HANDBUCH FÜR ADMINISTRATOREN

CosyTrack.Drive 60.0 – Admin-Handbuch

Installation, Konfiguration und Betrieb auf Arbeitsplätzen und RD-Sitzungshosts.

Angabe	Wert
Gilt für	CosyTrack.Drive 60.0
Zielgruppe	IT-Abteilungen und Systemhäuser
Stand	November 2026
Herausgeber	Ulrich B. Boddenberg
Web	boddenberg.de

Inhalt

1 Architektur 4
2 Voraussetzungen 7
3 App-Registrierung 7
3.1 Anmeldung der Benutzer 9
4 Installation 10
4.1 Pakete 10
4.2 Befehle 12
4.3 Öffentliche Eigenschaften 13
4.4 Reihenfolge auf Terminalservern 13
4.5 Verteilung per Gruppenrichtlinie 13
4.6 Verteilung mit SCCM/MECM 14
4.7 Verteilung mit Intune 14
5 Update 14
6 Konfiguration 15
6.1 Vorrang 15
6.2 Gruppenrichtlinien 16
6.3 Konfigurations-App 16
7 Lizenzierung 21
8 Lizenznutzung (Admin-Kit) 23
8.1 Voraussetzungen 24
8.2 App-Registrierung anlegen, Variante A: interaktiv 24
8.3 App-Registrierung anlegen, Variante B: unbeaufsichtigt 25
8.4 Historie und Abdeckung 25
8.5 Variante Log Analytics 26
8.6 Geplante Aufgabe 26
8.7 Namensanzeige und warum sie doppelt abgesichert ist 26
8.8 Fehlermeldungen 27
8.9 Named User sauber verwalten 27
9 Speicherorte 28
10 Betrieb 30
10.1 Normalbetrieb 30
10.2 Abmeldung und Terminalserver 31
10.3 Hängende Uploads und Not-Aus 33
11 Überwachung 33
11.1 Leistungsindikatoren 33
11.2 Ereignisse 34
11.3 Statusfenster und Protokoll 35
12 Datensicherung und Wiederherstellung 36
13 Bekannte Einschränkungen 37

13.1 Bibliotheken ohne Versionierung 37
13.2 Sehr große Ordner 37
14 Fehlersuche 38
15 Deinstallation 39

Auf einen Blick: Das Wichtigste in Kürze

- Zwei MSI-Pakete: das Benutzerpaket für jeden Rechner bzw. Sitzungshost und das Admin-Kit für Administratoren und Systemhäuser.
- Je Benutzersitzung ein Agent im Benutzerkontext; jede Änderung steht zuerst im Journal und wird asynchron über Microsoft Graph hochgeladen.
- Konfiguration über Gruppenrichtlinien bzw. Intune; die Konfigurations-App dient Tests, Pilotbetrieb und Einzelplätzen.
- Journal und ungesendete Inhalte liegen im Benutzerprofil und wandern mit FSLogix mit; Cache und Überlauf liegen auf dem Host.
- Eine fehlende Lizenz sperrt nie das Lesen und nie das Hochladen ungesendeter Inhalte.
- Ergänzend: Richtlinienreferenz, Ereignis- und Fehlerreferenz, Admin-Kit-Handbuch, Benutzerhandbuch.

1 Architektur

CosyTrack.Drive bindet SharePoint-Online- und Teams-Dokumentbibliotheken sowie das OneDrive des Benutzers als echte Windows-Laufwerksbuchstaben ein. Anwendungen arbeiten mit einem normalen Dateipfad und wissen nichts von SharePoint. Die Skizze zeigt die Bausteine auf einem Rechner bzw. Sitzungshost und ihren Weg zu Microsoft 365:

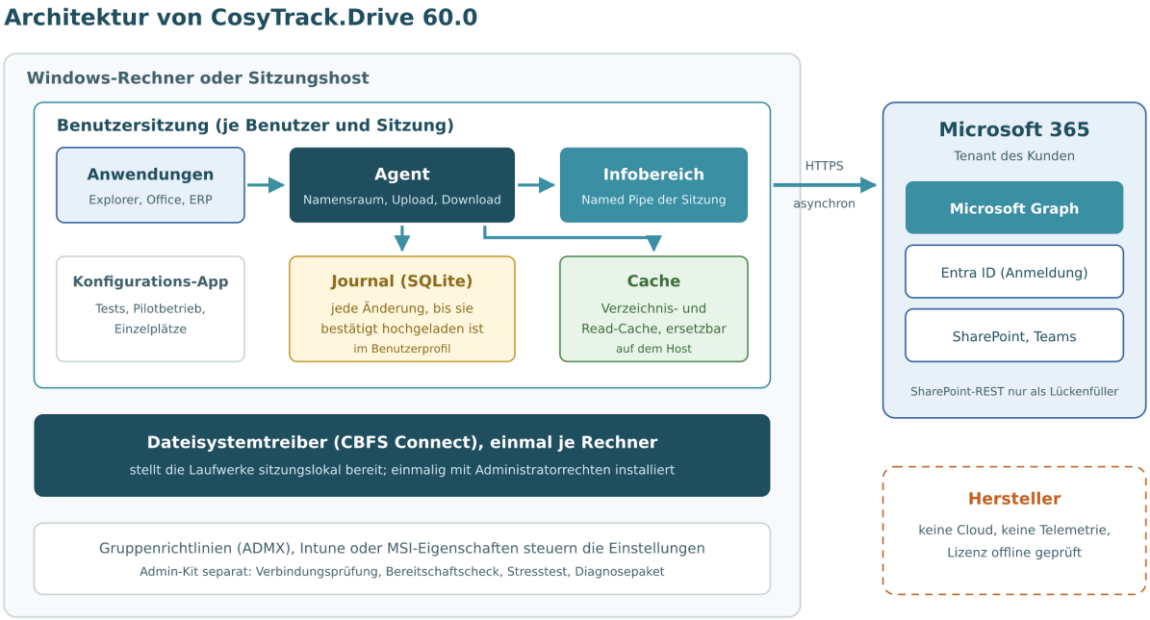

Abbildung 1: Architektur: Treiber, Agent, Journal, Cache und Microsoft Graph

Baustein	Aufgabe
Agent (`CosyTrack.Drive.Agent.exe`)	je Benutzersitzung genau ein Prozess im Benutzerkontext, gestartet bei der Anmeldung (`HKLM\…\Run`); bindet die Laufwerke ein, führt das Journal, lädt hoch und herunter
Infobereich (`CosyTrack.Drive.UI.exe`)	Symbol, Menü, Statusfenster, Protokollfenster, Anmeldung; eigener Prozess, spricht per Named Pipe mit dem Agent; stürzt er ab, bleiben die Laufwerke stehen
Konfigurations-App (`CosyTrack.Drive.Config.exe`)	lokale Konfiguration für Tests, Pilotbetrieb und Einzelplätze; zeigt per Richtlinie festgelegte Werte gesperrt an
Dateisystemtreiber (CBFS Connect)	einmalig mit Administratorrechten installiert; danach binden Benutzer ohne Administratorrechte ein, sitzungslokal
Setup (`CosyTrack.Drive.Setup.exe`)	Treiber, Registrierungen, Lizenzimport, Prüfung vor der Deinstallation; wird vom MSI aufgerufen
Admin-Kit	separates Paket mit Werkzeugen für Systemhäuser (Admin-Kit-Handbuch)

Datenfluss. Jede Dateioperation wirkt sofort auf einen lokalen Namensraum und steht in einem persistenten Journal (SQLite). SharePoint wird ausschließlich asynchron aus dem Journal abgeglichen: Eine Anwendung wartet nie auf SharePoint, und SharePoint sieht nie Zwischenstände eines Speichervorgangs. Journal- und Cache-Einträge sind an Drive-ID und Item-ID gebunden; ein Upload landet nie in einer anderen Bibliothek als der, für die er erfasst wurde.

Microsoft 365. Der Datenpfad läuft über Microsoft Graph (Delta-Abfragen, Download, Upload mit Upload-Sitzungen für große Dateien). SharePoint-REST dient nur als Lückenfüller (Versionierung, Rechte, Website-Suche, Listen). Drosselung: Retry-After wird beachtet, dazu exponentieller Rückzug mit Zufallsanteil und begrenzte Parallelität.

Terminalserver. Laufwerke, Pipe und Agent sind je Sitzung getrennt; jeder Benutzer kann andere Laufwerke haben. Journal und ungesendete Inhalte liegen im Profil (FSLogix-Container) und wandern mit dem Benutzer zum nächsten Host.

So läuft ein einzelner Upload vom Speichern bis zur bestätigten Ankunft in SharePoint:

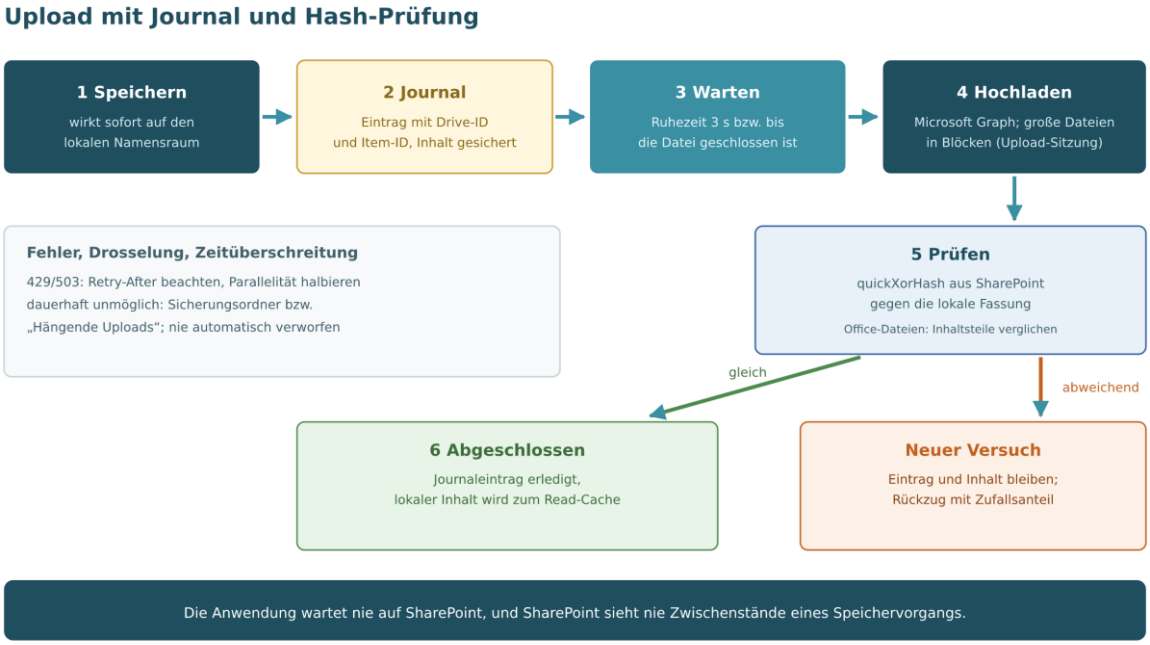

Abbildung 2: Upload-Ablauf mit Journal und Hash-Prüfung

> **Hinweis: Prüfung jedes Uploads**
> Nach jedem Upload vergleicht der Agent den quickXorHash aus SharePoint mit der lokalen Fassung. Bei Office-Dateien im Open-XML-Format schreibt SharePoint Dokumenteigenschaften selbst neu; dann vergleicht der Agent alle Inhaltsteile. Bei den alten Office-Binärformaten (.doc, .xls, .ppt) ist ein Vergleich nicht möglich, der Agent protokolliert das. Bei einer Abweichung bleiben Journaleintrag und Inhalt erhalten, und der Upload wird wiederholt.

2 Voraussetzungen

Bereich	Voraussetzung
Betriebssystem	Windows 10/11 (64 Bit) oder Windows Server 2019/2022/2025, auch mit Remotedesktop-Sitzungshost
.NET	nicht nötig, das Programm bringt seine Laufzeit mit
Rechte	Installation mit Administratorrechten; Betrieb ohne
Microsoft 365	SharePoint Online; App-Registrierung in Microsoft Entra ID (siehe Kapitel 3 „App-Registrierung“)
Netzwerk	HTTPS zu `login.microsoftonline.com`, `graph.microsoft.com` und `<tenant>.sharepoint.com` bzw. `<tenant>-my.sharepoint.com`; keine TLS-Inspektion für diese Ziele
Datenträger	Platz für den Read-Cache (Standard 2 GB je Benutzer) auf einem lokalen NTFS-Datenträger
Virenscanner	Ausnahmen für das Cache-Stammverzeichnis und `%LOCALAPPDATA%\CosyTrack.Drive` empfohlen

> **Praxistipp: Vorher messen statt hinterher suchen**
> Vor dem Kauf misst die Verbindungsprüfung im Admin-Kit Antwortzeiten, Durchsatz und Drosselung am Standort; vor dem Rollout prüft der Bereitschaftscheck den Zielrechner. Beides beschreibt das Admin-Kit-Handbuch.

3 App-Registrierung

CosyTrack.Drive meldet sich mit dem Konto des Benutzers über eine eigene App-Registrierung an: öffentlicher Client, nur delegierte Berechtigungen, kein Client-Geheimnis und kein Zertifikat.

Ressource	Berechtigung (delegiert)	Zweck
Microsoft Graph	User.Read, offline_access	Anmeldung, Aktualisierungstoken
Microsoft Graph	Files.ReadWrite.All	Dateien lesen und schreiben
Microsoft Graph	Sites.ReadWrite.All	Websites und Bibliotheken auflisten
Microsoft Graph	Team.ReadBasic.All, Channel.ReadBasic.All	Teams-Automatik
SharePoint	AllSites.Write	Versionierung der Bibliotheken lesen

> **Hinweis: Keine zusätzlichen Rechte für Benutzer**
> Die Benutzer sehen nur, was sie in SharePoint ohnehin sehen dürfen. Alle Berechtigungen sind delegiert; Anwendungsberechtigungen mit Zugriff auf den ganzen Tenant gibt es nicht.

> **Achtung: Keine Protokollrechte in dieser App-Registrierung**
> `AuditLog.Read.All` und `Directory.Read.All` gehören nie in die App-Registrierung von CosyTrack.Drive, sondern nur in die eigene App-Registrierung des Admin-Kits für die Lizenznutzung (Kapitel „Lizenznutzung (Admin-Kit)“). Der Bereitschaftscheck mit Anmeldung meldet GELB („Keine Protokollrechte in der App von CosyTrack.Drive“), wenn die App-Registrierung von CosyTrack.Drive `AuditLog.Read.All` oder `Directory.Read.All` enthält, erteilt oder nur eingetragen, delegiert oder als Anwendungsberechtigung. Diese Rechte gehören in die eigene App-Registrierung des Admin-Kits. Entfernen: Entra Admin Center › App-Registrierungen › App von CosyTrack.Drive › API-Berechtigungen › bei der Berechtigung „…“ › „Berechtigung entfernen“; eine bereits erteilte Zustimmung zusätzlich unter Unternehmensanwendungen › App von CosyTrack.Drive › Berechtigungen prüfen bzw. widerrufen. Das ist nur ein Hinweis, CosyTrack.Drive sperrt deswegen nichts.

Anlegen: `tools\New-CosyTrackDriveAppRegistration.ps1` legt die Registrierung an, trägt die Umleitungs-URI `http://localhost` (Mobile und Desktopanwendungen) ein, erlaubt öffentliche Clientflows und erteilt die Administratorzustimmung. Von Hand: App-Registrierung „CosyTrack.Drive“, Konten nur in diesem Verzeichnis, Plattform „Mobile und Desktopanwendungen“ mit `http://localhost`, „Öffentliche Clientflows zulassen“, die Berechtigungen oben hinzufügen und „Administratorzustimmung erteilen“. Notieren Sie Anwendungs-ID (Client-ID) und Verzeichnis-ID (Tenant-ID).

