HANDBUCH FÜR SYSTEMHÄUSER

CosyTrack.Drive 60.0 – Admin-Kit-Handbuch

Werkzeuge für Prüfung, Rollout, Abnahme und Störung, als Oberfläche und an der Kommandozeile.

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

Inhalt

1 Überblick 3
2 Anmeldung 5
3 Verbindungsprüfung 6
4 Bereitschaftscheck 7
5 Stresstest 9
6 Hängende Uploads, Not-Aus, verwaiste Uploads 11
7 Lizenz und Lizenznutzung 13
7.1 App-Registrierung anlegen, Variante A: interaktiv 14
7.2 App-Registrierung anlegen, Variante B: unbeaufsichtigt 14
7.3 Bedienung 15
7.4 Kommandozeile und Rückgabecodes 16
8 Diagnosepaket 18
9 Vorlagen 20

Auf einen Blick: Das Wichtigste in Kürze

- Eigenes Paket, läuft ohne Installation von CosyTrack.Drive und braucht keine Benutzerlizenz.
- Jedes Werkzeug gibt es als Kachel (`CosyTrack.Drive.AdminKit.exe`) und an der Kommandozeile (`ctd-admin.exe`).
- Vor dem Kauf: Verbindungsprüfung. Vor dem Rollout: Bereitschaftscheck und Vorlagen. Abnahme: Stresstest. Betrieb: Lizenznutzung, Diagnosepaket, hängende Uploads.
- Berichte enthalten Benutzer- und Dateinamen nur, wo sie ausdrücklich angefordert werden.
- Die Lizenznutzung ist mitbestimmungspflichtig und liefert nur einen Orientierungswert (Untergrenze), keinen Ersatz für die Verwaltung der Named User.
- Die Beispielberichte in diesem Handbuch sind Musterberichte mit fiktiven Daten (Musterfirma GmbH).

1 Überblick

Das Admin-Kit begleitet ein Projekt vom ersten Test bis zum Betrieb. Die Zeitleiste zeigt, wann welches Werkzeug zum Einsatz kommt:

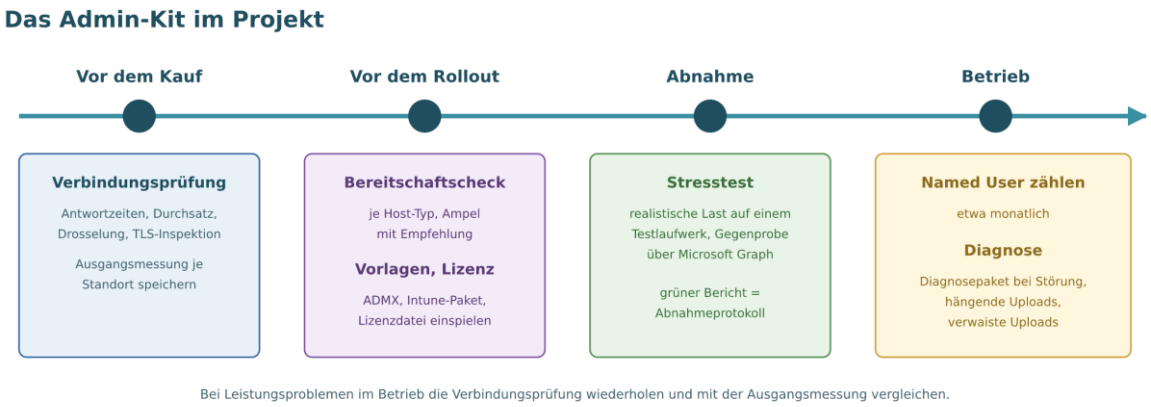


Abbildung 1: Einsatz des Admin-Kits im Projekt als Zeitleiste

Nach dem Start zeigt das Admin-Kit alle Werkzeuge als Kacheln:

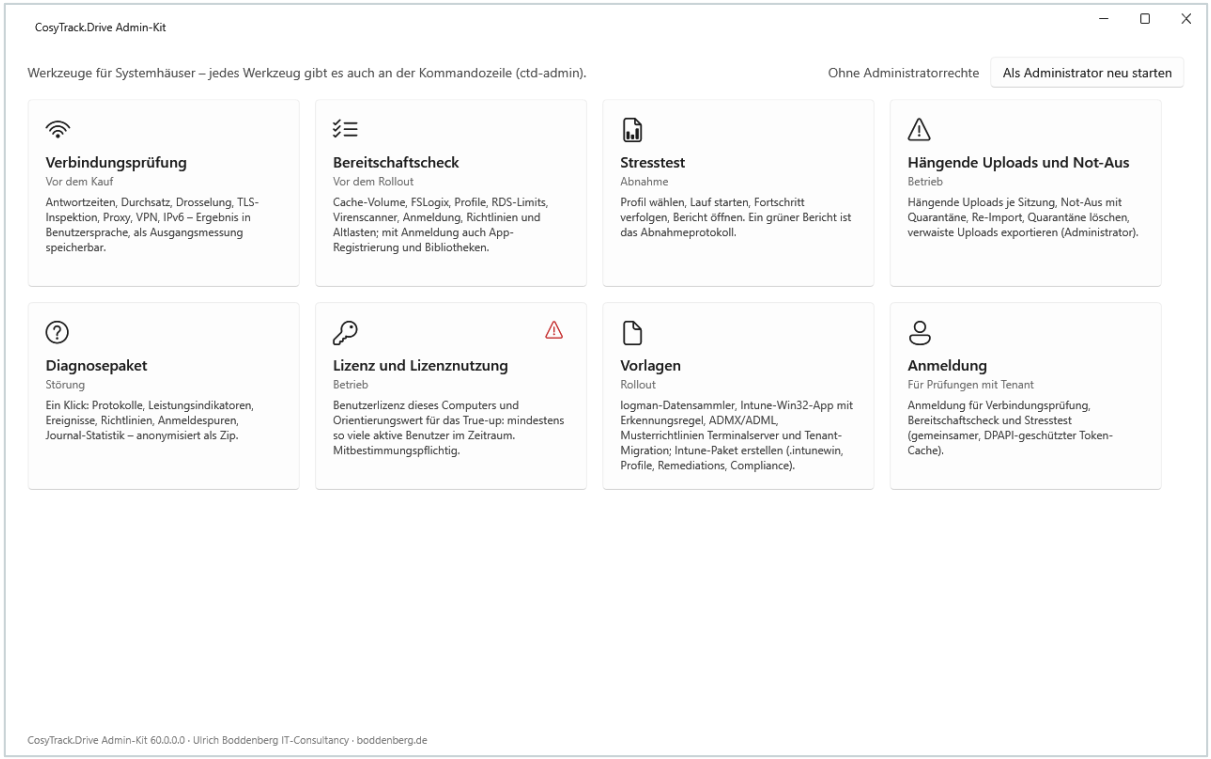


Abbildung 2: Admin-Kit, Kachelübersicht

Werkzeug	Vor dem Kauf	Vor dem Rollout	Abnahme	Betrieb und Störung
Verbindungsprüfung	ja	ja	–	bei Leistungsproblemen
Bereitschaftscheck	–	ja	ja	nach Änderungen am Host
Stresstest	–	–	ja	–
Hängende Uploads, Not-Aus, verwaiste Uploads	–	–	–	ja
Lizenz und Lizenznutzung	–	ja	–	regelmäßig
Diagnosepaket	–	–	–	Störung
Vorlagen	–	ja	–	–

Installation: `CosyTrack.Drive.AdminKit-60.0.0.0-x64.msi` (Programmordner `%ProgramFiles%\CosyTrack.Drive Admin-Kit`, Startmenü, `ctd-admin` im Suchpfad) oder ohne Installation aus dem ZIP.

Berichte: Alle Werkzeuge schreiben Berichte im einheitlichen Layout als HTML und Markdown, standardmäßig unter `Dokumente\CosyTrack.Drive Admin-Kit`. Kopf mit Werkzeug, Host, Zeit und Version; Benutzer- und Dateinamen nur, wo sie ausdrücklich angefordert werden.

Rückgabecodes der Kommandozeile: 0 grün bzw. erfolgreich, 1 gelb bzw. nur Vorschau, 2 Fehler bzw. abgebrochen, 3 rot, 4 Anmeldung nötig; die Lizenznutzung kennt zusätzlich 5 bis 10 (Abschnitt „Lizenz und Lizenznutzung“).

> **Praxistipp: Kommandozeile für Serien**
> Für viele Hosts lohnt sich `ctd-admin` in einem Skript: Die Rückgabecodes lassen sich auswerten, die Berichte landen gesammelt im Berichtsordner.

