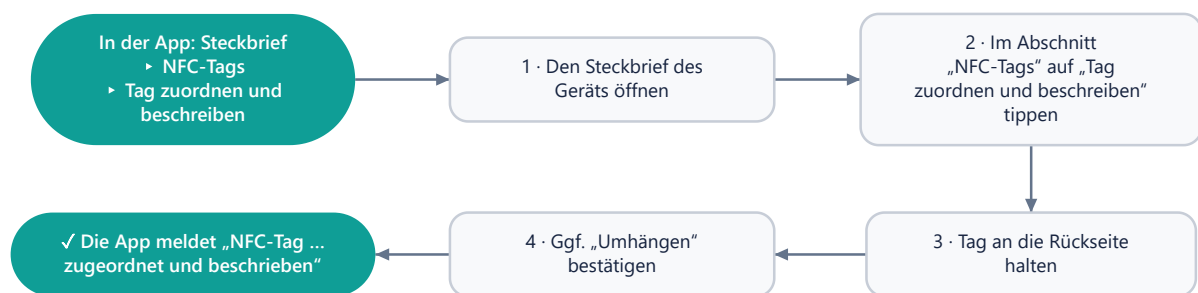
✓ **Ergebnis:** Die App meldet „Wareneingang gebucht.“. Im Lebenszyklus steht der Wareneingang mit dem heutigen Datum; ein Gerät im Zustand *Bestellt* rückt auf *In Vorbereitung*. Ein Gerät, das schon in Betrieb ist, wird **nicht** zurückgestuft.

8.4 NFC-Tag zuordnen

Ein NFC-Tag ist ein kleiner Aufkleber mit Chip. Hält man ihn ans Telefon, findet die App das Gerät – auch dort, wo ein Etikett schlecht zu sehen ist. An einem Gerät dürfen mehrere Tags kleben.

⚙ In der App: *Steckbrief* ▶ *NFC-Tags* ▶ *Tag zuordnen und beschreiben* · 🔑 `cmdb.ci.update`

Voraussetzung: Das Telefon hat NFC, und NFC ist in den Android-Einstellungen eingeschaltet.



Klickweg – NFC-Tag zuordnen

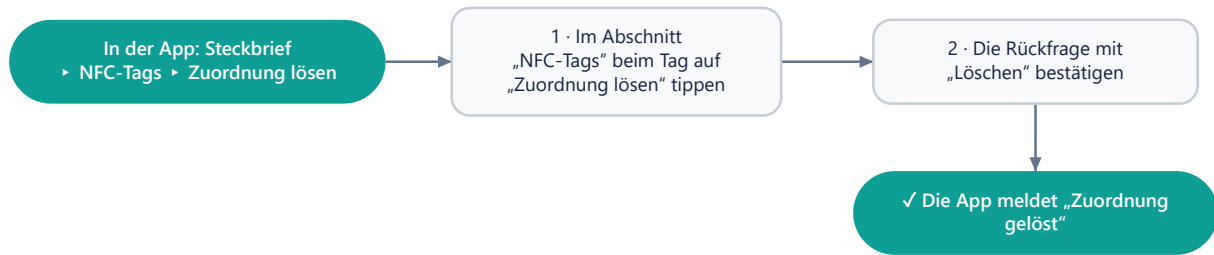
1. Öffnen Sie den Steckbrief des Geräts.
2. Tippen Sie im Abschnitt *NFC-Tags* auf *Tag zuordnen und beschreiben*.
3. Halten Sie den Tag innerhalb von 20 Sekunden an die Rückseite des Telefons, wenn die App „Jetzt den NFC-Tag an die Rückseite des Telefons halten.“ meldet.
4. Bestätigen Sie mit *Umhängen*, falls die App meldet, dass der Tag schon an einem anderen Gerät hängt – aber nur, wenn das gewollt ist.

✓ **Ergebnis:** Die App meldet „NFC-Tag ... zugeordnet und beschrieben.“; der Tag steht in der Liste mit dem Kennzeichen *signiert*. Beschrieben heißt: Auf dem Tag steht ein Verweis mit Prüfwert, den auch ein anderes Telefon prüfen kann.

Achtung: Lässt sich der Tag nicht beschreiben (schreibgeschützt oder zu klein), meldet die App „Der Tag wurde zugeordnet, ließ sich aber nicht beschreiben: ...“. Diese Meldung stimmt **nicht**: Die Zuordnung ist dann **nicht** angelegt. Prüfen Sie die Liste *NFC-Tags* und versuchen Sie es mit einem anderen Tag.

8.5 NFC-Zuordnung lösen

⚙ In der App: *Steckbrief* ▶ *NFC-Tags* ▶ *Zuordnung lösen* · 🔑 `cmdb.ci.update`



Klickweg – NFC-Zuordnung lösen

1. Tippen Sie im Abschnitt *NFC-Tags* beim Tag auf *Zuordnung lösen*.
2. Bestätigen Sie die Rückfrage mit *Löschen*.

✓ **Ergebnis:** Die App meldet „Zuordnung gelöst.“. Der Aufkleber bleibt am Gerät kleben; beim nächsten Scan ist er ein „Unbekannter NFC-Tag“.

Hinweis: *Zuordnung lösen* steht auch bei Konten ohne `cmdb.ci.update` da. Der Server weist es dann ab, und die App zeigt die Ablehnung.

9 Reiter Scannen

Der Reiter *Scannen* liest Etiketten mit der Kamera und NFC-Tags gleichzeitig. Jeder Treffer landet in einer Liste – so lassen sich viele Geräte nacheinander erfassen, etwa beim Gang durch ein Lager. Abbildung 2 zeigt, was die App mit einem gelesenen Code macht.

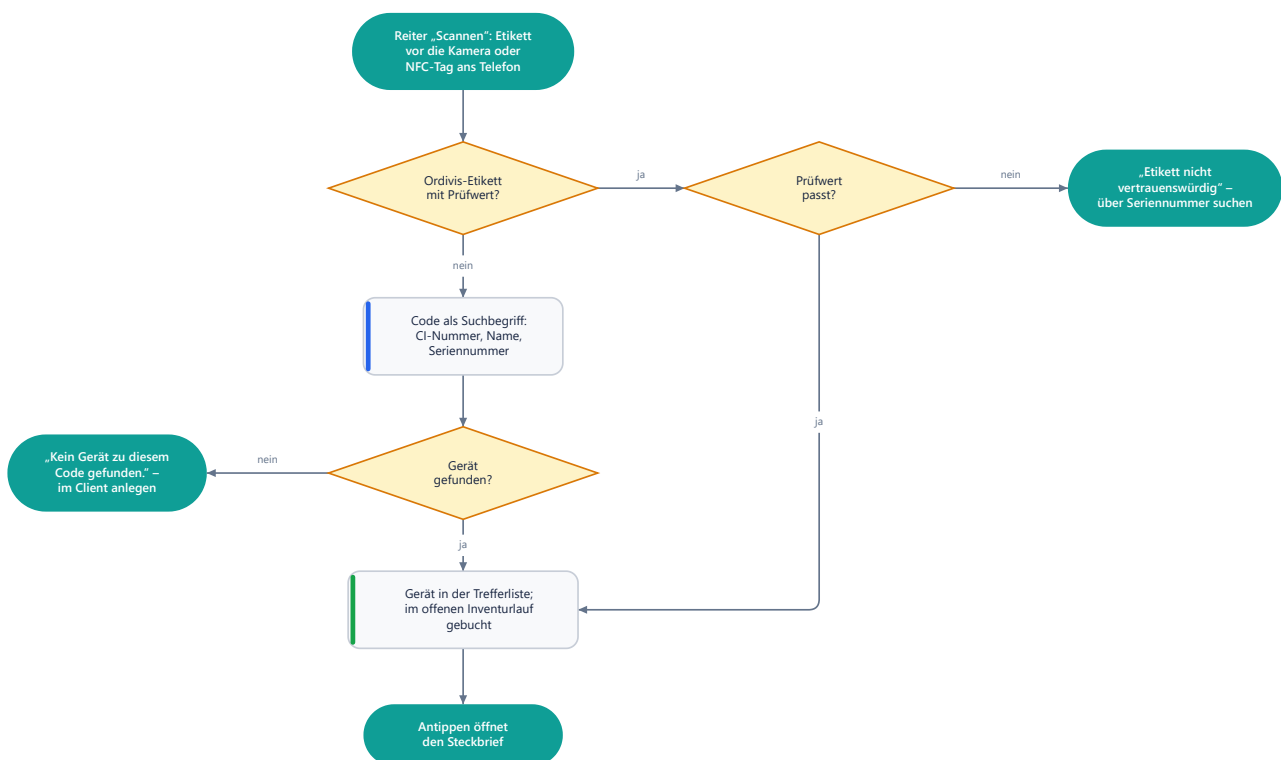
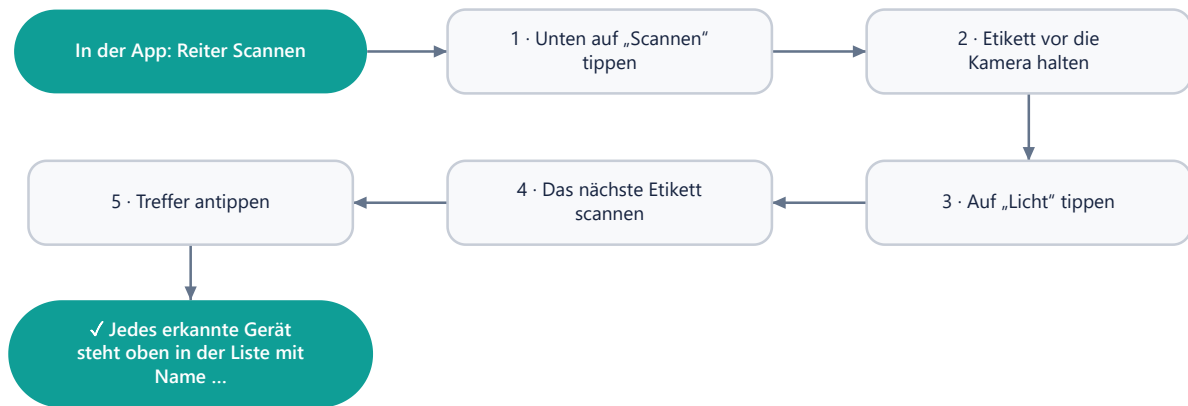


Abb. 2 – Vom gescannten Code zum Gerät.

9.1 Etiketten scannen

 In der App: Reiter *Scannen* ·  `cldb.ci.read`

Voraussetzung: Die App darf die Kamera nutzen. Android fragt beim ersten Öffnen danach.



Klickweg – Etiketten scannen

1. Tippen Sie unten auf *Scannen*.
2. Halten Sie ein Etikett vor die Kamera oder einen NFC-Tag an die Rückseite des Telefons.
3. Tippen Sie auf *Licht*, wenn es zu dunkel ist.
4. Scannen Sie das nächste Etikett, bis alle erfasst sind.
5. Tippen Sie auf einen Treffer, um den Steckbrief zu öffnen.

✓ **Ergebnis:** Jedes erkannte Gerät steht oben in der Liste mit Name, CI-Nummer, Klasse und Seriennummer; die Statuszeile meldet zum Beispiel „Drucker 3. OG erfasst“. *Liste leeren* beginnt von vorn.