In der Konfigurations-App prüft die Seite „Verbindung und Anmeldung“, ob die Registrierung vollständig ist und welche Berechtigungen erteilt sind:

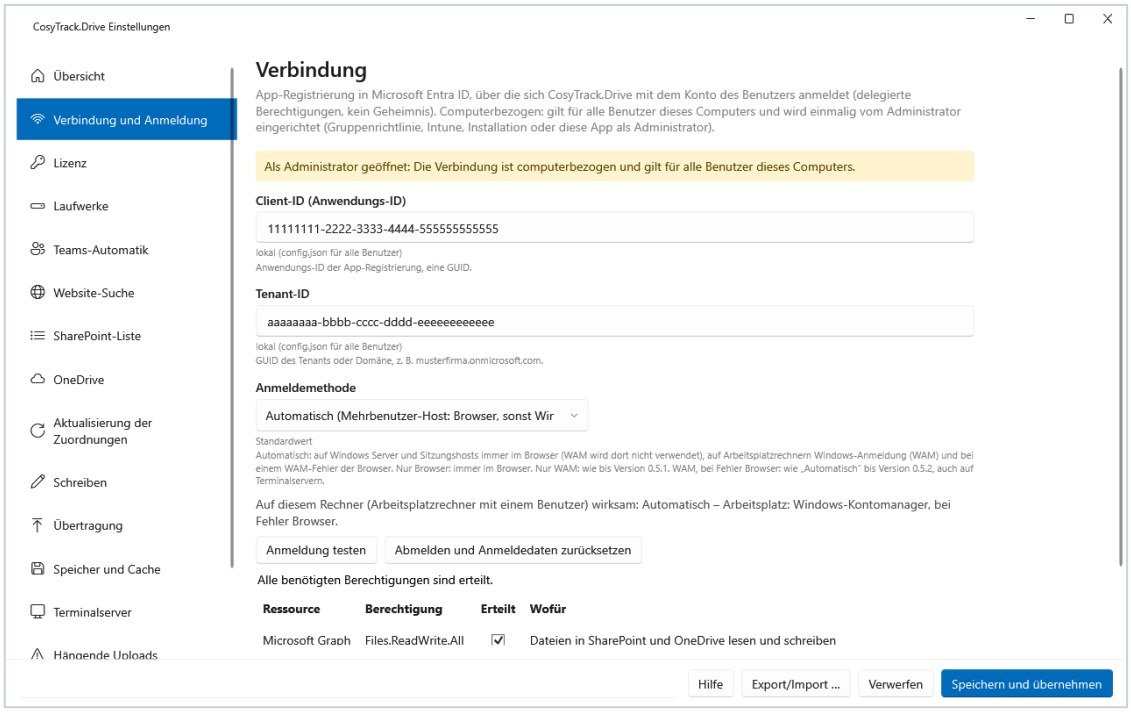

Abbildung 3: Konfigurations-App, Seite „Verbindung und Anmeldung“

3.1 Anmeldung der Benutzer

Auf Arbeitsplatzrechnern in Entra ID meldet sich der Agent still über das Windows-Konto an (Windows-Kontomanager). Auf Windows Server und Hosts mit mehreren Sitzungen meldet sich der Benutzer einmalig im Browser an, danach still über den gespeicherten Token-Cache. Richtlinien für bedingten Zugriff gelten wie für jede Microsoft-365-Anwendung. Die Skizze zeigt, wie der Agent die Anmeldemethode wählt:

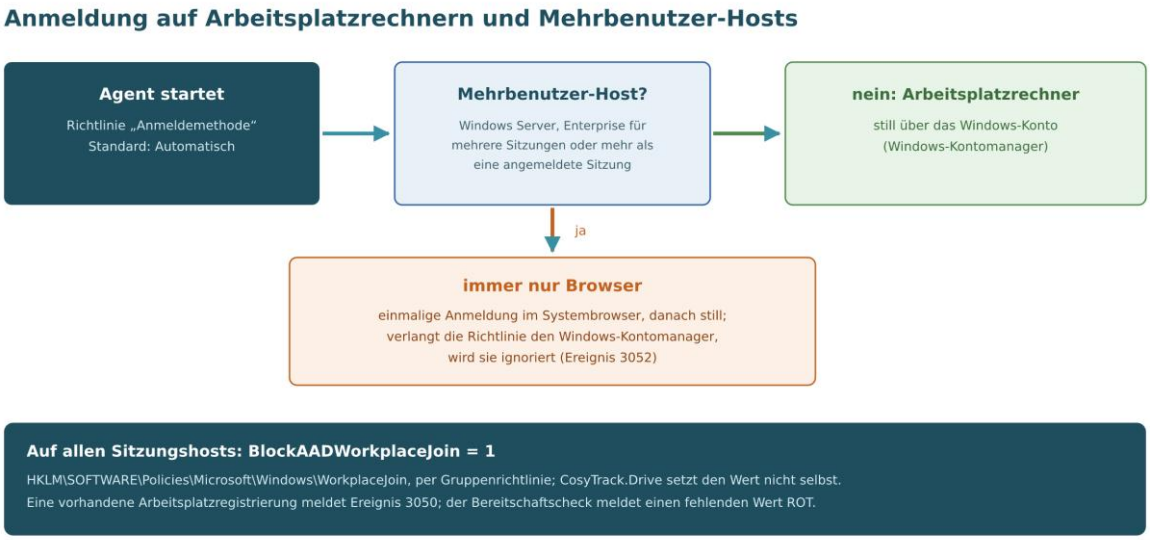

Abbildung 4: Anmeldung auf Arbeitsplatzrechnern und Mehrbenutzer-Hosts

Auf einem Terminalserver sieht der Benutzer beim ersten Start diese Benachrichtigung:



Abbildung 5: Hinweis zur Anmeldung im Browser auf dem Terminalserver (Nachbildung)

> **Achtung: Arbeitsplatzregistrierung auf Sitzungshosts verhindern**
> Auf Terminalservern immer `BlockAADWorkplaceJoin = 1` setzen (`HKLM\SOFTWARE\Policies\Microsoft\Windows\WorkplaceJoin`), damit bei der Anmeldung keine Arbeitsplatzregistrierung entsteht. CosyTrack.Drive setzt den Wert nicht selbst. Der Bereitschaftscheck meldet einen fehlenden Wert ROT; die Vorlage „Terminalserver“ des Admin-Kits setzt ihn.

4 Installation

4.1 Pakete

Paket	Inhalt	Programmordner
`CosyTrack.Drive-60.0.0.0-x64.msi`	Agent, Infobereich, Konfigurations-App, Treiber, Ereignisprotokoll, Leistungsindikatoren, Richtlinienvorlagen	`%ProgramFiles%\CosyTrack.Drive`
`CosyTrack.Drive.AdminKit-60.0.0.0-x64.msi`	Admin-Kit (Kacheln und `ctd-admin`)	`%ProgramFiles%\CosyTrack.Drive AdminKit`

Beide Pakete installieren pro Computer (x64), brauchen Administratorrechte und sind signiert. Eine neue Version löst die alte selbst ab. Die Oberfläche folgt der Anzeigesprache von Windows (deutsch bzw. englisch). Die Skizze zeigt den Ablauf von Installation, Update und Deinstallation:

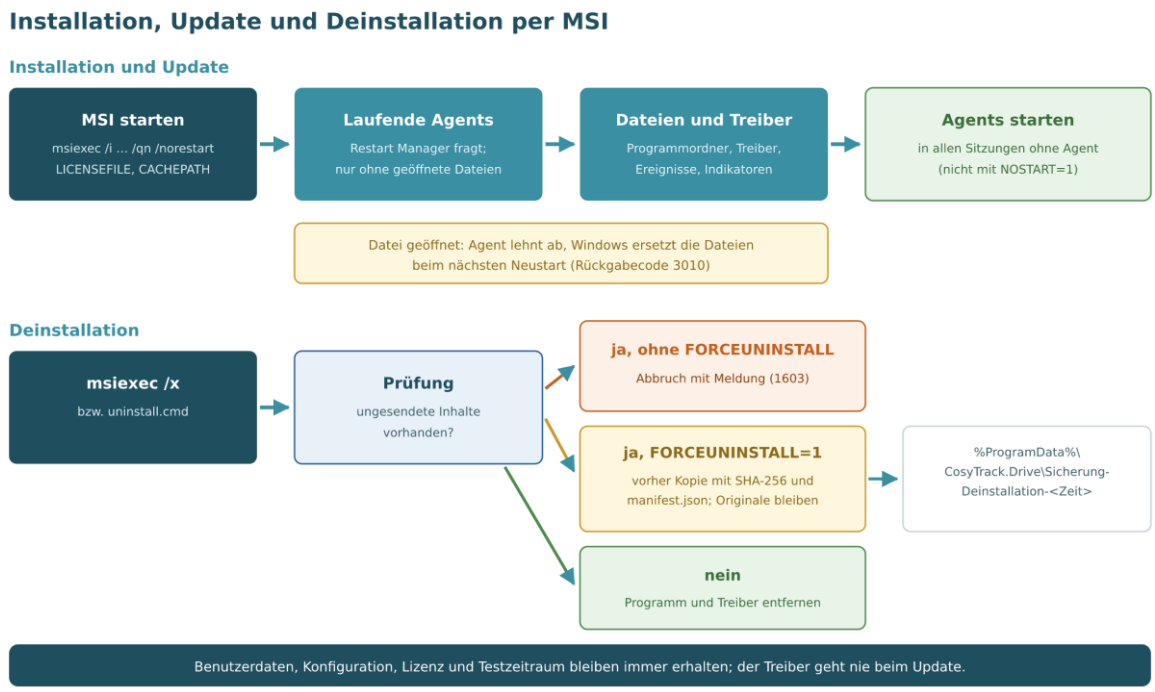

Abbildung 6: Installation und Update per MSI mit FORCEUNINSTALL und Sicherung ungesendeter Inhalte

Bei einer Installation mit Oberfläche zeigt das MSI zuerst die Lizenzbedingungen:



Abbildung 7: Lizenzbedingungen im MSI (Nachbildung)

Vor dem Schritt prüfen: Vor der Installation

- App-Registrierung angelegt, Client-ID und Tenant-ID notiert (Kapitel 3 „App-Registrierung“); sie kommen bei der Installation (`CLIENTID`, `TENANTID`) oder per Richtlinie auf den Rechner, nie durch die Benutzer.
- Lizenzdatei bzw. Lizenzschlüssel liegt vor; für den Testzeitraum ist nichts nötig.
- Cache-Stammverzeichnis festgelegt, auf einem lokalen NTFS-Datenträger.
- Auf Terminalservern: `BlockAADWorkplaceJoin = 1` und FSLogix-Ausschlüsse geprüft.
- Bereitschaftscheck des Admin-Kits auf einem Rechner je Host-Typ ohne roten Punkt.

4.2 Befehle

Zweck	Befehl
Mit Oberfläche	Doppelklick auf das MSI bzw. `install.cmd`
Still	`msiexec /i CosyTrack.Drive-60.0.0.0-x64.msi /qn /norestart /l*v "%ProgramData%\CosyTrack.Drive\Setup\msi-install.log"` bzw. `install.cmd /quiet`
Mit Lizenz und Cache-Ort	`install.cmd /quiet LICENSEFILE="\\server\netlogon\cosytrack.ubl" CACHEPATH="D:\CosyTrackCache"`
Mit Verbindung	`install.cmd /quiet CLIENTID=11111111-2222-3333-4444-555555555555 TENANTID=aaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeeee`
Nur prüfen	`install.cmd /check` (Signatur, 64 Bit; ändert nichts)
Reparieren	Programme und Features › CosyTrack.Drive › Reparieren bzw. `msiexec /fa …msi /qn`

Eine stille Installation mit Protokoll sieht so aus:

```
msiexec /i CosyTrack.Drive-60.0.0.0-x64.msi /qn /norestart
LICENSEFILE="\\server\netlogon\cosytrack.ubl" /l*v
"%ProgramData%\CosyTrack.Drive\Setup\msi-install.log"
```

> **Achtung: Bei stiller Installation immer /norestart**
> Ohne `/norestart` kann Windows Installer den Computer selbst neu starten, auch auf einem Terminalserver mit angemeldeten Benutzern. Der Rückgabecode 3010 bedeutet: erfolgreich, Neustart erforderlich (neuer Treiber).

4.3 Öffentliche Eigenschaften

Eigenschaft	Wirkung
`LICENSEFILE`	Lizenzdatei (.ubl, auch UNC); wird geprüft und für alle Benutzer gespeichert. Ein ungültiger Schlüssel bricht die Installation nicht ab.
`LICENSEKEY`	der Lizenzschlüssel selbst; verborgen, nicht im MSI-Protokoll
`CACHEPATH`	Cache-Stammverzeichnis als Wert der Installation (nur lokales NTFS; die Gruppenrichtlinie hat Vorrang)
`CLIENTID`, `TENANTID`	Verbindung zu Microsoft 365: Client-ID der App-Registrierung und Tenant-ID, beide als GUID und nur gemeinsam. Sie landen in der computerbezogenen Konfiguration `%ProgramData%\CosyTrack.Drive\config.json`; setzt eine Gruppenrichtlinie den Wert, hat sie Vorrang. Ungültige Angaben brechen die Installation vor jeder Änderung ab.
`ADDLOCAL`	Funktionen `Main`, `Config` (Konfigurations-App), `PolicyDefinitions`; Standard alle, z. B. `ADDLOCAL=Main,PolicyDefinitions` ohne Konfigurations-App
`NOSTART=1`	Agents nach der Installation nicht starten (sie starten bei der nächsten Anmeldung)
`FORCEUNINSTALL=1`	nur bei der Deinstallation: trotz ungesendeter Inhalte deinstallieren, vorher sichern

Ohne `NOSTART` startet das MSI den Agent in allen angemeldeten Sitzungen, in denen noch keiner läuft, mit den Rechten des jeweiligen Benutzers.

4.4 Reihenfolge auf Terminalservern

Die Verbindung zu Microsoft 365 (Client-ID und Tenant-ID) ist computerbezogen und gilt für alle Benutzer des Hosts. Benutzer können sie ohne Administratorrechte nicht einrichten; fehlt sie, zeigen Infobereich und Konfigurations-App „Verbindung fehlt“, und es erscheinen keine Laufwerke. Halten Sie deshalb auf Terminalservern diese Reihenfolge ein:

1. **Installation** mit Administratorrechten, mit `CLIENTID` und `TENANTID` oder anschließend per Gruppenrichtlinie „Anmeldung: App-Registrierung“ bzw. Intune.
2. **Verbindung prüfen:** Bereitschaftscheck des Admin-Kits auf dem Host; der Punkt „Verbindung zu Microsoft 365“ muss GRÜN sein.
3. **Erst dann Benutzer anmelden lassen.**

Eine stille Installation mit Verbindung sieht so aus (Beispielwerte):

```
msiexec /i CosyTrack.Drive-60.0.0.0-x64.msi /qn /norestart CLIENTID=11111111-2222-3333-
4444-555555555555 TENANTID=aaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeeee /l*v
"%ProgramData%\CosyTrack.Drive\Setup\msi-install.log"
```

Wird die Verbindung erst nach der Anmeldung der Benutzer gesetzt, übernimmt der Agent sie innerhalb einer Minute von selbst; eine neue Anmeldung ist nicht nötig. Benutzereinstellungen, die bis dahin gespeichert wurden (Laufwerke, Teams-Automatik, OneDrive), bleiben erhalten und werden dann wirksam.

4.5 Verteilung per Gruppenrichtlinie

1. MSI auf eine Freigabe legen, die die Computerkonten lesen dürfen.

2. Computerkonfiguration › Richtlinien › Softwareeinstellungen › Softwareinstallation › Neu › Paket › „Zugewiesen“.
3. Lizenz per Richtlinie „Lizenz“ und Cache-Ort per Richtlinie „Cache-Stammverzeichnis“ verteilen (Eigenschaften lassen sich bei der Softwareinstallation nicht direkt angeben; alternativ eine Transformation).
4. Updates: neues Paket hinzufügen, unter „Aktualisierungen“ das alte Paket mit „Paket kann darüber aktualisiert werden“ angeben.