2 Anmeldung

Das Admin-Kit verwendet für Verbindungsprüfung, Bereitschaftscheck und Stresstest dieselbe App-Registrierung wie CosyTrack.Drive (delegiert, Anmeldung im Systembrowser, Umleitungs-URI `http://localhost`). Ausnahme ist die Lizenznutzung: Sie meldet sich mit einer eigenen App-Registrierung des Admin-Kits und einem eigenen Token-Cache an (Abschnitt „Lizenz und Lizenznutzung“). Client- und Tenant-ID kommen aus den Richtlinien bzw. der config.json des Rechners oder werden angegeben. Der Token-Cache ist mit DPAPI geschützt, wird mit dem Stresstest geteilt und nie mit dem Agent. Die Kachel „Anmeldung“ zeigt das angemeldete Konto:

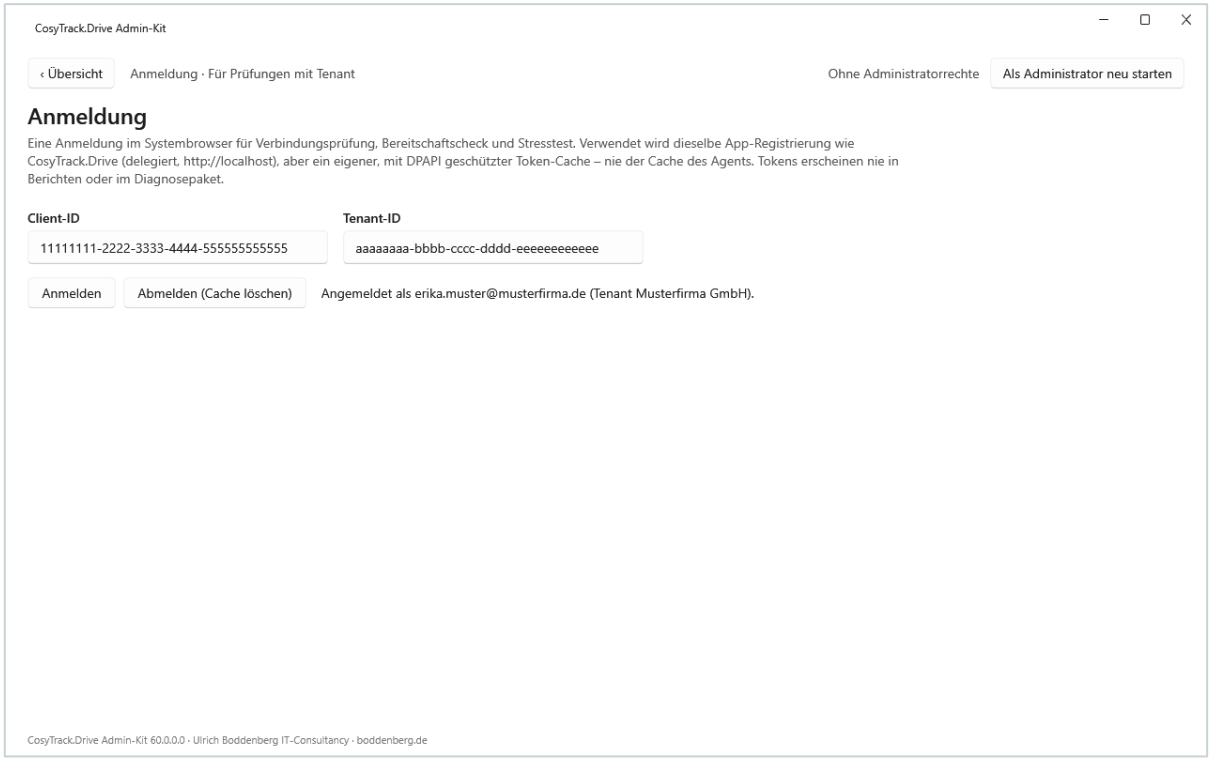


Abbildung 3: Admin-Kit, Kachel „Anmeldung“

```
ctd-admin anmelden --client-id <id> --tenant-id <id>
ctd-admin abmelden
```

3 Verbindungsprüfung

Zweck: misst, wie schnell und zuverlässig ein Standort mit SharePoint Online arbeitet, bevor CosyTrack.Drive gekauft bzw. eingeführt wird, und hält eine Ausgangsmessung für den späteren Vergleich fest.

Einsatzzeitpunkt: vor dem Kauf; vor dem Rollout je Standort; bei Leistungsproblemen im Betrieb.

Bedienung: Kachel „Verbindungsprüfung“: Test-Website angeben, Runden (Standard 6, etwa 10 bis 15 Minuten), optional Standort und „Ausgangsmessung speichern“, Start:

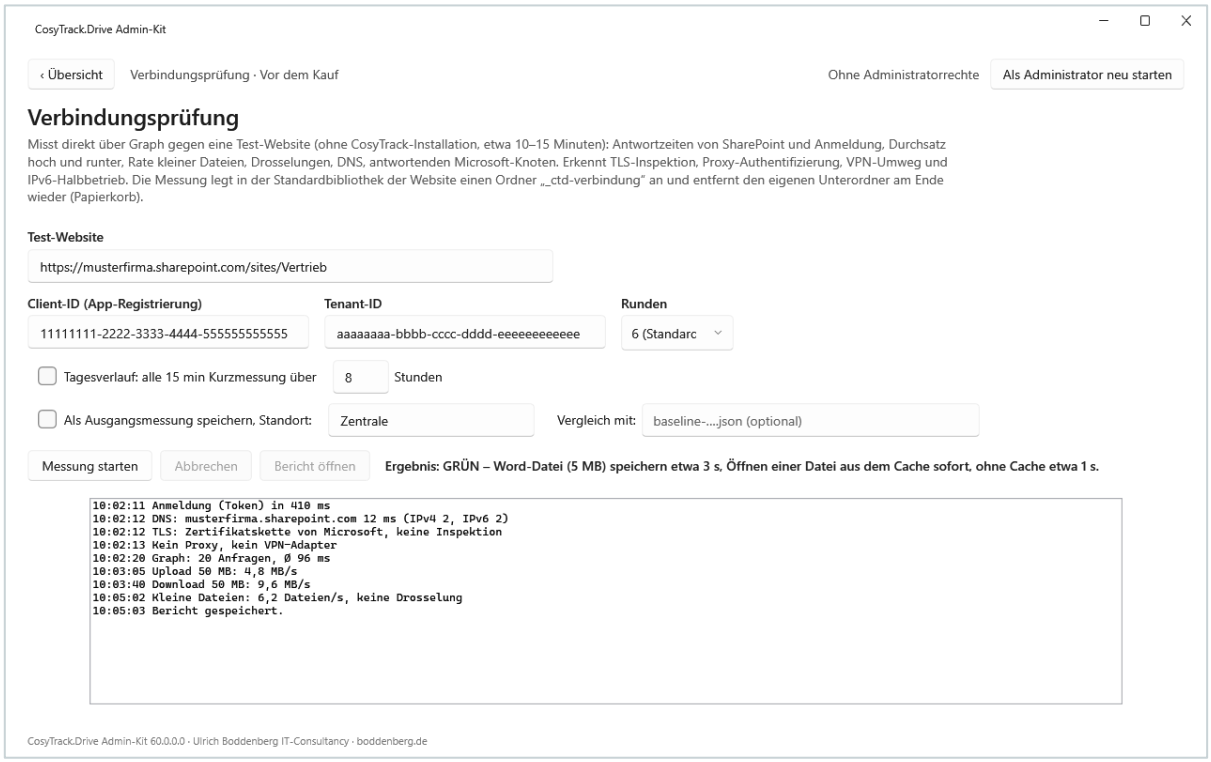


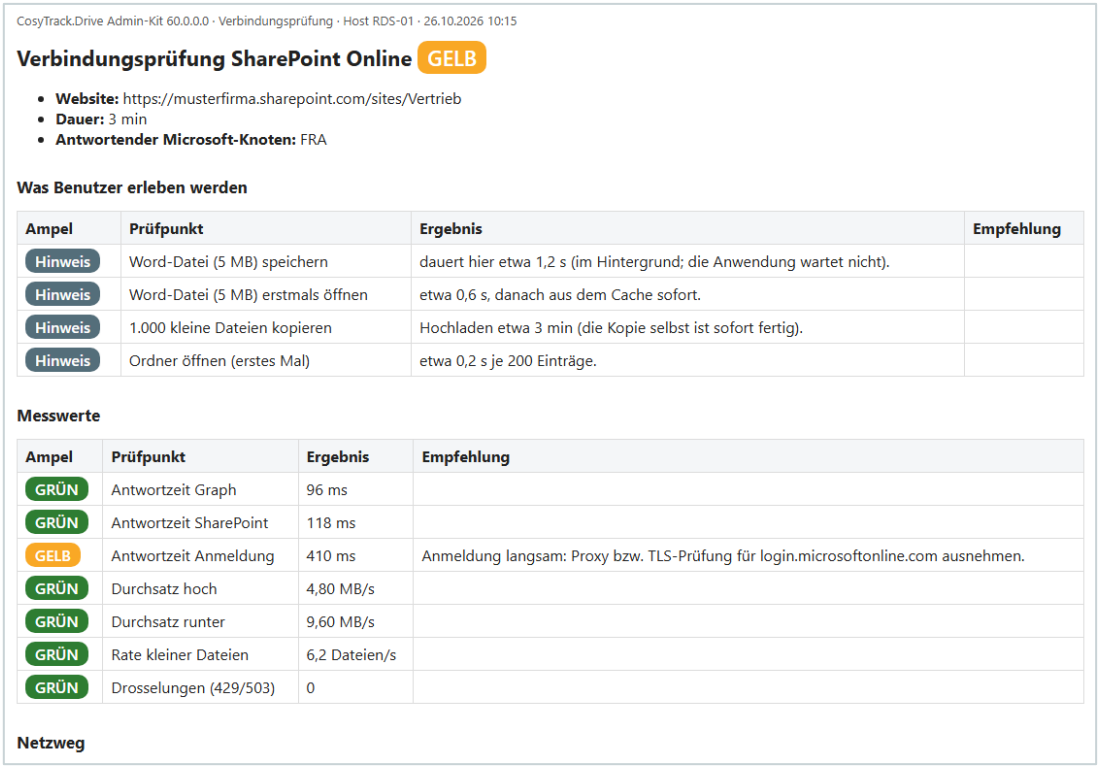
Abbildung 4: Admin-Kit, Verbindungsprüfung

```
ctd-admin verbindung --website https://musterfirma.sharepoint.com/sites/Test [--runden 6]
[--tagesverlauf 8]
                    [--standort Zentrale --baseline-speichern] [--vergleich baseline-
Zentrale.json]
```

Die Prüfung legt in der Standardbibliothek der Website den Ordner `_ctd-verbindung\<Zeit>` an und entfernt den eigenen Unterordner am Ende (Papierkorb). Sie misst Antwortzeiten von Graph, SharePoint und Anmeldung, Durchsatz hoch und runter, die Rate kleiner Dateien, Drosselungen und DNS. Sie erkennt TLS-Inspektion, Proxy-Authentifizierung, VPN-Umwege und IPv6-Halbbetrieb. Das Ergebnis steht in Benutzersprache im Bericht, etwa „Speichern einer 5-MB-Word-Datei dauert hier etwa 1,8 s“.

> **Praxistipp: Ausgangsmessung mit perfmon vergleichen**
> Die Ausgangsmessung (`baseline-<Standort>.json`) verwendet die Namen der Leistungsindikatoren. So lassen sich spätere Messungen mit perfmon bzw. logman direkt vergleichen.

Der Bericht fasst die Messung in Benutzersprache zusammen:



CosyTrack.Drive Admin-Kit 60.0.0.0 · Verbindungsprüfung · Host RDS-01 · 26.10.2026 10:15

Verbindungsprüfung SharePoint Online GELB

- **Website:** https://musterfirma.sharepoint.com/sites/Vertrieb
- **Dauer:** 3 min
- **Antwortender Microsoft-Knoten:** FRA

Was Benutzer erleben werden

Ampel	Prüfpunkt	Ergebnis	Empfehlung
Hinweis	Word-Datei (5 MB) speichern	dauert hier etwa 1,2 s (im Hintergrund; die Anwendung wartet nicht).	
Hinweis	Word-Datei (5 MB) erstmals öffnen	etwa 0,6 s, danach aus dem Cache sofort.	
Hinweis	1.000 kleine Dateien kopieren	Hochladen etwa 3 min (die Kopie selbst ist sofort fertig).	
Hinweis	Ordner öffnen (erstes Mal)	etwa 0,2 s je 200 Einträge.	

Messwerte

Ampel	Prüfpunkt	Ergebnis	Empfehlung
GRÜN	Antwortzeit Graph	96 ms	
GRÜN	Antwortzeit SharePoint	118 ms	
GELB	Antwortzeit Anmeldung	410 ms	Anmeldung langsam: Proxy bzw. TLS-Prüfung für login.microsoftonline.com ausnehmen.
GRÜN	Durchsatz hoch	4,80 MB/s	
GRÜN	Durchsatz runter	9,60 MB/s	
GRÜN	Rate kleiner Dateien	6,2 Dateien/s	
GRÜN	Drosselungen (429/503)	0	

Netzweg

Abbildung 5: Musterbericht der Verbindungsprüfung

4 Bereitschaftscheck

Zweck: prüft einen Zielrechner vor der Einführung bzw. nach Änderungen: Installation, Richtlinien, Speicherorte, Terminalserver und FSLogix, Virenscanner-Ausnahmen, Anmeldung, Lizenz. Jeder Punkt erhält eine Ampel und eine Handlungsempfehlung.

Einsatzzeitpunkt: vor dem Rollout auf jedem Host-Typ; bei der Abnahme; nach Änderungen an Profilen, FSLogix oder Richtlinien.

Bedienung: auf dem Zielrechner ausführen, am besten als Administrator (sonst sind die Defender-Ausnahmen nicht lesbar). Kachel „Bereitschaftscheck“, optional „Host persistent?“, „Tenant-Migration“ und „Mit Anmeldung“ (prüft zusätzlich Zustimmung, Berechtigungen, App-Registrierung und Zielbibliotheken). 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.