Die Kamera erkennt **QR-Code**, **DataMatrix**, **Code 128**, **Code 39**, **EAN-13** und **EAN-8**. Ein zweiter Scan desselben Geräts ergibt „Bereits erfasst: ...“ statt einer doppelten Zeile.

Hinweis: Die normale Kamera-App des Telefons öffnet Ordvis-Etiketten **nicht** in der App. Scannen Sie immer über den Reiter *Scannen*.

9.2 Was die App mit einem Code macht

Gelesen	Was geschieht	Meldung
Ordvis-Etikett mit Prüfwert	Der Server prüft den Prüfwert; passt er, erscheint das Gerät.	„... erfasst.“
Ordvis-Etikett mit falschem Prüfwert	Das Gerät wird nicht geöffnet. Die Warnung bleibt auch beim erneuten Scan stehen.	„Etikett nicht vertrauenswürdig“
fremder Barcode, Seriennummer, Inventarnummer	Der Code wird als Suchbegriff verwendet (CI-Nummer, Name, Seriennummer).	ein Treffer: „... erfasst.“; mehrere: „3 Treffer zu „...“ — bitte auswählen.“
Code ohne passendes Gerät	Der Code bleibt als Zeile in der Liste.	„Kein Gerät zu diesem Code gefunden.“

Gelesen	Was geschieht	Meldung
beschriebener NFC-Tag	wie ein Ordavis-Etikett	„... erfasst.“
NFC-Tag, der keinem Gerät gehört	Die Kennung bleibt in der Liste.	„Unbekannter NFC-Tag“

Hinweis: Ist die Prüfung des Prüfwerts gerade nicht erreichbar, läuft der Scan **ohne** Warnung weiter. Ein gefälschtes Etikett fällt dann nicht auf.

Ein **unbekanntes Gerät** legt die App nicht an. Angelegt wird es im Windows-Client oder Portal (ID-21); einen unbekannten NFC-Tag ordnet man danach im Steckbrief zu (Abschnitt 8.4).

9.3 Inventur

Eine Inventur zählt, was tatsächlich vor Ort ist. In der App legen Sie einen **Inventurlauf** an und scannen; jeder Scan wird auf den Lauf gebucht. Den Abgleich gegen den Sollbestand – was fehlt, was ist unerwartet da – und den Abschluss erledigen Sie am Arbeitsplatz.

 **In der App:** Start ▶ Kachel *Inventur* (oder *Zahnrad* ▶ *Werkzeuge* ▶ *Inventur*) ·  `cmbd.ci.update`

Voraussetzung: Netz. Inventurbuchungen merkt die App **nicht** vor.



Klickweg – Inventur

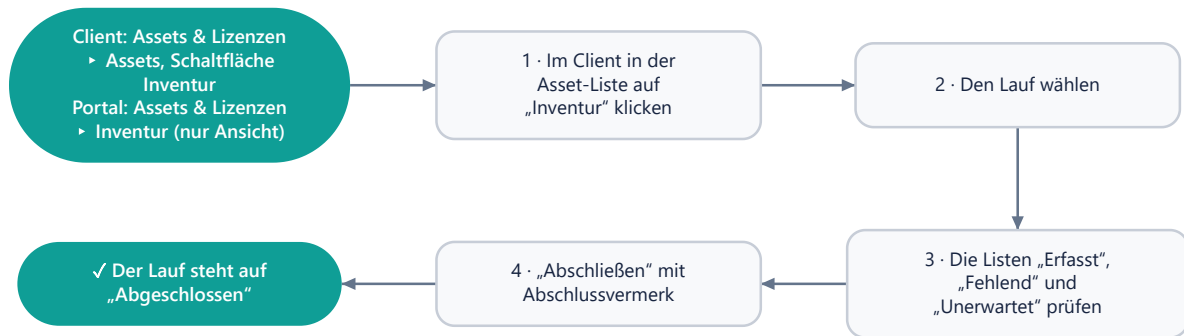
1. Tippen Sie auf der Startseite auf *Inventur*.
2. Tippen Sie auf *Neuer Lauf* – oder tippen Sie auf einen offenen Lauf, um dort weiterzumachen.
3. Scannen Sie die Geräte nacheinander, wenn die App „Inventur: Geräte nacheinander scannen.“ meldet.

✓ **Ergebnis:** Ein neuer Lauf heißt „Inventur 02.10.2026 09:15“ (Datum und Uhrzeit des Anlegens) und steht unter *INVENTURLAUF* über dem Sucher. Jeder Scan meldet „... erfasst · in der Inventur gebucht.“, ein zweiter Scan „... · in der Inventur bereits erfasst.“. Auch ein Code ohne Gerät wird gebucht – er erscheint später als *Unerwartet*.

Die Liste der Läufe zeigt *Offen* („seit ... · 12 erfasst“) und *Abgeschlossen*. Ein abgeschlossener Lauf nimmt nichts mehr an: „Dieser Lauf ist abgeschlossen — Erfassungen sind nicht mehr möglich.“

Abgleich und Abschluss am Arbeitsplatz:

 **Client:** Assets & Lizenzen ▶ Assets, Schaltfläche *Inventur* ·  **Portal:** Assets & Lizenzen ▶ *Inventur* (nur Ansicht) ·  `cmbd.ci.read`, zum Abschließen `cmbd.ci.update`



Klickweg – Inventur

1. Klicken Sie im Client in der Asset-Liste auf *Inventur*.
2. Wählen Sie den Lauf.
3. Prüfen Sie die Listen *Erfasst*, *Fehlend* und *Unerwartet*.
4. Klicken Sie auf *Abschließen*, tragen Sie einen *Abschlussvermerk* ein und bestätigen Sie mit *Abschließen*.

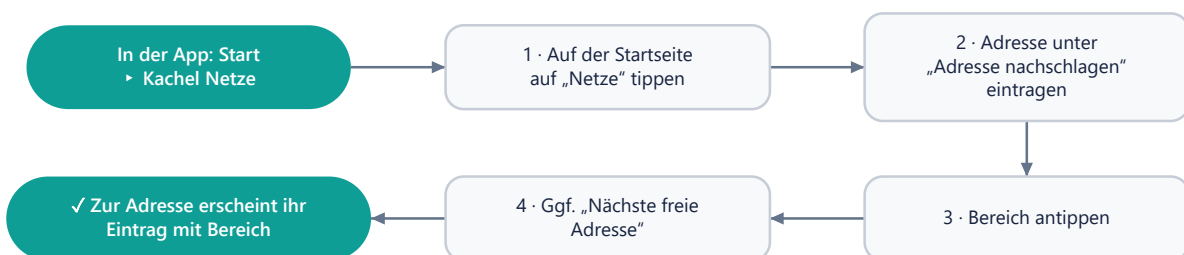
✓ **Ergebnis:** Der Lauf steht auf *Abgeschlossen*. Das Portal zeigt Läufe und *Abweichungen*, schließt aber nicht ab.

10 Weitere Kacheln der Startseite

10.1 Netze

⚙️ **In der App:** Start ► Kachel Netze · 🔑 `ipam.prefix.read` , zum Nachschlagen einzelner Adressen
`ipam.ip.read`

Voraussetzung: Das Modul Netzverwaltung ist für Ihren Mandanten eingeschaltet. Sonst meldet die App „Netzverwaltung ist nicht eingeschaltet“ – das ist keine Störung.



Klickweg – Netze

1. Tippen Sie auf der Startseite auf *Netze*.
2. Tragen Sie unter *Adresse nachschlagen* die vollständige IP-Adresse ein, zum Beispiel `10.0.1.5` .
3. Tippen Sie auf einen Bereich, um *Auslastung*, *DHCP*, *Reservierungen* und *Adressen in diesem Bereich* zu sehen.
4. Tippen Sie im Bereich auf *Nächste freie Adresse*, wenn Sie eine freie Adresse brauchen.

✓ **Ergebnis:** Zur Adresse erscheint ihr Eintrag mit Bereich („in ...“); zu einem Bereich die Belegung. *Nächste freie Adresse* nennt eine Adresse.

Achtung: *Nächste freie Adresse* ist ein **Vorschlag**, keine **Reservierung**. Bis die Adresse zugewiesen ist, kann sie jemand anders nehmen. Zuweisen und reservieren Sie im Windows-Client oder Portal (ID-22).

Die Suche nach Adressen braucht die **vollständige** Adresse („Bitte die vollständige Adresse eingeben — vier Teile bei IPv4.“). Passen mehrere, zeigt die App bewusst nicht einfach die erste.

10.2 Wissen und Kennzahlen

Wissen (Recht `knowledge.read.internal`) durchsucht die Wissensdatenbank nach Stichwort, Fehlermeldung oder Titel und zeigt höchstens 200 Treffer. Jeder **geöffnete** Artikel wird auf dem Telefon gemerkt und ist danach auch ohne Netz lesbar – mit dem Hinweis „Ohne Netz — gemerkter Stand vom ...“. Artikel schreiben oder freigeben können Sie in der App nicht (ID-25).

Kennzahlen (Recht `reporting.read`) zeigt die Lage des Service-Desks für *7 Tage*, *30 Tage* (Vorgabe) oder *90 Tage*: offener Bestand nach Alter, Durchsatz im Zeitraum, Einhaltung der Reaktions- und Lösungsfrist, durchschnittliche Lösungsdauer und Zufriedenheit (ID-27).

10.3 Handbücher und Checklisten für den Notfall mitnehmen

Im Notfall ist oft kein Netz da – gerade dann braucht man das Notfallhandbuch. Die App lädt freigegebene Handbücher und zugewiesene Checklisten auf Wunsch auf das Telefon.

⚙ **In der App:** Start ▶ Kachel Handbücher bzw. Checklisten ▶ Für den Notfall mitnehmen · 🔑 `handbook.read` bzw. `checklist.read`



Klickweg – Handbücher und Checklisten für den Notfall mitnehmen

1. Tippen Sie auf der Startseite auf *Handbücher*.
2. Tippen Sie auf *Für den Notfall mitnehmen*.
3. Tippen Sie auf der Startseite auf *Checklisten* und dort ebenfalls auf *Für den Notfall mitnehmen*.