4.6 Verteilung mit SCCM/MECM

Anwendung vom Typ Windows Installer, Installationsprogramm `msiexec /i "CosyTrack.Drive-60.0.0.0-x64.msi" /qn /norestart`, Erkennung über den Produktcode, Rückgabecode 3010 als Soft Reboot.

4.7 Verteilung mit Intune

Win32-App mit dem MSI als Setup-Datei, Erkennung per MSI-Produktcode. Das Admin-Kit erstellt das Paket („Vorlagen“ › „Intune-Paket erstellen“ bzw. `ctd-admin intune-paket`) samt Erkennungsskript, Musterprofilen, Remediations und Compliance-Regel. Die ADMX lässt sich in Intune importieren (Geräte › Konfiguration › Importierte administrative Vorlagen).

Einstellung	Wert
Installationsbefehl	`msiexec /i "CosyTrack.Drive-60.0.0.0-x64.msi" /qn /norestart` (optional `LICENSEFILE=…`)
Deinstallationsbefehl	`msiexec /x {ProductCode} /qn /norestart`
Rückgabecodes	0 Erfolg, 3010 Soft Reboot, 1641 Hard Reboot, 1618 Wiederholen, 1603 Fehler
Erkennung	MSI-Produktcode
Ablösung	bisherige App ablösen, **ohne** „Vorherige Version deinstallieren“

> **Achtung: Bei der Ablösung nicht vorher deinstallieren**
> Mit „Vorherige Version deinstallieren“ entfernt Intune die alte Version vor der neuen. Bei ungesendeten Inhalten bricht diese Deinstallation ab (1603), und das Update scheitert. Das MSI löst die alte Version selbst ab.

5 Update

- Ein neues MSI installiert man einfach darüber; Benutzerdaten, Konfiguration und Lizenz bleiben erhalten.
- **Update von einer Vorabversion (0.5.2 bis 0.7.0):** Das MSI übernimmt die frühere Installation an Ort und Stelle, aber nur, wenn CosyTrack.Drive in keiner Sitzung mehr läuft. Deshalb vorher alles hochladen lassen, alle Benutzer abmelden (auch getrennte Sitzungen) und über die Softwareverteilung oder per Remote-PowerShell installieren, nicht aus einer angemeldeten Sitzung auf demselben Rechner.

- **Ältere Vorabversionen (0.3.x, 0.5.0, 0.5.1, 0.5.1a):** kein direktes Update. Alles hochladen lassen, die alte Version mit ihrem `uninstall.cmd` deinstallieren, danach 60.0 neu installieren.
- In beiden Fällen bricht das MSI sonst ab, bevor es etwas ändert, und nennt den Grund; still endet es mit 1603. Den genauen Ablauf für Terminalserver und Einzelplätze beschreibt die Update-Anleitung für 60.0.
- **Laufende Agents:** Windows Installer fragt über den Restart Manager, ob Agent, Infobereich und Konfigurations-App beendet werden dürfen. Ist auf den Laufwerken einer Sitzung keine Datei geöffnet, beendet sich der Agent wie bei der Abmeldung (was in der Frist hochladbar ist, wird hochgeladen) und startet nach dem Update wieder. Ist eine Datei geöffnet, lehnt der Agent ab; Windows ersetzt die Dateien beim nächsten Neustart (3010).

Bei einem Update mit Oberfläche meldet Windows Installer laufende Programme so:

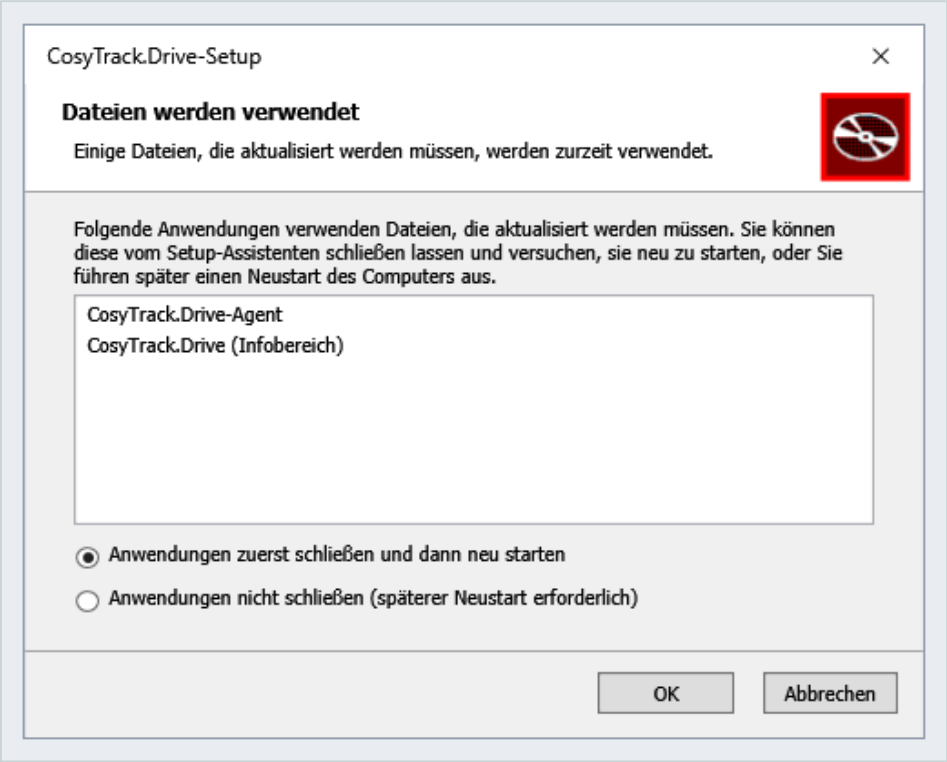

Abbildung 8: Dateien werden verwendet, Update bei laufendem Agent (Nachbildung)

> **Praxistipp: Updates im Wartungsfenster**
> Auf Terminalservern Updates im Wartungsfenster einspielen und danach neu starten, damit Agents mit geöffneten Dateien sicher auf die neue Version wechseln.

6 Konfiguration

6.1 Vorrang

Einstellungen kommen aus bis zu vier Quellen; die höhere gewinnt immer:

1. Gruppenrichtlinie (`HKLM\SOFTWARE\Policies\boddenberg\CosyTrack.Drive` bzw. `HKCU\…`). Bei Teams-Automatik, Website-Suche und OneDrive gilt die Computerrichtlinie als Standard, die

Benutzerrichtlinie überschreibt je Einstellung. Laufwerkszuordnungen und SharePoint-Listen gibt es nur als Benutzerrichtlinie.

2. Werte der Installation (`HKLM\SOFTWARE\boddenberg\CosyTrack.Drive`, z. B. aus `CACHEPATH`).
3. Lokale Konfiguration: `%ProgramData%\CosyTrack.Drive\config.json` (Computer) und `%APPDATA%\CosyTrack.Drive\config.json` (Benutzer).
4. Standardwerte.

Die Richtlinienreferenz zeigt den Vorrang als Skizze und beschreibt jede Richtlinie einzeln.

6.2 Gruppenrichtlinien

ADMX und ADML (deutsch, englisch) liegen im Paket unter `PolicyDefinitions` und nach der Installation in `%ProgramFiles%\CosyTrack.Drive\PolicyDefinitions`. In den Central Store kopieren: `\\<Domäne>\SYSVOL\<Domäne>\Policies\PolicyDefinitions`. Die Vorlage hat 66 Richtlinien in den Kategorien Allgemein, Laufwerke, Teams-Automatik, OneDrive, Website-Suche, SharePoint-Listen, Cache, Schreiben, Übertragung, Aktualisierung der Zuordnungen, Leistungsmessung, Protokoll und „Admin-Kit: Lizenznutzung“ (nur für das Admin-Kit). Jede Richtlinie mit Registry-Wert, Standard und Grenzen beschreibt die Richtlinienreferenz.

Die wichtigsten Richtlinien für den Einstieg:

Richtlinie	Wofür
Allgemein › App-Registrierung (Client-ID und Tenant-ID)	Pflicht
Allgemein › Lizenz	Lizenzschlüssel bzw. Lizenzdatei
Laufwerke › Laufwerksplatz 1 bis 10 (Benutzer)	feste Zuordnungen mit Buchstabe, URL, Anzeigename, Zugriffsmodus
Teams-Automatik	ein Laufwerk mit einem Ordner je Team
Cache › Cache-Stammverzeichnis	Ort der Host-Daten, nur lokales NTFS
Schreiben › Ablage ungesendeter Inhalte	Profil mit Überlauf (Standard) oder nur lokal

Im Gruppenrichtlinien-Editor erscheinen die Richtlinien unter Administrative Vorlagen › CosyTrack.Drive.

> **Praxistipp: Erst lokal erproben, dann als Richtlinie verteilen**
> Richten Sie im Pilotbetrieb einen Rechner mit der Konfigurations-App ein. „Export/Import …“ erzeugt daraus eine `.reg`-Datei bzw. eine Liste der Gruppenrichtlinien, die Sie für den Rollout übernehmen.

6.3 Konfigurations-App

Die Konfigurations-App („CosyTrack.Drive – Einstellungen“) ist für Tests, Pilotbetrieb und Einzelplätze gedacht. Sie zeigt jede Einstellung mit Herkunft; per Richtlinie oder Installation festgelegte Werte sind gesperrt („Von der Organisation festgelegt“). Benutzerbezogene Einstellungen (Laufwerke, Teams-Automatik, OneDrive) speichert jeder Benutzer ohne Administratorrechte. Computerbezogene Einstellungen, darunter die Verbindung, sind ohne

Administratorrechte nur lesbar; die App fragt dafür nie nach Administratorrechten. Zum Ändern öffnet ein Administrator die App über „Als Administrator bearbeiten …“ auf der Seite „Verbindung“ bzw. startet sie als Administrator.

Die Seite „Übersicht“ zeigt, welche Laufwerke der Benutzer wirklich bekommt und warum, berechnet mit demselben Code wie im Agent:

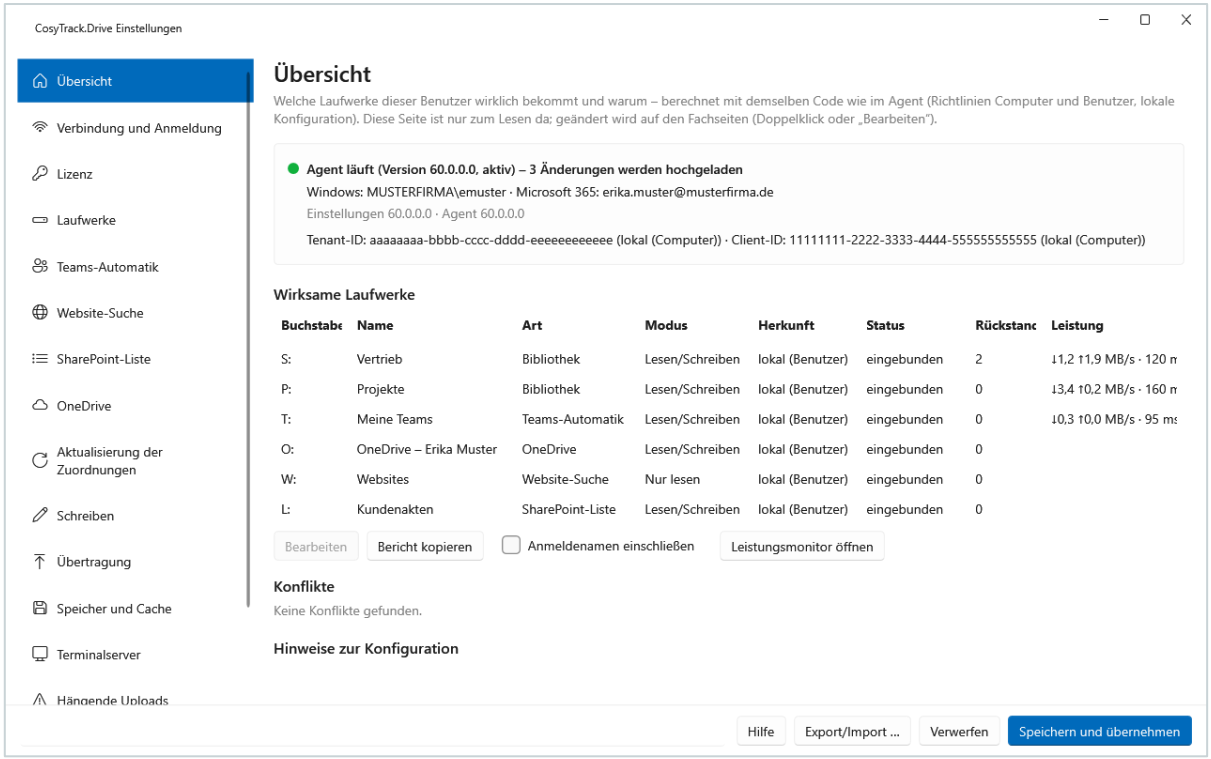

Abbildung 9: Konfigurations-App, Übersicht

Feste Zuordnungen legen Sie auf der Seite „Laufwerke“ an:

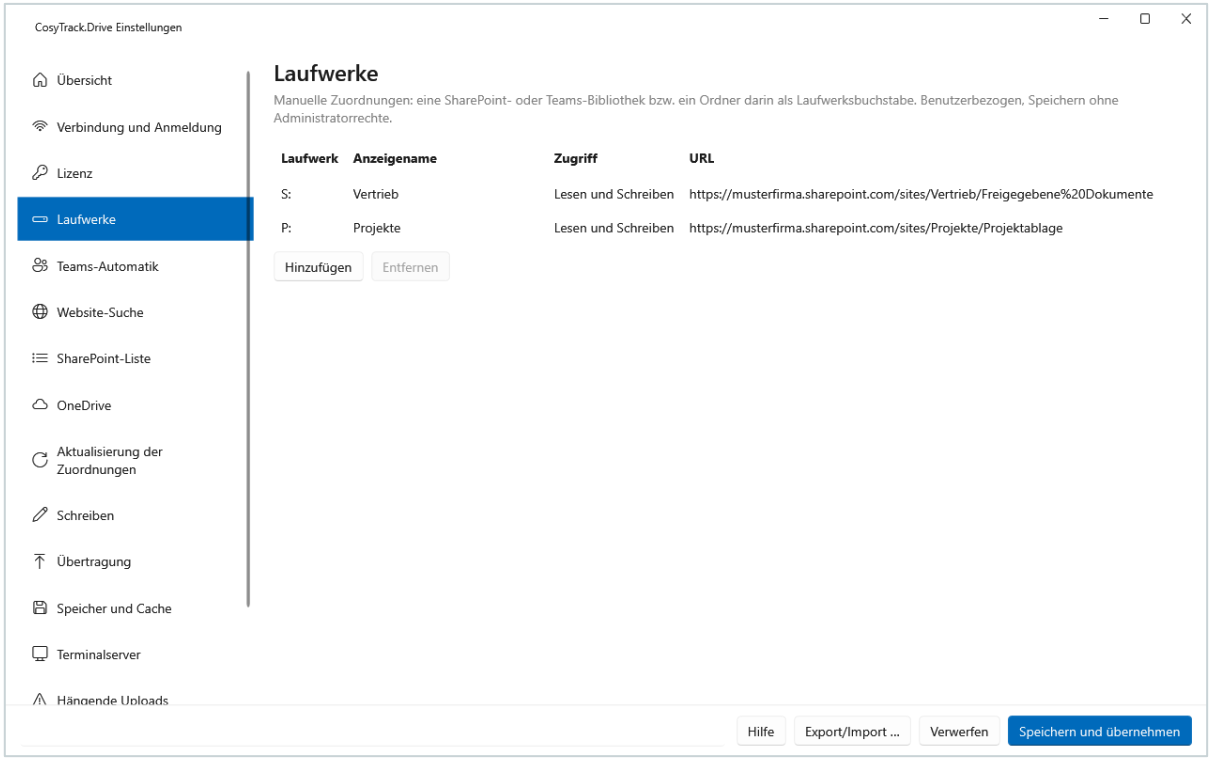

Abbildung 10: Konfigurations-App, Seite „Laufwerke“

Die Teams-Automatik zeigt vor dem Speichern eine Vorschau der Teams, die eingebunden würden:

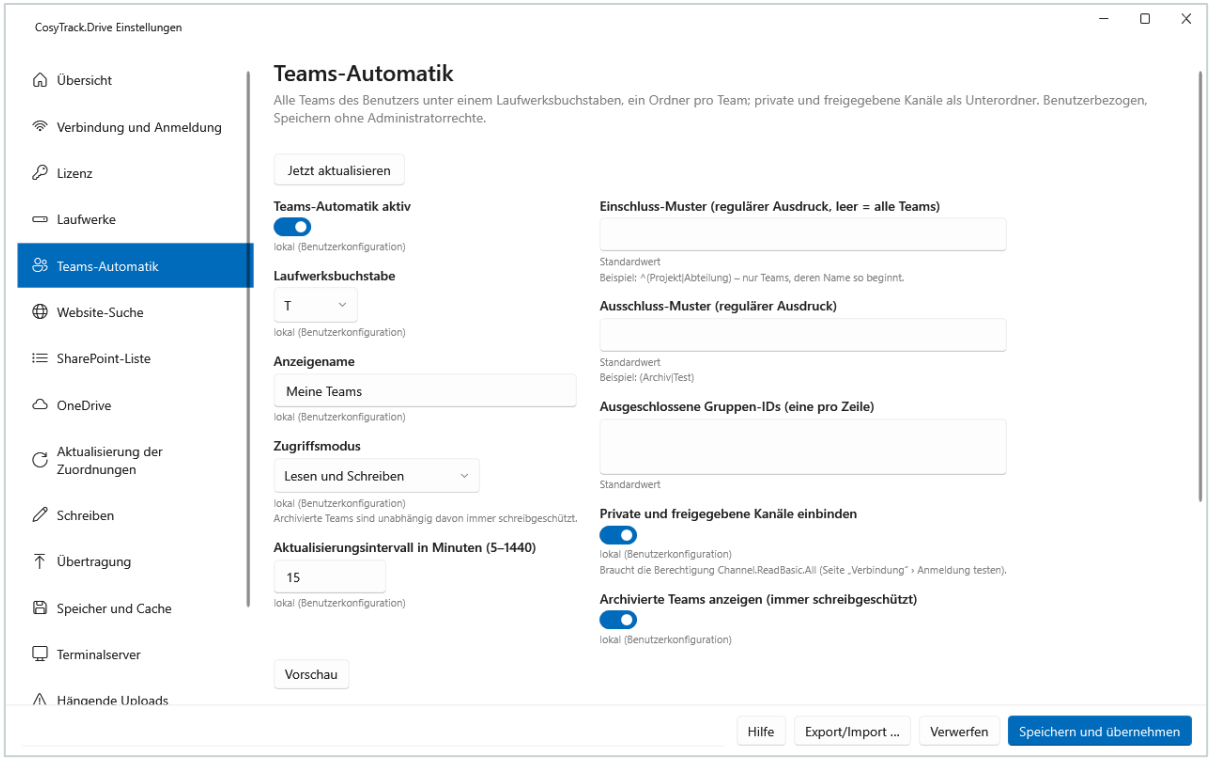

Abbildung 11: Konfigurations-App, Seite „Teams-Automatik“

Per Gruppenrichtlinie festgelegte Werte sind gesperrt und mit ihrer Herkunft gekennzeichnet:

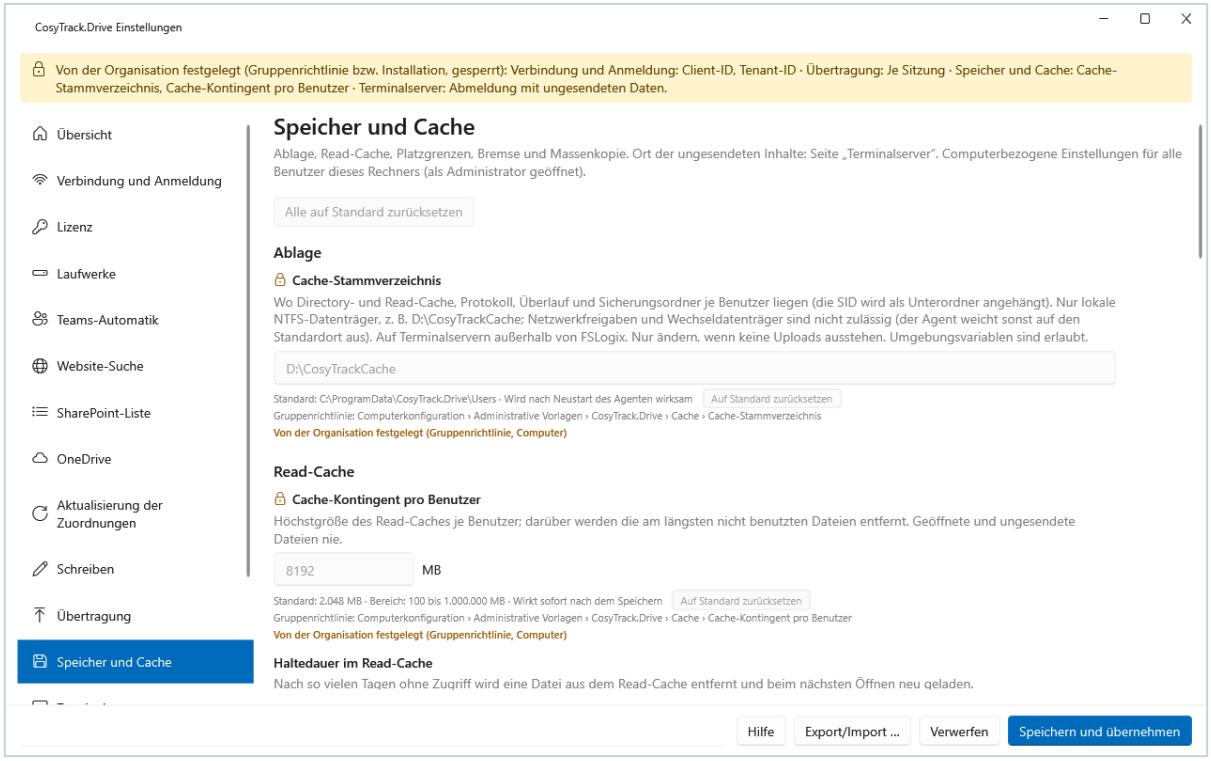

Abbildung 12: Konfigurations-App, per Gruppenrichtlinie festgelegte Werte

Beim ersten Start ohne Konfiguration führt ein Assistent durch Verbindung und erstes Laufwerk:

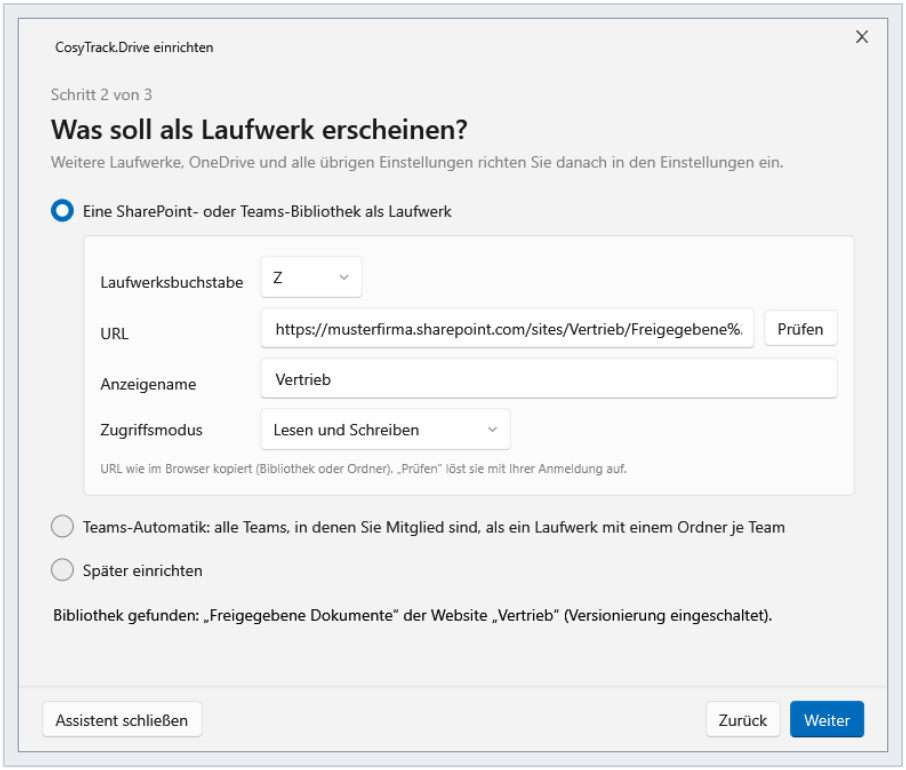

Abbildung 13: Ersteinrichtungs-Assistent, erstes Laufwerk

Startet ein Benutzer ohne Administratorrechte den Assistenten, bevor die Verbindung eingerichtet ist, zeigt der erste Schritt die Felder nur lesbar und einen Hinweis an die IT. Laufwerk bzw. Teams-Automatik speichert der Assistent trotzdem; sie werden wirksam, sobald die Verbindung gesetzt ist:

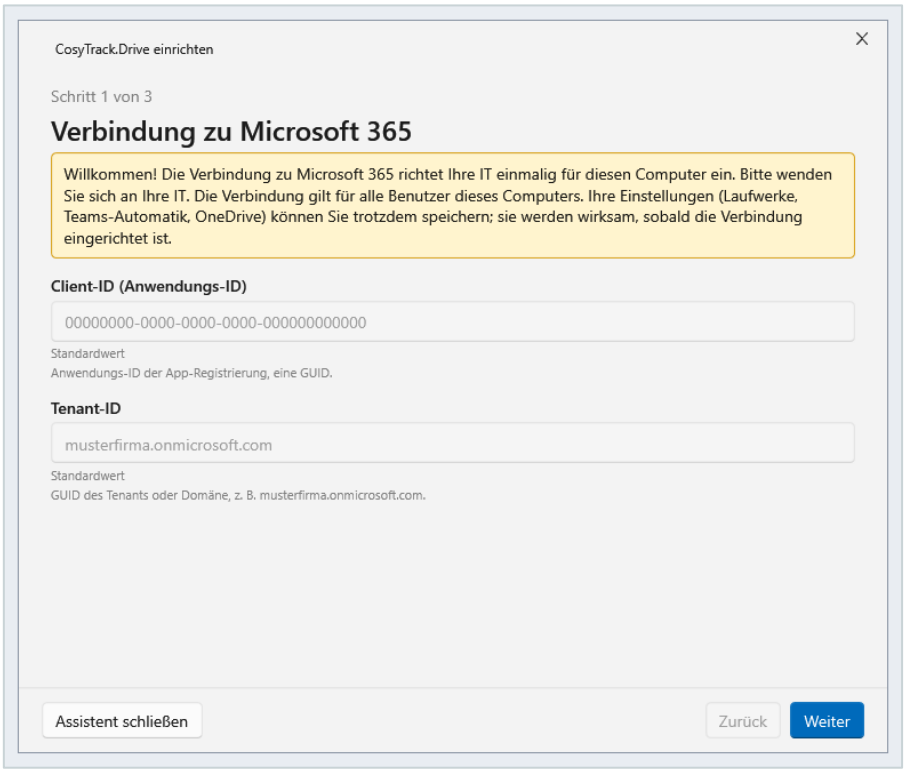

Abbildung 14: Ersteinrichtungs-Assistent ohne Administratorrechte, Verbindung fehlt

> **Hinweis: Die Konfigurations-App ersetzt keine Richtlinie**
> Sobald eine Richtlinie einen Wert setzt, gilt sie; die lokale Einstellung bleibt wirkungslos. Für den Betrieb vieler Rechner sind Gruppenrichtlinien bzw. Intune vorgesehen.

7 Lizenzierung

CosyTrack.Drive wird je Benutzer lizenziert (Named User, gebunden an die Tenant-IDs des Kunden). Die Prüfung erfolgt offline anhand der Signatur; CosyTrack.Drive nimmt dafür keinen Kontakt zum Hersteller auf. Die Skizze zeigt die Zustände und was in jedem Zustand möglich bleibt:

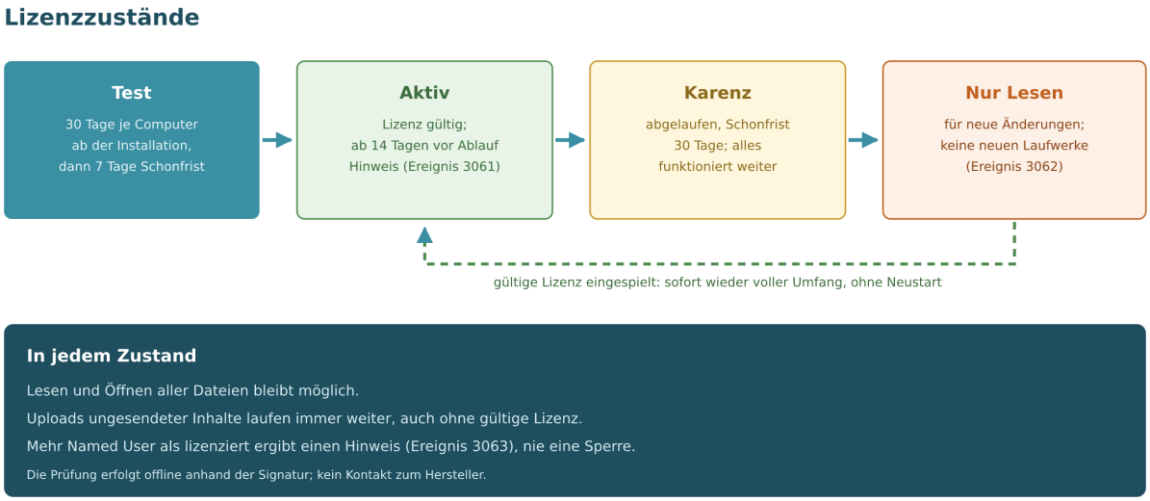

Abbildung 15: Lizenzzustände: Test, aktiv, Karenz, nur Lesen für neue Änderungen

Zustand	Neue Laufwerke	Neue Änderungen
Testzeitraum (30 Tage je Computer ab der Installation)	ja	ja
Schonfrist nach dem Testzeitraum (7 Tage, täglicher Hinweis)	ja	ja
Lizenz gültig	ja	ja
läuft bald ab (ab 14 Tagen vorher, Ereignis 3061, Bereitschafts-check GELB)	ja	ja
abgelaufen, Schonfrist (30 Tage)	ja	ja
nach dem Ende der Schonfrist ohne gültige Lizenz	nein	**nein**, nur lesen

> **Rechtlicher Hinweis: Was eine fehlende Lizenz nie sperrt**
> Eine fehlende oder abgelaufene Lizenz sperrt nie den Zugriff auf Daten und verhindert nie das Hochladen bereits gespeicherter Änderungen. Nach dem Einspielen einer gültigen Lizenz gilt sofort wieder der volle Funktionsumfang, ohne Neustart.

Die Lizenzdatei legt Edition und Zusatzfunktionen fest; unbekannte Angaben aus neueren Lizenzen werden ignoriert.

