Ordivis

ORDIVIS TOOLBOX

Benutzerhandbuch

Alle Werkzeuge der Ordivis Toolbox – Schritt für Schritt.

Produktversion 2026.08.07.001 · Handbuch-Revision 1.0

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

TB-B

Inhalt

1 Über dieses Handbuch

Dieses Buch beschreibt **Ordivis Toolbox** aus der Sicht derer, die damit arbeiten: Es erklärt jedes Werkzeug, das im Menü steht, sagt wozu es da ist, was es braucht und was am Ende herauskommt.

Es ist der erste von zwei Bänden.

Band	Kennung	Für wen	Inhalt
Benutzerhandbuch (dieses Buch)	TB-B	Alle, die die Toolbox bedienen	Alle Werkzeuge, Schritt für Schritt
Administratorhandbuch	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.

> **Wichtig:** Die Toolbox ist ein **Werkzeugkasten für Fachleute**. Viele Werkzeuge greifen tief in Netzwerk, Verzeichnisdienst und Betriebssystem ein — ein Kennwort zurücksetzen, einen Dienst beenden, eine FSMO-Rolle verschieben. Dieses Handbuch setzt deshalb voraus, dass Sie wissen, was Sie tun, und benennt an jeder Stelle, wo eine Handlung nicht mehr rückgängig zu machen ist.

1.1 Wie dieses Buch aufgebaut ist

Nach diesem Kapitel folgen drei Blöcke:

- **Grundlagen** — was die Toolbox ist, wie sie bedient wird, wie sie eingerichtet ist.
- **Die Werkzeuge** — ein Kapitel je Menügruppe, in der Reihenfolge des Menüs. Wer im Programm auf einer Seite steht, findet sie hier an derselben Stelle wieder.
- **Anhang** — Fehlerbilder, Fachbegriffe, Verzeichnisse.

Jedes Werkzeug wird nach demselben Muster beschrieben: *Wofür es da ist — was es voraussetzt — wie man es bedient — was das Ergebnis bedeutet*. Wenn Sie ein Werkzeug schon kennen, reichen die ersten beiden Absätze; wenn nicht, führt Sie die nummerierte Schrittfolge hindurch.

1.2 Konventionen und Symbole

Handlungsanweisungen beginnen immer mit einem **Anleitungskopf**. Er nennt den Menüpfad und die Rechte, die die Handlung braucht — bevor Sie den ersten Schritt tun und nicht erst, wenn er scheitert:

> 💻 **Menü:** *Werkzeug-Suiten* ▸ *IP Werkzeuge* ▸ *ARP Tabelle* · 🔑 **Rechte:** Standardbenutzer

Mehr Symbole als diese sechs kommen nicht vor. Jedes trägt sein Wort daneben, damit es auch dann verständlich bleibt, wenn das Zeichen einmal nicht sauber druckt:

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

Farbige Kästen heben Aussagen hervor, die sonst überlesen werden:

Voraussetzung: Gelb — etwas muss vorher erfüllt sein, sonst geht es nicht weiter.

Achtung: Rot — Datenverlust, Betriebsunterbrechung oder ein Eingriff, der sich nicht ohne Weiteres zurücknehmen lässt.

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

Hinweis: Blau — eine Ergänzung zum Verständnis.

Weiter gilt:

- *Kursiv* stehen Beschriftungen der Oberfläche: Schaltflächen, Felder, Reiter, Menüpunkte.
- `Nichtproportionalschrift` steht für alles, was wörtlich eingetippt oder wörtlich angezeigt wird: Pfade, Adressen, Befehle, Dateinamen.
- **Fett** hebt den Begriff hervor, um den es im Satz geht.

1.2.1 Die Rechte-Stufen

Drei Stufen kommen im Anleitungskopf vor. Sie sind nicht dasselbe, und die Toolbox kann die eine nicht durch die andere ersetzen:

Stufe	Was gemeint ist
Standardbenutzer	Ein gewöhnliches Windows-Konto. Kein UAC-Dialog, keine Sonderrechte.
Lokaler Administrator	Die Toolbox muss *als Administrator* laufen (siehe *Immer als Administrator ausführen* im Kapitel Einstellungen).
Domänenrechte	Ein Konto mit Schreibrechten im Active Directory. Es kann Ihr angemeldetes Konto sein oder das in den Einstellungen hinterlegte AD-Administrator-Konto.

> **Hinweis:** Wo *Domänenrechte* stehen, ist damit nicht automatisch *Domänen-Administrator* gemeint. Welches Recht genau nötig ist, steht jeweils beim Werkzeug — meistens genügt eine gezielte Delegation. Das Administratorhandbuch führt die Rechte je Werkzeug in einer Tabelle zusammen.

1.3 Stand dieses Buches

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

Die Programmversion steht jederzeit unten rechts in der Statusleiste des Fensters und in den Einstellungen ganz unten. Weicht sie von der oben genannten ab, kann die Oberfläche in Einzelheiten abweichen; das Handbuch wird mit jeder Auslieferung neu gesetzt.

1.4 Rückmeldungen zum Handbuch

Fehlt etwas, ist etwas missverständlich oder stimmt eine Beschreibung nicht mehr mit dem Programm überein: https://ordivis.eu/kontakt.html. Nennen Sie dabei bitte die Kapitelnummer und die Handbuch-Revision von der Titelseite — beides ändert sich mit jeder Ausgabe.

1.5 Impressum

Ordivis Toolbox ist ein Produkt der Grams IT.

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

Alle in diesem Handbuch genannten Marken- und Produktnamen sind Eigentum ihrer jeweiligen Inhaber. *Windows*, *Active Directory*, *Microsoft Edge* und *PowerShell* sind Marken der 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 — insbesondere bei Eingriffen in Verzeichnisdienst, Zertifikatsdienste und laufende Systeme.

2 Was die Ordivis Toolbox ist

Die Ordivis Toolbox ist eine **Windows-Anwendung mit über dreißig Werkzeugen für Netzwerk, Active Directory, Zertifikate und Systemdiagnose** — zusammengefasst in einem Fenster, mit einer Oberfläche und einer gemeinsamen Einrichtung.

Sie ersetzt den Griff zu einem Dutzend Einzelprogrammen: `ping`, `tracert`, `nslookup`, `arp`, `dcdiag`, `repadmin`, `gpresult`, `certreq`, `openssl`, dazu Nmap, ein SNMP-Werkzeug, ein WHOIS-Werkzeug, ein Paket-Mitschneider und ein Verbindungsmanager für RDP und SFTP. Was diese Programme können, können sie auch in der Toolbox — nur ohne Konsolensyntax, mit auswertbaren Tabellen und mit Ergebnissen, die zueinander passen.

2.1 Wofür sie gemacht ist

Die Toolbox ist das Werkzeug für die **Stelle vor dem Problem**: den Arbeitsplatz der Administratorin, den Laptop des Technikers im Serverraum, den Sprungrechner im Kundennetz. Sie läuft dort, wo das Netz tatsächlich erreichbar ist, und beantwortet Fragen, die sich nur von dort beantworten lassen:

- Welche Geräte antworten in diesem Subnetz, und auf welchen Ports?
- Warum kommt der Rechner nicht an den Domain Controller?
- Wer ist der zweite DHCP-Server, der hier gerade Adressen verteilt?
- Passt dieser private Schlüssel zu diesem Zertifikat?
- Wann läuft das Zertifikat auf dem Webserver ab, und wer hat es ausgestellt?
- Welche Route nimmt der Verkehr zum Rechenzentrum, und wo geht Zeit verloren?
- Ist die Systemzeit dieses Servers noch synchron?

2.2 Wofür sie **nicht** gemacht ist

Ebenso wichtig — damit niemand vergeblich sucht:

- **Kein Monitoring.** Die Toolbox misst, wenn Sie sie starten. Sie läuft nicht als Dienst, alarmiert nicht und schreibt keine Historie fort. Wer dauerhafte Überwachung braucht, braucht ein Monitoringsystem.
- **Keine Bestandsdatenbank.** Ergebnisse stehen in der Anzeige und lassen sich weitergeben, aber die Toolbox verwaltet keinen Bestand. Genau dafür gibt es die Übergabe an **Ordivis Platform** (Kapitel *Ergebnisse an Ordivis übergeben*).
- **Kein Ersatz für die Konsolen.** Wo Microsoft eine MMC mitbringt, kann die Toolbox das Alltägliche schneller — aber nicht alles. Die RSAT-Konsolen lassen sich aus der Toolbox heraus installieren, statt sie zu ersetzen.
- **Kein Angriffswerkzeug.** Scanner und Mitschneider sind Diagnosewerkzeuge. Sie auf fremde Netze zu richten, für die keine Erlaubnis vorliegt, ist in Deutschland strafbar (§ 202a ff. StGB). Der Abschnitt *Was Sie dürfen müssen* sagt dazu mehr.

2.3 Was Sie dürfen müssen

Achtung: Ein Netzwerk-Scan, ein Paket-Mitschnitt und eine WHOIS-Abfrage sind technisch harmlos und rechtlich nicht beliebig. Setzen Sie die Scanner, den Paket-Mitschneider und den SNMP-Inspector **nur in Netzen ein, für die Sie zuständig sind oder für die Ihnen eine schriftliche Erlaubnis vorliegt.**

Für den betrieblichen Einsatz kommt hinzu: Der Paket-Mitschneider, der Verbindungsmonitor und die Prozessliste zeigen, welcher Rechner mit wem spricht. Wo Beschäftigte betroffen sein können, ist das mitbestimmungspflichtig (§ 87 Abs. 1 Nr. 6 BetrVG) und berührt den Datenschutz. Klären Sie den Einsatz mit der Personalvertretung und der oder dem Datenschutzbeauftragten, bevor Sie ihn brauchen — nicht danach.

2.4 Was sie kostet

Die Ordivis Toolbox ist **kostenlos**. Es gibt keine Lizenzdatei, keine Aktivierung, keinen Freischaltcode und keine Funktionen, die hinter einer Bezahlschranke liegen. Der Bezug erfolgt über https://ordivis.eu/toolbox/.

Sie ist zugleich das Werkzeug, mit dem sich **Ordivis Platform** — das ITSM-/ITAM-System desselben Hauses — mit Netzdaten füllen lässt. Diese Verbindung ist ein Angebot und keine Bedingung: Ohne eingerichtete Verbindung fehlt genau eine Menüseite, alles andere arbeitet unverändert.

2.5 Wie sie gebaut ist — in drei Sätzen

Die Toolbox ist eine **native Windows-Anwendung** auf Basis von WinUI 3 und .NET 10. Sie bringt ihre Laufzeitumgebung mit, braucht also kein separat installiertes .NET und kein Framework aus dem Store. Sie speichert ihre Einstellungen im Profil des angemeldeten Benutzers und arbeitet — bis auf wenige, im Administratorhandbuch einzeln benannte Abfragen — ausschließlich in Ihrem eigenen Netz.

Technische Einzelheiten dazu — Systemvoraussetzungen, Ablageorte, ausgehende Verbindungen — stehen im **Administratorhandbuch**.

2.6 Der Aufbau des Programms

Das Fenster gliedert sich in drei Teile, die im ganzen Buch so benannt werden:

- Den **Navigationsbereich** links: das Menü mit allen Werkzeugen, gegliedert in Gruppen. Er lässt sich über die Schaltfläche oben links ein- und ausklappen.
- Die **Arbeitsfläche** rechts: das gewählte Werkzeug.
- Die **Statusleiste** unten: links der Betriebszustand, rechts die Programmversion.

Der Navigationsbereich ist in vier Blöcke geteilt, und diese Gliederung ist zugleich die Gliederung dieses Handbuchs:

Block	Werkzeuge
(ohne Überschrift, ganz oben)	Dashboard, Verbindungen, Pakete (Live), Topologie
Werkzeug-Suiten	Host- & Systemverwaltung, Active Directory, CA & PKI, IP Werkzeuge, Scanner Werkzeuge, DNS Werkzeuge, Remote Werkzeuge, E-Mail Werkzeuge
System & LAN	NTP & Zeitzonen, Wake on LAN, Dokumentation Erstellen
(unten)	Ordivis, Einstellungen

Die Einträge unter *Werkzeug-Suiten* sind **Gruppen**: Ein Klick darauf klappt sie auf, statt eine Seite zu öffnen. Die Werkzeuge liegen eine Ebene darunter.

3 Erste Schritte

Dieses Kapitel bringt Sie von der heruntergeladenen Datei bis zum ersten Ergebnis. Wer die Toolbox bereits installiert vorfindet — weil die IT sie verteilt hat —, beginnt beim Abschnitt *Das Fenster kennenlernen*.

3.1 Voraussetzungen

Punkt	Anforderung
Betriebssystem	Windows 10 (ab Version 1809) oder Windows 11
Architektur	x64; auf ARM64 über die Windows-Emulation
Laufzeitumgebung	Keine. Die Toolbox bringt .NET 10 und WinUI 3 mit.
Plattenplatz	rund 350 MB
Rechte zur Installation	lokaler Administrator
Rechte zur Benutzung	Standardbenutzer; einzelne Werkzeuge verlangen mehr (siehe unten)

Hinweis: Die Installation braucht Administratorrechte, weil die Toolbox unter `C:\Program Files\Grams IT\Ordivis Toolbox` landet. Das *Arbeiten* mit ihr braucht sie nicht — nur die Werkzeuge, die tatsächlich ins System eingreifen.

3.2 Herunterladen und installieren

💻 **Menü:** — · 🔑 **Rechte:** lokaler Administrator (nur für die Installation)

1. Öffnen Sie https://ordivis.eu/toolbox/ und laden Sie das Installationsprogramm herunter. Die Datei heißt `Ordivis-Toolbox-Setup-<Version>.exe`.
2. Starten Sie die Datei. Windows fragt nach Administratorrechten — bestätigen Sie.
3. Wählen Sie die Sprache des Installationsprogramms (Deutsch oder Englisch). Diese Auswahl betrifft nur den Installationsvorgang; die Sprache des Programms stellen Sie später in den Einstellungen ein.
4. Bestätigen Sie den Installationspfad. Die Vorgabe ist `C:\Program Files\Grams IT\Ordivis Toolbox`.
5. Entscheiden Sie, ob eine Verknüpfung auf dem Desktop angelegt werden soll. Der Eintrag im Startmenü entsteht in jedem Fall.
6. Klicken Sie auf *Installieren*.

✅ **Ergebnis:** Im Startmenü steht *Ordivis Toolbox*. Beim Beenden des Installationsprogramms lässt sich das Programm direkt starten.

> **Hinweis:** Fand das Installationsprogramm eine ältere Installation unter dem früheren Namen **NetzDesk**, entfernt es diese zuerst still und übernimmt danach deren Platz. Ihre Einstellungen, gespeicherten Verbindungen und die Ordivis-Anbindung bleiben dabei erhalten — sie liegen im Benutzerprofil und werden von der Deinstallation nicht angefasst.

Wie sich die Toolbox ohne Rückfragen an viele Rechner verteilen lässt, steht im **Administratorhandbuch**, Kapitel *Verteilung im Netz*.

3.3 Das Programm starten

Starten Sie *Ordivis Toolbox* über das Startmenü oder die Desktop-Verknüpfung.

Zwei Eigenheiten sind beim ersten Start gut zu wissen:

- **Es läuft nur eine Instanz.** Ein zweiter Start bringt kein zweites Fenster, sondern beendet sich still. Wenn scheinbar nichts passiert, läuft die Toolbox bereits — suchen Sie sie in der Taskleiste.
- **Beim ersten Start sind noch keine Rechte angefordert.** Die Toolbox startet als gewöhnliches Programm. Wer regelmäßig Dienste steuert oder die HOSTS-Datei bearbeitet, schaltet dafür einmalig *Immer als Administrator ausführen* in den Einstellungen ein (siehe Kapitel *Einstellungen*).

3.4 Das Fenster kennenlernen

Das Fenster öffnet sich in 1280 × 920 Bildpunkten und lässt sich frei verändern. Es besteht aus vier Teilen:

Teil	Wo	Was darin steht
Titelzeile	oben	Produktzeichen und der Name *Ordivis Toolbox*
Navigationsbereich	links	Das Menü mit allen Werkzeugen
Arbeitsfläche	rechts	Das gewählte Werkzeug
Statusleiste	unten	Links der Betriebszustand (*Bereit*), rechts `Grams IT | v<Version>`

Die Programmversion in der Statusleiste ist die verlässliche Auskunft darüber, welchen Stand Sie vor sich haben — nennen Sie sie bei jeder Rückfrage an den Support.

3.4.1 Im Menü navigieren

Der Navigationsbereich ist in vier Blöcke geteilt (siehe Kapitel *Was die Ordivis Toolbox ist*, Abschnitt *Der Aufbau des Programms*). Die Bedienung ist überall gleich:

- Ein Klick auf einen **Werkzeug-Eintrag** öffnet das Werkzeug in der Arbeitsfläche.
- Ein Klick auf eine **Gruppe** unter *Werkzeug-Suiten* — etwa *IP Werkzeuge* — klappt sie auf oder zu, ohne die Arbeitsfläche zu wechseln. Das ist Absicht: Eine Gruppe ist kein Werkzeug.
- Über die Schaltfläche mit den drei Strichen ganz oben links lässt sich der ganze Bereich zu einer schmalen Symbolleiste einklappen. Auf kleinen Bildschirmen gewinnt man so spürbar Platz für breite

Tabellen.

- Ganz unten steht *Einstellungen* — mit dem Zahnrad, wie in Windows üblich.

> **Tipp:** Die Werkzeuge behalten ihren Zustand nicht, wenn Sie zwischen ihnen wechseln. Ein laufender Scan, ein Dauer-Ping und ein Trace werden beim Verlassen der Seite beendet. Wenn eine Messung lange läuft, lassen Sie die Seite offen.

3.5 Die drei Einstellungen, die sich zuerst lohnen

Alles Weitere zu den Einstellungen steht im Kapitel *Einstellungen*. Drei davon ändert man am besten gleich beim ersten Start:

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

1. **Sprache.** Unter *Sprache / Language* stellen Sie Deutsch oder Englisch ein. Die Oberfläche wechselt sofort, ohne Neustart.
2. **Farbschema.** Unter *Erscheinungsbild* wählen Sie *Systemstandard*, *Helles Design* oder *Dunkles Design*. Auch das wirkt sofort.
3. **Immer als Administrator ausführen.** Unter *Systemverhalten & Berechtigungen*. Wer Dienste steuert, Prozesse beendet oder die HOSTS-Datei bearbeitet, spart sich damit den Umweg über *Als Administrator ausführen* im Kontextmenü.

> **Achtung:** *Immer als Administrator ausführen* fordert bei **jedem** Start die Rechteerhöhung an — auch dann, wenn Sie nur kurz einen Hostnamen auflösen wollen. Wer die Toolbox überwiegend für Abfragen benutzt, lässt die Einstellung besser aus und startet sie im Bedarfsfall gezielt erhöht.

3.6 Ein erster Durchgang

Damit Sie das Muster einmal gesehen haben — drei Minuten, ohne Vorbereitung, ohne Sonderrechte:

1. **Was tut mein Rechner gerade im Netz?** Klicken Sie auf *Verbindungen*. Die Liste zeigt jede offene TCP-Verbindung mit Prozessnamen. Tippen Sie in das Suchfeld einen Prozessnamen — die Liste filtert mit.
2. **Wer ist sonst noch in diesem Netz?** *Werkzeug-Suiten* ▸ *Scanner Werkzeuge* ▸ *IP Scanner*, dann *Lokales Subnetz laden* und *Starten*. Nach einigen Sekunden stehen die erreichbaren Adressen mit Hostnamen in der Tabelle.
3. **Ist der Server erreichbar, und wie lange dauert der Weg?** *Werkzeug-Suiten* ▸ *IP Werkzeuge* ▸ *ICMP (Ping)*, Ziel eintragen, *Ping Starten*. Unten stehen laufend Minimum, Maximum, Mittelwert und Paketverlust.

Wenn diese drei Handgriffe sitzen, ist der Rest des Buches Nachschlagewerk: Jedes weitere Werkzeug funktioniert nach demselben Muster — Ziel eintragen, starten, Tabelle lesen.

3.7 Wenn ein Werkzeug nicht so kann wie es soll

Drei Ursachen erklären fast alle Fälle. Das Kapitel *Wenn etwas nicht funktioniert* geht ins Einzelne; für den Anfang:

Beobachtung	Ursache in aller Regel
Listen bleiben leer, Aktionen werden verweigert	Die Toolbox läuft **ohne** Administratorrechte
Alles rund um *Active Directory* meldet „keine Domäne"	Der Rechner ist nicht Mitglied einer Domäne, oder kein Domain Controller ist erreichbar
Ein Werkzeug meldet ein fehlendes Programm (`nmap` , `dcdiag` , `openssl`)	Das externe Werkzeug ist nicht installiert — die Toolbox bietet die Nachinstallation jeweils an Ort und Stelle an

4 Dashboard

Das Dashboard ist die Startseite: ein Blick auf das, was **auf diesem Rechner gerade im Netz passiert**. Es beantwortet drei Fragen gleichzeitig — welche Schnittstellen tragen wie viel Verkehr, wohin bestehen die meisten Verbindungen, und ist der Weg nach draußen gerade in Ordnung.

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

> **Hinweis:** Das Dashboard misst **nur diesen Rechner**. Es ist keine Netzüberwachung: Es sieht keine anderen Geräte, keine Switche und keinen Verkehr, der nicht über diese Maschine läuft.

4.1 Die vier Bereiche

4.1.1 Durchsatz (RX und TX)

Ganz oben stehen zwei Zahlen mit je einem Verlaufsdiagramm:

- ▼ **RX** — was gerade **hereinkommt**, in Byte pro Sekunde, über alle Schnittstellen zusammen.
- ▲ **TX** — was gerade **hinausgeht**.

Die Balken darunter zeigen den Verlauf der letzten Messwerte. Sie sind **relativ** skaliert: Der höchste Balken ist immer der größte Wert im gezeigten Zeitraum, nicht etwa die Leitungskapazität. Ein hoher Ausschlag heißt also „viel im Vergleich zu gerade eben", nicht „Leitung voll". Wie viele Balken nebeneinander passen, richtet sich nach der Fensterbreite — ein breiteres Fenster zeigt mehr Verlauf.

> **Tipp:** Fahren Sie mit dem Zeiger über einen Balken. Der Kurzhinweis nennt den Messwert dieses Zeitpunkts.

4.1.2 Schnittstellen

Die Tabelle listet **alle Netzwerkkarten außer Loopback** — auch abgeschaltete, virtuelle und die von VPN-Software angelegten.

Spalte	Bedeutung
Schnittstelle	Der Windows-Name der Karte, auf 15 Zeichen gekürzt
IP-Adresse	Die erste IPv4-Adresse; `–`, wenn keine vergeben ist
RX Rate / TX Rate	Aktueller Durchsatz je Sekunde
RX Gesamt / TX Gesamt	Summe seit dem Start von Windows
Status	*UP* (grün) oder *DOWN* (grau)

Aktive Karten stehen oben, danach wird alphabetisch sortiert.