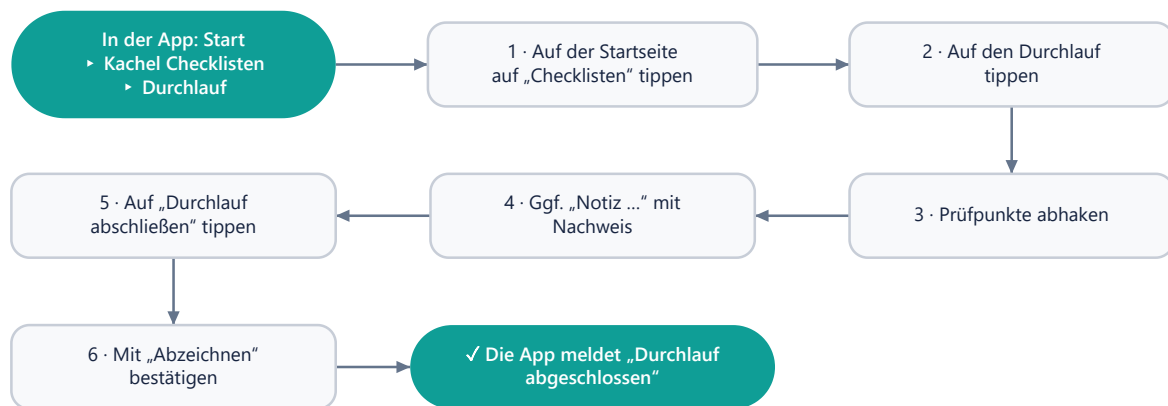
✅ **Ergebnis:** Die App meldet zum Beispiel „4 Handbücher liegen jetzt auf dem Gerät.“; jedes Handbuch trägt „auf dem Gerät seit ...“. Ohne Netz zeigt die App diesen Stand mit dem Hinweis „Kein Netz — Stand vom ... Alarmierungsketten und Rufnummern können sich seither geändert haben.“

Die App zeigt nur **freigegebene** Handbücher, keine Entwürfe. Wird ein Handbuch zurückgezogen, entfernt die App es beim nächsten Abruf auch vom Telefon. Holen Sie den Stand regelmäßig neu – etwa vor jeder Bereitschaftswoche.

10.4 Checkliste abarbeiten

⚙️ In der App: Start ▶ Kachel Checklisten ▶ Durchlauf · 🔑 `checkList.read` , zum Abhaken
`checklist.run.execute.self`

Voraussetzung: Ihnen ist ein Durchlauf zugewiesen, und er *läuft*.



Klickweg – Checkliste abarbeiten

1. Tippen Sie auf der Startseite auf *Checklisten*.
2. Tippen Sie auf den Durchlauf.
3. Tippen Sie auf einen Prüfpunkt, um ihn abzuholen; ein zweites Tippen öffnet ihn wieder.
4. Tippen Sie bei Bedarf auf *Notiz ...* und tragen Sie Notiz und Nachweis ein, zum Beispiel eine Ticketnummer.
5. Tippen Sie auf *Durchlauf abschließen*.
6. Bestätigen Sie mit *Abzeichnen*.

✅ **Ergebnis:** Die App meldet „Durchlauf abgeschlossen.“; der Durchlauf ist mit Ihrem Namen abgezeichnet und lässt sich nicht mehr ändern. Sind noch Pflicht-Prüfpunkte offen, nennt die App sie („Ein Pflicht-Prüfpunkt ist noch offen.“) und schließt nicht ab.

Ohne Netz merkt die App Haken, Notizen und den Abschluss vor und sendet sie später. Einzelheiten zu Checklisten stehen in ID-29a.

10.5 Sicherungsprüfung abschließen

⚙️ In der App: Start ▶ Kachel Sicherungsprüfungen · 🔑 `backup.read` , zum Abschließen `backup.verify`

Voraussetzung: Netz. Eine Prüfung wird gegen den Bestand des Zeitraums beurteilt und lässt sich ohne Verbindung nicht abschließen.



Klickweg – Sicherungsprüfung abschließen

1. Tippen Sie auf der Startseite auf *Sicherungsprüfungen*.
2. Prüfen Sie bei Ihrem Prüfzeitraum die Bilanz, zum Beispiel „28 von 30 grün · 1 beanstandet · 1 offen“.
3. Tippen Sie auf *Abschließen*.

✓ **Ergebnis:** Die App meldet „Der Zeitraum ist abgeschlossen; der Nachweis ist festgeschrieben.“ Einzelheiten zur Datensicherung stehen in ID-35.

11 Ohne Netz arbeiten

Unterwegs bricht das Netz regelmäßig ab – im Keller, im Aufzug, im Funkloch. Die App ist darauf eingerichtet: Viele Handlungen **merkt sie vor** und sendet sie, sobald der Server wieder erreichbar ist. Was gemerkt ist, steht noch nicht im Server; der Bildschirm zeigt deshalb weiterhin den Stand, den der Server zuletzt bestätigt hat.

11.1 Was ohne Netz geht

Geht ohne Netz – wird gemerkt und später gesendet	Bleibt ohne Netz lesbar	Geht nur mit Netz
Vorgang melden (auch mit Foto)	einmal geöffnete Wissensartikel	Anmelden
Ticket übernehmen, Status setzen, interne Notiz	mitgenommene Handbücher	Suchen in Tickets und Geräten
Checkliste: Haken, Notiz, Abschluss	mitgenommene Checklisten	Scannen und Inventur
Bestellung aus dem Katalog (wenn der Katalog schon geladen war)		Alarme ansehen und beantworten
		Sicherungsprüfung abschließen, Katalog öffnen

Achtung: Der Datenschutztext der App nennt einen „Auszug der Geräteliste“ zum Nachschlagen ohne Netz. Die App legt ihn zwar an, **liest ihn aber nirgends**: Ohne Netz finden Sie kein Gerät. Nehmen Sie für Einsätze ohne Netz die nötigen Angaben auf anderem Weg mit.

11.2 Liegeengebliebenes senden

Die App sendet die Warteschlange von selbst, sobald die Startseite geladen wird und der Server antwortet. Von Hand geht es so:

⚙️ **In der App:** Start ▶ *Noch nicht beim Server* ▶ *Jetzt abgleichen* (oder *Zahnrad* ▶ *Abgleich*) · 🔑 dieselben Rechte wie die gemerkten Handlungen



Klickweg – Liegengebliebenes senden

1. Tippen Sie auf der Startseite im Bereich *Noch nicht beim Server* auf *Jetzt abgleichen*.

✓ **Ergebnis:** Die App meldet zum Beispiel „3 gemerkte Handlung(en) gesendet.“, und der Bereich verschwindet. Unter *Zahnrad* ▶ *Abgleich* steht dann „Nichts ausstehend“ und „Zuletzt abgeglichen: ...“.

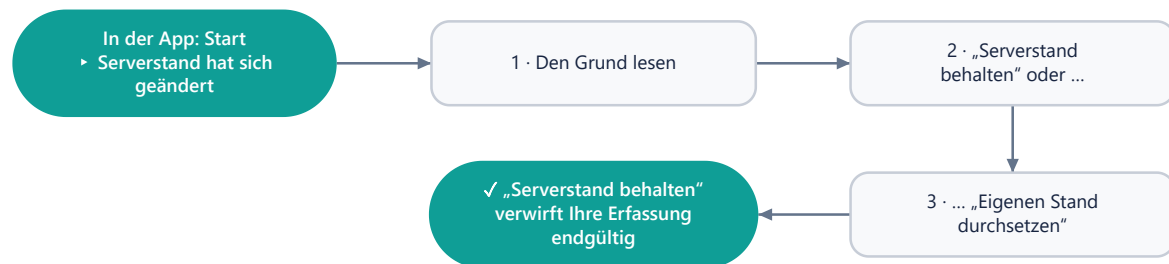
Ein Foto, das sich auch nach fünf Versuchen nicht anhängen ließ, gibt die App auf: „Der Vorgang wurde angelegt, das Foto ließ sich nicht anhängen.“ Reichen Sie es dann im Client oder Portal nach.

11.3 Abgelehnte und kollidierende Handlungen

Abgelehnt heißt: Der Server hat eine gemerkte Handlung nicht angenommen, etwa weil das Recht fehlt. Die Startseite zeigt dann zum Beispiel „1 abgelehnt“ und die Schaltflächen *Abgelehnte erneut senden* und *Abgelehnte verwerfen*.

Kollidiert heißt: Am Server hat sich der Vorgang inzwischen geändert – jemand anderes hat ihn übernommen oder den Status geändert. Die App schreibt dann nicht blind darüber, sondern fragt im Bereich *Serverstand hat sich geändert*.

⚙️ **In der App:** Start ▶ *Serverstand hat sich geändert* · 🔑 dieselben Rechte wie die gemerkte Handlung



Klickweg – Abgelehnte und kollidierende Handlungen

1. Lesen Sie den Grund, zum Beispiel „Das Ticket ist inzwischen jemand anderem zugewiesen.“

2. Tippen Sie auf *Serverstand behalten*, wenn die Änderung am Server gilt, und bestätigen Sie.

3. Tippen Sie stattdessen auf *Eigenen Stand durchsetzen* und bestätigen Sie mit *Durchsetzen*, wenn Ihre Erfassung gelten soll.

✓ **Ergebnis:** *Serverstand behalten* verwirft Ihre Erfassung endgültig („... Handlung(en) verworfen — der Serverstand bleibt.“). *Eigenen Stand durchsetzen* sendet sie erneut und überschreibt die zwischenzeitliche Änderung.

Hinweis: Im Konflikttext kann der Ticketzustand in der internen englischen Schreibweise stehen, etwa „Das Ticket steht inzwischen auf „InProgress“ ...“. *InProgress* ist *In Arbeit*.

12 Benachrichtigungen und Alarme

Die App kann zwei Arten von Nachrichten anzeigen: **Benachrichtigungen** zu Tickets und Fristen und **Alarme** der Alarmierung im Notfallmanagement. Beide kommen als Push-Nachricht über den Zustelldienst von Google (Firebase Cloud Messaging). Betreff und Text sind **Ende-zu-Ende verschlüsselt**: Google und der Vermittler des Herstellers sehen nur „Neue Meldung“ bzw. „Alarm“ und die Kennung des Vorgangs.

Android legt für die App zwei Kanäle an, die Sie in den Android-Einstellungen der App getrennt einstellen können:

Kanal	Wofür	Verhalten
<i>Benachrichtigungen</i>	Tickets, Zuweisungen, Fristen	normale Benachrichtigung
<i>Alarme</i>	Alarme, die sofortiges Handeln verlangen	eigener Alarmton über die Wecker-Lautstärke, Vibration, auf dem Sperrbildschirm sichtbar; Vollbild und Durchbrechen von „Bitte nicht stören“ nur mit Freigabe (Abschnitt 12.3)

Antippen einer Nachricht öffnet das Ziel in der App: das Ticket, das Gerät, den Wissensartikel, *Meine Alarme* oder *Anmeldung bestätigen*. Abbildung 3 hilft, wenn nichts ankommt.