Verteilung: Richtlinie „Lizenz“ (Schlüssel oder Pfad zur `.ubl`-Datei), MSI-Eigenschaft `LICENSEFILE`, Konfigurations-App (Seite „Lizenz“, „Für alle Benutzer speichern“) oder `ctd-admin lizenz --import`. Die Seite „Lizenz“ der Konfigurations-App zeigt den Zustand ohne den Schlüssel:

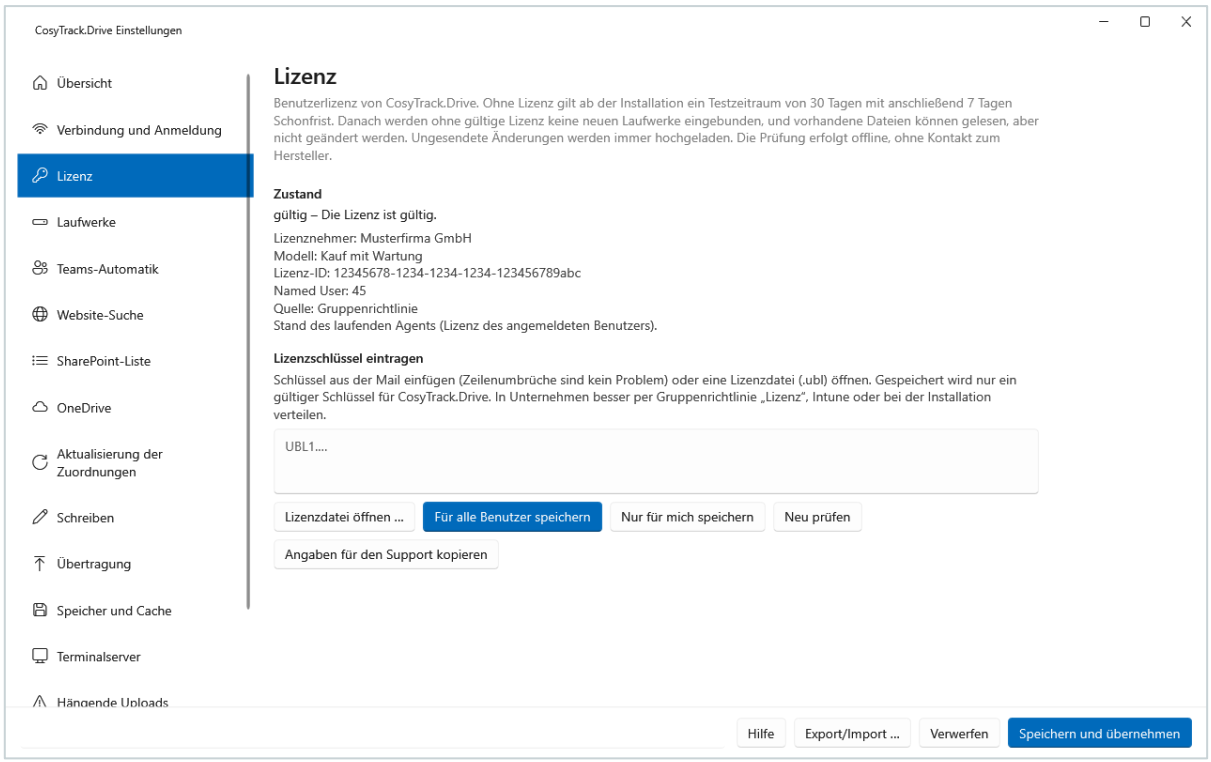

Abbildung 16: Konfigurations-App, Seite „Lizenz“ mit gültiger Lizenz

Nach dem Ende von Testzeitraum und Schonfrist sieht dieselbe Seite so aus:

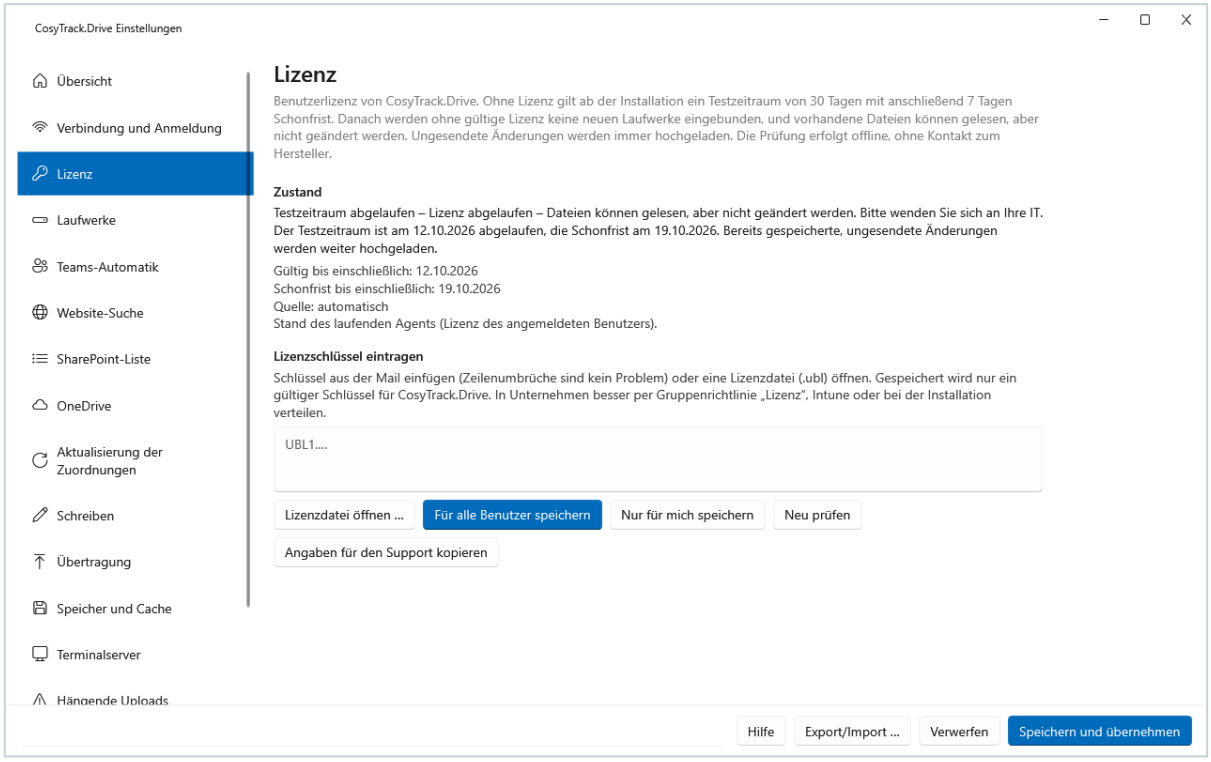

Abbildung 17: Konfigurations-App, Seite „Lizenz“ nach Ablauf, nur lesen

Named User zählen: Admin-Kit, Kachel „Lizenz und Lizenznutzung“ (nächstes Kapitel), als Orientierungswert und Untergrenze. Liegt die Zahl über der Lizenz, gibt es einen Hinweis (Ereignis 3063, Bereitschaftscheck GELB), nie eine Sperre.

8 Lizenznutzung (Admin-Kit)

> **Hinweis: Orientierungswert, kein Ersatz für die Verwaltung der Named User**
> Diese Zahl ist ein Orientierungswert und eine Untergrenze. Erfasst werden nur Benutzer, die sich im gewählten Zeitraum an CosyTrack.Drive angemeldet haben. Named User, die in dieser Zeit abwesend waren, etwa wegen Urlaub, Elternzeit, Krankheit oder Projektpause, fehlen in der Zählung. Die Auswertung ersetzt keine saubere Verwaltung der Named User. Maßgeblich für die Lizenzierung sind alle Personen, die CosyTrack.Drive gemäß den Lizenzbedingungen nutzen dürfen.

> **Rechtlicher Hinweis: Mitbestimmungspflichtig – vor dem Einsatz klären!**
> Dieses Werkzeug wertet Anmeldedaten von Mitarbeiterinnen und Mitarbeitern aus den Entra-Anmeldeprotokollen aus. Auch wenn im Standard nur eine Anzahl angezeigt wird, ist es eine technische Einrichtung, die objektiv geeignet ist, Verhalten oder Leistung zu überwachen (§ 87 Abs. 1 Nr. 6 BetrVG; im öffentlichen Dienst entsprechende Regelungen des Personalvertretungsrechts). Setzen Sie es erst ein, wenn Betriebsrat oder Personalrat beteiligt und der Datenschutzbeauftragte eingebunden ist. Hinweis, keine Rechtsberatung.

Zweck: ein schneller Orientierungswert für das True-up. Das Werkzeug liefert im Kern eine Zahl, etwa „Mindestens 97 aktive Benutzer in den letzten 90 Tagen“ (eindeutige Benutzer mit erfolgreicher Anmeldung an CosyTrack.Drive im Zeitraum), daneben die lizenzierte Anzahl. Keine Diagramme, keine Detailauswertungen, keine Geräte- oder Zeitverläufe je Benutzer.

Gezählte App: die Client-ID von CosyTrack.Drive, ermittelt wie von CosyTrack.Drive selbst (Richtlinie „App-Registrierung“, sonst Installation bzw. `config.json`); im Werkzeug überschreibbar. Abgefragt wird über eine **eigene App-Registrierung des Admin-Kits**; die App-Registrierung von CosyTrack.Drive bekommt keine Protokollberechtigungen.

Vergleich mit der Lizenz: Liegt die Zahl über der lizenzierten Anzahl, erscheint in Warnfarbe „Mehr aktive Benutzer als Lizenzen: Lizenzierung prüfen“. Liegt sie darunter, lautet der Hinweis neutral „Weniger aktive Benutzer als Lizenzen. Das bedeutet nicht, dass Lizenzen frei sind (siehe Hinweis).“ Das Werkzeug empfiehlt nie, Lizenzen zu reduzieren.

8.1 Voraussetzungen

Voraussetzung	Einzelheiten
Lizenz im Tenant	Microsoft Entra ID P1 oder P2 für die Abfrage über Microsoft Graph. Ohne sie gibt Graph die Anmeldeprotokolle nicht heraus (siehe Fehlermeldungen).
Zeitraum	Graph reicht 30 Tage zurück. Für 60, 90, 180 oder 365 Tage führt das Werkzeug eine eigene Historie (Läufe mindestens alle 30 Tage) oder zählt über Log Analytics.
App-Registrierung	eigene Registrierung für das Admin-Kit, Anleitung unten
Rolle (interaktiv)	mindestens „Berichtsleser“, „Sicherheitsleser“ oder „Globaler Leser“; Log Analytics: „Log Analytics-Leser“ auf dem Arbeitsbereich
Zustimmung	einmalig durch einen „Administrator für privilegierte Rollen“ oder „Globalen Administrator“

8.2 App-Registrierung anlegen, Variante A: interaktiv

Für die Zählung per Kachel oder `ctd-admin lizenznutzung --interaktiv`. Angemeldet wird immer im Systembrowser, ohne Windows-Kontomanager und damit ohne Arbeitsplatzregistrierung, auch auf Terminalservern.

1. Im Microsoft Entra Admin Center (`https://entra.microsoft.com`) mit einem Konto anmelden, das App-Registrierungen anlegen darf (z. B. „Anwendungsadministrator“).
2. **Entra ID › App-Registrierungen › Neue Registrierung** wählen.
3. **Name:** „CosyTrack.Drive Admin-Kit Lizenznutzung“. **Unterstützte Kontotypen:** „Nur Konten in diesem Organisationsverzeichnis“.
4. **Umleitungs-URI:** Plattform „Öffentlicher Client/nativ (mobil und Desktop)“, Wert `http://localhost`. **Registrieren** wählen.
5. Auf der Seite **Übersicht** die **Anwendungs-ID (Client)** und die **Verzeichnis-ID (Mandant)** notieren.
6. **API-Berechtigungen › Berechtigung hinzufügen › Microsoft Graph › Delegierte Berechtigungen** wählen, `AuditLog.Read.All` und `Directory.Read.All` ankreuzen, **Berechtigungen hinzufügen**.
7. Nur bei Log Analytics: **Berechtigung hinzufügen › Von meiner Organisation verwendete APIs** › „Log Analytics API“ › **Delegierte Berechtigungen** › `Data.Read`.
8. **Administratorzustimmung für „<Tenant>“ erteilen** wählen und bestätigen (Rolle „Administrator für privilegierte Rollen“ oder „Globaler Administrator“). Alle Zeilen zeigen danach in der Spalte „Status“ ein grünes Häkchen.
9. Empfohlen: **Entra ID › Unternehmensanwendungen** › „CosyTrack.Drive Admin-Kit Lizenznutzung“ › **Eigenschaften › Zuweisung erforderlich** auf „Ja“ stellen und unter **Benutzer und Gruppen** nur die Administratoren zuweisen, die das Werkzeug verwenden dürfen.
10. Den ausführenden Konten unter **Entra ID › Rollen und Administratoren** die Rolle „Berichtsleser“ zuweisen (oder „Sicherheitsleser“ bzw. „Globaler Leser“). Bei Log Analytics zusätzlich im Azure-Portal am Arbeitsbereich **Zugriffssteuerung (IAM) › Rollenzuweisung hinzufügen** › „Log Analytics-Leser“.

11. Im Admin-Kit Client-ID und Tenant-ID eintragen und **Einstellungen speichern**, oder die Richtlinie „Lizenznutzung: App-Registrierung des Admin-Kits“ setzen.

8.3 App-Registrierung anlegen, Variante B: unbeaufsichtigt

Für die geplante Aufgabe: App-only mit Zertifikat, kein Client-Geheimnis. Die geplante Aufgabe fragt nie Namen ab. Dieselbe App-Registrierung wie in Variante A kann beides; eine getrennte Registrierung ist übersichtlicher.

1. Auf dem Rechner der geplanten Aufgabe ein Zertifikat erzeugen (PowerShell als Administrator); der private Schlüssel bleibt nicht exportierbar auf diesem Rechner:
2. Den Fingerabdruck (Thumbprint) notieren. Läuft die Aufgabe nicht als SYSTEM, dem Konto der Aufgabe Lesezugriff auf den privaten Schlüssel geben: `certlm.msc` › Eigene Zertifikate › Zertifikat › Alle Aufgaben › Private Schlüssel verwalten.
3. Im Entra Admin Center die App-Registrierung öffnen: **Zertifikate & Geheimnisse › Zertifikate › Zertifikat hochladen**, `lizenznutzung.cer` wählen, **Hinzufügen**. Kein Client-Geheimnis anlegen.
4. **API-Berechtigungen › Berechtigung hinzufügen › Microsoft Graph › Anwendungsberechtigungen**, `AuditLog.Read.All` ankreuzen, **Berechtigungen hinzufügen**, dann **Administratorzustimmung erteilen**. Für den Rückfall ohne P1/P2 optional zusätzlich `Application.Read.All`.
5. Nur bei Log Analytics: der App (Dienstprinzipal) am Arbeitsbereich die Rolle „Log Analytics-Leser“ zuweisen (Azure-Portal, Arbeitsbereich, **Zugriffssteuerung (IAM)**).
6. Richtlinien „Lizenznutzung: App-Registrierung des Admin-Kits“ und „Lizenznutzung: Zertifikat für den unbeaufsichtigten Modus“ setzen, gegebenenfalls „Lizenznutzung: Log-Analytics-Arbeitsbereich“.
7. Das Werkzeug einmal interaktiv als Administrator öffnen und den Hinweis zur Mitbestimmung bestätigen. Ohne eine Bestätigung auf diesem Computer endet der unbeaufsichtigte Lauf mit Rückgabecode 6.
8. Die geplante Aufgabe anlegen, z. B. wöchentlich als SYSTEM (mindestens alle 30 Tage, sonst entstehen Lücken):
9. Die Aufgabe einmal von Hand starten und den Rückgabecode prüfen (Aufgabenplanung, Spalte „Ergebnis der letzten Ausführung“). Auswertungen und `lizenznutzung-letzter-lauf.txt` liegen unter `%ProgramData%\CosyTrack.Drive\AdminKit\Berichte`.

> **Achtung: Zertifikat erneuern**
> Läuft das Zertifikat ab, endet die Aufgabe mit Rückgabecode 4 und die Historie bekommt Lücken. Rechtzeitig ein neues Zertifikat erzeugen, in der App-Registrierung hochladen und den neuen Fingerabdruck in der Richtlinie eintragen.