> **Hinweis:** Die Zahlen stammen aus der **IPv4-Statistik** der Schnittstelle. Reiner IPv6-Verkehr taucht deshalb nicht auf. Unmittelbar nach dem Öffnen der Seite stehen die Raten auf Null — es braucht zwei Messungen, um eine Rate zu bilden.

4.1.3 Top Verbindungen

Die 50 wichtigsten offenen TCP-Verbindungen; hergestellte Verbindungen zuerst.

Spalte	Bedeutung
Prozess	Das Programm, dem die Verbindung gehört
Proto	Immer `TCP`
Status	Der Zustand: *Hergestellt*, *Abhören*, *Wartend*, *Schließen wartend*
Ziel (Remote)	Gegenstelle mit Port, dazu die Einordnung *Lokal* oder *Extern*

Die vollständige Liste mit Suchfeld steht im Kapitel *Verbindungen*.

4.1.4 System-Health und Latenz-Heatmap

Rechts prüft die Toolbox laufend zwei Ziele mit einem Ping:

- **GW** — das **Standardgateway** der ersten aktiven Schnittstelle. Wird keines gefunden, steht dort *Nicht gefunden*.
- **DNS** — die feste Adresse **1.1.1.1** (Cloudflare) als Stellvertreter für „das Internet ist erreichbar".

Zu jedem Ziel stehen Laufzeit und Paketverlust. Der Zeitüberschreitungswert liegt bei 800 Millisekunden. Der Farbpunkt folgt einer festen Staffel:

Farbe	Bedeutung
Grün	Antwort unter 50 ms
Orange	Antwort zwischen 50 und 150 ms
Rot	Antwort über 150 ms — oder keine Antwort (*Err*, *100% loss*)
Grau	Noch nicht gemessen oder Ziel unbekannt

Die **Latenz-Heatmap** darunter reiht die letzten **30 Messungen** aneinander, die jüngste rechts. Sie zeigt auf einen Blick, ob eine Störung dauerhaft ist oder sprunghaft: Ein durchgehend grüner Streifen mit einzelnen roten Feldern bedeutet Aussetzer, ein durchgehend roter Streifen einen echten Ausfall.

> **Hinweis:** Die Prüfung gegen **1.1.1.1** ist die einzige Verbindung, die das Dashboard nach draußen aufbaut. Wo ausgehendes ICMP gesperrt ist, steht der DNS-Punkt dauerhaft auf Rot, **ohne** dass etwas kaputt wäre. Das Administratorhandbuch führt alle ausgehenden Verbindungen der Toolbox auf.

4.2 Wie oft aktualisiert wird

Der gesamte Inhalt wird in einem festen Takt neu erhoben. Vorgabe ist **eine Sekunde**; einstellbar unter *Einstellungen ▸ Live-Updates & Dashboard*.

> **Tipp:** Auf einem Rechner mit vielen Verbindungen kostet ein Sekundentakt spürbar Rechenzeit — die Prozessliste wird jedes Mal vollständig neu aufgelöst. Zwei oder fünf Sekunden reichen für die meisten Fälle und halten das Fenster flüssig.

Beim Verlassen der Seite hält der Takt an. Das Dashboard misst also nur, solange es sichtbar ist, und schreibt keine Historie über den Programmlauf hinaus fort.

4.3 Die Einheit umstellen

Unter *Einstellungen ▸ Daten-Einheiten* legen Sie fest, wie Durchsatz dargestellt wird. In der Stellung *Automatisch* wählt die Toolbox je Wert die passende Größe (B, KB, MB, GB, TB) — praktisch beim Überfliegen, unpraktisch beim Vergleichen, weil zwei Zeilen unterschiedliche Einheiten tragen können.

4.4 Was das Dashboard nicht kann

- **Keine Alarme.** Rot bleibt rot, bis Sie hinsehen. Es gibt keine Meldung, keine E-Mail, keinen Ton.
- **Keine Aufzeichnung.** Schließen Sie das Programm oder wechseln Sie die Seite, ist der Verlauf fort.
- **Kein Vergleich mit gestern.** Für Verlauf über Tage brauchen Sie ein Monitoringsystem.

5 Verbindungen

Diese Seite zeigt **jede offene TCP-Verbindung dieses Rechners mit dem Programm, dem sie gehört**. Sie beantwortet die Frage, die `netstat -ano` beantwortet — nur ohne den Umweg, die Prozess-ID anschließend im Task-Manager nachzuschlagen.

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

5.1 Wofür man sie braucht

- Herausfinden, **welches Programm** eine Verbindung nach draußen hält.
- Prüfen, ob ein Dienst tatsächlich **lauscht** (Status *Abhören*) und auf welchem Port.
- Nachvollziehen, wohin eine Anwendung spricht, wenn sie es nicht sagt.
- Feststellen, ob eine Verbindung noch **hergestellt** ist oder schon im Abbau (*Wartend*, *Schließen wartend*).

5.2 Die Tabelle lesen

Spalte	Bedeutung
PID	Prozess-ID des Besitzers
Prozess	Name des Programms
Lokal	Eigene Adresse und Port
Remote	Gegenstelle und Port, dazu die Einordnung *Lokal* oder *Extern*
Protokoll	Immer `TCP`
Status	Zustand der Verbindung

Die Zustände in deutscher Schreibweise:

Anzeige	Was sie bedeutet
Hergestellt	Die Verbindung steht und wird benutzt
Abhören	Ein Dienst wartet auf diesem Port auf eingehende Verbindungen
Wartend	Die Verbindung ist beendet; Windows hält den Port noch kurz belegt
Schließen wartend	Die Gegenstelle hat beendet, das lokale Programm noch nicht

Lokal oder **Extern** in der Spalte *Remote* ordnet die Gegenstelle ein: Adressen aus den privaten Bereichen (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16), der Loopback-Adresse und der Link-Local-Bereich gelten als

Lokal, alles andere als *Extern*. Das ist eine Einordnung nach Adressbereich, keine Auskunft über den Standort der Gegenstelle.

> **Hinweis:** Die Liste enthält **nur TCP**. UDP-Sockets stehen nicht darin, weil UDP keine Verbindung kennt und daher auch keinen Zustand hat.

5.3 Verbindungen filtern

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

1. Tippen Sie in das Suchfeld über der Tabelle. Gesucht wird gleichzeitig in **Prozessname, IP-Adresse, Port und Status**.
2. Die Tabelle filtert bei jedem Tastendruck mit; ein Bestätigen ist nicht nötig.
3. Zum Aufheben leeren Sie das Feld.

Nützliche Suchbegriffe:

Eingabe	Findet
`chrome`	Alle Verbindungen des Browsers
`:443`	Alles, was gegen HTTPS spricht
`Abhören`	Alle Dienste, die auf diesem Rechner lauschen
`192.168.`	Alles im lokalen Netz

5.4 Auffrischen

Über der Tabelle stehen zwei Bedienelemente:

- **Auto-Refresh** — ein Schalter. Ist er ein, wird die Liste laufend neu erhoben, im Takt aus *Einstellungen ▸ Live-Updates & Dashboard*.
- **Aktualisieren** — holt die Liste einmalig neu.

> **Tipp:** Beim Beobachten eines kurzlebigen Verbindungsaufbaus hilft *Auto-Refresh* mit einem kurzen Takt. Beim Vergleichen zweier Zustände schalten Sie ihn besser aus — eine Liste, die sich unter dem Zeiger neu sortiert, lässt sich nicht lesen.

5.5 Was Sie sehen und was nicht

Voraussetzung: Ohne Administratorrechte zeigt Windows für **fremde** Prozesse keinen Namen. Die Verbindung selbst steht in der Liste, in der Spalte *Prozess* steht dann aber nur die PID oder ein leerer Wert. Wer die Zuordnung vollständig braucht, startet die Toolbox als Administrator.

Weiter gilt:

- Die Prozessnamen werden bei **jedem** Durchlauf neu aufgelöst. Das kostet Zeit, ist aber richtig: Windows vergibt Prozess-IDs wieder, und eine über Stunden mitgeschleppte Zuordnung zeigt irgendwann den falschen Prozess.
- Verbindungen, die zwischen zwei Durchläufen entstehen und wieder vergehen, erscheinen nie. Wer flüchtige Verbindungen jagt, braucht einen Mitschnitt.

5.6 Weiterführend

- Eine **Zusammenfassung** derselben Daten samt Durchsatz steht auf dem *Dashboard*.
- Eine **grafische** Darstellung, welche Schnittstelle mit welchen Gegenstellen spricht, zeigt das Kapitel *Topologie*.

6 Paket-Mitschnitt (IPv4)

💻 **Menü:** *Pakete (Live)* · 🔑 **Rechte: lokaler Administrator**

Schneidet den Verkehr **einer Netzwerkkarte** mit — ein- und ausgehend, so wie er auf der Leitung liegt. Das ist das Werkzeug für die Fragen, die keine Statistik beantwortet: *Geht das Paket überhaupt raus? Kommt eine Antwort? Was steht im SYN, das die Gegenstelle mit RST beantwortet?*

Achtung: Ein Mitschnitt zeigt, **wer mit wem spricht**. Wo Beschäftigte betroffen sein können, ist der Einsatz nach § 87 Abs. 1 Nr. 6 BetrVG mitbestimmungspflichtig und berührt den Datenschutz. Klären Sie ihn mit der Personalvertretung und der oder dem Datenschutzbeauftragten, **bevor** Sie ihn brauchen. Und schneiden Sie nur in Netzen mit, für die Sie zuständig sind.

6.1 Was der Mitschnitt sieht — und was nicht

Die Toolbox benutzt dafür den Rohsocket von Windows mit `SIO_RCVALL`. Das braucht **keinen Treiber und keine Fremdsoftware** — und es kostet drei Einschränkungen. Sie stehen dauerhaft als Hinweisbalken auf der Seite, weil sie sich nicht wegbauen lassen:

Enthalten	Nicht enthalten
IPv4: TCP, UDP, ICMP, IGMP und alles Weitere mit IP-Kopf	**IPv6**
Ein- **und** ausgehend	**ARP**, VLAN-Marken, alles unterhalb von IP
Die **gewählte** Schnittstelle	Alle übrigen Karten; Loopback

Grenze: ARP fehlt, weil ARP keinen IP-Kopf trägt — der Rohsocket sieht es nicht, egal wie lange man wartet. Ein Fehlen in der Liste ist deshalb **kein Beweis für Abwesenheit**. Wer ARP, IPv6 oder die Sicherungsschicht braucht, braucht Wireshark mit **Npcap**; das bringt einen Netzwerktreiber mit.

6.2 Einen Mitschnitt aufnehmen

Voraussetzung: Windows vergibt Rohsockets nur an erhöhte Prozesse. Läuft die Toolbox ohne Administratorrechte, ist die Schaltfläche gesperrt und der Hinweisbalken sagt es. Abhilfe: Toolbox als Administrator neu starten, oder *Einstellungen ▸ Systemverhalten & Berechtigungen ▸ Immer als Administrator ausführen* einschalten.

1. Wählen Sie unter *Schnittstelle* die Netzwerkkarte. Angeboten werden alle aktiven Karten mit IPv4-Adresse; VPN-Anschlüsse sind dabei.

2. Klicken Sie auf *Mitschnitt starten*.
3. Die Tabelle füllt sich, viermal je Sekunde.
4. *Mitschnitt stoppen* beendet ihn.

✅ **Ergebnis:** Unter den Bedienelementen läuft der Zähler mit — *„1 284 Pakete gesehen · 1 000 im Verlauf"*.

Beim Verlassen der Seite endet der Mitschnitt von selbst. Er läuft nie im Hintergrund weiter.

6.3 Die Tabelle lesen

Spalte	Inhalt
Zeit	Empfangszeitpunkt mit Millisekunden
Quelle / Ziel	Die IPv4-Adressen aus dem IP-Kopf
Proto	Das **IP-Protokoll**: `TCP`, `UDP`, `ICMP`, `IGMP`, `GRE`, `ESP`, …
Länge	Die Gesamtlänge des IP-Pakets in Byte
Info	Ports, TCP-Merker, Nutzlastgröße — je nach Protokoll

Beispiele für die Spalte *Info*:

```
51234 → 443 (HTTPS) [SYN] Len=0
443 → 51234 (HTTPS) [ACK, PSH] Len=1440
55123 → 53 (DNS) Len=30
Echo-Anforderung
Ziel nicht erreichbar (Port)
Fragment (Versatz 1480)
```

Hinweis: Der Dienstname in Klammern — `(HTTPS)`, `(DNS)` — ist eine **Vermutung aus der Portnummer**, keine Feststellung. Auf Port 443 kann alles laufen. Deshalb steht er in der Info-Spalte und in Klammern und **nicht** in der Protokollspalte: Dort steht ausschließlich, was wirklich im IP-Kopf stand.

Die TCP-Merker sind die üblichen: `SYN`, `ACK`, `PSH`, `FIN`, `RST`, `URG`. `Len=` ist die Nutzlast **ohne** Kopfdaten — ein reines `ACK` hat `Len=0`.

6.4 Filtern

Das Feld *Filter* schränkt die angezeigten Zeilen ein und sucht dabei gleichzeitig in **Protokoll, Quelle, Ziel und Info**. Es filtert die Anzeige, nicht den Mitschnitt — gefiltert wird also nachträglich, und ein Löschen des Feldes bringt alles zurück.

Eingabe	Findet
`icmp`	Alle Ping-Pakete
`→ 53`	Alles, was an DNS geht
`[RST]`	Abgewiesene Verbindungsversuche
`10.8.`	Alles zu einem bestimmten Netz

6.5 Verlauf und verworfene Pakete

Gehalten werden die letzten **1 000** Pakete, angezeigt die letzten **100** — neueste oben. Was darüber hinausläuft, fällt hinten heraus.

Wichtig: Bei starkem Verkehr kann die Anzeige nicht mithalten. Dann steht im Zähler zusätzlich „… *verworfen (Anzeige kam nicht nach)*". Diese Zahl ist ernst zu nehmen: **Der Mitschnitt hat dann Lücken.** Ein Paket, das Sie suchen, kann durchgelaufen sein, ohne dass es in der Tabelle steht. Für die Fehlersuche in einem Netz unter Last ist der Filter kein Ersatz — dort brauchen Sie ein Werkzeug, das in eine Datei schreibt.

6.6 Wenn nichts erscheint

Beobachtung	Ursache
Schaltfläche ist gesperrt, gelber Balken	Keine Administratorrechte
Gelber Balken „*Keine Schnittstelle gefunden*"	Keine aktive Karte mit IPv4-Adresse
Roter Balken mit `WSA`-Nummer	Windows hat den Rohsocket abgewiesen — der Wortlaut steht dabei. Häufigste Ursache: eine Sicherheitssoftware, die Rohsockets sperrt
Zähler läuft, Tabelle leer	Der Filter passt auf nichts. Feld leeren
Zähler bleibt bei 0	Auf dieser Karte läuft gerade kein IPv4-Verkehr — oder der Verkehr läuft über eine andere Karte

Tipp: Zum Nachweis, dass der Mitschnitt arbeitet, lassen Sie nebenher einen Dauer-Ping laufen (*IP Werkzeuge ▸ ICMP (Ping)*, Anzahl `0`) und filtern hier auf `icmp`. Wenn dort im Sekundentakt Echo-Anforderung und Echo-Antwort erscheinen, stimmt die Kette.

6.7 Was andere Werkzeuge besser können

Frage	Werkzeug
Welches **Programm** hält diese Verbindung?	*Verbindungen* — der Mitschnitt kennt keine Prozesse
Wie viel Verkehr trägt welche Karte?	*Dashboard*
Wo auf dem **Weg** gehen Pakete verloren?	*IP Werkzeuge* ▸ *Trace (MTR)*
Was steht **in** der Nutzlast?	Wireshark — dieser Mitschnitt zeigt nur die Kopfdaten
ARP, IPv6, Sicherungsschicht	Wireshark mit Npcap

7 Topologie

Die Topologie-Ansicht zeigt dieselben Daten wie *Verbindungen* — aber **geordnet nach Schnittstelle**: Welche Netzwerkkarte spricht gerade mit welchen Gegenstellen?

💻 **Menü:** *Topologie* · 🔑 **Rechte:** Standardbenutzer

Hinweis: Der Name führt leicht in die Irre. Dies ist **keine Netzplan-Karte**: Die Toolbox zeichnet nicht das Netz, sondern die Verbindungen **dieses einen Rechners**. Switche, Router und fremde Geräte kommen nicht vor — nur die Gegenstellen, mit denen dieser Rechner selbst gerade spricht.

7.1 Was die Darstellung zeigt

Für jede Netzwerkkarte entsteht ein Knoten mit:

- dem Namen der Schnittstelle und ihrer IPv4-Adresse,
- dem Zustand samt Gesamtvolumen: `Status: UP | Gesamt RX: 4,2 GB | TX: 812,0 MB`,
- den aktuellen Raten `RX:` und `TX:` — grün beziehungsweise orange, solange etwas fließt, sonst grau,
- darunter, mit `---►` angehängt, die **Gegenstellen** dieser Karte.

Zu jeder Gegenstelle steht die Adresse mit Port und dahinter die Einordnung: `[TCP] Hergestellt | chrome (PID: 8412)`.

Aktive Karten sind blau und weiß gezeichnet, abgeschaltete grau.

Hinweis: Je Schnittstelle werden höchstens **15 Gegenstellen** gezeichnet. Auf einem Rechner mit hunderten offenen Verbindungen wäre die Ansicht sonst unlesbar. Die Zähler in der Fußzeile rechnen mit **allen** Verbindungen, nicht nur mit den gezeichneten — die Zahl dort kann also höher sein, als die Ansicht zeigt.

7.2 Die Zähler in der Fußzeile

Zähler	Was er zählt
Gesamt Interfaces/Ziele	Schnittstellen / Summe der eindeutigen Gegenstellen
Verbindungen Global	Alle offenen TCP-Verbindungen des Rechners
Aktive Remote-IPs	Wie viele **verschiedene** Gegenstellen-Adressen angesprochen werden

Der Unterschied zwischen *Verbindungen Global* und *Aktive Remote-IPs* ist aufschlussreich: 300 Verbindungen zu 4 Adressen sehen ganz anders aus als 300 Verbindungen zu 280 Adressen. Das Erste ist ein gesprächiger Dienst, das Zweite kann ein Scan sein — oder ein Browser mit vielen offenen Seiten.

7.3 Wenn nichts angezeigt wird

Zwei Meldungen kommen vor:

- **„Keine aktiven Verbindungen"** — die Schnittstelle hat gerade keine Gegenstellen. Das ist der Normalzustand einer stillen Karte.
- **„Wartet auf Netzwerkverkehr…"** — es steht noch keine Messung an. Die Ansicht füllt sich mit dem nächsten Takt.

Eine Schnittstelle ohne IPv4-Adresse bekommt nie Gegenstellen zugeordnet: Die Zuordnung geschieht über die **lokale Adresse** der Verbindung. Reine IPv6-Verbindungen erscheinen aus demselben Grund nicht.

7.4 Takt

Die Ansicht wird im selben Takt erneuert wie das Dashboard (*Einstellungen ▸ Live-Updates & Dashboard*, Vorgabe eine Sekunde). Beim Verlassen der Seite hält sie an. Die Bildlaufposition bleibt beim Erneuern erhalten — die Knoten werden an Ort und Stelle aktualisiert und nicht neu aufgebaut.

8 Host- & Systemverwaltung

Drei Werkzeuge für die Maschine selbst — die eigene oder eine entfernte:

Werkzeug	Wofür
System Inspector	Hardware, Leistungsdaten, Prozesse, Dienste, Treiber, installierte Software — lokal oder über das Netz
Service & Process Controller	Dienste starten, stoppen, neu starten; Prozesse beenden
Windows HOSTS	Die lokale Namensauflösung ansehen und bearbeiten

8.1 System Inspector

💻 **Menü:** *Werkzeug-Suiten* ▸ *Host- & Systemverwaltung* ▸ *System Inspector* · 🔑 **Rechte:** lokaler Administrator (lokal) bzw. ein Konto mit WinRM-Berechtigung auf dem Ziel

Der System Inspector nimmt ein System vollständig auf: Betriebssystem, Startzeit, Prozessor, Arbeitsspeicher, Grafik, Datenträger, die 50 speicherhungrigsten Prozesse, alle Dienste, alle Treiber und die installierte Software. Er benutzt dafür **CIM über WS-Management (WinRM)** — nicht das alte WMI über DCOM, das in gehärteten Netzen ohnehin gesperrt ist.

Für Geräte, die kein Windows sind — Switche, Drucker, Speichersysteme, Linux mit SNMP-Agent —, gibt es eine zweite Betriebsart über **SNMP**.

8.1.1 Ein System aufnehmen

1. Tragen Sie unter *Ziel (IP / Hostname)* das System ein. Für den eigenen Rechner genügt `localhost` oder `127.0.0.1`.
2. Wählen Sie das Verfahren: * **WinRM** für Windows-Systeme. * **SNMP** für alles andere.
3. Bei **WinRM**: Lassen Sie Benutzername und Kennwort leer, um mit Ihrer eigenen Windows-Anmeldung zu arbeiten. Tragen Sie beides ein, wenn ein anderes Konto nötig ist. Bei **SNMP**: Tragen Sie in das Benutzerfeld die **Community** ein. Bleibt es leer, wird `public` verwendet.
4. Klicken Sie auf *System analysieren* — oder drücken Sie im Zielfeld die Eingabetaste.

✅ **Ergebnis:** Die Reiter *Dashboard & Hardware*, *Top 50 Prozesse*, *Dienste*, *Installierte Software* und *Treiber* füllen sich.

Voraussetzung: Für ein **entferntes** Windows-System muss dort PowerShell Remoting laufen (`Enable-PSRemoting`), Port 5985 (HTTP) beziehungsweise 5986 (HTTPS) erreichbar sein und Ihr Konto berechtigt. Fehlt eines davon, meldet die Toolbox den Fehler im Klartext und weist auf WinRM hin.

> **Hinweis:** Auf dem **eigenen** Rechner läuft die Abfrage ohne Remoting direkt. Ohne Administratorrechte bleiben Teile der Auskunft leer — insbesondere die Treiberliste und Prozesse anderer Benutzer.

8.1.2 Die Reiter im Einzelnen

Dashboard & Hardware — Betriebssystem und Startzeit, Prozessorauslastung im Mittel, belegter und freier Arbeitsspeicher, Grafikkarten und alle lokalen Datenträger mit Belegung. Netzlaufwerke und Wechselmedien sind ausgenommen; gezeigt werden nur feste Platten.

Top 50 Prozesse — nach Arbeitsspeicher absteigend. Das beantwortet die häufigste Frage („wer frisst den Speicher?") und lässt den Rest weg.

Dienste — Name, Anzeigename, Status, Starttyp.

