ANWENDERHANDBUCH

Anwenderhandbuch

Alles zu OTScan 3 an einem Ort: Installation, Scannen, Ergebnisse, Berichte, Stammdaten und Erstinbetriebnahme – mit Bildern aus dem Musterwerk Halle 3.

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

Inhalt

1 Über dieses Handbuch 4

2 Grundlagen 5

2.1 Überblick und erste Schritte 5

2.2 Installation unter Windows und Einrichtungsassistent 6

2.3 Installation unter Linux 10

2.4 Hilfe im Programm: Info und Handbuch 11

2.5 Sicherheit und Datenschutz 12

2.6 Sicherheit mit Administratorrechten 14

3 Neu in OTScan 3 17

4 Scannen 19

4.1 Schnellscan – Netzwerk prüfen 19

4.2 Scan-Zentrale und Stufenlauf 20

4.3 Netzwerkkette – viele Netzwerke nacheinander 23

4.4 Zeitplan – wiederkehrende Scans 26

4.5 Erstinbetriebnahme und Erstabnahme 27

4.6 Direktanschluss an eine Maschine 30

4.7 Abnahmen 31

5 Ergebnisse 33

5.1 Verlauf 33

5.2 Splunk-Abgleich, Splunk-Ablage und Splunk-Datenbank 34

5.3 CMDB-Abgleich 37

5.4 Inventar je Netzwerk 38

5.5 Herstellermeldungen (CSAF) und Maßnahmenliste 40

5.6 Berichte und Dokumente 42

5.7 Nachweise & Fristen 46

6 Einstellungen 49

6.1 Datenpflege – alle Stammdaten selbst pflegen 49

6.2 Netzwerke anlegen, bearbeiten, importieren 51

6.3 Adapter einrichten und Scan-MAC 53

6.4 CSV-Vorlagen herunterladen, ausfüllen, hochladen 55

6.5 Scan-Profile und Portsets 57

6.6 Hersteller-Regeln 58

6.7 Kameraprofil und Kamera-Zugangsdaten 60

6.8 Datensicherung und Umzug auf einen neuen Rechner 62

6.9 Sprache der Oberfläche / Language 63

6.10 Eigenes Firmenlogo in Berichten 65

6.11 KI-Assistent (Claude Desktop, MCP) 66

7 Berichte und Exporte 69

7.1 PDF-Kompaktbericht 69

7.2 PDF ausführlich 69

7.3 Excel-Bericht je Netzwerk 70

7.4 PowerPoint (Manager) 70
7.5 Maßnahmenliste (Excel) 70
7.6 CMDB-Delta (Excel) 71
7.7 CMDB-Nachtrag (Excel) 71
7.8 Netzwerk-Check (PDF) 72
7.9 Geräte-Detailansicht (PDF) 72
7.10 Gesamtinventar CMDB · Scan · Splunk (Excel) 72
7.11 Standortbericht (PDF) 73
7.12 Geräteverzeichnis (PDF) 73
7.13 Splunk-Abgleich (CSV und Bericht) 74
7.14 Inventar je Netzwerk (HTML/CSV) 74
7.15 Erstinbetriebnahme: Protokoll und Paket 74

8 Nachschlagen 76
8.1 Wie entstehen die Daten? 76
8.2 Prüffragen der Erstinbetriebnahme 76
8.3 Glossar 80
8.4 Häufige Fragen 82

9 Dokumente im Paket und Hilfe 83

1 Über dieses Handbuch

Dieses Handbuch ist die Druckfassung des Nutzerhandbuchs, das OTScan 3 über „Info“ → „Handbuch“ im Browser öffnet (`handbuch/index.html`). Es hat dieselben Kapitel wie die Info-Hilfe im Programm; jedes Kapitel beginnt mit „Wozu?“, dann folgen „So geht's“, „Was trage ich wo ein?“ und Bildschirmfotos.

Herausgegeben von HanselCraft (hanselcraft.de). Bildschirmfotos und Muster stammen aus dem erfundenen „Musterwerk Halle 3“ (Netzwerke Montage_Anlagennetz, Halle3_CAM, Presse_Maschinennetz, Energieverteilung, Lackiererei_Leitstand, Prueffeld; 192.168.30.0/24 bis 192.168.35.0/24). Gerätenamen, Adressen und MAC-Adressen sind Beispiele.

> 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.

Knopf- und Menütexte sind so geschrieben, wie sie im Programm stehen, z. B. **Info** . Version 3.0.0, Stand 12.11.2026.

2 Grundlagen

2.1 Überblick und erste Schritte

Was OTScan 3 ist, wie die Oberfläche aufgebaut ist und wie der erste Scan abläuft.

Wozu?

OTScan 3 ist ein Netzwerkscanner für Anlagennetzwerke (OT). Er findet Geräte, erkennt ihre Dienste und bewertet sie nach anpassbaren Verkehrsregeln (HanselCraft-Voreinstellung, angelehnt an IEC 62443). Es gibt zwei Editionen in einem Programm: den Schnellscan (ein Knopf, für alle Anwender) und die Advanced Edition (Stufenlauf, Netzwerkkette, Abgleiche, Erstinbetriebnahme – für geschulte Anwender). Das Programm läuft unter Windows und unter Linux mit denselben Funktionen. Dieser Bereich ist der Einstieg für neue Anwender.

Achtung

- OTScan 3 liest nur: keine Schreibbefehle, keine Passwortversuche, keine Schwachstellen-Tests. Einzige Zugangsdaten im Standardlauf sind die SNMP-Community „public“ und – in CAM-Netzwerken – ein freiwillig hinterlegter, nur lesender ONVIF-Benutzer.
- Scannen Sie ein Netzwerk nur mit Freigabe des Anlagenverantwortlichen. Ändern oder löschen Sie während eines Laufs keine Dateien und Einstellungen.
- Das Programm sieht nur, was antwortet, und nur auf den geprüften Ports. Ein stummes Gerät fehlt im Ergebnis.
- Alle Daten bleiben auf dem Scan-PC (keine Cloud, keine Telemetrie). Datenbank und Einstellungen liegen in %APPDATA%\OTScan3, Berichte im Ordner Dokumente.

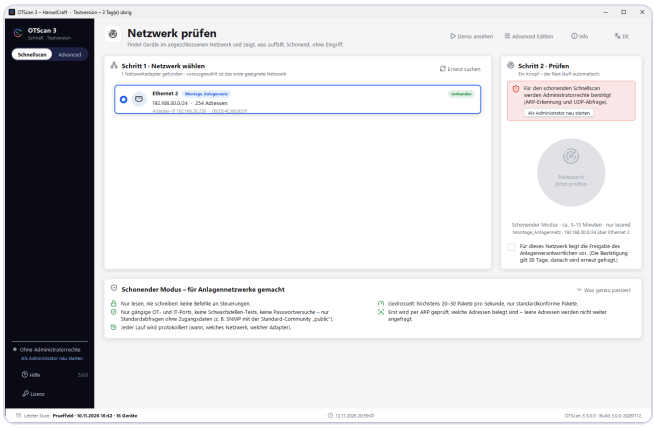
So geht's

1. Programm über das Desktop-Symbol „OTScan 3“ starten und die Abfrage nach Administratorrechten mit „Ja“ bestätigen.
2. Oben links zwischen „Schnellscan“ und „Advanced“ umschalten. OTScan 3 merkt sich Edition und Seite für den nächsten Start.
3. Die Seitenleiste der Advanced Edition hat drei Gruppen: SCANNEN (Scan-Zentrale, Zeitplan, Erstinbetriebnahme), ERGEBNISSE (Verlauf, Splunk-Abgleich, Inventar & CMDB) und EINSTELLUNGEN (Scan-Profile, Datenpflege).
4. Zusammengelegte Bereiche haben oben im Seitenkopf Reiter: Erstinbetriebnahme | Abnahmen, CMDB-Abgleich | Inventar je Netzwerk und in der Datenpflege Stammdaten | Hersteller-Regeln | Splunk-Datenbank … | Kamera-Zugangsdaten ….
5. Auf jeder Seite oben rechts: „Info“ öffnet die Schritt-für-Schritt-Hilfe zur Seite. F1 öffnet ebenfalls die Info.
6. Vor dem ersten Scan: Freigabe des Anlagenverantwortlichen einholen, das Netzwerk in der Datenpflege (Reiter Netzwerke) anlegen oder per CSV-Vorlage importieren und den passenden Adapter einrichten.
7. Ersten Scan starten: im Schnellscan „Netzwerk jetzt prüfen“ oder in der Scan-Zentrale „Netzwerk komplett scannen“.

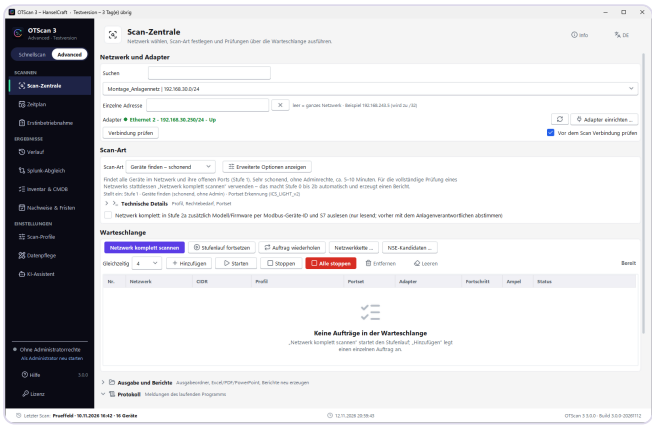
8. Ergebnis lesen: PDF Seite 1 (Ampel, das Wichtigste, was ist zu tun), Excel für Einzelheiten, PowerPoint für Besprechungen. Wo welche Datei liegt, erklärt der Bereich „Berichte und Dokumente“.
9. Unten links steht „Administratorrechte aktiv“, wenn OTScan 3 als Administrator läuft. Ohne Administratorrechte gibt es keinen Schnellscan, kein ARP und keine UDP-Abfragen. Unten rechts steht die Build-Kennung, zum Beispiel „OTScan 3 3.0.0 · Build 3.0.0-20261112“.

Was trage ich wo ein?

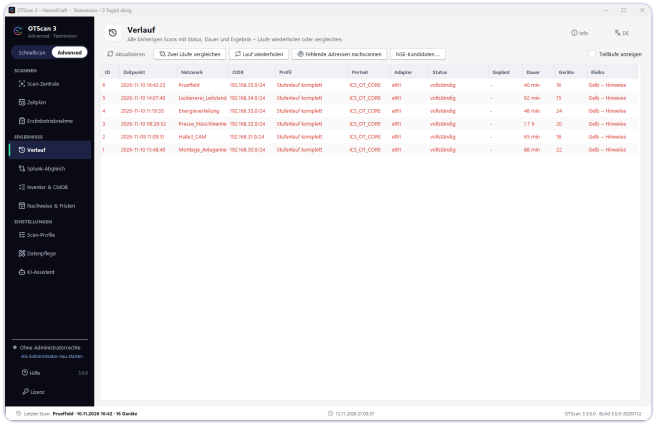
Feld	Bedeutung
Schnellscan | Advanced	Umschalter oben links: einfache Prüfung mit einem Knopf oder die volle Advanced Edition.
Seitenleiste	Auswahl der Seite: SCANNEN, ERGEBNISSE, EINSTELLUNGEN.
Reiter im Seitenkopf	Umschalter zwischen zusammengehörenden Teilen einer Seite, zum Beispiel CMDB-Abgleich und Inventar je Netzwerk.



Überblick und erste Schritte



Überblick und erste Schritte



Überblick und erste Schritte

2.2 Installation unter Windows und Einrichtungsassistent

OTScan 3 unter Windows installieren und beim ersten Start mit dem Einrichtungsassistenten einrichten.

Wozu?

Die Installation unter Windows erledigt INSTALL.bat: Sie fragt einmal nach Administratorrechten, prüft, ob nmap und Npcap installiert sind, kopiert das Programm nach C:\Program Files\OTScan3 und legt das Desktop-Symbol „OTScan 3“ an. Auf einem neuen Rechner startet OTScan 3 ohne Daten. Dann öffnet sich der Einrichtungsassistent von selbst und fragt, was Sie brauchen: Minimal (nur Schnellscan), Standard (Netzwerkliste, Berichte, CMDB-Abgleich) oder Vollständig (zusätzlich Scan-MAC-Liste, Netzwerkkette, Splunk, Kameras, Erstinbetriebnahme). „Automatisch erkennen“ sucht vorhandene Netzwerklisten, CMDB und Scan-MAC-Listen und schlägt die passende Vorlage vor.

Achtung

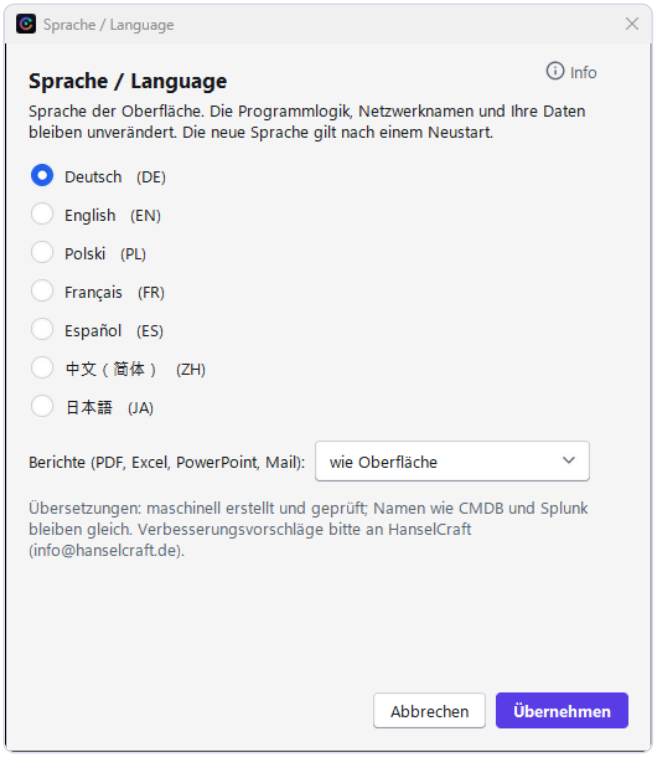
- „Später einrichten“ schließt den Assistenten. Sie öffnen ihn jederzeit wieder über Datenpflege → „Einrichtungsassistent …“.
- „Automatisch erkennen“ übernimmt nichts ohne Ihren Klick – gefundene Dateien werden nur vorgeschlagen.
- Während ERSTINSTALLATION_MIT_BILDERN.bat läuft, Maus und Tastatur nicht benutzen (das Skript macht Bildschirmfotos).
- Ein Arbeitsplatz, der schon Netzwerke hat, bekommt den Assistenten nicht automatisch. Vorhandene Daten in %APPDATA%\OTScan3 bleiben bei einer Neuinstallation erhalten.

So geht's

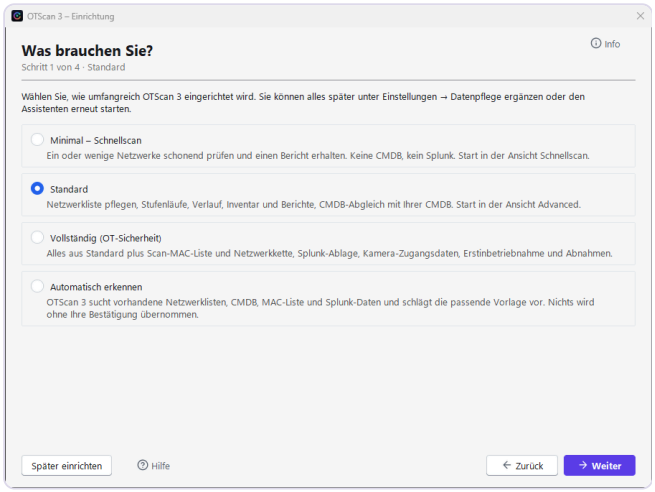
1. ZIP-Paket vollständig in einen Ordner entpacken (nicht aus der ZIP heraus starten).
2. INSTALL.bat doppelklicken und die Frage nach Administratorrechten mit „Ja“ beantworten. Das Fenster zeigt, ob nmap und Npcap gefunden wurden, richtet das Programm ein und meldet am Ende das Ergebnis. nmap und Npcap gehören nicht zum Paket: Fehlen sie, zuerst das nmap-Setup von https://nmap.org/download.html als Administrator ausführen (Npcap dabei mitinstallieren) und INSTALL.bat danach erneut starten.
3. Zum Ausprobieren ohne Eingriff ins System gibt es TESTINSTALLATION.bat (eigener Ordner, eigene Daten). ERSTINSTALLATION_MIT_BILDERN.bat legt zusätzlich eine bebilderte Anleitung (PDF) dieses Rechners an.
4. OTScan 3 über das Desktop-Symbol starten und die Abfrage nach Administratorrechten mit „Ja“ bestätigen. Ohne Daten öffnet sich nach wenigen Sekunden der Einrichtungsassistent.
5. Vorlage wählen: Minimal, Standard, Vollständig oder „Automatisch erkennen“ – dann „Weiter“.
6. Netzwerke eintragen: Name, Netzwerk (CIDR) und Gateway, dann „Hinzufügen“. Oder „Netzwerkliste importieren …“ bzw. „Leere Vorlage öffnen“.
7. Standard und Vollständig: CMDB-Datei wählen, eine leere CMDB anlegen oder den Schritt überspringen.
8. Vollständig: Scan-MAC-Liste importieren oder die Vorschläge übernehmen, Splunk-Eingang anlegen, Kamera-Zugangsdaten hinterlegen.
9. „Fertigstellen“ – OTScan 3 öffnet die passende Ansicht. Später erneut: EINSTELLUNGEN → Datenpflege → Knopf „Einrichtungsassistent …“.
10. SELBSTTEST.bat prüft die Installation, ohne ein Netzwerk zu scannen.