8.4 Historie und Abdeckung

Ohne Log Analytics speichert das Werkzeug je Benutzer nur einen HMAC-SHA256 der Benutzer-ID (Schlüssel zufällig, per DPAPI an den Computer gebunden) und das Datum der letzten gesehenen Anmeldung, dazu die Zeiträume, die jeder Lauf abgedeckt hat. Die Zahl ist die Anzahl der Hashes mit letzter Anmeldung im gewählten Zeitraum. Reicht die Historie nicht über den ganzen Zeitraum

oder liegen zwischen zwei Läufen mehr als 30 Tage, steht neben der Zahl „Daten erst ab … vorhanden, Zahl kann zu niedrig sein“ bzw. die Lücke. Für eine lückenlose Zählung das Werkzeug mindestens alle 30 Tage laufen lassen, am besten als geplante Aufgabe. Die Aufbewahrung regelt die Richtlinie „Lizenznutzung: Aufbewahrung der Historie“ (Standard und Minimum 13 Monate).

8.5 Variante Log Analytics

Exportiert der Tenant die Anmeldeprotokolle per Entra-Diagnoseeinstellung („SignInLogs“ und „NonInteractiveUserSignInLogs“) in einen Log-Analytics-Arbeitsbereich, zählt das Werkzeug dort per KQL über die Tabellen `SigninLogs` und `AADNonInteractiveUserSignInLogs` (Filter auf die App-ID, nur erfolgreiche Anmeldungen). Der Zeitraum ist im Rahmen der Aufbewahrung des Arbeitsbereichs sofort verfügbar. Workspace-ID per Richtlinie „Lizenznutzung: Log-Analytics-Arbeitsbereich“ oder in der Kachel. Nötig: Rolle „Log Analytics-Leser“ (oder „Leser“) auf dem Arbeitsbereich, Berechtigung „Log Analytics API“, `Data.Read`.

8.6 Geplante Aufgabe

`CosyTrack.Drive.AdminKit.exe --lizenznutzung --unbeaufsichtigt` (oder `ctd-admin lizenznutzung --unbeaufsichtigt`), mindestens alle 30 Tage. Sie zählt nur, fragt nie Namen ab und legt die Auswertung unter `%ProgramData%\CosyTrack.Drive\AdminKit\Berichte` ab. Rückgabecodes:

Rückgabecode	Bedeutung
0	ausgeführt; Zahl höchstens so hoch wie die lizenzierte Anzahl oder keine Lizenzzahl bekannt
1	ausgeführt; mehr aktive Benutzer als Lizenzen (Lizenzierung prüfen; keine Sperre)
2	Fehler (Konfiguration, Netzwerk, Historie nicht zugänglich)
4	Anmeldung bzw. Zertifikat
5	Werkzeug durch Richtlinie deaktiviert
6	Hinweis zur Mitbestimmung auf diesem Computer noch nie bestätigt
7	keine Entra-ID-P1/P2-Lizenz im Tenant
8	Berechtigung, Administratorzustimmung oder Rolle fehlt
9	keine erfolgreichen Anmeldungen der App im Zeitraum (Client-ID prüfen)
10	Log-Analytics-Arbeitsbereich nicht erreichbar

8.7 Namensanzeige und warum sie doppelt abgesichert ist

Wer CosyTrack.Drive wann genutzt hat, ist eine personenbezogene, mitbestimmungspflichtige Auswertung. Das Werkzeug zeigt Namen deshalb nur, wenn alles zusammenkommt:

1. Die Richtlinie „Lizenznutzung: Namensanzeige zulassen“ ist aktiviert (Standard: nein; sonst ist der Knopf ausgeblendet).
2. Erste Bestätigung: Warnung „Die Anzeige von Namen ist heikel …“ mit „Abbrechen“ als Standard.
3. Zweite Bestätigung: das Wort NAMEN eintippen und einen Zweck wählen („Lizenzbereinigung“, „Prüfung durch Lizenzgeber“ oder „Sonstiges“ mit Pflichttext).

Erst dann fragt das Werkzeug live UPN und Datum der letzten Anmeldung ab, bei Graph höchstens für die letzten 30 Tage. Über der Liste steht: „Die Liste enthält nur Benutzer mit Anmeldung im Zeitraum. Wer fehlt, ist nicht automatisch kein Named User." Namen werden nie gespeichert, nicht in der Historie, nicht in Protokollen, nicht im Diagnosepaket, nicht in der Auswertung; beim Schließen des Fensters sind sie weg. Ein Export als CSV verlangt eine weitere Bestätigung und trägt Mitbestimmungshinweis und Disclaimer im Kopf. Jede Anzeige und jeder Export wird mit Zeitpunkt, Windows-Konto, Zweck und Anzahl protokolliert, ohne Namen.

8.8 Fehlermeldungen

Meldung (gekürzt)	Ursache	Abhilfe
„Der Tenant hat keine Lizenz für Microsoft Entra ID P1 oder P2 …"	Graph verweigert die Anmeldeprotokolle	Ist bei der Unternehmensanwendung von CosyTrack.Drive „Zuweisung erforderlich" aktiv, zeigt das Werkzeug die zugewiesenen Benutzer, gekennzeichnet als „berechtigt, nicht zwingend aktiv" (Rolle „Verzeichnisleser" nötig); sonst ist eine Zählung so nicht möglich. Alternativ Log Analytics.
„… fehlt die Berechtigung bzw. die Administratorzustimmung"	Berechtigung oder Zustimmung fehlt	Variante A Schritte 6 bis 8 bzw. Variante B Schritt 4
„Dem angemeldeten Konto fehlt eine Entra-Rolle …"	Konto ohne Berichtsleser, Sicherheitsleser oder Globalen Leser	Rolle zuweisen, neu anmelden
„Keine erfolgreichen Anmeldungen … Stimmt die Client-ID?"	falsche Client-ID oder keine Nutzung im Zeitraum	gezählte App prüfen (die von CosyTrack.Drive, nicht die des Admin-Kits)
„Der Log-Analytics-Arbeitsbereich ist nicht erreichbar …"	falsche Workspace-ID, Rolle fehlt, Tabellen nicht exportiert	Workspace-ID, Rolle und Diagnoseeinstellung prüfen
„Die Client-ID des Admin-Kits ist dieselbe wie die von CosyTrack.Drive …"	gleiche App-Registrierung eingetragen	eigene Registrierung anlegen
„Zertifikat … nicht gefunden …"	Zertifikat fehlt, abgelaufen, kein Zugriff auf den privaten Schlüssel	Variante B, Schritte 1 bis 3

8.9 Named User sauber verwalten

Die Zählung ist eine Plausibilitätsprüfung, keine Verwaltung. Bewährt hat sich:

- **Zuweisung über eine Entra-Gruppe:** eine Gruppe „CosyTrack.Drive-Benutzer" anlegen, bei der Unternehmensanwendung von CosyTrack.Drive **Zuweisung erforderlich** auf „Ja" stellen und nur diese Gruppe zuweisen. Die Mitglieder der Gruppe sind die Named User; wer nicht Mitglied ist, kann sich nicht anmelden.

- **Laufwerke an dieselbe Gruppe binden:** Richtlinien mit den Laufwerkszuordnungen per Gruppenrichtlinie bzw. Intune nur auf diese Gruppe anwenden.
- **Ein- und Austritt:** Aufnahme in die Gruppe als Schritt im Eintrittsprozess, Entfernen im Austrittsprozess; bei längerer Abwesenheit bleibt die Person Mitglied, sie bleibt Named User.
- **Regelmäßig abgleichen:** Anzahl der Gruppenmitglieder mit der lizenzierten Anzahl vergleichen, z. B. vierteljährlich und vor jeder Verlängerung.
- **Werkzeug als Gegenprobe:** Liegt der Orientierungswert über der Zahl der Gruppenmitglieder oder der Lizenzen, stimmt etwas an der Zuweisung oder Lizenzierung nicht. Liegt er darunter, ist das normal (Abwesenheiten) und kein Grund, Lizenzen zu reduzieren.

9 Speicherorte

Journal und ungesendete Inhalte gehören zum Benutzer und liegen im Profil; alles, was sich ersetzen lässt, liegt auf dem Host. Die Skizze zeigt die Aufteilung und die Einstellungen, die sie steuern:

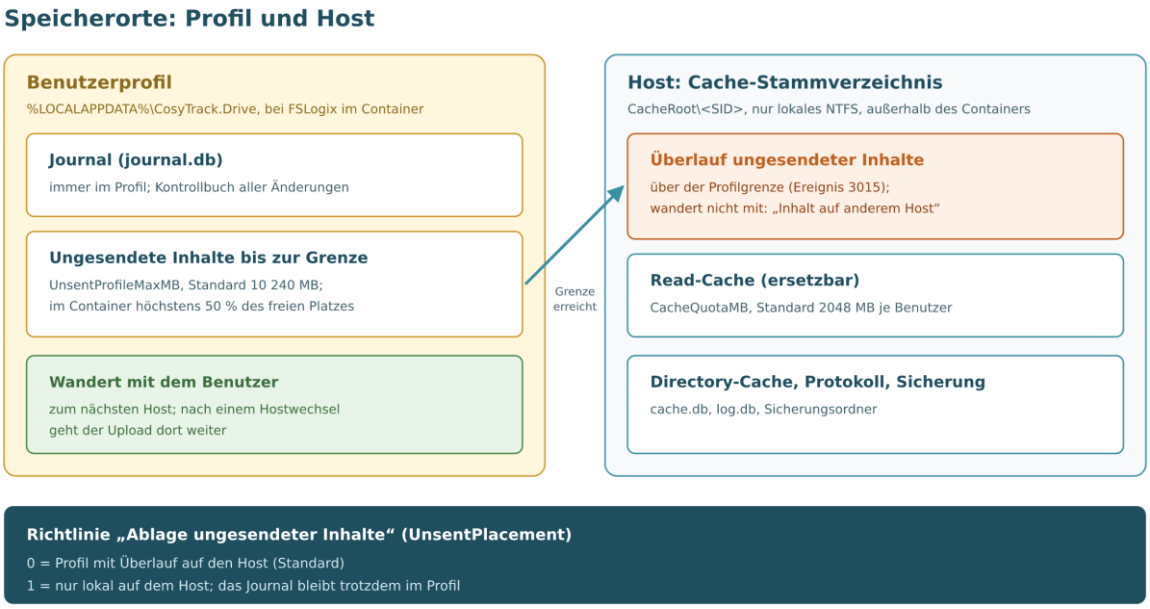

Abbildung 18: Speicherorte: Profil gegen Host mit UnsentPlacement, UnsentProfileMaxMB und CacheQuotaMB

Ort	Inhalt	wandert mit dem Profil
`%LOCALAPPDATA%\CosyTrack.Drive\journal.db`	Journal	ja
`%LOCALAPPDATA%\CosyTrack.Drive\ungesendet\`	ungesendete Inhalte bis zur Grenze (`UnsentProfileMaxMB`, Standard 10 240 MB, im FSLogix-Container höchstens 50 % des freien Platzes)	ja
`<CacheRoot>\<SID>\cache.db`, `cache\`	Directory-Cache und Read-Cache (`CacheQuotaMB`, Standard 2048 MB)	nein
`<CacheRoot>\<SID>\log.db`	Protokoll	nein
`<CacheRoot>\<SID>\ungesendet\`	Überlauf ungesendeter Inhalte	nein
`<CacheRoot>\<SID>\Sicherung\`	Sicherungsordner	nein
`%ProgramData%\boddenberg\cosytrack.drive\`	Lizenz für alle Benutzer und Testzeitraum (dazu `TrialStartUtc` unter `HKLM\SOFTWARE\boddenberg\CosyTrack.Drive`)	–
`%LOCALAPPDATA%\boddenberg\cosytrack.drive\license.ubl`	Lizenz nur für diesen Benutzer (Import ohne Administratorrechte)	ja

`<CacheRoot>` ist das Cache-Stammverzeichnis, Standard `%ProgramData%\CosyTrack.Drive\Users`. Es muss auf einem lokalen NTFS-Datenträger liegen. Netzwerkfreigaben, Wechseldatenträger und andere Dateisysteme sind nicht zulässig, weil die Datenbanken dort beschädigt werden können: Die Konfigurations-App lehnt sie ab, der Agent weicht auf den Standardort aus (Ereignis 3070), und der Bereitschaftscheck meldet ROT.

Die Konfigurations-App lehnt ein Cache-Stammverzeichnis auf einer Freigabe sofort ab:

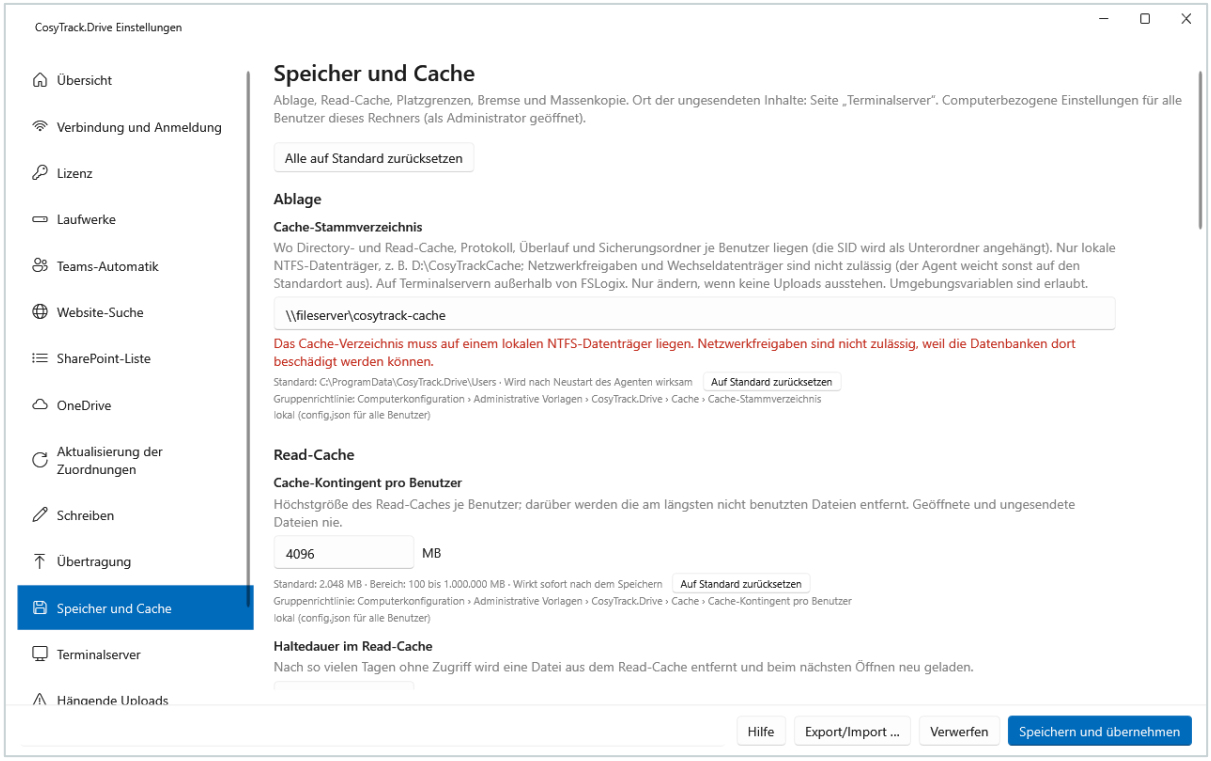

Abbildung 19: Konfigurations-App lehnt ein Cache-Verzeichnis auf einer Freigabe ab

> **Achtung: FSLogix: Datenordner nicht ausschließen**
> Auf Terminalservern liegt das Cache-Stammverzeichnis lokal auf dem Host und außerhalb des FSLogix-Containers. `%LOCALAPPDATA%\CosyTrack.Drive` darf in `redirections.xml` nicht ausgeschlossen sein, sonst wandern Journal und ungesendete Inhalte nicht mit (Ereignis 3014). Ist das Profil nicht dauerhaft oder liegt `%LOCALAPPDATA%` auf einer Freigabe, legt der Agent das Journal ersatzweise auf dem Host ab (Ereignisse 3012 und 3013).