Installierte Software — Name, Hersteller, Version. Grundlage für den Sicherheits-Check im nächsten Abschnitt.

Treiber — Anzeigename, Systemname, Pfad, Zustand und Startart.

Über allen Tabellen steht ein Suchfeld. Es filtert **die gerade sichtbare** Tabelle.

> **Hinweis:** Über SNMP liefert das Ziel deutlich weniger: Systembeschreibung, Name, Betriebsdauer und Arbeitsspeicher. In den Reitern *Dienste* und *Treiber* steht dann der Hinweis, dass es dafür WinRM braucht — die Reiter bleiben nicht leer, sondern sagen, woran es liegt.

8.1.3 Sicherheits-Check (CVE & WID)

> 💻 **Menü:** … ▸ *System Inspector* ▸ *Installierte Software* ▸ *Sicherheits-Check (CVE & WID)* · 🔑 **Rechte:** wie oben, zusätzlich ausgehender HTTPS-Zugang

Der Sicherheits-Check nimmt die aufgenommene Softwareliste und fragt zu jedem Eintrag zwei öffentliche Quellen ab:

- **CVE** über die Datenbank **CIRCL** (`cve.circl.lu`) — gibt es bekannte Schwachstellen zu diesem Hersteller und Produkt?
- **BSI WID** — liegt zu dem Fund eine Warnmeldung des Bundesamts für Sicherheit in der Informationstechnik vor (Kennung `WID-SEC-…`)?

1. Nehmen Sie zuerst ein System auf (siehe oben).
2. Wechseln Sie auf den Reiter *Installierte Software*.
3. Klicken Sie auf *Sicherheits-Check (CVE & WID)*.
4. Die Spalten *CVE Status* und *BSI WID Status* füllen sich. Bis zu zehn Abfragen laufen gleichzeitig; für rund 500 Programme dauert der Durchgang etwa eine Viertelminute.

✅ **Ergebnis:** Je Programm steht eine Einstufung; wo ein Treffer vorliegt, führt ein Verweis zur Fundstelle.

Achtung: Der Check schickt **Hersteller- und Produktnamen der installierten Software an einen Dienst im Internet** (`cve.circl.lu`). Wo das nicht erwünscht oder nicht erlaubt ist — abgeschottete Netze, besonders schützenswerte Systeme —, benutzen Sie ihn nicht. Es werden keine Versionsnummern, Rechnernamen oder Kennungen übertragen, aber die Liste sagt etwas über das System aus.

Grenze: Der Abgleich geschieht über **Hersteller und erstes Wort des Produktnamens**, nicht über die Version. Ein Treffer heißt deshalb *„zu diesem Produkt sind Schwachstellen bekannt"* und **nicht** *„diese Installation ist verwundbar"*. Umgekehrt bedeutet ein leeres Feld nicht, dass nichts vorliegt: Wer seine Programme unter abweichenden Namen führt, fällt durch das Raster. Der Check ist eine **Vorsortierung**, kein Schwachstellenscanner.

Windows-Updates und Sprachpakete werden übersprungen — sie stehen ohnehin in der Update-Verwaltung und würden die Liste zumüllen.

Beide Ergebnisse lassen sich an **Ordivis Platform** übergeben; siehe Kapitel *Ergebnisse an Ordivis übergeben*.

8.2 Service & Process Controller

💻 **Menü:** *Werkzeug-Suiten* ▸ *Host- & Systemverwaltung* ▸ *Service & Process Controller* · 🔑 **Rechte:** lokaler Administrator (lokal) bzw. WinRM-Berechtigung auf dem Ziel

Dienste starten, stoppen, neu starten und Prozesse beenden — lokal wie entfernt, ohne den Weg über `services.msc` und `mstsc`.

Achtung: Einen Dienst zu stoppen oder einen Prozess zu beenden, unterbricht den Betrieb — sofort und ohne Rückfrage. Auf einem Produktivsystem gehört vorher geprüft, wer daran hängt. Beendete Prozesse speichern nichts.

8.2.1 Dienste und Prozesse laden

1. Tragen Sie unter *Ziel-Computer* den Rechnernamen ein. Für den eigenen Rechner `localhost`.
2. Klicken Sie auf *Daten laden*.
3. Wechseln Sie zwischen den Reitern *Dienste* und *Prozesse*.
4. Das Feld *Liste filtern…* schränkt die jeweils sichtbare Tabelle ein.

Die Prozesse sind nach **Arbeitsspeicher** absteigend sortiert.

Voraussetzung: Läuft die Toolbox ohne Administratorrechte, erscheint oben ein roter Hinweis: *Fehlende lokale Administrator-Rechte*. Die Liste bleibt dann unvollständig, und jede Steuerung schlägt fehl. Das ist kein Fehler des Programms, sondern Windows.

8.2.2 Eine Aktion ausführen

1. Markieren Sie die Zeile.
2. Klicken Sie auf *Starten*, *Stoppen*, *Neu starten* (Dienste) oder *Beenden* (Prozesse).
3. Unter der Tabelle erscheint *Aktion erfolgreich ausgeführt.* oder die Fehlermeldung von Windows im Klartext.

Hinweis: Für **entfernte** Ziele verwendet der Controller automatisch das unter *Einstellungen ▸ Active Directory Administrator-Konto* hinterlegte Konto, falls eines gespeichert ist. Ist keines hinterlegt, gilt Ihre eigene Anmeldung. Es gibt auf dieser Seite kein eigenes Anmeldefeld — das ist der Grund, warum die Einstellung dort und nicht hier steht.

8.3 Windows HOSTS

💻 **Menü:** *Werkzeug-Suiten ▸ Host- & Systemverwaltung ▸ Windows HOSTS* · 🔑 **Rechte:** Standardbenutzer zum Ansehen, lokaler Administrator zum Ändern

Die Datei `C:\Windows\System32\drivers\etc\hosts` überschreibt die Namensauflösung dieses Rechners. Sie ist der erste Ort, an dem man nachsieht, wenn ein Name irgendwohin zeigt, wo er nicht hingehört — und der erste Ort, an dem man einen Umzug testet, bevor man das DNS ändert.

8.3.1 Die Einträge ansehen

1. Öffnen Sie die Seite. Die Datei wird sofort gelesen.
2. Die Tabelle zeigt *IP-Adresse*, *Hostname (Ziel)* und den *Kommentar*, der in derselben Zeile hinter einem `#` steht.
3. *Neu laden* liest die Datei erneut ein — nötig, wenn Sie sie außerhalb geändert haben.

Hinweis: Reine Kommentarzeilen werden **nicht** angezeigt. Die Tabelle zeigt nur, was tatsächlich wirkt. Steht dort *„Die Hosts-Datei enthält keine aktiven Weiterleitungen oder Routen."*, ist die Datei im Auslieferungszustand.

8.3.2 Einträge bearbeiten

💻 **Menü:** … ▸ *Windows HOSTS ▸ In Notepad bearbeiten* · ⚙️ **Außerhalb:** Der Editor ist Windows-Notepad, nicht die Toolbox · 🔑 **Rechte:** lokaler Administrator

1. Klicken Sie auf *In Notepad bearbeiten*. Die Datei öffnet sich in Notepad.

2. Ändern Sie sie. Aufbau je Zeile: IP-Adresse, Leerzeichen oder Tabulator, Hostname, optional `# Kommentar`.
3. Speichern Sie in Notepad.
4. Klicken Sie in der Toolbox auf *Neu laden*.

Voraussetzung: Die HOSTS-Datei liegt in einem geschützten Systemverzeichnis. Läuft die Toolbox **ohne** Administratorrechte, öffnet Notepad die Datei zwar, kann sie aber nicht speichern — Windows meldet dann „Zugriff verweigert". Schalten Sie in diesem Fall *Immer als Administrator ausführen* ein oder starten Sie die Toolbox einmalig erhöht.

Achtung: Ein Eintrag in der HOSTS-Datei gilt **dauerhaft** und für **alle** Programme dieses Rechners — auch für Update-Dienste und Sicherheitssoftware. Testeinträge werden erfahrungsgemäß vergessen; schreiben Sie einen Kommentar mit Datum dahinter, und räumen Sie sie weg.

Tipp: Nach einer Änderung wirkt der Eintrag nicht immer sofort, weil Windows Namen zwischenspeichert. `ipconfig /flushdns` in einer Eingabeaufforderung leert den Zwischenspeicher.

9 Active Directory

Sechs Werkzeuge für den Verzeichnisdienst. Sie reichen vom reinen Nachsehen bis zu Eingriffen, die eine ganze Gesamtstruktur betreffen — lesen Sie die Berechtigungshinweise ernst.

Werkzeug	Wofür
AD Diagnose	Domäne, FSMO-Rollen, `dcdiag`, `repadmin`, RSAT nachinstallieren
AD Explorer	Standorte, Vertrauensstellungen, Funktionsebenen
AD Suche	Benutzer, Gruppen und Computer suchen; BitLocker- und LAPS-Auskunft
AD Benutzer-Manager	Kennzahlen, Attribute bearbeiten, entsperren, Kennwort zurücksetzen
Gruppenrichtlinien (GPO) Verwaltung	GPOs auflisten, Berichte, RSOP, verwaiste SIDs
AD Papierkorb	Gelöschte Objekte suchen und wiederherstellen

Voraussetzung: Alle sechs Werkzeuge setzen voraus, dass dieser Rechner **Mitglied einer Domäne** ist und einen Domain Controller erreicht. Ist er es nicht, melden sie das im Klartext — es liegt dann kein Fehler des Programms vor.

Hinweis: Wo Ihr angemeldetes Konto nicht genügt, greifen die Werkzeuge auf das unter *Einstellungen ▸ Active Directory Administrator-Konto* hinterlegte Konto zurück. Es einmal dort einzutragen erspart es an sechs Stellen. Wie es gespeichert wird, steht im Kapitel *Einstellungen* und ausführlich im Administratorhandbuch.

9.1 AD Diagnose

💻 **Menü:** *Werkzeug-Suiten ▸ Active Directory ▸ AD Diagnose* · 🔑 **Rechte:** Lesen als Domänenbenutzer; `dcdiag` / `repadmin` brauchen Administratorrechte auf dem Domain Controller; FSMO-Transfer und RSAT-Installation brauchen mehr (siehe unten)

Die Seite gliedert sich in fünf Blöcke, die von oben nach unten immer tiefer eingreifen.

9.1.1 Aktuelle Domäne

Wird beim Öffnen automatisch ermittelt: NETBIOS-Name, FQDN, Gesamtstruktur (Forest) und die Liste der Domain Controller.

Steht dort *„Keine AD Domäne gefunden (oder keine Berechtigung)"*, ist der Rechner nicht in einer Domäne — oder er erreicht gerade keinen Domain Controller.

9.1.2 FSMO Rollen Inhaber

Die fünf Betriebsmasterrollen mit ihrem aktuellen Inhaber: *Schema Master*, *Domain Naming*, *PDC Emulator*, *RID Pool Manager*, *Infrastructure*.

Reines Lesen — jeder Domänenbenutzer darf das.

9.1.3 Eine FSMO-Rolle verschieben

💻 **Menü:** … ▸ *AD Diagnose* ▸ *FSMO Rolle auf anderen DC verschieben* · 🔑 **Rechte:** Domänen-Administrator; für *Schema Master* und *Domain Naming* zusätzlich Organisations-Administrator (Enterprise Admin)

Achtung: Ein FSMO-Transfer verändert die Gesamtstruktur. Er ist der geordnete Weg — der Vorbesitzer gibt die Rolle ab und weiß davon —, aber er wirkt sofort und replikationsweit. Führen Sie ihn nur durch, wenn Sie wissen, warum. Für den Fall eines **ausgefallenen** Rollenbesitzers ist dieses Werkzeug nicht gedacht; dann braucht es eine Beschlagnahme (*seize*) über `ntdsutil`.

1. Wählen Sie unter *Rolle* die zu verschiebende Rolle.
2. Wählen Sie unter *Ziel Domain Controller* den neuen Inhaber aus der Liste der gefundenen DCs.
3. Klicken Sie auf *Verschieben*.
4. Die Toolbox zeigt *Verschiebe … Bitte warten.* und prüft anschließend selbst nach, wer die Rolle jetzt hält.

✅ **Ergebnis:** *„Verifiziert! Die Rolle … liegt nun gesichert auf dem neuen Inhaber: …"*

Hinweis: Meldet die Prüfung noch den alten Inhaber, ist das in aller Regel nur die Replikationsverzögerung — die Toolbox sagt das auch so. Prüfen Sie nach einigen Minuten erneut nach. Kommt *„Zugriff verweigert"*, fehlen die Rechte: Hinterlegen Sie ein passendes Konto in den Einstellungen.

9.1.4 DCDIAG

Führt die Diagnosetests von Microsoft aus und wertet ihre Ausgabe in einer Tabelle aus — je Test *Bestanden*, *Fehler*, *Übersprungen* oder *Info*.

1. Wählen Sie den *Test-Umfang*:

Auswahl	Was sie tut
Standard (Zeigt nur Fehler)	Der schnelle Durchlauf, nur Auffälligkeiten
Standard (Zeigt alle Ergebnisse)	Derselbe Durchlauf mit allen Zeilen
Umfassend (/c)	Alle Tests, deutlich länger
Alle DNS Tests (/test:dns)	Nur die DNS-Prüfungen, dafür vollständig

2. Tragen Sie unter *Ziel-DC (Optional)* einen bestimmten Domain Controller ein, oder lassen Sie das Feld leer für den nächstgelegenen.
3. Klicken Sie auf *Start DCDIAG*.

✅ **Ergebnis:** Bei *„Keine Fehler gefunden!"* steht darunter, wie viele Tests bestanden und wie viele übersprungen wurden.

Voraussetzung: `dcdiag.exe` muss vorhanden sein. Fehlt es, zeigt die Seite oben einen Hinweis und verweist auf den RSAT-Block weiter unten. Liefert `dcdiag` unerwartete Ausgaben, fragt die Toolbox zurück, ob sie als Administrator gestartet wurde — genau das ist meistens die Ursache.

9.1.5 REPADMIN

Der Replikationsmonitor. Wählen Sie den *Kommando-Schalter*, ergänzen Sie bei Bedarf unter *Zusatz (Server / Optional)* ein Ziel — `*` für alle DCs oder ein Name wie `DC01` — und klicken Sie auf *Start Repadmin*. Die Ausgabe erscheint unverändert im Textfeld darunter.

Hinweis: Kommt *„Befehl wurde ausgeführt, aber keine Rückgabe erhalten"*, fehlen fast immer die Administratorrechte. Kommt *„RSAT … sind nicht installiert"*, installieren Sie sie im nächsten Block.

9.1.6 RSAT nachinstallieren

💻 **Menü:** … ▸ *AD Diagnose* ▸ *RSAT (Remote Server Administration Tools)* · ⚙️ **Außerhalb:** Der Vorgang läuft in einem PowerShell-Fenster · 🔑 **Rechte:** lokaler Administrator

Fünf Funktionspakete lassen sich hier an- und abschalten:

Paket	Was es mitbringt
Active Directory Tools (AD DS & LDS)	AD-Benutzer und -Computer, `dcdiag`, `repadmin`, `dsquery`
DNS-Servertools	`dnsmgmt.msc` und die Befehlszeilenwerkzeuge
DHCP-Servertools	`dhcpmgmt.msc` und die Befehlszeilenwerkzeuge
Gruppenrichtlinienverwaltung	`gpmc.msc` und die PowerShell-Befehle
Server-Manager	Die Server-Manager-Konsole

1. *Aktualisieren* liest den aktuellen Zustand — *Installiert* oder *Nicht installiert*.
2. *Installieren* oder *Entfernen* startet den Vorgang in einem sichtbaren PowerShell-Fenster, das nach dem Abschluss in zehn Sekunden von selbst schließt.
3. Nach dem Ende noch einmal *Aktualisieren*.

Achtung: Das kann mehrere Minuten dauern, und Windows lädt die Pakete aus dem Internet nach (*Features on Demand*).

Stolperfalle: In Firmennetzen blockiert häufig der lokale **WSUS-Server** den Bezug von Features on Demand — die Installation scheitert dann ohne erkennbaren Grund. Die Toolbox weist selbst darauf hin. Abhilfe: RSAT als MSI-Paket manuell laden oder die Gruppenrichtlinie *„Alternativen Quellpfad für die Komponenteninstallation angeben"* beziehungsweise *„Downloads von Windows Update zulassen"* setzen.

9.2 AD Explorer

💻 **Menü:** *Werkzeug-Suiten* ▸ *Active Directory* ▸ *AD Explorer* · 🔑 **Rechte:** Domänenbenutzer (nur Lesen)

Zeigt den Aufbau der Gesamtstruktur — die Dinge, die man selten braucht und dann sofort:

Funktionsebenen — *Domain Level* und *Forest Level*. Sie entscheiden, welche AD-Funktionen überhaupt zur Verfügung stehen; der AD-Papierkorb etwa setzt mindestens Windows Server 2008 R2 voraus.

AD Standorte (Sites) & Subnetze — je Standort der Name, die zugewiesenen Subnetze und die Anzahl der Domain Controller. Hier fällt auf, wenn ein Subnetz keinem Standort zugeordnet ist: Clients darin suchen sich dann einen beliebigen DC, womöglich am anderen Ende der Leitung.

Vertrauensstellungen (Trusts) — Ziel-Domäne, Richtung und Typ. Steht dort *„Keine Vertrauensstellungen (Trusts) konfiguriert"*, gibt es keine.

Die Seite ändert nichts. Sie liest.

9.3 AD Suche & Deep-Inspect

💻 **Menü:** *Werkzeug-Suiten* ▸ *Active Directory* ▸ *AD Suche* · 🔑 **Rechte:** Domänenbenutzer zum Suchen; **erhöhte Rechte** für BitLocker, LAPS und das Zurücksetzen von Computerkennwörtern

Zwei Reiter: *Benutzer & Gruppen* und *Computer*.

9.3.1 Benutzer und Gruppen finden

1. Tippen Sie in das Suchfeld einen Namen oder `sAMAccountName`.
2. Wählen Sie in der Ergebnisliste einen Eintrag.
3. Rechts erscheinen die Objekt-Attribute: Status, Abteilung, Erstellungsdatum, letzte Anmeldung, Vorgesetzter, Stadt — und unter *Mitgliedschaften (Vererbung)* die Gruppen, **einschließlich der geerbten**.

Die Mitgliedschaften mit Vererbung sind der eigentliche Grund für dieses Werkzeug: Sie beantworten die Frage „warum kommt diese Person an diese Freigabe?" in einem Schritt statt in fünf.

9.3.2 Computer untersuchen

Auf dem Reiter *Computer* liefert die Suche zusätzlich:

- **System Informationen** — DNS-Name, Betriebssystemversion, Service Pack.
- **BitLocker Wiederherstellungsschlüssel** — die im AD hinterlegten Schlüssel (`msFVE-RecoveryInformation`).
- **Lokales Admin-Passwort (LAPS)** — sowohl das ältere `ms-Mcs-AdmPwd` als auch Windows LAPS (`msLAPS-Password`).

Achtung: BitLocker-Wiederherstellungsschlüssel und LAPS-Kennwörter sind die **schutzwürdigsten Daten im ganzen Verzeichnis**. Wer sie liest, kann jede verschlüsselte Platte öffnen und sich auf jedem Rechner lokal anmelden. Zeigen Sie diese Ansicht niemandem über die Schulter, und teilen Sie keine Bildschirmfotos davon.

Voraussetzung: Ein gewöhnlicher Domänenbenutzer hat auf diese Attribute **keine Leserechte**. Steht dort *„Keine BitLocker-Schlüssel im AD gefunden"* oder *„Keine LAPS-Daten verfügbar"*, kann das zweierlei heißen: Es gibt wirklich keine — oder Ihnen fehlt das Recht, sie zu sehen. Hinterlegen Sie in diesem Fall ein berechtigtes Konto in den Einstellungen; die Toolbox verwendet es dann gezielt für diese beiden Abfragen.

Hinweis: Diese beiden Werte werden **niemals** an Ordivis Platform übertragen — auch dann nicht, wenn Sie AD-Computer melden. Siehe Kapitel *Ergebnisse an Ordivis übergeben*.

9.3.3 Ein Computerkennwort zurücksetzen

💻 **Menü:** … ▸ *AD Suche* ▸ *Computer* ▸ *Kennwort Reset* · 🔑 **Rechte:** Recht zum Zurücksetzen von Computerkonten in der Domäne

Achtung: Das Zurücksetzen des Kennworts eines Computerkontos **unterbricht die Vertrauensstellung** zwischen Rechner und Domäne. Der Rechner muss danach der Domäne neu beitreten oder die Vertrauensstellung wiederherstellen (`Test-ComputerSecureChannel -Repair`). Das ist der übliche Weg, eine kaputte Vertrauensstellung zu reparieren — und der sichere Weg, eine funktionierende kaputtzumachen.

1. Wählen Sie das Computerkonto in der Ergebnisliste.
2. Klicken Sie auf *Kennwort Reset*.
3. Die Toolbox fragt nach und benennt die Folge. Bestätigen Sie mit *Ja, Zurücksetzen*.

9.4 AD Benutzer-Manager

💻 **Menü:** *Werkzeug-Suiten* ▸ *Active Directory* ▸ *AD Benutzer-Manager* · 🔑 **Rechte:** Lesen als Domänenbenutzer; Ändern, Entsperren und Kennwort-Zurücksetzen brauchen entsprechende Schreibrechte

Drei Reiter: *Dashboard*, *Benutzer bearbeiten*, *Audit Log*.

9.4.1 Dashboard

Fünf Kennzahlen über alle Benutzerkonten der Domäne: *Gesamt*, *Aktiviert*, *Deaktiviert*, *Gesperrt*, *Nie angemeldet*. *Daten aktualisieren* erhebt sie neu.

Nie angemeldet ist die nützlichste Zahl davon: Konten, die es gibt und die niemand benutzt, sind entweder Vorräte oder Altlasten.

9.4.2 Benutzer bearbeiten

1. Suchen Sie über das Feld *Suchen…* den Benutzer und wählen Sie ihn aus.
2. Oben stehen die unveränderlichen Angaben: letzte Anmeldung, Erstellungsdatum, letzte Kennwortänderung, Ablaufdatum des Kennworts.
3. Darunter lassen sich vier Gruppen bearbeiten:

Gruppe	Felder
Kontaktinformationen	Telefon, Mobil, Fax, Webseite
Adresse	Straße/Postfach, PLZ, Stadt, Bundesland, Land
Profil und Anmeldeskript	Profilpfad, Anmeldeskript, Basisverzeichnis, Laufwerksbuchstabe
Mitarbeiter-Informationen	Firma, Vorgesetzter (als Distinguished Name), Mitarbeiter-ID, Personalnummer, Mitarbeiter-Typ, Info/Notizen

4. *Änderungen speichern* schreibt alle Felder in einem Zug ins Verzeichnis.