Was trage ich wo ein?

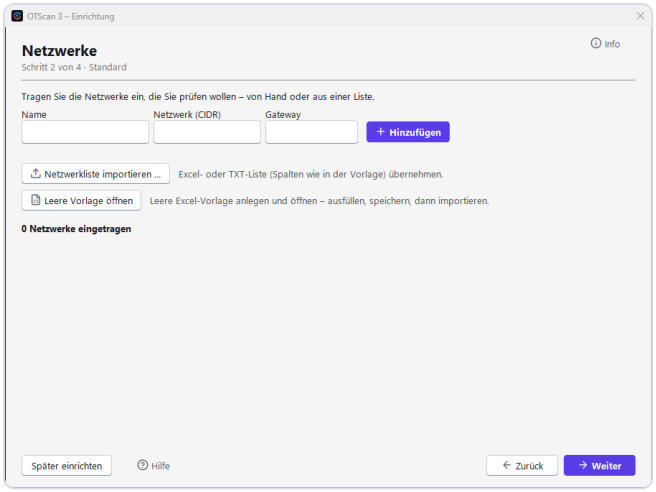
Feld	Bedeutung
Vorlage	Minimal, Standard, Vollständig oder Automatisch erkennen – bestimmt, welche Schritte der Assistent zeigt.
Name	Netzwerkname, zum Beispiel Montage_Anlagennetz. Muss genau so heißen wie in Splunk und in der Scan-MAC-Liste.
Netzwerk (CIDR)	Adressbereich mit Maske, zum Beispiel 192.168.6.0/24. Die Hostbits müssen 0 sein.
Gateway	Adresse des Gateways im Netzwerk, zum Beispiel 192.168.6.1 (optional).
CMDB-Datei	Ihre Inventar-Excel (Blatt „CMDB“). Wird nur gelesen.
Scan-MAC-Liste	Excel- oder CSV-Liste mit Scan-MAC und Scan-IP je Netzwerk (nur Vorlage Vollständig).
Kamera-Zugangsdaten	Nur lesender ONVIF-Benutzer und Passwort für CAM-Netzwerke (optional).



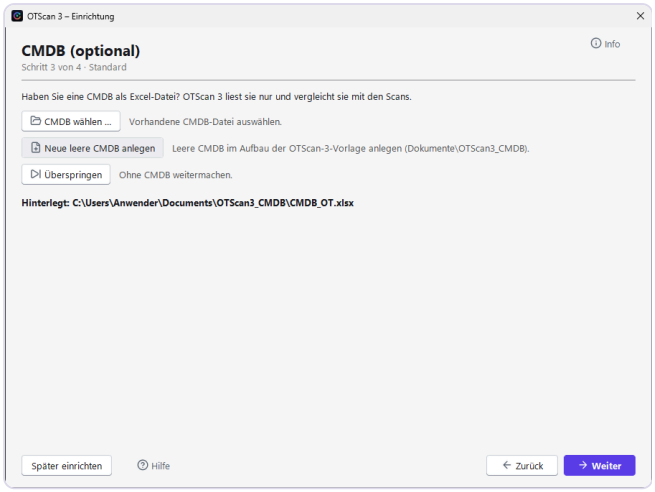
Installation unter Windows und Einrichtungsassistent



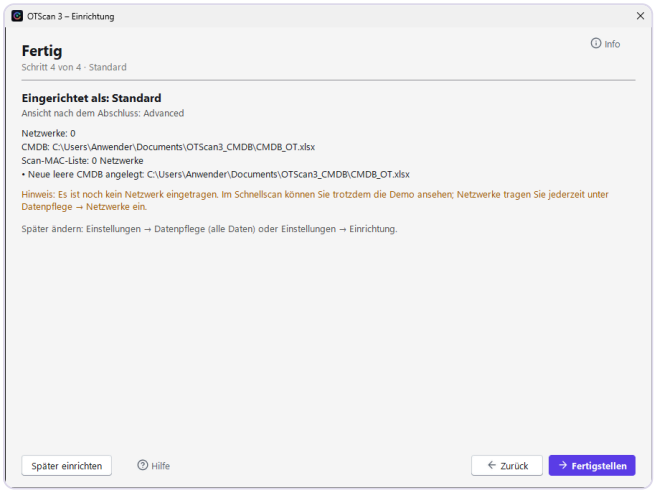
Installation unter Windows und Einrichtungsassistent



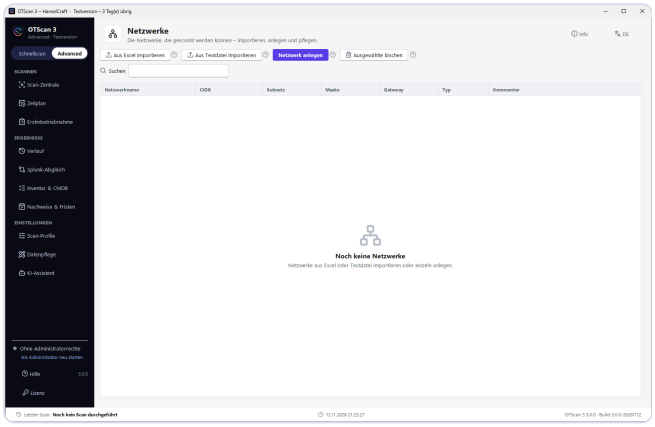
Installation unter Windows und Einrichtungsassistent



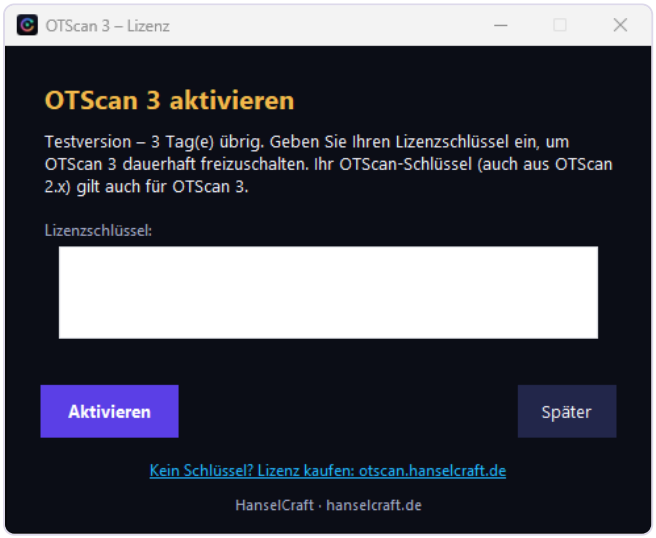
Installation unter Windows und Einrichtungsassistent



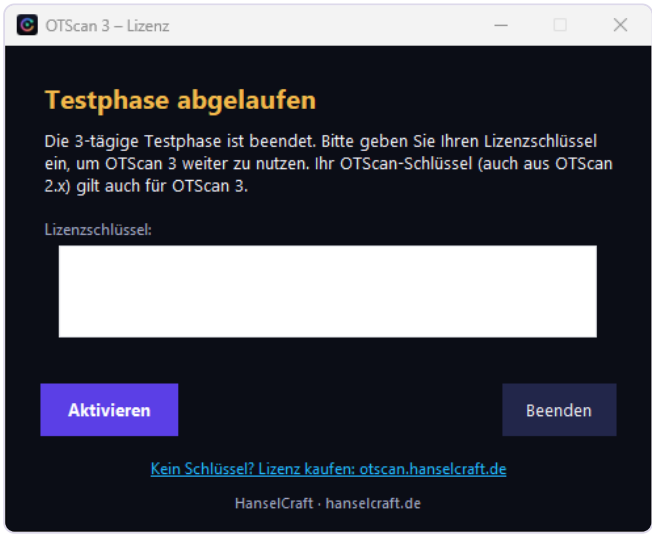
Installation unter Windows und Einrichtungsassistent



Installation unter Windows und Einrichtungsassistent



Installation unter Windows und Einrichtungsassistent



Installation unter Windows und Einrichtungsassistent

2.3 Installation unter Linux

OTScan 3 unter Ubuntu, Debian oder Fedora mit install_linux.sh einrichten, starten, prüfen, Daten übernehmen und wieder entfernen.

Wozu?

Unter Linux richtet das Skript install_linux.sh einmalig alles ein: Pakete (nmap, python3-tk, iproute2, iputils-arping, cron, Chromium, secret-tool, mpg123), eine Python-Umgebung im Unterordner ./venv, die nmap-Rechte per setcap (Scans ohne root) und die Gruppe „otscan3“ mit einer sudo-Regel nur für den Netzwerk-Helfer /usr/local/lib/otscan3/otsp-netz. Der Helfer führt nur die Befehle aus, die das Umstellen des Scan-Adapters braucht (ip, arping, nmcli, dhclient, dhcpcd oder networkctl), prüft jedes Argument und lehnt alles andere ab. Danach starten Sie OTScan 3 als normaler Benutzer.

Achtung

- OTScan 3 nie mit sudo starten. Die nötigen Rechte kommen über setcap (nmap) und die sudo-Regel der Gruppe „otscan3“.
- Ohne sudo-Regel (Einrichtung mit OTSP_OHNE_SUDOREGEL=1) scannt OTScan 3 normal, das Umstellen des Adapters (Adapter einrichten, Netzwerkkette, Direktanschluss) ist dann aber gesperrt – mit Hinweis.
- Nach einem Update von nmap gehen die Rechte verloren. Dann install_linux.sh erneut ausführen oder die Rechte mit getcap prüfen.
- PDF-Berichte brauchen Chromium, Google Chrome oder Microsoft Edge. Fehlt Chromium nach der Installation, meldet das Skript es mit einem Hinweis.

So geht's

1. Paket entpacken und den Programmordner an seinen festen Ort kopieren, zum Beispiel nach /opt/otscan3. Im Programmordner ein Terminal öffnen.
2. Einrichten: sudo ./install_linux.sh <benutzername> eingeben. Als Benutzername den Anmeldenamen der Person angeben, die später scannt.
3. Das Skript arbeitet sechs Abschnitte ab: „== 1. Pakete“ (Kernpakete getrennt; fehlende Zusatzpakete nur als Hinweis), „== 2. Python-Bibliotheken (./venv)“ (wird neu gebaut und erst bei Erfolg getauscht), „== 3. nmap-Rechte“ (zeigt die getcap-Zeile), „== 4. sudo-Regel ...“ (zeigt „Gruppe otscan3: <benutzer>“), „== 5. Startmenü“ und „== 6. Selbsttest“. Am Ende steht „Fertig.“
4. Einmal ab- und wieder anmelden. Erst dann ist die Gruppe „otscan3“ wirksam.
5. Rechte prüfen: getcap "$(readlink -f "$(command -v nmap)")" muss „cap_net_admin,cap_net_bind_service,cap_net_raw=eip“ zeigen; sudo -n /usr/local/lib/otscan3/otsp-netz ip link show lo muss ohne Passwortabfrage antworten; id muss die Gruppe „otscan3“ enthalten.
6. Starten: ./otscan3.sh im Programmordner oder Startmenü „OTScan 3“ – als normaler Benutzer, NICHT mit sudo. Unten links muss „Administratorrechte aktiv“ stehen. Beim ersten Start ohne Daten öffnet sich der Einrichtungsassistent.
7. Daten von Windows übernehmen (optional): OTScan 3 auf beiden Rechnern schließen. Den Windows-Datenordner OTScan 3 (im Benutzerprofil unter AppData/Roaming) nach ~/.local/share/OTScan3 kopieren und die Ordner Dokumente/OTScan3_* nach ~/Dokumente. Kamera-Passwörter danach neu eingeben; geplante Scans mit crontab -l prüfen und fehlende im Zeitplan neu anlegen.
8. Netzwerkadapter: Verwaltet NetworkManager den Scan-Adapter, legt OTScan 3 beim Einrichten ein eigenes Verbindungsprofil „OTScan 3 <Netzwerk>“ an (ohne Standard-Gateway, bleibt nach einem

Neustart erhalten) – zuerst nur mit Scan-MAC, nach der Adresskonflikt-Prüfung mit der Scan-IP. Scheitert ein Schritt, entfernt OTScan 3 das Profil wieder. „Zurücksetzen“ löscht dieses Profil und aktiviert die vorherige Verbindung wieder; war keine aktiv, wird der Adapter freigegeben. Verwaltet systemd-networkd den Adapter, bricht OTScan 3 mit einem Hinweis ab.

9. Deinstallieren: Programmordner mit dem Unterordner venv löschen; sudo rm /etc/sudoers.d/otscan3; sudo rm -r /usr/local/lib/otscan3; nmap-Rechte entfernen mit sudo setcap -r "$(readlink -f "$(command -v nmap)")"; Startmenü-Eintrag ~/.local/share/applications/otscan3.desktop löschen; geplante Scans mit crontab -e entfernen. Ihre Daten in ~/.local/share/OTScan3 und ~/Dokumente bleiben erhalten, bis Sie sie selbst löschen.

Was trage ich wo ein?

Feld	Bedeutung
<benutzername>	Anmeldename der Person, die OTScan 3 nutzt. Sie wird Mitglied der Gruppe „otscan3“.
OTSP_OHNE_SUDOREGEL=1	Optional vor dem Aufruf setzen: Das Skript legt dann keine sudo-Regel an (kein Umstellen des Adapters).
Programmordner	Fester Ort des Programms, zum Beispiel /opt/otscan3. Dort liegen otscan3.sh und venv.

2.4 Hilfe im Programm: Info und Handbuch

Oben rechts auf jeder Seite „Info“ (Schritt-für-Schritt-Hilfe). F1 öffnet die Info zur aktuellen Seite.

Wozu?

Die Hilfe ist dort, wo Sie arbeiten: „Info“ öffnet rechts neben der Seite das Fenster „Info – So geht's“ mit Kurzbeschreibung, „Wozu?“, den nummerierten Schritten „So gehen Sie vor“, „Was trage ich wo ein?“ und „Wichtig“. Von dort öffnen Sie bei Bedarf das Handbuch. Alles läuft offline, ohne Internet.

> **Achtung**
> - Ist kein Handbuch installiert, öffnen die Handbuch-Knöpfe stattdessen die Info zum passenden Thema.

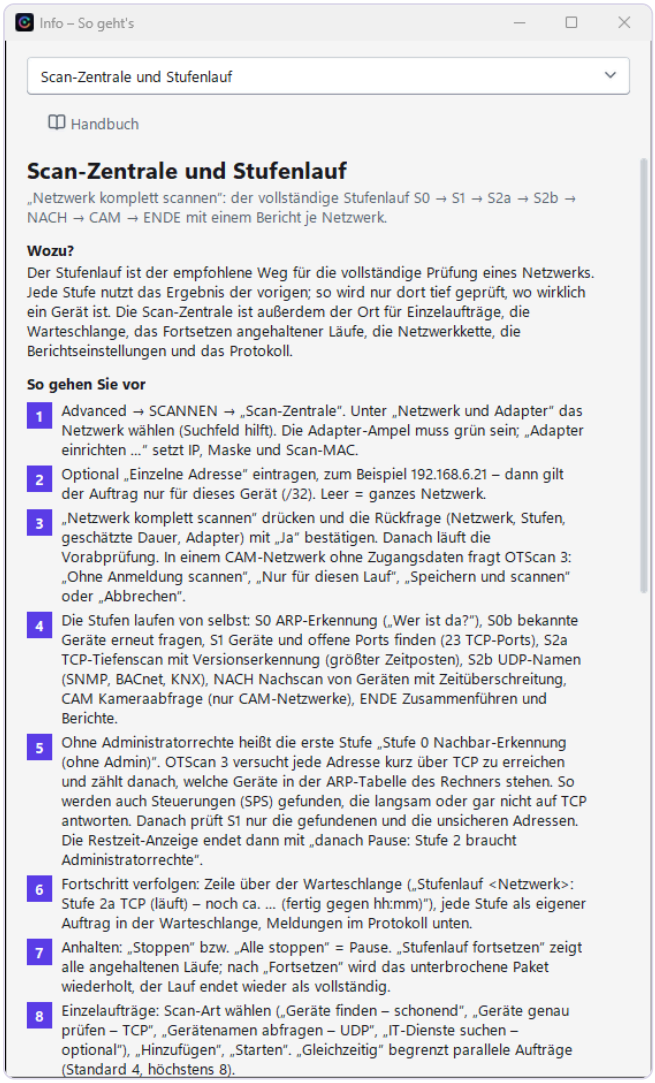
So geht's

1. Oben rechts auf der Seite „Info“ klicken – oder F1 drücken. Rechts öffnet sich „Info – So geht's“ zum Thema der Seite.
2. Lesen: Titel und Kurzbeschreibung, „Wozu?“, „So gehen Sie vor“ (nummerierte Schritte), „Was trage ich wo ein?“ (jedes Feld erklärt) und „Wichtig“.
3. „Handbuch“ öffnet dieses Handbuch im Browser direkt beim passenden Abschnitt.
4. Oben im Info-Fenster lässt sich jedes andere Thema wählen – auch „Berichte und Dokumente“ und „CSV-Vorlagen“. In der Datenpflege richtet sich das Thema nach dem offenen Reiter.
5. Auch die wichtigen Fenster haben oben rechts „Info“: Netzwerkadapter einrichten, Netzwerkkette, Direktanschluss, Splunk-Datenbank, Kamera-Zugangsdaten, Einrichtungsassistent, Berichte & Muster, CSV-Vorlagen und die Zeitplan-Dialoge.

