Ordivis

ORDIVIS TOOLBOX

Administratorhandbuch

Installation, Verteilung, Rechte, Sicherheit und Betrieb.

Produktversion 2026.08.07.001 · Handbuch-Revision 1.0

Stand 28.08.2026 · Plattform Windows 10/11 · .NET 10 · WinUI 3

TB-A

Inhalt

1 Über dieses Handbuch

Dieses Buch beschreibt **Ordivis Toolbox** aus der Sicht derer, die sie **bereitstellen und betreiben**: Es sagt, was die Anwendung auf einem Rechner anlegt, was sie über das Netz spricht, welche Rechte sie wofür braucht, wie man sie an viele Arbeitsplätze verteilt und was zu tun ist, wenn sie sich nicht so verhält wie erwartet.

Es ist der zweite von zwei Bänden.

Band	Kennung	Für wen	Inhalt
Benutzerhandbuch	TB-B	Alle, die die Toolbox bedienen	Alle Werkzeuge, Schritt für Schritt
Administratorhandbuch (dieses Buch)	TB-A	Wer die Toolbox verteilt und betreibt	Installation, Verteilung, Rechte, Datenablage, Sicherheit, Betrieb

Beide Bände stehen unter https://ordivis.eu/dokumentation.html zum Herunterladen bereit.

> **Hinweis:** Was ein einzelnes Werkzeug tut und wie es bedient wird, steht **nicht** in diesem Band. Dieses Buch nennt zu jedem Werkzeug nur, was die Bereitstellung daran angeht: Rechte, Ports, externe Abhängigkeiten, Datenabfluss. Für alles andere gilt das Benutzerhandbuch.

1.1 Wie dieses Buch aufgebaut ist

- **Grundlagen** — Architektur und Systemvoraussetzungen.
- **Bereitstellung** — Installation von Hand, unbeaufsichtigte Verteilung, Upgrade und Deinstallation.
- **Betriebsvoraussetzungen** — Rechte je Werkzeug, Netzwerkanforderungen, Verzeichnisdienst, externe Werkzeuge.
- **Daten und Sicherheit** — was wo abgelegt wird, wie Geheimnisse geschützt sind, was den Rechner verlässt.
- **Betrieb** — Ordivis-Anbindung, Zeitsynchronisation, Protokolle, Fehlersuche, Updates.
- **Anhang** — Schlüsselverzeichnis, Portliste, Befehlsübersicht, Glossar.

1.2 Konventionen und Symbole

Handlungsanweisungen beginnen mit einem **Anleitungskopf**. Er nennt, wo die Handlung stattfindet und welche Rechte sie verlangt:

> ⚙️ **Außerhalb:** Eingabeaufforderung mit erhöhten Rechten · 🔑 **Rechte:** lokaler Administrator

Symbol	Bedeutung
🖥️ **Menü**	Ein Ort im Programmfenster der Toolbox
▸	Trennt die Ebenen eines Menüpfads
🔑 **Rechte**	Welche Berechtigung die Handlung verlangt
⚙️ **Außerhalb**	Ein Handgriff außerhalb der Toolbox (Windows, Konsole, anderes Werkzeug)
🔒 **Pflichtreihenfolge**	Die Schritte müssen genau so und in dieser Folge ablaufen
✅ **Ergebnis**	Was danach zutrifft — die Probe, ob es geklappt hat

Farbige Kästen:

Voraussetzung: Gelb — etwas muss vorher erfüllt sein.

Achtung: Rot — Datenverlust, Betriebsunterbrechung oder ein Sicherheitsrisiko.

Tipp: Grün — spart Arbeit, ist aber nicht nötig.

Hinweis: Blau — eine Ergänzung zum Verständnis.

Weiter gilt:

- *Kursiv* steht für Beschriftungen der Oberfläche.
- `Nichtproportionalschrift` steht für Pfade, Adressen, Registrierungsschlüssel, Befehle, Dateinamen und Schlüsselnamen.

1.3 Stand dieses Buches

Dieses Handbuch beschreibt **Ordivis Toolbox 2026.08.07.001**. Handbuch-Revision 1.0, Stand 28.08.2026.

1.4 Impressum

Ordivis Toolbox ist ein Produkt der Grams IT.

Grams IT · Christian Grams · https://ordivis.eu Anschrift und Kontaktdaten: https://ordivis.eu/impressum.html

Microsoft Corporation.

Die Angaben in diesem Handbuch wurden mit Sorgfalt erstellt. Eine Haftung für Schäden, die aus der Anwendung der beschriebenen Handgriffe entstehen, ist ausgeschlossen, soweit gesetzlich zulässig.

2 Architektur und Systemvoraussetzungen

2.1 Was für ein Programm das ist

Die Ordivis Toolbox ist eine **native Windows-Desktopanwendung**. Keine Weboberfläche, kein Dienst, kein Agent, keine Datenbank, kein Server.

Merkmal	Ausprägung
Oberfläche	WinUI 3 (Windows App SDK)
Laufzeit	.NET 10, **mitgeliefert** — es muss nichts vorinstalliert sein
Auslieferung	Unverpackte EXE mit Inno-Setup-Installationsprogramm; **kein** MSIX, **kein** Store
Architektur	x64; auf ARM64 über die Windows-Emulation
Ausführung	Als angemeldeter Benutzer; einzelne Werkzeuge verlangen Rechteerhöhung
Instanzen	Genau eine je Sitzung (systemweiter Mutex)
Zustand	Ausschließlich Dateien im Benutzerprofil

Wichtig: Es gibt **keinen Hintergrunddienst**. Was die Toolbox misst, misst sie, solange ihr Fenster offen und die betreffende Seite sichtbar ist. Nach dem Beenden läuft nichts weiter, es wird nichts protokolliert und nichts gesendet.

2.1.1 Woraus sie besteht

- Ein Hauptfenster mit Navigationsbereich, Arbeitsfläche und Statusleiste.
- Rund 35 Werkzeugseiten, jede für sich.
- Wenige gemeinsame Dienste: Einstellungen, Übersetzung, Pfade, Prozessaufrufe, Netzabfragen, die Ordivis-Anbindung.
- Eine eingebettete **WebView2**-Komponente für zwei Zwecke: die Kartenansichten und die Anzeige der GPO-Berichte.

2.1.2 Wie sie mit dem System spricht

Die Toolbox macht nichts, wozu Windows nicht ohnehin eine Schnittstelle anbietet. Drei Wege kommen vor:

1. **.NET-Schnittstellen** — Netzwerkstatistik, TCP-Tabelle, ICMP, DNS, Sockets, Zertifikatsspeicher, `System.DirectoryServices` für das Active Directory.
2. **Aufruf von Windows-Werkzeugen** — `powershell.exe`, `cmd.exe`, `dcdiag.exe`, `repadmin.exe`, `certreq.exe`, `tzutil.exe`, `cmdkey.exe`, `mstsc.exe`, `notepad.exe`, `ServerManager.exe`.
3. **Aufruf mitgebrachter Fremdwerkzeuge** — `nmap.exe` und `openssl.exe`, sofern installiert.

Hinweis: Alle externen Aufrufe laufen über eine gemeinsame Naht, die beide Ausgabeströme gleichzeitig leert, den Prozessbaum bei Abbruch und Zeitüberschreitung sicher beendet und den Prozess freigibt. Das ist kein Detail: Wer stdout und stderr nacheinander liest, hängt zuverlässig, sobald ein Werkzeug mehr als die Puffergröße auf stderr schreibt.

2.2 Systemvoraussetzungen

2.2.1 Betriebssystem

Punkt	Anforderung
Windows-Fassung	Windows 10 ab Version 1809 (Build 17763), Windows 11
Server	Windows Server 2019, 2022, 2025 — mit Desktopdarstellung
Architektur	x64 nativ; ARM64 über Emulation
Sprache des Systems	beliebig; die Oberfläche kennt Deutsch und Englisch

Hinweis: Die Toolbox läuft auf einem Server, ist dafür aber nicht gedacht. Ihr Platz ist der Arbeitsplatz oder der Sprungrechner — dort, wo das zu untersuchende Netz erreichbar ist.

2.2.2 Hardware

Punkt	Empfehlung
Arbeitsspeicher	4 GB frei; bei großen Scans und dem Sicherheits-Check mehr
Plattenplatz	rund 350 MB für die Installation, wenige Megabyte im Benutzerprofil
Bildschirm	ab 1280 × 920 Punkten; das Fenster öffnet in dieser Größe
Skalierung	DPI-fähig je Bildschirm (PerMonitorV2)

2.2.3 Mitgelieferte Bestandteile

Die Installation bringt mit:

- die Anwendung selbst,
- die **.NET-10-Laufzeit** (selbstenthaltend),
- das **Windows App SDK / WinUI 3** (selbstenthaltend),
- die Programmsymbole.

> **Voraussetzung:** Nicht mitgeliefert wird die **WebView2-Laufzeit**. Sie ist auf Windows 11 und auf gepflegten Windows-10-Systemen bereits vorhanden (Microsoft liefert sie mit Edge aus). Fehlt sie, arbeitet die Toolbox weiter — nur die Kartenansichten und die GPO-Berichtsanzeige bleiben leer. Siehe Kapitel *Externe Werkzeuge und Abhängigkeiten*.

2.2.4 Nicht vorausgesetzt

Ausdrücklich **nicht** nötig sind:

- eine vorinstallierte .NET-Laufzeit,
- eine Datenbank,
- ein Server, ein Dienst oder ein Agent,
- eine Lizenzdatei, ein Schlüssel oder eine Aktivierung,
- eine Anmeldung an einem Konto,
- eine Internetverbindung für den Kernbetrieb.

2.3 Lizenz und Bezug

Die Ordivis Toolbox ist **kostenlos** und ohne Aktivierung nutzbar. Es gibt keine Funktion, die hinter einer Bezahlschranke liegt, und keinen Zwang zur Registrierung.

Bezug: https://ordivis.eu/toolbox/

Die Datei heißt `Ordivis-Toolbox-Setup-<Version>.exe`, wobei `<Version>` der Auslieferungsstand im Schema `JJJJ.MM.TT.NNN` ist.

2.4 Betrieb ohne Internetzugang

Die Toolbox arbeitet in einem abgeschotteten Netz weitgehend vollständig. Was dann nicht geht:

Betroffen	Folge
Speedtest	Meldet, dass kein Testserver erreichbar ist
Standortangaben und Kartenansichten	Bleiben leer; die übrigen Ergebnisse der Seite stehen
MAC Scanner, manuelle Suche	Meldet Zeitüberschreitung — die eigenen Karten und die Anreicherung im IP Scanner werden **ohne Netz** aufgelöst
WHOIS Abfrage	Keine Antwort
Sicherheits-Check (CVE & WID)	Keine Antwort
Statusanzeige *DNS* auf dem Dashboard	Dauerhaft rot — sie prüft `1.1.1.1`

Betroffen	Folge
Nachinstallation von Nmap, OpenSSL und RSAT	Nicht möglich; die Werkzeuge müssen auf dem üblichen Weg bereitgestellt werden

Alles andere — Netzabfragen, Scanner, Active Directory, PKI, Dienste, Zeitprüfung gegen einen internen Server, Ordivis-Anbindung an einen internen Endpunkt — arbeitet unverändert.

3 Installation

3.1 Was das Installationsprogramm tut

Das Installationsprogramm ist ein **Inno-Setup-Paket**. Es legt an:

Was	Wo
Programmdateien	`C:\Program Files\Grams IT\Ordivis Toolbox`
Startmenü-Eintrag	*Ordivis Toolbox*
Desktop-Verknüpfung	Nur auf Wunsch (Vorgabe: **aus**)
Deinstallationseintrag	`HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{D3F8A9C1-7B2E-45A6-9012-3456789ABCDE}_is1`

Es legt **nicht** an: einen Dienst, eine geplante Aufgabe, einen Autostart-Eintrag, eine Firewall-Regel, einen Treiber, einen Dateizuordnungs- oder Protokoll-Handler.

Voraussetzung: Die Installation braucht **lokale Administratorrechte**, weil sie nach `Program Files` schreibt. Die *Benutzung* der Toolbox braucht sie nicht.

3.2 Installation von Hand

⚙️ **Außerhalb:** Windows-Installationsassistent · 🔑 **Rechte:** lokaler Administrator

1. Laden Sie `Ordivis-Toolbox-Setup-<Version>.exe` von https://ordivis.eu/toolbox/.
2. Starten Sie die Datei und bestätigen Sie die UAC-Rückfrage.
3. Wählen Sie die Sprache des Installationsprogramms — **Deutsch** oder **Englisch**. Diese Wahl betrifft nur den Installationsvorgang, nicht die Oberfläche des Programms.
4. Bestätigen oder ändern Sie den Zielordner.
5. Entscheiden Sie über die Desktop-Verknüpfung.
6. *Installieren*.

✅ **Ergebnis:** Das Programm steht im Startmenü. Am Ende bietet der Assistent an, es zu starten.

3.3 Upgrade

Ein Upgrade ist ein gewöhnlicher Lauf des neuen Installationsprogramms über die vorhandene Installation. Inno Setup erkennt sie an der Anwendungskennung und ersetzt die Dateien.

Hinweis: Einstellungen, gespeicherte Verbindungen, das Prüfprotokoll des AD-Managers und die Ordivis-Anbindung liegen im **Benutzerprofil** und werden von einem Upgrade nicht angefasst.

Voraussetzung: Die Toolbox muss beendet sein. Läuft sie noch, kann Inno die EXE nicht ersetzen.

3.3.1 Upgrade von der Vorgängerinstallation unter dem Namen „NetzDesk"

Bis August 2026 hieß das Programm **NetzDesk**. Das Installationsprogramm nimmt dieser Umbenennung ihre Fallstricke ab — es ist hilfreich zu wissen, wie:

1. Es installiert **immer** nach `…\Grams IT\Ordivis Toolbox`, auch wenn in der Registrierung noch der alte Pfad steht. Ohne diesen Griff landete das Programm weiterhin unter `…\Grams IT\NetzDesk`, während überall sonst der neue Name steht.
2. Damit daraus keine **zweite** Installation wird, entfernt es die alte zuerst still (`/VERYSILENT`) und wartet, bis deren Aufräumlauf durch ist.
3. Liegt die alte Installation bereits am neuen Ort, gilt der gewöhnliche Upgrade-Weg. Dateien unter dem alten Namen — `NetzDesk.exe`, `NetzDesk.dll`, die zugehörigen Begleitdateien, die Verknüpfungen im Startmenü und auf dem Desktop — werden dabei ausdrücklich entfernt. Inno räumt sonst nichts weg, was es diesmal nicht mitbringt; zurück bliebe eine startbare, veraltete `NetzDesk.exe`.

Achtung: Lässt sich die alte Installation nicht entfernen, **bricht das Setup sichtbar ab** statt zwei Installationen zu hinterlassen. Die Meldung nennt den Pfad. Deinstallieren Sie *NetzDesk* dann über *Windows-Einstellungen* ▸ *Apps* und starten Sie das Setup erneut.

Hinweis: Die Benutzerdaten ziehen **von selbst** um. Sie lagen unter `%LOCALAPPDATA%\NetzDesk` und werden beim ersten Start nach `%LOCALAPPDATA%\OrdivisToolbox` **verschoben** — genau einmal, und gutmütig: Scheitert der Umzug, weil eine Datei noch offen ist, arbeitet das Programm am alten Ort weiter und versucht es beim nächsten Start erneut. Näheres im Kapitel *Datenablage und Konfiguration*.