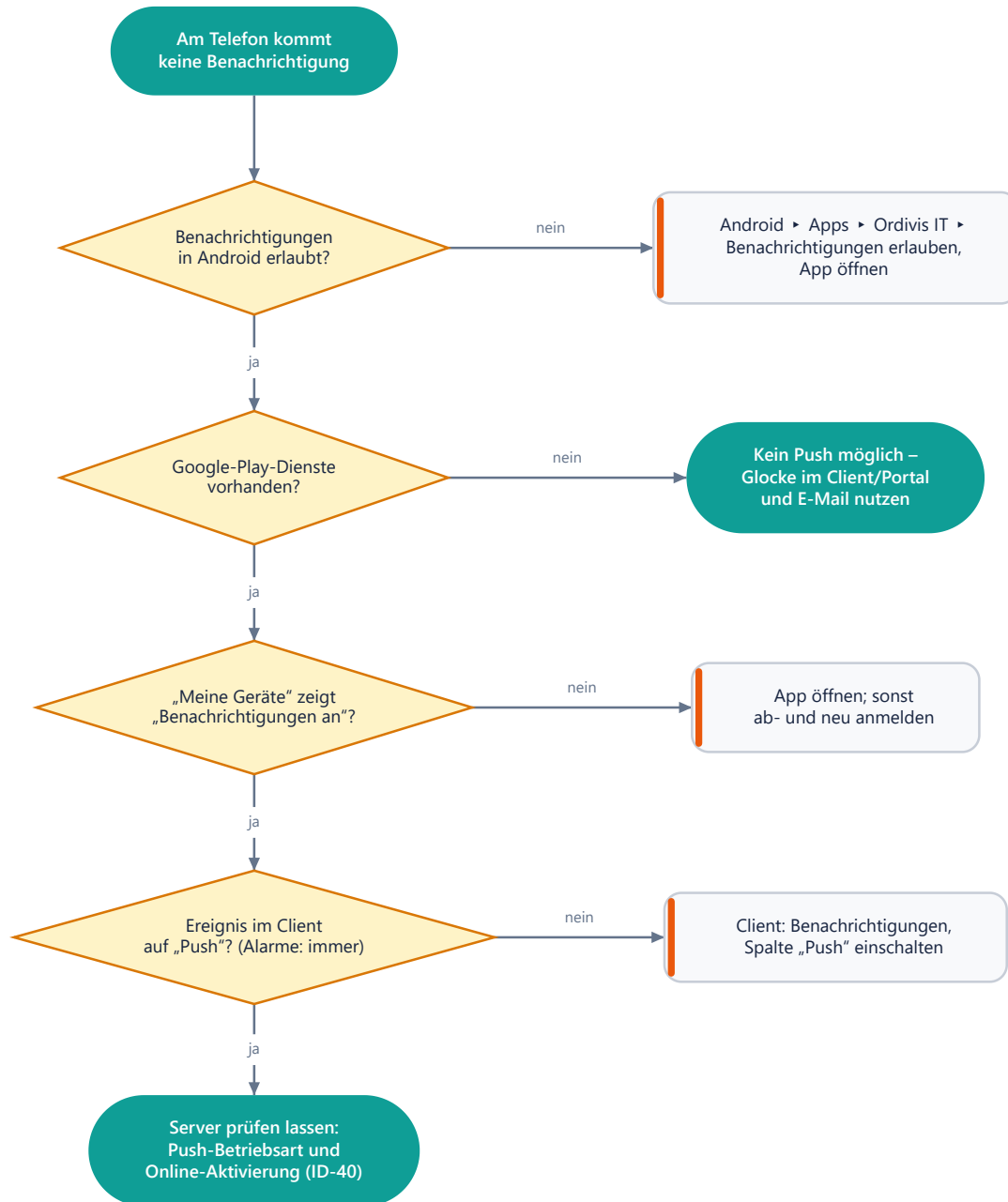


Abb. 3 – Warum kommt keine Benachrichtigung? Prüfreihefolge am Telefon.

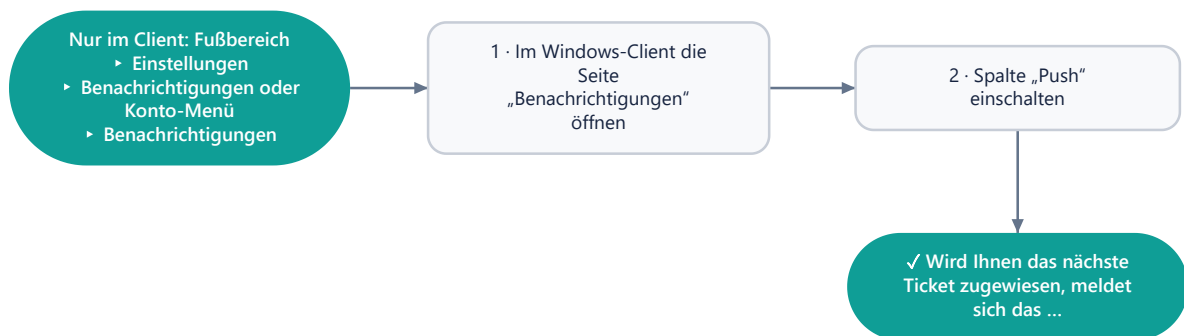
12.1 Was aufs Telefon kommt

- **Gewöhnliche Ereignisse** – etwa „Ticket mir zugewiesen“ oder „SLA verletzt“ – kommen nur, wenn Sie für das Ereignis die Spalte *Push* eingeschaltet haben. Vorgabe ist **aus**. Einschalten lässt sie sich nur im Windows-Client (Abschnitt 12.2); das Portal und die App haben dafür keine Einstellung.
- **Alarmer** kommen ohne diese Einstellung, wenn Sie im Empfängerkreis stehen. Aufgehalten werden sie trotzdem durch Ihre **Ruhezeit** (Abschnitt 12.5), durch ein Telefon ohne Google-Play-Dienste und durch „Bitte nicht stören“ ohne Freigabe (Abschnitt 12.3).

Hinweis: Die App hat **keine** Liste der Benachrichtigungen. Was Sie weggewischt haben, finden Sie in der Glocke des Windows-Clients oder des Portals (ID-31). Fehlen die Google-Play-Dienste, kommt am Telefon gar nichts an; In-App-Meldung und E-Mail erreichen Sie weiterhin.

12.2 Push für ein Ereignis einschalten

 **Nur im Client:** Fußbereich ▶ Einstellungen ▶ Benachrichtigungen oder Konto-Menü ▶ Benachrichtigungen ·
 kein Recht nötig – jede Person stellt ihre eigenen Wege ein — Das Portal hat in seinen Benachrichtigungseinstellungen keine Spalte *Push*.



Klickweg – Push für ein Ereignis einschalten

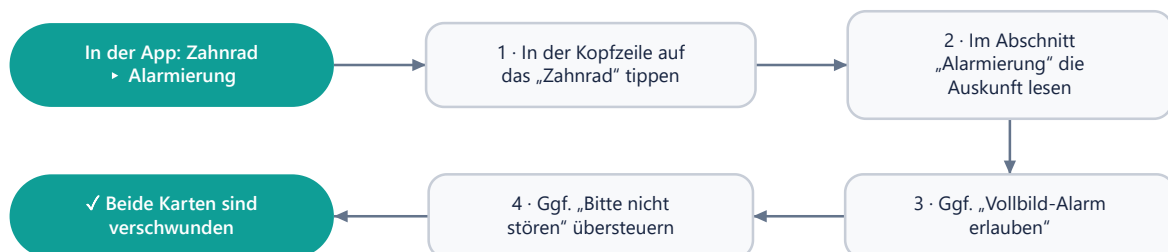
1. Öffnen Sie im Windows-Client die Seite *Benachrichtigungen*.
2. Schalten Sie in der Zeile des Ereignisses, zum Beispiel *Ticket mir zugewiesen*, die Spalte *Push* ein.

✓ **Ergebnis:** Wird Ihnen das nächste Ticket zugewiesen, meldet sich das Telefon. Die Benachrichtigungswege im Ganzen beschreibt ID-31.

12.3 Das Telefon für Alarme vorbereiten

Wer nachts geweckt werden muss – Bereitschaft, Krisenstab –, prüft diese Einstellungen **vorher**. Unter *Zahnrad* ▶ *Alarmierung* sagt die App im Klartext, was ein Alarm auf diesem Telefon gerade bewirkt, zum Beispiel „Ein Alarm uebernimmt den Bildschirm und durchbricht „Bitte nicht stoeren.“ – die Texte schreibt die App derzeit ohne Umlaute.

 **In der App:** *Zahnrad* ▶ *Alarmierung* ·  kein Recht nötig



Klickweg – Das Telefon für Alarme vorbereiten

1. Tippen Sie in der Kopfzeile auf das *Zahnrad*.

2. Lesen Sie im Abschnitt *Alarmierung* die Auskunft.
3. Tippen Sie auf *Vollbild-Alarm erlauben*, falls die Karte erscheint, und erteilen Sie die Freigabe in Android.
4. Tippen Sie auf „*Bitte nicht stören*“ *übersteuern*, falls die Karte erscheint, und erteilen Sie die Freigabe in Android.

✓ **Ergebnis:** Beide Karten sind verschwunden, und die Auskunft lautet „Ein Alarm uebernimmt den Bildschirm und durchbricht „Bitte nicht stoeren“.“

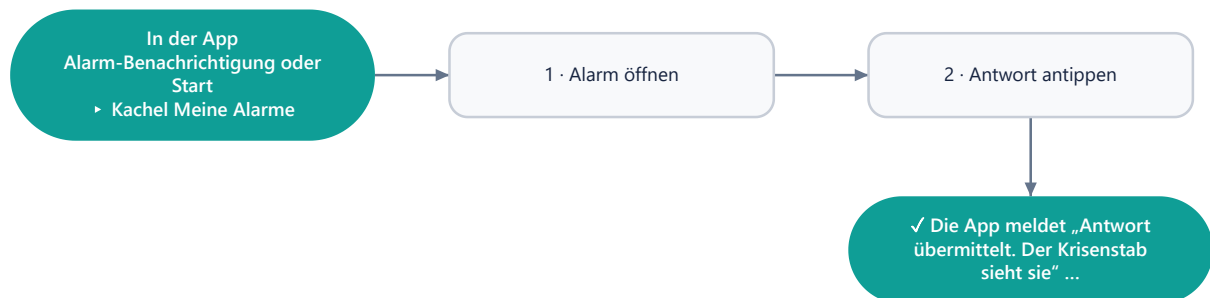
Achtung: Ohne die Freigabe für „Bitte nicht stören“ bleibt ein Alarm **still**, sobald der Ruhemodus läuft: „Ein Alarm erreicht Sie derzeit NICHT ...“. Schalten Sie außerdem den Android-Kanal *Alarme* der App nicht stumm.

Die Karte *Vollbild-Alarm erlauben* erscheint nur ab Android 14; ältere Fassungen erlauben das Vollbild von selbst.

12.4 Einen Alarm beantworten

⚙ **In der App:** Alarm-Benachrichtigung oder *Start* ▶ Kachel *Meine Alarme* · 🔑 kein Recht nötig – Sie müssen im Empfängerkreis stehen

Voraussetzung: Netz. Eine Antwort, die nur auf dem Telefon steht, erreicht den Krisenstab nicht.



Klickweg – Einen Alarm beantworten

1. Tippen Sie auf die Alarm-Benachrichtigung – oder öffnen Sie auf der Startseite *Meine Alarme*.
2. Tippen Sie beim Alarm auf *Ich komme*, *Zur Kenntnis* oder *Nicht verfügbar*.

✓ **Ergebnis:** Die App meldet „Antwort übermittelt. Der Krisenstab sieht sie im Lagebild.“; beim Alarm steht „Ihre Antwort: ...“.

Die drei Knöpfe stehen auch direkt in der Alarm-Benachrichtigung. Danach meldet das Telefon „Antwort gesendet“ – oder „Antwort NICHT gesendet“.