10 Betrieb

10.1 Normalbetrieb

- Änderungen werden nach einer Ruhezeit von 3 Sekunden bzw. nach dem Schließen der Datei hochgeladen; parallel je Sitzung bis zu 8, je Server bis zu 32 Übertragungen.
- Der Read-Cache wird nach 14 Tagen ohne Zugriff bzw. über dem Kontingent (Standard 2048 MB je Benutzer) aufgeräumt. Geöffnete und ungesendete Dateien werden nie entfernt.
- Teams, Websites und Listen werden alle 30 Minuten und bei Ereignissen aktualisiert; entfernt wird ein Ordner erst nach zwei erfolgreichen Durchläufen und nie mit Rückstand.

Wie die Übertragung eingestellt ist, zeigt die Seite „Übertragung“ der Konfigurations-App:

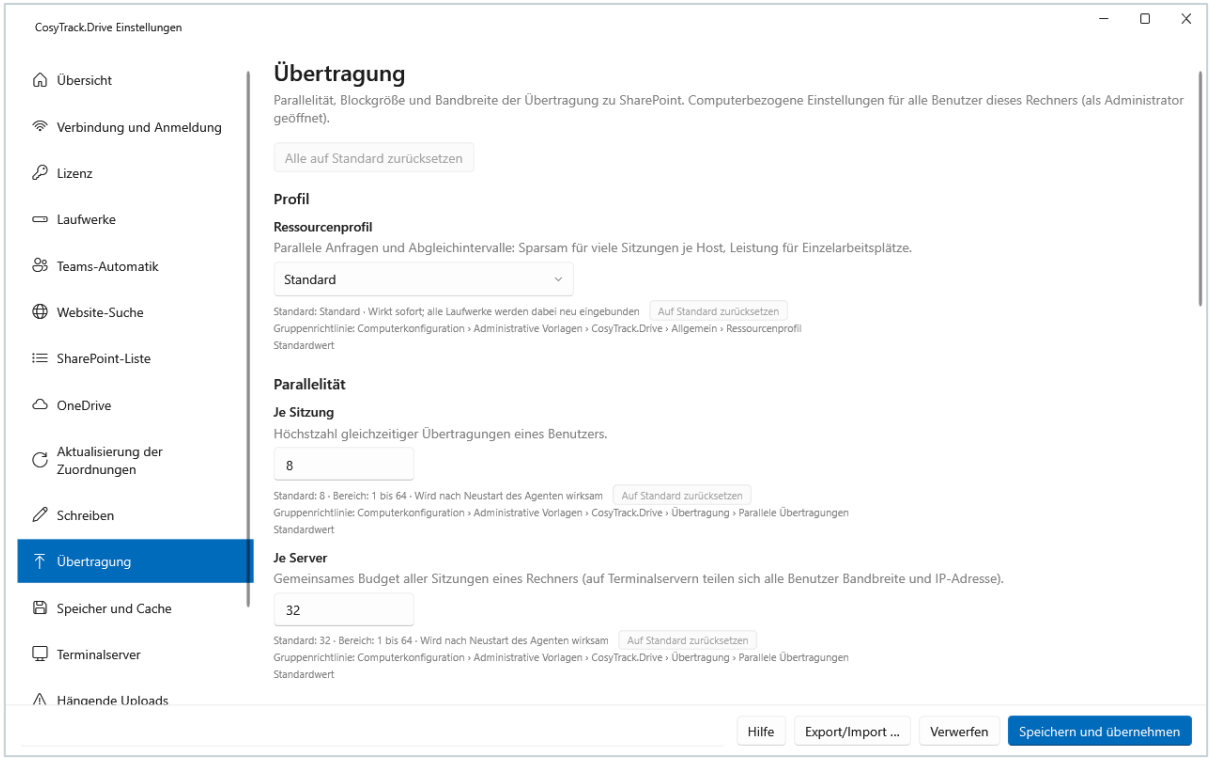

Abbildung 20: Konfigurations-App, Seite „Übertragung“

10.2 Abmeldung und Terminalserver

- Bei der Abmeldung wartet Windows bis zu 30 Sekunden, wenn der Rest voraussichtlich in dieser Zeit hochgeladen werden kann; sonst geht es beim nächsten Start weiter, auch auf einem anderen Host.
- Derselbe Benutzer in zwei Sitzungen: Nur eine schreibt, die andere ist schreibgeschützt (Ereignis 1003). Empfehlung: `fSingleSessionPerUser = 1`.
- Inhalte im Überlauf eines Hosts bleiben dort, bis der Benutzer sich dort wieder anmeldet („Inhalt auf anderem Host“, Ereignis 3002), oder werden mit dem Admin-Kit exportiert und beim nächsten Start übernommen.

Die Einstellungen für Terminalserver fasst die Konfigurations-App auf einer eigenen Seite zusammen:

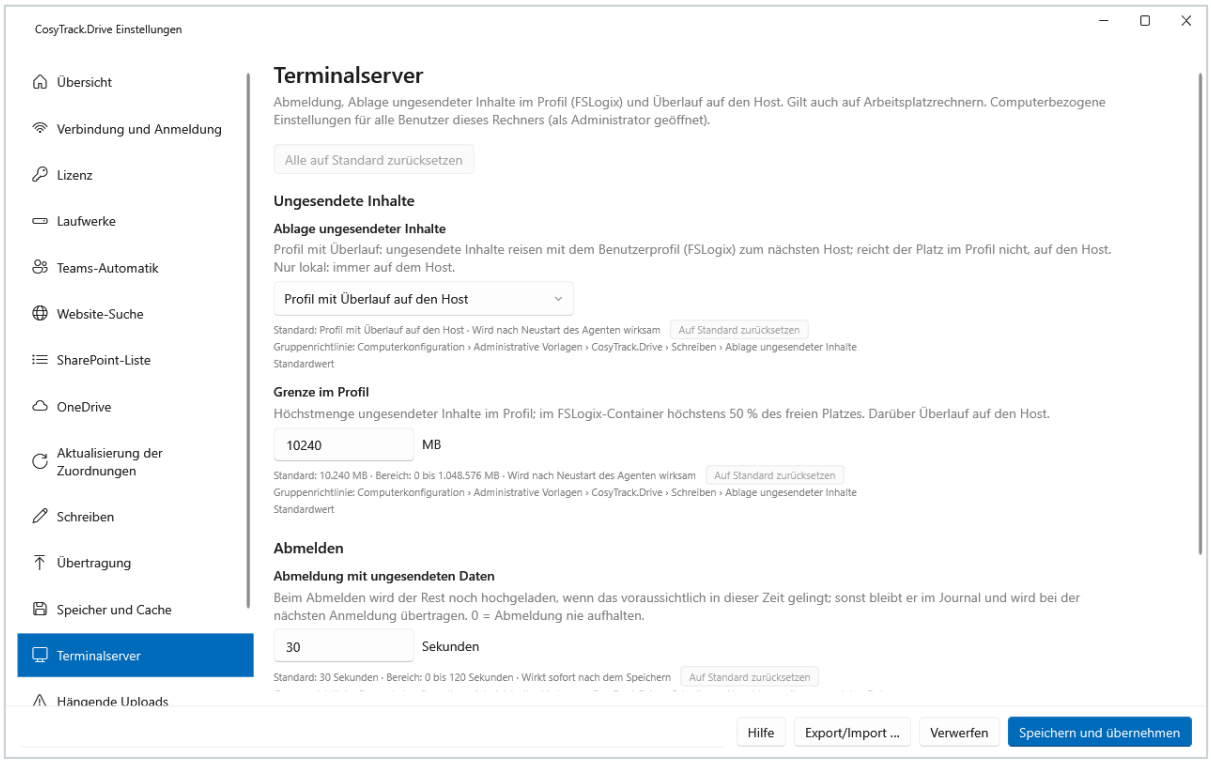

Abbildung 21: Konfigurations-App, Seite „Terminalserver“

> **Praxistipp: Eine Sitzung je Benutzer**
> Mit `fSingleSessionPerUser = 1` landet ein Benutzer immer in derselben Sitzung. Das vermeidet schreibgeschützte Zweitsitzungen und Überlauf auf mehreren Hosts.

10.3 Hängende Uploads und Not-Aus

Dateien, die sich dauerhaft nicht hochladen lassen, zeigt die Konfigurations-App unter „Hängende Uploads“, gruppiert nach Grund. Je Datei sind erneut versuchen, umbenennen, als Kopie an ein anderes Ziel speichern und einzeln in eine Quarantäne auslagern möglich:

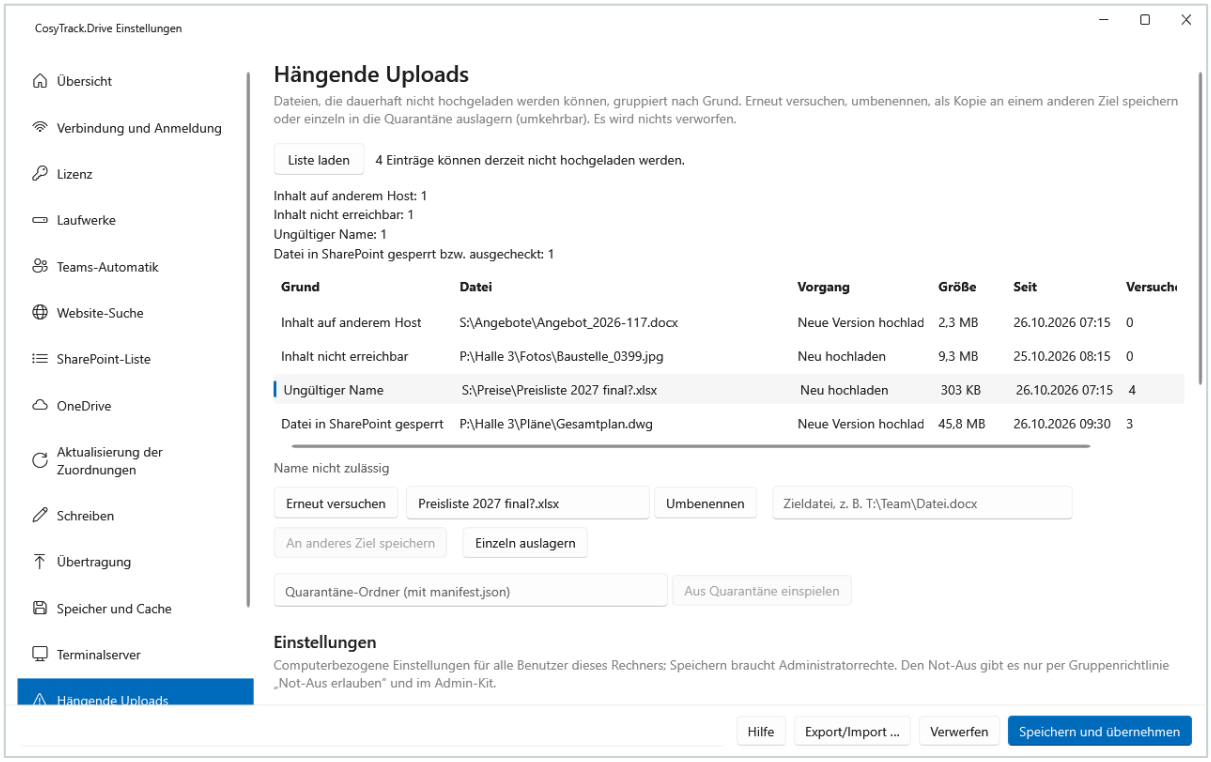

Abbildung 22: Konfigurations-App, hängende Uploads

> **Achtung: Not-Aus nur als bewusste Administratorhandlung**
> Den Not-Aus (Einträge nach geprüfter Sicherung in die Quarantäne aus dem Journal entfernen) gibt es nur im Admin-Kit, mit Administratorrechten, der Richtlinie „Not-Aus erlauben“, einer Bestätigung mit der Anzahl der Einträge und einer Begründung. Kein automatischer Vorgang verwirft ungesendete Inhalte.

11 Überwachung

11.1 Leistungsindikatoren

CosyTrack.Drive registriert die Kategorie `CosyTrack.Drive` (Leistungsmonitor, `logman`, PRTG, Checkmk, Zabbix, Azure Monitor Agent). Instanzen: `S<Sitzung>`, `S<Sitzung> <Buchstabe>:` und `_Total`, ohne Benutzernamen.

Indikator	Bedeutung	Auffällig
`Avg Open Wait ms`	Wartezeit beim Öffnen einer nicht zwischengespeicherten Datei	dauerhaft über 1000 ms
`Avg Graph Request Latency ms`	Antwortzeit von Microsoft Graph	dauerhaft über 1000 ms
`Throttled Requests/sec`	Drosselung durch Microsoft	über 0
`Backlog Items`, `Oldest Backlog Age sec`	ungesendete Änderungen und ihr Alter	steigt stetig
`Read Cache Hit Ratio %`	Anteil aus dem Cache bedienter Öffnungen	unter 30 % bei wiederkehrenden Dateien
`Avg Upload Throughput MB/s`	Upload-Geschwindigkeit	dauerhaft deutlich unter der Leitung

Im Leistungsmonitor fügen Sie die Indikatoren der Kategorie „CosyTrack.Drive“ hinzu.

> **Rechtlicher Hinweis: Mitbestimmung bei dauerhafter Aufzeichnung**
> Das Admin-Kit erzeugt einen fertigen `logman`-Datensammler („Vorlagen“). Leistungsdaten sind technisch geeignet, Rückschlüsse auf das Arbeitsverhalten zu ziehen. Vor einer dauerhaften Aufzeichnung ist gegebenenfalls der Betriebs- oder Personalrat zu beteiligen.

11.2 Ereignisse

- Anwendungsprotokoll, Quelle „CosyTrack.Drive“: kritische Zustände (z. B. 1300 Anmeldung fehlgeschlagen, 1704 Upload scheitert wiederholt).
- Kanal „CosyTrack.Drive/Betrieb“ (Anwendungs- und Dienstprotokolle): Sitzungen, Speicherorte, Journal-Prüfung, Grenzen, Lizenz, Cache-Stammverzeichnis; geeignet für Windows Event Forwarding.

Ereignisse enthalten keine Datei-, Pfad- oder Benutzernamen. Ausnahme sind der Not-Aus (3030) und das endgültige Löschen der Quarantäne (3032): Sie nennen die SID des ausführenden Administrators und seine Begründung. Jede ID mit Maßnahme beschreibt die Ereignis- und Fehlerreferenz.