3.4 Deinstallation

⚙ **Außerhalb:** *Windows-Einstellungen* ▸ *Apps* ▸ *Installierte Apps* · 🔑 **Rechte:** lokaler Administrator

1. *Ordivis Toolbox* suchen, *Deinstallieren*.
2. UAC bestätigen.

Wichtig: Die Deinstallation entfernt die **Programmdateien**. Sie entfernt **nicht** den Datenordner im Benutzerprofil. Dort bleiben Einstellungen, das verschlüsselte AD-Kennwort, der Ordivis-Token, die gespeicherten Remote-Verbindungen samt Kennwörtern und die Protokolle liegen.

Für eine restlose Entfernung — etwa beim Rückgeben eines Geräts — muss der Datenordner je Benutzerprofil zusätzlich gelöscht werden:

```
%LOCALAPPDATA%\OrdivisToolbox
```

Und, falls ein Umzug aus der Zeit vor der Umbenennung nie stattfand:

```
%LOCALAPPDATA%\NetzDesk
```

Achtung: Der Ordner liegt **je Benutzerprofil**. Auf einem Rechner mit mehreren Benutzern muss er in jedem Profil entfernt werden. Wie das unbeaufsichtigt geht, steht im Kapitel *Verteilung im Netz*.

4 Verteilung im Netz

Das Installationsprogramm ist ein Inno-Setup-Paket und versteht dessen Befehlszeilenschalter. Damit lässt es sich unbeaufsichtigt über jedes gängige Verteilverfahren ausbringen.

4.1 Unbeaufsichtigte Installation

⚙️ **Außerhalb:** Eingabeaufforderung oder Verteilsystem · 🔑 **Rechte:** lokaler Administrator (bzw. `SYSTEM`)

Die knappste Form:

```
Ordivis-Toolbox-Setup-2026.08.07.001.exe /VERYSILENT /SUPPRESSMSGBOXES /NORESTART
```

Die brauchbaren Schalter im Einzelnen:

Schalter	Wirkung
`/SILENT`	Fortschrittsfenster, keine Rückfragen
`/VERYSILENT`	Gar keine Anzeige
`/SUPPRESSMSGBOXES`	Unterdrückt Meldungsfenster; nur zusammen mit `/SILENT` oder `/VERYSILENT` sinnvoll
`/NORESTART`	Kein Neustart, auch wenn das Setup einen für nötig hielte
`/LANG=german`	Sprache des Installationsvorgangs (`german` oder `english`)
`/DIR="C:\Pfad"`	Abweichender Zielordner
`/TASKS="desktopicon"`	Legt zusätzlich eine Desktop-Verknüpfung an
`/MERGETASKS="!desktopicon"`	Vorhandene Aufgabenauswahl beibehalten, Desktop-Symbol abwählen
`/LOG="C:\Temp\toolbox-setup.log"`	Schreibt ein Installationsprotokoll
`/NOCANCEL`	Nimmt dem Benutzer die Abbruchmöglichkeit

Eine vollständige Zeile, wie sie in einem Verteilsystem stehen kann:

```
Ordivis-Toolbox-Setup-2026.08.07.001.exe /VERYSILENT /SUPPRESSMSGBOXES /NORESTART
/NOCANCEL /LANG=german /LOG="C:\Windows\Temp\ordivis-toolbox-setup.log"
```

Voraussetzung: Die Toolbox darf beim Upgrade **nicht laufen**. Verteilen Sie außerhalb der Arbeitszeit, oder beenden Sie den Prozess `OrdivisToolbox.exe` vorher.

Achtung: Beim Upgrade von einer Installation unter dem alten Namen *NetzDesk* deinstalliert das Setup diese zuerst still. Das dauert einige Sekunden länger als eine gewöhnliche Installation — setzen Sie die Zeitgrenze Ihres Verteilsystems nicht zu knapp. Scheitert die Entfernung, **bricht das Setup ab** und meldet einen Fehler; das ist Absicht und keine Störung, der man mit einem Wiederholungslauf begegnet.

4.2 Unbeaufsichtigte Deinstallation

🔑 **Rechte:** lokaler Administrator

Der Pfad zum Deinstallationsprogramm steht in der Registrierung. Aus PowerShell:

```
$k = 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{D3F8A9C1-7B2E-45A6-9012-3456789ABCDE}_is1'
$exe = (Get-ItemProperty $k -ErrorAction SilentlyContinue).UninstallString
if ($exe) { Start-Process $exe.Trim('"') -ArgumentList '/VERYSILENT','/SUPPRESSMSGBOXES','/NORESTART' -Wait }
```

Die Anwendungskennung `{D3F8A9C1-7B2E-45A6-9012-3456789ABCDE}` ist über alle Fassungen hinweg gleich — auch über die Umbenennung hinweg. Sie ist deshalb der verlässliche Anker für Erkennung und Deinstallation.

4.2.1 Restlose Entfernung samt Benutzerdaten

Die Deinstallation lässt den Datenordner im Benutzerprofil stehen (siehe Kapitel *Installation*). Zum vollständigen Entfernen über alle Profile hinweg:

```
# Nach der Deinstallation, mit Administratorrechten.
Get-ChildItem 'C:\Users' -Directory | ForEach-Object {
    foreach ($n in 'OrdivisToolbox','NetzDesk') {
        $p = Join-Path $_.FullName "AppData\Local\$n"
        if (Test-Path $p) { Remove-Item $p -Recurse -Force -ErrorAction SilentlyContinue }
    }
}
```

Achtung: Damit sind auch die gespeicherten Remote-Verbindungen samt Kennwörtern, das hinterlegte AD-Konto und der Ordivis-Token fort. Auf einem Gerät, das weiterbenutzt wird, ist das selten gewollt.

4.3 Erkennung im Verteilsystem

Für Verteilsysteme, die vor der Installation prüfen, ob das Produkt schon da ist:

Verfahren	Wert
Registrierungsschlüssel	`HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{D3F8A9C1-7B2E-45A6-9012-3456789ABCDE}_is1`
Wert für den Versionsvergleich	`DisplayVersion` (Schema `JJJJ.MM.TT.NNN`)
Datei	`C:\Program Files\Grams IT\Ordivis Toolbox\OrdivisToolbox.exe`

Ein Erkennungsskript, das auch die Version prüft:

```
$k = 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{D3F8A9C1-7B2E-45A6-9012-3456789ABCDE}_is1'
$v = (Get-ItemProperty $k -ErrorAction SilentlyContinue).DisplayVersion
if ($v -and [version]($v -replace '^(\d+)\.(\d+)\.(\d+)\.(\d+)$','$1.$2.$3.$4') -ge [version]'2026.8.7.1') { 'Installed' }
```

Hinweis: Die angezeigte Version trägt **führende Nullen** (`2026.08.07.001`), die Dateiversion nicht (`2026.8.7.1`). Wer Zeichenketten vergleicht, muss darauf achten; wer nach `[version]` wandelt, ist auf der sicheren Seite.

4.4 Verteilung über Intune

1. Wandeln Sie das Setup in ein `.intunewin`-Paket (*Microsoft Win32 Content Prep Tool*).
2. Installationsbefehl: `Ordivis-Toolbox-Setup-<Version>.exe /VERYSILENT /SUPPRESSMSGBOXES /NORESTART`
3. Deinstallationsbefehl: das Deinstallationsprogramm aus dem Registrierungsschlüssel oben, mit denselben Schaltern.
4. Erkennungsregel: Registrierungsschlüssel wie oben, Wert `DisplayVersion`, Vergleich *größer oder gleich*.
5. Installationsverhalten: **System**.
6. Anforderungen: 64 Bit, Windows 10 1809 oder neuer.

4.5 Verteilung über eine Gruppenrichtlinie

Wichtig: Eine Softwareverteilung per Gruppenrichtlinie (*Softwareinstallation*) setzt ein **MSI**-Paket voraus. Das Setup der Toolbox ist eine EXE — dieser Weg steht also nicht offen.

Der gangbare Weg über Gruppenrichtlinien ist ein **Startskript** (Computerstart, läuft als `SYSTEM`), das die Installation ausführt, wenn die gewünschte Version noch nicht vorliegt:

```
$quelle  = '\\dateiserver\software$\OrdivisToolbox\Ordivis-Toolbox-Setup-
2026.08.07.001.exe'
$sollVer = '2026.08.07.001'
$k = 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{D3F8A9C1-7B2E-45A6-9012-
3456789ABCDE}_is1'

if ((Get-ItemProperty $k -ErrorAction SilentlyContinue).DisplayVersion -ne $sollVer) {
    Start-Process $quelle -ArgumentList '/VERYSILENT','/SUPPRESSMSGBOXES','/NORESTART' -
Wait
}
```

Voraussetzung: Das Computerkonto braucht Leserecht auf die Freigabe — bei Startskripten läuft der Zugriff unter dem **Computerkonto**, nicht unter dem des Benutzers.

4.6 Einstellungen vorbelegen

Die Toolbox liest ihre Einstellungen aus einer JSON-Datei im Benutzerprofil. Es gibt **keine** Gruppenrichtlinien-Vorlage und keine maschinenweite Vorgabe.

Vorbelegen lässt sich trotzdem — über ein Anmeldeskript, das die Datei anlegt, wenn sie noch nicht existiert. Welche Schlüssel es gibt, steht im Kapitel *Datenablage und Konfiguration*; ein vollständiges Beispiel steht dort ebenfalls.

Achtung: Vorbelegen Sie **niemals** die verschlüsselten Felder (`AdPasswordProtected` , `InfraDeskTokenProtected`). Sie sind an Benutzerkonto und Rechner gebunden und auf einem anderen Rechner wertlos. Ein zentral verteilter Wert wäre entweder unbrauchbar — oder, wenn er im Klartext danebenläge, ein Kennwort in einer Skriptdatei.

5 Rechte und Berechtigungen

Die Toolbox verlangt **keine** besonderen Rechte, um zu starten. Was Rechte verlangt, ist das einzelne Werkzeug — und zwar in drei voneinander unabhängigen Dimensionen:

1. **Lokale Rechte** auf dem Rechner, auf dem die Toolbox läuft.
2. **Rechte auf dem Ziel**, wenn ein Werkzeug entfernt arbeitet.
3. **Rechte im Verzeichnisdienst** für die Active-Directory-Werkzeuge.

Dieses Kapitel führt sie je Werkzeug zusammen.

5.1 Lokale Rechte

5.1.1 Was ohne Administratorrechte geht

Der weitaus größte Teil. Alle rein abfragenden Werkzeuge — Netzabfragen, DNS, Zertifikatsprüfung, Subnetzrechner, E-Mail-Analyse, WHOIS, Wake on LAN, Zeitprüfung — arbeiten als gewöhnlicher Benutzer vollständig.

5.1.2 Was Administratorrechte verlangt

Werkzeug / Funktion	Warum
Pakete (Live) — Mitschnitt	Windows vergibt Rohsockets nur an erhöhte Prozesse
Service & Process Controller	Dienste steuern und Prozesse beenden ist eine geschützte Handlung
Windows HOSTS, Speichern	Die Datei liegt in einem geschützten Systemverzeichnis
IP Scanner mit `-sS` oder `-O`	Nmap braucht dafür Rohsockets
AD Diagnose: `dcdiag`, `repadmin`	Die Werkzeuge selbst verlangen es
AD Diagnose: RSAT installieren/entfernen	Windows-Features ändern
AD Suche: BitLocker und LAPS	Die Attribute sind lesegeschützt
DHCP: Adresse erneuern	Eingriff in die Netzwerkkonfiguration
NTP: Zeit oder Zeitzone setzen	Systemweite Änderung
Verbindungen / Dashboard: Prozessnamen	Windows nennt fremde Prozesse sonst nicht
System Inspector lokal, vollständig	Treiberliste und fremde Prozesse

5.1.3 Wie die Rechte angefordert werden

Zwei Wege, und der Unterschied ist wichtig:

Dauerhaft — *Einstellungen* ▸ *Systemverhalten & Berechtigungen* ▸ *Immer als Administrator ausführen*. Der Schalter wird in der Einstellungsdatei vermerkt (`RunAsAdmin`). Bei jedem Start prüft die Anwendung, ob sie

erhöht läuft; wenn nicht, startet sie sich selbst mit Rechteanforderung neu und beendet die ursprüngliche Instanz.

> **Hinweis:** Wird die UAC-Rückfrage verneint, **läuft die Anwendung trotzdem** — dann eben ohne erhöhte Rechte. Sie bleibt nicht stehen und meldet nichts. Das ist gewollt: Ein Programm, das sich verweigert, weil es Rechte nicht bekam, die es für die Hälfte seiner Funktionen gar nicht braucht, wäre unbrauchbar.

Punktuell — zwei Werkzeuge fordern die Rechte im Moment der Handlung an, ohne dass die Anwendung selbst erhöht laufen muss:

- *NTP & Zeitzonen* beim Setzen von Zeit und Zeitzone,
- *AD Diagnose* beim Installieren und Entfernen von RSAT.

> **Empfehlung:** Setzen Sie `RunAsAdmin` **nicht** flächendeckend. Wer die Toolbox überwiegend zum Nachsehen benutzt, sammelt damit nur UAC-Rückfragen. Für Arbeitsplätze, an denen regelmäßig Dienste gesteuert oder die HOSTS-Datei bearbeitet wird, ist der Schalter richtig — und dann als bewusste Entscheidung je Arbeitsplatz.

5.2 Rechte im Active Directory

> **Wichtig:** Die Toolbox verlangt an keiner Stelle *Domänen-Administrator*, außer dort, wo Windows selbst es verlangt. Für den Alltag genügt gezielte Delegation.

Werkzeug / Funktion	Nötiges Recht
AD Diagnose, Domäne und FSMO lesen	Authentifizierter Benutzer
AD Diagnose, FSMO **verschieben**	Domänen-Administrator; für *Schema Master* und *Domain Naming* zusätzlich Organisations-Administrator
AD Explorer	Authentifizierter Benutzer (Standorte, Trusts, Funktionsebenen sind lesbar)
AD Suche, Benutzer/Gruppen/Computer	Authentifizierter Benutzer
AD Suche, **BitLocker-Schlüssel**	Leserecht auf `msFVE-RecoveryInformation` (üblicherweise delegiert)
AD Suche, **LAPS-Kennwörter**	Leserecht auf `ms-Mcs-AdmPwd` bzw. `msLAPS-Password`
AD Suche, Computerkennwort zurücksetzen	*Kennwort zurücksetzen* auf Computerobjekte
AD Benutzer-Manager, Kennzahlen und Lesen	Authentifizierter Benutzer

Werkzeug / Funktion	Nötiges Recht
AD Benutzer-Manager, Attribute schreiben	Schreibrecht auf die betreffenden Attribute der Zielobjekte
AD Benutzer-Manager, entsperren	*Gesperrtes Konto lesen und schreiben* (`lockoutTime`)
AD Benutzer-Manager, Kennwort setzen	*Kennwort zurücksetzen* auf Benutzerobjekte
GPO Verwaltung, lesen und Berichte	Leserecht auf die GPOs (Vorgabe für authentifizierte Benutzer)
GPO Verwaltung, RSOP	Leserecht auf dem Zielcomputer, praktisch: Mitglied der lokalen Administratoren oder delegiertes RSOP-Recht
AD Papierkorb, Objekte laden	Leserecht auf den Container *Deleted Objects*
AD Papierkorb, wiederherstellen	*Gelöschte Objekte wiederherstellen* am Zielcontainer
AD Papierkorb, **aktivieren**	Organisations-Administrator
Dokumentation Erstellen, AD-Teil	Authentifizierter Benutzer
Ordivis, AD-Computer und Standort-Subnetze melden	Authentifizierter Benutzer

5.2.1 Delegation statt Vollrechten

Für die drei häufigsten Alltagsaufgaben genügt eine Delegation im Assistenten *Objektverwaltung zuweisen* auf der betreffenden Organisationseinheit:

Aufgabe	Zu delegieren
Kennwörter zurücksetzen und Konten entsperren	*Benutzerkennwörter zurücksetzen und Kennwortänderung bei der nächsten Anmeldung erzwingen*, dazu Lesen/Schreiben auf `lockoutTime`
Kontaktdaten und Adressen pflegen	Schreibrecht auf die betreffenden Attribute der Benutzerobjekte
LAPS und BitLocker lesen	Leserecht auf die genannten Attribute — bewusst und eng, siehe unten

Achtung: LAPS-Kennwörter und BitLocker-Wiederherstellungsschlüssel sind die schutzwürdigsten Daten im Verzeichnis. Wer sie lesen darf, kann sich auf jedem Rechner lokal anmelden und jede verschlüsselte Platte öffnen. Delegieren Sie dieses Leserecht nur an einen benannten, kleinen Personenkreis — und prüfen Sie regelmäßig, wer es hat.

