KURZANLEITUNG

OTScan 3 in 15 Minuten

Erster Start, Oberfläche, Schnellscan und Stufenlauf, Ergebnisse, Berichte und Stammdaten – das Wichtigste auf wenigen Seiten.

Version 3.0.0 · Stand 12.11.2026
HanselCraft · otscan.hanselcraft.de

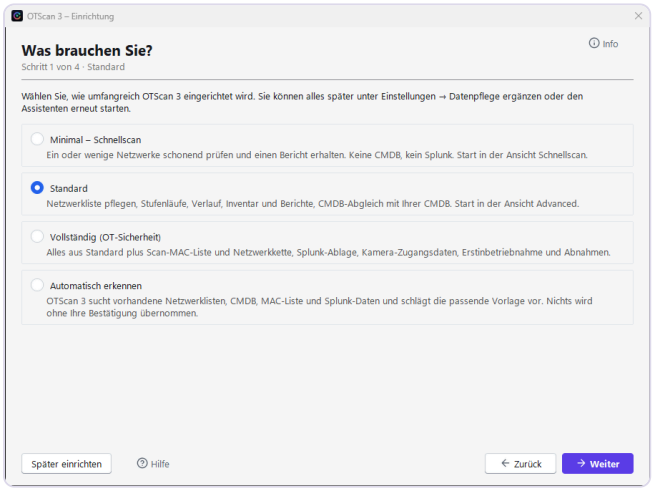
1 Was OTScan 3 macht

OTScan 3 prüft Anlagennetzwerke (OT): Es findet die Geräte, erkennt Hersteller, Modell, Firmware und offene Dienste und bewertet, welche Dienste unsicher sind. Es gleicht die Ergebnisse auf Wunsch mit Firewall-Verkehr (z. B. aus Splunk) und Ihrem Inventar (CMDB) ab und erstellt Berichte für Anlagenverantwortliche, Technik und Management.

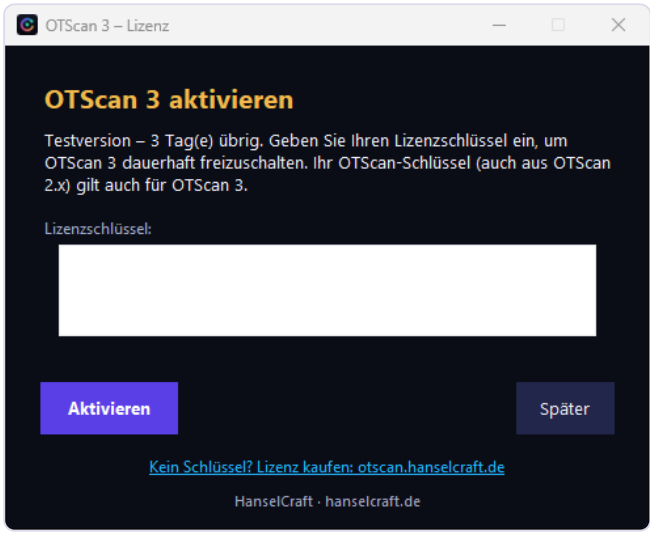
> OTScan 3 liest nur. Es ändert nichts an Geräten, probiert keine Passwörter durch und nutzt keine Angriffs- oder Lasttest-Skripte. Trotzdem ist ein Scan Netzwerkverkehr: Holen Sie vor dem ersten Scan die Freigabe des Anlagenverantwortlichen ein.

2 Erster Start

1. OTScan 3 über das Desktop-Symbol bzw. den Startmenü-Eintrag **OTScan 3** starten (Linux: `/opt/otscan3/otscan3.sh`).
2. Beim ersten Start fragt OTScan 3 nach der Sprache und zeigt das Fenster **OTScan 3 aktivieren**. Lizenzschlüssel eingeben und **Aktivieren** – oder **Später** für die Testversion.
3. Der **Einrichtungsassistent** fragt, was Sie brauchen: *Minimal – Schnellscan*, *Standard*, *Vollständig (OT-Sicherheit)* oder *Automatisch erkennen*. Danach Netzwerke eintragen, optional eine CMDB wählen und **Fertigstellen**.