11.3 Statusfenster und Protokoll

Das Statusfenster des Benutzers zeigt Aktivität, Leistung, Rückstau, Cache, Laufwerke, Meldungen und alle wirksamen Einstellungen mit Herkunft. Die Registerkarte „Leistung“ zeigt dieselben Werte wie die Leistungsindikatoren:

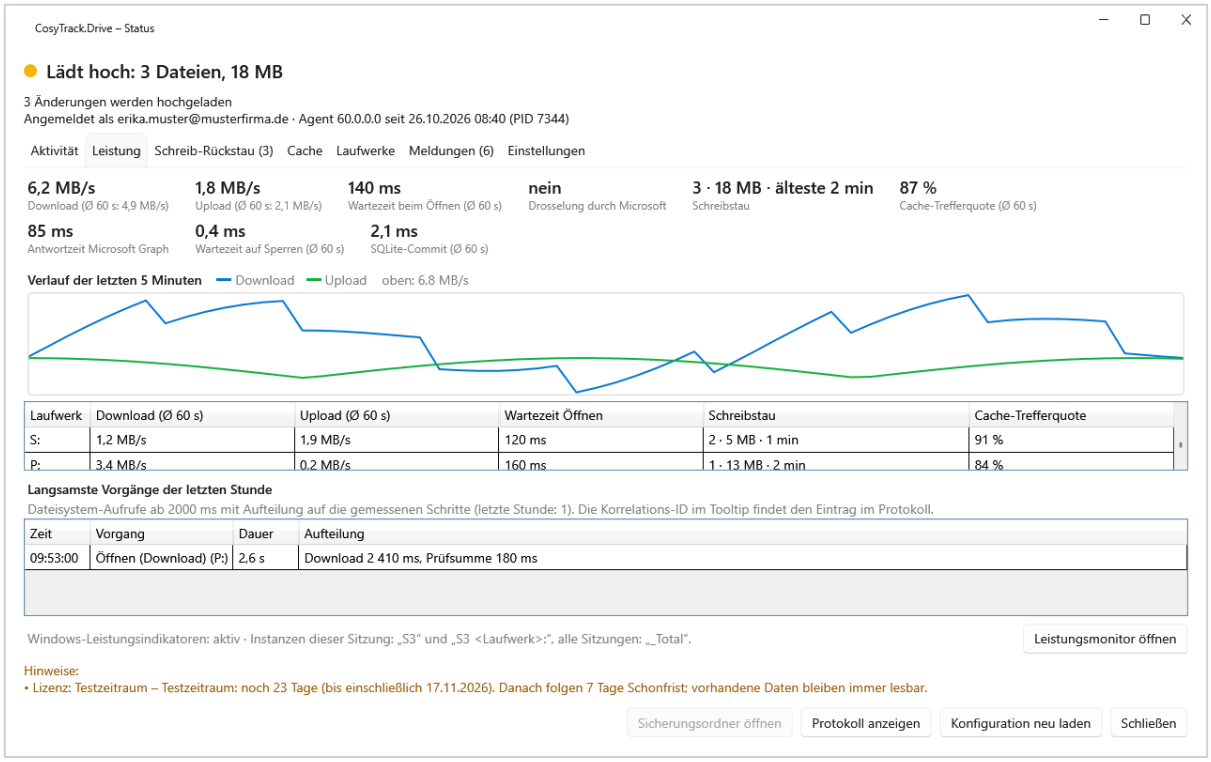

Abbildung 23: Statusfenster, Registerkarte „Leistung“

Das Protokollfenster durchsucht das Agent-Protokoll (`log.db`) nach Zeit, Pfad, Kategorie und Korrelations-ID; die Korrelations-ID aus einem Ereignis führt zum Vorgang:

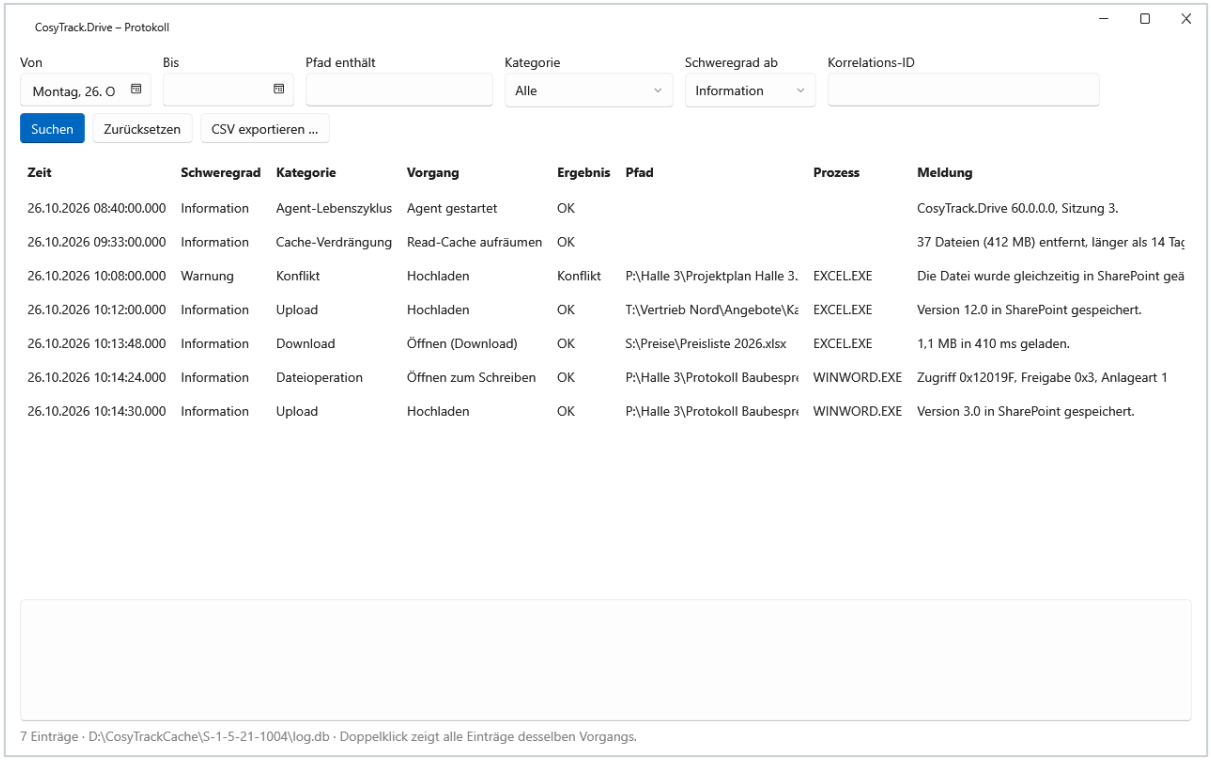

Abbildung 24: Protokollfenster mit den letzten Vorgängen

12 Datensicherung und Wiederherstellung

- **Maßgeblich sind die Daten in SharePoint.** Ihre Sicherung (Papierkorb, Versionsverlauf, Aufbewahrung, ggf. Backup-Lösung für Microsoft 365) gilt unverändert.
- **Lokale Daten:** Journal und ungesendete Inhalte sind nur bis zum Upload lokal. Den Read-Cache muss man nicht sichern; er wird bei Bedarf neu geladen.
- **Sicherungsordner:** Fassungen, die sich nicht hochladen ließen, liegen im Sicherungsordner (`<CacheRoot>\<SID>\Sicherung` bzw. Richtlinie „Sicherungsordner“, für Farmen eine Freigabe). Sie werden nie automatisch gelöscht.
- **Quarantäne:** Ausgelagerte Inhalte (einzeln oder per Not-Aus) liegen mit Manifest und Prüfsummen in der Quarantäne und lassen sich wieder einspielen (Konfigurations-App bzw. `ctd-admin reimport`).
- **Deinstallation mit `FORCEUNINSTALL=1`:** Kopien aller ungesendeten Inhalte und Journale unter `%ProgramData%\CosyTrack.Drive\Sicherung-Deinstallation-<Zeit>` mit `manifest.json`; die Originale bleiben und werden nach einer Neuinstallation hochgeladen.

Vor dem Schritt prüfen: Vor Rechnerwechsel oder Neuaufbau eines Hosts

- Statusfenster bzw. `CosyTrack.Drive.Setup.exe summary auto`: Steht noch etwas aus?
- Verwaiste Uploads im Überlauf mit dem Admin-Kit exportieren.
- Sicherungsordner und Quarantäne sichten, bevor der Datenträger gelöscht wird.

13 Bekannte Einschränkungen

Zwei Einschränkungen dieser Version sollten Administratoren kennen; beide betreffen nie ungesendete Inhalte, die CosyTrack.Drive selbst hält.

13.1 Bibliotheken ohne Versionierung

SharePoint bearbeitet Office-Dateien nach dem Hochladen teilweise selbst nach. CosyTrack.Drive erkennt das daran, dass Versionsnummer und Bearbeiter gleich bleiben, und wertet es nicht als Konflikt. In einer Bibliothek **ohne** Versionierung bleibt die Versionsnummer aber auch gleich, wenn derselbe Benutzer die Datei kurz nach dem Hochladen im Browser ändert. Diese Browser-Änderung kann dann von der nächsten Speicherung über das Laufwerk überschrieben werden, ohne dass eine Konfliktkopie entsteht; ohne Versionierung gibt es in SharePoint keinen Weg zurück. Änderungen anderer Benutzer werden weiterhin erkannt.

- **Warnung beim Einbinden:** Ist in einer Bibliothek die Versionierung ausgeschaltet, schreibt CosyTrack.Drive beim Einbinden eine Warnung ins Protokoll und das Ereignis 1500 ins Anwendungsprotokoll (Quelle CosyTrack.Drive).
- **Empfehlung:** Die Versionierung in SharePoint eingeschaltet lassen (Standard in SharePoint Online). Dann tritt die Einschränkung nicht auf.
- **Alternative:** Lässt sich die Versionierung nicht einschalten, die Richtlinie „Bibliotheken ohne Versionierung“ (Computerkonfiguration › Administrative Vorlagen › CosyTrack.Drive › Schreiben) auf „Nur lesen“ setzen. Solche Bibliotheken sind dann über das Laufwerk nur lesbar; geändert wird im Browser.

13.2 Sehr große Ordner

Beim ersten Öffnen eines Ordners erscheinen die ersten Einträge nach rund einer Sekunde. SharePoint liefert danach 1000 Einträge je Abruf, nacheinander; ein Ordner mit rund 8.500 Einträgen ist deshalb erst nach etwa 6 Sekunden vollständig. Bis dahin füllt sich die Ansicht im Explorer schrittweise, und Sortierung und Suche umfassen noch nicht alle Einträge. Das betrifft nur das erste Öffnen; danach kommt der Ordner aus dem lokalen Verzeichnis-Cache und wird im Hintergrund aktuell gehalten.

> **Praxistipp: Große Ablagen gliedern**
> Ordner mit mehreren tausend Dateien in Unterordner aufteilen (etwa nach Jahr oder Vorgang). Das beschleunigt das erste Öffnen und hilft auch im Browser und in Teams.

14 Fehlersuche

Symptom	Prüfen
Keine Laufwerke	Agent läuft? Infobereich bzw. Ereignis 1000; Client-ID und Tenant-ID gesetzt (1200)? Zuordnungen vorhanden (1201)?
Symbol grau, „Anmeldung erforderlich“	Benutzer anmelden lassen; auf Terminalservern immer Browser; Zustimmung der App-Registrierung prüfen (1300/1301)
Laufwerk fehlt	Buchstabe belegt (1401)? Berechtigung (1402)? URL (1403)? Lizenz: nach dem Ende der Schonfrist keine neuen Laufwerke (3062)
Uploads hängen	Statusfenster › Schreib-Rückstau (Grund); Konfigurations-App › Hängende Uploads; Drosselung (`Throttled Requests/sec`)
Langsames Öffnen	`Avg Open Wait ms`, Verbindungsprüfung im Admin-Kit; TLS-Inspektion oder Proxy-Authentifizierung?
Dateien schreibgeschützt	Zugriffsmodus „nur lesen“, archiviertes Team, zweite Sitzung (1003), Inhalt auf anderem Host (3002), Lizenz abgelaufen (3062)
Cache-Warnung 3070	Cache-Stammverzeichnis auf ein lokales NTFS-Volume legen
Auf Terminalservern Office-Aktivierung gestört	Arbeitsplatzregistrierung (3050) bereinigen, `BlockAADWorkplaceJoin` setzen

Läuft der Agent nicht, zeigt das die Seite „Übersicht“ der Konfigurations-App deutlich an:

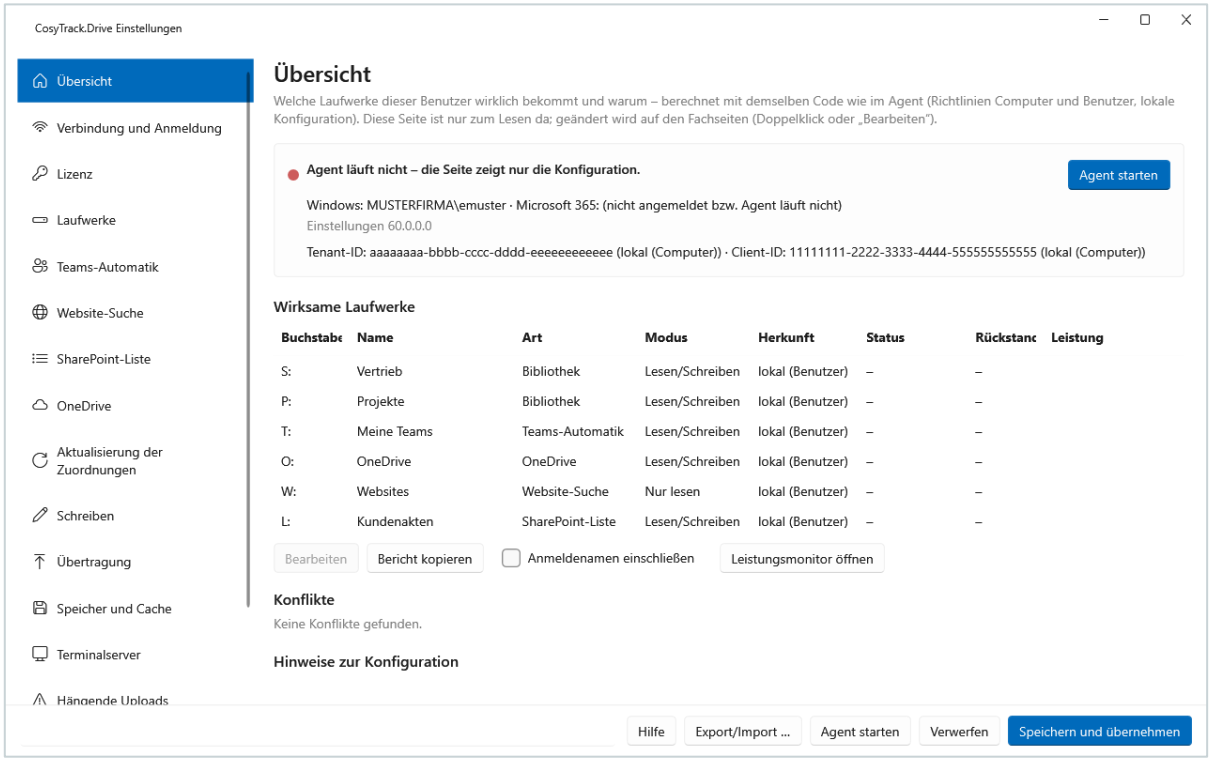

Abbildung 25: Konfigurations-App, Agent läuft nicht

> **Praxistipp: Diagnosepaket aus dem Admin-Kit**
> Für den Support erstellt das Admin-Kit ein anonymisiertes Diagnosepaket (Kachel „Diagnosepaket“ bzw. `ctd-admin diagnose`). Vor dem Versand die Inhaltsübersicht im Zip ansehen. Das Diagnosepaket der Konfigurations-App ist nicht anonymisiert und nicht für die Weitergabe an Dritte gedacht.

15 Deinstallation

Zweck	Befehl
Deinstallieren	Programme und Features bzw. `uninstall.cmd`, still `uninstall.cmd /quiet` oder `msiexec /x {ProductCode} /qn /norestart`
Trotz ungesendeter Inhalte	`uninstall.cmd /force` bzw. `msiexec /x {ProductCode} FORCEUNINSTALL=1`

- Vor dem Entfernen prüft das MSI auf noch nicht hochgeladene Änderungen, auch im Ausweichort des Cache-Stammverzeichnisses und in den gerade eingebundenen Profilen. Gibt es welche, bricht die Deinstallation mit einer Meldung ab (1603).
- Mit `FORCEUNINSTALL=1` werden die Inhalte vorher gesichert (siehe Kapitel 12 „Datensicherung und Wiederherstellung“).
- Benutzerdaten, Konfiguration, Lizenz und Testzeitraum bleiben immer erhalten.
- Der Treiber wird nur bei der vollständigen Deinstallation entfernt, nie bei einem Update.

Bricht die Deinstallation wegen ungesendeter Inhalte ab, meldet das MSI das so:



Abbildung 26: MSI vorzeitig beendet, z. B. bei ungesendeten Inhalten (Nachbildung)

> **Achtung: Profilcontainer abgemeldeter Benutzer sind nicht prüfbar**
> Das MSI sieht nur die gerade eingebundenen Profile. Ungesendete Inhalte in den FSLogix-Containern abgemeldeter Benutzer erkennt es nicht. Benutzerdaten löscht ein Administrator deshalb bewusst von Hand (`<CacheRoot>\<SID>`), nachdem nichts mehr aussteht.