5.3 Das hinterlegte AD-Administrator-Konto

Reicht das angemeldete Windows-Konto nicht, greifen die AD-Werkzeuge auf das Konto zurück, das unter *Einstellungen* ▸ *Active Directory Administrator-Konto* hinterlegt ist. Es wird verwendet von:

- *AD Benutzer-Manager* — alle schreibenden Aktionen,
- *AD Diagnose* — FSMO-Transfer,

- *AD Suche* — BitLocker- und LAPS-Auskunft,
- *AD Papierkorb* — Wiederherstellen,
- *Service & Process Controller* — entfernte Ziele,
- *System Inspector* — sofern kein eigenes Konto angegeben wird.

Achtung: Die Toolbox benutzt dieses Konto **ohne weitere Rückfrage**. Wer Zugriff auf die angemeldete Windows-Sitzung hat, arbeitet mit dessen Rechten. Hinterlegen Sie deshalb ein Konto mit **gezielt delegierten** Rechten — nicht das eines Domänen-Administrators, wenn es nicht sein muss.

Hinweis: Wie das Kennwort gespeichert wird, steht im Kapitel *Zugangsdaten und Kryptografie*. Kurz: verschlüsselt und an Benutzerkonto und Rechner gebunden.

5.4 Rechte auf entfernten Zielen

Werkzeug	Auf dem Ziel nötig
System Inspector (WinRM)	PowerShell Remoting aktiv, Konto in *Remoteverwaltungsbenutzer* oder lokaler Administrator
System Inspector (SNMP)	SNMP-Agent aktiv, gültige Lese-Community
Service & Process Controller	PowerShell Remoting aktiv, Konto mit Recht zum Steuern von Diensten und Beenden von Prozessen — praktisch: lokaler Administrator
GPO, RSOP	Zugriff auf den Zielcomputer, Firewall für `gpresult` offen
SNMP Inspector	SNMP-Agent aktiv, gültige Lese-Community
Remote Manager	Was das jeweilige Protokoll verlangt (RDP, SSH, FTP, SFTP)

Voraussetzung: PowerShell Remoting aktivieren Sie auf dem Ziel mit `Enable-PSRemoting -Force`. In einer Domäne geschieht das üblicherweise über eine Gruppenrichtlinie. Ohne das melden *System Inspector* und *Service & Process Controller* einen Verbindungsfehler und weisen ausdrücklich auf WinRM hin.

6 Netzwerkanforderungen

Die Toolbox öffnet **keine** eingehenden Ports und braucht keine Firewall-Ausnahme für eingehenden Verkehr. Sie ist ausschließlich Client. Was sie braucht, ist **ausgehend** — und zwar je nach benutztem Werkzeug.

> **Hinweis:** Das Installationsprogramm legt **keine** Firewall-Regel an. Wo die Windows-Firewall ausgehenden Verkehr grundsätzlich blockiert (in den meisten Umgebungen tut sie das nicht), braucht `OrdivisToolbox.exe` eine ausgehende Erlaubnis.

6.1 Ausgehend ins eigene Netz

Werkzeug	Protokoll / Port	Ziel
Dashboard, ICMP (Ping), Trace (MTR), IP Scanner, Wake-on-LAN-Prüfung, Remote Manager	**ICMP Echo**	Das jeweilige Ziel
DHCP Scanner	**UDP 67** (senden, Broadcast), **UDP 68** (empfangen)	Broadcast im lokalen Segment
Wake on LAN	**UDP 7 und 9** (Broadcast)	Broadcast im lokalen Segment
SNMP Inspector, SNMP-Anreicherung im IP Scanner, System Inspector über SNMP	**UDP 161**	Das jeweilige Gerät
NTP & Zeitzonen	**UDP 123**	Die eingetragenen Zeitserver
System Inspector, Service & Process Controller	**TCP 5985** (HTTP) bzw. **TCP 5986** (HTTPS)	Das Ziel — WinRM
Active-Directory-Werkzeuge	**TCP 389 / 636** (LDAP, LDAPS), **TCP 3268 / 3269** (Globaler Katalog), **TCP/UDP 88** (Kerberos), **TCP 135** und dynamische RPC-Ports	Domain Controller
GPO-Verwaltung	zusätzlich **TCP 445** (SMB für SYSVOL)	Domain Controller
Zertifikats-Wizard, AD CS	**TCP 135** und dynamische RPC-Ports (`certreq.exe`)	Die Zertifizierungsstelle
Basis Scanner (DNS), Zone Lookup, SMTP Diagnose	**UDP/TCP 53**	Die konfigurierten DNS-Server
IP Scanner, Basis Scanner	**TCP**, die geprüften Zielports	Die gescannten Adressen

Werkzeug	Protokoll / Port	Ziel
Remote Manager	**TCP 3389** (RDP), **22** (SSH/SFTP), **21** (FTP)	Die gespeicherten Ziele
Ordivis-Anbindung	**TCP**, der Port des eingetragenen Endpunkts (üblich **5001**, HTTPS)	Ordivis Platform

> **Hinweis:** Broadcasts überqueren keine Router. *DHCP Scanner* und *Wake on LAN* wirken deshalb nur im **eigenen Netzsegment**. Ein DHCP-Relay hilft dem Scanner nicht: Er sucht Antworten, die im selben Segment entstehen.

6.2 Ausgehend ins Internet

Nur die folgenden Werkzeuge sprechen mit Diensten außerhalb. **Wo Ihr Netz keinen Internetzugang hat, arbeitet alles Übrige unverändert weiter.**

Werkzeug	Ziel	Port	Was übertragen wird
Dashboard, Statusanzeige *DNS*	`1.1.1.1`	ICMP	Nichts außer dem Ping
Speedtest	`www.speedtestx.de`, `speed.hetzner.de`, `ash-speed.hetzner.com`	TCP 443	Nichts — es wird nur geladen
Basis Scanner, Trace (MTR), Zone Lookup	`ip-api.com`	**TCP 80**	Die abgefragte öffentliche IP-Adresse
Zone Lookup	`api.bgpview.io`	TCP 443	Die abgefragte öffentliche IP-Adresse
Kartenansichten	`www.openstreetmap.org`, `unpkg.com`	TCP 443	Die anzuzeigenden Koordinaten
MAC Scanner, manuelle Suche	`api.macvendors.com`	TCP 443	Die eingegebene MAC-Adresse
System Inspector, Sicherheits-Check	`cve.circl.lu`	TCP 443	Hersteller- und Produktnamen der installierten Software
WHOIS Abfrage	Der gewählte WHOIS-Server	**TCP 43**	Die eingegebene Domain oder IP-Adresse
WHOIS Abfrage, RDAP	`rdap.arin.net`	TCP 443	Die eingegebene IP-Adresse
IP Scanner, Nmap nachinstallieren	`nmap.org`	TCP 443	Nichts — es wird nur geladen

Werkzeug	Ziel	Port	Was übertragen wird
OpenSSL nachinstallieren	Winget-Quellen (`cdn.winget.microsoft.com` u. a.)	TCP 443	Nichts — es wird nur geladen
AD Diagnose, RSAT nachinstallieren	Windows Update / WSUS	TCP 80/443	Nichts — es wird nur geladen

Wichtig: Private Adressen (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16) und Loopback werden **nie** an einen dieser Dienste übertragen. Die Standortabfrage prüft das ausdrücklich und überspringt private Adressen.

Achtung: Der **Sicherheits-Check (CVE & WID)** überträgt eine Liste von Hersteller- und Produktnamen an `cve.circl.lu`. Es werden keine Versionsnummern, keine Rechnernamen und keine Kennungen mitgeschickt — die Liste sagt aber etwas über das aufgenommene System aus. Wo das nicht erwünscht ist, sperren Sie `cve.circl.lu` oder weisen Sie an, den Check nicht zu benutzen. Alle übrigen Funktionen des System Inspectors bleiben davon unberührt.

Achtung: Die Standortabfrage geht über **HTTP** (Port 80), nicht HTTPS. Sie überträgt nur die abgefragte öffentliche IP-Adresse und keine Kennung — der Abfragende ist dabei aber für Zwischenstationen erkennbar. In Umgebungen, die unverschlüsselten ausgehenden Verkehr grundsätzlich unterbinden, entfällt damit die Standortangabe. Alles Übrige der betreffenden Seiten funktioniert weiter.

6.3 Ausgehende Sperrung, gezielt

Wenn Sie den Internetzugang der Toolbox einschränken wollen, ohne sie unbrauchbar zu machen, ist diese Staffelung sinnvoll:

Stufe	Freigeben	Wirkung
Vollständig offline	nichts	Alle Kernfunktionen arbeiten; siehe Kapitel *Architektur und Systemvoraussetzungen*
Datenschutzfreundlich	`nmap.org`, Winget, Windows Update	Nachinstallation möglich, keine Abfrage über Ihre Daten
Diagnosefähig	zusätzlich WHOIS/RDAP, `ip-api.com`, `api.bgpview.io`, OSM	Standortangaben und Registerauskünfte
Vollständig	zusätzlich `cve.circl.lu`, Speedtest-Server, `api.macvendors.com`	Alles

6.4 Ordivis Platform

Der Endpunkt ist frei einstellbar und liegt üblicherweise im eigenen Netz, etwa `https://ordivis.firma.local:5001`. Verwendet werden:

Zweck	Pfad
Verbindungstest	`GET /api/v1/ipam/ingest/health`
Scan-Ergebnisse	`POST /api/v1/ipam/ingest/scan`
Bekannte Subnetze abrufen	`GET /api/v1/ipam/ingest/prefixes`
Unbestätigte Adressen abrufen	`GET /api/v1/ipam/ingest/unconfirmed`
Adresse bestätigen	`POST /api/v1/ipam/ingest/ips/{id}/confirm`
DHCP-Bereiche	`POST /api/v1/ipam/ingest/dhcp`
DNS-Abgleich	`POST /api/v1/ipam/ingest/dns`
Geräte (AD-Computer, SNMP)	`POST /api/v1/discovery/ingest/devices`
Zertifikate	`POST /api/v1/discovery/ingest/certificates`
Schwachstellenbefunde	`POST /api/v1/security/ingest/findings`
Informationsverbünde abrufen	`GET /api/v1/security/ingest/scopes`

Die Anmeldung erfolgt über einen Bearer-Token im Kopf jeder Anfrage. Die Zeitgrenze je Anfrage liegt bei 120 Sekunden.

> **Voraussetzung:** Das Serverzertifikat wird standardmäßig **geprüft**. Bei einer Installation mit selbstsigniertem Zertifikat muss die Prüfung bewusst abgeschaltet werden — siehe Kapitel *Anbindung an Ordivis Platform*.

7 Datenablage und Konfiguration

7.1 Der Datenordner

Alles, was die Toolbox zur Laufzeit schreibt, liegt in einem Ordner im Profil des **angemeldeten Benutzers**:

```
%LOCALAPPDATA%\OrdivisToolbox
```

also üblicherweise `C:\Users\<Benutzer>\AppData\Local\OrdivisToolbox`.

> **Wichtig:** Die Toolbox schreibt **nichts** in `Program Files`, **nichts** in `ProgramData` und **nichts** in die Registrierung (außer dem Deinstallationseintrag, den Inno Setup anlegt). Es gibt keine maschinenweite Konfiguration.

Datei / Ordner	Inhalt
`settings.json`	Alle Einstellungen, einschließlich der verschlüsselten Geheimnisse
`settings.json.tmp`	Nur kurzzeitig während des Speicherns
`remotes.json`	Die gespeicherten Remote-Verbindungen samt verschlüsselter Kennwörter
`ad_audit_log.json`	Das lokale Protokoll der Änderungen aus dem AD-Benutzer-Manager
`outbox\*.json`	Zwischengespeicherte Ordivis-Pakete, je Paket eine Datei
`WebView2\`	Das Browserprofil der eingebetteten Anzeige
`crash.log`	Absturzprotokoll
`karte.log`	Warum eine Kartenansicht nicht erschien

7.1.1 Umzug aus der Zeit vor der Umbenennung

Bis August 2026 hieß der Ordner `%LOCALAPPDATA%\NetzDesk`. Beim ersten Zugriff wird er **verschoben**, nicht neu angelegt:

- Der Umzug läuft **genau einmal**: nur wenn der alte Ordner existiert **und** der neue noch nicht.
- Existieren beide, gilt der neue. Der alte bleibt unangetastet liegen — beide zu verschmelzen wäre geraten, nicht gewusst.
- Scheitert der Umzug — etwa weil eine Datei noch offen ist —, arbeitet die Anwendung am **alten** Ort weiter, statt ohne Einstellungen zu starten. Beim nächsten Start wird es erneut versucht.

> **Hinweis:** Wer beim Aufräumen `%LOCALAPPDATA%\NetzDesk` findet, sollte prüfen, ob daneben auch `%LOCALAPPDATA%\OrdivisToolbox` steht. Wenn ja, ist der alte Ordner ein Rest und kann weg. Wenn nein, ist er der **aktive** Datenbestand.

7.2 Die Einstellungsdatei

`settings.json` ist eine flache JSON-Zuordnung von Zeichenketten auf Zeichenketten. Alle Werte sind Text — auch Zahlen und Wahrheitswerte.