Einrichtungsassistent: Schritt 1



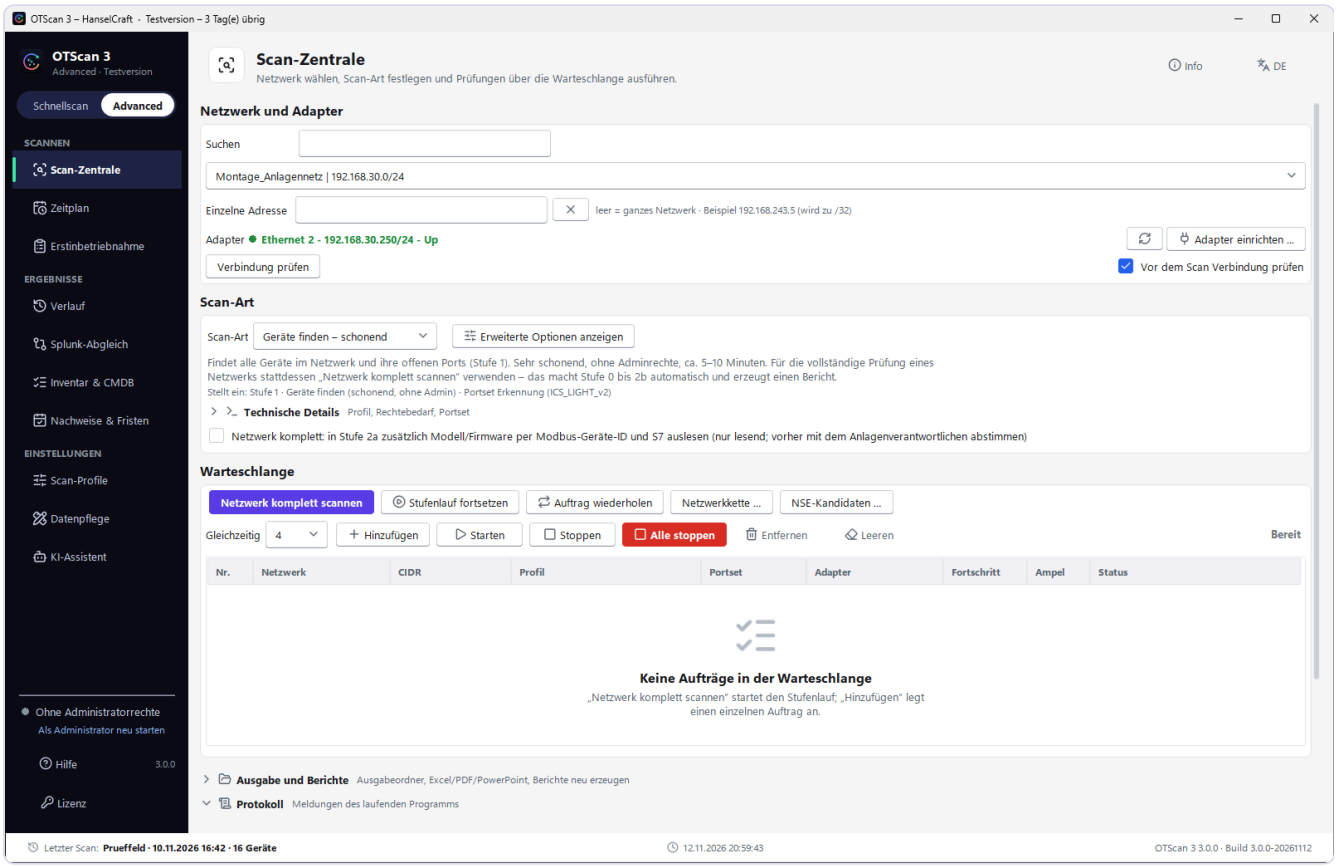
Lizenz aktivieren

3 Die Oberfläche

Oben links schalten Sie zwischen **Schnellscan** (ein Knopf, für alle) und **Advanced** um. Die Seitenleiste von Advanced hat drei Bereiche:

Bereich	Seiten	Wofür
SCANNEN	Scan-Zentrale · Zeitplan · Erstinbetriebnahme	Netzwerk prüfen, Läufe planen, neue Geräte abnehmen
ERGEBNISSE	Verlauf · Splunk-Abgleich · Inventar & CMDB	Läufe ansehen, mit Firewall-Verkehr und Inventar abgleichen
EINSTELLUNGEN	Scan-Profile · Datenpflege	Profile, Netzwerke, Scan-MAC-Liste, CMDB, Hersteller-Regeln

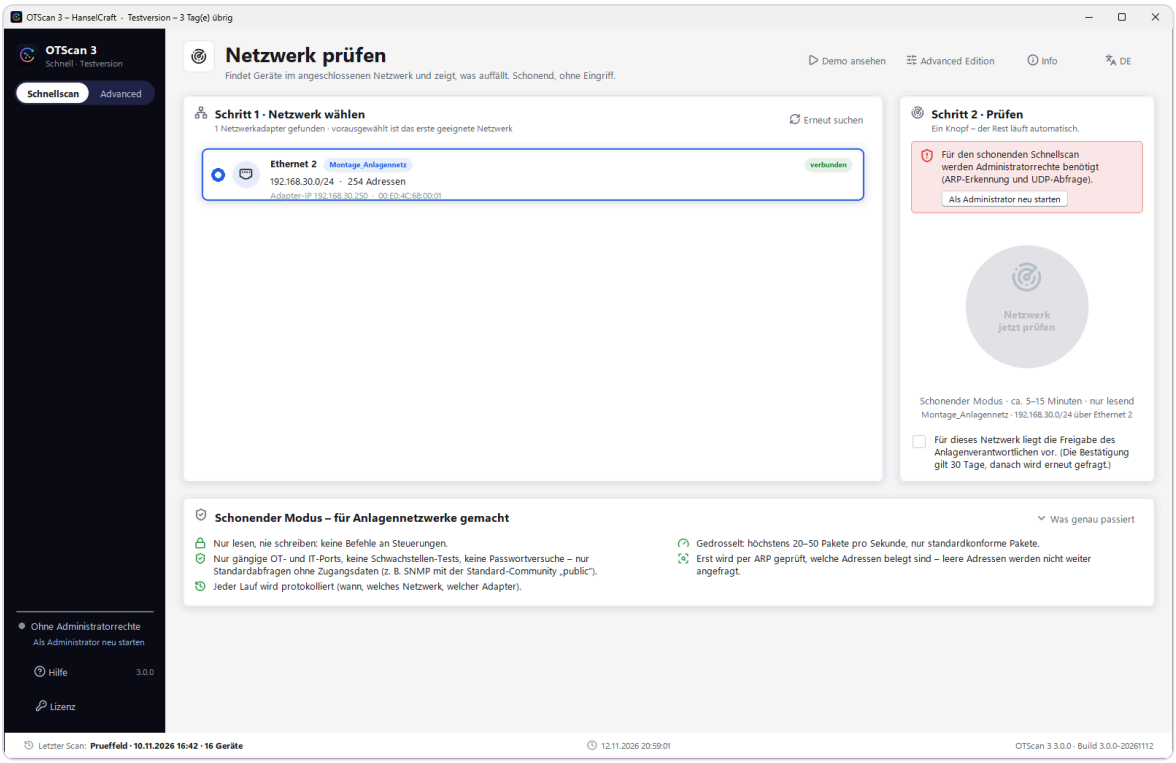
Oben rechts auf jeder Seite: **Info** (Schritt-für-Schritt-Hilfe, auch mit F1) und der Sprachknopf. Unten links stehen Administratorrechte, **Hilfe** und **Lizenz**; die Fußzeile zeigt den letzten Scan und die Version.



Advanced → SCANNEN → Scan-Zentrale

4 Netzwerk schnell prüfen (Schnellscan)

1. Oben links **Schnellscan** wählen.
2. Netzwerk wählen (der Adapter muss im Zielnetzwerk stecken) und die Freigabe bestätigen.
3. Scan starten. Nach einigen Minuten erscheinen Ampel und Ergebnis; die Knöpfe öffnen PDF, Excel und Kurzbericht.