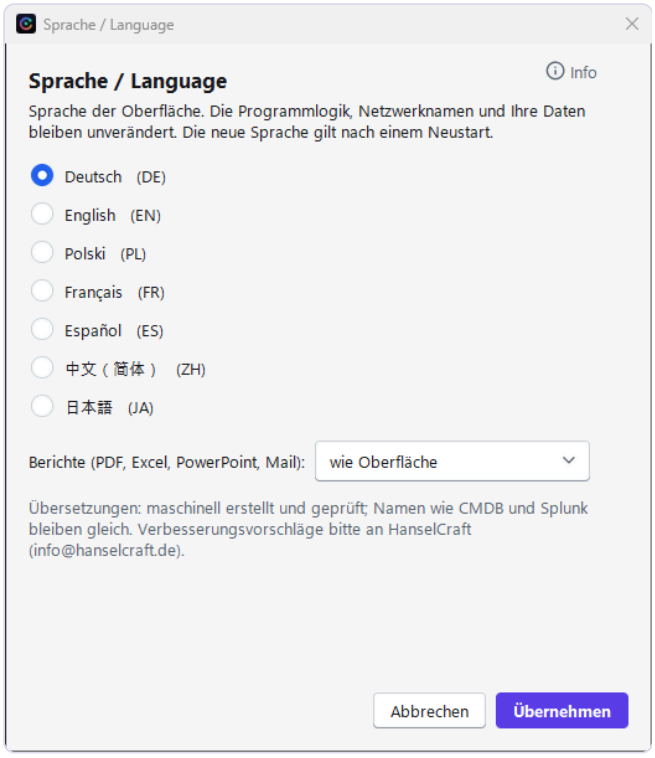
6. Erstinbetriebnahme: Der Info-Punkt (i) vor jeder Prüffrage erklärt „Was ist das? Wofür? Warum?“ mit Beispiel; „Im Handbuch lesen“ führt zur Frage im Handbuch.

Was trage ich wo ein?

Feld	Bedeutung
Themen-Auswahl	Liste oben im Info-Fenster: wählt ein anderes Thema als das der aktuellen Seite.



Hilfe im Programm: Info und Handbuch



Hilfe im Programm: Info und Handbuch

2.5 Sicherheit und Datenschutz

Was ein Scan im Netzwerk tut, welche Daten entstehen, wo sie liegen und welche Regeln gelten.

Wozu?

Ein Scan ist Netzwerkverkehr in einer Anlage. Dieser Bereich erklärt, was Geräte vom Scan merken, welche Daten gespeichert werden und welche Betriebsregeln gelten. Lesen Sie ihn vor dem ersten Scan und bevor Sie Ergebnisse an Dritte geben.

Achtung

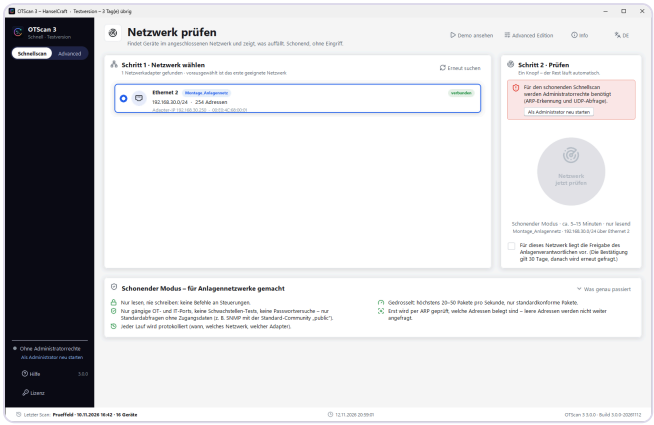
- Was über das Netzwerk geht: ARP-Anfragen (höchstens 20 Pakete pro Sekunde), TCP-Verbindungsaufbau auf feste Portlisten (höchstens 50 Pakete pro Sekunde), wenige UDP-Standardabfragen (SNMP GET mit „public“, BACnet, KNX), in Stufe 2a Versionsproben an offene Ports; in CAM-Netzwerken zusätzlich WS-Discovery und ONVIF GetDeviceInformation (nur lesend).
- Nicht verwendet: nmap-Skripte der Kategorien vuln, brute, exploit, dos; keine Betriebssystem-Erkennung im Stufenlauf. Ausnahme nur auf Wunsch: die Option „Modell/Firmware per Modbus-Geräte-ID und S7“ (liest nur).
- Die Datenbank ist nicht verschlüsselt. Schutz über das Windows-Benutzerprofil und die Laufwerksverschlüsselung. Alle Ausgaben enthalten Netzwerkdaten und sind vertraulich zu behandeln.
- Zeitplan und Netzwerkkette laufen unbeaufsichtigt – nur mit organisatorischer Freigabe. Informieren Sie Netzwerkbetrieb und Sicherheitsteam über Scan-MACs und Scan-IPs.
- Was OTScan 3 mit Administratorrechten sperrt und was die Meldung „nmap gesperrt“ bedeutet, steht im Thema „Sicherheit mit Administratorrechten“.

So geht's

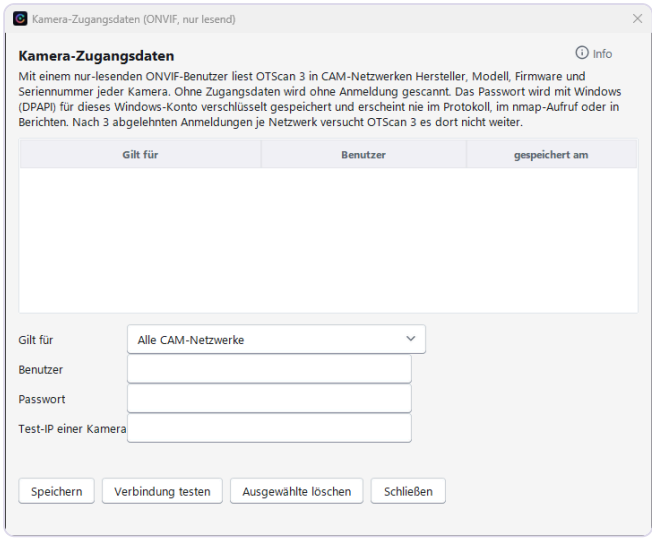
1. Freigabe einholen: Vor dem ersten Scan eines Netzwerks das Einverständnis des Anlagenverantwortlichen. Der Haken im Programm ist eine Selbstauskunft, gilt 30 Tage und ersetzt keine schriftliche Freigabe.
2. Tiefenscans (Stufe 2a, Erstinbetriebnahme „vollständig“) möglichst im Wartungsfenster. Ältere Steuerungen reagieren auf Versionserkennung manchmal träge.
3. Ein Netzwerk, ein Scanner: nie zwei Programme oder Rechner gleichzeitig auf dasselbe Netzwerk. OTScan 3 warnt vor fremden nmap-Prozessen.
4. Richtigen Adapter nutzen: nie über das Büronetzwerk scannen. Gelbe Hinweise wie „Adapter hat ein Standard-Gateway“ beachten.
5. Berichte nach außen (Dienstleister, Hersteller) nur ohne IP-Adressen, MAC-Adressen und Standorte weitergeben – die Dienstleister-PDF der Erstinbetriebnahme ist dafür gemacht.
6. Kamera-Passwörter gibt nur der Anwender im Programm ein. Sie werden mit Windows-DPAPI verschlüsselt und erscheinen nie in Protokollen, XML oder Berichten.
7. Daten löschen: Das Programm löscht nichts automatisch. Zum vollständigen Löschen eines Netzwerks Programm beenden, Dateien mit dem Netzwerknamen im Ausgabeordner, in Splunk\, Dokumente\OTScan3_Inventar und Dokumente\OTScan3_Splunk entfernen, Zustandsdateien unter %APPDATA%\OTScan3\stufenlauf löschen und das Netzwerk in der Datenpflege entfernen.

Was trage ich wo ein?

Feld	Bedeutung
Freigabe-Haken	„Für dieses Netzwerk liegt die Freigabe des Anlagenverantwortlichen vor“ – nur setzen, wenn die Freigabe wirklich vorliegt. Gilt 30 Tage.



Sicherheit und Datenschutz



Sicherheit und Datenschutz

2.6 Sicherheit mit Administratorrechten

Was OTScan 3 mit Administratorrechten zulässt und sperrt – und was bei der Meldung „nmap gesperrt“ zu tun ist.

Wozu?

Mit Administratorrechten (OTScan 3 (Admin), geplante Scans) darf ein Programm fast alles auf dem Rechner. Andere Programme ohne Administratorrechte dürfen das nicht ausnutzen können, indem sie Dateien ändern, die OTScan 3 später mit Administratorrechten verwendet. Deshalb startet OTScan 3 mit Administratorrechten nur Programme aus geschützten Ordnern und lässt nur geprüfte Einstellungen zu. Im normalen Betrieb merken Sie davon nichts.

Achtung

- Datensicherung einspielen geht nur ohne Administratorrechte. Ist eine Sicherung vorgemerkt und OTScan 3 startet mit Administratorrechten, startet es sich selbst ohne Administratorrechte neu. Klappt das nicht, wird die Sicherung nicht eingespielt – dann OTScan 3 über „OTScan 3 (ohne Admin)“ starten.
- Outlook-Entwürfe (z. B. Mails an Dienstleister) erzeugt OTScan 3 nur ohne Administratorrechte. Läuft OTScan 3 mit Administratorrechten, erscheint ein Hinweis; die Entwürfe dann in „OTScan 3 (ohne Admin)“ erzeugen.
- Mit Administratorrechten öffnet OTScan 3 Ordner, Berichte und Dokumente über den Explorer ohne Administratorrechte. Programme, Skripte und Verknüpfungen öffnet es dann nicht.
- Erscheint die Warnung „OTScan 3 – Installation“, OTScan 3 mit INSTALL.bat neu installieren. Bis dahin starten geplante Scans aus so einem Ordner nmap nicht mit Administratorrechten.
- Den Ordner %APPDATA%\nmap nie selbst anlegen und keine eigenen Skripte oder Dateien in den nmap-Programmordner legen. Neue Prüfungen kommen nur mit einer neuen OTScan-3-Fassung.
- Mit Administratorrechten startet OTScan 3 nur bekannte Programme: Windows-Werkzeuge, nmap, das eigene Python und Edge/Chrome aus „Programme“. Riskante Umgebungsvariablen (z. B. NMAP_ARGS, OPENSSL_CONF) entfernt es vorher. Meldet OTScan 3 „… nicht gestartet“, das Scan-Profil bzw. den Rechner von Ihrem IT-Ansprechpartner prüfen lassen.

So geht's

1. Installieren: INSTALL.bat legt OTScan 3 unter C:\Program Files\OTScan3 ab. Diesen Ordner können nur Administratoren ändern. Eine ältere Installation im Benutzerordner zieht INSTALL.bat dorthin um: Geplante Scans werden auf den neuen Ordner umgestellt, die alten Programmdateien entfernt. Datenbank und Einstellungen bleiben in %APPDATA%\OTScan3. Vorher OTScan 3 beenden: Solange es läuft, zieht INSTALL.bat nicht um.
2. Die Zusammenfassung von INSTALL.bat lesen: Geplante Aufgaben, die noch ein Programm aus einem Benutzerordner starten würden (z. B. aus älteren Fassungen), werden deaktiviert und dort genannt. Diese Scans bei Bedarf in OTScan 3 unter „Zeitplan“ neu planen.
3. Für Arbeiten, die nur ohne Administratorrechte gehen (Datensicherung einspielen, Outlook-Entwürfe), OTScan 3 über den Startmenü-Eintrag „OTScan 3 (ohne Admin)“ starten.
4. Meldung „OTScan 3 – nmap gesperrt“: Der Scan wurde nicht gestartet. Die Meldung nennt den Grund – je nach Grund wie in den folgenden Schritten vorgehen.
5. Grund „Der Ordner … nmap existiert“: Die Meldung nennt den Ordner (meist %APPDATA%\nmap). Genau diesen Ordner im Explorer öffnen, den Inhalt prüfen und den Ordner entfernen. OTScan 3 braucht ihn nicht. Danach den Scan neu starten. Ist unklar, woher der Ordner kommt, vorher Ihren IT-Ansprechpartner informieren.
6. Grund „Option …“, „Skript …“, „Skript-Argument …“ oder „Ziel …“: Das Scan-Profil enthält etwas, das mit Administratorrechten nicht zugelassen ist. Unter „Scan-Profile“ das Profil öffnen und die genannte Stelle entfernen; bei einem geplanten Scan das Profil des Zeitplans prüfen. Zugelassen sind nur nmap-Optionen aus einer festen Liste erlaubter Optionen und Skripte, die im nmap-Programmordner installiert sind (Name oder Kategorie, kein Dateipfad).
7. Grund „keine nmap-Installation …“ oder „Datenordner … unvollständig“: nmap neu installieren (nmap-Setup von https://nmap.org/download.html) und INSTALL.bat erneut ausführen.

Was trage ich wo ein?

Feld	Bedeutung
Programmordner	C:\Program Files\OTScan3 – nur Administratoren können ihn ändern. Daten und Einstellungen liegen weiter in %APPDATA%\OTScan3.
OTScan 3 (ohne Admin)	Startmenü-Eintrag (bzw. OTScan3_ohne_Admin.bat) für Arbeiten, die nur ohne Administratorrechte gehen.
Meldung „nmap gesperrt“	nmap oder ein anderes Programm wurde aus Sicherheitsgründen nicht gestartet; ein Scan läuft dann nicht. Die Meldung nennt den Grund (siehe Schritte).
Warnung „OTScan 3 – Installation“	Erscheint beim Start mit Administratorrechten, wenn OTScan 3 aus einem Ordner läuft, den auch normale Benutzer ändern können.

3 Neu in OTScan 3

Was OTScan 3.0 gegenüber OTScan 2.3 neu kann – auf einen Blick.

Wozu?

OTScan 3 ist der Nachfolger von OTScan 2.3. Aus dem Netzwerkscanner ist ein Werkzeug für den ganzen Ablauf geworden: Netzwerke vollständig und schonend in Stufen prüfen, Ergebnisse mit Firewall-Verkehr (z. B. aus Splunk) und Ihrem Inventar (CMDB) abgleichen, Herstellermeldungen zuordnen, Geräte beim Einbau abnehmen und Berichte für alle Zielgruppen erzeugen. Die Oberfläche gibt es in 7 Sprachen, das Programm läuft unter Windows und Linux.

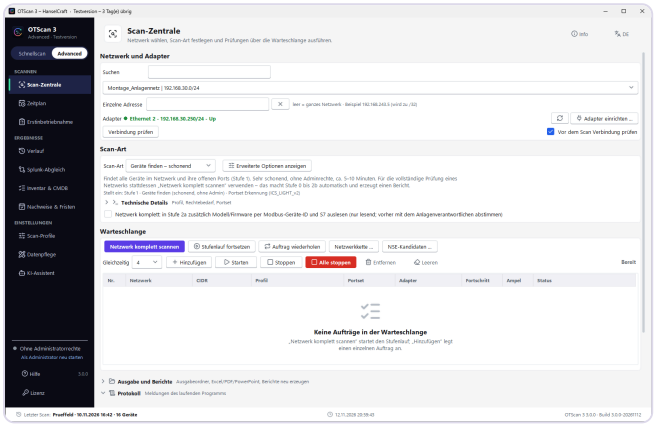
Achtung

- Daten aus OTScan 2.3 werden nicht automatisch übernommen: OTScan 3 hat einen eigenen Datenordner (OTScan3). Netzwerke lassen sich über die CSV-Vorlagen oder den Einrichtungsassistenten übernehmen.
- Lizenzschlüssel aus OTScan 2.x gelten auch für OTScan 3 (gleiche Rechnergrenze). Nach der Testphase aktivieren Sie OTScan 3 mit Ihrem vorhandenen oder einem neuen Schlüssel (otscan.hanselcraft.de).
- Die Verkehrsregeln sind eine Voreinstellung, keine Norm. Passen Sie sie an die Vorgaben Ihres Betriebs an, bevor Sie Berichte weitergeben.

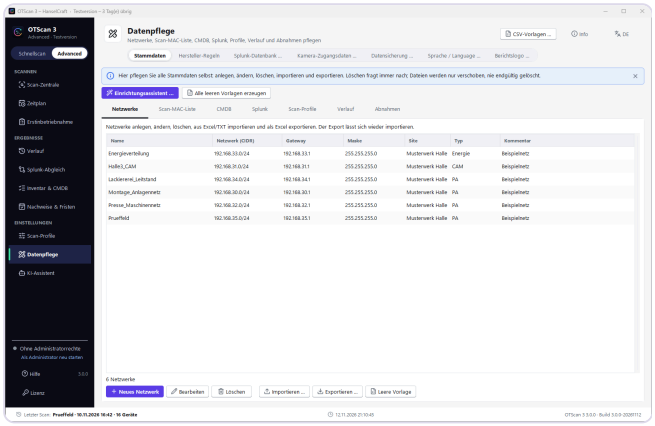
So geht's

1. Zwei Ansichten in einem Programm: „Schnellscan“ (ein Knopf, für alle Anwender) und „Advanced“ (Scan-Zentrale, Zeitplan, Erstinbetriebnahme, Verlauf, Splunk-Abgleich, Inventar & CMDB, Scan-Profile, Datenpflege).
2. Stufenlauf „Netzwerk komplett scannen“: Stufe 0 bis 2b, Nachscan und Kameraabfrage laufen nacheinander, jede Stufe nutzt das Ergebnis der vorigen; ohne Administratorrechte beginnt der Lauf mit der Nachbar-Erkennung. Anhalten und Fortsetzen sind jederzeit möglich.
3. Netzwerkkette: viele Netzwerke nacheinander über einen Adapter scannen – mit Scan-MAC je Netzwerk oder über einen Trunk-Port mit VLAN-Nummer.
4. Splunk-Abgleich: Firewall-Exporte (z. B. Splunk-Suche über FortiGate-Logs) einlesen und mit dem Scan vergleichen – Geräte nur im Verkehr, Port-Lücken, Nachscan-Vorschläge; Zonen, Services und Policies erscheinen in den Berichten.
5. Inventar & CMDB: Abgleich mit Ihrer Excel-Geräteliste, CMDB-Delta (neu, geändert, fehlt), CMDB-Nachtrag für Geräte, die nur im Verkehr auftauchen, und ein Gesamtinventar über alle Quellen. Die CMDB wird nur gelesen.
6. Herstellermeldungen: mitgelieferter Offline-Bestand öffentlicher CSAF-Quellen (Hersteller-PSIRTs, CERT@VDE, CISA) statt der 11 Einzelmeldungen von OTScan 2.3; Aktualisierung nur auf Knopfdruck „Online aktualisieren“.
7. Erstinbetriebnahme und Abnahmen: Prüfliste mit Erklärungen je Frage, Scan vorher/nachher am Gerät, Direktanschluss, Protokoll und Paket für den Dienstleister; Sollzustand übernehmen und spätere Scans dagegen vergleichen.