7.2.1 Alle Schlüssel

Schlüssel	Werte	Vorgabe	Bedeutung
`Language`	`de`, `en`	leer (Systemsprache)	Anzeigesprache
`AppTheme`	`Default`, `Light`, `Dark`	`Default`	Farbschema
`UpdateInterval`	200–5000	`1000`	Takt in Millisekunden für Dashboard, Verbindungen, Topologie
`DataUnit`	`Auto`, `KB`, `MB`	`Auto`	Einheit für Durchsatzangaben
`RunAsAdmin`	`True`, `False`	`False`	Beim Start Administratorrechte anfordern
`AdDomain`	Text	leer	Domäne des hinterlegten AD-Kontos
`AdUsername`	Text	leer	Benutzername des hinterlegten AD-Kontos
`AdPasswordProtected`	Base64	leer	**Verschlüsseltes** Kennwort (DPAPI, Benutzerkontext)
`AdPassword`	Base64	—	**Veraltet.** Nur kodiert, nicht verschlüsselt; wird beim Start einmalig umgewandelt und entfernt
`DocSavePath`	Pfad	Desktop	Zielordner für erzeugte Dokumentationen
`DocLogoPath`	Pfad	leer	Firmenlogo für den Bericht
`DocEmail`	E-Mail	leer	Adresse für den Sofort-Versand
`InfraDeskEndpoint`	URL	leer	Adresse von Ordivis Platform
`InfraDeskTokenProtected`	Base64	leer	**Verschlüsselter** Integrations-Token
`InfraDeskTenantName`	Text	leer	Angezeigter Mandantenname aus dem Verbindungstest
`InfraDeskAllowInvalidCert`	`True`, `False`	`False`	Zertifikatsprüfung des Endpunkts abschalten

Achtung: Die vier Schlüssel mit dem Präfix `InfraDesk…` heißen bewusst noch so und dürfen **nicht** umbenannt werden. Sie sind keine Bezeichner im Quelltext, sondern die Schlüssel in bestehenden Dateien. Wer sie umbenennt, trennt jede vorhandene Installation von ihrem Endpunkt und ihrem gespeicherten Token — die Verbindung wäre nach einem Update wortlos weg. Derselbe Grund, aus dem beim Ordivis-Rebrand auch Datenbank- und Dienstnamen stehen blieben: Der Nutzen einer Umbenennung ist null, das Risiko ist es nicht.

7.2.2 Beispiel

```
{
  "Language": "de",
  "AppTheme": "Dark",
  "UpdateInterval": "2000",
  "DataUnit": "MB",
  "RunAsAdmin": "False",
  "AdDomain": "contoso.local",
  "AdUsername": "svc-toolbox",
  "DocSavePath": "\\\\dateiserver\\it$\\Dokumentation",
  "DocLogoPath": "C:\\ProgramData\\Firma\\logo.png",
  "DocEmail": "it@beispiel.de",
  "InfraDeskEndpoint": "https://ordivis.firma.local:5001"
}
```

7.2.3 Wie geschrieben wird

Die Datei wird **erst vollständig daneben geschrieben und dann ersetzt**. Ein Absturz mitten in einem direkten Schreibvorgang hinterließ sonst eine abgeschnittene Datei — und die wird beim nächsten Start verworfen, samt aller Einstellungen einschließlich AD-Kennwort und Ordivis-Token.

Hinweis: Findet die Anwendung eine unlesbare `settings.json`, fängt sie **wortlos mit leeren Einstellungen** neu an. Wer nach einem Absturz plötzlich ohne Verbindung und ohne hinterlegtes Konto dasteht, sollte die Datei ansehen, bevor er alles neu einträgt.

7.3 Einstellungen vorbelegen

Es gibt keine Gruppenrichtlinien-Vorlage. Vorbelegen lässt sich die Datei über ein **Anmeldeskript**, das sie anlegt, wenn sie noch nicht existiert:

```
# Anmeldeskript (läuft im Benutzerkontext). Legt Vorgaben an, ohne
# vorhandene Einstellungen zu überschreiben.
$ordner = Join-Path $env:LOCALAPPDATA 'OrdivisToolbox'
$datei  = Join-Path $ordner 'settings.json'
if (-not (Test-Path $datei)) {
    New-Item -ItemType Directory -Force -Path $ordner | Out-Null
    @{
        Language           = 'de'
        AppTheme           = 'Default'
        UpdateInterval     = '2000'
        DataUnit           = 'Auto'
        RunAsAdmin         = 'False'
        DocSavePath        = '\\dateiserver\it$\Dokumentation'
        DocLogoPath        = 'C:\ProgramData\Firma\logo.png'
        InfraDeskEndpoint  = 'https://ordivis.firma.local:5001'
    } | ConvertTo-Json | Set-Content -Path $datei -Encoding UTF8
}
```

Achtung: Belegen Sie **niemals** `AdPasswordProtected` oder `InfraDeskTokenProtected` vor. Beide sind an Benutzerkonto **und** Rechner gebunden; ein zentral verteilter Wert ist auf jedem anderen Rechner unbrauchbar. Und ein Klartextwert daneben wäre ein Kennwort in einer Skriptdatei.

Achtung: Setzen Sie `InfraDeskAllowInvalidCert` nicht per Skript auf `True`. Diese Entscheidung gehört an die Stelle, an der jemand das Zertifikat der eigenen Installation kennt — nicht in ein Skript, das für alle gilt.

7.4 Die weiteren Dateien

7.4.1 `remotes.json`

Die gespeicherten Ziele des Remote Managers: Anzeigename, Host, Protokoll, Benutzername, die RDP-Umleitungsoptionen — und das Kennwort im Feld `PasswordProtected`, verschlüsselt.

Achtung: Ein älteres Feld `Password` konnte das Kennwort im Klartext tragen. Beim Laden wird ein solcher Wert übernommen und beim nächsten Speichern durch die verschlüsselte Form ersetzt. Wer alte Dateien aus Sicherungen wiederherstellt, holt sich damit unter Umständen Klartextkennwörter zurück.

7.4.2 `ad_audit_log.json`

Das lokale Protokoll der über den AD-Benutzer-Manager ausgeführten Änderungen: Zeitstempel, ausführendes Konto, Zielobjekt, Aktion.

Wichtig: Das ist ein **Arbeitsprotokoll**, keine revisionssichere Aufzeichnung. Es liegt beschreibbar im Benutzerprofil, gilt nur für diesen Rechner und dieses Windows-Konto und lässt sich löschen. Die verbindliche Nachweisführung über Änderungen im Verzeichnis liefert das Sicherheitsprotokoll der Domain Controller. Wer den Nachweis braucht, aktiviert dort die entsprechende Überwachungsrichtlinie und wertet sie im SIEM aus.

7.4.3 `outbox\`

Je wartendem Ordivis-Paket eine JSON-Datei, benannt nach der Paketkennung. Nach erfolgreicher Übertragung wird sie gelöscht.

Hinweis: Der Inhalt sind Scan-Ergebnisse — IP-Adressen, Hostnamen, offene Ports. Wo das schützenswert ist, gehört der Ordner zum Datenbestand, der bei einer Geräterückgabe entfernt wird.

7.4.4 `WebView2\`

Das Profilverzeichnis der eingebetteten Browserkomponente: Zwischenspeicher und lokaler Zustand der Kartenansichten und der GPO-Berichtsanzeige. Es lässt sich gefahrlos löschen, wenn die Toolbox nicht läuft; es wird neu angelegt.

7.5 Sicherung und Umzug auf einen anderen Rechner

Was	Lässt sich mitnehmen?
Allgemeine Einstellungen (Sprache, Design, Takt, Einheit, Dokumentationspfade)	**Ja** — `settings.json` kopieren und die verschlüsselten Schlüssel entfernen
Ordivis-Endpunkt	**Ja** (`InfraDeskEndpoint`)
Ordivis-Token	**Nein** — muss neu eingetragen werden
AD-Kennwort	**Nein** — muss neu eingetragen werden
Remote-Verbindungen	**Teilweise** — die Einträge ja, die Kennwörter nicht
Prüfprotokoll, Warteschlange, Browserprofil	Nicht sinnvoll

Der Grund ist derselbe für alle drei Geheimnisse: Sie sind mit Windows DPAPI an **dieses Benutzerkonto auf diesem Rechner** gebunden. Näheres im Kapitel *Zugangsdaten und Kryptografie*.

8 Zugangsdaten und Kryptografie

Die Toolbox speichert drei Geheimnisse. Dieses Kapitel sagt, wie — und ebenso wichtig: wo Geheimnisse den geschützten Bereich wieder verlassen.

8.1 Die drei gespeicherten Geheimnisse

Geheimnis	Wo	Schlüssel / Feld
Kennwort des AD-Administrator-Kontos	`settings.json`	`AdPasswordProtected`
Integrations-Token für Ordivis Platform	`settings.json`	`InfraDeskTokenProtected`
Kennwörter der Remote-Verbindungen	`remotes.json`	`PasswordProtected` je Eintrag

Alle drei werden mit **Windows DPAPI im Benutzerkontext** (`DataProtectionScope.CurrentUser` beziehungsweise `LOCAL=user`) verschlüsselt und Base64-kodiert abgelegt.

Daraus folgt:

- Der Schlüssel hängt am **Anmeldegeheimnis des Windows-Kontos**. Ein anderer Benutzer auf demselben Rechner kann die Werte nicht entschlüsseln.
- Auf einem **anderen Rechner** sind die Werte wertlos — Kopieren der Datei nützt nichts.
- Wer die **angemeldete Sitzung** des Benutzers hat, hat auch die Geheimnisse. DPAPI schützt gegen das Lesen der Datei, nicht gegen jemanden, der am entsperrten Rechner sitzt.

Achtung: Der wirksame Schutz ist damit das Windows-Kennwort des Benutzers und die Bildschirmsperre. Wo die Toolbox mit hinterlegtem AD-Konto auf einem Gerät läuft, das andere anfassen können, ist das hinterlegte Konto so gut geschützt wie dieses Gerät.

8.2 Die abgelöste Speicherform des AD-Kennworts

Frühere Fassungen legten das AD-Kennwort unter dem Schlüssel `AdPassword` als **reines Base64** ab — also kodiert, nicht verschlüsselt. Jeder, der die Datei lesen konnte, konnte es in einem Schritt zurückwandeln.

Beim Start wird ein solcher Wert **einmalig umgewandelt**: entschlüsselt, DPAPI-geschützt unter `AdPasswordProtected` abgelegt und der schwache Wert entfernt. Schlägt die Umwandlung fehl — etwa weil DPAPI in dem Moment nicht verfügbar ist —, bleibt der alte Wert unangetastet, damit keine gespeicherten Zugangsdaten verloren gehen.

Achtung: Wer alte `settings.json` aus Sicherungen wiederherstellt, holt sich unter Umständen ein Base64-Kennwort zurück. Es wird beim nächsten Start umgewandelt — bis dahin liegt es aber wieder schwach geschützt auf der Platte. Dasselbe gilt für ein altes Feld `Password` in `remotes.json`.

8.3 Wo Geheimnisse den geschützten Bereich verlassen

Drei Stellen — sie sind der übliche Weg der beteiligten Werkzeuge und lassen sich nicht wegdefinieren.

8.3.1 RDP-Verbindungen

Beim Verbinden schreibt die Toolbox das Kennwort über `cmdkey.exe` in den **Windows-Anmeldeinformationsspeicher** (`TERMSRV/<Host>`), damit `mstsc.exe` es verwenden kann.

Achtung: Der Eintrag bleibt dort stehen. Er ist zwar seinerseits DPAPI-geschützt und benutzerbezogen, aber er ist ein zweiter Ort, an dem das Kennwort liegt — außerhalb der Toolbox und außerhalb ihrer Deinstallation. Prüfen lässt er sich mit `cmdkey /list`, entfernen mit `cmdkey /delete:TERMSRV/<Host>`.

8.3.2 FTP- und SFTP-Verbindungen

Benutzername und Kennwort werden als Bestandteil der übergebenen Adresse an WinSCP beziehungsweise den Explorer gereicht (`sftp://benutzer:kennwort@host`).

Achtung: Eine Adresse mit eingebettetem Kennwort kann in der Prozessliste, in der Sprungliste des Zielprogramms und in dessen eigener Sitzungsgeschichte auftauchen. Für hochprivilegierte Konten ist es die bessere Wahl, das Kennwortfeld leer zu lassen und beim Verbinden zu tippen.

8.3.3 PowerShell-Aufrufe mit hinterlegtem Konto

System Inspector und *Service & Process Controller* bauen für entfernte Ziele ein PowerShell-Skript, das das hinterlegte Kennwort enthält, und übergeben es an `powershell.exe`.

Achtung: Das Skript wird über Standardeingabe beziehungsweise als Argument übergeben, nicht auf die Platte geschrieben. Trotzdem gilt: Wo die PowerShell-Skriptblockprotokollierung (*Script Block Logging*) eingeschaltet ist, landen solche Aufrufe im Ereignisprotokoll — mitsamt dem Kennwort. Prüfen Sie das, bevor Sie ein privilegiertes Konto hinterlegen, und ziehen Sie stattdessen eine gezielte Delegation vor.

8.4 Was nicht gespeichert wird

Wert	Verbleib
Private Schlüssel aus dem Zertifikats-Wizard	Nur im Textfeld der Oberfläche; beim Verlassen der Seite fort

Wert	Verbleib
Eingaben im OpenSSL-Konverter	Nur im Arbeitsspeicher; Ausgabedateien schreiben Sie selbst
PFX-Kennwörter	Nur für den einzelnen Aufruf
SNMP-Communities	Nur für die einzelne Abfrage
Kennwörter im System Inspector	Nur für die einzelne Abfrage
Neue Kennwörter aus dem AD-Kennwortdialog	Nur für die einzelne Aktion

Wichtig: Der Zertifikats-Wizard erzeugt den privaten Schlüssel **lokal**. Er verlässt den Rechner nicht und wird nirgends abgelegt. Wer ihn behalten will, muss ihn aus dem Textfeld herauskopieren, **bevor** er die Seite verlässt.

8.5 Was aus dem Verzeichnis gelesen, aber nie weitergegeben wird

AD Suche kann **BitLocker-Wiederherstellungsschlüssel** und **LAPS-Kennwörter** anzeigen. Beide:

- werden **nicht** in einer Datei gespeichert,
- werden **nicht** an Ordivis Platform übertragen — auch nicht beim Melden von AD-Computern, obwohl sie im Verzeichnis teils an denselben Objekten hängen,
- stehen nur so lange in der Anzeige, wie die Seite offen ist.

Achtung: Sie stehen aber **auf dem Bildschirm**. In einer geteilten Sitzung, bei einer Bildschirmaufzeichnung oder auf einem Bildschirmfoto sind sie damit weitergegeben. Behandeln Sie diese Ansicht wie ein offenes Kennworttresor-Fenster.

8.6 Empfehlungen für den Betrieb

1. **Hinterlegen Sie ein Dienstkonto mit delegierten Rechten**, nicht das eines Domänen-Administrators. Welche Rechte je Aufgabe genügen, steht im Kapitel *Rechte und Berechtigungen*.
2. **Ein Konto je Person, nicht ein gemeinsames.** Das lokale Prüfprotokoll des AD-Managers vermerkt das ausführende Konto; ein Sammelkonto macht diesen Eintrag wertlos.
3. **Lassen Sie das Kennwortfeld im Remote Manager leer**, wo das Ziel hoch privilegiert ist.
4. **Nehmen Sie den Datenordner in die Geräterückgabe auf.** Die Deinstallation entfernt ihn nicht (siehe Kapitel *Installation*).
5. **Schalten Sie die Zertifikatsprüfung des Ordivis-Endpunkts nicht ab**, außer die Installation nutzt wirklich ein selbstsigniertes Zertifikat — und dann als bewusste, dokumentierte Entscheidung.

9 Active Directory: Voraussetzungen

Sechs Werkzeuge der Toolbox arbeiten gegen den Verzeichnisdienst. Dieses Kapitel nennt, was dafür vorhanden sein muss — die Rechte stehen im Kapitel *Rechte und Berechtigungen*.

9.1 Grundvoraussetzung

Voraussetzung: Der Rechner, auf dem die Toolbox läuft, muss **Mitglied der Domäne** sein und einen Domain Controller erreichen. Die Werkzeuge ermitteln die Domäne über die Mitgliedschaft des Rechners; es gibt kein Feld, in das sich eine Domäne von Hand eintragen ließe.