Voraussetzung: Kommt der rote Kasten *„Fehlende AD-Berechtigungen (Zugriff verweigert)"*, hat Ihr Windows-Konto keine Schreibrechte. Hinterlegen Sie unter *Einstellungen* ▸ *Active Directory* *Administrator-Konto* ein Konto, das sie hat.

9.4.3 Ein Konto entsperren

1. Benutzer auswählen.
2. *Konto entsperren*.

✅ **Ergebnis:** *„Erfolgreich entsperrt!"* Bei *„Entsperren verweigert!"* fehlen die Rechte.

9.4.4 Ein Kennwort zurücksetzen

Achtung: Der Benutzer kann sich anschließend mit dem alten Kennwort nicht mehr anmelden. Gespeicherte Anmeldedaten in Diensten, geplanten Aufgaben und auf Mobilgeräten laufen ins Leere — und sperren das Konto unter Umständen kurz darauf wieder, weil sie es weiter versuchen.

1. Benutzer auswählen, *Kennwort zurücksetzen*.
2. Neues Kennwort eintragen.
3. *Benutzer muss Kennwort bei nächster Anmeldung ändern* setzen oder weglassen.
4. *Bestätigen*.

9.4.5 Audit Log

Jede über diese Seite ausgeführte Änderung wird protokolliert: Zeitstempel, wer sie ausgeführt hat, welches Objekt betroffen war und was geschah.

Wichtig: Dieses Protokoll ist ein **lokales Arbeitsprotokoll**, keine revisionssichere Aufzeichnung. Es liegt als Datei im Benutzerprofil, gilt nur für diesen Rechner und dieses Windows-Konto und lässt sich löschen. Die verbindliche Nachweisführung liefert das Sicherheitsprotokoll der Domain Controller. Wo die Datei genau liegt, steht im Administratorhandbuch.

9.5 Gruppenrichtlinien (GPO) Verwaltung

💻 **Menü:** *Werkzeug-Suiten* ▸ *Active Directory* ▸ *Gruppenrichtlinien (GPO) Verwaltung* · 🔑 **Rechte:** Domänenbenutzer mit Leserecht auf die GPOs · **Voraussetzung:** RSAT *Gruppenrichtlinienverwaltung*

Voraussetzung: Ohne die RSAT-Gruppenrichtlinienwerkzeuge zeigt die Seite oben einen Hinweis und bleibt leer. Installieren lassen sie sich unter *AD Diagnose*.

9.5.1 Übersicht & HTML Reports

1. *GPOs laden* holt alle Richtlinien der Domäne.
2. Die Tabelle zeigt Name, Status, Erstellungs- und Änderungsdatum. Das Feld *GPOs filtern…* schränkt sie ein.
3. *Ansicht* zu einer Zeile erzeugt den vollständigen HTML-Bericht von Microsoft und zeigt ihn im Fenster an — derselbe Bericht wie in der Gruppenrichtlinienkonsole.
4. *Schließen* kehrt zur Liste zurück.

Die Spalte *Status* ist der schnelle Blick auf Richtlinien, die ganz oder halb abgeschaltet sind — ein häufiger Grund für „die GPO greift nicht".

9.5.2 RSOP (Resultant Set of Policy)

Was kommt bei einem bestimmten Rechner und Benutzer tatsächlich an?

1. Tragen Sie unter *Zielcomputer* den Namen oder FQDN ein.
2. Optional einen *Zielbenutzer*.
3. *RSOP-Report generieren*. Die Toolbox ruft `gpresult` auf und zeigt den Bericht an.

9.5.3 Verwaiste SIDs

Sucht in allen GPOs nach Sicherheitskennungen in Sicherheitsfiltern und Delegierungen, zu denen es kein Objekt mehr gibt — Überbleibsel gelöschter Benutzer und Gruppen.

1. *Nach verwaisten SIDs suchen*.
2. Die Tabelle nennt die verwaiste SID, die betroffene GPO und die Berechtigung.

> **Hinweis:** Verwaiste SIDs sind kein Fehler, aber Schmutz: Sie machen Berechtigungsprüfungen unübersichtlich und können bei einer Migration Verwirrung stiften. Die Toolbox **findet** sie; entfernen müssen Sie sie in der Gruppenrichtlinienkonsole.

9.6 AD Papierkorb

> 💻 **Menü:** *Werkzeug-Suiten* ▸ *Active Directory* ▸ *AD Papierkorb* · 🔑 **Rechte:** Recht zum Wiederherstellen gelöschter Objekte; zum **Aktivieren** des Papierkorbs Domänen-Administrator

Gelöschte Benutzer, Computer und Gruppen suchen und zurückholen — mit ihren Attributen und Gruppenmitgliedschaften, ohne Sicherung.

9.6.1 Den Papierkorb aktivieren

> **Achtung:** Das Aktivieren des AD-Papierkorbs ist **endgültig**. Es lässt sich nicht rückgängig machen. Die Funktion ist gut und ihre Aktivierung eine bewusste Entscheidung — sie verändert, wie die Gesamtstruktur mit gelöschten Objekten umgeht.

Ist der Papierkorb in der Domäne abgeschaltet, zeigt die Seite den Kasten *AD Papierkorb aktivieren* mit Erläuterung und der Schaltfläche *Jetzt aktivieren*.

> ✅ **Ergebnis:** *„AD Papierkorb wurde erfolgreich aktiviert!"* — ab jetzt lassen sich gelöschte Objekte laden.

> **Grenze:** Der Papierkorb wirkt **ab dem Zeitpunkt der Aktivierung**. Objekte, die vorher gelöscht wurden, sind damit nicht wiederherstellbar.

9.6.2 Ein Objekt wiederherstellen

1. Tragen Sie unter *Im AD nach Name suchen* einen Namensteil ein — oder lassen Sie das Feld leer für alles.
2. Wählen Sie unter *Objekt-Klasse* die Art des Objekts oder *Alle Objekte*.
3. *AD Objekte laden*.
4. Die Tabelle zeigt den gelöschten Objektnamen, die Klasse, das Löschdatum und den **Ursprungsort (Last Known Parent)** — die OU, in der das Objekt stand.
5. Das Feld *Geladene Objekte lokal filtern…* schränkt die geladene Liste weiter ein, ohne erneut abzufragen.
6. Zeile wählen, *Wiederherstellen*.

✅ **Ergebnis:** *„Objekt erfolgreich wiederhergestellt!"* Das Objekt steht wieder an seinem Ursprungsort.

Hinweis: Existiert der Ursprungsort nicht mehr — weil auch die OU gelöscht wurde —, schlägt die Wiederherstellung fehl. Stellen Sie in diesem Fall zuerst die OU wieder her und dann das Objekt darin.

10 CA & PKI

Drei Werkzeuge rund um Zertifikate. Sie greifen ineinander: Der *Zertifikats-Wizard* erzeugt Schlüssel und Anforderung, die *Lokalen Zertifikate* prüfen das Ergebnis, und der *OpenSSL Converter* bringt es in das Format, das der Zielserver erwartet.

Werkzeug	Wofür
Lokale Zertifikate (PKI)	Zertifikatsdateien prüfen, Schlüssel zuordnen, Fullchain bauen
Zertifikats-Wizard (ACME/CA)	Schlüssel und CSR erzeugen, bei der internen CA einreichen oder Let's Encrypt vorbereiten
OpenSSL Converter	Zwischen PEM, PFX und DER umwandeln; selbstsignierte Zertifikate; OpenSSL-Terminal

Achtung: Private Schlüssel sind Geheimnisse. Alles, was in diesen drei Werkzeugen in einem Feld *Privater Schlüssel* steht, gehört nicht in eine E-Mail, nicht in ein Ticket und nicht in einen Chat. Die Toolbox speichert diese Felder nicht — sie sind fort, sobald Sie die Seite verlassen. Was Sie auf die Platte schreiben, liegt dort aber weiter.

10.1 Lokale Zertifikate (PKI) & Chain-Builder

💻 **Menü:** *Werkzeug-Suiten* ▸ *CA & PKI* ▸ *Lokale Zertifikate (PKI)* · 🔑 **Rechte:** Standardbenutzer

Beantwortet die drei Fragen, die vor jedem Einspielen eines Zertifikats zu klären sind: Was steht drin? Passt der Schlüssel dazu? Ist die Kette vollständig?

10.1.1 Ein Zertifikat prüfen

1. Füllen Sie die Felder — jeweils per *Aus Datei laden* oder durch Einfügen des PEM-Textes:

Feld	Inhalt
Eigenes Zertifikat (CRT)	Das zu prüfende Zertifikat
Privater Schlüssel (KEY)	Optional — nur nötig für die Schlüsselprüfung
CA Kette (Root/Intermediate)	Optional — nur nötig für die Kettenprüfung

2. Klicken Sie auf *Zertifikat prüfen*.

✅ **Ergebnis:** Unter *Analysiertes Zertifikat* stehen Inhaber, Aussteller, Gültigkeitszeitraum, Schlüssellänge, Signaturalgorithmus und Fingerabdruck. Unter *Prüfungs-Ergebnisse* stehen zwei Befunde.

Die beiden Befunde im Klartext:

Befund	Anzeige	Bedeutung
Private-Key Match	„Der Key passt exakt zum Zertifikat."	Schlüssel und Zertifikat gehören zusammen
	„Der angegebene Key passt nicht zu diesem Zertifikat."	Falsche Datei — mit dieser Kombination startet kein Dienst
	„Kein privater Schlüssel (KEY) zur Prüfung angegeben."	Feld war leer, es wurde nichts geprüft
CA-Chain Audit	„Das Zertifikat wird durch die angegebene Kette verifiziert."	Die Kette trägt
	„Kette unvollständig oder ungültig."	Es fehlt ein Zwischenzertifikat, oder es passt nicht
	„Keine CA-Kette … zur Prüfung angegeben."	Feld war leer

Tipp: Die häufigste Ursache für „Browser meckert, Server läuft doch" ist eine **unvollständige Kette**: Der Server liefert nur sein eigenes Zertifikat, nicht das Zwischenzertifikat. Diese Prüfung findet das, bevor die Anwender es tun.

10.1.2 Eine Full-Chain-Datei bauen

1. Zertifikat und CA-Kette wie oben füllen.
2. *Full-Chain Datei exportieren*.
3. Speicherort wählen.

✅ **Ergebnis:** Eine PEM-Datei, in der das eigene Zertifikat zuerst und die Kette darunter steht — das Format, das nginx, Apache und die meisten Appliances erwarten.

Leeren setzt alle Felder zurück.

10.2 Zertifikats-Wizard (CSR / AD CS / ACME)

💻 **Menü:** *Werkzeug-Suiten* ▸ *CA & PKI* ▸ *Zertifikats-Wizard (ACME/CA)* · 🔑 **Rechte:** Standardbenutzer zum Erzeugen; für AD CS ein Konto, das bei der internen CA anfordern darf

10.2.1 Schritt 1 — Schlüssel und Anforderung erzeugen

1. Füllen Sie die Subject-Angaben:

Feld	Beispiel	Anmerkung
Common Name (CN)	`www.beispiel.de`	Der Hauptname des Zertifikats
Organisation (O)	`Beispiel GmbH`	
Land (C)	`DE`	Zwei Buchstaben
Subject Alternative Names (SANs)	`beispiel.de`, `mail.beispiel.de`	Optional, aber praktisch immer nötig

2. Wählen Sie die *Schlüssellänge*: **2048 Bit (Standard)** oder **4096 Bit (High Security)**.
3. Klicken Sie auf *Private Key & CSR generieren*.

✅ **Ergebnis:** Zwei Textfelder füllen sich: *Private Key (Geheim halten!)* und *Zertifikats-Anforderung (CSR)*. Der Schlüssel wird lokal erzeugt und verlässt den Rechner nicht.

Achtung: Browser prüfen seit Jahren **ausschließlich die SANs**, nicht mehr den Common Name. Ein Zertifikat ohne SAN-Eintrag für den tatsächlich aufgerufenen Namen gilt als ungültig, auch wenn der CN stimmt. Tragen Sie den CN also **zusätzlich** bei den SANs ein.

Wichtig: Der private Schlüssel existiert nur in diesem Textfeld. Kopieren Sie ihn heraus und sichern Sie ihn, **bevor** Sie die Seite verlassen — sonst ist die gerade ausgestellte Anforderung wertlos.

10.2.2 Schritt 2a — Bei der internen CA einreichen (AD CS)

⚙️ **Außerhalb:** Die Anforderung läuft über `certreq.exe` von Windows.

1. Wechseln Sie auf den Reiter *Eigene CA (Microsoft AD CS)*.
2. Tragen Sie unter *CA Server* die Kennung im Format `ServerName\CA-Name` ein — genau so, wie sie in der Zertifizierungsstellen-Konsole steht.
3. Tragen Sie unter *Template* die Vorlage ein. Vorgabe ist `WebServer`.
4. Klicken Sie auf *Zertifikat via certreq.exe anfordern*.

✅ **Ergebnis:** Bei Erfolg erscheint *„Zertifikat erfolgreich ausgestellt!"*. Übernehmen Sie Zertifikat und Schlüssel in *Lokale Zertifikate (PKI)*, um daraus eine Fullchain- oder PFX-Datei für den Zielserver zu bauen.

Voraussetzung: Die Vorlage muss auf der CA veröffentlicht sein, und Ihr Konto braucht das Recht *Registrieren* darauf. Ist die Vorlage auf automatische Genehmigung gestellt, kommt das Zertifikat sofort; steht sie auf Administratorgenehmigung, bleibt die Anforderung auf der CA liegen und muss dort freigegeben werden.

10.2.3 Schritt 2b — Let's Encrypt vorbereiten (ACME)

Die Toolbox ist ein Desktop-Programm. Sie kann deshalb keine HTTP-01-Challenge beantworten — dafür müsste sie unter dem beantragten Namen aus dem Internet erreichbar sein. Der Weg führt über die **DNS-01-Challenge**.

1. Wechseln Sie auf den Reiter *Let's Encrypt (ACME / DNS-01)*.
2. Die Toolbox erzeugt ein **kopierfertiges PowerShell-Skript** für Posh-ACME, passend zu den oben eingetragenen Namen.
3. Führen Sie das Skript auf einem Rechner aus, der Ihren DNS bearbeiten darf.

> **Voraussetzung:** Posh-ACME muss dort installiert sein (`Install-Module -Name Posh-ACME -Scope CurrentUser`), und Sie brauchen einen DNS-Anbieter, den Posh-ACME automatisieren kann — sonst tragen Sie den TXT-Eintrag von Hand ein.

10.3 OpenSSL Converter & Studio

> 💻 **Menü:** *Werkzeug-Suiten* ▸ *CA & PKI* ▸ *OpenSSL Converter* · ⚙️ **Außerhalb:** Ruft das installierte `openssl.exe` auf · 🔑 **Rechte:** Standardbenutzer; für die Installation lokaler Administrator

Oben auf der Seite steht der *OpenSSL Status*:

Anzeige	Bedeutung
Installiert	Gefunden an einem der üblichen Orte
Installiert (PATH)	Über die Umgebungsvariable `PATH` gefunden
Nicht gefunden	Es gibt kein OpenSSL auf diesem Rechner

10.3.1 OpenSSL nachinstallieren

Steht dort *Nicht gefunden*, erscheint der Hinweis *„OpenSSL Binary wurde nicht gefunden."* mit der Schaltfläche *Jetzt installieren*. Die Toolbox lädt OpenSSL dann über **Winget** (Paket *ShiningLight.OpenSSL*) und installiert es unbeaufsichtigt.

> **Voraussetzung:** Winget muss vorhanden und der Bezug aus dem Internet erlaubt sein. In abgeschotteten Netzen scheitert das; installieren Sie OpenSSL dort auf dem üblichen Weg.

10.3.2 Reiter 1 — Format Konverter

Wandelt zwischen den drei Formaten, in denen Zertifikate üblicherweise vorliegen:

Modus	Aus	Nach	Wofür
PEM zu PFX (PKCS#12)	Zertifikat + privater Schlüssel	`.pfx`	Import in Windows, IIS, Exchange

Modus	Aus	Nach	Wofür
PFX zu PEM (Entpacken)	`.pfx` mit Kennwort	Zertifikat + Schlüssel	Für nginx, Apache, Appliances
DER zu PEM (Base64)	`.der` / `.cer` (binär)	`.pem` (Text)	Wenn ein Werkzeug nur Text mag

1. Modus wählen.
2. Eingabedatei(en) wählen. Bei *PEM zu PFX* ist der private Schlüssel **Pflicht**.
3. Kennwort eintragen: bei *PEM zu PFX* das zu setzende Exportkennwort (optional), bei *PFX zu PEM* das vorhandene Archivkennwort.
4. Ausgabedatei unter *Speichern unter* festlegen.
5. *Konvertieren*.

✅ **Ergebnis:** *„Erfolgreich gespeichert unter: …"*. Die vollständige Ausgabe von OpenSSL steht darunter unter *Protokoll Ausgabe* — auch im Fehlerfall, und dort ist sie am nützlichsten.

10.3.3 Reiter 2 — Self-Signed Generator

Erzeugt ein selbstsigniertes Zertifikat für interne Tests.

1. *Common Name (CN)* eintragen — Pflichtfeld.
2. *Gültigkeit (Tage)* festlegen.
3. *Ausgabe-Ordner* wählen.
4. *Zertifikat generieren*.

✅ **Ergebnis:** Zertifikat und Schlüssel liegen im gewählten Ordner; die Dateinamen stehen in der Statusmeldung.

Achtung: Ein selbstsigniertes Zertifikat wird von keinem Client vertraut. Es ist für Testaufbauten und für den Zeitraum bis zum echten Zertifikat gedacht — nicht für den Betrieb. Wer es dauerhaft einsetzt, gewöhnt seine Anwender daran, Zertifikatswarnungen wegzuklicken.

10.3.4 Reiter 3 — Terminal & Debug

Ein Eingabefeld für beliebige OpenSSL-Befehle mit der vollständigen Ausgabe darunter. Nützlich für alles, was die beiden anderen Reiter nicht abdecken:

```
x509 -in zertifikat.pem -noout -text
s_client -connect www.beispiel.de:443 -servername www.beispiel.de
req -in anforderung.csr -noout -verify
```

Hinweis: Der Befehl wird ohne das führende `openssl` eingetragen. Steht dort *„Befehl ausgeführt (Keine Ausgabe)*", war der Befehl erfolgreich und wortlos — bei OpenSSL ist das oft dasselbe.

11 IP Werkzeuge

Sieben Werkzeuge für die Ebene, auf der die meisten Störungen sitzen: Adressen, Erreichbarkeit, Wege, Zuständigkeiten.

Werkzeug	Wofür
ARP Tabelle	Zuordnung von IP- zu MAC-Adressen im lokalen Netz
DHCP Info & Scanner	Eigene Leases erneuern, fremde DHCP-Server finden
ICMP (Ping)	Erreichbarkeit und Laufzeit, mit Statistik
Speedtest	Durchsatz der Internetanbindung messen
Subnetz Rechner	Netz, Broadcast, Hostbereich, Maske, Binärdarstellung
Trace (MTR)	Der Weg zum Ziel, dauerhaft gemessen, mit Karte
WHOIS Abfrage	Wem gehört diese Domain, wem dieser Adressbereich

11.1 ARP Tabelle

💻 **Menü:** *Werkzeug-Suiten* ▸ *IP Werkzeuge* ▸ *ARP Tabelle* · 🔑 **Rechte:** Standardbenutzer

Zeigt den ARP-Zwischenspeicher dieses Rechners: welche IP-Adresse zu welcher MAC-Adresse gehört, gesehen über welche Schnittstelle. Es ist der Blick auf das, was dieser Rechner in **seinem eigenen Netzsegment** tatsächlich angesprochen hat.

Spalte	Bedeutung
IP-Adresse	Die Adresse der Gegenstelle
Physische Adresse (MAC)	Die zugehörige Hardware-Adresse
Status / Typ	Der Zustand des Eintrags
Schnittstelle	Über welche Karte der Eintrag gelernt wurde

Die Zustände:

Anzeige	Bedeutung
Erreichbar	Der Eintrag ist frisch bestätigt
Statisch	Von Hand gesetzt, verfällt nicht
Veraltet	Der Eintrag ist alt; beim nächsten Zugriff wird nachgefragt
Verzögert / Wird geprüft	Windows prüft den Eintrag gerade nach

Anzeige	Bedeutung
Unvollständig	Auf die Anfrage kam keine Antwort — das Gerät ist nicht da

Aktualisieren liest die Tabelle neu.

Tipp: Zwei IP-Adressen mit **derselben MAC-Adresse** sind normal (ein Gerät mit zwei Adressen). Zwei **verschiedene MAC-Adressen für dieselbe IP** über die Zeit sind es nicht — das ist entweder ein Adresskonflikt oder ein Hinweis auf ARP-Spoofing.

Grenze: ARP ist auf das eigene Netzsegment beschränkt. Alles hinter einem Router steht hier nie — dort sehen Sie nur die MAC-Adresse des Routers.

11.2 DHCP Diagnose & Scanner

💻 **Menü:** *Werkzeug-Suiten* ▸ *IP Werkzeuge* ▸ *DHCP Info & Scanner* · 🔑 **Rechte:** Standardbenutzer zum Ansehen; lokaler Administrator zum Erneuern

11.2.1 Die eigene Konfiguration ansehen

Die Tabelle *Aktuelle lokale IP-Konfiguration (Leases & Statisch)* zeigt je Schnittstelle, ob die Adresse per DHCP bezogen oder *Statisch* gesetzt ist, welcher DHCP-Server sie vergeben hat, wann sie erhalten wurde und wann sie abläuft.

Die Schaltfläche in der Spalte *Aktion* erneuert die Adresse (*Renew*).

Voraussetzung: Das Erneuern greift in die Netzwerkkonfiguration ein und braucht Administratorrechte.

Achtung: Ein Renew unterbricht die Netzverbindung dieser Schnittstelle kurz. Auf dem Rechner, über den Sie gerade fernwarten, ist das eine schlechte Idee.

11.2.2 Nach DHCP-Servern suchen

Achtung: Der Scanner sendet einen echten **DHCPDISCOVER-Broadcast** ins Netz. Er verhält sich dabei wie ein Client, der eine Adresse sucht. In fremden Netzen ohne Erlaubnis ist das nichts, was man tut.

1. Klicken Sie auf *DHCP Scanner starten*.
2. Die Toolbox sendet einen Broadcast auf UDP-Port 67 und lauscht auf Port 68.
3. Jede Antwort erscheint als Karte unter *Scanner Ergebnisse*, mit angebotener IP, Subnetz, Router/Gateway, DNS-Servern, Lease-Dauer und Domäne.

✅ **Ergebnis:** Eine Karte je antwortendem Server. Kommt *„Zeitüberschreitung: Keine DHCPOFFER Antworten im Netzwerk erhalten."*, antwortet niemand — das kann an einem fehlenden DHCP-Relay liegen oder daran, dass es in diesem Segment keinen Server gibt.