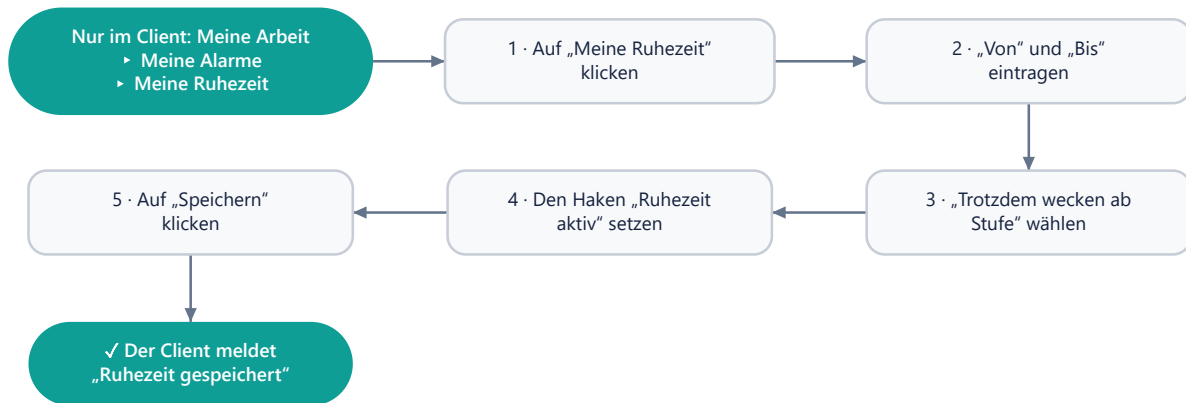
Achtung: Die Knöpfe **in der Benachrichtigung** brauchen eine laufende Sitzung der App. Wurde die App seit dem Einschalten des Telefons nicht geöffnet oder hat Android sie beendet, scheitert die Antwort voraussichtlich mit „Antwort NICHT gesendet“. Dann gilt: Benachrichtigung antippen, in *Meine Alarme* antworten. Kommt keine Verbindung zustande, melden Sie sich auf anderem Weg beim Krisenstab – etwa telefonisch. Antworten können Sie auch im Windows-Client (*Meine Arbeit* ▶ *Meine Alarme*) und im Portal (*Meine Vorgänge* ▶ *Meine Alarme*).

„Die Alarme konnten nicht geladen werden. Das ist KEINE Entwarnung ...“ heißt: Die App weiß nicht, ob ein Alarm offen ist. Sehen Sie im Client oder Portal nach. Einzelheiten zur Alarmierung stehen in ID-29.

12.5 Ruhezeit einstellen

Eine **Ruhezeit** hält nachts den Alarmton fern, nicht die Information: In-App-Meldung und E-Mail kommen weiter. Ab einer Stufe, die Sie wählen, weckt ein Alarm trotzdem.

 **Nur im Client:** *Meine Arbeit* ▶ *Meine Alarme* ▶ *Meine Ruhezeit* ·  kein Recht nötig — Portal und App bieten keine Einstellung der Ruhezeit.



Klickweg – Ruhezeit einstellen

1. Klicken Sie auf *Meine Ruhezeit*.
2. Tragen Sie unter *Von* (HH:mm) und *Bis* (HH:mm) den Zeitraum ein, zum Beispiel **22:00** und **06:00**.
3. Wählen Sie unter *Trotzdem wecken ab Stufe* *Notfall – sofortiges Handeln, auch nachts* oder *Kritisch – sofortiges Handeln nötig*.
4. Setzen Sie den Haken *Ruhezeit aktiv*.
5. Klicken Sie auf *Speichern*.

✓ **Ergebnis:** Der Client meldet „Ruhezeit gespeichert.“; die Ruhezeit gilt für Ihr Konto, also auf jedem Telefon. Das Feld *Zeitzone* ist mit der Zeitzone des Rechners vorbelegt; ist sie unlesbar, gilt die Ruhezeit nicht.

13 Aktualisierung und Mindestfassung

Die App hält sich **selbst** aktuell. Sie holt neue Fassungen direkt beim Hersteller (<https://update.ordavis.eu/v1/app/aktuell.json>, ersatzweise <https://ordavis.eu/app/aktuell.json>) – nicht bei Ihrem Server und nicht über den Play Store. Die Adresse ist fest eingebaut und lässt sich nicht ändern: Wer sie ändern könnte, könnte fremden Programmcode auf die Telefone bringen. Das Telefon braucht dafür einen Weg ins Internet.

Bevor installiert wird, prüft die App zweifach: Die Angabe, welche Fassung gilt, ist vom Hersteller **unterschrieben**, und die geladene Datei muss genau die **Prüfsumme** aus dieser Angabe haben. Was nicht passt, wird verworfen. Installiert wird nie im Hintergrund – Android fragt jedes Mal. Wie alle Komponenten aktualisiert werden, beschreibt ID-50a.

13.1 Hinweis beim Start und Pflichtband

Einmal je Programmstart sieht die App nach, ob es eine neue Fassung gibt:

- **Neue Fassung verfügbar:** Ein Dialog *Aktualisierung verfügbar* mit *Ansehen* und *Später*. *Ansehen* führt zu den Einstellungen.

- **Ihre Fassung liegt unter der Mindestfassung:** Der Dialog heißt *Diese Fassung wird nicht mehr unterstützt (Jetzt aktualisieren oder Später)*. Danach steht auf **jeder** Seite außer den Einstellungen oben ein rotes **Hinweisband**: „Diese Fassung wird nicht mehr unterstützt — gefordert ist mindestens 2026.10.01.1643. Zum Aktualisieren tippen.“

Das Band lässt sich nicht wegwischen; es verschwindet erst mit der neuen Fassung. Es **sperrt aber nichts** – Sie können weiterarbeiten, etwa wenn Sie gerade vor einem Rack stehen. Tippen auf das Band führt zu den Einstellungen.

13.2 Von Hand aktualisieren

 In der App: Zahnrad ▶ Aktualisierung ·  kein Recht nötig



Klickweg – Von Hand aktualisieren

1. Tippen Sie in der Kopfzeile auf das *Zahnrad*.
2. Tippen Sie im Abschnitt *Aktualisierung* auf *Nach Aktualisierung suchen*.
3. Tippen Sie auf *Herunterladen*.
4. Tippen Sie auf *Freigabe erteilen*, falls die Schaltfläche erscheint, und erlauben Sie der App in Android, Apps zu installieren.
5. Tippen Sie auf *Jetzt installieren*.
6. Bestätigen Sie die Rückfrage von Android.

✓ **Ergebnis:** Die App startet kurz neu; unter *Über* ▶ *APP AUF DIESEM GERÄT* steht die neue Fassung.

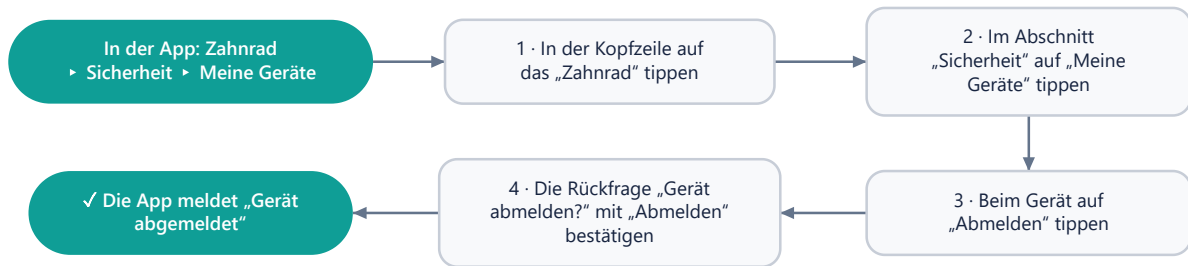
Im Mobilfunknetz weist die App darauf hin, dass der Download rund 40 MB misst. Die eigene Fassung steht unter *Auf diesem Gerät*:

14 Sicherheit und Datenschutz

14.1 Meine Geräte: ein Gerät abmelden

Die Liste *Meine Geräte* zeigt jedes Mobilgerät, mit dem Ihr Konto angemeldet ist – mit den Kennzeichen *Dieses Gerät*, *Abgemeldet*, *Benachrichtigungen an*, *kann Anmeldung freigeben* und *Schlüssel im Sicherheitsbaustein*, dazu „Erstmals ...“ und „Zuletzt ...“.

 In der App: Zahnrad ▶ Sicherheit ▶ Meine Geräte ·  kein Recht nötig – jede Person sieht nur ihre eigenen Geräte



Klickweg – Meine Geräte: ein Gerät abmelden

1. Tippen Sie in der Kopfzeile auf das *Zahnrad*.
2. Tippen Sie im Abschnitt *Sicherheit* auf *Meine Geräte*.
3. Tippen Sie beim Gerät auf *Abmelden*.
4. Bestätigen Sie die Rückfrage *Gerät abmelden?* mit *Abmelden*.

✓ **Ergebnis:** Die App meldet „Gerät abgemeldet.“; das Gerät trägt das Kennzeichen *Abgemeldet*. Seine Sitzung ist beendet, Benachrichtigungen gehen nicht mehr dorthin, und die Freigabe per App ist erloschen. Ist es das Telefon, das Sie gerade in der Hand haben, meldet die App Sie sofort ab.

Achtung: Abmelden ist **keine Fernlöschung** und **keine Sperre**. Auf dem abgemeldeten Gerät wird nichts gelöscht, auch nicht die noch nicht gesendeten Handlungen. Wer dort Ihr Kennwort kennt, meldet sich einfach neu an. Ein Gerät, das Sie nicht kennen, melden Sie deshalb ab **und** ändern danach Ihr Kennwort. Dauerhaft ausschließen lässt sich jemand nur, indem die Verwaltung das Konto sperrt (ID-41).

14.2 Ein Gerät im Windows-Client abmelden

Ist das Telefon verloren, melden Sie es am Arbeitsplatz ab.

🖥️ **Nur im Client:** Fußbereich ▸ *Einstellungen* ▸ *Mein Profil* oder *Konto-Menü* ▸ *Mein Profil* · 🔑 kein Recht nötig — Das Portal zeigt die Mobilgeräte nicht; dort heißt *Meine Geräte* etwas anderes (die Ihnen zugewiesenen Arbeitsgeräte).



Klickweg – Ein Gerät im Windows-Client abmelden

1. Öffnen Sie *Mein Profil*.
2. Klicken Sie in der Karte *Meine Geräte* beim Telefon auf *Löschen*.
3. Bestätigen Sie die Rückfrage *Gerät abmelden?* mit *Löschen*.

✓ **Ergebnis:** Der Client meldet „Gerät abgemeldet.“. Ein schon ausgegebener Zugriff gilt höchstens noch zehn Minuten. Ändern Sie danach Ihr Kennwort (ID-41).

Hinweis: Beendet die Verwaltung im Client Ihre **Sitzungen** in der Benutzerverwaltung, bleibt das Telefon in *Meine Geräte* stehen und bekommt weiter Benachrichtigungen. Zum Abschneiden eines Telefons ist *Löschen* in *Meine Geräte* der richtige Weg.

14.3 Lokale Daten löschen

Bevor ein Telefon den Besitzer wechselt, gehört Ihre Anmeldung samt Zwischenspeicher herunter.

⚙️ **In der App:** *Zahnrad* ▶ *Datenschutz* ▶ *Lokale Daten löschen* · 🔑 kein Recht nötig

Voraussetzung: Liegt noch etwas in der Warteschlange, senden Sie es vorher (Abschnitt 11.2) – sonst geht es verloren.