Ist der Rechner kein Mitglied, melden alle sechs Werkzeuge *„Keine AD Domäne gefunden (oder keine Berechtigung)."* Das ist kein Fehler, sondern die richtige Auskunft.

9.2 Erreichbarkeit

Dienst	Ports
LDAP	TCP 389, LDAPS TCP 636
Globaler Katalog	TCP 3268, 3269
Kerberos	TCP/UDP 88
RPC-Endpunktzuordnung	TCP 135 und die dynamischen Ports
SMB (SYSVOL, für GPO-Berichte)	TCP 445
DNS	UDP/TCP 53

Hinweis: Die Zeit muss stimmen. Kerberos verwirft Tickets bei mehr als fünf Minuten Abweichung — dann schlägt jede AD-Abfrage fehl, ohne dass es nach einem Zeitproblem aussieht. Siehe Kapitel *Zeitsynchronisation im Netz*.

9.3 Funktionsebenen

Funktion	Mindestens nötig
AD Diagnose, AD Explorer, AD Suche, AD Benutzer-Manager	Keine besondere Ebene
AD Papierkorb	Gesamtstruktur-Funktionsebene **Windows Server 2008 R2** — und der Papierkorb muss aktiviert sein

Funktion	Mindestens nötig
Windows LAPS (`msLAPS-Password`)	Schemaerweiterung für Windows LAPS
Legacy LAPS (`ms-Mcs-AdmPwd`)	Schemaerweiterung für Microsoft LAPS
BitLocker-Schlüssel im AD	Die Sicherung im AD muss per Gruppenrichtlinie erzwungen sein

Die aktuellen Funktionsebenen zeigt *AD Explorer* an.

9.4 RSAT — welche Werkzeuge wofür

Drei Werkzeugbereiche der Toolbox rufen Windows-Programme auf, die **nicht** standardmäßig installiert sind:

Toolbox-Funktion	Braucht	RSAT-Paket
AD Diagnose ▸ DCDIAG	`dcdiag.exe`	*Active Directory Tools (AD DS & LDS)*
AD Diagnose ▸ REPADMIN	`repadmin.exe`	*Active Directory Tools (AD DS & LDS)*
Gruppenrichtlinien (GPO) Verwaltung	Die GPO-PowerShell-Befehle	*Gruppenrichtlinienverwaltung*
AD Papierkorb	Die AD-PowerShell-Befehle	*Active Directory Tools (AD DS & LDS)*

Die Toolbox erkennt das Fehlen selbst und bietet die Nachinstallation unter *AD Diagnose ▸ RSAT* an.

9.4.1 RSAT unbeaufsichtigt bereitstellen

⚙️ **Außerhalb:** PowerShell mit erhöhten Rechten · 🔑 **Rechte:** lokaler Administrator

```
Get-WindowsCapability -Online -Name 'Rsat.ActiveDirectory*','Rsat.GroupPolicy*' |
    Where-Object State -ne 'Installed' |
    Add-WindowsCapability -Online
```

Stolperfalle: RSAT-Pakete sind **Features on Demand** und werden von Windows Update bezogen. Zeigt eine Gruppenrichtlinie den Client auf einen **WSUS**, holt er sie dort — und dort liegen sie in aller Regel nicht. Die Installation scheitert dann ohne erkennbaren Grund. Die Toolbox weist selbst darauf hin.

Abhilfe, eines von dreien:

1. Die Richtlinie *Einstellungen für die Installation von optionalen Komponenten und für die Komponentenreparatur angeben* setzen und *Direkt von Windows Update herunterladen…* aktivieren.
2. Einen alternativen Quellpfad auf eine Freigabe mit dem *Features-on-Demand*-Datenträger legen.
3. Die RSAT-Pakete über das Betriebssystem-Abbild vorinstallieren.

9.5 Das AD-Prüfprotokoll richtig einordnen

Der *AD Benutzer-Manager* führt ein eigenes Protokoll über die von ihm ausgeführten Änderungen (`ad_audit_log.json` im Benutzerprofil).

Wichtig: Das ist ein **Arbeitsprotokoll**, keine Nachweisführung. Es liegt beschreibbar im Benutzerprofil, gilt nur für diesen Rechner und dieses Windows-Konto und lässt sich löschen.

Wer den Nachweis über Änderungen im Verzeichnis führen muss, aktiviert die Überwachung auf den Domain Controllern:

⚙ **Außerhalb:** Gruppenrichtlinienverwaltung, *Default Domain Controllers Policy*

Computerkonfiguration ▸ *Richtlinien* ▸ *Windows-Einstellungen* ▸ *Sicherheitseinstellungen* ▸ *Erweiterte Überwachungsrichtlinienkonfiguration* ▸ *Kontenverwaltung*:

- *Benutzerkontenverwaltung überwachen* — Erfolg und Fehler
- *Computerkontenverwaltung überwachen* — Erfolg und Fehler

Und unter *DS-Zugriff*:

- *Verzeichnisdienstzugriff überwachen* — Erfolg
- *Verzeichnisdienständerungen überwachen* — Erfolg

Die einschlägigen Ereigniskennungen im Sicherheitsprotokoll der Domain Controller:

Kennung	Ereignis
4720	Benutzerkonto erstellt
4722	Benutzerkonto aktiviert
4723 / 4724	Kennwort geändert / zurückgesetzt
4725 / 4726	Konto deaktiviert / gelöscht
4738	Benutzerkonto geändert
4767	Konto entsperrt
5136	Attribut eines Verzeichnisobjekts geändert
5141	Verzeichnisobjekt gelöscht

Tipp: Ein Dienstkonto für die Toolbox — statt der persönlichen Konten — verwischt genau diese Spur: Im Sicherheitsprotokoll steht dann das Dienstkonto und nicht, wer gehandelt hat. Wo Nachvollziehbarkeit zählt, arbeitet jede Person mit ihrem eigenen delegierten Konto.

9.6 Vor dem ersten Einsatz prüfen

Eine kurze Reihenfolge, die die üblichen Stolpersteine in einem Durchgang abräumt:

1. *AD Diagnose* öffnen. Steht die Domäne mit NETBIOS-Name, FQDN, Forest und DC-Liste da? → Grundvoraussetzung erfüllt.
2. Stehen die fünf FSMO-Rollen mit Inhaber da? → LDAP-Zugriff funktioniert.
3. *AD Explorer* öffnen. Standorte und Funktionsebenen sichtbar? → Leserechte ausreichend.
4. *AD Diagnose* ▸ *RSAT*: Sind *Active Directory Tools* und *Gruppenrichtlinienverwaltung* installiert? Wenn nein, jetzt nachinstallieren.
5. *DCDIAG* mit *Standard (Zeigt nur Fehler)* laufen lassen. Kommen Ergebnisse? → Administratorrechte vorhanden.
6. *GPO Verwaltung* ▸ *GPOs laden*. Kommt die Liste? → GPO-Werkzeuge einsatzbereit.
7. *AD Papierkorb* ▸ *AD Objekte laden*. Kommt die Liste oder der Aktivierungshinweis? → Der Zustand des Papierkorbs ist damit geklärt.

10 Externe Werkzeuge und Abhängigkeiten

Die Toolbox bringt ihre Laufzeitumgebung mit, aber nicht jedes Werkzeug, das sie aufrufen kann. Dieses Kapitel führt auf, was nachinstalliert werden muss, was die Toolbox selbst nachinstallieren kann und was in einem abgeschotteten Netz zu tun ist.

10.1 Übersicht

Werkzeug	Von wem	Wofür in der Toolbox	Nachinstallation aus der Toolbox
WebView2-Laufzeit	Microsoft	Kartenansichten, GPO-Berichte	nein
RSAT (AD-Tools, GPO)	Microsoft, Windows-Feature	`dcdiag`, `repadmin`, GPO- und AD-Befehle	**ja**
Nmap	nmap.org	IP Scanner, Nmap-Motor	**ja**
OpenSSL	Shining Light Productions, über Winget	OpenSSL Converter	**ja**
WinSCP	winscp.net	SFTP-Verbindungen im Remote Manager	nein
`certreq.exe`	Windows, vorhanden	Zertifikats-Wizard, AD CS	entfällt
`tzutil.exe`, `cmdkey.exe`, `mstsc.exe`, `notepad.exe`, `powershell.exe`	Windows, vorhanden	verschiedene	entfällt
Posh-ACME	PowerShell-Katalog	Das erzeugte ACME-Skript ausführen	nein (läuft ohnehin auf einem anderen Rechner)

10.2 WebView2-Laufzeit

Die eingebettete Browserkomponente wird an zwei Stellen benutzt: für die Kartenansichten (*Basis Scanner*, *Zone Lookup*, *Trace (MTR)*) und für die Anzeige der **GPO-HTML-Berichte**.

> **Voraussetzung:** Auf Windows 11 und auf gepflegten Windows-10-Systemen ist sie vorhanden — Microsoft liefert sie mit Edge aus. Fehlt sie, arbeitet die Toolbox weiter: Die betroffenen Seiten liefern ihre Ergebnisse vollständig, nur die Kartenfläche bleibt leer. Der Grund steht in `karte.log` im Datenordner.

Fehlt sie, liefert Microsoft das *Evergreen Standalone Installer*-Paket aus. Es lässt sich unbeaufsichtigt ausbringen:

```
MicrosoftEdgeWebView2RuntimeInstallerX64.exe /silent /install
```

10.3 RSAT

Siehe Kapitel *Active Directory: Voraussetzungen*, Abschnitt *RSAT*. Dort steht auch, warum die Nachinstallation hinter einem WSUS scheitert und was dagegen hilft.

10.4 Nmap

> 💻 **Menü:** *Werkzeug-Suiten* ▸ *Scanner Werkzeuge* ▸ *IP Scanner* ▸ *Jetzt installieren*

Der IP Scanner arbeitet ohne Nmap vollständig — der eingebaute Motor prüft Ping und TCP-Ports und löst Hostnamen auf. Nmap braucht es für Dienstversionen, Betriebssystemerkennung und Schwachstellen-Skripte.

Ist `nmap.exe` nicht vorhanden, lädt die Toolbox das Installationsprogramm von `nmap.org` und startet es.

> **Voraussetzung:** Der Assistent muss **bedient** werden — er läuft nicht unbeaufsichtigt durch. Für eine Verteilung an viele Arbeitsplätze ist das der falsche Weg.

Für die Verteilung nehmen Sie stattdessen:

```
nmap-7.95-setup.exe /S
```

> **Achtung:** Nmap installiert **Npcap** mit. Npcap bringt einen Netzwerktreiber mit — das ist eine Änderung am System, die in vielen Organisationen eine eigene Freigabe braucht. Klären Sie das, bevor Sie Nmap flächendeckend ausrollen.

> **Wichtig:** Die Nmap-Profile *Intense Scan* (`-sV -O`) und *Stealth Scan* (`-sS`) brauchen Rohsockets und damit **Administratorrechte**. Läuft die Toolbox ohne, startet sie den Scan gar nicht erst und sagt das.

10.5 OpenSSL

> 💻 **Menü:** *Werkzeug-Suiten* ▸ *CA & PKI* ▸ *OpenSSL Converter* ▸ *Jetzt installieren*

Die Toolbox sucht `openssl.exe` an den üblichen Orten und im `PATH`. Fehlt es, installiert sie es über **Winget**:

```
winget install ShiningLight.OpenSSL --accept-package-agreements --accept-source-agreements --silent
```

Für eine Verteilung führen Sie denselben Befehl im Systemkontext aus, oder Sie bringen OpenSSL auf dem in Ihrer Organisation üblichen Weg aus. Die Toolbox findet es danach selbst.

Voraussetzung: Winget muss vorhanden sein und Zugriff auf seine Quellen haben. In abgeschotteten Netzen scheitert das.

Hinweis: Ohne OpenSSL fehlt genau eine Seite. *Lokale Zertifikate (PKI)* und der *Zertifikats-Wizard* arbeiten ohne OpenSSL — sie benutzen die eingebauten Kryptografie-Schnittstellen von .NET.

10.6 WinSCP

Nur für **SFTP** im Remote Manager. FTP öffnet notfalls der Windows-Explorer, SFTP kann er nicht. Ist kein Programm für SFTP registriert, meldet die Toolbox *„WinSCP wird benötigt"*.

WinSCP lässt sich unbeaufsichtigt installieren:

```
WinSCP-<Version>-Setup.exe /VERYSILENT /ALLUSERS /NORESTART
```

10.7 In einem abgeschotteten Netz

Wo kein Internetzugang besteht, funktioniert **keine** der eingebauten Nachinstallationen. Stellen Sie die Werkzeuge dann vorab bereit:

Werkzeug	Weg
WebView2	Evergreen Standalone Installer, unbeaufsichtigt (siehe oben)
RSAT	Features-on-Demand-Datenträger oder alternativer Quellpfad
Nmap	Setup mit `/S` verteilen; Npcap-Treiber vorher freigeben
OpenSSL	Über den üblichen Paketweg der Organisation
WinSCP	Setup unbeaufsichtigt verteilen

Tipp: Verteilen Sie **nur, was gebraucht wird**. Nmap mit Npcap auf jedem Arbeitsplatz ist eine größere Änderung als die Toolbox selbst. Für die Frage „wer ist in diesem Subnetz erreichbar?" reicht der eingebaute Motor.

10.8 Wie externe Werkzeuge aufgerufen werden

Alle externen Aufrufe laufen über eine gemeinsame Naht mit vier Eigenschaften, die für den Betrieb zählen:

1. **Beide Ausgabeströme werden gleichzeitig geleert.** Wer stdout und stderr nacheinander liest, hängt dauerhaft, sobald das Kind mehr als die Puffergröße (rund 4 KB) auf stderr schreibt — es schließt stdout dann nie.
2. **Zeitgrenzen** je Aufruf; bei Überschreitung wird der **Prozessbaum** beendet.
3. **Abbruch** durch den Benutzer beendet den Prozess wirklich.
4. Der Prozess wird sicher **freigegeben**.

> **Hinweis:** Das ist der Grund, warum ein hängendes `dcdiag` oder ein Nmap-Lauf gegen ein stummes Netz die Oberfläche nicht mit einfriert.

11 Anbindung an Ordivis Platform

Die Toolbox kann ihre Befunde an **Ordivis Platform** übergeben — das ITSM- und ITAM-System desselben Hauses. Dieses Kapitel beschreibt die Einrichtung und den Betrieb der Verbindung; was fachlich übertragen wird, steht im Benutzerhandbuch, Kapitel *Ergebnisse an Ordivis übergeben*.

> **Hinweis:** Die Anbindung ist **freiwillig**. Ohne sie fehlt genau eine Menüseite und die Schaltflächen *An Ordivis senden* auf den Werkzeugseiten. Alles andere arbeitet unverändert.

11.1 Vorbereitung auf der Ordivis-Seite

> 🔑 **Rechte:** Eine Administratorin von Ordivis Platform stellt den Token unter *Einstellungen* ▸ *Plattform* ▸ *Integrations-Token* aus.

Der Token ist an einen **Mandanten** gebunden. Nach dem Verbindungstest zeigt die Toolbox dessen Anzeigenamen an — das ist die Kontrolle, dass an die richtige Stelle gemeldet wird.

> **Achtung:** Der Token trägt **Schreibrecht auf das IPAM**. Behandeln Sie ihn wie ein Kennwort: Weitergabe nur an die Person, die ihn einträgt, nicht per E-Mail an einen Verteiler, und ein eigener Token je Arbeitsplatz, wo das zumutbar ist — dann lässt sich ein einzelner zurückziehen, ohne alle zu treffen.