Schnellscan

5 Netzwerk vollständig prüfen (Stufenlauf)

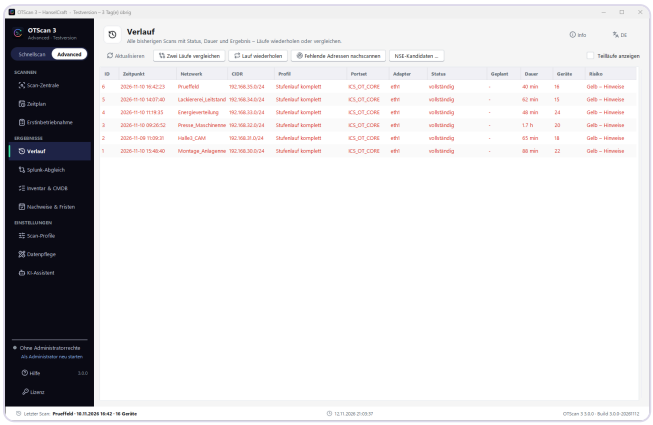
1. Advanced → SCANNEN → **Scan-Zentrale**. Unter „Netzwerk und Adapter" das Netzwerk suchen und wählen.
2. Adapter prüfen (grün = bereit). Falls nötig **Adapter einrichten …** – feste Scan-IP ohne Standard-Gateway, auf Wunsch mit Scan-MAC.
3. **Netzwerk komplett scannen** drücken und die Rückfrage (Netzwerk, Stufen, geschätzte Dauer) bestätigen.
4. Die Stufen laufen nacheinander: Stufe 0 (wer ist da?), Stufe 1 (Geräte und Ports), Stufe 2a (Dienste und Versionen), Stufe 2b (UDP-Namen), Nachscan, in CAM-Netzwerken die Kameraabfrage. **Stoppen** hält an, **Stufenlauf fortsetzen** macht weiter.
5. Am Ende entstehen die Berichte im Ausgabeordner (Standard: Dokumente).

> Mehrere Netzwerke nacheinander über einen Adapter: **Netzwerkkette …**. Wiederkehrende Scans: Seite **Zeitplan** → **Geplanten Scan anlegen**.

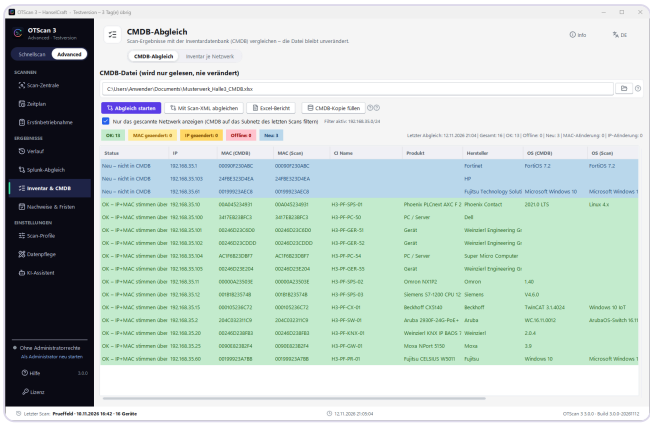
6 Ergebnisse ansehen

- **Verlauf**: alle Läufe mit Status, Dauer, Geräten und Ampel; **Zwei Läufe vergleichen**, **Lauf wiederholen**.
- **Splunk-Abgleich**: Firewall-Export mit **Export übernehmen …** einlesen, dann je Netzwerk **Abgleichen**. Geräte, die nur im Verkehr auftauchen, kommen in den CMDB-Nachtrag.

- **Inventar & CMDB**: CMDB-Datei wählen, **Abgleich starten**. Grün = stimmt, rot = nicht im Scan, blau = neu.