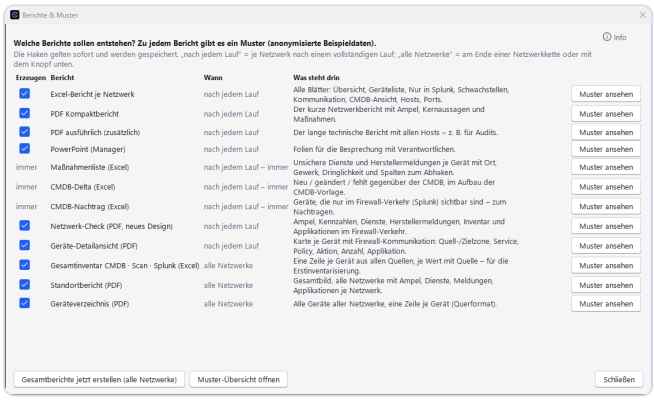
8. Neue Berichte: Netzwerk-Check, Geräte-Detailansicht mit Firewall-Kommunikation, Standortbericht und Geräteverzeichnis (PDF), Maßnahmenliste (Excel), PowerPoint für Besprechungen – mit Mustern unter „Berichte & Muster“.
9. Bewertung nach Verkehrsregeln: eine an IEC 62443 (Zonen und Conduits) angelehnte HanselCraft-Voreinstellung, die Sie an Ihre eigenen Regeln anpassen.
10. Kameraprofil und Kamera-Zugangsdaten (ONVIF, nur lesend), Hersteller-Regeln, Zeitplan, CSV-Vorlagen für alle Stammdaten, Datensicherung mit Umzug zwischen Windows und Linux.
11. Hilfe dort, wo Sie arbeiten: „Info“ oben rechts auf jeder Seite (F1), Einrichtungsassistent beim ersten Start, Nutzerhandbuch im Programmordner. Oberfläche und Berichte in Deutsch, Englisch, Spanisch, Französisch, Polnisch, Japanisch und Chinesisch.



Neu in OTScan 3



Neu in OTScan 3



Neu in OTScan 3

4 Scannen

4.1 Schnellscan – Netzwerk prüfen

Ein Netzwerk mit einem Knopf schonend prüfen – ohne Tiefenscan, mit Bericht.

Wozu?

Der Schnellscan ist für alle Anwender gedacht, auch ohne Netzwerkkenntnisse. Er findet die Geräte eines direkt angeschlossenen Netzwerks (bis /22), prüft 23 gängige TCP-Ports und fragt Gerätenamen per SNMP, BACnet und KNX ab. Er eignet sich für den laufenden Betrieb (mit Freigabe) und für die regelmäßige Sichtkontrolle; den vollständigen Stufenlauf erledigt die Advanced Edition.

Achtung

- Der Schnellscan braucht Administratorrechte (ARP und UDP). Ohne sie startet er nicht – OTScan 3 neu starten und die Abfrage mit „Ja“ bestätigen.
- Bildschirm-Auffälligkeiten (auch Modbus, S7, BACnet) und die Ampel nach den Verkehrsregeln im PDF sind zwei Maßstäbe: Der Bildschirm kann „Modbus/TCP ohne Anmeldung – Wichtig“ zeigen, das PDF trotzdem GRÜN. Für Maßnahmen gilt der Bericht.
- Dauer-Richtwerte: /25 etwa 3 bis 7 Minuten, /24 etwa 5 bis 15 Minuten, /23 etwa 10 bis 30 Minuten. Kommt keine ARP-Antwort, prüft Schritt 3 alle Adressen – das dauert deutlich länger.
- Passt die Netzmaske des Adapters nicht zum hinterlegten Netzwerk, sperrt OTScan 3 den Start mit rotem Hinweis. Die Maske setzen Sie in der Scan-Zentrale über „Adapter einrichten …“.

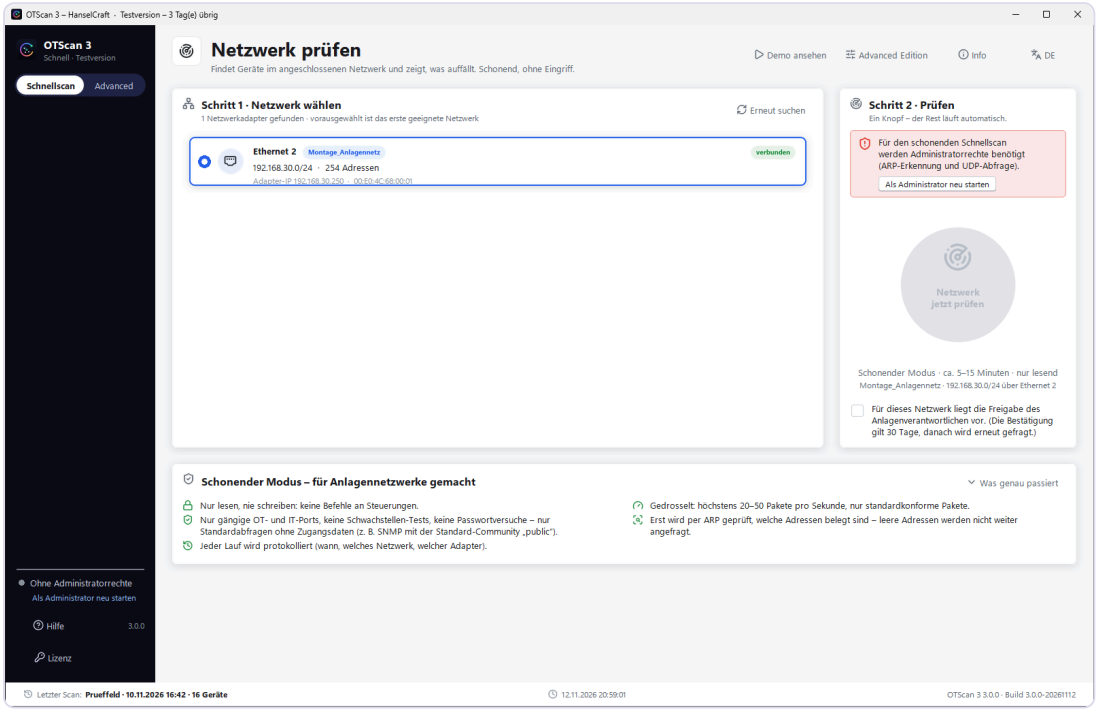
So geht's

1. Oben links „Schnellscan“ wählen. Die Seite „Netzwerk prüfen“ listet unter „Schritt 1 · Netzwerk wählen“ alle Netzwerkadapter mit Ampel: grün „verbunden“, gelb Büronetzwerk-Hinweis, rot „nicht verbunden“, „ungeeignet“ bei Netzwerken über 1022 Adressen.
2. Den Adapter des Anlagennetzwerks anklicken. Ist das Netzwerk in OTScan 3 hinterlegt, steht sein Name dabei; unbekannte Netzwerke legt OTScan 3 beim Start automatisch an.
3. Rechts unter „Schritt 2 · Prüfen“ den Haken „Für dieses Netzwerk liegt die Freigabe des Anlagenverantwortlichen vor“ setzen (gilt 30 Tage).
4. „Netzwerk jetzt prüfen“ drücken. Die Vorabprüfung meldet fremde nmap-Scans, laufende Aufträge, Windows Update oder Neustart und getrennte Adapter – mit „Trotzdem starten“ oder „Abbrechen“.
5. Während der Prüfung zeigt die Schrittkarte fünf Schritte (Netzwerk erkennen, Geräte finden, Dienste prüfen, Gerätetyp und Hersteller, Bericht erstellen) mit Restzeit; links erscheint ein Zwischenstand der Geräte.
6. „Prüfung anhalten“ pausiert. Abgeschlossene Schritte bleiben, der laufende wird beim Fortsetzen wiederholt. Fortsetzen: Advanced → Scan-Zentrale → „Stufenlauf fortsetzen“.
7. Ergebnis: Kennzahlen (Geräte, OT-Geräte, Hinweise, davon wichtig), Gerätekarten oder Tabelle mit Filter, Auffälligkeiten mit Empfehlung. Knöpfe „Bericht öffnen (PDF)“, „Excel“, „Kurzbericht (HTML)“, „In Advanced öffnen“, „Neue Prüfung“.

8. „Demo ansehen“ zeigt den Ablauf mit erfundenen Daten ohne Netzwerkverkehr. „Info“ oben rechts erklärt die Seite Schritt für Schritt.

Was trage ich wo ein?

Feld	Bedeutung
Schritt 1 · Netzwerk wählen	Adapter des Anlagennetzwerks anklicken. Nur grün markierte Adapter sind sofort geeignet.
Freigabe-Haken	Bestätigt, dass die Freigabe des Anlagenverantwortlichen vorliegt. Gilt 30 Tage je Netzwerk.
Filter (Ergebnis)	Schränkt die Geräteliste ein, zum Beispiel auf Geräte mit Hinweisen.



Schnellscan – Netzwerk prüfen

4.2 Scan-Zentrale und Stufenlauf

„Netzwerk komplett scannen“: der vollständige Stufenlauf S0 → S1 → S2a → S2b → NACH → CAM → ENDE mit einem Bericht je Netzwerk.

Wozu?

Der Stufenlauf ist der empfohlene Weg für die vollständige Prüfung eines Netzwerks. Jede Stufe nutzt das Ergebnis der vorigen; so wird nur dort tief geprüft, wo wirklich ein Gerät ist. Die Scan-Zentrale ist außerdem der Ort für Einzelaufträge, die Warteschlange, das Fortsetzen angehaltener Läufe, die Netzwerkkette, die Berichtseinstellungen und das Protokoll.

Achtung

- Ohne Administratorrechte beginnt der Lauf mit „Stufe 0 Nachbar-Erkennung (ohne Admin)“ und S1. Vor S2a hält er an („Stufe 2a TCP braucht Administratorrechte …“). Dann OTScan 3 als Administrator neu starten und „Stufenlauf fortsetzen“.
- Dauer-Richtwerte: /25 mit etwa 30 Geräten gut eine Stunde, /23 mit etwa 150 Geräten 6 bis 7 Stunden. „Geräte genau prüfen – TCP“ auf ein ganzes Netzwerk dauert Stunden – dafür ist der Stufenlauf da.
- Ein Neustart während des Laufs bricht ihn ab; der Zustand bleibt in %APPDATA%\OTScan3\stufenlauf und ist über „Stufenlauf fortsetzen“ erreichbar. Windows Update und Energiesparen vorher abschalten.
- Mehrere Netzwerke parallel nur mit je eigenem Adapter. Die Option „in Stufe 2a zusätzlich Modell/Firmware per Modbus-Geräte-ID und S7 auslesen“ ist standardmäßig aus – vorher mit dem Anlagenverantwortlichen abstimmen.
- Die Nachbar-Erkennung funktioniert nur, wenn das Netzwerk direkt am Adapter liegt. Liegt es hinter einem Router, einem VPN oder einer Route, prüft S1 wie bisher alle Adressen einzeln.
- Große Netzwerke ohne Administratorrechte: Ab /20 (4094 nutzbare Adressen) fragt OTScan 3 vor dem Start nach („Großes Netzwerk“) und nennt die geschätzte Dauer. Ab /18 empfiehlt es, das Netzwerk in kleinere Teilnetzwerke (z. B. /22) aufzuteilen oder OTScan 3 als Administrator zu starten.
- Liefert die Nachbar-Erkennung in einem sehr großen Netzwerk (ab /21, also mehr als 1024 nutzbare Adressen) kein verwertbares Ergebnis, hält der Stufenlauf an („Stufenlauf angehalten“), statt tagelang alle Adressen einzeln zu prüfen. Empfehlung: OTScan 3 als Administrator starten und „Stufenlauf fortsetzen“ oder das Netzwerk aufteilen. Wer ohne Administratorrechte „Stufenlauf fortsetzen“ wählt, startet S1 bewusst über alle Adressen.
- Melden sehr viele Adressen dieselbe MAC-Adresse (Proxy-ARP), steht eine Warnung im Protokoll; S1 prüft dann alle gemeldeten Adressen. Große Trefferlisten arbeitet S1 ohne Administratorrechte in Paketen ab; nach „Stoppen“ wiederholt „Stufenlauf fortsetzen“ das unterbrochene Paket.

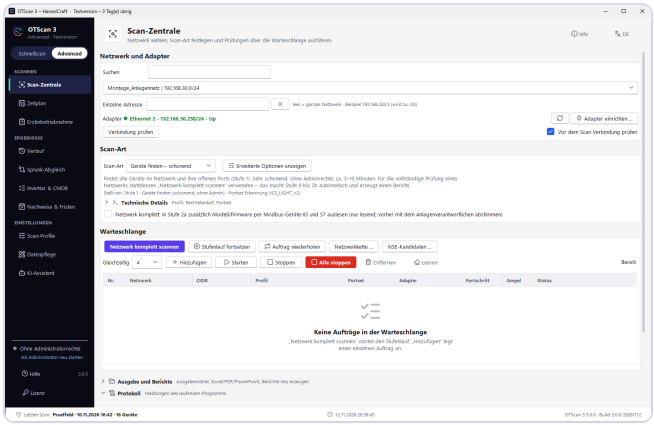
So geht's

1. Advanced → SCANNEN → „Scan-Zentrale“. Unter „Netzwerk und Adapter“ das Netzwerk wählen (Suchfeld hilft). Die Adapter-Ampel muss grün sein; „Adapter einrichten …“ setzt IP, Maske und Scan-MAC.
2. Optional „Einzelne Adresse“ eintragen, zum Beispiel 192.168.6.21 – dann gilt der Auftrag nur für dieses Gerät (/32). Leer = ganzes Netzwerk.
3. „Netzwerk komplett scannen“ drücken und die Rückfrage (Netzwerk, Stufen, geschätzte Dauer, Adapter) mit „Ja“ bestätigen. Danach läuft die Vorabprüfung. In einem CAM-Netzwerk ohne Zugangsdaten fragt OTScan 3: „Ohne Anmeldung scannen“, „Nur für diesen Lauf“, „Speichern und scannen“ oder „Abbrechen“.
4. Die Stufen laufen von selbst: S0 ARP-Erkennung („Wer ist da?“), S0b bekannte Geräte erneut fragen, S1 Geräte und offene Ports finden (23 TCP-Ports), S2a TCP-Tiefenscan mit Versionserkennung (größter Zeitposten), S2b UDP-Namen (SNMP, BACnet, KNX), NACH Nachscan von Geräten mit Zeitüberschreitung, CAM Kameraabfrage (nur CAM-Netzwerke), ENDE Zusammenführen und Berichte.