Achtung: Antworten **mehrere verschiedene** Server, zeigt die Toolbox den roten Kasten *„ACHTUNG: Rogue DHCP-Server Verdacht!"*. Das ist ernst zu nehmen: Es führt zu IP-Konflikten und ist eines der klassischen Bilder eines Man-in-the-Middle-Angriffs. Häufigste harmlose Ursache ist ein privater WLAN-Router, den jemand verkehrt herum angeschlossen hat.

Die Ergebnisse lassen sich an **Ordivis Platform** übergeben; siehe Kapitel *Ergebnisse an Ordivis übergeben*.

11.3 ICMP (Ping)

💻 **Menü:** *Werkzeug-Suiten* ▸ *IP Werkzeuge* ▸ *ICMP (Ping)* · 🔑 **Rechte:** Standardbenutzer

Ping mit den Einstellungen, für die man sonst Schalter auswendig lernt.

1. Tragen Sie unter *Ziel (Domain / IP)* das Ziel ein.
2. Stellen Sie ein, was Sie brauchen:

Feld	Bedeutung
Größe (Bytes)	Nutzlast je Paket
Anzahl (0 = Endlos)	Wie viele Pakete; `0` läuft bis zum Stopp
Protokoll	*Automatisch*, *IPv4 erzwingen* oder *IPv6 erzwingen*
Nicht fragmentieren (DF)	Setzt das DF-Bit

3. *Ping Starten*. *Stoppen* bricht ab.

Die Tabelle zeigt je Paket Sequenznummer, antwortende Adresse, Byte-Zahl, Zeit, TTL und Status. Unten laufen die Kennzahlen mit: *Gesendet*, *Empfangen*, *Verlust*, *Min*, *Max*, *Durchschnitt*.

Tipp: Die Kombination aus **DF-Bit und Paketgröße** ist der schnellste Weg, eine MTU-Grenze zu finden — der Klassiker bei VPN- und Tunnelstrecken. Erhöhen Sie die Größe, bis *„Paket zu groß (DF-Bit gesetzt)"* erscheint; der letzte Wert, der noch durchkam, plus 28 Byte für die Kopfdaten ist die MTU des Weges.

Die Statusmeldungen:

Anzeige	Bedeutung
Erfolgreich	Antwort erhalten

Anzeige	Bedeutung
Zeitüberschreitung der Anforderung	Keine Antwort im Zeitfenster
Paket zu groß (DF-Bit gesetzt)	Ein Gerät auf dem Weg müsste zerlegen, darf aber nicht
Host konnte nicht aufgelöst werden.	Der Name lässt sich nicht in eine Adresse übersetzen
Keine IP-Adresse für das gewählte Protokoll gefunden.	Der Name hat keine Adresse der erzwungenen Familie

Hinweis: Keine Antwort heißt **nicht** „Gerät aus". Viele Systeme und fast alle Firewalls beantworten ICMP grundsätzlich nicht. Für die Frage „lebt es?" ist ein TCP-Port-Test aussagekräftiger — siehe *Scanner Werkzeuge ▸ IP Scanner*.

11.4 Speedtest

💻 **Menü:** *Werkzeug-Suiten ▸ IP Werkzeuge ▸ Speedtest* · 🔑 **Rechte:** Standardbenutzer · **ausgehender HTTPS-Zugang nötig**

Misst die **Download**-Geschwindigkeit, indem eine Testdatei über mehrere gleichzeitige Verbindungen geladen wird. Mehrere Ströme sind Absicht: Eine einzelne TCP-Verbindung schöpft eine schnelle Leitung meist nicht aus.

1. Wählen Sie die Größe der Testdatei (100 MB, 1 GB oder 10 GB).
2. *Start Test*. *Abbrechen* hält an.
3. Während des Laufs steht dort, wie viel bereits übertragen wurde.

✅ **Ergebnis:** *„Test erfolgreich abgeschlossen."* mit der gemessenen Geschwindigkeit unter *Download Geschwindigkeit*.

Achtung: Der Test lädt die gewählte Datenmenge **wirklich herunter**. Bei 10 GB über eine volumenbegrenzte Leitung — Mobilfunk, LTE-Router, Satellit — kostet das echtes Datenvolumen und echtes Geld.

Hinweis: Die Testdateien kommen von öffentlichen Messservern (`speedtestx.de` , `speed.hetzner.de` , `ash-speed.hetzner.com`). Die Toolbox versucht sie der Reihe nach; ist keiner erreichbar, meldet sie *„Keine Verbindung zu den Test-Servern möglich."*. Es wird **nur der Download** gemessen — kein Upload, keine Latenz, kein Jitter.

11.5 IPv4 Subnetz Rechner

💻 **Menü:** *Werkzeug-Suiten* ▸ *IP Werkzeuge* ▸ *Subnetz Rechner* · 🔑 **Rechte:** Standardbenutzer · **keine Netzverbindung nötig**

Rechnet aus einer Adresse und einer Präfixlänge alles aus, was man beim Planen braucht.

1. Tragen Sie eine IP-Adresse ein, etwa `192.168.1.1`.
2. Wählen Sie die Präfixlänge (CIDR).

✅ **Ergebnis:** Unter *Subnetz Informationen* stehen Netzwerkadresse, Broadcastadresse, erster und letzter Host, Subnetzmaske, Wildcard-Maske und die Zahl der nutzbaren Hosts. Unter *Binäre Darstellung* stehen Adresse und Maske Bit für Bit.

Tipp: Die Binärdarstellung ist mehr als Zierde. Wer sie einmal nebeneinander gesehen hat, versteht auf einen Blick, warum `/26` vier Netze aus einem `/24` macht — und warum eine Wildcard-Maske in einer Router-ACL genau umgekehrt aussieht.

11.6 Live Trace (MTR) & Map

💻 **Menü:** *Werkzeug-Suiten* ▸ *IP Werkzeuge* ▸ *Trace (MTR)* · 🔑 **Rechte:** Standardbenutzer · Kartenansicht und Standortangaben brauchen ausgehenden HTTPS-Zugang

`traceroute` zeigt den Weg einmal. MTR misst ihn **dauerhaft** — und erst dadurch sieht man, an welchem Knoten Pakete verloren gehen.

1. Tragen Sie das Ziel ein.
2. *Start Trace*.
3. Die Tabelle füllt sich Sprung für Sprung; jede Zeile wird danach **fortlaufend im Sekundentakt** weiter gemessen.
4. *Stop Trace* beendet die Messung.

Spalte	Bedeutung
#	Sprungnummer (TTL)
Hostname / IP	Der Knoten; der Name wird nachgeschlagen
Loss %	Anteil unbeantworteter Pakete an diesem Knoten
Snt / Rcv	Gesendet / empfangen
Best / Avg / Worst / Last	Laufzeiten in Millisekunden
Jitter	Schwankung der Laufzeit

Es werden bis zu **30 Sprünge** verfolgt.

> **Wichtig:** Verlust an einem **mittleren** Knoten ist meist harmlos. Viele Router beantworten TTL-Abläufe nur mit niedriger Priorität oder gar nicht, leiten den Verkehr aber tadellos weiter. Aussagekräftig ist Verlust, der **ab einem Knoten bis zum Ziel durchgehend bleibt** — dort geht wirklich etwas verloren.

> **Tipp:** Die Spalte *Jitter* ist bei Sprach- und Videoverbindungen die wichtigere: Ein gleichmäßig langsamer Weg trägt ein Telefonat, ein sprunghafter nicht.

Unter *Routenverfolgung (GeoIP)* zeichnet die Toolbox die Standorte der öffentlichen Knoten auf einer Karte.

> **Hinweis:** Für die Standorte fragt die Toolbox einen öffentlichen Dienst (`ip-api.com`) — **nur für öffentliche Adressen**. Private Adressen (10.x, 172.x, 192.168.x) und Loopback werden nie übertragen. Ohne Internetzugang bleibt die Karte leer; die Messung läuft unverändert weiter.

11.7 WHOIS & RDAP Lookup

> 💻 **Menü:** *Werkzeug-Suiten* ▸ *IP Werkzeuge* ▸ *WHOIS Abfrage* · 🔑 **Rechte:** Standardbenutzer · ausgehend TCP 43 (WHOIS) bzw. 443 (RDAP)

Beantwortet, wem eine Domain oder ein Adressbereich gehört.

1. Tragen Sie eine Domain (`beispiel.de`) oder eine IP-Adresse (`8.8.8.8`) ein.
2. Wählen Sie unter *WHOIS Server* die Registrierungsstelle. Zur Auswahl stehen unter anderem `whois.denic.de` (.de), `whois.verisign-grs.com` (.com/.net), `whois.eu` , `whois.nic.ch` , `whois.nic.at` , `whois.ripe.net` (IP-Adressen Europa), `whois.arin.net` (Amerika), `whois.apnic.net` (Asien) und `whois.iana.org` als Ausgangspunkt.
3. *Abfragen*.

Bei **Domains** läuft eine klassische WHOIS-Abfrage über TCP-Port 43. Die Antwort steht unverändert unter *Terminal Ausgabe (Raw Data)*; *Kopieren* legt sie in die Zwischenablage.

Bei **IP-Adressen** benutzt die Toolbox zusätzlich **RDAP** — die moderne, in JSON antwortende Nachfolgeschnittstelle. Das Ergebnis erscheint aufbereitet:

- *Netzwerk Zuweisung* — welcher Bereich, an wen vergeben,
- *Zuständige Kontakte (Entities)* — Rolle, Name, E-Mail, Telefon,
- *Ereignisse & Bemerkungen* — Registrierung, letzte Änderung,
- *Rohe JSON-Daten (RDAP) anzeigen* — die vollständige Antwort zum Aufklappen.

Hinweis: Seit der Datenschutz-Grundverordnung geben die meisten Registrierungsstellen zu Domains **keine Halterdaten** mehr heraus. Was Sie bekommen, sind technische Angaben: Nameserver, Registrar, Status, Datumsangaben. Bei **IP-Adressen** ist die Auskunft nach wie vor vollständig — dort sind die Zuständigen Organisationen und keine natürlichen Personen.

Tipp: Steht bei einer Domain nur wenig, fragen Sie den Registrar direkt: In der Antwort der Registrierungsstelle steht meist ein weiterer WHOIS-Server, den Sie oben auswählen können.

12 Scanner Werkzeuge

Drei Werkzeuge, um herauszufinden, **was in einem Netz steht**.

Werkzeug	Wofür
IP Scanner	Adressbereiche durchsuchen, Ports prüfen, Betriebssysteme erkennen
MAC Scanner	Hersteller aus einer MAC-Adresse bestimmen
SNMP Inspector	Aktive Netzkomponenten abfragen und ihren MIB-Baum durchlaufen

Achtung: Alle drei senden Pakete an fremde Geräte. Setzen Sie sie **nur in Netzen ein, für die Sie zuständig sind oder für die Ihnen eine schriftliche Erlaubnis vorliegt.** Ein Portscan gegen ein fremdes Netz ist in Deutschland strafbar, und ein Scan gegen Steuerungstechnik kann Anlagen zum Stillstand bringen.

12.1 IP Range & Security Scanner

💻 **Menü:** *Werkzeug-Suiten* ▸ *Scanner Werkzeuge* ▸ *IP Scanner* · 🔑 **Rechte:** Standardbenutzer für den nativen Scan; **lokaler Administrator** für die Nmap-Profile mit `-sS` oder `-O`

Der Scanner hat zwei Motoren, zwischen denen Sie oben umschalten.

12.1.1 Nativer Fast-Scan (C# TCP)

Eingebaut, ohne Zusatzsoftware. Er prüft je Adresse einen Ping und die angegebenen TCP-Ports und löst Hostnamen auf. Für die tägliche Frage „wer ist da?" reicht das und ist schnell.

12.1.2 Nmap Security Engine

Benutzt das installierte **Nmap**. Es kann deutlich mehr: Dienstversionen erkennen, Betriebssysteme raten, Schwachstellen-Skripte laufen lassen.

Voraussetzung: `nmap.exe` muss installiert sein. Fehlt es, zeigt die Seite „⚠️ *nmap.exe fehlt.*" mit der Schaltfläche *Jetzt installieren* — die Toolbox lädt dann das Installationsprogramm von `nmap.org` und startet es. Sie müssen dem Installationsassistenten folgen; unbeaufsichtigt läuft er nicht.

Fünf Profile stehen zur Wahl:

Profil	Nmap-Schalter	Was es tut	Admin nötig
Schneller Ping Sweep	`-sn`	Nur Erreichbarkeit, keine Ports	nein

Profil	Nmap-Schalter	Was es tut	Admin nötig
Quick Scan (Top 100 Ports)	`-F`	Die 100 häufigsten Ports	nein
Intense Scan (OS & Service)	`-sV -O -T4`	Dienstversionen und Betriebssystem	**ja**
Stealth Scan (SYN Half-Open)	`-sS`	Halboffener SYN-Scan	**ja**
Security Audit (Vuln Scripts)	`-sV --script vuln -T4`	Schwachstellen-Skripte	nein

Voraussetzung: *Intense Scan* und *Stealth Scan* brauchen Rohsockets und damit **Administratorrechte**. Läuft die Toolbox ohne, sagt sie das und startet den Scan nicht — eine Rechteerhöhung mitten im Lauf ist nicht möglich.

Achtung: *Security Audit* führt aktive Prüf-Skripte gegen die gefundenen Dienste aus. Das ist ein Eingriff und kein Blick: Ältere Geräte — Drucker, Steuerungen, Medizintechnik — können daran hängenbleiben oder abstürzen. Kündigen Sie diesen Lauf an, und führen Sie ihn nicht im laufenden Betrieb aus.

12.1.3 Einen Scan ausführen

1. Legen Sie den Bereich fest — auf einem von drei Wegen: * *IP Bereich (Start)* und *IP Bereich (Ende)* von Hand eintragen, * *Lokales Subnetz laden* — die Toolbox trägt das eigene Netz ein, * *Subnetz wählen* unter *Aus Ordivis* — ein in Ordivis Platform bekanntes Netz übernehmen (siehe Kapitel *Ergebnisse an Ordivis übergeben*).
2. Tragen Sie unter *Ports scannen* die Ports kommagetrennt ein, etwa `22,80,443,3389`.
3. Schalten Sie bei Bedarf zu: * *Nur erreichbare (Alive) Hosts anzeigen* — blendet stumme Adressen aus, * *SNMP-Anreicherung* — fragt zusätzlich per SNMP nach Gerätename, Standort und Geräteklasse (ein zusätzliches UDP-Paket je Host).
4. *Starten*. *Stopp* bricht ab.

Die Tabelle zeigt IP-Adresse, Hostname, Ports/Status sowie OS- und Dienstangaben. Die Farben:

Farbe	Bedeutung
Grün	Online, mit offenen Ports
Blau	Online, aber keiner der geprüften Ports offen
Grau	Keine Antwort

Unten laufen die Zähler *Geprüft*, *Alive* und *Threads* mit.

Tipp: Ein Gerät, das auf Ping nicht antwortet, aber einen offenen Port hat, ist **online**. Genau deshalb lohnt es sich, ein paar typische Ports mitzugeben, statt sich auf den Ping zu verlassen — die meisten Windows-Rechner blocken ICMP standardmäßig.

Das Ergebnis lässt sich an Ordivis Platform übergeben (*An Ordivis senden*); siehe Kapitel *Ergebnisse an Ordivis übergeben*.

12.2 MAC Scanner & Vendor Lookup

💻 **Menü:** *Werkzeug-Suiten* ▸ *Scanner Werkzeuge* ▸ *MAC Scanner* · 🔑 **Rechte:** Standardbenutzer

Die ersten drei Byte einer MAC-Adresse — die **OUI** — sind beim IEEE auf einen Hersteller registriert. Daraus lässt sich sagen, was für ein Gerät hinter einer Adresse steckt, ohne es anzufassen.

12.2.1 Eine MAC-Adresse nachschlagen

1. Tragen Sie die Adresse ein, etwa `00:1A:2B:3C:4D:5E`. Auch Schreibweisen mit Bindestrichen oder ohne Trennzeichen werden erkannt.
2. *Suchen*.

✅ **Ergebnis:** Unter *Suchergebnis* stehen die eingegebene Adresse, das OUI-Präfix und der Hersteller.

Hinweis: Steht dort *„Unbekannt / Nicht registriert"*, gibt es zu diesem Präfix keinen Eintrag. Das ist bei virtuellen Maschinen, Containern und bei Geräten mit zufällig gewürfelter MAC-Adresse normal — moderne Mobiltelefone ändern ihre WLAN-MAC absichtlich, um sich nicht wiedererkennen zu lassen.

12.2.2 Die eigenen Schnittstellen

Unter *Lokale Netzwerkschnittstellen & Hersteller* stehen alle Karten dieses Rechners mit Name, MAC-Adresse, Hersteller und Typ. Der Hersteller einer virtuellen Karte verrät oft, welche Software sie angelegt hat.

Hinweis: Für die manuelle Suche fragt die Toolbox einen öffentlichen Dienst (`api.macvendors.com`) ab; kommt keine Antwort, steht dort *„API-Fehler oder Timeout"*. Die Hersteller der **eigenen** Karten und die Anreicherung im IP Scanner werden dagegen **ohne Netzverbindung** aus einer eingebauten Tabelle aufgelöst.

12.3 SNMP Device Inspector & MIB Walker

💻 **Menü:** *Werkzeug-Suiten* ▸ *Scanner Werkzeuge* ▸ *SNMP Inspector* · 🔑 **Rechte:** Standardbenutzer · ausgehend UDP 161 zum Ziel

Fragt Switche, Router, Drucker, USV-Anlagen und alles andere ab, was einen SNMP-Agenten hat.

12.3.1 Ein Gerät abfragen

1. Tragen Sie unter *Ziel (IP / Host)* das Gerät ein.
2. Tragen Sie unter *Community* die Lese-Community ein — üblich ist `public`.
3. Wählen Sie die *Version*: `v1`, `v2c` (Vorgabe) oder `v3`.
4. *Abfragen*.

✅ **Ergebnis:** Auf dem Reiter *System-Übersicht (Auto-Scan)* stehen die erkannte Geräteklasse und die Systemangaben: Hostname (`sysName`), Betriebsdauer, Standort, Kontakt und die Objektkennung (`sysObjectID`).

Die drei Fehlerbilder und was sie bedeuten:

Meldung	Ursache
„… ist erreichbar, aber der SNMP-Port (UDP 161) ist geschlossen."	Das Gerät lebt, SNMP ist dort abgeschaltet oder gefiltert
„Falsche Community / Version"	Gerät und Community/Version passen nicht zusammen
„… ist offline oder blockiert alle Anfragen (Ping & SNMP Timeout)."	Keine Antwort auf beides

Wichtig: Die Community ist bei **v1 und v2c** ein Kennwort, das **im Klartext** über das Netz geht. Wer im selben Netz mitschneidet, liest sie mit. Setzen Sie v1/v2c nur in Netzen ein, denen Sie das zutrauen, und benutzen Sie eine **Lese**-Community — nie die Schreib-Community für eine Abfrage.

Grenze: Für **v3** — die Fassung mit Authentifizierung und Verschlüsselung — steht in der Auswahl ein Eintrag, aber es gibt kein Feld für Benutzer, Authentifizierungs- und Verschlüsselungsverfahren. Rechnen Sie deshalb bei v3-Geräten nicht mit einer Antwort. Wo v3 vorgeschrieben ist, greifen Sie zu einem SNMP-Werkzeug, das es vollständig unterstützt.

12.3.2 Den MIB-Baum durchlaufen

Auf dem Reiter *MIB-Baum (Walk)* lässt sich der ganze Objektbaum eines Geräts auslesen.

1. Tragen Sie unter *Root OID (Startpunkt)* die Wurzel ein. `1.3.6.1.2.1` ist die MIB-2 und damit der übliche Ausgangspunkt.
2. *Walk starten*. *Walk stoppen* bricht ab.

Tipp: Ein Walk über `1.3.6.1.2.1.2.2.1.2` liefert die Namen aller Ports eines Switches, ein Walk über `1.3.6.1.2.1.2.2.1.8` ihren Betriebszustand. Das ist der schnellste Weg, um zu sehen, an welchem Port etwas hängt — ohne sich am Gerät anzumelden.

Achtung: Ein Walk über die gesamte Wurzel `1` kann bei großen Geräten sehr lange dauern und Tausende Zeilen liefern. Fangen Sie so tief wie möglich an.

Das Ergebnis lässt sich als Gerät an Ordivis Platform übergeben; siehe Kapitel *Ergebnisse an Ordivis übergeben*.

13 DNS Werkzeuge

Zwei Werkzeuge für Namen und Adressen.

Werkzeug	Wofür
Basis Scanner	Ein Ziel von allen Seiten ansehen: Auflösung, Standort, Erreichbarkeit, Ports, TLS-Zertifikat, alle DNS-Einträge
Zone Lookup	Eine Zone möglichst vollständig abklopfen — oder eine IP-Adresse rückwärts auflösen

13.1 DNS, IP & Host Lookup (Basis Scanner)

💻 **Menü:** *Werkzeug-Suiten* ▸ *DNS Werkzeuge* ▸ *Basis Scanner* · 🔑 **Rechte:** Standardbenutzer · Standort und Karte brauchen ausgehenden HTTPS-Zugang

Ein Feld, ein Klick, sechs Antworten. Das ist das Werkzeug, mit dem man anfängt, wenn jemand sagt „die Seite geht nicht".

1. Tragen Sie eine Domain oder IP-Adresse ein, etwa `www.beispiel.de`.
2. *Lookup*.

Die Ergebnisse stehen untereinander:

13.1.1 Schnell-Auflösung (Basis)

Eingabe, aufgelöste IP-Adresse, Hostname und die **Aliase (CNAMEs)**. Die Aliase sind oft schon die halbe Antwort: Wenn `www.beispiel.de` auf einen Cloud-Anbieternamen zeigt, weiß man, wen man fragen muss.

13.1.2 Standort & Provider (GeoIP)

Land, Region, Stadt, Provider (ISP), Organisation und Koordinaten. Darunter eine **Kartenansicht**.

> **Hinweis:** Der Standort wird bei einem öffentlichen Dienst (`ip-api.com`) abgefragt und ist eine **Schätzung** — er nennt den Standort der Registrierung, nicht unbedingt den des Servers. Für private Adressen wird er nicht abgefragt. Bleibt die Karte leer, fehlt der Internetzugang oder die WebView2-Komponente ist nicht bereit; die übrigen Ergebnisse sind davon unberührt.

13.1.3 Erreichbarkeit (ICMP Ping)

Status und Laufzeit (RTT) eines einzelnen Pings.

13.1.4 Basis Port-Scan (TCP)

Sechs feste Ports werden geprüft:

Port	Dienst
21	FTP
22	SSH
53	DNS
80	HTTP
443	HTTPS
3389	RDP

Hinweis: Diese Auswahl ist fest. Wer andere Ports braucht, nimmt *Scanner Werkzeuge ▸ IP Scanner* — dort ist die Portliste frei.