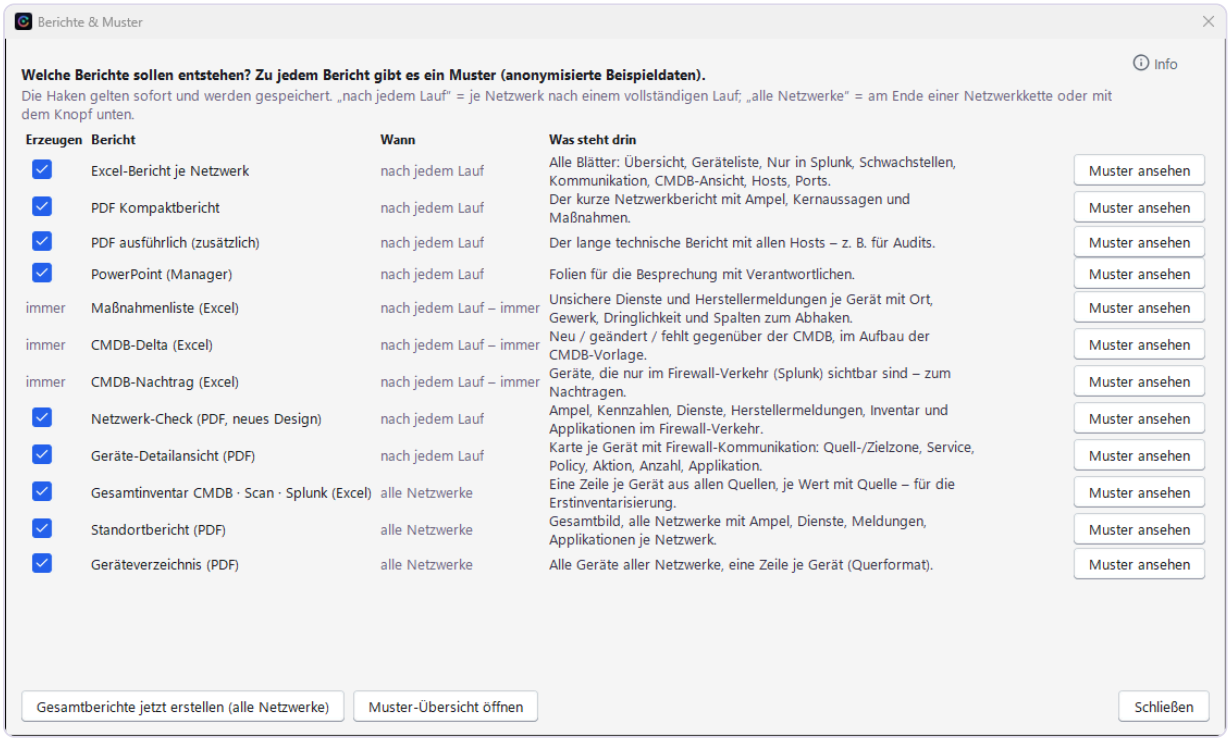
Verlauf



CMDB-Abgleich

7 Berichte

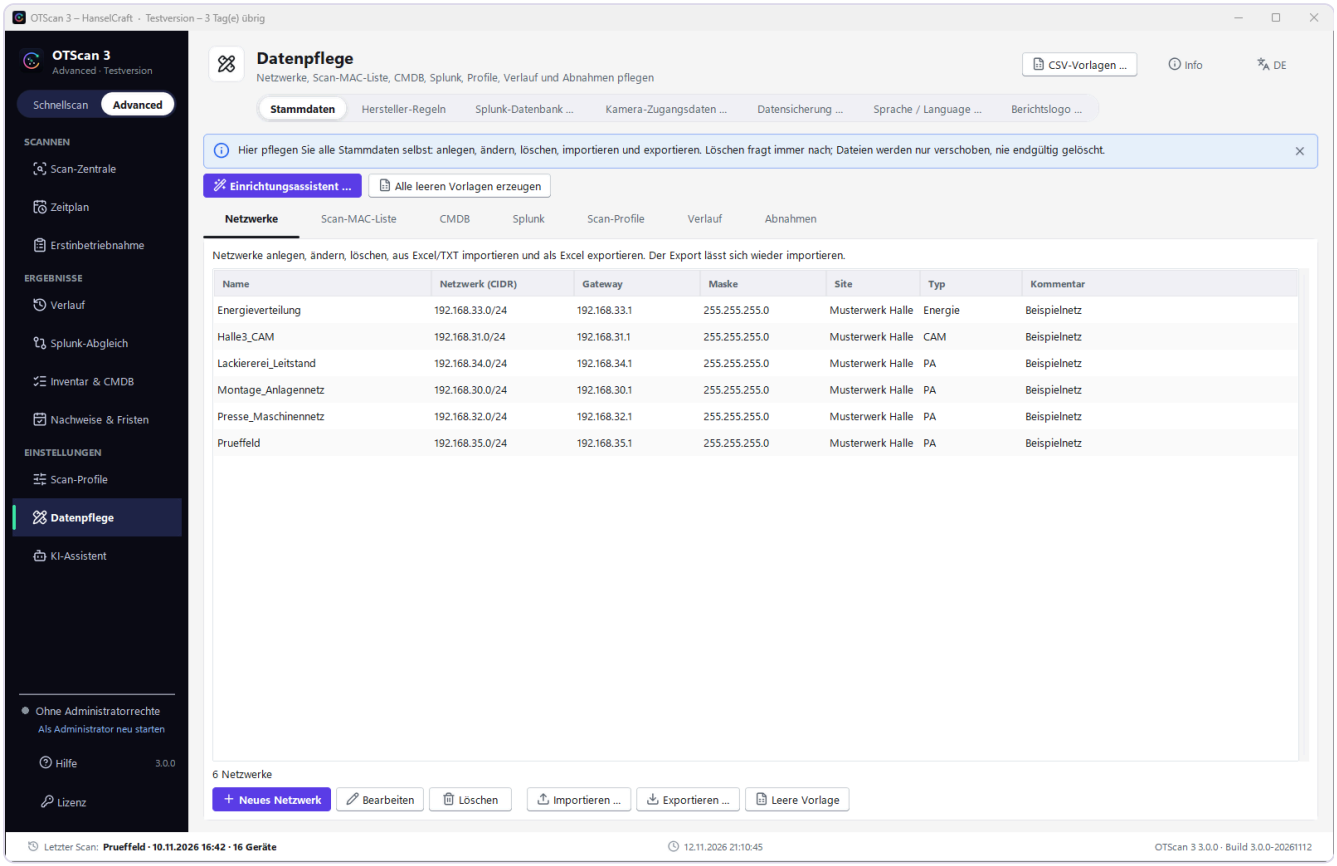
Unter „Ausgabe und Berichte“ (Scan-Zentrale) setzen Sie die Haken für Excel, PDF und PowerPoint. **Berichte & Muster …** zeigt alle Berichtsarten mit Haken und **Muster ansehen**. Welcher Bericht wofür gedacht ist, steht in *OTScan3_Berichte_lesen.pdf*.



Fenster „Berichte & Muster“

8 Stammdaten pflegen

Advanced → EINSTELLUNGEN → **Datenpflege**: Reiter Netzwerke, Scan-MAC-Liste, CMDB, Splunk, Scan-Profile, Verlauf, Abnahmen; oben außerdem Hersteller-Regeln, Splunk-Datenbank, Kamera-Zugangsdaten, Datensicherung und Sprache. Viele Einträge auf einmal: **CSV-Vorlagen …** – Vorlage herunterladen, in Excel ausfüllen, hochladen; OTScan 3 prüft jede Zeile.



Datenpflege → Stammdaten → Netzwerke

9 Wenn etwas nicht klappt

Meldung / Beobachtung	Was tun
Adapter rot oder gelb	Kabel im Zielnetzwerk? Scan-MAC registriert? **Adapter einrichten …** und **Verbindung prüfen**.
Stufe pausiert „braucht Administratorrechte“	OTScan 3 über das Desktop-Symbol (mit Administratorrechten) starten und **Stufenlauf fortsetzen**.
„nmap gesperrt“	Die Meldung nennt den Grund (z. B. unsichere Profiloption). Info → Thema „Sicherheit mit Administratorrechten“.
HTML statt PDF	Für die neuen PDF-Berichte Microsoft Edge, Google Chrome oder Chromium installieren.
Weniger Geräte als erwartet	Splunk-Abgleich nutzen; Nachscan-Vorschläge übernehmen; Geräte ohne Antwort vor Ort prüfen.

Ausführliche Hilfe: **Info** auf jeder Seite (F1) und das Nutzerhandbuch im Programmordner (`handbuch/index.html`, 7 Sprachen).