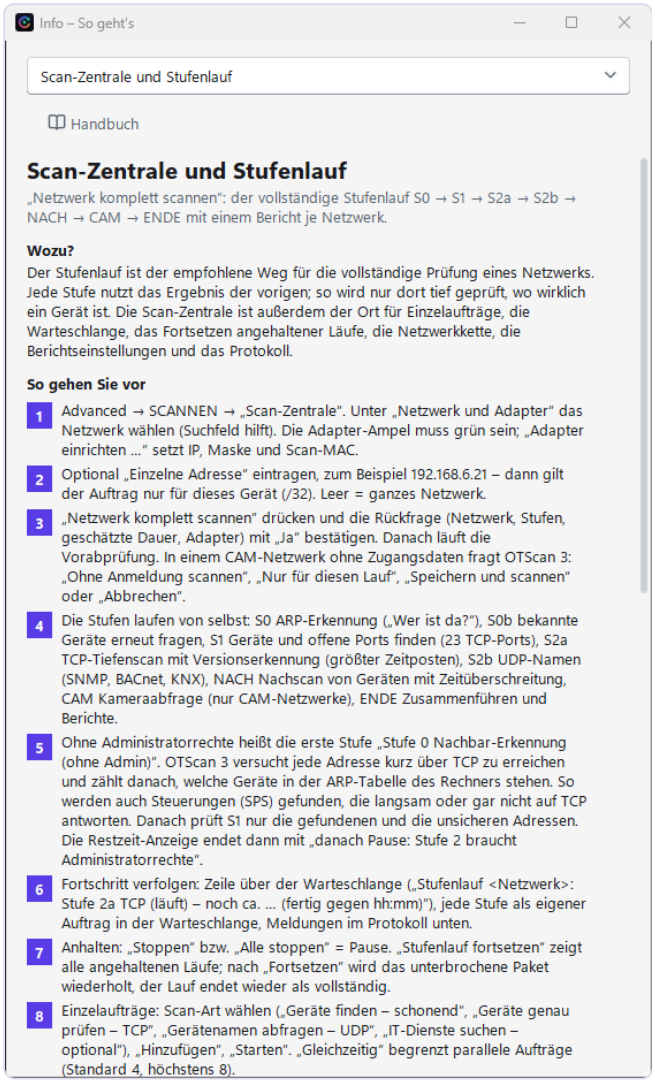
5. Ohne Administratorrechte heißt die erste Stufe „Stufe 0 Nachbar-Erkennung (ohne Admin)“. OTScan 3 versucht jede Adresse kurz über TCP zu erreichen und zählt danach, welche Geräte in der ARP-Tabelle des Rechners stehen. So werden auch Steuerungen (SPS) gefunden, die langsam oder gar nicht auf TCP antworten. Danach prüft S1 nur die gefundenen und die unsicheren Adressen. Die Restzeit-Anzeige endet dann mit „danach Pause: Stufe 2 braucht Administratorrechte“.
6. Fortschritt verfolgen: Zeile über der Warteschlange („Stufenlauf <Netzwerk>: Stufe 2a TCP (läuft) – noch ca. … (fertig gegen hh:mm)“), jede Stufe als eigener Auftrag in der Warteschlange, Meldungen im Protokoll unten.
7. Anhalten: „Stoppen“ bzw. „Alle stoppen“ = Pause. „Stufenlauf fortsetzen“ zeigt alle angehaltenen Läufe; nach „Fortsetzen“ wird das unterbrochene Paket wiederholt, der Lauf endet wieder als vollständig.
8. Einzelaufträge: Scan-Art wählen („Geräte finden – schonend“, „Geräte genau prüfen – TCP“, „Gerätenamen abfragen – UDP“, „IT-Dienste suchen – optional“), „Hinzufügen“, „Starten“. „Gleichzeitig“ begrenzt parallele Aufträge (Standard 4, höchstens 8).
9. „Ausgabe und Berichte“ aufklappen: Ausgabeordner (Standard Dokumente), Haken „Nach jedem Scan erzeugen“ für Excel, PDF und PowerPoint, „PDF ausführlich zusätzlich“, „Berichte & Muster …“, „Berichte aus XML erzeugen“, „Berichte für markierten Auftrag neu erzeugen“.
10. Nach dem Lauf: Im Verlauf steht er als „Netzwerk komplett (Stufenlauf)“. Die Berichte liegen im Ausgabeordner (siehe „Berichte und Dokumente“).

Was trage ich wo ein?

Feld	Bedeutung
Suchen / Netzwerk	Netzwerk aus der Liste wählen; das Suchfeld filtert nach Namen.
Einzelne Adresse	Leer = ganzes Netzwerk. Eine Adresse, zum Beispiel 192.168.6.21, beschränkt den Auftrag auf ein Gerät.
Adapter	Zeigt den Adapter für das Netzwerk mit Ampel. Über „Adapter einrichten …“ ändern.
Scan-Art	Nur für Einzelaufträge: Geräte finden, Geräte genau prüfen (TCP), Gerätenamen abfragen (UDP), IT-Dienste suchen.
Gleichzeitig	Wie viele Aufträge parallel laufen dürfen (Standard 4, höchstens 8).
Modbus/S7-Haken	Liest in Stufe 2a zusätzlich Modell und Firmware per Modbus-Geräte-ID und S7 (standardmäßig aus).
Ausgabeordner	Wohin Berichte geschrieben werden. Standard: Dokumente.
Nach jedem Scan erzeugen	Haken für Excel, PDF und PowerPoint; „PDF ausführlich zusätzlich“ für Audits.



Scan-Zentrale und Stufenlauf



Scan-Zentrale und Stufenlauf

4.3 Netzwerkkette – viele Netzwerke nacheinander

Ein Adapter an einer Netzwerkdose scannt alle gewählten Netzwerke nacheinander – mit Scan-MAC, Gegenprobe, Pause und Startfenster. Über einen Trunk-Port setzt die Kette statt der Scan-MAC je Netzwerk die VLAN-Nummer.

Wozu?

An vielen Standorten gibt die Netzwerkzugangskontrolle (zum Beispiel MAC-basierte Portfreigabe) ein Anlagennetzwerk nur für eine registrierte MAC-Adresse frei. Die Netzwerkkette setzt je Netzwerk die registrierte Scan-MAC und eine freie Scan-IP auf einen Adapter, prüft das Netzwerk gegen, scannt, pausiert und geht zum nächsten Netzwerk. So laufen Nacht- oder Wochenendläufe über viele Netzwerke ohne Umstecken. An Standorten ohne diese Zugangskontrolle kann der Switchport stattdessen als Trunk eingerichtet sein: Dann setzt die Kette je Netzwerk die VLAN-Nummer am Adapter.

Achtung

- Startklar sind nur Netzwerke mit registrierter Scan-MAC (Scan-MAC-Liste, Spalte „MAC-Herkunft“ bzw. „MAC-Registrierung“ = registriert), Scan-IP und gültiger Freigabe (30 Tage, keine automatische Verlängerung). Mit Trunk-Port braucht jedes Netzwerk stattdessen eine gültige VLAN-Nummer (1–4094) in den Netzwerk-Stammdaten; eine ungültige Nummer steht als „Trunk: nicht bereit – VLAN ungültig“ in der Liste.
- Schlägt die Gegenprobe fehl (MAC, IP oder Gateway passt nicht), wird das Netzwerk nicht gescannt. Nach 3 Fehlern in Folge hält die Kette an.
- OTScan 3 (als Administrator) muss geöffnet bleiben; Energiesparen und Windows-Neustart abschalten. Nach einem Neustart steht die Kette auf „unterbrochen“ und läuft erst nach „Fortsetzen“ weiter.
- Die Scan-MAC-Liste nicht ändern, solange eine Kette läuft. Je Adapter eine eigene Kette; ein Netzwerk darf nicht in zwei Ketten stehen. Die Kette fragt nie nach Kamera-Zugangsdaten.
- Trunk-Port nur verwenden, wenn das Netzwerkteam den Switchport als Trunk mit genau den freigegebenen VLANs eingerichtet hat. Kann der Adapter kein VLAN, bricht OTScan 3 ab, bevor etwas am Adapter geändert wird. Im Trunk-Betrieb setzt die Kette keine Scan-MAC; gemischte Ketten (Scan-MAC und VLAN) gibt es nicht.
- „Beenden + Adapter zurücksetzen“ stellt auch die VLAN-Einstellung zurück. Meldet die Kette am Ende „Zurücksetzen nicht bestätigt - Adapter von Hand prüfen ('Adapter einrichten' -> Zurücksetzen)“, den Adapter über „Adapter einrichten“ → „Zurücksetzen“ von Hand prüfen. Im Protokoll steht dann „VLAN am Adapter nicht zurückgesetzt“.

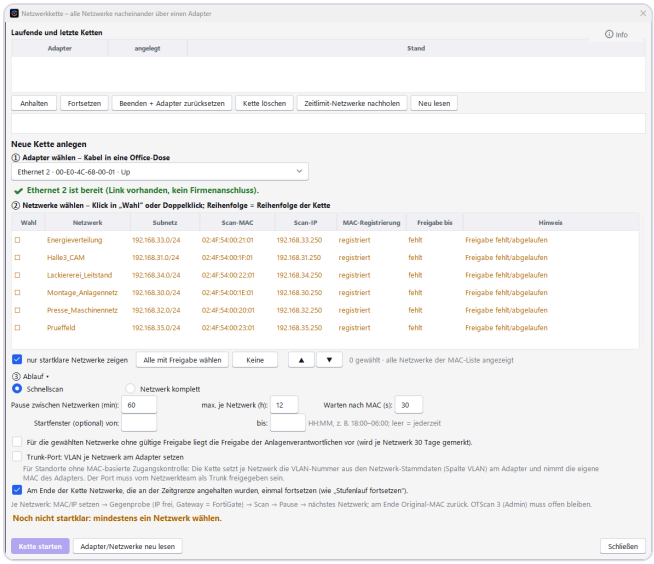
So geht's

1. Advanced → SCANNEN → Scan-Zentrale → Warteschlange → „Netzwerkkette …“. Oben stehen „Laufende und letzte Ketten“ mit Adapter, angelegt und Stand.
2. „Neue Kette anlegen“ – ① Adapter wählen (Kabel in eine Netzwerkdose). Der passende Adapter ist meist vorgewählt und grün „bereit“; rot nennt den Grund (Funk, Firmenanschluss, kein Kabel).
3. ② Netzwerke wählen: Klick in die Spalte „Wahl“ oder Doppelklick. Aus ☐ wird ✔ 1, ✔ 2 … (Reihenfolge der Kette). Spalten: Netzwerk, Subnetz, Scan-MAC, Scan-IP, MAC-Registrierung, Freigabe bis, Hinweis. Hilfen: „nur startklare Netzwerke zeigen“, „Alle mit Freigabe wählen“, „Keine“, Pfeile zum Umsortieren.
4. Trunk-Port (für Standorte ohne MAC-basierte Zugangskontrolle): Haken „Trunk-Port: VLAN je Netzwerk am Adapter setzen“ setzen. Die Kette setzt dann je Netzwerk die VLAN-Nummer aus den Netzwerk-Stammdaten (Spalte VLAN) am Adapter und nutzt die eigene MAC des Adapters – keine Scan-MAC. Die Liste zeigt dann auch Netzwerke mit VLAN-Nummer aus den Stammdaten; die Spalte Scan-MAC bleibt leer. Voraussetzung: Der Treiber des Adapters kann VLAN (Eigenschaft „VLAN ID“). OTScan 3 sichert die Einstellung vorher und stellt sie am Ende zurück.
5. ③ Ablauf einstellen: „Schnellscan“ oder „Netzwerk komplett“, Pause zwischen Netzwerken (Standard 60 Minuten), höchstens je Netzwerk (Stunden), Warten nach MAC (Sekunden), optional ein Startfenster, zum Beispiel 18:00–06:00. Mit Haken „Trunk-Port“ heißt das Feld „Warten nach Adapter-Neustart (s)“. Auf kleinen Bildschirmen (z. B. 1366×768) ist ③ eingeklappt und zeigt eine Kurzfassung; ein Klick auf „③ Ablauf“ klappt die Felder auf.
6. Den Freigabe-Haken für Netzwerke ohne gültige Freigabe nur setzen, wenn die Freigaben wirklich vorliegen. Die Zeile über den Knöpfen muss grün „Startklar …“ zeigen – dann „Kette starten“.

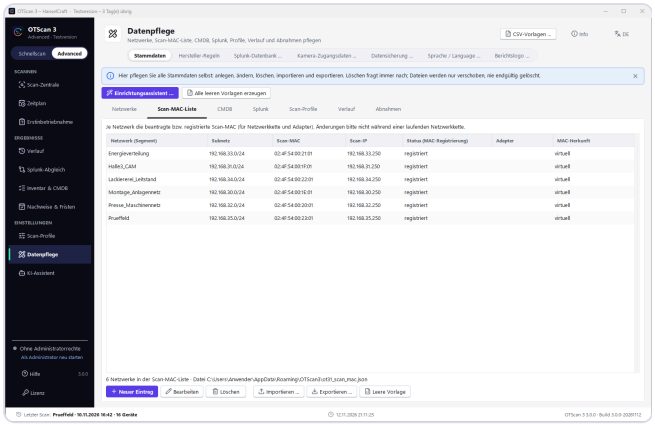
7. Je Netzwerk läuft: Scan-MAC und Scan-IP setzen → auf die Netzwerkzuweisung warten → Gegenprobe (IP frei, Gateway ist eine FortiGate) → Lauf → Pause → nächstes Netzwerk. Mit Trunk-Port: VLAN-Nummer statt Scan-MAC setzen und warten, bis der Switchport wieder Verkehr durchlässt.
8. Am Ende stellt OTScan 3 die Original-MAC wieder her und schreibt Netzkette_<Adapter>_<Zeit>.csv in den Ausgabeordner.
9. Knöpfe oben: „Anhalten“ (nach dem laufenden Netzwerk), „Fortsetzen“ (auch nach einem Programmneustart), „Beenden + Adapter zurücksetzen“, „Kette löschen“, „Neu lesen“.
10. „Kette löschen“: eine oder mehrere fertige oder abgebrochene Ketten markieren und die Rückfrage bestätigen. Die Kettendatei wandert nach %APPDATA%\OTScan3\netzkette_geloescht (wiederherstellbar); Scans, Berichte und Übersichts-CSV bleiben.

Was trage ich wo ein?

Feld	Bedeutung
① Adapter	Adapter für die ganze Kette. Grün „bereit“ = geeignet; rot nennt den Grund.
② Wahl	Klick oder Doppelklick wählt ein Netzwerk; die Zahl gibt die Reihenfolge an.
Scan-Art	„Schnellscan“ (schneller) oder „Netzwerk komplett“ (Stufenlauf) für alle Netzwerke der Kette.
Pause zwischen Netzwerken	Wartezeit nach jedem Netzwerk in Minuten (Standard 60).
max. je Netzwerk (h)	Zeitlimit je Netzwerk in Stunden; danach geht die Kette weiter.
Warten nach MAC (s)	Wartezeit nach dem Setzen der Scan-MAC, bis die Netzwerkzuweisung greift.
Startfenster	Optional, zum Beispiel 18:00–06:00: Netzwerke starten nur in diesem Zeitraum.
Freigabe-Haken	Bestätigt die Freigabe für die gewählten Netzwerke ohne gültige Freigabe; wird je Netzwerk 30 Tage gemerkt.
Trunk-Port	Setzt je Netzwerk die VLAN-Nummer aus den Netzwerk-Stammdaten am Adapter (eigene MAC des Adapters). Ohne Haken: Access-Port, Scan-MAC je Netzwerk.
Warten nach Adapter-Neustart (s)	Nur mit Trunk-Port: Wartezeit nach dem Setzen der VLAN-Nummer, bis der Switchport wieder Verkehr durchlässt.



Netzwerkkette – viele Netzwerke nacheinander



Netzwerkkette – viele Netzwerke nacheinander

4.4 Zeitplan – wiederkehrende Scans

Einzelaufträge täglich, wöchentlich oder monatlich über die Windows-Aufgabenplanung laufen lassen.

Wozu?

Der Zeitplan legt einen geplanten Scan an, der zur festgelegten Zeit automatisch läuft – auch ohne geöffnetes Programm. OTScan 3 trägt ihn dafür in die Windows-Aufgabenplanung ein. Geeignet für wiederkehrende Sichtkontrollen mit einem festen Profil. Für die vollständige Prüfung mehrerer Netzwerke ist die Netzwerkkette der bessere Weg.

Achtung

- Ein geplanter Scan ist ein einzelner Auftrag mit dem gewählten Profil – kein Stufenlauf, keine Vorabprüfung, keine Freigabe-Abfrage. Er erzeugt Excel und PDF.
- Es gilt dieselbe Freigabe-Pflicht wie für einen Scan von Hand: nur mit Einverständnis des Anlagenverantwortlichen planen.
- Die Aufgabe läuft unbeaufsichtigt mit höchsten Rechten aus dem Programmordner. Nach dem Entfernen einer Programmversion verwaiste Aufgaben in der Aufgabenplanung löschen.
- Der Scan läuft über den Adapter, der im Zielnetzwerk steckt – ein geplanter Scan setzt keine Scan-MAC.

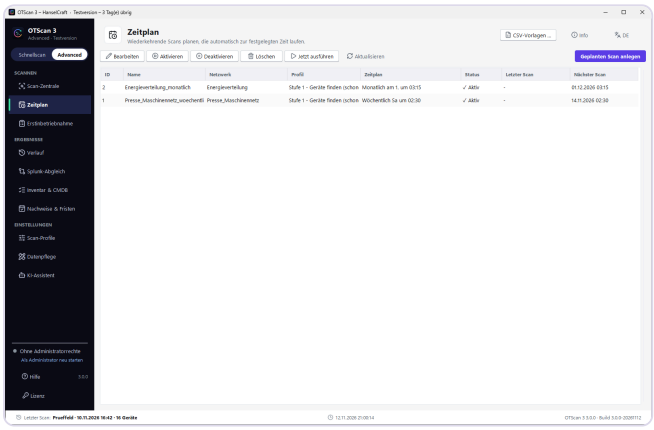
So geht's

1. Advanced → SCANNEN → „Zeitplan“.
2. „Geplanten Scan anlegen“: Name, Netzwerk, Profil und Portset wählen, Rhythmus (täglich, wöchentlich, monatlich), Uhrzeit (HH:MM) und bei wöchentlich den Wochentag bzw. bei monatlich den Tag (1–28) eintragen. „Info“ oben rechts im Dialog erklärt jedes Feld.
3. Speichern – OTScan 3 legt eine Aufgabe in der Windows-Aufgabenplanung mit erhöhten Rechten an.
4. Die Tabelle zeigt ID, Name, Netzwerk, Profil, Zeitplan, Status, letzten und nächsten Scan. „Nächster Lauf“ stimmt jetzt auch bei wöchentlichen Plänen.