11.2 Einrichtung in der Toolbox

> 💻 **Menü:** *Ordivis* · 🔑 **Rechte:** Standardbenutzer

1. *Ordivis-Adresse (URL)* eintragen, etwa `https://ordivis.firma.local:5001`.
2. *Integrations-Token* einfügen.
3. *Verbindung testen & speichern*.

> ✅ **Ergebnis:** *Verbunden (\<Mandant>)*. Die Toolbox hat dafür `GET /api/v1/ipam/ingest/health` abgefragt.

> **Hinweis:** Ist bereits ein Token gespeichert, lassen Sie das Feld beim erneuten Speichern **leer** — dann bleibt der vorhandene Token unverändert. Er lässt sich nicht wieder anzeigen.

11.2.1 Wie Endpunkt und Token abgelegt werden

Wert	Schlüssel in `settings.json`	Form
Endpunkt	`InfraDeskEndpoint`	Klartext
Token	`InfraDeskTokenProtected`	DPAPI-verschlüsselt, Base64
Mandantenname	`InfraDeskTenantName`	Klartext, aus dem Verbindungstest
Zertifikatsprüfung	`InfraDeskAllowInvalidCert`	`True` / `False`

Achtung: Die vier Schlüssel tragen noch das Präfix `InfraDesk…` und dürfen **nicht** umbenannt werden — sie sind die Schlüssel in bestehenden Dateien. Näheres im Kapitel *Datenablage und Konfiguration*.

Der Token ist an **Benutzerkonto und Rechner** gebunden. Er lässt sich nicht vorbelegen und nicht auf einen anderen Rechner mitnehmen.

11.3 Zertifikatsprüfung

Standardmäßig wird das Serverzertifikat des Endpunkts **geprüft**.

Achtung: Über diese Verbindung reist ein Token mit Schreibrecht. Wer die Prüfung abschaltet, nimmt jedes Zertifikat an — und damit auch das eines Angreifers, der sich in die Verbindung hängt. Der Token wäre dann seiner.

Abschalten ist nur dann richtig, wenn die Ordivis-Installation wirklich ein **selbstsigniertes** Zertifikat benutzt. Und selbst dann ist die bessere Lösung:

Empfehlung: Nehmen Sie die ausstellende Zertifizierungsstelle in die vertrauenswürdigen Stammzertifizierungsstellen der Arbeitsplätze auf — per Gruppenrichtlinie, einmal für alle. Danach greift die Prüfung wieder, und der Schalter bleibt aus.

Achtung: Setzen Sie `InfraDeskAllowInvalidCert` **nicht** per Verteilskript. Diese Entscheidung gehört an die Stelle, an der jemand das Zertifikat der eigenen Installation kennt.

11.4 Der Offline-Zwischenspeicher

Ist Ordivis beim Senden nicht erreichbar, wird das Paket lokal abgelegt:

```
%LOCALAPPDATA%\OrdivisToolbox\outbox\<Paketkennung>.json
```

Über *Jetzt synchronisieren* werden die wartenden Pakete übertragen und nach Erfolg gelöscht.

Drei Verhaltensregeln, die für den Betrieb zählen:

Fall	Verhalten
Netzfehler (Server nicht erreichbar)	Paket wandert in die Warteschlange
Ablehnung durch den Server (4xx/5xx)	Paket wandert **nicht** in die Warteschlange — ein zweiter Versuch brächte denselben Fehler
Abbruch durch den Benutzer	Kein Offline-Fall; das Paket wird verworfen

Hinweis: Ein erneuter Versand ist **gefahrlos**. Jedes Paket trägt eine eigene Kennung, an der Ordivis erkennt, dass es dieses schon hatte — es entstehen keine Dubletten.

Hinweis: Wächst die Warteschlange über längere Zeit, ist entweder der Endpunkt dauerhaft nicht erreichbar oder der Token abgelaufen. Der Fall „abgelaufener Token" füllt die Warteschlange **nicht** — er führt zu *„Von Ordivis abgelehnt."* Eine wachsende Warteschlange ist also immer ein Erreichbarkeitsproblem.

11.5 Was übertragen wird — und was nicht

Die vollständige Aufstellung steht im Benutzerhandbuch. Für die Freigabe durch Datenschutz und Informationssicherheit sind vor allem die Ausnahmen wichtig:

Wichtig — ausdrücklich NICHT übertragen:

- **LAPS-Kennwörter** und **BitLocker-Wiederherstellungsschlüssel**, obwohl sie im Verzeichnis teils an denselben Computerobjekten hängen.
- **Private Schlüssel** von Zertifikaten — nur die öffentlichen Merkmale.
- **Stammzertifizierungsstellen** — sie sind Windows-Ausstattung und kein Inventar der Organisation.
- **Deaktivierte Computerkonten.**

Übertragen werden Bestandsangaben: IP-Adressen, Hostnamen, offene Ports, erkannte Dienste und Betriebssysteme, AD-Computerobjekte mit Betriebssystem und Organisationseinheit, Subnetze, Zertifikatsmerkmale, DNS-Namen, installierte Software und Schwachstellenbefunde.

Wichtig: Alles landet in Ordivis zunächst als **Fund**, nicht als Bestandsdatensatz. Erst durch Bestätigung dort wird daraus ein Configuration Item.

11.6 Betriebsempfehlungen

1. **Ein Token je Arbeitsplatz**, wo möglich — dann lässt sich ein einzelner zurückziehen.

2. **Endpunkt zentral vorbelegen** (`InfraDeskEndpoint` im Anmeldeskript), Token nicht. Das erspart das Abtippen der Adresse und ihre Tippfehler.
3. **Den Mandantennamen nach dem Verbindungstest prüfen lassen.** Er ist die einzige Kontrolle, dass ein Token zum richtigen Mandanten gehört.
4. **Beim Ausscheiden eines Arbeitsplatzes den Token in Ordivis zurückziehen.** Die Deinstallation der Toolbox entfernt den Datenordner nicht — der verschlüsselte Token bleibt liegen. Er ist zwar an Konto und Rechner gebunden, aber ein zurückgezogener Token ist die verlässlichere Grenze.

12 Zeitsynchronisation im Netz

Die Toolbox bringt mit *NTP & Zeitzonen* ein Werkzeug mit, das die Zeit **eines** Rechners prüft und stellt. Dieses Kapitel behandelt, was darunter liegt: die Zeitversorgung des Netzes — denn wer die Uhr eines einzelnen Rechners stellt, hat selten das Problem gelöst.

12.1 Warum das zählt

Wirkung	Ab welcher Abweichung
Kerberos verwirft Tickets — keine Anmeldung, keine AD-Abfrage	**5 Minuten** (Vorgabe)
Zertifikate gelten als noch nicht oder nicht mehr gültig	Je nach Gültigkeitsfenster
Protokolle mehrerer Systeme lassen sich nicht zusammenführen	Sekunden
Geplante Aufgaben und Sicherungen laufen zur falschen Zeit	Minuten
Signaturen und Zeitstempel werden abgelehnt	Je nach Verfahren

Achtung: Ein Zeitproblem sieht nie nach einem Zeitproblem aus. Es sieht aus wie „die Anmeldung geht nicht" oder „das Zertifikat wird nicht angenommen". Wenn mehrere unzusammenhängende Dinge gleichzeitig aufhören zu funktionieren, prüfen Sie die Uhr **zuerst**.

12.2 Die Kette in einer Domäne

Windows baut die Zeitversorgung als Kette:

1. Der Domain Controller mit der **PDC-Emulator-Rolle** der Stammdomäne holt die Zeit von einer **externen** Quelle.
2. Alle übrigen Domain Controller holen sie von ihm — über die AD-Hierarchie.
3. Mitgliedsserver und Arbeitsplätze holen sie von ihrem Domain Controller.

Wichtig: Genau **ein** Rechner im Wald bezieht die Zeit von außen. Wer auf mehreren Domain Controllern eine externe Quelle einträgt, erzeugt zwei Wahrheiten.

Welcher DC den PDC-Emulator hält, sagt die Toolbox: *Active Directory ▸ AD Diagnose ▸ FSMO Rollen Inhaber*.

12.3 Die externe Quelle einrichten

⚙️ **Außerhalb:** Eingabeaufforderung auf dem PDC-Emulator · 🔑 **Rechte:** lokaler Administrator auf dem DC

```
w32tm /config /manualpeerlist:"ptbtime1.ptb.de ptbtime2.ptb.de de.pool.ntp.org"
/syncfromflags:manual /reliable:yes /update
```

Danach den Dienst neu starten und einen Abgleich anstoßen:

```
net stop w32time && net start w32time
w32tm /resync /rediscover
```

Tipp: In Deutschland sind `ptbtime1.ptb.de` bis `ptbtime3.ptb.de` die Zeitserver der Physikalisch-Technischen Bundesanstalt und damit die amtliche Quelle. Mehrere Server eintragen: Fällt einer aus, übernimmt der nächste.

Voraussetzung: UDP 123 ausgehend muss vom PDC-Emulator ins Internet erlaubt sein. Wo das nicht geht, nehmen Sie eine interne Quelle — eine Funkuhr-Appliance oder einen GPS-Empfänger.

12.4 Die Kette prüfen

⚙ **Außerhalb:** Eingabeaufforderung

Befehl	Antwortet auf
`w32tm /query /status`	Woher holt **dieser** Rechner die Zeit, und wie genau ist sie?
`w32tm /query /source`	Nur die Quelle
`w32tm /query /configuration`	Die vollständige Einstellung
`w32tm /monitor /domain:contoso.local`	Die Abweichung **aller** Domain Controller auf einen Blick
`w32tm /stripchart /computer:dc01 /samples:5 /dataonly`	Der laufende Unterschied zu einem bestimmten Rechner

Tipp: `w32tm /monitor /domain:` ist der schnellste Weg zum Befund. Er zeigt je DC Quelle und Abweichung — wenn dort einer aus der Reihe tanzt, ist er der Grund.

Was die Toolbox dazu beiträgt: Auf *NTP & Zeitzonen* tragen Sie unter *Eigener Server* den internen Zeitserver ein und lassen die drei öffentlichen Referenzen stehen. Weichen **alle** ab, geht die eigene Uhr falsch; weicht **nur der interne** ab, geht er falsch — und mit ihm die ganze Domäne.

12.5 Rechner außerhalb der Domäne

Auf einem Rechner ohne Domäne holt Windows die Zeit von `time.windows.com`. Das ist oft ungenau und in abgeschotteten Netzen gar nicht erreichbar.

```
w32tm /config /manualpeerlist:"zeitserver.firma.local" /syncfromflags:manual /update
net stop w32time && net start w32time
w32tm /resync
```

Für einen einzelnen Rechner, bei dem der Zeitdienst nicht greift, ist die Funktion *Zeitabgleich prüfen ▸ Synchronisieren* in der Toolbox der schnelle Weg.

Achtung: Auf einem **Domänenmitglied** ist der Handeingriff über die Toolbox fast immer der falsche Weg: Windows holt sich die Zeit ohnehin vom Domain Controller, und die Handkorrektur wird beim nächsten Abgleich überschrieben. Wenn ein Domänenmitglied dauerhaft falsch geht, liegt der Fehler in der Kette — nicht auf diesem Rechner.

12.6 Virtualisierung

Stolperfalle: Virtuelle Maschinen bekommen von ihrem Wirt eine Zeitsynchronisation angeboten. Auf einem **virtualisierten Domain Controller** ist das eine Falle: Der DC nimmt dann die Zeit des Wirts statt der der Kette, und wenn der Wirt selbst falsch geht, zieht er die ganze Domäne mit.

Auf Hyper-V: Die Integrationsdienst-Komponente *Zeitsynchronisierung* für den Domain Controller **abschalten**. Auf VMware: *Synchronize guest time with host* abschalten.

12.7 Die Zeitzone

Die Zeitzone ist **nicht** dasselbe wie die Uhrzeit. Windows speichert die Zeit intern in UTC und rechnet sie für die Anzeige um.

Achtung: Eine falsche Zeitzone verschiebt die **Anzeige**, nicht die tatsächliche Zeit. Sie zu ändern, um eine Abweichung zu korrigieren, ist der häufigste Fehler an dieser Stelle: Die Anzeige stimmt danach, die Abweichung gegenüber allen anderen Systemen bleibt bestehen. Erst die Zone richtig setzen, dann die Zeit prüfen.

Setzen lässt sie sich in der Toolbox (*NTP & Zeitzonen ▸ Zeitzone auf System anwenden*) oder auf der Konsole:

```
tzutil /g
tzutil /s "W. Europe Standard Time"
```

Zentral setzt man sie per Gruppenrichtlinie oder Skript — nicht von Hand auf jedem Gerät.

13 Sicherheit und Datenschutz

Dieses Kapitel ist für die Freigabe gedacht: Was tut die Toolbox, was sendet sie, wo entstehen Risiken und wie werden sie eingegrenzt.

13.1 Kurzfassung für die Freigabe

Frage	Antwort
Läuft ein Dienst oder Agent?	**Nein.** Nur die Anwendung, solange ihr Fenster offen ist.
Werden Daten an den Hersteller gesendet?	**Nein.** Es gibt keine Telemetrie, keine Nutzungsstatistik, keine Fehlerübermittlung.
Wird eine Anmeldung verlangt?	**Nein.** Keine Lizenz, keine Aktivierung, kein Konto.
Öffnet sie eingehende Ports?	**Nein.** Sie ist ausschließlich Client.
Schreibt sie in die Registrierung?	**Nein**, außer dem Deinstallationseintrag des Setups.
Wo liegen die Daten?	Ausschließlich im Profil des angemeldeten Benutzers.
Werden Geheimnisse verschlüsselt?	**Ja**, mit Windows DPAPI im Benutzerkontext.
Verlassen Daten den Rechner?	Nur bei den im Abschnitt *Ausgehender Datenverkehr* benannten Werkzeugen.

13.2 Ausgehender Datenverkehr

Die vollständige Aufstellung mit Zielen und Ports steht im Kapitel *Netzwerkanforderungen*. Nach dem, was tatsächlich **Ihre** Daten enthält, gestaffelt:

13.2.1 Was Daten über Ihre Umgebung überträgt

Werkzeug	An wen	Was
Sicherheits-Check (CVE & WID)	`cve.circl.lu`	Hersteller- und Produktnamen der auf dem aufgenommenen System installierten Software
MAC Scanner, manuelle Suche	`api.macvendors.com`	Die eingegebene MAC-Adresse
Standortabfrage	`ip-api.com`	Die abgefragte **öffentliche** IP-Adresse
Netzblock- und ASN-Abfrage	`api.bgpview.io`	Die abgefragte **öffentliche** IP-Adresse
WHOIS / RDAP	Der gewählte Server, `rdap.arin.net`	Die eingegebene Domain oder IP-Adresse

Werkzeug	An wen	Was
Kartenansichten	`openstreetmap.org`, `unpkg.com`	Die anzuzeigenden Koordinaten

13.2.2 Was nur lädt und nichts überträgt

Speedtest-Server, `nmap.org`, Winget-Quellen, Windows Update — und der Ping auf `1.1.1.1` in der Statusanzeige des Dashboards.

13.2.3 Was nie übertragen wird

Wichtig: Private Adressen (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16) und Loopback gehen an **keinen** dieser Dienste. Die Standortabfrage prüft das ausdrücklich und überspringt private Adressen. Über die interne Netzstruktur erfährt kein externer Dienst etwas.