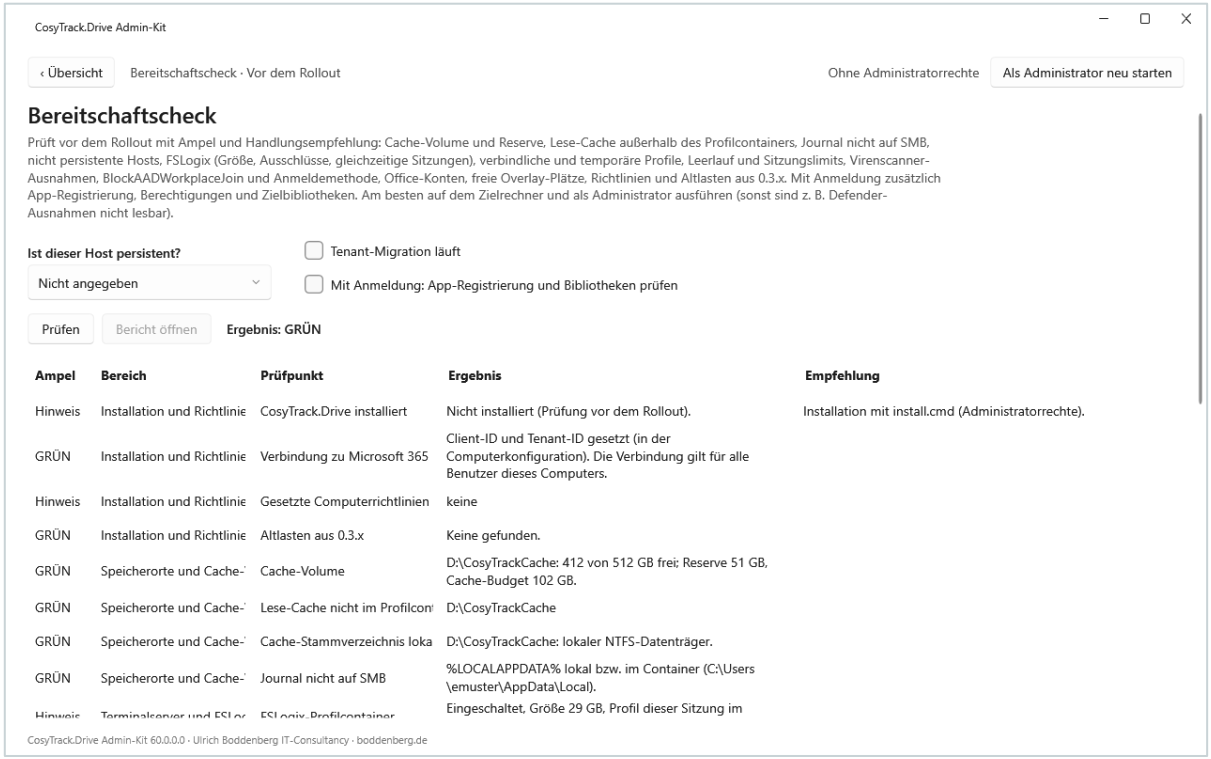


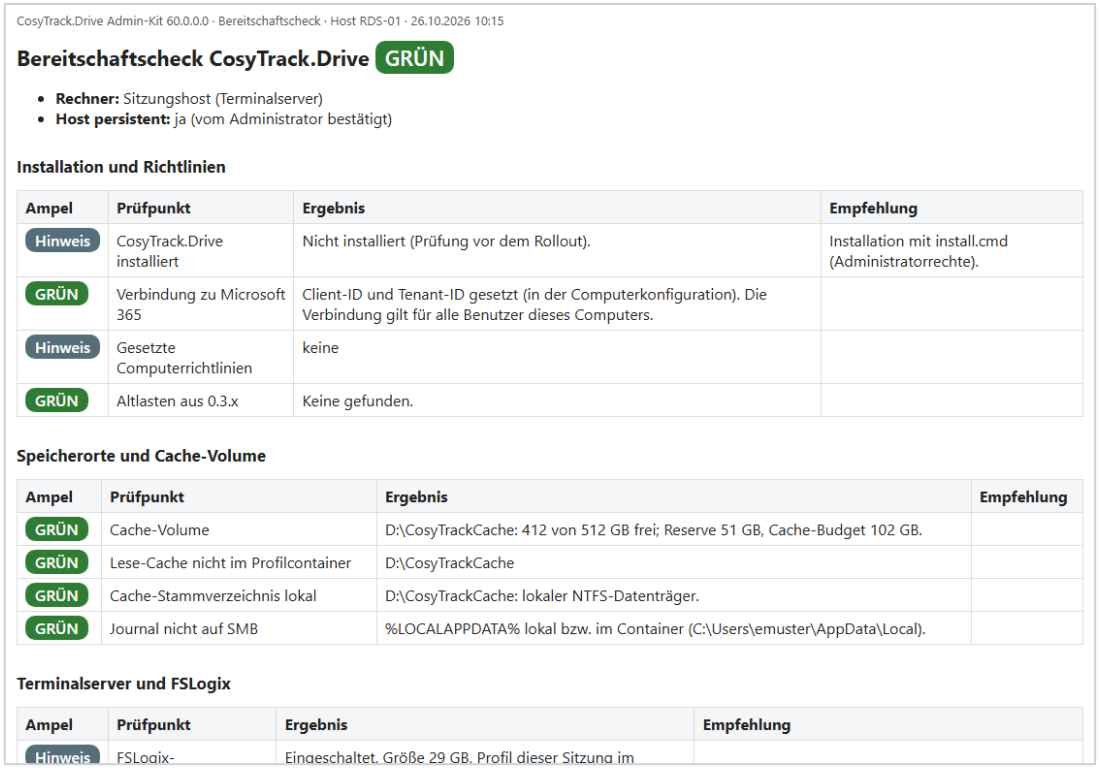
Abbildung 6: Admin-Kit, Bereitschaftscheck

```
ctd-admin bereitschaft [--host-persistent ja|nein] [--migration] [--mit-anmeldung]
```

Rückgabe: 0 grün, 1 gelb, 3 rot.

> **Achtung: Rote Punkte vor dem Rollout beheben**
> Rote Punkte führen im Betrieb zu Störungen oder Datenverlustrisiken. Typisch auf Terminalservern: fehlendes `BlockAADWorkplaceJoin`, `AppData\Local\CosyTrack.Drive` in den FSLogix-Ausschlüssen, Cache-Stammverzeichnis nicht auf lokalem NTFS.

Jeder Punkt des Berichts hat eine Ampel und eine Handlungsempfehlung:



CosyTrack.Drive Admin-Kit 60.0.0.0 · Bereitschaftscheck · Host RDS-01 · 26.10.2026 10:15

Bereitschaftscheck CosyTrack.Drive GRÜN

- **Rechner:** Sitzungshost (Terminalserver)
- **Host persistent:** ja (vom Administrator bestätigt)

Installation und Richtlinien

Ampel	Prüfpunkt	Ergebnis	Empfehlung
Hinweis	CosyTrack.Drive installiert	Nicht installiert (Prüfung vor dem Rollout).	Installation mit install.cmd (Administratorrechte).
GRÜN	Verbindung zu Microsoft 365	Client-ID und Tenant-ID gesetzt (in der Computerkonfiguration). Die Verbindung gilt für alle Benutzer dieses Computers.	
Hinweis	Gesetzte Computerrichtlinien	keine	
GRÜN	Altlasten aus 0.3.x	Keine gefunden.	

Speicherorte und Cache-Volume

Ampel	Prüfpunkt	Ergebnis	Empfehlung
GRÜN	Cache-Volume	D:\CosyTrackCache: 412 von 512 GB frei; Reserve 51 GB, Cache-Budget 102 GB.	
GRÜN	Lese-Cache nicht im Profilcontainer	D:\CosyTrackCache	
GRÜN	Cache-Stammverzeichnis lokal	D:\CosyTrackCache: lokaler NTFS-Datenträger.	
GRÜN	Journal nicht auf SMB	%LOCALAPPDATA% lokal bzw. im Container (C:\Users\emuster\AppData\Local).	

Terminalserver und FSLogix

Ampel	Prüfpunkt	Ergebnis	Empfehlung
Hinweis	FSLogix-	Eingeschaltet. Größe 29 GB. Profil dieser Sitzung im	

Abbildung 7: Musterbericht des Bereitschaftschecks

5 Stresstest

Zweck: belastet ein eingebundenes Laufwerk realitätsnah (Office-Speichermuster, viele kleine Dateien, große Dateien, Umbenennen, Löschen) und prüft am Ende per Graph, dass alles korrekt in SharePoint angekommen ist. Ein grüner Bericht dient als Abnahmeprotokoll.

Einsatzzeitpunkt: Abnahme nach der Einrichtung, auf einem Testlaufwerk mit eigener Testbibliothek.

Bedienung: Kachel „Stresstest“: Profil, Dauer, Laufwerk, Zielordner bzw. Trockenlauf, weitere Parameter; Fortschritt live, Ampel, „Bericht öffnen“:

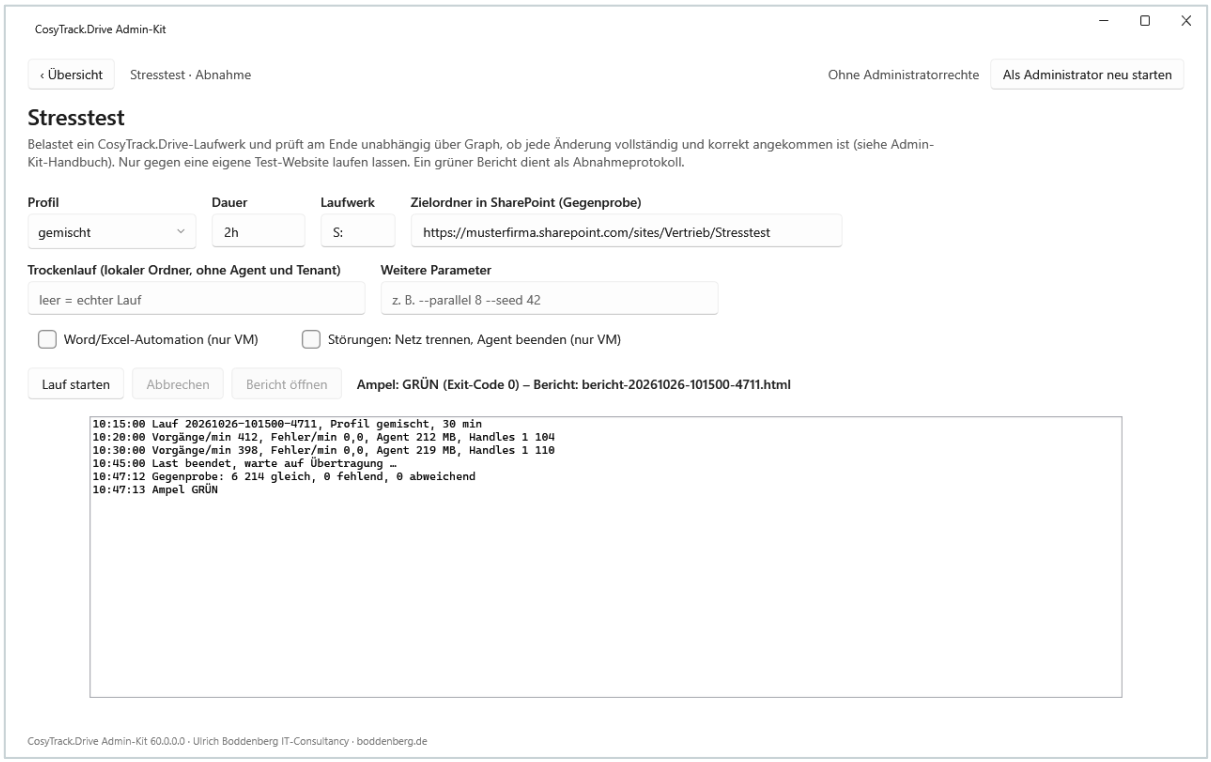
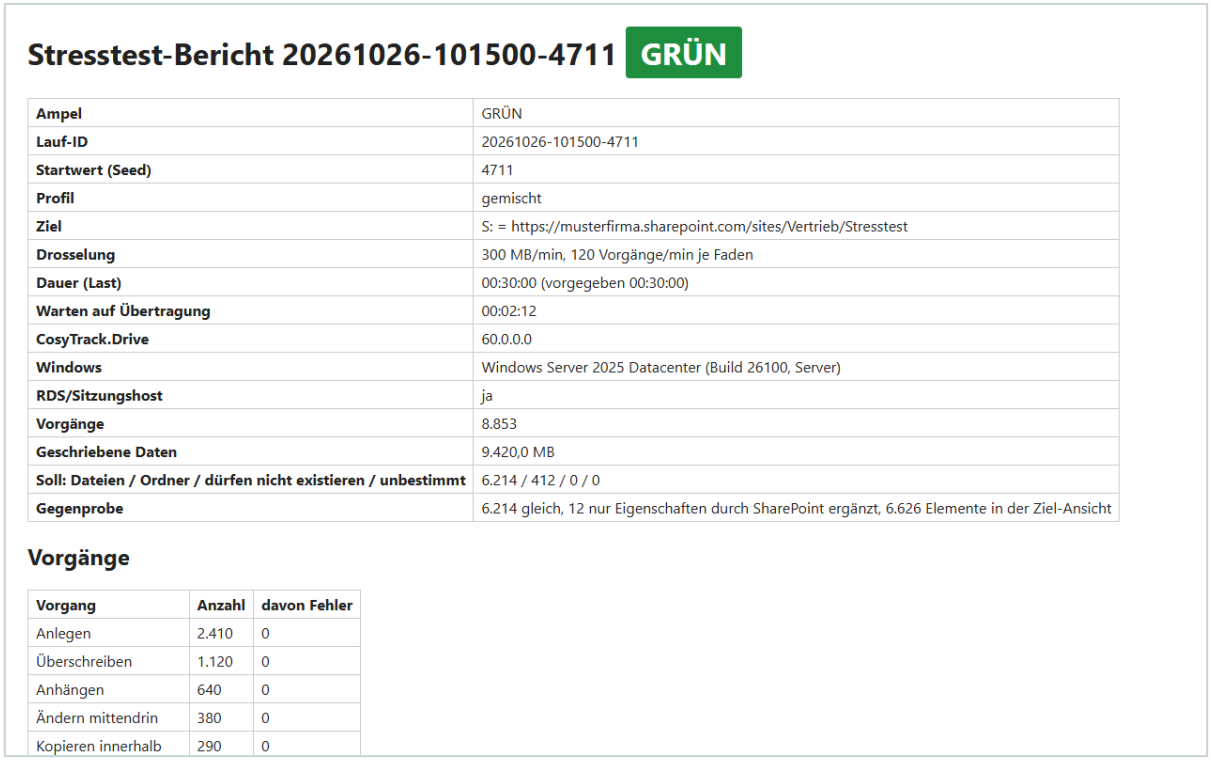


Abbildung 8: Admin-Kit, Stresstest

```
ctd-admin stresstest --profil gemischt --dauer 2h --laufwerk X: --ziel-url
https://musterfirma.sharepoint.com/sites/Test/Freigegebene%20Dokumente/Stresstest
```

> **Achtung: Nur gegen eine Testbibliothek**
> Den Stresstest nur gegen eine Testbibliothek laufen lassen. Störungen (Word, Netztrennung) nur auf einer virtuellen Maschine aktivieren.

Ein grüner Bericht dient als Abnahmeprotokoll:



Stresstest-Bericht 20261026-101500-4711 GRÜN

Ampel	GRÜN
Lauf-ID	20261026-101500-4711
Startwert (Seed)	4711
Profil	gemischt
Ziel	S: = https://musterfirma.sharepoint.com/sites/Vertrieb/Stresstest
Drosselung	300 MB/min, 120 Vorgänge/min je Faden
Dauer (Last)	00:30:00 (vorgegeben 00:30:00)
Warten auf Übertragung	00:02:12
CosyTrack.Drive	60.0.0.0
Windows	Windows Server 2025 Datacenter (Build 26100, Server)
RDS/Sitzungshost	ja
Vorgänge	8.853
Geschriebene Daten	9.420,0 MB
Soll: Dateien / Ordner / dürfen nicht existieren / unbestimmt	6.214 / 412 / 0 / 0
Gegenprobe	6.214 gleich, 12 nur Eigenschaften durch SharePoint ergänzt, 6.626 Elemente in der Ziel-Ansicht

Vorgänge

Vorgang	Anzahl	davon Fehler
Anlegen	2.410	0
Überschreiben	1.120	0
Anhängen	640	0
Ändern mittendrin	380	0
Kopieren innerhalb	290	0

Abbildung 9: Musterbericht des Stresstests

6 Hängende Uploads, Not-Aus, verwaiste Uploads

Zweck: zeigt Änderungen, die sich dauerhaft nicht hochladen lassen, und bietet die bewussten, protokollierten Eingriffe eines Administrators: Not-Aus mit Quarantäne, Wiedereinspielen, Export und Übernahme verwaister Uploads nach einem Hostwechsel.

Einsatzzeitpunkt: Störung im Betrieb; vor dem Abbau bzw. Neuaufbau eines Hosts; vor einer Deinstallation, die wegen ungesendeter Inhalte abbricht.

Bedienung: Kachel „Hängende Uploads“, nur mit erhöhten Rechten. Vor jedem Senden prüft das Admin-Kit den Agent der Zielsitzung (Sitzung, Programmpfad, digitale Signatur). Pfade und Dateinamen erscheinen erst nach „Pfade anzeigen“:

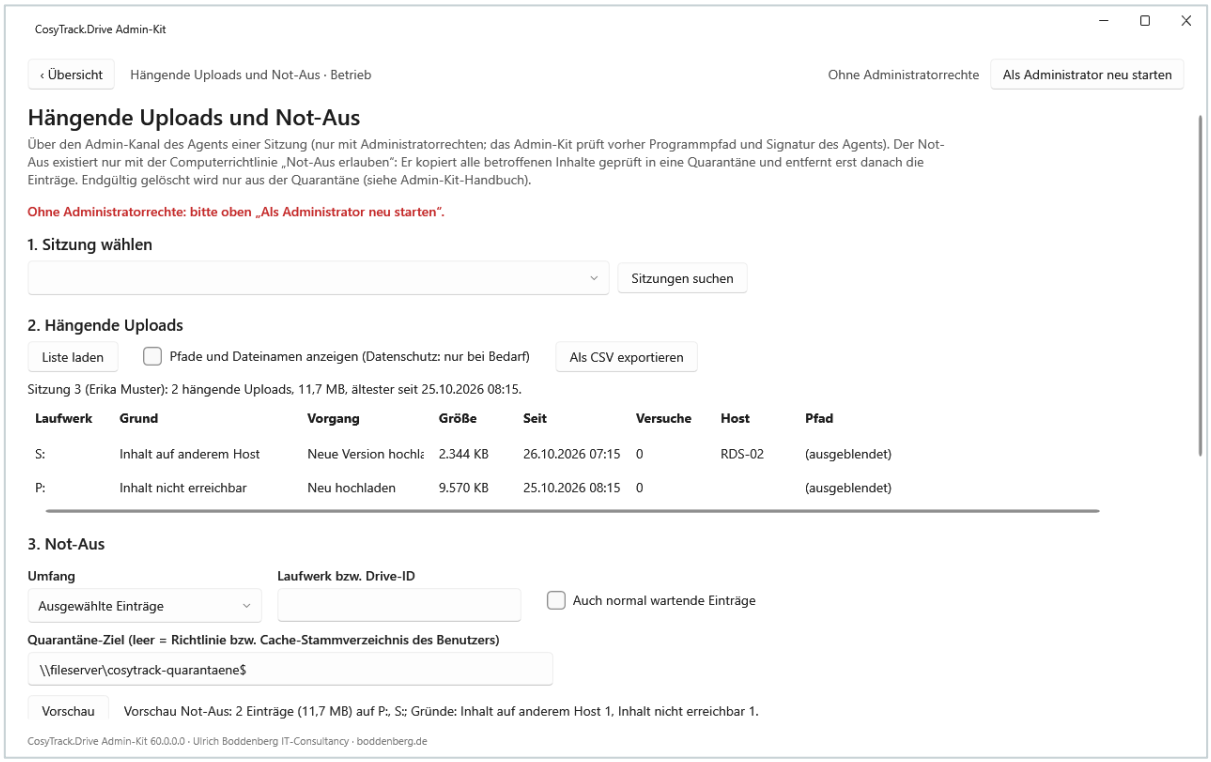


Abbildung 10: Admin-Kit, hängende Uploads

Vor dem Schritt prüfen: Vor einem Not-Aus

- Ursache geklärt (Berechtigung, Ziel gelöscht, Name ungültig) und kein anderer Weg möglich (erneut versuchen, umbenennen, als Kopie speichern).
- Quarantäneordner mit genug Platz festgelegt (Richtlinie „Quarantäne“).
- Vorschau ohne `--bestaetigung` ausgeführt und die Anzahl der Einträge geprüft.
- Begründung, z. B. Ticketnummer, liegt vor.

Die Befehle für Sitzungen, hängende und verwaiste Uploads:

```
ctd-admin sitzungen
ctd-admin haengend --sitzung 3 [--pfade] [--csv liste.csv]
ctd-admin notaus --sitzung 3 --laufwerk P                        # nur Vorschau
ctd-admin notaus --sitzung 3 --laufwerk P --bestaetigung "VERWERFEN 12" --begruendung
"Ticket 4711"
ctd-admin reimport --sitzung 3 --ordner E:\Quarantaene\<SID>\20261019-140000
ctd-admin verwaiste-suchen
ctd-admin verwaiste-exportieren --freigabe \\server\verwaist [--sid <SID>]
ctd-admin verwaiste-importieren --sitzung 3 [--freigabe \\server\verwaist]
```

> **Achtung: Not-Aus erst nach geprüfter Sicherung**
> Der Not-Aus entfernt Einträge erst aus dem Journal, nachdem ihre Inhalte in die Quarantäne kopiert und per Prüfsumme bestätigt sind. Er setzt die Richtlinie „Not-Aus erlauben“, eine Bestätigung mit der Anzahl der Einträge und eine Begründung voraus und schreibt Ereignis 3030. Kein automatischer Vorgang verwirft ungesendete Inhalte.

Ein Export als CSV ohne „Pfade anzeigen“ (Musterdaten) sieht so aus:

```
Laufwerk;Vorgang;Größe;Seit (UTC);Versuche;Grund;Host;Inhalt;Pfad;Fehler
"P";"Upload";2516582;2026-10-19 07:12;14;"Berechtigung fehlt";"RDS01";ja;"";"403
accessDenied"
"P";"Upload";831488;2026-10-19 08:40;9;"Website bzw. Ziel nicht mehr
vorhanden";"RDS01";ja;"";"404 itemNotFound"
```

7 Lizenz und Lizenznutzung

> **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.

> **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.

Zweck: zeigt die Benutzerlizenz des Computers ohne den Schlüssel und liefert für das True-up einen Orientierungswert: „Mindestens N aktive Benutzer in den letzten D Tagen“, daneben die lizenzierte Anzahl. Hintergrund, Historie, Log Analytics, Namensanzeige und „Named User sauber verwalten“ beschreibt das Admin-Handbuch im Kapitel „Lizenznutzung (Admin-Kit)“.

Einsatzzeitpunkt: vor dem Rollout (Lizenz einspielen); im Betrieb als geplante Aufgabe, mindestens alle 30 Tage; vor einem True-up bzw. einer Verlängerung.

Voraussetzungen: Entra ID P1 oder P2 (für Graph), eine eigene App-Registrierung des Admin-Kits (nie die von CosyTrack.Drive), Rolle „Berichtsleser“, „Sicherheitsleser“ oder „Globaler Leser“; für Log Analytics „Log Analytics-Leser“ auf dem Arbeitsbereich.

7.1 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.

7.2 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.

7.3 Bedienung

Kachel „Lizenz und Lizenznutzung“. Ganz oben steht der Hinweis zur Mitbestimmung; er lässt sich nicht ausblenden. Beim ersten Start je Windows-Benutzer erscheint er als Dialog, weiter erst mit „Ich habe den Hinweis gelesen“; die Bestätigung steht mit Zeitpunkt und Windows-Konto im Protokoll des Werkzeugs. Ist das Werkzeug per Richtlinie deaktiviert, ist die Kachel ausgegraut („Durch Richtlinie deaktiviert“).

1. Unter **Einstellungen** Zeitraum (30, 60, 90, 180, 365 Tage oder frei; Standard 90), lizenzierte Named User (falls die Lizenzdatei keine Zahl nennt), Client-ID und Tenant-ID des Admin-Kits und gegebenenfalls die Workspace-ID eintragen. Werte aus Richtlinien sind gesperrt. „Längere Zeiträume erfassen mehr Benutzer mit langen Abwesenheiten, aber nie alle.“
2. **Ermitteln** wählen und im Browser anmelden. **Abbrechen** beendet den Lauf.
3. Ergebnis: die Kennzahl, direkt darunter der Disclaimer, dann Vergleich mit der Lizenz, Quelle, Zeitraum, Zeitpunkt und gegebenenfalls in Orange der Abdeckungshinweis („Daten erst ab …, Zahl kann zu niedrig sein“).
4. **Auswertung speichern** legt die „Auswertung der Lizenznutzung“ ab: Mitbestimmungshinweis und Disclaimer im Kopf, Zahl, Zeitraum, Quelle, Abdeckung, lizenzierte Anzahl, Zeitpunkt, Tenant-ID und ausführendes Konto, ohne Namen.

5. **Namen anzeigen …** erscheint nur mit der Richtlinie „Lizenznutzung: Namensanzeige zulassen“ und verlangt zwei Bestätigungen (Admin-Handbuch).

Ohne Graph-Zugang lässt sich ein Download der Anmeldeprotokolle aus dem Entra-Portal einlesen (**Aus Download des Entra-Portals …**, CSV oder JSON, interaktive und nicht interaktive Anmeldungen); Namen werden daraus nie angezeigt.