Klickweg – Lokale Daten löschen

1. Tippen Sie in der Kopfzeile auf das *Zahnrad*.
2. Tippen Sie im Abschnitt *Datenschutz* auf *Lokale Daten löschen*.
3. Bestätigen Sie die Rückfrage mit *Löschen*.

✓ **Ergebnis:** Die App meldet „Lokale Daten gelöscht.“; Anmeldung, Zwischenspeicher und Warteschlange sind vom Telefon entfernt. Lagen noch Handlungen in der Warteschlange, hat die Rückfrage mit „Achtung: ... noch nicht gesendete Handlung(en) gehen dabei verloren.“ gewarnt. Am Server ändert sich nichts.

Hinweis: Gelöscht werden nur die Daten der **gerade gewählten** Verbindung. Andere gemerkte Verbindungen (Abschnitt 4.4) und das Protokoll der App bleiben liegen. Wer das Telefon ganz zurückgibt, deinstalliert die App oder setzt das Telefon zurück.

14.4 Was auf dem Telefon liegt

Was	Wo auf dem Telefon	Geschützt
gemerkte Anmeldung (je Verbindung)	Schlüsselspeicher von Android	ja, vom System verschlüsselt
Zugriff der laufenden Sitzung	nur im Arbeitsspeicher	–
Geräteschlüssel für die Anmeldung per App	Schlüsselspeicher, wenn vorhanden im Sicherheitsbaustein	ja

Was	Wo auf dem Telefon	Geschützt
Schlüssel zum Entschlüsseln der Push-Nachrichten	Schlüsselspeicher	ja
Warteschlange samt Fotos, gemerkte Wissensartikel, mitgenommene Handbücher und Checklisten	Datenbank der App, je Verbindung eine	nein , nur durch die Gerätesperre
Serveradressen, Fingerabdrücke, Einstellungen	Einstellungen der App	nein
Protokoll der App	Datei <code>mobile-JJJJMMTT.log</code> im App-Verzeichnis	nein

Die App erhebt **keinen Standort** und sendet keine Nutzungsstatistik. Fingerabdruck und Gesicht prüft nur Android. Jede Anfrage an den Server trägt eine zufällige Geräteerkennung, damit das Protokoll des Servers festhält, von welchem Gerät eine Handlung kam (ID-40).

Hinweis: Das Protokoll lässt sich in der App weder ansehen noch exportieren. Für eine Fehleranalyse beschreiben Sie Ihrer IT, was Sie getan haben und welche Meldung erschien.

15 Referenz: die Einstellungsseite der App

Das *Zahnrad* öffnet die *Einstellungen* mit diesen Abschnitten:

Abschnitt	Inhalt
<i>Profil</i>	Name, <i>ANMELDENAME</i> , <i>RECHTE</i> (Anzahl Ihrer Berechtigungen), <i>SITZUNG</i> ; <i>Anmelden</i> bzw. <i>Abmelden</i> (Abschnitt 5.5)
<i>Sicherheit</i>	<i>Gemerkte Anmeldung biometrisch schützen</i> (Abschnitt 5.4), <i>Meine Geräte</i> (Abschnitt 14.1)
<i>Alarmierung</i>	Auskunft über die Alarmzustellung, <i>Vollbild-Alarm erlauben</i> , „Bitte nicht stören“ <i>übersteuern</i> (Abschnitt 12.3)
<i>Verbindung</i>	<i>SERVER</i> mit Adresse und Verbindungsstand, <i>Serveradresse einrichten</i> bzw. <i>Serveradresse ändern</i> (Abschnitt 4), <i>Verbindung prüfen</i>
<i>Werkzeuge</i>	<i>Inventur</i> – nur mit <code>cldb.ci.update</code> (Abschnitt 9.3)
<i>Abgleich</i>	<i>Offline-Warteschlange</i> , „Zuletzt abgeglichen: ...“, <i>Jetzt abgleichen</i> (Abschnitt 11.2)
<i>Datenschutz</i>	<i>Was dieses Gerät speichert</i> , Hinweise zu Fotos, Biometrie, Standort und Push, <i>Lokale Daten löschen</i> (Abschnitt 14.3)
<i>Über</i>	<i>APP AUF DIESEM GERÄT</i> und <i>SERVER</i> mit Fassung und Stand
<i>Aktualisierung</i>	<i>Nach Aktualisierung suchen</i> , <i>Herunterladen</i> , <i>Jetzt installieren</i> (Abschnitt 13.2)

16 Fehlerbehebung

Meldung (wörtlich)	Ursache	Abhilfe
„Bitte zuerst die Adresse des Ordavis-Servers hinterlegen.“ / „Es ist noch keine Serveradresse eingerichtet.“	Keine Serveradresse eingetragen.	Adresse eintragen (Abschnitt 4.1).
„Ungültige Adresse. Beispiel: <code>https://server.firma.local:5001</code> “	Kein gültiger Rechnername oder ein anderes Schema als <code>http/https</code> .	Adresse mit <code>https://</code> und Port eintragen.

Meldung (wörtlich)	Ursache	Abhilfe
„Server ordavis.musterstadt.local:5001 nicht erreichbar. Adresse, WLAN/Mobilfunk und Firewall prüfen.“	Kein Netz, falscher Rechner oder Port, Firewall, kein VPN.	WLAN oder VPN prüfen, Adresse bei der IT erfragen.
„Zeitüberschreitung — der Server hat nicht rechtzeitig geantwortet.“	Mehr als 15 Sekunden ohne Antwort.	Später erneut; bei Dauer die IT informieren.
„Die Adresse antwortet, ist aber keine Ordavis-API.“	Adresse des Portals, eines Proxys oder Routers statt der Schnittstelle.	Adresse der API eintragen (Abschnitt 2.2).
„Das Serverzertifikat ist nicht vertrauenswürdig. Sein Fingerabdruck: ... — gleichen Sie ihn mit dem Serveradministrator ab, bevor Sie ihm vertrauen.“	Eigenes Zertifikat ohne bekannte Zertifizierungsstelle, oder das Zertifikat wurde erneuert.	Fingerabdruck abgleichen, <i>Diesem Zertifikat vertrauen</i> (Abschnitt 4.3).
„Der Fingerabdruck muss ein SHA-256-Wert sein: 64 Hex-Zeichen, Doppelpunkte erlaubt.“	Fingerabdruck unvollständig oder falsch eingefügt.	Vollständig eintragen.
„Die Verbindungen gibt der Administrator vor.“	Die Geräteverwaltung gibt die Verbindungen vor.	Kein Fehler; Änderungen über die IT (Abschnitt 3.3).
„Es sind höchstens 12 eigene Verbindungen möglich. (Parameter 'apiBaseUrl')“	Die Liste der gemerkten Verbindungen ist voll.	Einen Eintrag <i>Entfernen</i> .
„Die gerade verbundene Adresse lässt sich nicht entfernen — erst umschalten. (Parameter 'id')“	Die aktive Verbindung soll entfernt werden.	Erst auf eine andere umschalten.
„Anmeldename oder Kennwort stimmt nicht.“	Falsche Zugangsdaten – oder das Konto ist gesperrt, deaktiviert, eingeschränkt, verlangt einen zweiten Faktor, der nicht eingerichtet ist, oder hat keinen Zugang zum gewählten Mandanten. Die App unterscheidet das nicht.	Eingabe prüfen; hilft das nicht, die Verwaltung bitten, Konto und Ereignisprotokoll zu prüfen (ID-41).
„Anmeldung abgelehnt — Code prüfen (er gilt nur kurz) oder erneut anmelden.“	Code falsch oder abgelaufen; Kennwort und Code sind geleert.	Kennwort und neuen Code eintragen.
„Zu diesem Anmeldename gibt es keinen Mandanten.“	Anmeldename unbekannt oder vertippt.	Schreibweise prüfen.
„Die Sitzung ist abgelaufen. Bitte erneut anmelden.“	12 Stunden ohne Nutzung, Gerät abgemeldet oder Sitzung am Server beendet.	Neu anmelden.
„Gemerkte Anmeldung ist gesperrt — App erneut öffnen und bestätigen oder neu anmelden.“	Die biometrische Abfrage wurde abgebrochen.	App ganz schließen und neu öffnen, oder neu anmelden (Abschnitt 5.4).
„Nicht angemeldet.“	In diesem Programmlauf besteht keine Sitzung, etwa nach einem Start ohne Netz.	App ganz schließen und mit Netz neu öffnen, oder anmelden.
„Dafür fehlt die Berechtigung.“	Der Server hat die Handlung abgewiesen (fehlendes Recht).	Recht bei der Verwaltung beantragen.
„Der Server kennt diese Funktion nicht.“ / „Das Modul '...' ist für diesen Mandanten nicht aktiviert.“	Der Server ist älter als die App, oder das Modul ist ausgeschaltet.	Server aktualisieren bzw. Modul einschalten lassen (ID-40).

Meldung (wörtlich)	Ursache	Abhilfe
„Netzverwaltung ist nicht eingeschaltet“	Modul Netzverwaltung aus.	Kein Fehler; bei Bedarf die Verwaltung fragen.
„Kamera nicht freigegeben“	Die Kamerafreigabe wurde verweigert.	In Android unter <i>Apps</i> ▶ <i>Ordavis IT</i> ▶ <i>Berechtigungen</i> die Kamera erlauben.
„NFC ist ausgeschaltet. Bitte in den Android-Einstellungen einschalten.“	NFC aus.	NFC einschalten.
„Dieses Gerät hat keine NFC-Hardware.“	Das Telefon hat kein NFC.	Etiketten mit der Kamera scannen.
„Es wurde kein Tag ans Telefon gehalten.“	20 Sekunden ohne Tag.	Erneut, Tag mittig an die Rückseite halten.
„Der Tag wurde zugeordnet, ließ sich aber nicht beschreiben: ...“	Tag schreibgeschützt oder zu klein. Die Zuordnung ist trotz des Wortlauts nicht angelegt.	Anderen Tag verwenden, Liste <i>NFC-Tags</i> prüfen (Abschnitt 8.4).
„Etikett nicht vertrauenswürdig“ / „Dieses Etikett stammt nicht aus dieser Ordavis IT. ...“	Der Prüfwert auf dem Aufkleber passt nicht zum Gerät.	Gerät über die Seriennummer suchen, Aufkleber melden.
„Kein Gerät zu diesem Code gefunden.“ / „Unbekannter NFC-Tag“	Der Code oder Tag gehört zu keinem erfassten Gerät.	Gerät im Client oder Portal anlegen bzw. Tag zuordnen.
„Dieser Lauf ist abgeschlossen — Erfassungen sind nicht mehr möglich.“	Der Inventurlauf ist abgeschlossen.	Neuen Lauf anlegen.
„ · Inventur fehlgeschlagen: ...“	Die Buchung in den Lauf wurde abgewiesen, etwa ohne Netz oder ohne <code>cmdb.ci.update</code> .	Netz und Recht prüfen, erneut scannen.
„Für das Melden fehlt die Berechtigung.“	Kein <code>tickets.create</code> .	Recht beantragen.
„Kein Netz — und die Meldung ließ sich nicht merken. Bitte notieren und später erneut melden.“	Die Ablage auf dem Telefon ist gescheitert, etwa bei vollem Speicher.	Meldung notieren, Speicher freimachen, später melden.
„Der Vorgang wurde angelegt, das Foto ließ sich nicht anhängen.“	Das Foto scheiterte fünfmal.	Foto im Client oder Portal nachreichen.
„... abgelehnt“ / „... kollidiert“	Der Server hat eine gemerkte Handlung abgewiesen bzw. der Stand hat sich geändert.	Abschnitt 11.3.
„Die Alarme konnten nicht geladen werden. Das ist KEINE Entwarnung: ...“	Server oder Netz gestört, oder das Modul Notfallmanagement ist aus.	Im Client oder Portal nachsehen.
„Ohne Verbindung lässt sich nicht quittieren — ...“	Kein Netz.	Netz suchen; sonst telefonisch beim Krisenstab melden.
„Sie stehen nicht im Empfängerkreis dieses Alarms und können ihn nicht quittieren.“	Der Alarm richtet sich nicht an Sie.	–