13.1.5 SSL/TLS Zertifikat & Security Audit

Antwortet das Ziel auf Port 443, baut die Toolbox eine TLS-Verbindung auf und untersucht sie. Das ist der nützlichste Teil der Seite.

Zertifikat — Inhaber, Aussteller (CA) und Gültigkeitsende. Das Ablaufdatum ist farbig hinterlegt, damit ein bald ablaufendes Zertifikat auffällt.

Verschlüsselung & Audit — Protokollversion, Cipher Suite, Schlüssellänge, Signaturalgorithmus. Veraltete Werte werden farblich markiert.

Integrität & Vertrauen — drei Prüfungen:

Prüfung	Frage
Hostname-Match	Gilt das Zertifikat für genau den Namen, den Sie eingegeben haben?
Zertifikatskette	Lässt sich die Kette bis zu einer vertrauten Wurzel schließen?
Sperrstatus (CRL)	Ist das Zertifikat zurückgezogen worden?

Tipp: Diese drei Zeilen erklären fast jede Browser-Warnung. *Hostname-Match* schlägt fehl, wenn ein Zertifikat für `beispiel.de` unter `www.beispiel.de` ausgeliefert wird; *Zertifikatskette* schlägt fehl, wenn das Zwischenzertifikat auf dem Server fehlt. Für den zweiten Fall bauen Sie die Kette in *CA & PKI ▸ Lokale Zertifikate (PKI)* zusammen.

13.1.6 Alle DNS Einträge

Eine Tabelle mit Typ und Wert — die Toolbox fragt `A`, `AAAA`, `MX`, `NS`, `TXT`, `SOA` und `CNAME` ab. Das entspricht dem, was `dig` oder `nslookup` liefern, ohne sieben Aufrufe.

13.2 DNS Zone & Reverse IP Lookup

> 💻 **Menü:** *Werkzeug-Suiten* ▸ *DNS Werkzeuge* ▸ *Zone Lookup* · 🔑 **Rechte:** Standardbenutzer · Rückwärtsauflösung braucht ausgehenden HTTPS-Zugang

Diese Seite erkennt an der Eingabe, was Sie wollen: Bei einer **Domain** klopft sie die Zone ab, bei einer **IP-Adresse** löst sie rückwärts auf.

13.2.1 Eine Zone abklopfen

1. Tragen Sie eine Domain ein, etwa `microsoft.com`.
2. *Lookup starten*.

Die Toolbox fragt zunächst alle üblichen Eintragsarten der Zone selbst ab — `SOA`, `NS`, `A`, `AAAA`, `MX`, `TXT`, `CNAME`, `SRV`, `CAA` — und probiert danach eine Liste gängiger Namen unterhalb der Domain durch:

`www`, `mail`, `m`, `blog`, `ftp`, `api`, `dev`, `remote`, `autodiscover`, `sip`, `test`, `portal`, `vpn`, `smtp`, `pop`, `imap`, `ns1`, `ns2`

> ✅ **Ergebnis:** Eine nach Eintragsart sortierte Tabelle mit Hostname, Typ, TTL und Wert, darüber die Zahl der gefundenen Einträge.

> **Wichtig:** Dies ist **kein echter Zonentransfer (AXFR)**. Ein AXFR liefert alles; hier wird geraten und geprüft. Das Ergebnis ist deshalb immer eine **Untermenge** — was nicht auf der Namensliste steht, taucht auch nicht auf. Wer die vollständige Zone braucht, holt sie beim zuständigen DNS-Server, wo ein Transfer erlaubt ist.

> **Hinweis:** Aus demselben Grund ist das Verfahren unauffällig: Es sind gewöhnliche DNS-Abfragen, wie sie jeder Client stellt.

13.2.2 Eine IP-Adresse rückwärts auflösen

1. Tragen Sie eine IP-Adresse ein, etwa `8.8.8.8`.
2. *Lookup starten*.

Die Tabelle zeigt:

Zeile	Bedeutung
IP-Adresse	Die Eingabe
Reverse DNS (PTR)	Der rückwärts eingetragene Name — oder *Kein PTR-Eintrag gefunden (NXDOMAIN)*
Netzwerk (CIDR)	Der Adressblock, zu dem sie gehört

Zeile	Bedeutung
Netzwerk (ASN) / Provider (ASN)	Das autonome System und sein Betreiber
Organisation	Wem der Block zugeteilt ist
Land, Region / Stadt, Zeitzone, Geo-Koordinaten	Die Standortschätzung

Dazu eine Karte.

Hinweis: Für Netzblock und ASN fragt die Toolbox `api.bgpview.io` ab, für den Standort `ip-api.com`. Bei privaten Adressen kommt *„Fehler bei der Abfrage oder IP ist lokal/privat."* — das ist richtig so: Über eine private Adresse weiß das Internet nichts.

Tipp: Ein fehlender PTR-Eintrag ist bei Mailservern ein handfestes Problem — viele Gegenstellen weisen Post von Adressen ohne Rückwärtsauflösung ab. Diese Seite beantwortet das in einem Schritt; die vollständige Mail-Prüfung leistet *E-Mail Werkzeuge ▸ SMTP Diagnose*.

14 Remote Werkzeuge

14.1 Remote Manager (RDP, SSH, FTP)

💻 **Menü:** *Werkzeug-Suiten* ▸ *Remote Werkzeuge* ▸ *Remote Manager* · 🔑 **Rechte:** Standardbenutzer

Eine Liste der Ziele, auf die Sie regelmäßig zugreifen — mit Anmeldedaten, mit laufender Erreichbarkeitsanzeige und mit einem Klick zum Verbinden. Es ersetzt die Sammlung von `.rdp`-Dateien auf dem Desktop und die Zettelwirtschaft daneben.

14.1.1 Eine Verbindung anlegen

1. Klicken Sie auf *Neu*.
2. Füllen Sie unter *Konfiguration* die Felder:

Feld	Inhalt
Anzeigename (Titel)	Wie die Verbindung in der Liste heißen soll
Ziel (Host / FQDN / IP)	Das Ziel
Protokoll	*RDP*, *SSH*, *FTP* oder *SFTP*
Benutzername	Das Konto auf dem Ziel
Passwort	Optional — bleibt es leer, fragt das Zielprogramm

3. Je nach Protokoll erscheinen weitere Abschnitte: * **RDP Einstellungen** — *Im Vollbildmodus starten*, *Zwischenablage umleiten (Clipboard)*, *Lokale Laufwerke umleiten*. * **Datei-Transfer (FTP/SFTP)** — ein Hinweis, dass die Verbindung in **WinSCP** geöffnet wird, falls installiert, sonst im Windows-Explorer.
4. *Speichern*.

Achtung: *Lokale Laufwerke umleiten* macht Ihre Festplatten auf dem entfernten System sichtbar. Auf einem Server, dem Sie vertrauen, ist das bequem; auf einem System, das kompromittiert sein könnte, ist es der Weg, auf dem Schadsoftware zu Ihnen kommt. Dasselbe gilt abgeschwächt für die Zwischenablage.

14.1.2 Verbinden

1. Wählen Sie die Verbindung in der Liste.
2. *Verbinden*.

Was dann geschieht, hängt vom Protokoll ab:

Protokoll	Was passiert
RDP	Die Toolbox schreibt eine `.rdp`-Datei mit Ihren Einstellungen, hinterlegt das Kennwort im Windows-Anmeldeinformationsspeicher (`cmdkey`) und startet `mstsc.exe`. Die Anmeldung läuft dadurch ohne Rückfrage durch.
SSH	Die Sitzung wird an das für SSH eingetragene Standardprogramm übergeben.
FTP / SFTP	Die Verbindung wird als URL an **WinSCP** übergeben, falls installiert; sonst öffnet der Windows-Explorer.

Voraussetzung: Ist für SFTP kein Programm registriert, meldet die Toolbox *„WinSCP wird benötigt"*. Installieren Sie WinSCP — der Windows-Explorer kann zwar FTP, aber kein SFTP.

14.1.3 Die Erreichbarkeitsanzeige

Die Toolbox prüft die Ziele im Hintergrund mit einem Ping (Zeitfenster 1,5 Sekunden) und zeigt in der Liste je Eintrag die Laufzeit, *Prüfe…*, *Offline* oder *Fehler*.

Hinweis: *Offline* heißt nur, dass auf ICMP keine Antwort kam. Viele Server beantworten Ping nicht und sind trotzdem erreichbar. Die Anzeige ist ein Anhaltspunkt, kein Urteil.

14.1.4 Wie Kennwörter gespeichert werden

Wichtig: Kennwörter werden **verschlüsselt** in Ihrem Benutzerprofil abgelegt — gebunden an **dieses Windows-Konto auf diesem Rechner** (Windows DPAPI). Die Datei ist auf einem anderen Rechner oder unter einem anderen Konto nicht lesbar. Das Feld in der Oberfläche sagt es selbst: *„Verschlüsselt gespeichert (nur dieses Konto, dieser Rechner)"*.

Daraus folgt zweierlei:

- Die Verbindungsliste lässt sich **nicht** durch Kopieren der Datei auf einen anderen Rechner mitnehmen — die Kennwörter wären dort unlesbar. Die Einträge selbst bleiben erhalten, die Kennwörter müssen neu eingetragen werden.
- Wer Zugriff auf Ihr angemeldetes Windows-Konto hat, kann sie lesen. Der Schutz ist Ihr Windows-Kennwort und die Bildschirmsperre.

Achtung: Beim Verbinden per RDP wird das Kennwort über `cmdkey` in den Windows-Anmeldeinformationsspeicher geschrieben, damit `mstsc` es benutzen kann. Bei FTP und SFTP steht es in der übergebenen URL. Beides ist der übliche Weg dieser Werkzeuge — beides bedeutet, dass das Kennwort den Bereich der Toolbox verlässt. Für hochprivilegierte Konten ist es die bessere Wahl, das Kennwortfeld leer zu lassen und beim Verbinden zu tippen.

Hinweis: Erscheint *„Verbindungen nicht gespeichert"*, ließ sich die Datei nicht schreiben. Die Änderungen gelten dann nur für diese Sitzung. Das passiert etwa, wenn das Benutzerprofil schreibgeschützt oder die Platte voll ist.

14.1.5 Eine Verbindung löschen

Wählen Sie sie in der Liste und klicken Sie auf *Löschen*. Es gibt keine Rückfrage und keinen Papierkorb.

15 E-Mail Werkzeuge

Zwei Werkzeuge für die zwei häufigsten Mail-Fragen: *„Warum kommt diese Mail nicht an?"* und *„Ist diese Mail echt?"*

Werkzeug	Wofür
E-Mail Header Analyse	Eine einzelne Mail auseinandernehmen: Weg, Zeitverlust, SPF/DKIM/DMARC
SMTP Diagnose	Eine Domain prüfen: MX, SPF, DMARC, DKIM

15.1 E-Mail Header Analyzer

💻 **Menü:** *Werkzeug-Suiten* ▸ *E-Mail Werkzeuge* ▸ *E-Mail Header Analyse* · 🔑 **Rechte:** Standardbenutzer · **keine Netzverbindung nötig**

Der Kopfbereich einer E-Mail enthält den vollständigen Weg, den sie genommen hat, und das Urteil des empfangenden Servers über ihre Echtheit. Beides steht dort in einer Form, die niemand freiwillig liest — dieses Werkzeug bereitet es auf.

15.1.1 Einen Header untersuchen

⚙️ **Außerhalb:** Den Rohtext des Headers holen Sie in Ihrem Mailprogramm.

1. Holen Sie den vollständigen, rohen Header: * **Outlook:** Mail öffnen ▸ *Datei* ▸ *Eigenschaften* ▸ *Internetkopfzeilen* * **Outlook im Web:** … ▸ *Anzeigen* ▸ *Nachrichtendetails anzeigen* * **Thunderbird:** *Ansicht* ▸ *Nachrichten-Quelltext* (Strg + U) * **Gmail:** … ▸ *Original anzeigen*
2. Fügen Sie ihn in das große Textfeld ein.
3. *Analysieren*.

15.1.2 Basis-Informationen

Betreff, Von, An, Datum und Message-ID.

15.1.3 Sicherheit (Authentication-Results)

Die drei Urteile, die der empfangende Server gefällt hat:

Prüfung	Was sie beantwortet
SPF	Durfte der absendende Server für diese Domain versenden?
DKIM	Ist die Signatur der Mail gültig und unverändert?
DMARC	Passen SPF- beziehungsweise DKIM-Domain zur Absenderadresse, und was sagt die Richtlinie der Domain dazu?

Wichtig: Diese Werte kommen **aus der Mail** und sind das Ergebnis der Prüfung des empfangenden Servers. Die Toolbox prüft hier nichts nach — sie liest ab. Wer die Domain selbst prüfen will, nimmt die *SMTP Diagnose*.

Achtung: Alle Kopfzeilen außer den Prüfergebnissen des **eigenen** Mailservers sind fälschbar. *Von*, *An* und die *Received*-Zeilen der Gegenseite kann ein Angreifer frei erfinden. Verlässlich sind allein die Zeilen, die Ihre eigene Infrastruktur hinzugefügt hat — sie stehen ganz oben.

15.1.4 Relay-Verlauf (Received Hops)

Eine Tabelle mit dem Weg der Mail, Station für Station:

Spalte	Bedeutung
Hop	Laufende Nummer, in der Reihenfolge der Zustellung
Übermittelt von (From)	Wer übergeben hat
Empfangen von (By)	Wer entgegengenommen hat
Zeitstempel	Wann
Verzögerung	Wie lange die Mail an dieser Station lag

Tipp: Die Spalte *Verzögerung* beantwortet die Frage „warum kam die Mail erst nach zwei Stunden?" in einer Zeile: Dort, wo die Sekunden stehen, wurde gewartet — meist an einer Greylisting-Stufe oder einem überlasteten Gateway.

Steht dort *„Keine gültigen Received-Header zur Verfolgung gefunden."*, war der eingefügte Text unvollständig — sehr wahrscheinlich wurde nur ein Ausschnitt kopiert.

15.2 E-Mail Delivery Diagnose (MX, SPF, DKIM, DMARC)

💻 **Menü:** *Werkzeug-Suiten* ▸ *E-Mail Werkzeuge* ▸ *SMTP Diagnose* · 🔑 **Rechte:** Standardbenutzer · DNS-Auflösung nach außen nötig

Prüft eine **Domain** darauf, ob sie Post empfangen kann und ob ihre Post bei anderen ankommt. Das ist die Seite, die man aufschlägt, bevor man einen Mailserver umzieht — und die, auf der man nachsieht, wenn die eigenen Mails im Spam landen.

1. Tragen Sie die Domain ein, etwa `beispiel.de` — **ohne** `@` und ohne Postfach.
2. *Prüfen*.

15.2.1 MX Records (Mail Exchange)

Welche Server nehmen Post für diese Domain an? Die Tabelle zeigt Präferenz, Hostname und aufgelöste IP-Adresse.

> **Hinweis:** Steht dort *„Keine MX-Einträge gefunden. Diese Domain kann keine E-Mails empfangen."*, ist das ein handfester Befund — und der häufigste Grund für Unzustellbarkeitsmeldungen nach einem DNS-Umzug.

15.2.2 SPF Record (Sender Policy Framework)

Der SPF-Eintrag wird nicht nur angezeigt, sondern **in seine Bestandteile zerlegt**: je Mechanismus Präfix, Typ, Wert, Ergebnis und eine Beschreibung im Klartext.

> **Tipp:** Achten Sie auf den Abschluss. `-all` weist alles ab, was nicht aufgeführt ist; `~all` markiert es nur als verdächtig; `?all` sagt gar nichts. Wer nach einem Umzug noch auf `?all` steht, hat SPF faktisch abgeschaltet.

> **Wichtig:** SPF erlaubt höchstens **zehn** DNS-Abfragen je Prüfung. Jedes `include:` zählt mit. Wer zu viele Dienstleister einträgt, überschreitet die Grenze — und dann schlägt SPF **für alle** Empfänger fehl, ohne dass sich am Eintrag sichtbar etwas geändert hätte.

15.2.3 DMARC Record

Der Eintrag unter `_dmarc.<domain>`, aufgeschlüsselt nach Tag, Wert und Bedeutung — etwa *DKIM Alignment* (`adkim`), Richtlinie (`p`) und Berichtsadressen (`rua`, `ruf`).

Steht dort *„Kein DMARC-Record unter _dmarc gefunden."*, hat die Domain keine DMARC-Richtlinie. Empfänger entscheiden dann nach eigenem Gutdünken.

15.2.4 DKIM (DomainKeys Identified Mail)

Hier liegt eine Besonderheit, die das Werkzeug selbst benennt: **DKIM hat keinen festen DNS-Namen.** SPF steht immer auf der Domain, DMARC immer unter `_dmarc` — den DKIM-Selektor darf sich jeder Versender frei wählen. Man kann ihn also nicht abfragen, sondern nur raten.

Die Toolbox probiert deshalb die gebräuchlichen Selektoren durch — darunter `default`, `dkim`, `mail`, `smtp`, `google`, `selector1`, `selector2`, `k1`, `s1`, `plesk`, `mandrill`, `sendgrid`, `mailjet` und `postmark` — und zeigt zu jedem Treffer Selektor, Verfahren, Schlüssellänge und einen Hinweis.

> **Wichtig:** *„Unter keinem der geprüften Selektoren wurde ein DKIM-Schlüssel gefunden"* bedeutet **nicht**, dass die Domain kein DKIM hat. Es bedeutet, dass der Selektor nicht auf der Liste stand. Den tatsächlich verwendeten Selektor finden Sie in einer echten Mail dieser Domain: im Header unter `DKIM-Signature`, Feld `s=`. Diese Mail untersuchen Sie mit dem *E-Mail Header Analyzer*.

Tipp: Eine Schlüssellänge unter 1024 Bit gilt als zu kurz; große Anbieter behandeln solche Signaturen wie gar keine. 2048 Bit ist heute der übliche Wert.

16 NTP & Zeitzonen

💻 **Menü:** *System & LAN* ▸ *NTP & Zeitzonen* · 🔑 **Rechte:** Standardbenutzer zum Prüfen; **lokaler Administrator** zum Setzen von Zeit oder Zeitzone (die Toolbox fordert die Rechte im Moment der Aktion an)

Eine falsch gehende Uhr ist die Ursache, an die man zuletzt denkt — und sie erklärt sehr viel: fehlgeschlagene Kerberos-Anmeldungen (mehr als fünf Minuten Abweichung genügen), abgelehnte Zertifikate, Protokolldateien, die nicht zusammenpassen, Sicherungen, die zur falschen Zeit laufen.

Diese Seite vergleicht die lokale Uhr **gleichzeitig mit mehreren Referenzservern** und stellt sie auf Wunsch nach.

16.1 Lokales System

Links oben stehen:

- **Aktuelle Zeit** — die Systemzeit, laufend, mit Millisekunden.
- **Sommerzeit (DST)** — *Aktiv (Sommerzeit)* oder *Inaktiv (Normal/Winterzeit)*.
- **Zeitzone** — die eingestellte Zone, in einer Auswahlliste.

16.2 Die Zeit prüfen

1. Tragen Sie unter *Zu prüfende Server* ein, wen Sie fragen wollen:

Feld	Vorgabe	Wofür
Eigener Server	leer	Der interne Zeitserver, meist der PDC-Emulator — Beispiel: `192.168.1.1`
Deutschland	`de.pool.ntp.org`	Öffentliche Referenz aus Deutschland
USA	`us.pool.ntp.org`	Zum Vergleich über eine lange Strecke
Taiwan	`tw.pool.ntp.org`	Zum Vergleich über eine sehr lange Strecke

Leere Felder werden übersprungen. 2. *Zeitabgleich prüfen*.

✅ **Ergebnis:** Unter *Ergebnisse* steht je Server die dort gemeldete Zeit und die *Abweichung (s)* zur eigenen Uhr. *Timeout* heißt, dass der Server nicht antwortete.

Tipp: Die drei öffentlichen Server sind nicht dazu da, die Zeit aus Taiwan zu holen. Sie sind die **Gegenprobe**: Weichen alle drei gleich ab, geht die eigene Uhr falsch. Weicht nur der interne Server ab, geht **er** falsch — und mit ihm die ganze Domäne.

Hinweis: Für jede Abfrage werden mehrere NTP-Pakete gesendet und gemittelt. Ein einzelnes Paket kann durch eine verzögerte Warteschlange auf dem Weg verfälscht sein; der Mittelwert ist belastbarer.

16.3 Die Systemzeit stellen

Achtung: Die Systemzeit zu ändern, wirkt sich auf **alles** aus, was auf diesem Rechner läuft: Protokolle, Zertifikatsprüfungen, geplante Aufgaben, Datenbanken, Kerberos-Tickets. Auf einem Domänenmitglied ist es fast immer der **falsche** Weg — dort holt sich Windows die Zeit ohnehin vom Domain Controller, und ein Handeingriff wird beim nächsten Abgleich überschrieben. Richtig ist dieser Weg auf einem Rechner **ohne** Domäne oder wenn der Zeitdienst selbst nicht mehr greift.

1. Klicken Sie in der Ergebniszeile des Servers, dem Sie folgen wollen, auf die Schaltfläche zum Synchronisieren.
2. Windows fragt nach Administratorrechten (UAC). Bestätigen Sie.

✅ **Ergebnis:** *„Systemzeit auf … synchronisiert."*, dahinter die **verbleibende Abweichung** in Millisekunden. Grün heißt unter einer Sekunde, orange darüber.

Hinweis: Die Toolbox macht dabei zweierlei richtig, was man leicht falsch macht: Sie fragt den Server **im Moment des Setzens erneut** — der Wert von der Prüfung ist zu diesem Zeitpunkt schon Sekunden bis Minuten alt — und sie übergibt eine **Korrektur** statt einer Uhrzeit. Eine Korrektur bleibt gültig, während die UAC-Rückfrage offen steht; ein Zeitpunkt nicht. Anschließend misst sie nach und nennt, was übrig blieb — eine Erfolgsmeldung, die nur wiederholt, was gesendet wurde, belegt nichts.

Hinweis: Kommt *„Synchronisierung abgebrochen — die Anforderung der Administrator-Rechte wurde abgelehnt oder das Setzen verweigert."*, wurde die UAC-Rückfrage verneint oder eine Richtlinie verbietet das Stellen der Uhr.

16.4 Die Zeitzone ändern

1. Wählen Sie unter *Zeitzone* die gewünschte Zone.
2. *Zeitzone auf System anwenden*.
3. Bestätigen Sie die UAC-Rückfrage.

✅ **Ergebnis:** *„Zeitzone auf '…' geändert."*

Hinweis: Die Umstellung erfolgt über das Windows-Werkzeug `tzutil`. Ändern Sie die Zeitzone **nicht**, um eine falsche Uhrzeit zu korrigieren — das verschiebt die Anzeige und lässt die eigentliche Abweichung bestehen. Erst die Zone richtig setzen, dann die Zeit prüfen.