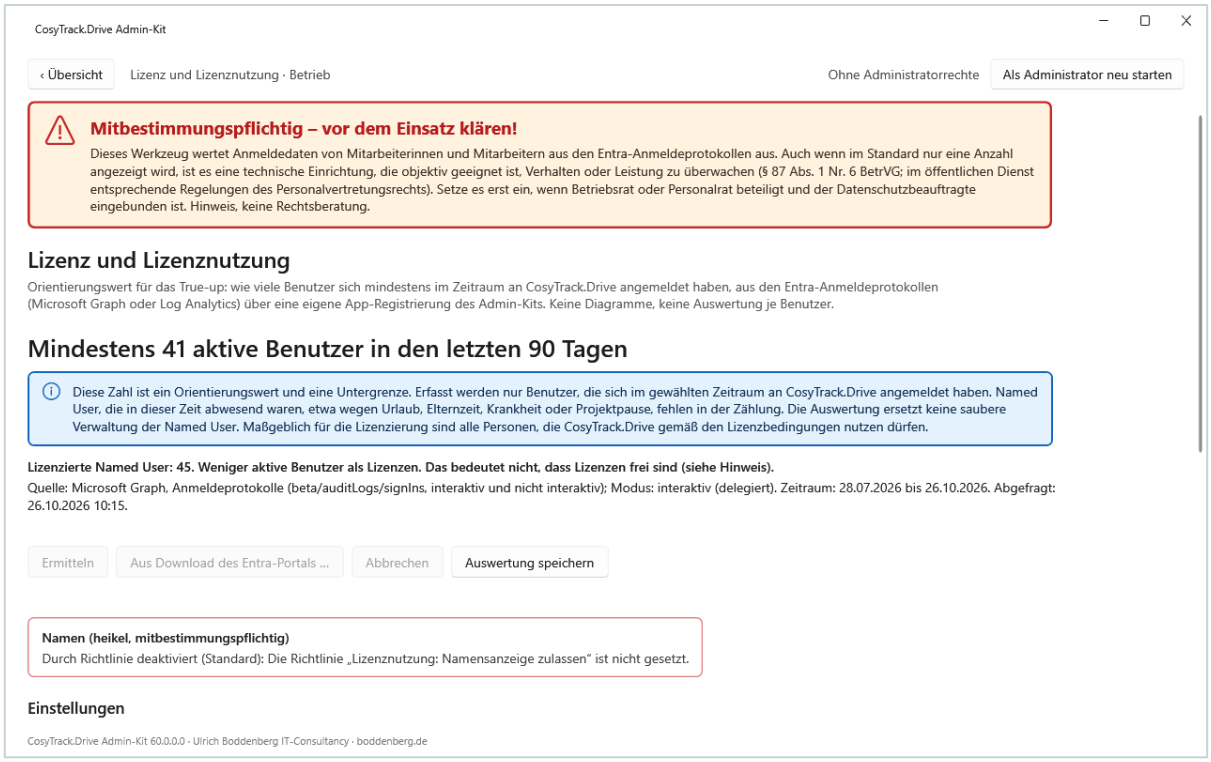


Abbildung 11: Admin-Kit, Lizenz und Lizenznutzung

Die Skizze zeigt, wie gezählt wird:

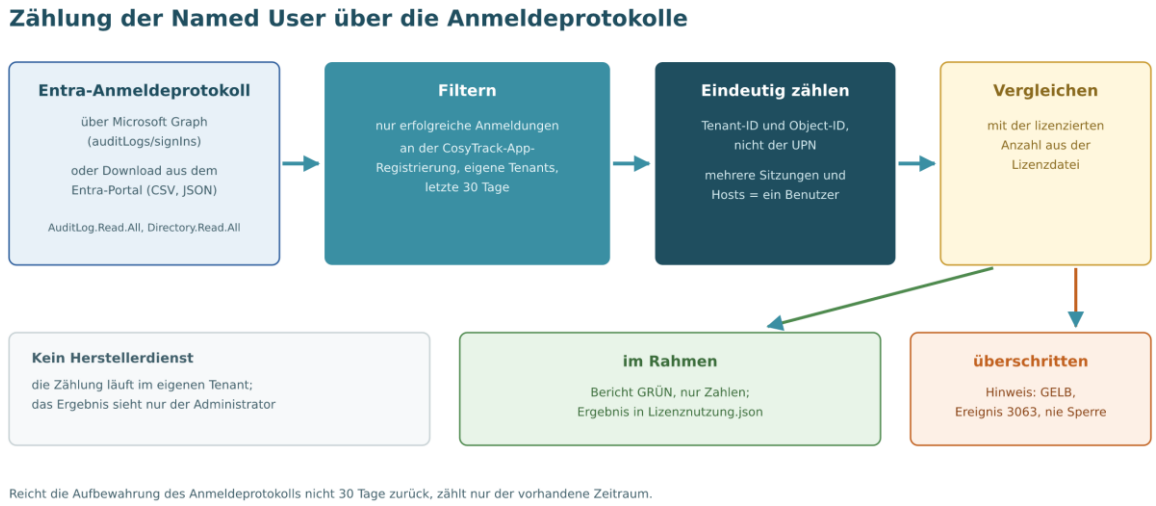


Abbildung 12: Ablauf der Named-User-Zählung über die Anmeldeprotokolle

7.4 Kommandozeile und Rückgabecodes

```
ctd-admin lizenz
```

```
ctd-admin lizenz --import lizenz.ubl          # für alle Benutzer, --nur-benutzer ohne
Administratorrechte
ctd-admin lizenznutzung --interaktiv --hinweis-gelesen --tage 90
ctd-admin lizenznutzung --tage 365 --lizenziert 120 --workspace <Workspace-ID>
ctd-admin lizenznutzung --datei Anmeldeprotokolle.csv
ctd-admin lizenznutzung --unbeaufsichtigt
CosyTrack.Drive.AdminKit.exe --lizenznutzung --unbeaufsichtigt
```

Ohne `--interaktiv` verwendet die Kommandozeile nur eine bereits vorhandene Anmeldung. `--hinweis-gelesen` bestätigt den Hinweis zur Mitbestimmung für das aktuelle Windows-Konto. Namen gibt es an der Kommandozeile nie.

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

Die Auswertung im Muster:

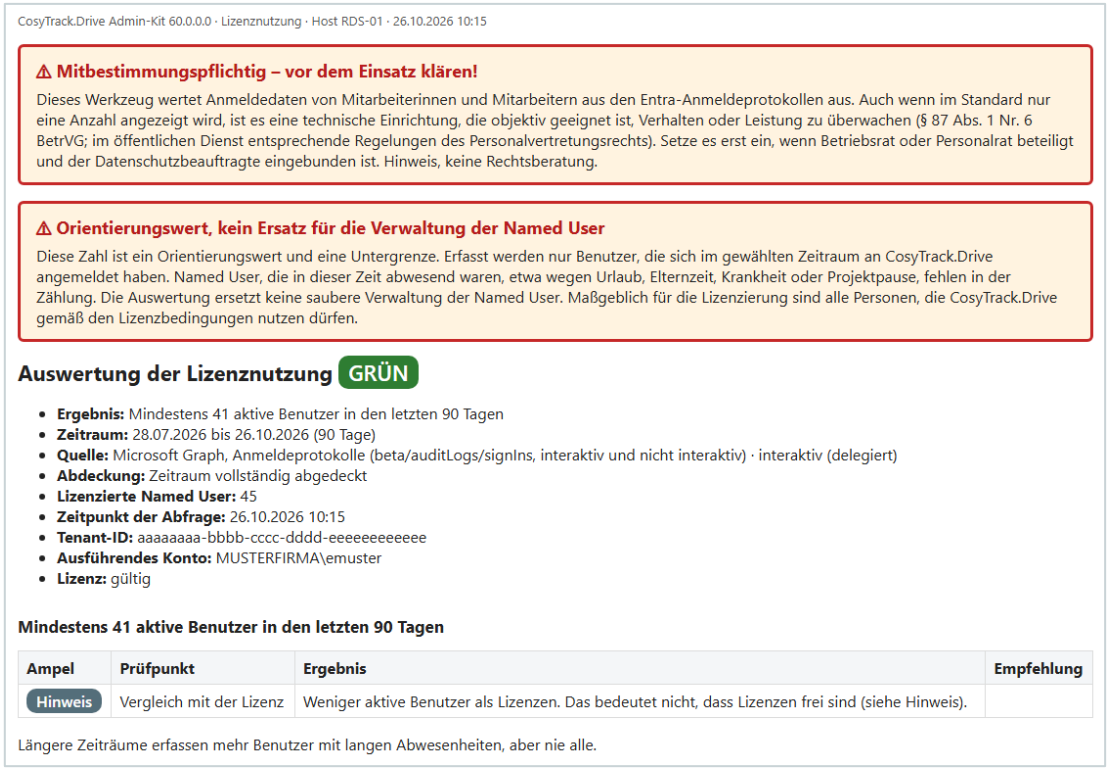


Abbildung 13: Musterauswertung der Lizenznutzung

8 Diagnosepaket

Zweck: sammelt alles für die Fehlersuche in einer anonymisierten Zip-Datei: Versionen, Protokoll, Statistik des Journals (ohne Namen und Inhalte), Richtlinien (Schlüssel nur als „vorhanden“), Kurzlauf des Bereitschaftschecks, Leistungsindikatoren, Ereignisse, Anmeldespuren, Lizenzstand ohne Schlüssel.

Einsatzzeitpunkt: Störung; vor einer Anfrage beim Hersteller bzw. Systemhaus.