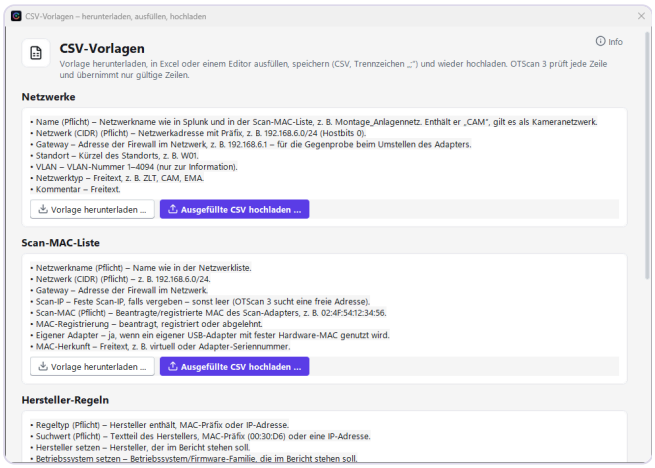
5. Weitere Knöpfe: „Bearbeiten“, „Aktivieren“, „Deaktivieren“, „Löschen“, „Jetzt ausführen“, „Aktualisieren“.
6. Viele Pläne auf einmal: „CSV-Vorlagen …“ oben rechts → Zeitplan → „Vorlage herunterladen …“, ausfüllen, „Ausgefüllte CSV hochladen …“.
7. Protokoll der geplanten Läufe: %APPDATA%\OTScan3\scheduler.log.

Was trage ich wo ein?

Feld	Bedeutung
Name	Frei wählbarer Name des Plans (Buchstaben, Ziffern, _ . -).
Netzwerk	Ein in OTScan 3 angelegtes Netzwerk, zum Beispiel Montage_Anlagennetz.
Profil	Scan-Profil des Auftrags, zum Beispiel „Stufe 1 · Geräte finden (schonend, ohne Admin)“.
Portset	Liste der geprüften Ports; leer = Standard-Portset des Profils.
Rhythmus	täglich, wöchentlich oder monatlich.
Uhrzeit	Startzeit im Format HH:MM, zum Beispiel 02:30.
Tag	Bei wöchentlich der Wochentag (Mo bis So), bei monatlich der Tag 1 bis 28.



Zeitplan – wiederkehrende Scans



Zeitplan – wiederkehrende Scans

4.5 Erstinbetriebnahme und Erstabnahme

Ein neues Gerät beim Einbau prüfen und dokumentieren: Teil A am Gerät, Teil B im Zielnetzwerk, Protokoll und Paket.

Wozu?

Wenn ein Dienstleister bei der Erstinbetriebnahme ein neues OT-Gerät (Steuerung, Kamera, Gateway) einbaut, prüft OTScan 3 es schonend und nur lesend, gleicht Typenschild und Scan ab, führt die Prüflisten mit dem Dienstleister und erzeugt ein Abnahmepaket mit Protokoll, offenen Punkten und Prüfsummen. Teil A passiert direkt am Gerät, solange der Dienstleister vor Ort ist; Teil B ist die Erstabnahme im Zielnetzwerk nach dem Einbau.

Achtung

- Scannen Sie nur mit Einverständnis des Anlagenverantwortlichen. Für Sicherheitssteuerungen und empfindliche Geräte den Modus „schonend“ wählen.
- Teil-A/B-Scans sind Teilläufe: kein PDF-Scanbericht, keine PowerPoint, kein CMDB-Abgleich, kein Eintrag als Gesamtlauf im Verlauf.
- Unterschrift nur durch den Dienstleister; auf Betreiberseite ist keine Unterschrift nötig. Die ZIP bleibt lokal, solange kein gemeinsamer Ablageort zugelassen ist.
- Nach außen geht nur die Dienstleister-Fassung (ohne IP, MAC, Standort und Netzwerkname; IPs und MACs in Freitexten maskiert) mit den offenen Punkten. Empfänger und Anhänge vor dem Senden prüfen.

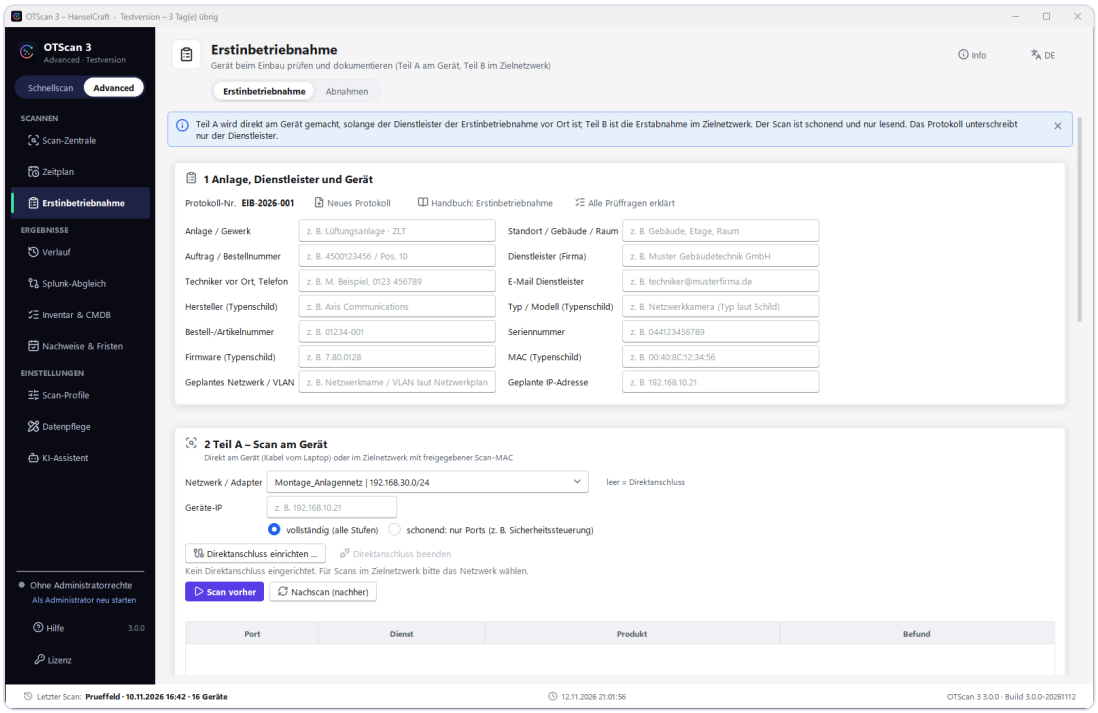
So geht's

1. Advanced → SCANNEN → „Erstinbetriebnahme“, oben Reiter „Erstinbetriebnahme“. Die Protokoll-Nr. (EIB-JJJJ-NNN) wird automatisch vergeben; „Neues Protokoll“ beginnt ein neues (mit Rückfrage).
2. 1 Anlage, Dienstleister und Gerät: Stammdaten eintragen (siehe „Was trage ich wo ein?“). Graue Beispieltexte zeigen, was in ein Feld gehört; sie verschwinden beim Hineinklicken und werden nie gespeichert.
3. Direkt am Gerät: Geräte-IP eintragen und „Direktanschluss einrichten …“ – OTScan 3 stellt den Laptop-Adapter auf eine freie Adresse im Netzwerk des Geräts und später wieder zurück (Bereich „Direktanschluss“).
4. 2 Teil A – Scan am Gerät: „Netzwerk / Adapter“ wählen (leer = Direktanschluss), Modus „vollständig (alle Stufen)“ oder „schonend: nur Ports (z. B. Sicherheitssteuerung)“, dann „Scan vorher“. Nach den Korrekturen des Dienstleisters „Nachscan (nachher)“.
5. Statustext und Tabelle lesen: offene Dienste, Befunde, Hersteller, Modell, Firmware, MAC und der Abgleich Typenschild ↔ Scan (✓ oder „≠ Scan: …“). Bei Kameras folgt automatisch die ONVIF-Abfrage. Befunde des ersten Scans werden als Vorschlag in „Offene Punkte“ übernommen.
6. 3 Prüfliste mit dem Dienstleister: je Frage ja, nein oder n. z. wählen und eine Bemerkung eintragen; dazu die Herstellerunterlagen (CRA-Konformität, IEC 62443, SBOM, Support-Ende, Härtungsleitfaden). Der Info-Punkt (i) erklärt jede Frage.
7. 4 Teil B – Erstabnahme im Zielnetzwerk: „Zielnetzwerk“ wählen, „Scan im Zielnetzwerk“. Der Statustext vergleicht mit Teil A („Im Zielnetzwerk zusätzlich offen: …“). Prüfliste B beantworten.
8. 5 Offene Punkte: je Zeile „Befund ; Maßnahme ; Frist“ – verantwortlich ist der Dienstleister.
9. 6 Abschluss: „Protokoll und Paket erzeugen“ (Ordner und ZIP unter Dokumente\OTScan3_Abnahmen\<Jahr>\EIB-JJJJ-NNN_<Typ>), „E-Mail-Entwürfe (Outlook)“ öffnet Outlook-Entwürfe – sie werden nie automatisch gesendet, „Sollzustand übernehmen“ (erscheint im Reiter „Abnahmen“), „Ablage öffnen“.
10. Vordrucke (Word) „Herstellerauskunft“ und „Erstinbetriebnahme/Erstabnahme“ liegen in Dokumente\OTScan3_Vorlagen.

Was trage ich wo ein?

Feld	Bedeutung
Anlage / Gewerk, Standort, Auftrag	Wo das Gerät eingebaut wird und zu welchem Auftrag es gehört.
Dienstleister (Firma), Techniker, E-Mail Dienstleister	Wer das Gerät einbaut; die E-Mail wird für den externen Mail-Entwurf genutzt.

Feld	Bedeutung
Hersteller, Typ, Artikelnummer, Seriennummer, Firmware, MAC	Angaben vom Typenschild; OTScan 3 gleicht MAC, Firmware und Hersteller mit dem Scan ab.
Geplantes Netzwerk / VLAN, geplante IP	Wo das Gerät nach dem Einbau hängen soll, zum Beispiel Halle3_CAM und 192.168.6.21.
Netzwerk / Adapter	Netzwerk für Teil A. Leer = Direktanschluss per Kabel vom Laptop.
Geräte-IP	Adresse des Geräts, zum Beispiel 192.168.6.21 (Typenschild, Dokumentation oder Dienstleister).
Modus	„vollständig (alle Stufen)“ oder „schonend: nur Ports“ für empfindliche Geräte.
Prüfliste	Je Frage ja / nein / n. z. und eine Bemerkung, zum Beispiel „Telnet und FTP aus“.
Zielnetzwerk	Netzwerk für Teil B, in dem das Gerät nach dem Einbau hängt.
Offene Punkte	Eine Zeile je Punkt: Befund ; Maßnahme ; Frist.



Erstinbetriebnahme und Erstabnahme

Berichte: Erstinbetriebnahme: Protokoll und Paket

Datei: `Dokumente/OTScan3_Abnahmen/<Jahr>/<Protokoll-Nr.>/ (ZIP, internes und externes PDF, offene Punkte)`

Wie erzeuge ich ihn?

1. Seite „Erstinbetriebnahme“ → „Protokoll und Paket erzeugen“.

Wie lese ich ihn?

- Internes Protokoll mit allen Angaben; externes PDF für den Dienstleister ohne Adressen; Liste offener Punkte mit Termin.

Woher kommen die Daten?

- Eingaben der Seite, Scan vorher/nachher am Gerät, Prüfliste.

Was sagt er nicht?

- Nur das externe PDF ist für Dritte gedacht.

4.6 Direktanschluss an eine Maschine

Laptop per Kabel direkt am Gerät: OTScan 3 richtet den Netzwerkadapter ein und stellt ihn danach zurück.

Wozu?

Bei der Ersterfassung hängt das Gerät oft noch nicht im Zielnetzwerk. Dann wird der Laptop direkt mit dem Gerät verbunden. Damit der Scan funktioniert, braucht der Laptop eine Adresse im Netzwerk des Geräts. OTScan 3 stellt dafür einen freien Adapter ein – ohne Gateway, die alte Einstellung wird gesichert – und stellt ihn danach wieder zurück. Firmen-LAN, WLAN, VPN und der Adapter einer laufenden Netzwerkkette werden nie angefasst.

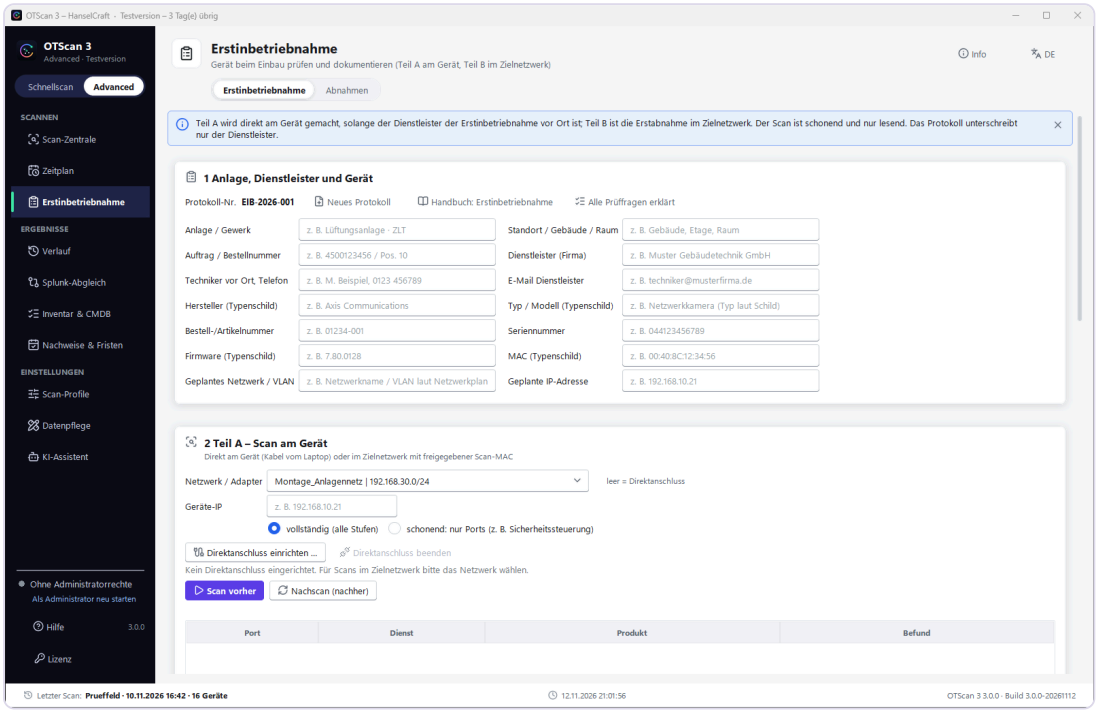
> **Achtung**
>
> - OTScan 3 muss mit Administratorrechten laufen, um den Adapter umzustellen.
> - Wählbar sind nur Adapter ohne Adresse oder mit 169.254.x.x, ohne Gateway, ohne Netzwerkkette und ohne Zuordnung zu einem OT-Netzwerk; WLAN, VPN und virtuelle Adapter nie.
> - Überschneidet sich das Gerätenetzwerk mit dem Netzwerk eines anderen Adapters, richtet OTScan 3 nichts ein – sonst liefe Firmen- oder Kettenverkehr über das Direktkabel.
> - Eine registrierte Scan-MAC ist nicht nötig – zwischen Laptop und Gerät liegt kein Firmennetzwerk.

So geht's

1. Laptop per Netzwerkkabel direkt mit dem Gerät verbinden (am besten über einen eigenen USB-Netzwerkadapter).
2. SCANNEN → Erstinbetriebnahme, Teil A: „Netzwerk / Adapter“ leer lassen und die „Geräte-IP“ eintragen (Typenschild, Dokumentation oder Dienstleister).
3. „Direktanschluss einrichten …“: Adapter wählen (nur geeignete sind wählbar), Präfix prüfen (meist /24), „Einrichten“. „Info“ oben rechts im Fenster erklärt jeden Punkt.
4. OTScan 3 sucht per ARP eine freie Adresse, stellt den Adapter im Hintergrund mit PowerShell ein und meldet, ob das Gerät antwortet und ob seine MAC zum Typenschild passt.
5. „Scan vorher“ – Korrekturen durch den Dienstleister – „Nachscan (nachher)“. Mit dem Haken stellt OTScan 3 den Adapter nach dem Nachscan automatisch zurück.
6. Sonst „Direktanschluss beenden“. Auch „Neues Protokoll“ und das Beenden von OTScan 3 stellen zurück; nach einem Absturz erscheint beim nächsten Öffnen ein Hinweis mit Knopf.
7. Im Protokoll steht je Teil „Anschluss: Direktanschluss über <Adapter> mit <Adresse>“ – in der Fassung für den Dienstleister ohne Adressen.

Was trage ich wo ein?

Feld	Bedeutung
Geräte-IP	Adresse des Geräts, zum Beispiel 192.168.6.21.
Adapter	Freier Netzwerkadapter des Laptops; nur geeignete sind wählbar.
Präfix	Netzmaske des Gerätenetzwerks, meist 24.
Haken „nach dem Nachscan zurückstellen“	Stellt den Adapter nach „Nachscan (nachher)“ automatisch wieder her.



Direktanschluss an eine Maschine

4.7 Abnahmen

Liste aller gespeicherten Erstinbetriebnahmen und Sollzustände mit Zugriff auf das Paket – Reiter „Abnahmen“ der Erstinbetriebnahme.

Wozu?