Meldung (wörtlich)	Ursache	Abhilfe
„Antwort NICHT gesendet“ – „Die Quittierung konnte nicht übermittelt werden. Der Alarm steht weiter — bitte in der App antworten.“	Kein Netz, Server gestört – oder keine laufende Sitzung der App (Abschnitt 12.4).	Benachrichtigung antippen und in <i>Meine Alarme</i> antworten.
„Ein Alarm erreicht Sie derzeit NICHT: „Bitte nicht stören“ ist eingeschaltet, und Ordavis darf es nicht uebersteuern. ...“	Ruhemodus an, Freigabe fehlt.	„Bitte nicht stören“ <i>übersteuern</i> (Abschnitt 12.3).
„Diese Anmeldeanfrage ist nicht mehr offen — sie wurde bereits beantwortet oder ist abgelaufen.“	Fünf Minuten vorbei oder schon beantwortet.	Am Rechner neu anmelden.
„Das hat nicht geklappt. Prüfen Sie die Zahl und versuchen Sie es erneut.“	Falsche Zahl – oder der Geräteschlüssel ist am Server nicht bekannt.	Richtige Zahl antippen; hilft das nicht, das Telefon in <i>Meine Geräte</i> abmelden und neu anmelden.
„Dieses Gerät ist nicht eingeschrieben — bitte in den Einstellungen erneut anmelden.“	Auf dem Telefon fehlt der Geräteschlüssel.	Ab- und neu anmelden (Abschnitt 5.5).
„Die Geräteliste konnte nicht geladen werden.“	Server oder Netz gestört.	Später erneut.
„Die lokalen Daten ließen sich nicht vollständig löschen.“	Eine Datei war gesperrt.	App schließen, erneut löschen; sonst App deinstallieren.
„Die geladene Datei stimmt nicht mit dem Manifest überein und wurde verworfen.“	Die Prüfsumme der geladenen Fassung stimmt nicht.	Erneut laden; bleibt es so, den Hersteller informieren.
„Android lässt die Installation erst zu, wenn diese App in den Systemeinstellungen unter „Unbekannte Apps installieren“ zugelassen ist.“	Die Installationsfreigabe fehlt.	<i>Freigabe erteilen</i> (Abschnitt 13.2).
„Android hat die Installation abgelehnt: Auf dem Gerät ist zu wenig Platz.“	Speicher voll.	Platz schaffen, erneut installieren.
„Android hat die Installation abgelehnt: Auf diesem Gerät läuft bereits eine neuere Fassung, und ein Rückschritt ist nicht zugelassen.“	Die angebotene Fassung ist älter als die installierte.	Nichts zu tun.

17 Beispiele aus der Praxis

17.1 Beispiel: Inventur im Bauhof Musterstadt

Ausgangslage: Im Bauhof der Gemeinde Musterstadt stehen rund 40 Geräte – Rechner, Etikettendrucker, Tablets, ein Switch. Alle tragen Ordavis-Etiketten. Der Techniker Jonas Beispiel hat das Recht `cmdb.ci.update`, ein Diensttelefon mit der App und im Bauhof WLAN.

 In der App: Start ▶ Kachel Inventur ·  cmdb.ci.update



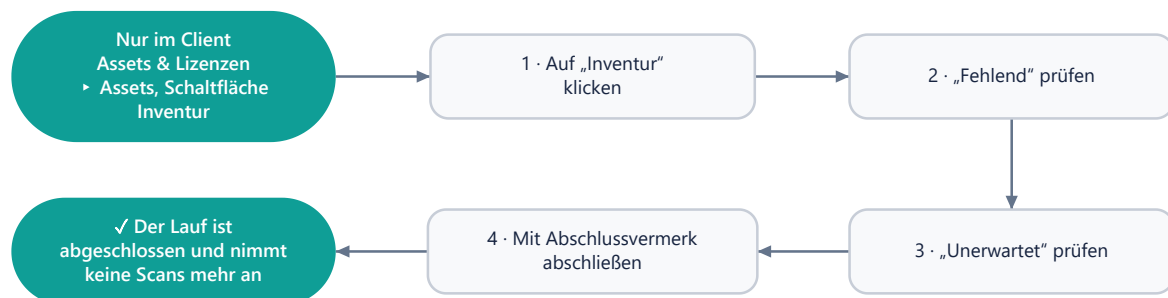
Klickweg – Beispiel: Inventur im Bauhof Musterstadt

1. Tippen Sie auf der Startseite auf *Inventur*.
2. Tippen Sie auf *Neuer Lauf*.
3. Scannen Sie im Büro des Bauhofs ein Etikett nach dem anderen.
4. Tippen Sie im dunklen Lagerraum auf *Licht* und scannen Sie dort weiter.
5. Scannen Sie auch den alten Drucker ohne Ordavis-Etikett über seinen Hersteller-Barcode.

✓ **Ergebnis:** Der Lauf „Inventur 02.10.2026 09:15“ zählt 38 Geräte; jeder Scan meldete „...“ in der Inventur gebucht.“. Der alte Drucker stand als „Kein Treffer — Code steht in der Liste“ in der Inventur gebucht.“ da.

Zurück im Rathaus wertet Herr Beispiel den Lauf aus:

 **Nur im Client: Assets & Lizenzen** ▶ Assets, Schaltfläche Inventur ·  cmdb.ci.update — Das Portal zeigt den Lauf unter Assets & Lizenzen ▶ Inventur an, schließt ihn aber nicht ab.



Klickweg – Beispiel: Inventur im Bauhof Musterstadt

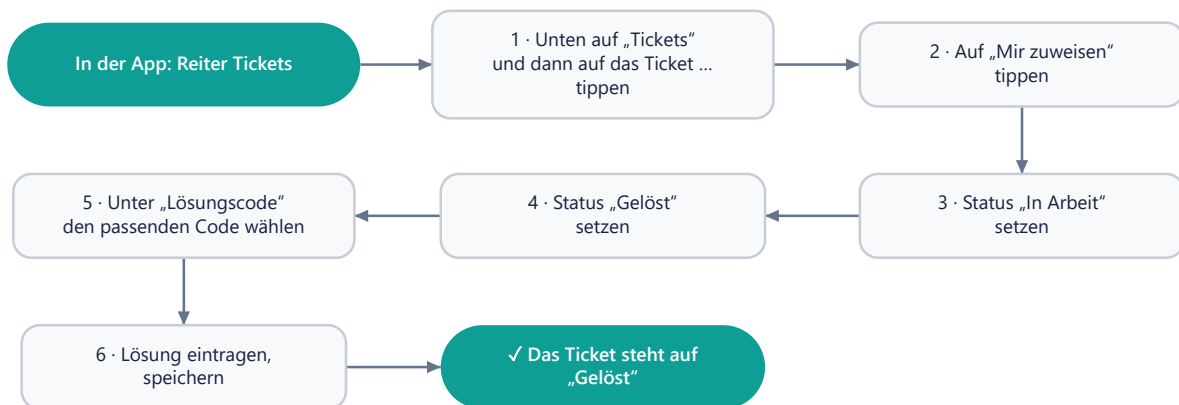
1. Klicken Sie auf *Inventur* und wählen Sie den Lauf.
2. Prüfen Sie *Fehlend*: Zwei Tablets fehlen – sie sind mit der Kolonne unterwegs.
3. Prüfen Sie *Unerwartet*: Der alte Drucker ist nicht erfasst und wird im Client nachgetragen (ID-21).
4. Klicken Sie auf *Abschließen*, tragen Sie unter *Abschlussvermerk* 2 Tablets bei der Kolonne, Drucker nachgetragen ein und bestätigen Sie mit *Abschließen*.

✓ **Ergebnis:** Der Lauf ist abgeschlossen und nimmt keine Scans mehr an. Die Abweichungen sind mit Begründung festgehalten.

17.2 Beispiel: Ein Ticket unterwegs lösen

Ausgangslage: Im Bürgerbüro der Stadtverwaltung Musterstadt druckt der Drucker im 3. OG nicht. Das Ticket liegt in der Gruppe *Vor-Ort-Service*. Die Technikerin Anna Muster hat die Rechte `tickets.read`, `tickets.assign` und `tickets.update` und ist gerade im Haus unterwegs.

⚙️ **In der App:** Reiter *Tickets* · 🔑 `tickets.assign` und `tickets.update`



Klickweg – Beispiel: Ein Ticket unterwegs lösen

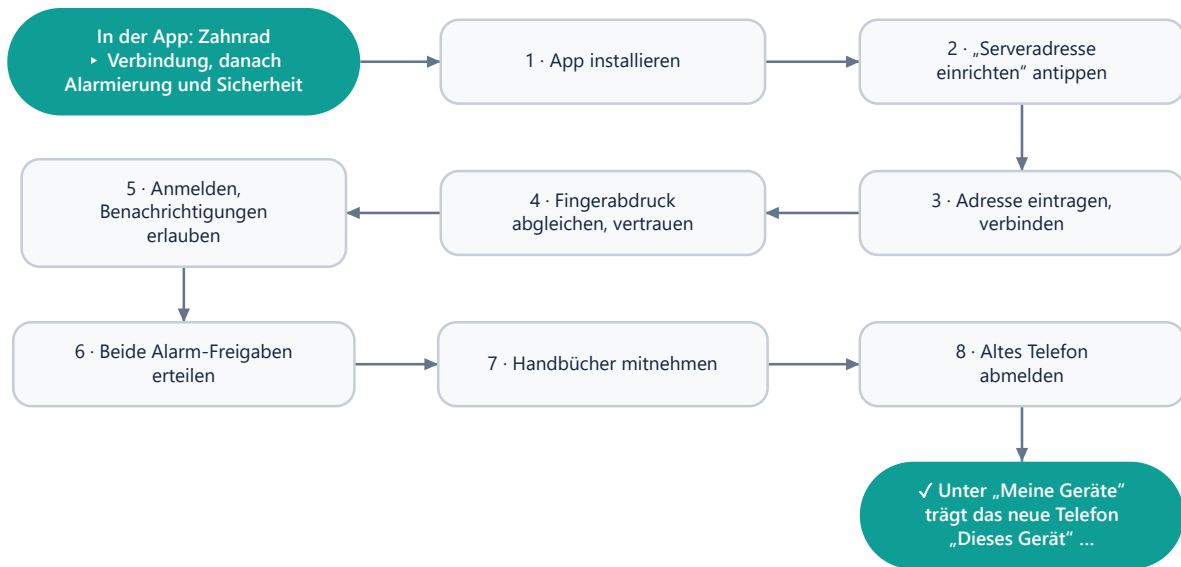
1. Tippen Sie unten auf *Tickets* und dann auf das Ticket „Drucker 3. OG druckt nicht“.
2. Tippen Sie auf *Mir zuweisen*.
3. Tippen Sie auf *Status setzen* und wählen Sie *In Arbeit*.
4. Tippen Sie nach dem Tonerwechsel auf *Status setzen* und wählen Sie *Gelöst*.
5. Wählen Sie unter *Lösungscod* den passenden Code.
6. Tragen Sie unter *Was wurde gemacht?* `Toner getauscht`, `Testseite gedruckt` ein und tippen Sie auf *Speichern*.