Bedienung: Kachel „Diagnosepaket“, ein Klick; mit Administratorrechten für alle Benutzer des Hosts, sonst nur für den eigenen:

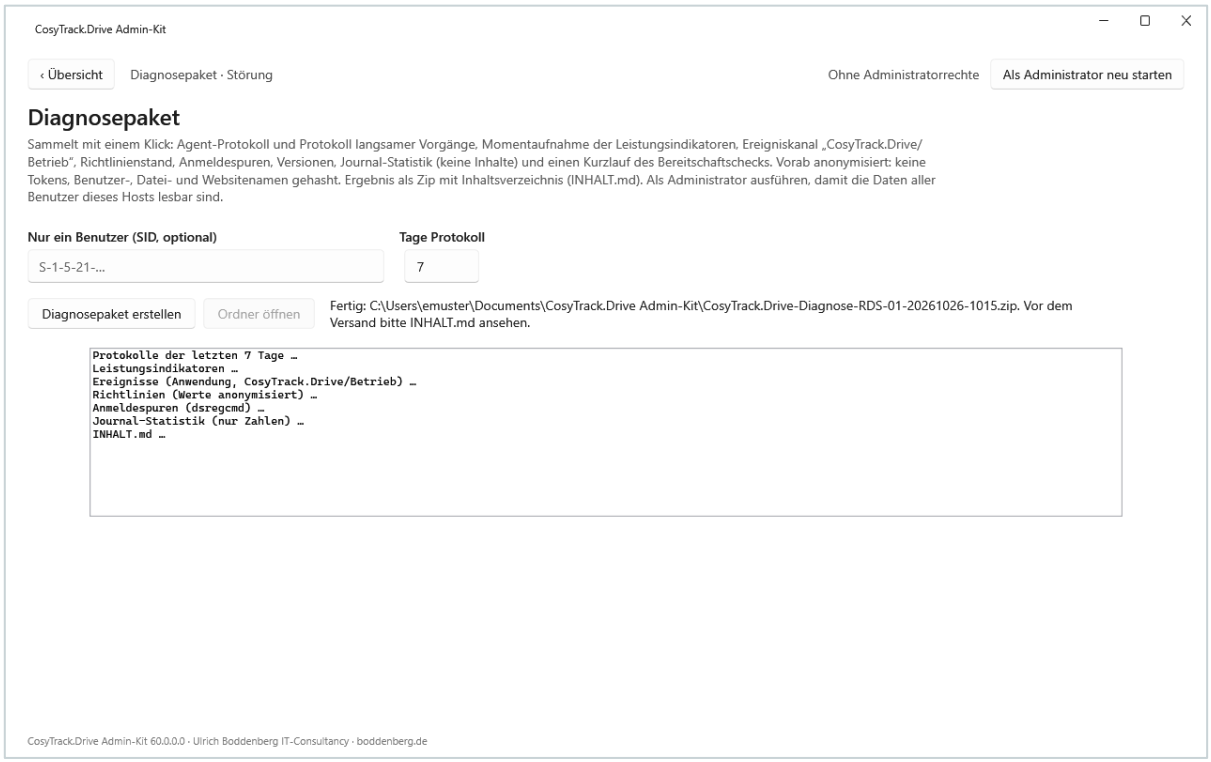


Abbildung 14: Admin-Kit, Diagnosepaket

```
ctd-admin diagnose [--sid <SID>] [--tage 7]
```

Benutzer, Rechner, Pfade, URLs und Kennungen werden vor dem Packen durch Kürzel ersetzt (HMAC-SHA256 mit einem Zufallswert je Paket); gleiche Namen haben im Paket dasselbe Kürzel, sind aber nicht über Pakete hinweg vergleichbar. Das Paket wird nicht versendet; die Weitergabe entscheiden Sie.

Ein Auszug aus der Inhaltsübersicht des Pakets (Musterdaten) zeigt, was es enthält:

Datei	Inhalt
versionen.txt	Versionen der Programmdateien, Windows, .NET
protokoll-1.csv	Agent-Protokoll der letzten 7 Tage (Benutzer #a3f9c1), anonymisiert
journal-statistik-profil-1.txt	Journal-Statistik (Profil), keine Inhalte und keine Namen
lizenz.txt	Benutzerlizenz dieses Computers (Zustand, Lizenz-ID, Daten, Testzeitraum; nie der Schlüssel)
ereignisse-betrieb.txt	Ereigniskanal CosyTrack.Drive/Betrieb (neueste 2000), anonymisiert

> **Achtung: Nur das Diagnosepaket des Admin-Kits weitergeben**
> Das Diagnosepaket der Konfigurations-App ist nicht anonymisiert. Für die Weitergabe an Dritte immer das Diagnosepaket des Admin-Kits verwenden.

9 Vorlagen

Zweck: liefert alles für die Verteilung: ADMX/ADML (deutsch, englisch), Musterrichtlinien `Terminalserver.reg` und `Tenant-Migration.reg`, `logman`-Datensammler für die Leistungsindikatoren, Intune-Paket mit Erkennungsskript, Musterprofilen, Remediations und Compliance-Regel.

Einsatzzeitpunkt: vor dem Rollout.

Bedienung: Kachel „Vorlagen“: Zielordner wählen, „Exportieren“ bzw. „Intune-Paket erstellen“ (das Microsoft Win32 Content Prep Tool gehört nicht zum Admin-Kit und wird angegeben):

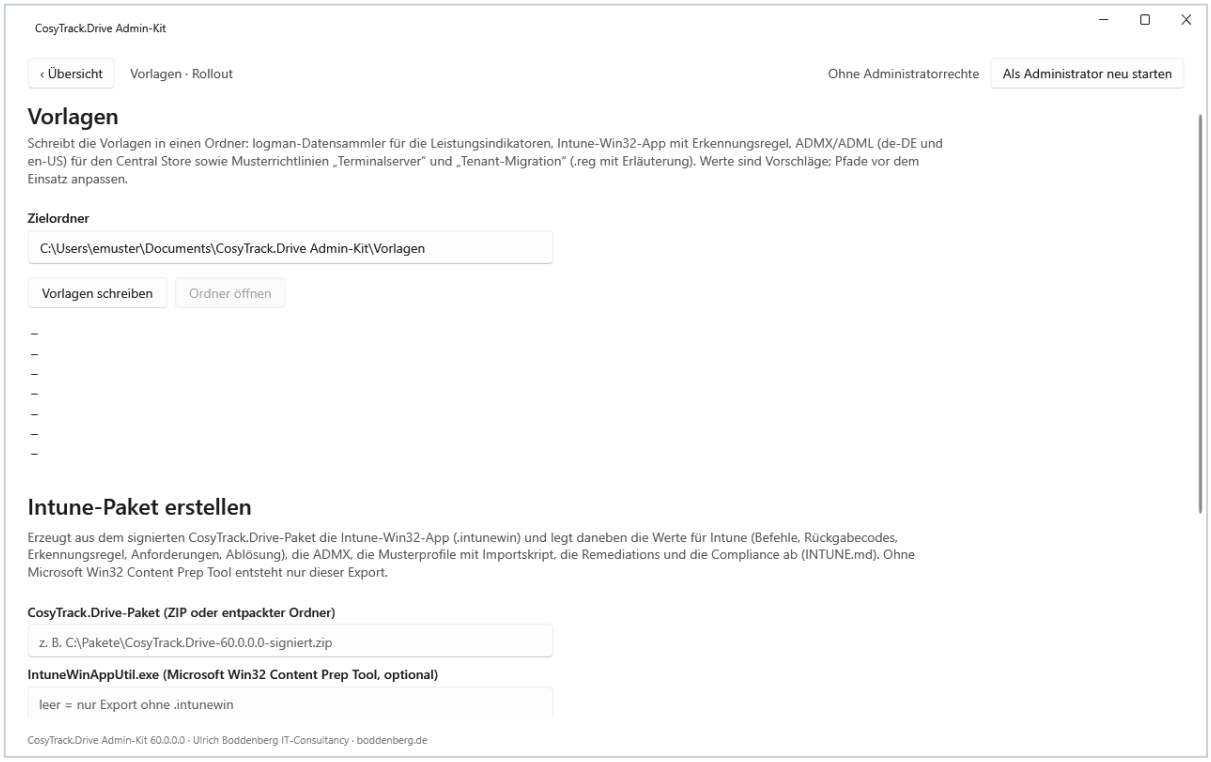


Abbildung 15: Admin-Kit, Vorlagen

```
ctd-admin vorlagen [--ziel <Ordner>]
ctd-admin intune-paket --paket <ZIP|Ordner> [--tool <IntuneWinAppUtil.exe>] [--ziel
<Ordner>]
```

> **Praxistipp: Musterrichtlinie als Vorlage nutzen**
> Die Musterrichtlinie `Terminalserver.reg` dient als Vorlage für die Gruppenrichtlinie. Im Betrieb die Werte über Gruppenrichtlinien setzen, nicht per .reg-Datei.