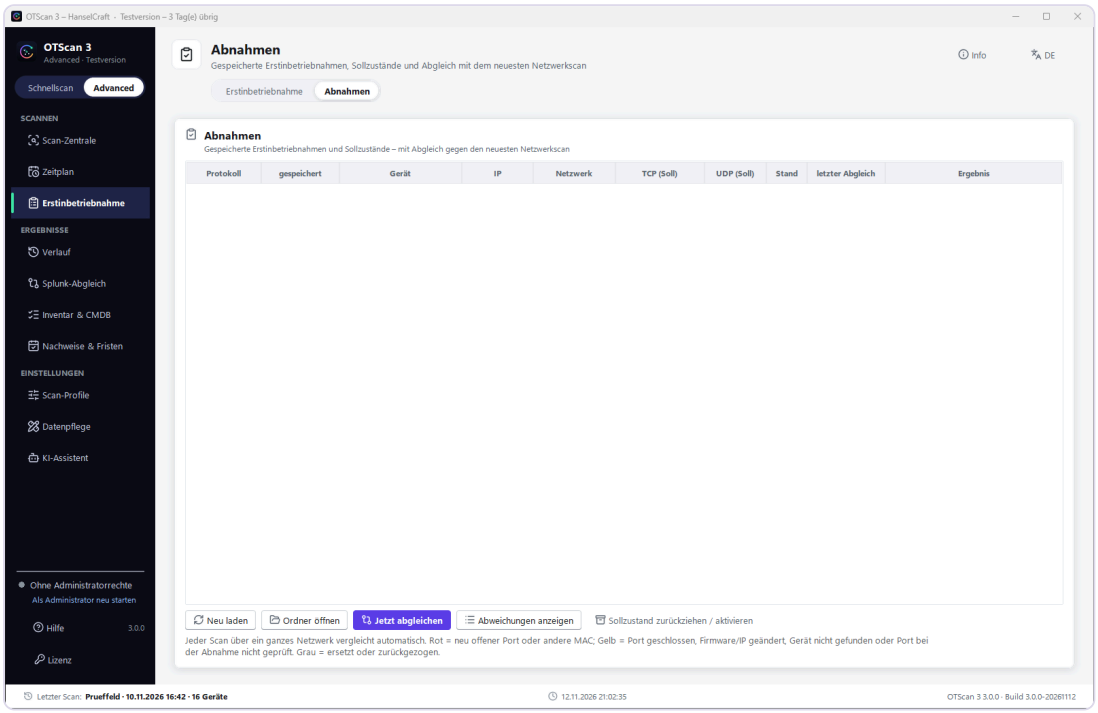
Der Reiter „Abnahmen“ zeigt jedes Protokoll der Erstinbetriebnahme, dessen Sollzustand übernommen wurde: Nummer, Datum, Gerät, IP, Netzwerk, die abgenommenen TCP- und UDP-Ports (Soll) und den Stand (Teil A oder Teil B). Von hier öffnen Sie den Paketordner. Der Sollzustand ist die Referenz für spätere Vergleiche.

Achtung

- Ein Eintrag entsteht nur über „Sollzustand übernehmen“ – nicht automatisch beim Paket.
- „Für diesen Eintrag wurde noch kein Paket gespeichert“ erscheint, wenn der Sollzustand vor „Protokoll und Paket erzeugen“ übernommen wurde.
- Sollzustände werden beim Löschen eines Netzwerks nicht automatisch entfernt.

So geht's

1. Advanced → SCANNEN → „Erstinbetriebnahme“ und oben den Reiter „Abnahmen“ wählen.
2. Spalten lesen: Protokoll, gespeichert, Gerät, IP, Netzwerk, TCP (Soll), UDP (Soll), Stand.
3. Eintrag markieren → „Ordner öffnen“ zeigt den Paketordner unter Dokumente\OTScan3_Abnahmen\<Jahr>. Ohne Auswahl öffnet sich der Basisordner.
4. „Neu laden“ aktualisiert die Liste, zum Beispiel nachdem im Reiter „Erstinbetriebnahme“ „Sollzustand übernehmen“ gedrückt wurde.
5. Einträge entfernen: EINSTELLUNGEN → Datenpflege → Reiter Stammdaten → „Abnahmen“, Eintrag markieren, „Löschen“ und Rückfrage bestätigen. Das Paket wandert in den Ordner _geloescht.



Abnahmen

5 Ergebnisse

5.1 Verlauf

Alle bisherigen Läufe mit Status, Dauer, Geräten und Ampel – wiederholen, vergleichen, nachscannen.

Wozu?

Der Verlauf ist das Gedächtnis des Programms: Jeder Lauf steht mit ID, Zeitpunkt, Netzwerk, CIDR, Profil, Portset, Adapter, Status, geplanter und tatsächlicher Dauer, Geräteanzahl und Risiko in der Liste. Hier erkennen Sie unvollständige Läufe, vergleichen zwei Läufe und legen Wiederholungen an.

Achtung

- Risiko zeigt „Grün – unauffällig“ oder „Gelb – Hinweise“. Sehr alte Läufe können noch „Rot – kritisch“ aus einer früheren Bewertung zeigen; die heutige Ampel kennt kein Rot.
- Das Vergleichsfenster des Verlaufs nutzt eine ältere Vorlaufwahl (auch Teilläufe). Maßgeblich ist die „Veränderung seit dem letzten Scan“ im Bericht.
- Datenbank und Verlauf liegen in %APPDATA%\OTScan3\otscan3.db und werden von allen Programmversionen dieses Benutzers geteilt.

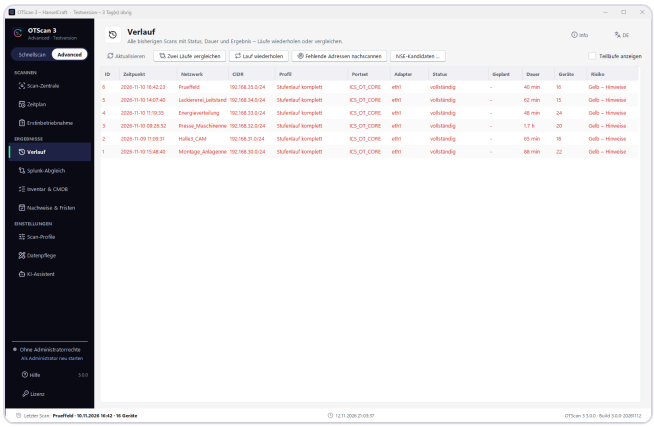
So geht's

1. Advanced → ERGEBNISSE → „Verlauf“. „Aktualisieren“ lädt die Liste neu.
2. Spalten lesen: Profil „Netzwerk komplett (Stufenlauf)“ = Stufenlauf, „Schnellscan“ = Schnellscan. Status: Vollständig (eventuell „(1 Host-Timeout)“), Abgebrochen, Gestoppt, Startfehler. Unvollständige Läufe stehen rot.
3. „Zwei Läufe vergleichen“: genau zwei Läufe markieren – zeigt neue, verschwundene und veränderte Geräte.
4. „Lauf wiederholen“: legt einen neuen Auftrag mit Netzwerk, CIDR, Zielen, Adapter, Profil und Portset des markierten Laufs an.
5. „Fehlende Adressen nachscannen“: für abgebrochene Einzelaufträge – scannt den Rest nach der zuletzt bearbeiteten Adresse. Angehaltene Stufenläufe stattdessen in der Scan-Zentrale mit „Stufenlauf fortsetzen“ weiterführen.
6. Haken „Teilläufe anzeigen“ blendet die Einzelschritte eines Stufenlaufs (S0, S0b, S1, S2a, S2b, NACH, Erstinbetriebnahme) ein; standardmäßig sind sie ausgeblendet.
7. Testläufe entfernen: Datenpflege → Reiter Stammdaten → „Verlauf“. Die Berichtsdateien bleiben erhalten.

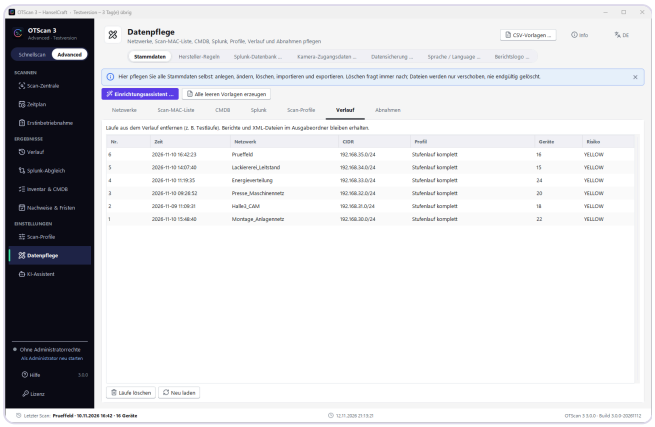
Was trage ich wo ein?

Feld	Bedeutung
Teilläufe anzeigen	Haken: zeigt auch die Einzelschritte eines Stufenlaufs.

Feld	Bedeutung
Markierung	Eine Zeile für „Lauf wiederholen“ oder „Fehlende Adressen nachscannen“, genau zwei Zeilen für „Zwei Läufe vergleichen“.



Verlauf



Verlauf

5.2 Splunk-Abgleich, Splunk-Ablage und Splunk-Datenbank

Firewall-Verkehr aus Splunk gegen den Scan halten: Geräte, die nur in Splunk sichtbar sind, Port-Lücken und gezielte Nachscans.

Wozu?

Die OT-Firewall (zum Beispiel FortiGate) protokolliert in einem Log-System (zum Beispiel Splunk), welche Geräte über die Firewall sprechen. Der Scan sieht, was antwortet. Der Abgleich bringt beides zusammen: Geräte, die der Scan übersehen hat (K3, K4, K6), Ports, die im Scan fehlen (K2a, K2b), und Scheinziele (K3b). Der Abgleich läuft automatisch mit jedem Netzwerkbericht, sobald Splunk-Daten in der Ablage liegen. Die Splunk-Ablage ist der Datenspeicher dafür, die Splunk-Datenbank ein Fenster für Fachleute.

Achtung

- Erst scannen, dann abgleichen: Verglichen wird mit bis zu drei jüngsten vollständigen Gesamtläufen des Netzwerks. Ohne solchen Lauf landen alle Splunk-Geräte in K3, K3b, K4 oder K6.
- Splunk sieht nur Verkehr über die Firewall, nicht innerhalb des Netzwerks. „Offen, aber über die Firewall nicht genutzt“ heißt nicht, dass ein Dienst unbenutzt ist – vor dem Abschalten mit dem Anlagenverantwortlichen klären.
- Splunk-Daten älter als 45 Tage werden im Netzwerkbericht nicht abgeglichen; Exporte älter als 14 Tage lösen eine Warnung aus. Fehlen Splunk-Daten, gilt ein Dienst nicht als „unsicher ohne Firewall-Verkehr“.
- Warnungen beachten: „keine abgewiesene Verbindung (deny)“, „Zeiträume überschneiden sich / Lücke“, „n Zeilen, laut _index.csv m“ (Datei verändert – neu exportieren).

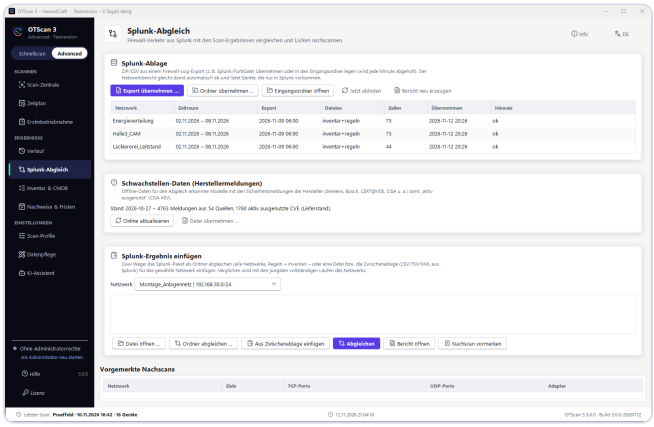
So geht's

1. Advanced → ERGEBNISSE → „Splunk-Abgleich“.

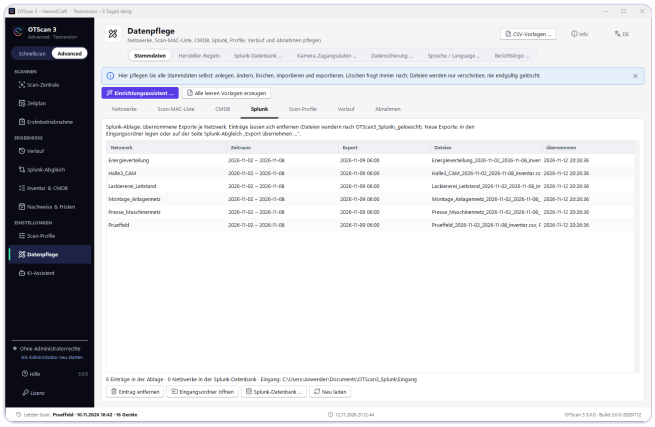
2. Daten hineingeben – Karte „Splunk-Ablage“: Export (ZIP oder CSV im Format „#FW-EXPORT v2“) in Dokumente\OTScan3_Splunk\Eingang legen – wird etwa alle 15 Sekunden abgeholt. Oder „Export übernehmen …“ bzw. „Ordner übernehmen …“; „Jetzt abholen“ holt sofort.
3. Die Tabelle der Ablage zeigt je Netzwerk Zeitraum, Export, Dateien, Zeilen, Übernommen und Hinweis. Die Daten liegen unter Dokumente\OTScan3_Splunk\Ablage\<Netzwerk>.
4. Netzwerknamen müssen in OTScan 3 genau so heißen wie in den Splunk-Dateien (zum Beispiel Montage_Anlagennetz), sonst wird das Netzwerk übersprungen.
5. Abgleich von Hand – Karte „Splunk-Ergebnis einfügen“: „Datei öffnen …“, „Ordner abgleichen …“ (alle Netzwerke) oder „Aus Zwischenablage einfügen“, dann „Abgleichen“.
6. „Bericht öffnen“ zeigt den Bericht je Netzwerk. „Nachscan vormerken“ übernimmt Ziele und Ports; „Alle vorgemerkten Nachscans starten“ reiht die Aufträge ein – nur in Absprache mit dem Anlagenverantwortlichen.
7. „Bericht neu erzeugen“ (Netzwerk in der Ablage markieren): erzeugt PDF, Excel, PowerPoint und CMDB-Nachtrag des jüngsten vollständigen Laufs mit den aktuellen Splunk-Daten neu.
8. Splunk-Datenbank: EINSTELLUNGEN → Datenpflege → Reiter „Splunk-Datenbank …“ öffnet das Fenster mit den hinterlegten Firewall-Exporten je Netzwerk (Netzwerk, CIDR, Flows, hochgeladen, Alter). Pflege etwa einmal jährlich.

Was trage ich wo ein?

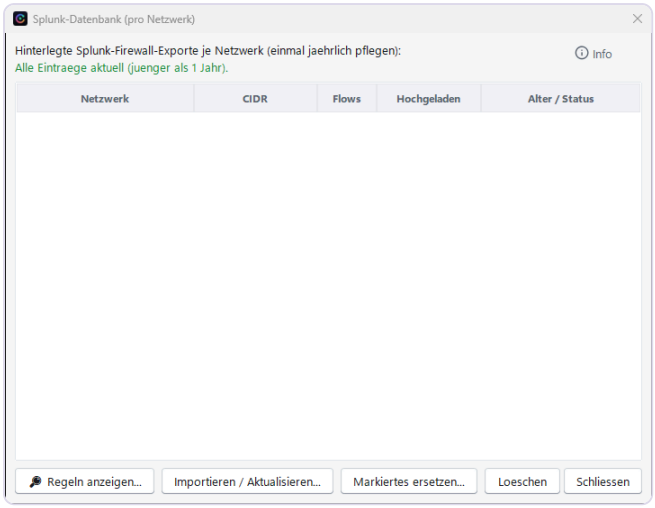
Feld	Bedeutung
Export übernehmen … / Ordner übernehmen …	Splunk-Export (ZIP oder CSV, Format #FW-EXPORT v2) bzw. einen Ordner mit Exporten wählen.
Datei öffnen … / Ordner abgleichen …	Regel-Datei eines Netzwerks oder einen Ordner mit allen Netzwerken für den Abgleich von Hand.
Aus Zwischenablage einfügen	Kopierte Splunk-Ergebniszeilen direkt einfügen.
Vorgemerkte Nachscans	Liste der Ziele und Ports für gezielte Nachscans; erst nach Absprache starten.



Splunk-Abgleich, Splunk-Ablage und Splunk-Datenbank



Splunk-Abgleich, Splunk-Ablage und Splunk-Datenbank



Splunk-Abgleich, Splunk-Ablage und Splunk-Datenbank

Berichte: CMDB-Nachtrag (Excel)

Datei: `<Netzwerk>_<Zeit>_stufenlauf_CMDB-Nachtrag.xlsx` · Muster ansehen: `assets/muster/Muster_07_CMDB-Nachtrag.xlsx`

Wie erzeuge ich ihn?

1. Entsteht, wenn Splunk Geräte zeigt, die weder im Scan noch in der CMDB stehen.

Wie lese ich ihn?

- Blatt „CMDB“ im Aufbau der Vorlage mit den gefundenen Adressen, Blatt „Suchhilfe“ mit Partnern, Ports und Zeitraum.

Woher kommen die Daten?

- Splunk-Inventar und Firewall-Verkehr des Netzwerks.

Was sagt er nicht?

- Die Geräte antworten nicht auf den Scan: vor Ort suchen (MAC, Switchport), bevor sie in die CMDB kommen.

Berichte: Geräte-Detailansicht (PDF)

Datei: `<Netzwerk>_<Zeit>_stufenlauf_Geraete-Details.pdf` · Muster ansehen: `assets/muster/Muster_09_Geraete-Detailansicht.pdf`

Wie erzeuge ich ihn?

1. Haken „Geräte-Detailansicht“ im Fenster „Berichte & Muster ...“.

Wie lese ich ihn?

- Eine Karte je Gerät: Scan-Angaben, Name und Ort aus der CMDB, kritische Ports im Klartext, Firewall-Kommunikation mit Quell-/Zielzone, Service, Policy, Aktion und Anzahl.
- Risk-Wert: 2 Punkte je kritischem Port (höchstens 8), +2 bei Herstellermeldung mit CVSS ≥ 7.