16.5 Wenn die Zeit im ganzen Netz nicht stimmt

Diese Seite behandelt **einen** Rechner. Die Zeitversorgung eines Netzes gehört in die Hand des Domain Controllers mit der PDC-Emulator-Rolle — welcher das ist, sagt *Active Directory ▸ AD Diagnose ▸ FSMO Rollen Inhaber*. Wie man die Kette einrichtet und prüft, steht im **Administratorhandbuch**, Kapitel *Zeitsynchronisation im Netz*.

17 Wake on LAN

💻 **Menü:** *System & LAN* ▸ *Wake on LAN* · 🔑 **Rechte:** Standardbenutzer

Weckt ein Gerät aus Standby oder Ruhezustand, indem ein **Magic Packet** an seine MAC-Adresse geschickt wird. Anschließend wartet die Toolbox darauf, dass das Gerät antwortet — und sagt, wann es so weit ist.

17.1 Ein Gerät aufwecken

1. Tragen Sie unter *IP-Adresse* die Adresse des Geräts ein. Pflichtfeld.
2. Tragen Sie unter *MAC-Adresse* die Hardware-Adresse ein — oder lassen Sie das Feld leer.
3. *Aufwecken*.

Was dann geschieht, steht im *Aktivitäts-Log* mit, Zeile für Zeile:

1. *Starte Wake-Vorgang für IP: …*
2. Ohne MAC-Adresse: *MAC-Adresse nicht angegeben. Versuche automatische Auflösung via ARP-Cache…* — und bei Erfolg *Erfolgreich aufgelöst: MAC = …*
3. *Magic Packet (WoL) wurde erfolgreich als Broadcast (Port 7 & 9) gesendet.*
4. *Warte auf Bootvorgang… Prüfe Erreichbarkeit von … (Timeout in 60s)*
5. *Erfolg! Das Gerät … hat geantwortet und ist nun ONLINE (Ping: … ms).*

Abbrechen hält das Warten an.

✅ **Ergebnis:** Die Erfolgsmeldung mit der gemessenen Antwortzeit. Bleibt sie aus, kommt nach 60 Sekunden *„Zeitüberschreitung: Das Gerät … hat nach 60 Sekunden nicht auf Pings reagiert."*

17.2 Die MAC-Adresse

Das Magic Packet spricht **die MAC-Adresse** an, nicht die IP-Adresse — ein schlafendes Gerät hat keine aktive IP-Konfiguration mehr. Die IP-Adresse dient hier nur zwei Zwecken: das richtige Netz zu bestimmen und danach die Erreichbarkeit zu prüfen.

Wird das MAC-Feld leer gelassen, sucht die Toolbox die Adresse im **ARP-Cache** — also in der Liste der Geräte, mit denen dieser Rechner kürzlich gesprochen hat.

Voraussetzung: Das funktioniert nur, wenn das Gerät **erst kürzlich** aktiv war. Steht es länger still, ist der Eintrag verfallen, und es kommt *„Gerät ist nicht im ARP-Cache. Wenn das Gerät schon lange offline ist, muss die MAC manuell eingegeben werden."*

Tipp: Notieren Sie sich die MAC-Adressen der Geräte, die Sie regelmäßig aufwecken, **solange sie laufen**. *IP Werkzeuge* ▸ *ARP Tabelle* und *Scanner Werkzeuge* ▸ *IP Scanner* zeigen sie beide an. Wer sie erst braucht, wenn das Gerät aus ist, kommt zu spät.

Die MAC-Adresse muss in der Form `XX:XX:XX:XX:XX:XX` eingetragen werden. Bei abweichender Schreibweise meldet die Toolbox *„Ungültiges MAC-Format"*.

17.3 Warum es manchmal nicht klappt

Wake on LAN scheitert selten am Magic Packet — es scheitert an den Voraussetzungen drumherum. Die Toolbox kann nur senden; der Rest liegt am Gerät und am Netz.

Voraussetzung: Alle vier Punkte müssen erfüllt sein:

Wichtig: Broadcasts überqueren **keine Router**. Wake on LAN funktioniert deshalb nur **innerhalb desselben Netzsegments**. Wer über Segmentgrenzen hinweg wecken will, braucht auf dem Router ein *Directed Broadcast Forwarding* oder ein WoL-Relais im Zielsegment — beides ist Sache der Netzkonfiguration und nicht der Toolbox.

Hinweis: Auch bei WLAN-Geräten geht es in aller Regel nicht: Die WLAN-Verbindung ist im Standby abgebaut, und nur wenige Karten beherrschen den Nachfolger *Wake on Wireless LAN*.

17.4 Wenn das Gerät antwortet, aber die Meldung ausbleibt

Das Warten endet nach 60 Sekunden. Manche Geräte brauchen länger — besonders solche mit Festplatte statt SSD oder mit langer BIOS-Prüfung. Eine Zeitüberschreitung heißt also nicht sicher, dass das Wecken fehlschlug: Prüfen Sie danach noch einmal mit *IP Werkzeuge* ▸ *ICMP (Ping)* nach.

18 Dokumentation erstellen

💻 **Menü:** *System & LAN* ▸ *Dokumentation Erstellen* · 🔑 **Rechte:** Standardbenutzer für den Netzwerkteil; **Domänenbenutzer mit Leserechten** für den Active-Directory-Teil

Erzeugt auf Knopfdruck einen Bericht über Netz und Verzeichnisdienst — als HTML-Datei mit Drucklayout, die sich in jedem Browser öffnen und als PDF ausgeben lässt.

Das ist die Antwort auf die Frage, die alle zwei Jahre kommt: *„Gibt es eine aktuelle Dokumentation der IT?"* Sie ersetzt keine gepflegte Dokumentation — aber sie ist in einer Minute erstellt und stimmt zum Zeitpunkt ihrer Erstellung.

18.1 Inhalte auswählen

Fünf Bausteine lassen sich einzeln zuschalten:

Active Directory

Baustein	Inhalt
Domänen-Basis & FSMO Rollen	Domänenname, Gesamtstruktur, Domain Controller, Inhaber der fünf Betriebsmasterrollen
Grafischer OU-Strukturbaum	Die Organisationseinheiten als Baum
Berechtigungsmatrix (Admin-Gruppen)	Wer in den privilegierten Gruppen steht

System & Netzwerk

Baustein	Inhalt
Lokale IP, DNS & DHCP Konfiguration	Die Netzeinstellungen dieses Rechners
Netzwerkkarten & IP-Bereiche	Die Schnittstellen mit ihren Adressbereichen

18.2 Einen Bericht erzeugen

1. Setzen Sie die Haken bei den gewünschten Bausteinen.
2. Klicken Sie auf *Dokumentation erstellen*.
3. Unter *Status-Protokoll* läuft mit, was gerade erhoben wird — und was dabei nicht klappt.

✅ **Ergebnis:** Eine Datei `IT_Doc_JJJJMMTT_HHMMSS.html` im eingestellten Ordner. Sie wird anschließend im Standardbrowser geöffnet.

Hinweis: Der Dateiname trägt Datum und Uhrzeit. Zwei Berichte überschreiben sich also nie — was praktisch ist, um zwei Stände nebeneinanderzulegen, und unpraktisch, wenn niemand den Ordner aufräumt.

18.3 Speicherort, Logo und E-Mail

Drei Dinge werden **nicht hier**, sondern in den Einstellungen festgelegt (*Einstellungen ▸ Automatisierte Dokumentation*):

Einstellung	Wirkung
Standard-Speicherordner	Wohin die Datei geschrieben wird. Vorgabe ist der Desktop.
Pfad zum eigenen Firmenlogo (PNG/JPG)	Wird oben in den Bericht eingebettet. Ohne Logo steht dort schlicht *Ordivis Toolbox IT Report*.
E-Mail Adresse für Sofort-Versand (Optional)	Ist sie gesetzt, öffnet die Toolbox nach dem Erstellen eine vorbereitete E-Mail im Standard-Mailprogramm.

Hinweis: Das Logo wird **in die Datei eingebettet** (als Daten-URI). Der Bericht bleibt dadurch eine einzelne Datei ohne Anhänge — man kann ihn weitergeben, ohne an Bilddateien zu denken. Ist das Logo nicht lesbar, steht das im Status-Protokoll und der Bericht entsteht trotzdem.

Wichtig: Die vorbereitete E-Mail enthält **keinen Anhang**. Der Sofort-Versand öffnet nur eine Nachricht mit Betreff und Text; die HTML-Datei müssen Sie selbst anhängen. Das liegt daran, dass Windows über `mailto:` keine Dateien anhängen kann.

18.4 Als PDF ausgeben

⚙ **Außerhalb:** Der Ausdruck geschieht im Browser.

Der Bericht bringt ein Drucklayout mit. Öffnen Sie ihn im Browser, drücken Sie Strg + P und wählen Sie als Drucker *Als PDF speichern*.

18.5 Was der Bericht ist — und was nicht

Achtung: Der Bericht enthält die **Struktur Ihres Verzeichnisdienstes und Ihres Netzes**, einschließlich der Mitglieder der Administratorgruppen. Das ist genau die Information, mit der ein Angriff anfängt. Behandeln Sie die Datei entsprechend: nicht im offenen Dateiablagebereich, nicht ungeschützt per E-Mail, nicht auf den Desktop eines Leihgeräts.

Grenze: Der Bericht ist eine **Momentaufnahme dieses Rechners und dieser Domäne**. Er enthält keine Server, keine Anwendungen, keine Verträge, keine Verantwortlichkeiten und keine Historie. Wer eine fortgeschriebene Dokumentation braucht — CMDB, IPAM, Assets, Verträge —, findet sie in **Ordivis Platform**; die Toolbox kann ihre Ergebnisse dorthin übergeben (siehe Kapitel *Ergebnisse an Ordivis übergeben*).

19 Ergebnisse an Ordivis übergeben

💻 **Menü:** *Ordivis* · 🔑 **Rechte:** Standardbenutzer; die einzelnen Meldungen brauchen jeweils die Rechte des zugrundeliegenden Werkzeugs

Ordivis Platform ist das ITSM- und ITAM-System desselben Hauses: CMDB, IPAM, Assets, Verträge, Discovery. Die Toolbox steht dort, wo das Netz erreichbar ist — und kann deshalb Dinge sehen, an die ein Server im Rechenzentrum nicht herankommt. Diese Seite ist die Brücke.

Hinweis: Diese Seite ist ein **Angebot**. Ohne eingerichtete Verbindung arbeitet die Toolbox vollständig; es fehlt genau diese eine Menüseite und die Schaltflächen *An Ordivis senden* auf den Werkzeugseiten.

Wichtig: Alles, was hierüber gemeldet wird, landet in Ordivis zunächst als **Fund** — nicht als Bestandsdatensatz. Erst wer es dort bestätigt, macht daraus ein Configuration Item. Nichts wird still aktiv.

19.1 Die Verbindung einrichten

🔑 **Rechte:** Sie brauchen einen **Integrations-Token**. Den stellt eine Administratorin von Ordivis Platform aus unter *Einstellungen* ▸ *Plattform* ▸ *Integrations-Token*.

1. Tragen Sie unter *Ordivis-Adresse (URL)* den Endpunkt ein, etwa `https://ordivis.firma.local:5001`.
2. Fügen Sie unter *Integrations-Token* den Token ein.
3. Klicken Sie auf *Verbindung testen & speichern*.

✅ **Ergebnis:** Der Status wechselt auf *Verbunden (…)*, in Klammern der Name des Mandanten, mit dem der Token verknüpft ist. Prüfen Sie diesen Namen — er ist die Kontrolle, dass Sie an die richtige Stelle melden.

Hinweis: Der Token wird **lokal verschlüsselt** gespeichert, gebunden an dieses Windows-Konto auf diesem Rechner (DPAPI). Er lässt sich nicht wieder anzeigen. Ist bereits einer gespeichert, lassen Sie das Feld beim erneuten Speichern leer — dann bleibt der vorhandene Token unverändert.

Verbindung entfernen löscht Endpunkt und Token.

Achtung: Über diese Verbindung reist ein Token mit **Schreibrecht auf das IPAM**. Die Toolbox prüft das Serverzertifikat deshalb standardmäßig. Nur wenn Ihre Installation ein selbstsigniertes Zertifikat benutzt, darf die Prüfung abgeschaltet werden — und dann bewusst, siehe Administratorhandbuch. Wer sie ohne Grund abschaltet, verschenkt den Token an jeden, der sich in die Verbindung hängt.

19.2 Offline-Zwischenspeicher

Ist Ordivis beim Senden nicht erreichbar, gehen die Daten nicht verloren: Sie werden lokal zwischengespeichert.

- Der Zähler nennt, wie viele Pakete warten.
- *Jetzt synchronisieren* überträgt sie.

Hinweis: Ein erneuter Versand ist **gefahrlos**. Jedes Paket trägt eine Kennung, an der Ordivis erkennt, dass es dieses schon hatte — es entstehen keine Dubletten. Wird ein Paket von Ordivis **abgelehnt** (etwa weil der Token nicht mehr gilt), wandert es *nicht* in den Zwischenspeicher: Ein zweiter Versuch brächte denselben Fehler.

19.3 Was sich melden lässt

19.3.1 Ergebnisse des IP Scanners

💻 **Menü:** *Scanner Werkzeuge* ▸ *IP Scanner* ▸ *An Ordivis senden*

1. Führen Sie einen Scan aus.
2. *An Ordivis senden*.
3. Die Toolbox schlägt ein **Ziel-Subnetz (CIDR)** vor und nennt die Zahl der Online-Hosts. Bestätigen oder anpassen.
4. *Senden*.

✅ **Ergebnis:** *„{n} neu, {m} aktualisiert. Status: …"*. Kannte Ordivis das Subnetz noch nicht, wird es angelegt — das steht dann dabei.

Umgekehrt geht es auch: Über *Aus Ordivis* ▸ *Subnetz wählen* übernehmen Sie einen dort bekannten Adressbereich in die Scanfelder, statt ihn abzutippen.

19.3.2 Unbestätigte Adressen bestätigen

Ordivis führt Scan-Treffer zunächst als **unbestätigt**. Die Toolbox steht im selben Netz und kann nachsehen, ob eine Adresse wirklich benutzt wird.

1. *Unbestätigte laden*.

2. *Prüfen (Ping)* — die Toolbox meldet, wie viele geantwortet haben.
3. *Erreichbare bestätigen*.

> **Wichtig:** Bestätigt wird **ausschließlich, was gerade geantwortet hat**. Eine Adresse, die stumm blieb, bleibt unbestätigt — auch dann, wenn sie belegt ist. Das ist Absicht: Eine Bestätigung soll etwas bedeuten.

19.3.3 DHCP-Bereiche

> 💻 **Menü:** *IP Werkzeuge* ▸ *DHCP Info & Scanner* ▸ *An Ordivis senden*

Überträgt die geladenen DHCP-Bereiche samt Reservierungen. Die Toolbox zeigt vorher eine Vorschau: wie viele Bereiche, wie viele neue Reservierungen, wie viele Dubletten.

19.3.4 Weitere Datenquellen

Vier Meldungen erheben ihre Daten selbst und brauchen keinen vorherigen Werkzeuglauf:

Schaltfläche	Was gemeldet wird
AD-Computer melden	Name, Betriebssystem, DNS-Name, Organisationseinheit und der Verwalter aus `managedBy`
AD-Standort-Subnetze melden	Die den AD-Standorten zugewiesenen Subnetze
Zertifikate melden	Zertifikate aus den Speichern dieses Rechners
DNS-Abgleich durchführen	Vorwärts- und Rückwärtsauflösung für die in Ordivis bekannten Bereiche

Jede Meldung fragt vorher nach und nennt die Zahl der Datensätze und den Mandanten.

> **Wichtig — was ausdrücklich NICHT übertragen wird:**
> - **LAPS-Kennwörter** und **BitLocker-Wiederherstellungsschlüssel**. Sie hängen im AD teils an denselben Computerobjekten. In einem Betriebsdatenbestand haben sie nichts zu suchen. Die Toolbox sagt das auf der Seite auch selbst.
> - **Private Schlüssel** von Zertifikaten. Übertragen werden nur die öffentlichen Merkmale — Aussteller, Inhaber, Gültigkeit, Fingerabdruck.
> - **Stammzertifizierungsstellen.** Deren mehrere Hundert Einträge sind Windows-Ausstattung und kein Inventar Ihrer Organisation. Erfasst werden die Speicher, in denen betriebsrelevante Zertifikate liegen.
> - **Deaktivierte Computerkonten.** Ein stillgelegter Rechner ist kein Fund, den jemand als CI übernehmen soll.

Zur Zertifikatsmeldung nennt die Rückmeldung zusätzlich, wie viele Zertifikate **in den nächsten 30 Tagen ablaufen** — das ist meist die eigentlich interessante Zahl.

Hinweis: Der DNS-Abgleich läuft bewusst zweistufig: erst rückwärts (welcher Name behauptet, diese Adresse zu sein?), dann vorwärts (auf welche Adresse zeigt dieser Name wirklich?). Erst wenn beide Richtungen vorliegen, ist ein Widerspruch überhaupt erkennbar — eine Richtung allein sieht immer stimmig aus. Ein Zonentransfer (AXFR) wird nicht versucht: Er ist auf den meisten Servern gesperrt und würde die Funktion dort unbrauchbar machen.

19.3.5 Software und Schwachstellen

💻 **Menü:** *Host- & Systemverwaltung* ▸ *System Inspector*

Nach einer Bestandsaufnahme stehen dort zwei zusätzliche Schaltflächen:

- *Software an Ordivis* — die installierte Software des aufgenommenen Systems.
- *Schwachstellen an Ordivis* — die Befunde des Sicherheits-Checks, als Risiken. Die Toolbox fragt dabei, in welchen **Informationsverbund** die Befunde gehören.

19.3.6 SNMP-Geräte

💻 **Menü:** *Scanner Werkzeuge* ▸ *SNMP Inspector* ▸ *Gerät an Ordivis*

Meldet das zuletzt abgefragte Gerät mit den ausgelesenen Systemangaben.

19.4 Wenn etwas nicht geht

Meldung	Bedeutung
„Ordivis-Verbindung ist nicht eingerichtet…"	Adresse und Token fehlen — zuerst unter *Ordivis* eintragen
„Keine Online-Hosts im Ergebnis…"	Erst scannen, dann senden
„Ordivis kennt für diesen Mandanten noch keine Subnetze."	In Ordivis ist noch kein Bereich angelegt
„Verzeichnis nicht erreichbar…"	Der Rechner ist nicht Mitglied einer Domäne
„Es wurde nichts gefunden, das gemeldet werden könnte."	Die Erhebung lief, lieferte aber nichts
„Offline — zwischengespeichert."	Ordivis war nicht erreichbar; später *Jetzt synchronisieren*
„Von Ordivis abgelehnt."	Der Server hat die Annahme verweigert — meist ein abgelaufener Token

20 Einstellungen

💻 **Menü:** *Einstellungen* (Zahnrad, ganz unten im Navigationsbereich) · 🔑 **Rechte:** Standardbenutzer

Alle Einstellungen gelten für **den angemeldeten Windows-Benutzer auf diesem Rechner**. Sie werden sofort wirksam; einen Neustart braucht keine von ihnen.

20.1 Erscheinungsbild

Drei Farbschemata:

Auswahl	Wirkung
Systemstandard verwenden	Folgt der Einstellung von Windows und wechselt mit
Helles Design (Light)	Immer hell
Dunkles Design (Dark)	Immer dunkel

Die Änderung wird sofort übernommen — auch die Fensterleiste passt sich an.

20.2 Sprache / Language

Deutsch oder Englisch. Die Oberfläche wechselt unmittelbar, ohne Neustart und ohne dass eine laufende Messung abbricht.

20.3 Live-Updates & Dashboard

Ein Schieberegler von **200 bis 5000 Millisekunden**, in Schritten von 100 ms. Vorgabe ist **1000 ms**.

Der Wert bestimmt den Takt für *Dashboard*, *Verbindungen* (bei eingeschaltetem Auto-Refresh) und *Topologie*.

Tipp: Unter 500 ms wird es auf Rechnern mit vielen offenen Verbindungen spürbar zäh — die Prozessliste wird bei jedem Durchlauf vollständig neu aufgelöst. 1000 bis 2000 ms sind der brauchbare Bereich; 200 ms lohnen nur, um ein kurzes Ereignis zu erwischen.

20.4 Daten-Einheiten

Wie Netzwerkdurchsatz dargestellt wird:

Auswahl	Wirkung
Automatisch (Auto)	Je Wert die passende Einheit (B, KB, MB, GB, TB)

Auswahl	Wirkung
Kilobyte (KB)	Alles in KB
Megabyte (MB)	Alles in MB

Tipp: *Automatisch* liest sich flüssiger, eine feste Einheit vergleicht sich besser. Wer zwei Schnittstellen gegeneinander stellen will, wählt MB.

20.5 Systemverhalten & Berechtigungen

20.5.1 Immer als Administrator ausführen

Startet die Toolbox künftig mit angeforderten Administratorrechten. Bei jedem Start kommt dann die UAC-Rückfrage von Windows.

Nötig für:

- *Pakete (Live)* (der Mitschnitt braucht einen Rohsocket)
- *Service & Process Controller* (Dienste steuern, Prozesse beenden)
- *Windows HOSTS* (Datei speichern)
- *IP Scanner* mit den Nmap-Profilen `-sS` und `-O`
- *AD Diagnose* (`dcdiag`, `repadmin`, RSAT installieren)
- *AD Suche* (BitLocker- und LAPS-Auskunft)
- Vollständige Prozessnamen in *Verbindungen* und auf dem *Dashboard*

Achtung: Die Rückfrage kommt bei **jedem** Start — auch dann, wenn Sie nur einen Hostnamen auflösen wollen. Wer die Toolbox überwiegend für Abfragen benutzt, lässt die Einstellung besser aus und startet sie im Bedarfsfall gezielt erhöht (Rechtsklick auf die Verknüpfung ▸ *Als Administrator ausführen*).

Hinweis: Wird die UAC-Rückfrage verneint, startet die Toolbox trotzdem — dann eben ohne erhöhte Rechte. Sie bleibt nicht stehen und meldet nichts.

20.6 Active Directory Administrator-Konto

Wenn Ihr angemeldetes Windows-Konto keine Schreibrechte im Verzeichnis hat, hinterlegen Sie hier ein Konto, das sie hat.

1. Tragen Sie *Domäne* (etwa `contoso.local`), *Benutzername* und *Kennwort* ein.
2. *Verbindung testen* prüft die Angaben gegen die Domäne.
3. *Speichern*.

✅ **Ergebnis:** *„Zugangsdaten OK!"* beim Test, *„Gespeichert!"* beim Speichern. Bei *„Fehler (Falsche Daten oder Domäne)"* stimmt eines von beidem nicht.