13.2.4 Der Sicherheits-Check verdient eine eigene Entscheidung

Achtung: Der Sicherheits-Check überträgt eine **Liste von Hersteller- und Produktnamen** an einen Dienst im Internet. Es fehlen Versionsnummern, Rechnernamen und Kennungen — die Liste sagt aber etwas über das aufgenommene System aus. Auf besonders schützenswerten Systemen und in abgeschotteten Netzen sollte er nicht benutzt werden.

Sperren lässt er sich, indem `cve.circl.lu` am Übergang geblockt wird. Alle übrigen Funktionen des System Inspectors bleiben davon unberührt.

Grenze: Der Abgleich geschieht über Hersteller und erstes Wort des Produktnamens, **nicht über die Version**. Ein Treffer bedeutet „zu diesem Produkt sind Schwachstellen bekannt", nicht „diese Installation ist verwundbar". Der Check ist eine Vorsortierung und kein Schwachstellenscanner — er ersetzt kein Schwachstellenmanagement.

13.3 Was die Toolbox auf dem Rechner anlegt

Vollständig im Kapitel *Datenablage und Konfiguration*. Für die Freigabe genügt:

- Ein Ordner im Benutzerprofil: `%LOCALAPPDATA%\OrdivisToolbox`.
- Darin Einstellungen, gespeicherte Verbindungen, ein lokales Arbeitsprotokoll, die Warteschlange der Ordivis-Anbindung, ein Browserprofil und zwei Protokolldateien.
- Kein Autostart, keine geplante Aufgabe, kein Dienst, kein Treiber.

Wichtig: Die **Deinstallation entfernt diesen Ordner nicht.** Bei einer Geräterückgabe gehört er in die Löschliste — dort liegen das verschlüsselte AD-Kennwort, der Ordivis-Token und die Remote-Kennwörter.

13.4 Datenschutz und Mitbestimmung

Vier Funktionen berühren personenbezogene Daten oder eignen sich zur Verhaltenskontrolle. Sie brauchen eine Entscheidung, bevor sie gebraucht werden — in dieser Reihenfolge, denn so tief greifen sie:

13.4.1 Paket-Mitschnitt

Er zeigt **jedes IPv4-Paket** der gewählten Karte mit Quelle, Ziel und Ports — also lückenlos, wer mit wem spricht. Von allen Werkzeugen der Toolbox greift dieses am tiefsten: Auf einem Netzsegment mit Arbeitsplätzen ist ein Mitschnitt eine Verhaltensüberwachung, auch wenn er nur zur Störungssuche läuft.

Achtung: Er schreibt **nichts auf die Platte** — die letzten 1 000 Pakete stehen im Arbeitsspeicher und sind beim Verlassen der Seite fort. Das mindert die Eingriffstiefe, hebt sie aber nicht auf: Was auf dem Bildschirm steht, ist gesehen.

13.4.2 Verbindungen, Dashboard und Topologie

Sie zeigen, **welcher Prozess mit welcher Gegenstelle spricht** — auf dem Rechner, auf dem die Toolbox läuft. Auf dem eigenen Arbeitsgerät ist das unproblematisch. Auf dem Gerät einer anderen Person — etwa im Rahmen einer Fernwartung — ist es eine Einsicht in deren Arbeitsverhalten.

13.4.3 System Inspector und Service & Process Controller

Sie lesen von einem entfernten System die laufenden Prozesse, die Dienste und die **installierte Software**. Die Softwareliste eines Arbeitsplatzrechners sagt etwas über die Person aus, die daran arbeitet.

13.4.4 AD Suche und AD Benutzer-Manager

Sie zeigen und ändern **Personendaten** aus dem Verzeichnis: Namen, Telefonnummern, Adressen, Vorgesetzte, Personalnummern, letzte Anmeldung.

Achtung: Wo Beschäftigte betroffen sein können, ist der Einsatz solcher Werkzeuge nach § 87 Abs. 1 Nr. 6 BetrVG **mitbestimmungspflichtig**. Klären Sie ihn mit der Personalvertretung und der oder dem Datenschutzbeauftragten, **bevor** Sie ihn brauchen. Eine Regelung, die im Störungsfall erst noch verhandelt werden muss, hilft niemandem.

Für das Verarbeitungsverzeichnis nach Art. 30 DSGVO ist festzuhalten: Die Toolbox **speichert** keine Personendaten dauerhaft. Sie zeigt an, was im Verzeichnis und auf dem Zielsystem ohnehin steht. Dauerhaft abgelegt werden nur der Name des hinterlegten Dienstkontos und — im lokalen Arbeitsprotokoll des AD-Managers — Zeitstempel, ausführendes Konto und Zielobjekt der ausgeführten Änderungen.

13.5 Rechtlicher Rahmen der aktiven Werkzeuge

Achtung: *IP Scanner*, *DHCP Scanner* und *SNMP Inspector* senden Pakete an fremde Geräte. Ein Portscan gegen ein Netz, für das keine Erlaubnis vorliegt, ist in Deutschland strafbar (§ 202a ff. StGB). Setzen Sie sie nur in Netzen ein, für die Sie zuständig sind oder für die eine **schriftliche** Erlaubnis vorliegt.

Achtung: Das Nmap-Profil *Security Audit* (`--script vuln`) führt aktive Prüf-Skripte gegen gefundene Dienste aus. Ältere Geräte — Drucker, Steuerungen, Medizintechnik — können daran hängenbleiben oder abstürzen. Kündigen Sie solche Läufe an, und führen Sie sie nicht im laufenden Betrieb aus.

13.6 Härtungsempfehlungen

1. `RunAsAdmin` **nicht flächendeckend setzen.** Nur dort, wo regelmäßig Dienste gesteuert oder die HOSTS-Datei bearbeitet wird.
2. **Ein delegiertes Dienstkonto hinterlegen**, nicht das eines Domänen-Administrators (Kapitel *Rechte und Berechtigungen*).
3. **LAPS- und BitLocker-Leserechte eng halten.** Wer sie hat, kommt auf jeden Rechner und an jede verschlüsselte Platte.
4. **Kennwortfelder im Remote Manager leer lassen**, wo das Ziel hoch privilegiert ist — das Kennwort verlässt beim Verbinden den geschützten Bereich (Kapitel *Zugangsdaten und Kryptografie*).
5. **PowerShell-Skriptblockprotokollierung prüfen**, bevor ein privilegiertes Konto hinterlegt wird: Aufrufe mit eingebettetem Kennwort landen sonst im Ereignisprotokoll.
6. **Ausgehenden Verkehr staffeln**, statt ihn ganz zu erlauben oder ganz zu sperren (Kapitel *Netzwerkanforderungen*, Abschnitt *Ausgehende Sperrung, gezielt*).
7. **Zertifikatsprüfung des Ordivis-Endpunkts anlassen** und stattdessen die ausstellende CA in die vertrauenswürdigen Stammzertifizierungsstellen aufnehmen.
8. **Den Datenordner in die Geräterückgabe aufnehmen.**
9. **Nmap nur dort ausrollen, wo es gebraucht wird** — es bringt den Npcap-Netzwerktreiber mit.

13.7 Schwachstellen melden

Sicherheitslücken in der Ordivis Toolbox melden Sie über den Weg, der unter https://ordivis.eu/produktsicherheit.html beschrieben ist. Dort steht auch, in welchem Zeitrahmen mit einer Rückmeldung zu rechnen ist.

14 Protokolle und Fehlersuche

14.1 Welche Protokolle es gibt

Die Toolbox schreibt zwei Protokolldateien, beide im Datenordner `%LOCALAPPDATA%\OrdivisToolbox`:

Datei	Inhalt	Wann sie entsteht
`crash.log`	Unbehandelte Ausnahmen mit vollständiger Aufrufkette	Bei einem Absturz
`karte.log`	Warum eine Kartenansicht nicht erschien	Wenn die eingebettete Anzeige nicht bereit war

Dazu, fachlich und kein Betriebsprotokoll:

Datei	Inhalt
`ad_audit_log.json`	Die über den AD-Benutzer-Manager ausgeführten Änderungen

Wichtig: Es gibt **kein** laufendes Betriebsprotokoll und keinen Ausführlichkeitsschalter. Die Toolbox schreibt nur, wenn etwas schiefging.

14.2 `crash.log`

Jeder Eintrag beginnt mit Zeitstempel und Quelle:

```
--- 2026-08-28 15:04:12 +02:00 [UI] ---
System.NullReferenceException: Object reference not set to an instance of an object.
   at OrdivisToolbox.Pages ...
```

Drei Quellen kommen vor:

Quelle	Bedeutung
`[UI]`	Ausnahme im Oberflächenstrang
`[Domain]`	Ausnahme außerhalb der Oberfläche
`[Task]`	Ausnahme in einer Hintergrundaufgabe, die niemand abgeholt hat

Hinweis: Die Datei wird **angehängt** und ist gedeckelt: Überschreitet sie ein Megabyte, fängt sie von vorn an. Nach einem Absturz also **zeitnah** sichern — nicht nach zwei Wochen Weiterarbeit.

> **Hinweis:** Ohne diese Protokollierung verschwände die Anwendung bei einem Fehler in einem asynchronen Ereignishandler **spurlos** — weder im Ereignisprotokoll noch sonst wo stünde etwas. Der Absturz bleibt ein Absturz, hinterlässt aber eine lesbare Spur.

14.3 `karte.log`

Kartenansichten kommen in *Basis Scanner*, *Zone Lookup* und *Trace (MTR)* vor. Wenn dort nur eine leere Fläche steht, sagt diese Datei, warum:

Eintrag	Ursache
Karte übersprungen: WebView2 war noch nicht bereit.	Die Komponente war beim Zeichnen noch nicht gestartet — oder sie fehlt
FEHLER bei Navigate: …	Die Adresse ließ sich nicht laden, meist mangels Internetzugang

> **Hinweis:** Eine fehlende Karte betrifft nur die Karte. DNS-Auflösung, Portprüfung, Zertifikatsanalyse und Laufzeitmessung derselben Seite laufen unabhängig davon und sind vollständig.

14.4 Vorgehen bei einer Störung

14.4.1 Schritt 1 — die drei Grundfragen

1. **Läuft die Toolbox als Administrator?** Probe: *Service & Process Controller* öffnen — fehlen die Rechte, steht dort ein roter Hinweis.
2. **Ist der Rechner Domänenmitglied und erreicht er einen DC?** Probe: *AD Diagnose* öffnen.
3. **Ist das benötigte externe Werkzeug installiert?** Probe: Die betreffende Seite sagt es selbst und bietet die Nachinstallation an.

14.4.2 Schritt 2 — die Meldung wörtlich lesen

Die Toolbox gibt die Fehler der aufgerufenen Werkzeuge **unverändert** weiter. Was `dcdiag`, `repadmin`, `certreq`, `openssl` oder PowerShell melden, steht wörtlich in der Oberfläche — das ist meist die eigentliche Auskunft.

14.4.3 Schritt 3 — außerhalb der Toolbox gegenprüfen

Fast jede Funktion hat ein Gegenstück auf der Konsole. Wenn das ebenfalls scheitert, liegt es nicht an der Toolbox:

Toolbox	Gegenprobe
System Inspector, Service Controller	`Test-WSMan -ComputerName <Ziel>`
AD-Werkzeuge	`nltest /dsgetdc:<Domäne>`

Toolbox	Gegenprobe
DCDIAG	`dcdiag /s:<DC>`
GPO-Verwaltung	`Get-GPO -All`
AD Papierkorb	`Get-ADOptionalFeature -Filter *`
Basis Scanner, Zone Lookup	`Resolve-DnsName <Name>`
SNMP Inspector	`Test-NetConnection <Ziel> -Port 161` (prüft nur die Erreichbarkeit)
Ordivis-Anbindung	`Invoke-RestMethod https://<endpunkt>/api/v1/ipam/ingest/health -Headers @{Authorization="Bearer <token>"}`
NTP	`w32tm /stripchart /computer:<Server> /samples:5 /dataonly`

14.5 Häufige Störungsbilder

14.5.1 Die Anwendung startet nicht

Beobachtung	Ursache	Abhilfe
Nichts passiert	Sie läuft bereits — es gibt nur eine Instanz je Sitzung	In der Taskleiste suchen; notfalls `OrdivisToolbox.exe` im Task-Manager beenden
UAC-Fenster, danach nichts	`RunAsAdmin` ist gesetzt und die Rückfrage wurde verneint	Bestätigen oder die Einstellung zurücknehmen
Fenster erscheint kurz und verschwindet	Absturz beim Start	`crash.log` ansehen

14.5.2 Alle Einstellungen sind plötzlich weg

Ursache: `settings.json` war beim Start nicht lesbar — dann fängt die Anwendung **wortlos mit leeren Einstellungen** an.

> **Hinweis:** Beim Speichern wird immer erst vollständig daneben geschrieben und dann ersetzt; eine abgeschnittene Datei kann dadurch eigentlich nicht entstehen. Wenn sie es doch ist, prüfen Sie die Platte und den Virenschutz — ein Wächter, der die Ersetzung abfängt, erzeugt genau dieses Bild.

Sehen Sie sich die Datei an, **bevor** Sie alles neu eintragen.

14.5.3 Die Toolbox arbeitet mit alten Einstellungen

Prüfen Sie, ob **beide** Datenordner existieren:

```
%LOCALAPPDATA%\OrdivisToolbox
%LOCALAPPDATA%\NetzDesk
```

Existieren beide, gilt der neue — der alte ist ein Rest. Existiert **nur** der alte, ist der einmalige Umzug nie gelungen: Er wird bei jedem Start erneut versucht, aber nur, wenn keine Datei darin offen ist. Beenden Sie die Toolbox, schließen Sie alles, was auf den Ordner zugreift, und starten Sie erneut.

14.5.4 Listen bleiben leer oder unvollständig

Werkzeug	Ursache
Verbindungen, Spalte *Prozess*	Keine Administratorrechte
System Inspector, *Service Controller*	WinRM nicht aktiv, Port gesperrt, Konto nicht berechtigt
GPO-Verwaltung	RSAT *Gruppenrichtlinienverwaltung* fehlt
AD Papierkorb	Der Papierkorb ist in der Domäne nicht aktiviert
AD Suche, LAPS/BitLocker	Kein Leserecht auf die Attribute — oder es gibt wirklich keine

14.5.5 Ordivis-Warteschlange wächst

Eine wachsende Warteschlange ist **immer** ein Erreichbarkeitsproblem: Ein abgelehntes Paket landet nicht darin.

1. *Ordivis* öffnen, *Verbindung testen & speichern* (ohne Token-Eingabe).
2. Kommt *Verbunden*, klicken Sie auf *Jetzt synchronisieren*.
3. Kommt eine Fehlermeldung, prüfen Sie Endpunkt, Erreichbarkeit und Zertifikat.

14.5.6 Der PDF-Druck der GPO-Berichte oder die Karte bleibt leer

Die WebView2-Laufzeit fehlt oder ist beschädigt. Siehe `karte.log` und das Kapitel *Externe Werkzeuge und Abhängigkeiten*. Ein beschädigtes Profil lässt sich zurücksetzen, indem der Ordner `WebView2` im Datenordner bei beendeter Toolbox gelöscht wird — er wird neu angelegt.

14.6 Was in eine Störungsmeldung gehört

Damit eine Rückfrage nicht nötig wird:

1. **Programmversion** — Statusleiste unten rechts, Form `2026.08.07.001`.
2. **Betroffenes Werkzeug** mit vollständigem Menüpfad.
3. **Die Meldung im Wortlaut** — abgetippt oder als Bildschirmfoto.
4. **Was erwartet wurde** und was stattdessen geschah.
5. Bei einem Absturz: die letzten Einträge aus `crash.log`.
6. Ob die Toolbox **als Administrator** lief.
7. Ob der Rechner **Domänenmitglied** ist.