✓ **Ergebnis:** Das Ticket steht auf *Gelöst*; die meldende Person wird nach den Regeln des Service-Desks informiert (ID-20). Der Kellerraum mit dem Druckerlager hatte kein Netz – die Zuweisung, die Frau Muster dort getippt hatte, meldete „Übernahme gemerkt“ und ging beim Verlassen des Kellers von selbst hinaus.

17.3 Beispiel: Ein neues Diensttelefon für die Bereitschaft einrichten

Ausgangslage: Herr Beispiel bekommt ein neues Diensttelefon mit Android 14 und Google-Play-Diensten. Er hat in der Bereitschaftswoche Rufdienst, muss nachts geweckt werden und hat das Recht `handbook.read`. Der Server der Gemeinde ist unter `https://ordavis.musterstadt.local:5001` erreichbar und trägt ein selbst ausgestelltes Zertifikat. Das alte Telefon ist noch angemeldet.

⚙️ **In der App:** *Zahnrad* ▶ *Verbindung*, danach *Alarmierung* und *Sicherheit* · 🔑 kein Recht nötig



Klickweg – Beispiel: Ein neues Diensttelefon für die Bereitschaft einrichten

1. Installieren Sie die App wie in Abschnitt 3.2.
2. Tippen Sie auf das *Zahnrad* und im Abschnitt *Verbindung* auf *Serveradresse einrichten*.
3. Tragen Sie `https://ordavis.musterstadt.local:5001` ein und tippen Sie auf *Speichern und verbinden*.
4. Gleichen Sie den angezeigten Fingerabdruck mit der IT ab und tippen Sie auf *Diesem Zertifikat vertrauen*.
5. Tippen Sie auf der Startseite auf *Anmelden*, melden Sie sich an und erlauben Sie Benachrichtigungen, wenn Android fragt.
6. Tippen Sie im Abschnitt *Alarmierung* auf *Vollbild-Alarm erlauben* und auf „Bitte nicht stören“ übersteuern und erteilen Sie beide Freigaben.
7. Tippen Sie auf der Startseite auf die Kachel *Handbücher* und dort auf *Für den Notfall mitnehmen*.
8. Tippen Sie unter *Sicherheit* ▸ *Meine Geräte* beim alten Telefon auf *Abmelden* und bestätigen Sie.

✓ **Ergebnis:** Unter *Meine Geräte* trägt das neue Telefon *Dieses Gerät*, *Benachrichtigungen an* und *kann Anmeldung freigeben*; das alte steht als *Abgemeldet* da. Die Auskunft unter *Alarmierung* lautet „Ein Alarm uebernimmt den Bildschirm und durchbricht „Bitte nicht stoeren.““ Die Notfallhandbücher liegen auf dem Gerät.

Tip: Lassen Sie sich zum Abschluss eine Probealarmierung schicken (ID-29) – nur so sehen Sie, dass das Telefon wirklich klingelt.

18 Häufige Fragen

Gibt es die App im Play Store? Nein. Sie kommt als APK vom Hersteller, über den Kundenbereich oder Ihre Geräteverwaltung (Abschnitt 3).

Gibt es die App für das iPhone? Nein, nur für Android.

Ab welcher Android-Fassung läuft die App? Ab Android 6.0. Der biometrische Schutz der gemerkten Anmeldung braucht Android 11 (Abschnitt 2.1).

Brauche ich ein Google-Konto? Nein – weder zum Installieren noch zum Anmelden oder Aktualisieren. Nur Push-Benachrichtigungen setzen die Google-Play-Dienste auf dem Telefon voraus (Abschnitt 12).

Welche Adresse trage ich ein? Die Adresse der Ordavis-Schnittstelle mit `https://` und Port, zum Beispiel `https://ordavis.musterstadt.local:5001` – nicht die des Portals (Abschnitt 4.1).

Kann ich das Telefon per QR-Code mit dem Server koppeln? Nein. Die Adresse wird eingetragen oder von der Geräteverwaltung vorgegeben (Abschnitt 3.3).

Unser Server hat ein selbst ausgestelltes Zertifikat. Geht das? Ja. Bestätigen Sie den Fingerabdruck nach dem Abgleich mit Ihrer IT, oder lassen Sie ihn per Geräteverwaltung vorgeben (Abschnitt 4.3).

Warum warnt die App gelb bei meiner Adresse? Die Adresse beginnt mit `http://`; Kennwort und Daten gehen dann unverschlüsselt über das Netz. Laut Ankündigung verbindet die nächste Fassung nur noch über HTTPS (Abschnitt 4.2).

Kann ich mehrere Server nutzen? Ja, bis zu zwölf gemerkte Verbindungen, jede mit eigener Anmeldung und eigenem Offline-Bestand (Abschnitt 4.4).

Wie lange bleibe ich angemeldet? Solange Sie die App wenigstens alle zwölf Stunden nutzen; danach ist eine neue Anmeldung nötig (Abschnitt 5.3).

Fliege ich am PC raus, wenn ich mich in der App anmelde? Nein. Arbeitsplatz und Telefon melden einander nicht ab (Abschnitt 5.2).

Warum fehlen mir Reiter oder Kacheln? Sie folgen Ihren Rechten. Die Tabelle in Abschnitt 2.3 nennt für jeden Reiter und jede Kachel das Recht; beantragen Sie es bei Ihrer Verwaltung.

Die Kachel *Meine Alarme* fehlt auf meiner Startseite. Sie erscheint nur, wenn wenigstens eine weitere Kachel sichtbar ist – ein Fehler der App. Eine Alarm-Benachrichtigung öffnet die Seite trotzdem; antworten können Sie auch im Client und im Portal (Abschnitt 6).

Kann ich dem Melder aus der App antworten? Nein. Die *Notiz* ist immer intern. Antworten Sie im Windows-Client oder Portal (Abschnitt 7.4).

Kann ich mit der App ein neues Gerät anlegen? Nein. Legen Sie es im Client oder Portal an und ordnen Sie danach Etikett oder NFC-Tag zu (Abschnitt 9.2).

Kann ich Etiketten mit der normalen Kamera-App scannen? Nein, nur über den Reiter *Scannen* (Abschnitt 9.1).

Was geht ohne Netz? Melden, Tickets übernehmen, Status und Notizen, Checklisten und Bestellungen werden gemerkt; gemerkte Wissensartikel, Handbücher und Checklisten bleiben lesbar. Suchen, Scannen, Inventur und Alarme brauchen Netz (Abschnitt 11.1).

Gehen ungesendete Meldungen beim Abmelden verloren? Nein, sie bleiben in der Warteschlange – und gehen unter dem Konto hinaus, das sich als Nächstes anmeldet. Verloren gehen sie nur bei *Lokale Daten löschen* (Abschnitte 5.5 und 14.3).

Was bedeutet „Serverstand hat sich geändert“? Jemand hat den Vorgang inzwischen am Server geändert. *Eigenen Stand durchsetzen* überschreibt die Änderung, *Serverstand behalten* verwirft Ihre Erfassung (Abschnitt 11.3).

Es kommen keine Benachrichtigungen. Was prüfe ich? Der Reihe nach: Benachrichtigungen in Android erlaubt? Google-Play-Dienste vorhanden? Steht unter *Meine Geräte* „Benachrichtigungen an“? Ist für das Ereignis im Windows-Client die Spalte *Push* eingeschaltet? Abbildung 3 zeigt die Reihenfolge.

Wo schalte ich ein, welche Ereignisse aufs Telefon kommen? Nur im Windows-Client unter *Benachrichtigungen*, Spalte *Push*. Vorgabe ist aus (Abschnitt 12.2).

Nachts kommt kein Alarmton. Warum? Meist fehlt die Freigabe für „Bitte nicht stören“, oder Ihre Ruhezeit hält den Alarm zurück, oder der Android-Kanal *Alarme* ist stumm geschaltet (Abschnitte 12.3 und 12.5).

Wie beantworte ich einen Alarm? Mit *Ich komme*, *Zur Kenntnis* oder *Nicht verfügbar* in der Benachrichtigung oder unter *Meine Alarmer* – nur mit Netz (Abschnitt 12.4).

Wo stelle ich meine Ruhezeit ein? Nur im Windows-Client unter *Meine Arbeit* ▶ *Meine Alarmer* ▶ *Meine Ruhezeit* (Abschnitt 12.5).

Warum steht in der Benachrichtigung nur „Neue Meldung“? Die App konnte den verschlüsselten Inhalt auf dem Telefon nicht öffnen, etwa nach einer Neuinstallation. Öffnen Sie die App einmal; sie meldet dabei ihren Schlüssel neu.

Muss ich aktualisieren? Steht das rote Band „Diese Fassung wird nicht mehr unterstützt ...“ da, ja. Sonst ist das Update freiwillig, aber empfohlen (Abschnitt 13).

Warum braucht das Update Internet, obwohl der Server im Haus steht? Die App holt neue Fassungen beim Hersteller, nicht bei Ihrem Server (Abschnitt 13).

Mein Telefon ist weg. Was tun? Im Windows-Client unter *Mein Profil* ▶ *Meine Geräte* das Telefon abmelden und danach das Kennwort ändern. Eine Fernlöschung gibt es nicht (Abschnitt 14.2).

Kann ich mein Telefon als privat kennzeichnen? Nein. Keine Oberfläche bietet das an; jedes Telefon gilt als dienstlich.

Erfasst die App meinen Standort? Nein. Sie fragt kein Standortrecht an, und Fotos verlieren vor dem Senden alle Metadaten (Abschnitt 14.4).

Muss ich bei jedem Start das Startbild abwarten? Nein, Antippen überspringt es (Abschnitt 1.1).

Verwandte Themen

- ID-01 – Einführung & Grundlagen – die Oberflächen von Ordavis IT im Überblick
- ID-11 – Agentenhandbuch – Service Desk – Tickets am Arbeitsplatz bearbeiten und dem Melder antworten
- ID-21 – Modul CMDB – Geräte anlegen, Etiketten und NFC-Tags
- ID-29 – Modul BCM – Alarmierung, Empfängerkreise und Probealarm
- ID-31 – Modul Benachrichtigungen & E-Mail-Integration – Benachrichtigungswege und die Spalte *Push*
- ID-40 – Administrationshandbuch – Push-Zustellung, App ohne Google-Dienste, Protokolle
- ID-41 – Modul Identität, Benutzer & Rollen – Konten, zweiter Faktor, *Mein Profil*
- ID-50 – Betriebshandbuch – HTTPS, Zertifikat und Fingerabdruck am Server
- ID-50a – Update-System – wie die App und alle anderen Komponenten aktualisiert werden