Dieses Konto wird verwendet von:

- *AD Benutzer-Manager* — für alle schreibenden Aktionen
- *AD Diagnose* — für den FSMO-Transfer
- *AD Suche* — für BitLocker- und LAPS-Auskunft
- *AD Papierkorb* — für das Wiederherstellen
- *Service & Process Controller* — für entfernte Ziele
- *System Inspector* — sofern kein eigenes Konto angegeben wird

Wichtig: Das Kennwort wird **verschlüsselt** gespeichert, gebunden an dieses Windows-Konto auf diesem Rechner (Windows DPAPI). Es lässt sich nicht wieder anzeigen und auf einem anderen Rechner nicht entschlüsseln.

Achtung: Hinterlegen Sie hier **nicht** das Konto eines Domänen-Administrators, wenn ein Konto mit gezielt delegierten Rechten genügt. Wer Zugriff auf Ihre angemeldete Windows-Sitzung hat, kann mit den hinterlegten Rechten arbeiten — die Toolbox benutzt sie ohne weitere Rückfrage. Welche Rechte je Werkzeug tatsächlich nötig sind, führt das Administratorhandbuch auf.

20.7 Automatisierte Dokumentation

Drei Angaben für das Werkzeug *Dokumentation Erstellen*:

Feld	Bedeutung
Standard-Speicherordner	Wohin der Bericht geschrieben wird. Vorgabe: Desktop.
Pfad zum eigenen Firmenlogo (PNG/JPG)	Wird in den Bericht eingebettet
E-Mail Adresse für Sofort-Versand (Optional)	Ist sie gesetzt, öffnet sich nach dem Erstellen eine vorbereitete Nachricht

20.8 Fußzeile

Ganz unten steht die Programmversion in der Form *Ordivis Toolbox v2026.08.07.001 — Entwickelt von Grams IT*. Dieselbe Nummer steht rechts unten in der Statusleiste des Hauptfensters.

20.9 Wo die Einstellungen liegen

Alle Einstellungen liegen in einer Datei im Benutzerprofil. Wo genau, was darin steht und wie sie sich vorbelegen oder verteilen lässt, steht im **Administratorhandbuch**, Kapitel *Datenablage und Konfiguration*.

Hinweis: Es gibt keine Schaltfläche *Auf Werkseinstellungen zurücksetzen*. Wer alles zurücksetzen will, schließt die Toolbox und löscht die Einstellungsdatei — sie wird beim nächsten Start neu angelegt. Achtung: Damit sind auch das hinterlegte AD-Konto und die Ordivis-Verbindung fort.

21 Wenn etwas nicht funktioniert

Dieses Kapitel ordnet die Fehlerbilder nach dem, was Sie sehen. Für jedes steht die wahrscheinlichste Ursache zuerst.

21.1 Zuerst die drei Fragen

Ehe Sie weiter suchen, klären Sie diese drei — sie erklären zusammen die große Mehrheit aller Fälle:

1. **Läuft die Toolbox als Administrator?** Ohne erhöhte Rechte bleiben Listen unvollständig und Aktionen werden verweigert. Prüfen: *Service & Process Controller* öffnen — fehlen die Rechte, steht dort ein roter Hinweis. Abhilfe: *Einstellungen ▸ Systemverhalten & Berechtigungen ▸ Immer als Administrator ausführen*, oder Rechtsklick auf die Verknüpfung ▸ *Als Administrator ausführen*.
2. **Ist der Rechner Mitglied einer Domäne und erreicht er einen Domain Controller?** Prüfen: *Active Directory ▸ AD Diagnose*. Steht dort *„Keine AD Domäne gefunden"*, brauchen die sechs AD-Werkzeuge gar nicht erst versucht zu werden.
3. **Ist das externe Werkzeug installiert, das die Seite benutzt?** `nmap`, `openssl`, `dcdiag`, `repadmin` und die GPO-Werkzeuge gehören nicht zur Toolbox. Jede betroffene Seite sagt es und bietet die Nachinstallation an.

21.2 Das Programm startet nicht

Beobachtung	Ursache	Abhilfe
Doppelklick, nichts passiert	Die Toolbox läuft bereits — sie startet nur einmal	In der Taskleiste suchen
Ein UAC-Fenster erscheint und danach nichts	*Immer als Administrator* ist an und die Rückfrage wurde verneint	Bestätigen — oder die Einstellung ausschalten
Das Fenster erscheint kurz und verschwindet	Absturz beim Start	Siehe *Absturzprotokoll* unten

21.3 Listen bleiben leer

Werkzeug	Wahrscheinliche Ursache
Verbindungen, Spalte *Prozess* leer	Keine Administratorrechte — Windows nennt fremde Prozesse dann nicht
Service & Process Controller	Keine Administratorrechte, oder WinRM auf dem Ziel nicht aktiv
System Inspector	WinRM auf dem Ziel nicht aktiv, Port 5985/5986 gesperrt oder Konto nicht berechtigt

Werkzeug	Wahrscheinliche Ursache
Windows HOSTS	Die Datei enthält wirklich keine aktiven Einträge — reine Kommentarzeilen werden nicht angezeigt
Gruppenrichtlinien (GPO)	RSAT *Gruppenrichtlinienverwaltung* fehlt
AD Papierkorb	Der Papierkorb ist in der Domäne nicht aktiviert
Dashboard, Raten stehen auf 0	Normal in den ersten ein bis zwei Takten — eine Rate braucht zwei Messungen

21.4 Alles rund um Active Directory schlägt fehl

Meldung	Bedeutung
„Keine AD Domäne gefunden (oder keine Berechtigung)."	Kein Domänenmitglied, oder kein DC erreichbar
„Zugriff verweigert. AD-Admin-Zugangsdaten in den Einstellungen prüfen."	Das verwendete Konto darf das nicht
„Fehlende AD-Berechtigungen (Zugriff verweigert)"	Dasselbe, beim Schreiben von Attributen
„DCDIAG Tool fehlt" / „RSAT … nicht installiert"	RSAT nachinstallieren unter *AD Diagnose*
„Befehl wurde ausgeführt, aber keine Rückgabe erhalten"	`repadmin` lief ohne Administratorrechte
Keine BitLocker- oder LAPS-Daten	Entweder gibt es keine — oder Ihnen fehlt das Leserecht darauf

Der Reihe nach: erst prüfen, ob die Domäne überhaupt erreichbar ist (*AD Diagnose*), dann ein berechtigtes Konto unter *Einstellungen* ▸ *Active Directory Administrator-Konto* hinterlegen, dann erneut versuchen.

21.5 Nichts antwortet im Netz

Beobachtung	Ursache
ICMP (Ping): durchweg Zeitüberschreitung	Das Ziel beantwortet ICMP nicht — viele Systeme und fast alle Firewalls tun das nicht. Prüfen Sie stattdessen einen TCP-Port mit dem *IP Scanner*.
IP Scanner: alles grau	Falscher Adressbereich, oder die lokale Firewall blockt ausgehend. *Lokales Subnetz laden* verwenden.
DHCP Scanner: *„Keine DHCPOFFER Antworten"*	Kein DHCP-Server in diesem Segment, oder das DHCP-Relay leitet nicht weiter
SNMP Inspector: *„SNMP-Port (UDP 161) ist geschlossen"*	Das Gerät lebt, SNMP ist dort aus oder gefiltert
SNMP Inspector: *„Falsche Community / Version"*	Community oder Version passen nicht — v3 wird nicht vollständig unterstützt

Beobachtung	Ursache
Wake on LAN: Zeitüberschreitung	Siehe die Voraussetzungsliste im Kapitel *Wake on LAN*
Trace (MTR): Verlust an einem mittleren Sprung	Meist harmlos — viele Router beantworten TTL-Abläufe nicht

21.6 Karten und Standortangaben fehlen

Betroffen sind *DNS Werkzeuge* ▸ *Basis Scanner*, *Zone Lookup* und die Karte in *Trace (MTR)*.

Ursache	Erkennungsmerkmal
Kein ausgehender HTTPS-Zugang	Auch der *Speedtest* und der *Sicherheits-Check* scheitern
Die WebView2-Komponente ist nicht bereit	Die übrigen Ergebnisse der Seite stehen vollständig da, nur die Karte bleibt leer
Private IP-Adresse	Beabsichtigt: Private Adressen werden nie an einen Dienst im Internet übertragen

Hinweis: Eine fehlende Karte ist nie ein Grund, dem übrigen Ergebnis zu misstrauen — DNS-Auflösung, Portprüfung und Zertifikatsanalyse laufen unabhängig davon.

21.7 Ein externes Werkzeug lässt sich nicht installieren

Werkzeug	Bezugsweg	Häufigste Hürde
RSAT	Windows Features on Demand	Der lokale WSUS blockt den Bezug
Nmap	Download von `nmap.org`	Kein Internetzugang; das Setup verlangt Bedienung
OpenSSL	Winget	Winget fehlt oder der Bezug ist gesperrt

In allen drei Fällen bleibt der Weg, das Werkzeug auf dem üblichen Weg Ihrer Organisation zu beziehen und zu installieren — die Toolbox findet es danach von selbst.

21.8 Das Absturzprotokoll

Stürzt die Toolbox ab, schreibt sie eine lesbare Spur in eine Datei `crash.log` in ihrem Datenordner im Benutzerprofil. Die Datei wächst nicht unbegrenzt: Bei mehr als einem Megabyte fängt sie von vorn an.

Daneben liegt `karte.log` — dort steht, warum eine Kartenansicht nicht erschienen ist.

Tipp: Bevor Sie ein Problem melden, halten Sie drei Angaben bereit: die Programmversion (Statusleiste unten rechts), das betroffene Werkzeug und die Meldung im Wortlaut. Wenn es einen Absturz gab, legen Sie die letzten Zeilen aus `crash.log` dazu. Wo die Dateien genau liegen, steht im **Administratorhandbuch**, Kapitel *Protokolle und Fehlersuche*.

21.9 Hilfe bekommen

- Handbücher und weitere Unterlagen: https://ordivis.eu/dokumentation.html
- Kontakt: https://ordivis.eu/kontakt.html
- Änderungen je Version: https://ordivis.eu/toolbox/changelog.html

22 Anhang

22.1 Alle Werkzeuge auf einen Blick

Die Übersicht nennt zu jedem Werkzeug den Menüpfad und die Rechte, die es mindestens braucht.

Werkzeug	Menüpfad	Mindestens nötig
Dashboard	*Dashboard*	Standardbenutzer
Verbindungen	*Verbindungen*	Standardbenutzer (Prozessnamen: Administrator)
Paket-Mitschnitt (IPv4)	*Pakete (Live)*	**Lokaler Administrator**
Topologie	*Topologie*	Standardbenutzer
System Inspector	*Werkzeug-Suiten* ▸ *Host- & Systemverwaltung* ▸ *System Inspector*	Administrator bzw. WinRM-Recht
Service & Process Controller	… ▸ *Host- & Systemverwaltung* ▸ *Service & Process Controller*	Administrator
Windows HOSTS	… ▸ *Host- & Systemverwaltung* ▸ *Windows HOSTS*	Standardbenutzer / Administrator zum Ändern
AD Diagnose	… ▸ *Active Directory* ▸ *AD Diagnose*	Domänenbenutzer / mehr je Aktion
AD Explorer	… ▸ *Active Directory* ▸ *AD Explorer*	Domänenbenutzer
AD Suche	… ▸ *Active Directory* ▸ *AD Suche*	Domänenbenutzer / mehr für LAPS & BitLocker
AD Benutzer-Manager	… ▸ *Active Directory* ▸ *AD Benutzer-Manager*	Domänenbenutzer / Schreibrecht zum Ändern
Gruppenrichtlinien (GPO)	… ▸ *Active Directory* ▸ *Gruppenrichtlinien (GPO) Verwaltung*	Domänenbenutzer + RSAT
AD Papierkorb	… ▸ *Active Directory* ▸ *AD Papierkorb*	Recht zum Wiederherstellen
Lokale Zertifikate (PKI)	… ▸ *CA & PKI* ▸ *Lokale Zertifikate (PKI)*	Standardbenutzer
Zertifikats-Wizard	… ▸ *CA & PKI* ▸ *Zertifikats-Wizard (ACME/CA)*	Standardbenutzer / CA-Recht für AD CS
OpenSSL Converter	… ▸ *CA & PKI* ▸ *OpenSSL Converter*	Standardbenutzer + OpenSSL
ARP Tabelle	… ▸ *IP Werkzeuge* ▸ *ARP Tabelle*	Standardbenutzer
DHCP Info & Scanner	… ▸ *IP Werkzeuge* ▸ *DHCP Info & Scanner*	Standardbenutzer / Administrator zum Erneuern
ICMP (Ping)	… ▸ *IP Werkzeuge* ▸ *ICMP (Ping)*	Standardbenutzer

Werkzeug	Menüpfad	Mindestens nötig
Speedtest	… ▸ *IP Werkzeuge* ▸ *Speedtest*	Standardbenutzer + Internet
Subnetz Rechner	… ▸ *IP Werkzeuge* ▸ *Subnetz Rechner*	Standardbenutzer
Trace (MTR)	… ▸ *IP Werkzeuge* ▸ *Trace (MTR)*	Standardbenutzer
WHOIS Abfrage	… ▸ *IP Werkzeuge* ▸ *WHOIS Abfrage*	Standardbenutzer + Internet
IP Scanner	… ▸ *Scanner Werkzeuge* ▸ *IP Scanner*	Standardbenutzer / Administrator für `-sS` / `-O`
MAC Scanner	… ▸ *Scanner Werkzeuge* ▸ *MAC Scanner*	Standardbenutzer
SNMP Inspector	… ▸ *Scanner Werkzeuge* ▸ *SNMP Inspector*	Standardbenutzer
Basis Scanner (DNS)	… ▸ *DNS Werkzeuge* ▸ *Basis Scanner*	Standardbenutzer
Zone Lookup	… ▸ *DNS Werkzeuge* ▸ *Zone Lookup*	Standardbenutzer
Remote Manager	… ▸ *Remote Werkzeuge* ▸ *Remote Manager*	Standardbenutzer
E-Mail Header Analyse	… ▸ *E-Mail Werkzeuge* ▸ *E-Mail Header Analyse*	Standardbenutzer
SMTP Diagnose	… ▸ *E-Mail Werkzeuge* ▸ *SMTP Diagnose*	Standardbenutzer
NTP & Zeitzonen	*System & LAN* ▸ *NTP & Zeitzonen*	Standardbenutzer / Administrator zum Setzen
Wake on LAN	*System & LAN* ▸ *Wake on LAN*	Standardbenutzer
Dokumentation Erstellen	*System & LAN* ▸ *Dokumentation Erstellen*	Standardbenutzer / Domänenbenutzer für den AD-Teil
Ordivis-Verbindung	*Ordivis*	Standardbenutzer + Integrations-Token
Einstellungen	*Einstellungen*	Standardbenutzer

22.2 Welches Werkzeug für welche Frage

Frage	Werkzeug
Wer benutzt hier gerade die Leitung?	Dashboard, Verbindungen
Welches Programm spricht mit dieser Adresse?	Verbindungen
Wer ist in diesem Subnetz erreichbar?	IP Scanner
Welche Ports hat dieser Rechner offen?	IP Scanner, Basis Scanner
Ist das Gerät wirklich aus?	ICMP (Ping), dann IP Scanner mit Ports
Wo geht der Verkehr verloren?	Trace (MTR)

Frage	Werkzeug
Geht das Paket überhaupt raus, kommt eine Antwort?	Paket-Mitschnitt (IPv4)
Wie schnell ist die Leitung?	Speedtest
Welches Gerät steckt hinter dieser MAC-Adresse?	MAC Scanner
Verteilt hier ein fremder DHCP-Server Adressen?	DHCP Info & Scanner
Wie ist dieses Netz aufgeteilt?	Subnetz Rechner
Warum löst dieser Name falsch auf?	Basis Scanner, Windows HOSTS
Welche DNS-Einträge hat diese Domain?	Basis Scanner, Zone Lookup
Wann läuft das Zertifikat ab?	Basis Scanner
Passt dieser Schlüssel zu diesem Zertifikat?	Lokale Zertifikate (PKI)
Wie bekomme ich ein Zertifikat von der internen CA?	Zertifikats-Wizard
Wie mache ich aus PEM eine PFX-Datei?	OpenSSL Converter
Warum kommt diese E-Mail nicht an?	SMTP Diagnose
Ist diese E-Mail echt?	E-Mail Header Analyse
Wem gehört diese Domain / dieser Adressblock?	WHOIS Abfrage
Warum kann sich niemand anmelden?	AD Diagnose, NTP & Zeitzonen
Warum greift diese Gruppenrichtlinie nicht?	Gruppenrichtlinien (GPO) Verwaltung
Warum kommt diese Person an diese Freigabe?	AD Suche (Mitgliedschaften mit Vererbung)
Wie stelle ich das gelöschte Konto wieder her?	AD Papierkorb
Was läuft auf diesem Server?	System Inspector
Wie starte ich den Dienst auf dem Server neu?	Service & Process Controller
Was steht in diesem Switch?	SNMP Inspector
Wie wecke ich den Rechner?	Wake on LAN

22.3 Ausgehende Verbindungen

Die Toolbox arbeitet überwiegend in Ihrem Netz. Diese Werkzeuge sprechen mit Diensten im Internet — und nur diese:

Werkzeug	Ziel	Was übertragen wird
Dashboard	`1.1.1.1` (ICMP)	Nichts außer dem Ping selbst
Speedtest	`speedtestx.de`, `speed.hetzner.de`, `ash-speed.hetzner.com`	Nichts — es wird nur geladen

Werkzeug	Ziel	Was übertragen wird
Basis Scanner, Trace (MTR)	`ip-api.com`	Die abgefragte **öffentliche** IP-Adresse
Zone Lookup	`api.bgpview.io`, `ip-api.com`	Die abgefragte **öffentliche** IP-Adresse
Kartenansichten	`openstreetmap.org`, `unpkg.com`	Die anzuzeigenden Koordinaten
MAC Scanner (manuelle Suche)	`api.macvendors.com`	Die eingegebene MAC-Adresse
System Inspector, Sicherheits-Check	`cve.circl.lu`	Hersteller- und Produktnamen der installierten Software
WHOIS Abfrage	Der gewählte WHOIS-Server, `rdap.arin.net`	Die eingegebene Domain oder IP-Adresse
IP Scanner (Nachinstallation)	`nmap.org`	Nichts — es wird nur geladen
OpenSSL (Nachinstallation)	Winget-Quellen	Nichts — es wird nur geladen
AD Diagnose (RSAT)	Windows Update	Nichts — es wird nur geladen

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 Verbindung zu **Ordivis Platform** geht an den von Ihnen eingetragenen Endpunkt — in aller Regel ein Server im eigenen Netz. Was dabei übertragen wird, steht im Kapitel *Ergebnisse an Ordivis übergeben*.

22.4 Glossar

ACME — Automatisiertes Verfahren, mit dem Zertifizierungsstellen wie Let's Encrypt Zertifikate ausstellen.

ARP — Address Resolution Protocol. Übersetzt IP-Adressen in MAC-Adressen innerhalb eines Netzsegments.

ASN — Autonomous System Number. Kennzeichnet den Netzbetreiber, dem ein Adressbereich gehört.

AXFR — Zonentransfer. Die vollständige Übertragung einer DNS-Zone; auf den meisten Servern gesperrt.

BitLocker — Windows-Festplattenverschlüsselung. Der Wiederherstellungsschlüssel kann im Active Directory hinterlegt werden.

CIDR — Schreibweise für Netzbereiche, etwa `192.168.1.0/24`.

CIM / WS-Management — Nachfolger von WMI/DCOM zur Systemabfrage über das Netz. Setzt WinRM voraus.

CSR — Certificate Signing Request. Die Zertifikatsanforderung, die eine Zertifizierungsstelle unterschreibt.

CVE — Common Vulnerabilities and Exposures. Weltweit einheitliche Kennung einer bekannten Schwachstelle.

DCDIAG — Microsoft-Werkzeug zur Prüfung von Domain Controllern.

DHCP — Vergibt IP-Adressen automatisch. Ein *Rogue DHCP* ist ein nicht autorisierter Server, der ebenfalls Adressen verteilt.

DKIM — Signaturverfahren für E-Mail. Der *Selektor* bestimmt, unter welchem DNS-Namen der öffentliche Schlüssel steht.

DMARC — Richtlinie einer Domain dazu, wie mit Mails umzugehen ist, die SPF und DKIM nicht bestehen.

DPAPI — Windows-Verfahren, das Geheimnisse an Benutzerkonto und Rechner bindet. Die Toolbox schützt damit gespeicherte Kennwörter und Token.

DF-Bit — *Don't Fragment*. Verbietet Routern das Zerlegen eines Pakets; dient dem Auffinden der MTU.

FSMO — Die fünf Betriebsmasterrollen im Active Directory: Schema Master, Domain Naming, PDC Emulator, RID Pool Manager, Infrastructure.

GPO — Gruppenrichtlinienobjekt.

LAPS — Verwaltet lokale Administratorkennwörter und hinterlegt sie im Active Directory.

Magic Packet — Das Weckpaket bei Wake on LAN.

MTR — Verbindet Traceroute und Ping: misst jeden Sprung dauerhaft.

MTU — Maximum Transmission Unit. Die größte Paketgröße, die eine Strecke ohne Zerlegen trägt.

OUI — Die ersten drei Byte einer MAC-Adresse; identifiziert den Hersteller.

Rohsocket / SIO_RCVALL — Der Weg, auf dem Windows einem Programm den gesamten IPv4-Verkehr einer Schnittstelle überlässt. Setzt Administratorrechte voraus und sieht nichts unterhalb von IP.

PEM / DER / PFX — Formate für Zertifikate. PEM ist Text, DER binär, PFX ein Archiv aus Zertifikat und privatem Schlüssel.

PTR — Der DNS-Eintrag für die Rückwärtsauflösung einer IP-Adresse.

RDAP — Moderne Nachfolgeschnittstelle von WHOIS; antwortet strukturiert in JSON.

RSAT — Remote Server Administration Tools. Die Verwaltungswerkzeuge von Windows Server für den Arbeitsplatz.

RSOP — Resultant Set of Policy. Die Richtlinien, die auf einem Rechner tatsächlich ankommen.

SNMP — Abfrageprotokoll für Netzkomponenten. Die *Community* ist bei v1 und v2c das Kennwort und geht im Klartext über das Netz.

SPF — Legt im DNS fest, welche Server für eine Domain Post versenden dürfen.

UAC — Benutzerkontensteuerung. Die Rückfrage von Windows vor einer Handlung mit erhöhten Rechten.

WID — *WID-SEC-…*: Kennung einer Warnmeldung des Bundesamts für Sicherheit in der Informationstechnik.

WinRM — Der Windows-Dienst, über den CIM-Abfragen und PowerShell-Remoting laufen (Port 5985 bzw. 5986).

Wake on LAN — Weckt ein Gerät über ein Netzwerkpaket an seine MAC-Adresse.

22.5 Weiterführende Unterlagen

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