Achtung: Bevor Sie ein Bildschirmfoto weitergeben: Es kann Hostnamen, IP-Adressen, Benutzernamen — und im Fall von *AD Suche* auch BitLocker-Schlüssel oder LAPS-Kennwörter enthalten. Sehen Sie hin, bevor Sie es anhängen.

Meldungen: https://ordivis.eu/kontakt.html

15 Betrieb, Updates und Support

15.1 Versionsschema

Die Ordivis Toolbox wird nach Datum versioniert:

```
JJJJ.MM.TT.NNN
2026.08.07.001
```

`NNN` ist die laufende Nummer der Auslieferungen dieses Tages. Aus der Nummer lässt sich also unmittelbar ablesen, wie alt ein Stand ist.

> **Hinweis:** Die **angezeigte** Version trägt führende Nullen (`2026.08.07.001`), die **Dateiversion** nicht (`2026.8.7.1`). Erkennungsregeln, die Zeichenketten vergleichen, müssen darauf achten; ein Vergleich nach `[version]` funktioniert in beiden Formen.

Wo die Version steht:

Ort	Form
Statusleiste unten rechts	`Grams IT | v2026.08.07.001`
Einstellungen, Fußzeile	*Ordivis Toolbox v2026.08.07.001 — Entwickelt von Grams IT*
Registrierung, `DisplayVersion`	`2026.08.07.001`
Dateieigenschaften der EXE	`2026.8.7.1`

15.2 Es gibt keine automatische Aktualisierung

> **Wichtig:** Die Toolbox prüft **nicht** selbst auf neue Fassungen, lädt nichts nach und meldet keinen verfügbaren Stand. Das ist Absicht: Sie ist ein Werkzeug für Fachleute, das in verwalteten Umgebungen ausgebracht wird — dort entscheidet die Verteilung, wann welcher Stand kommt, nicht das Programm.

Ein Update ist ein gewöhnlicher Lauf des neuen Installationsprogramms über die vorhandene Installation. Wie das unbeaufsichtigt geht, steht im Kapitel *Verteilung im Netz*.

15.3 Wie Sie von neuen Fassungen erfahren

Quelle	Was dort steht
https://ordivis.eu/toolbox/	Der aktuelle Stand zum Herunterladen

Quelle	Was dort steht
https://ordivis.eu/toolbox/changelog.html	Was sich je Fassung geändert hat
https://ordivis.eu/dokumentation.html	Die Handbücher, jeweils zum ausgelieferten Stand

Tipp: Die Handbücher tragen auf der Titelseite die **Produktversion**, zu der sie gesetzt wurden. Weicht sie vom installierten Stand ab, kann die Oberfläche in Einzelheiten abweichen.

15.4 Ein Update planen

Eine brauchbare Reihenfolge für eine verwaltete Umgebung:

1. **Änderungen lesen.** Der Änderungsverlauf sagt, ob überhaupt etwas dabei ist, was Sie betrifft.
2. **Auf einem Gerät prüfen.** Die Toolbox hat keine serverseitigen Abhängigkeiten; ein einzelnes Gerät genügt als Probe.
3. **Verteilen**, außerhalb der Arbeitszeit — die Anwendung darf beim Upgrade nicht laufen.
4. **Erkennung prüfen.** Nach dem Lauf sollte `DisplayVersion` im Registrierungsschlüssel den neuen Stand tragen.

Hinweis: Ein Update fasst den Datenordner im Benutzerprofil **nicht** an. Einstellungen, hinterlegtes AD-Konto, Remote-Verbindungen, Ordivis-Anbindung und die Warteschlange bleiben erhalten.

15.5 Zurückgehen auf eine ältere Fassung

Ein Rückschritt ist möglich: die ältere Fassung installieren, nachdem die neuere deinstalliert wurde.

Achtung: Das Installationsprogramm verweigert eine ältere Fassung nicht ausdrücklich, aber ein Wechsel ohne vorherige Deinstallation ist ungetestet. Deinstallieren Sie zuerst; der Datenordner bleibt dabei ohnehin erhalten.

Hinweis: Eine Einbahnstraße gibt es: Wurde das AD-Kennwort einmal in die verschlüsselte Form überführt, liest eine sehr alte Fassung, die nur das Base64-Format kennt, es nicht mehr. Sie fragt dann nach dem Kennwort — kein Datenverlust, aber eine erneute Eingabe.

15.6 Betrieb auf mehreren Benutzerprofilen

Die Toolbox wird **maschinenweit** installiert, legt ihre Daten aber **je Benutzerprofil** an. Auf einem gemeinsam genutzten Gerät bedeutet das:

- Jede Person hat eigene Einstellungen, eigene Remote-Verbindungen, ein eigenes hinterlegtes AD-Konto und einen eigenen Ordivis-Token.

- Keine Person kann die Geheimnisse einer anderen lesen — DPAPI bindet sie an das Benutzerkonto.
- Beim Aufräumen muss der Datenordner **je Profil** entfernt werden (Kapitel *Verteilung im Netz*).

> **Hinweis:** Es läuft **eine** Instanz je Sitzung. Auf einem Terminalserver mit mehreren gleichzeitigen Sitzungen läuft in jeder Sitzung eine eigene Instanz — der Ausschluss gilt je Sitzung, nicht je Rechner.

15.7 Support

Anliegen	Weg
Fragen zur Bedienung	Benutzerhandbuch, https://ordivis.eu/dokumentation.html
Fragen zum Betrieb	Dieses Handbuch
Fehlermeldungen und Rückmeldungen	https://ordivis.eu/kontakt.html
Sicherheitslücken	https://ordivis.eu/produktsicherheit.html
Was sich geändert hat	https://ordivis.eu/toolbox/changelog.html

Was in eine Störungsmeldung gehört, steht im Kapitel *Protokolle und Fehlersuche*.

> **Hinweis:** Die Ordivis Toolbox ist ein **kostenloses** Produkt. Es gibt dazu keine Reaktionszeitvereinbarung. Für Ordivis Platform gelten eigene Bedingungen, siehe https://ordivis.eu/sla.html.

16 Anhang

16.1 A — Schlüssel in `settings.json`

Ablage: `%LOCALAPPDATA%\OrdivisToolbox\settings.json`. Alle Werte sind Zeichenketten.

Schlüssel	Werte	Vorgabe	Verschlüsselt
`Language`	`de`, `en`	leer	—
`AppTheme`	`Default`, `Light`, `Dark`	`Default`	—
`UpdateInterval`	`200` … `5000`	`1000`	—
`DataUnit`	`Auto`, `KB`, `MB`	`Auto`	—
`RunAsAdmin`	`True`, `False`	`False`	—
`AdDomain`	Text	leer	—
`AdUsername`	Text	leer	—
`AdPasswordProtected`	Base64	leer	**DPAPI**
`AdPassword`	Base64	—	**nein** — veraltet, wird beim Start umgewandelt
`DocSavePath`	Pfad	Desktop	—
`DocLogoPath`	Pfad	leer	—
`DocEmail`	E-Mail	leer	—
`InfraDeskEndpoint`	URL	leer	—
`InfraDeskTokenProtected`	Base64	leer	**DPAPI**
`InfraDeskTenantName`	Text	leer	—
`InfraDeskAllowInvalidCert`	`True`, `False`	`False`	—

Achtung: Die `InfraDesk…`-Schlüssel dürfen nicht umbenannt werden. Näheres im Kapitel *Datenablage und Konfiguration*.

16.2 B — Dateien im Datenordner

Pfad	Inhalt	Bei Geräterückgabe löschen
`settings.json`	Einstellungen samt verschlüsselter Geheimnisse	**ja**
`remotes.json`	Remote-Verbindungen samt verschlüsselter Kennwörter	**ja**
`ad_audit_log.json`	Lokales Arbeitsprotokoll des AD-Managers	**ja**
`outbox\*.json`	Wartende Ordivis-Pakete (Scan-Ergebnisse)	**ja**
`WebView2\`	Browserprofil der eingebetteten Anzeige	ja
`crash.log`	Absturzprotokoll	ja
`karte.log`	Diagnose der Kartenansichten	ja

16.3 C — Ports und Protokolle

16.3.1 Ausgehend, eigenes Netz

Protokoll / Port	Werkzeug
ICMP Echo	Dashboard, ICMP, Trace, IP Scanner, Wake-on-LAN-Prüfung, Remote Manager
UDP 67 / 68 (Broadcast)	DHCP Scanner
UDP 7 / 9 (Broadcast)	Wake on LAN
UDP 123	NTP & Zeitzonen
UDP 161	SNMP Inspector, SNMP-Anreicherung, System Inspector über SNMP
UDP/TCP 53	Basis Scanner, Zone Lookup, SMTP Diagnose
TCP 88 (auch UDP)	Kerberos, für alle AD-Werkzeuge
TCP 135 + dynamische RPC-Ports	AD-Werkzeuge, `certreq`
TCP 389 / 636 / 3268 / 3269	LDAP, LDAPS, Globaler Katalog
TCP 445	SYSVOL für GPO-Berichte
TCP 5985 / 5986	WinRM: System Inspector, Service & Process Controller
TCP 3389 / 22 / 21	Remote Manager: RDP, SSH/SFTP, FTP
TCP, frei gewählt	IP Scanner, Basis Scanner: die geprüften Zielports
TCP, Endpunktport (üblich 5001)	Ordivis Platform

16.3.2 Ausgehend, Internet

Ziel	Port	Werkzeug
`1.1.1.1`	ICMP	Dashboard, Statusanzeige *DNS*
`www.speedtestx.de`, `speed.hetzner.de`, `ash-speed.hetzner.com`	443	Speedtest
`ip-api.com`	**80**	Standortangaben
`api.bgpview.io`	443	Zone Lookup
`www.openstreetmap.org`, `unpkg.com`	443	Kartenansichten
`api.macvendors.com`	443	MAC Scanner, manuelle Suche
`cve.circl.lu`	443	Sicherheits-Check
Gewählter WHOIS-Server	**43**	WHOIS
`rdap.arin.net`	443	RDAP
`nmap.org`	443	Nmap nachinstallieren
Winget-Quellen	443	OpenSSL nachinstallieren
Windows Update / WSUS	80/443	RSAT nachinstallieren

16.4 D — Befehle für die Bereitstellung

Unbeaufsichtigt installieren

```
Ordivis-Toolbox-Setup-<Version>.exe /VERYSILENT /SUPPRESSMSGBOXES /NORESTART /LANG=german
```

Unbeaufsichtigt deinstallieren

```
$k = 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{D3F8A9C1-7B2E-45A6-9012-3456789ABCDE}_is1'
$exe = (Get-ItemProperty $k -ErrorAction SilentlyContinue).UninstallString
if ($exe) { Start-Process $exe.Trim('"') -ArgumentList '/VERYSILENT','/SUPPRESSMSGBOXES','/NORESTART' -Wait }
```

Installierte Version ermitteln

```
(Get-ItemProperty 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{D3F8A9C1-7B2E-45A6-9012-3456789ABCDE}_is1').DisplayVersion
```

RSAT bereitstellen

```
Get-WindowsCapability -Online -Name 'Rsat.ActiveDirectory*','Rsat.GroupPolicy*' |
    Where-Object State -ne 'Installed' | Add-WindowsCapability -Online
```

Nmap unbeaufsichtigt (bringt den Npcap-Treiber mit)

```
nmap-<Version>-setup.exe /S
```

OpenSSL unbeaufsichtigt

```
winget install ShiningLight.OpenSSL --accept-package-agreements --accept-source-
agreements --silent
```

WebView2-Laufzeit unbeaufsichtigt

```
MicrosoftEdgeWebView2RuntimeInstallerX64.exe /silent /install
```

PowerShell Remoting auf dem Ziel

```
Enable-PSRemoting -Force
```

16.5 E — Kennungen

Was	Wert
Anwendungskennung (Inno Setup)	`{D3F8A9C1-7B2E-45A6-9012-3456789ABCDE}`
Deinstallations-Registrierungsschlüssel	`HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{D3F8A9C1-7B2E-45A6-9012-3456789ABCDE}_is1`
Installationspfad (Vorgabe)	`C:\Program Files\Grams IT\Ordivis Toolbox`
Programmdatei	`OrdivisToolbox.exe`
Datenordner	`%LOCALAPPDATA%\OrdivisToolbox`
Datenordner vor der Umbenennung	`%LOCALAPPDATA%\NetzDesk`
Einzelinstanz-Mutex	`OrdivisToolbox_SingleInstance_Mutex`
Dateiname des Setups	`Ordivis-Toolbox-Setup-<Version>.exe`

16.6 F — Von der Toolbox aufgerufene Programme

Programm	Herkunft	Wofür
`powershell.exe`	Windows	AD, GPO, WinRM, DNS-Abfragen, Zeit setzen
`cmd.exe`	Windows	Hilfsaufrufe
`dcdiag.exe`	RSAT	AD Diagnose
`repadmin.exe`	RSAT	Replikationsmonitor
`certreq.exe`	Windows	Zertifikatsanforderung bei AD CS
`tzutil.exe`	Windows	Zeitzone setzen
`cmdkey.exe`	Windows	RDP-Anmeldedaten hinterlegen
`mstsc.exe`	Windows	RDP-Sitzung starten
`notepad.exe`	Windows	HOSTS-Datei bearbeiten
`ServerManager.exe`	RSAT	Server-Manager öffnen
`nmap.exe`	Nmap	IP Scanner, Nmap-Motor
`openssl.exe`	OpenSSL	OpenSSL Converter

16.7 G — Glossar

AD CS — Active Directory Certificate Services, die Zertifizierungsstelle von Microsoft.

DPAPI — Data Protection API. Windows-Verfahren, das Geheimnisse an Benutzerkonto und Rechner bindet.

Features on Demand — Optionale Windows-Bestandteile, die bei Bedarf aus dem Netz nachgeladen werden. RSAT gehört dazu.

FSMO — Die fünf Betriebsmasterrollen im Active Directory.

Inno Setup — Das Werkzeug, mit dem das Installationsprogramm gebaut ist. Es versteht die im Kapitel *Verteilung im Netz* genannten Schalter.

LAPS — Local Administrator Password Solution. Verwaltet lokale Administratorkennwörter und hinterlegt sie im Verzeichnis.

Npcap — Der Mitschnitt-Treiber, den Nmap mitbringt.

PDC-Emulator — Die FSMO-Rolle, deren Inhaber die Zeit für die Domäne vorgibt.

RSAT — Remote Server Administration Tools.

WebView2 — Die eingebettete Browserkomponente von Microsoft.

WinRM — Windows Remote Management. Trägt CIM-Abfragen und PowerShell Remoting (TCP 5985/5986).

Winget — Der Paketverwalter von Windows.

16.8 H — Weiterführende Unterlagen

Was	Wo
Benutzerhandbuch	https://ordivis.eu/dokumentation.html
Produktseite	https://ordivis.eu/toolbox/
Änderungen je Version	https://ordivis.eu/toolbox/changelog.html
Alle Ordivis-Handbücher	https://ordivis.eu/dokumentation.html
Produktsicherheit und Meldewege	https://ordivis.eu/produktsicherheit.html
Barrierefreiheit	https://ordivis.eu/barrierefreiheit.html
Kontakt	https://ordivis.eu/kontakt.html