Woher kommen die Daten?

- Scan, CMDB, Splunk-Export (Zonen, Services, Policies) und Dokumentations-Datenbank.

Was sagt er nicht?

- Je Richtung nur die 5 häufigsten erlaubten Verbindungen und alle geblockten.

Berichte: Splunk-Abgleich (CSV und Bericht)

Datei: `Unterordner Splunk des Ausgabeordners: <Netzwerk>_splunkabgleich_<Zeit>.csv, _bericht.md, _ziele.txt, _nachscan.bat bzw. .sh`

Wie erzeuge ich ihn?

1. Seite „Splunk-Abgleich“: Export einfügen oder Datei/Ordner wählen und „Abgleichen“.

Wie lese ich ihn?

- Je IP eine Klasse K1–K6: bestätigt, Port-Lücke, nur Splunk (Server/Client), nur Scan, nur abgewiesen.
- Die Nachscan-Datei prüft gezielt die fehlenden Ports.

Woher kommen die Daten?

- Firewall-Export (z. B. Splunk-Suche über FortiGate-Logs) und die Scan-XML des Netzwerks.

Was sagt er nicht?

- Splunk sieht nur Verkehr über die Firewall.

5.3 CMDB-Abgleich

Scan-Ergebnisse mit der Inventar-Excel (CMDB) vergleichen – OK, MAC geändert, IP geändert, Offline, Neu. Reiter „CMDB-Abgleich“ in „Inventar & CMDB“.

Wozu?

Das Inventar (CMDB) ist die selbst gepflegte Inventar-Excel im Format der OTScan-3-Vorlage. Der Abgleich zeigt, welche Geräte im Scan und in der CMDB übereinstimmen, wo MAC oder IP abweichen, welche CMDB-Einträge nicht antworten (Offline) und welche Geräte neu sind. Die CMDB-Datei wird nur gelesen, nie verändert. Nach jedem Gesamtlauf läuft der Abgleich automatisch; der Reiter dient der Sicht und dem Export.

> **Achtung**
>
> - Das Original der CMDB bleibt immer unverändert. Änderungen übernehmen Sie selbst aus den erzeugten Kopien und Delta-Dateien.
> - „Offline“ heißt nur: im Scan nicht gefunden – ausgeschaltet, umgezogen oder stumm. „Neu“ = im Scan, nicht in der CMDB – prüfen und nachtragen.
> - Firmware wird als ganzes Wort verglichen; Leerraum und „V“- oder „Version“-Präfix werden normiert. Kameras liefern Firmware über ONVIF in den Abgleich.

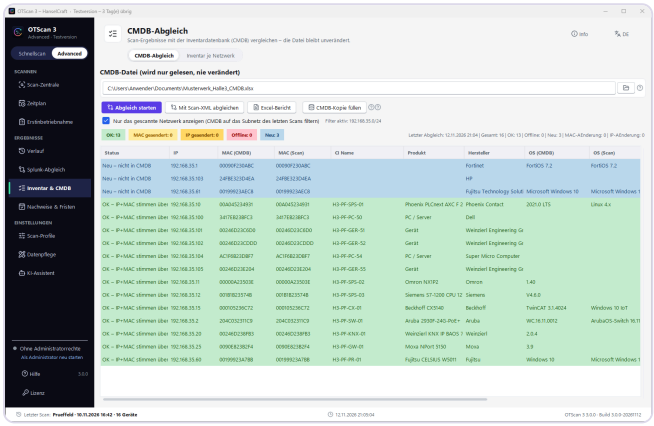
So geht's

1. Advanced → ERGEBNISSE → „Inventar & CMDB“ und oben den Reiter „CMDB-Abgleich“ wählen.
2. CMDB-Datei mit „...“ wählen: Excel mit Blatt „CMDB“, Daten ab Zeile 18 (IP in Spalte AB, MAC in Spalte AF, CI-Name in Spalte B).
3. „Abgleich starten“ vergleicht den letzten gespeicherten Scan; „Mit Scan-XML abgleichen“ nimmt eine beliebige Ergebnisdatei.
4. Haken „Nur das gescannte Netzwerk anzeigen“ blendet CMDB-Einträge anderer Netzwerke aus.
5. Lesen: Zähler oben (OK, MAC geändert, IP geändert, Offline, Neu); die Tabelle zeigt je Gerät Status (farbig), IP, MAC laut CMDB und Scan, CI-Name, Produkt, Hersteller, Betriebssystem, Gebäude/Raum, Gewerk und offene Ports.

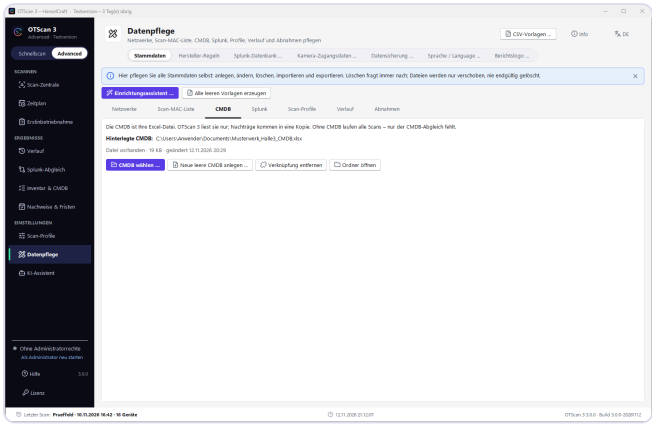
6. „Excel-Bericht“ speichert den farbigen Abgleich mit Blatt „Statistik“. „CMDB-Kopie füllen“ erzeugt eine Kopie der CMDB im Originalformat mit Scan-Daten in leeren Feldern.
7. Automatisch nach jedem vollständigen Lauf „Netzwerk komplett“ entstehen zusätzlich <Bericht>_CMDB-Delta.xlsx und – mit Splunk-Daten – <Bericht>_CMDB-Nachtrag.xlsx.

Was trage ich wo ein?

Feld	Bedeutung
CMDB-Datei	Pfad zur Inventar-Excel (Blatt „CMDB“, Daten ab Zeile 18).
Nur das gescannte Netzwerk anzeigen	Haken: filtert die CMDB auf das Subnetz des letzten Scans.



CMDB-Abgleich



CMDB-Abgleich

Berichte: CMDB-Delta (Excel)

Datei: `<Netzwerk>_<Zeit>_stufenlauf_CMDB-Delta.xlsx` · Muster ansehen: `assets/muster/Muster_06_CMDB-Delta.xlsx`

Wie erzeuge ich ihn?

1. Entsteht immer nach einem vollständigen Lauf, wenn eine CMDB hinterlegt ist.

Wie lese ich ihn?

- Blatt „Delta-Übersicht“: neu (grün), geändert (orange), fehlt im Scan (grau), Hinweise (blau).
- Blatt „CMDB“ hat das Format der CMDB-Vorlage – geprüfte Zeilen in die eigene CMDB übernehmen.

Woher kommen die Daten?

- Scan des Netzwerks gegen die hinterlegte CMDB-Datei (nur gelesen).

Was sagt er nicht?

- Andere offene Ports hängen von der Portauswahl des Laufs ab und sind nur Hinweise.

5.4 Inventar je Netzwerk

Alle gefundenen Geräte eines Netzwerks in einer Liste – mit Name, Hersteller, MAC und offenen Diensten. Reiter „Inventar je Netzwerk“ in „Inventar & CMDB“.

Wozu?

Das Inventar fasst die Scan-Ergebnisse eines Netzwerks zu einer Zeile je Gerät zusammen. Es entsteht automatisch am Ende jedes Stufenlaufs und Schnellscans und lässt sich von Hand über alle Scans eines

Netzwerks neu aufbauen. Es ist die Grundlage für die CMDB-Pflege und das Gesamtinventar über alle Netzwerke.

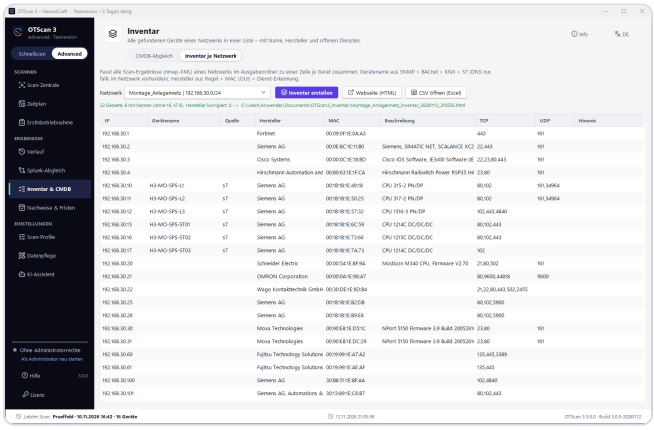
> **Achtung**
>
> - Gerätenamen kommen nur aus SNMP, BACnet und KNX; in Anlagennetzwerken gibt es meist kein DNS. Geräte ohne diese Dienste bleiben namenlos.
> - Die eigenen Adapter-Adressen des Scan-Laptops sind ausgeschlossen. Kameras erscheinen als „IP-Kamera (ONVIF)“, wenn die CAM-Stufe gelaufen ist.
> - Das Inventar fasst zusammen, was geantwortet hat – es ist keine Bewertung und kein Ersatz für die CMDB.

So geht's

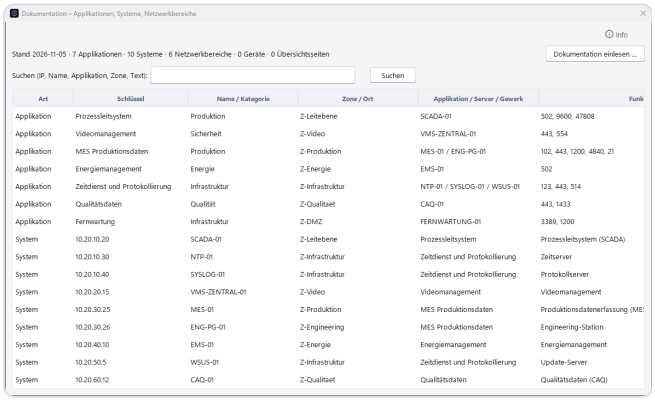
1. Advanced → ERGEBNISSE → „Inventar & CMDB“ und oben den Reiter „Inventar je Netzwerk“ wählen.
2. Netzwerk wählen und „Inventar erstellen“ drücken – fasst alle Scan-Ergebnisse dieses Netzwerks im Ausgabeordner zusammen.
3. Spalten lesen: IP, Gerätename, Quelle des Namens (SNMP vor BACnet vor KNX vor S7 vor DNS), Hersteller (Regel vor MAC-OUI vor Dienst-Erkennung), MAC, Beschreibung, TCP, UDP, Hinweis.
4. „Webseite (HTML)“ öffnet das Inventar im Browser, „CSV öffnen (Excel)“ in der Tabellenkalkulation. Ablage: Dokumente\OTScan3_Inventar (CSV und HTML je Netzwerk).
5. Falsch erkannte Hersteller dauerhaft über die Hersteller-Regeln korrigieren (Datenpflege → Reiter „Hersteller-Regeln“) und das Inventar neu erstellen.
6. Gesamtinventar über alle Netzwerke: Scan-Zentrale → „Ausgabe und Berichte“ → „Gesamtinventar jetzt erstellen“ (siehe „Berichte und Dokumente“).

Was trage ich wo ein?

Feld	Bedeutung
Netzwerk	Das Netzwerk, dessen Scans zusammengefasst werden.



Inventar je Netzwerk



Inventar je Netzwerk

Berichte: Gesamtinventar CMDB · Scan · Splunk (Excel)

Datei: `OTScan3_Gesamtinventar_<Datum>.xlsx im Ausgabeordner` · Muster ansehen: `assets/muster/Muster_10_Gesamtinventar.xlsx`

Wie erzeuge ich ihn?

1. Haken „Gesamtinventar“ im Fenster „Berichte & Muster …“ oder Knopf „Gesamtinventar jetzt erstellen“.

Wie lese ich ihn?

- Blatt „Übersicht“: Anzahl je Inventar-Status mit „Was tun?“. Blatt „Gesamtinventar“: eine Zeile je Gerät, je Wert mit Quelle (CMDB, SCAN, SPLUNK).

Woher kommen die Daten?

- CMDB, neuester vollständiger Stufenlauf je Netzwerk und neuestes Splunk-Inventar je Netzwerk.

Was sagt er nicht?

- Netzwerke ohne vollständigen Lauf erscheinen als „Netzwerk offen“.

Berichte: Geräteverzeichnis (PDF)

Datei: `OTScan3_Geraeteverzeichnis_<Datum>.pdf` · Muster ansehen: `assets/muster/Muster_12_Geraeteverzeichnis.pdf`

Wie erzeuge ich ihn?

1. Haken „Geräteverzeichnis“; entsteht zusammen mit dem Standortbericht.

Wie lese ich ihn?

- Alle Geräte aller Netzwerke, eine Zeile je Gerät (Querformat), mit Inventar-Status.

Woher kommen die Daten?

- Gesamtinventar.

Was sagt er nicht?

- Enthält alle Adressen – vertraulich behandeln.

Berichte: Inventar je Netzwerk (HTML/CSV)

Datei: `Dokumente/OTScan3_Inventar/<Netzwerk>_inventar_<Zeit>.html und .csv`

Wie erzeuge ich ihn?

1. Inventar & CMDB → Reiter „Inventar je Netzwerk“ → „Inventar erstellen“; entsteht auch am Ende jedes Stufenlaufs.

Wie lese ich ihn?

- Eine Zeile je Gerät mit Namen, Quelle des Namens, Hersteller, MAC, Beschreibung und offenen Ports.

Woher kommen die Daten?

- Alle Scan-Dateien des Netzwerks im Ausgabeordner, Hersteller-Regeln.

Was sagt er nicht?

- Ohne CMDB-Abgleich – dafür CMDB-Delta oder Gesamtinventar nutzen.

5.5 Herstellermeldungen (CSAF) und Maßnahmenliste

Erkannte Modelle und Firmware-Stände offline gegen Sicherheitsmeldungen der Hersteller abgleichen und als Maßnahmen ausgeben.

Wozu?

Im Stufenlauf erkannte Modelle und Firmware-Stände (S7, BACnet, KNX, CODESYS, SNMP, ONVIF bei Kameras) werden mit einem Offline-Index der Sicherheitsmeldungen (CSAF 2.0) von Siemens ProductCERT, CERT@VDE, Bosch PSIRT, CISA ICS und weiteren abgeglichen, ergänzt um „aktiv ausgenutzt“ (CISA KEV) und die Ausnutzungswahrscheinlichkeit (EPSS). Das Ergebnis steht im PDF-Abschnitt „Bekannte Schwachstellen“, im Excel-Blatt „Schwachstellen“ und in der Maßnahmenliste.

Achtung

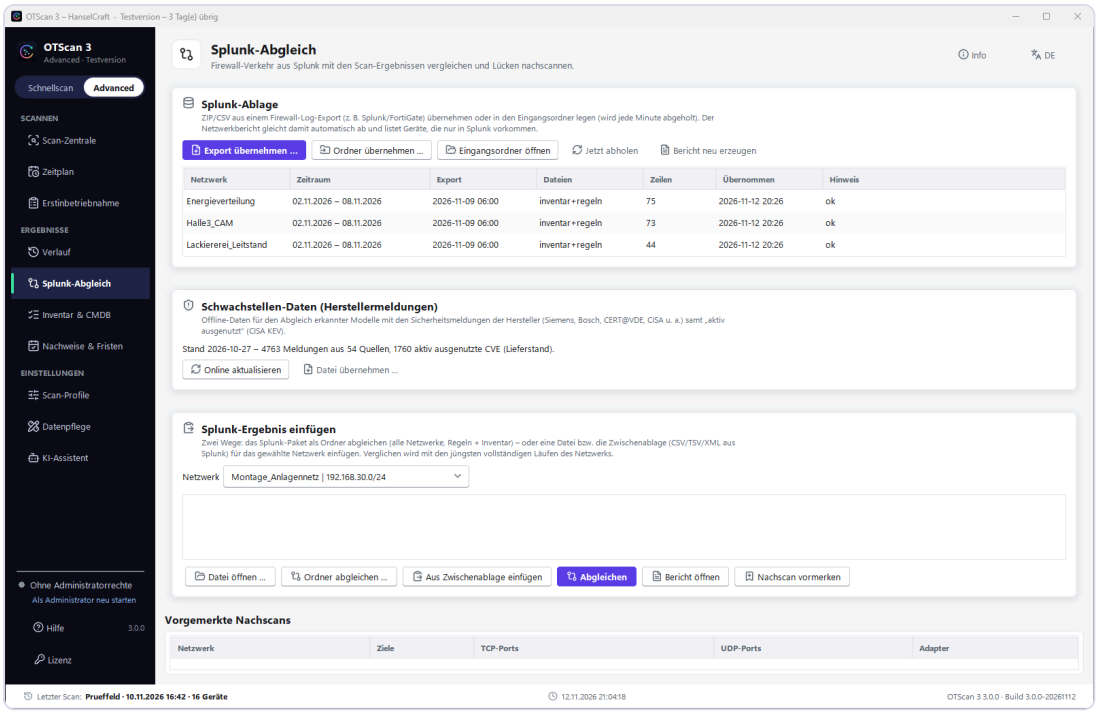
- Dringlichkeit in der Maßnahmenliste bedeutet, wie leicht sich etwas abstellen lässt – nicht das Risiko.
- Treffer „Modell“ und „Hersteller“ immer am Gerät prüfen; der Index ersetzt nicht die Original-Meldung (Link in der Excel). Ohne erkanntes Modell kann ein Gerät nicht geprüft werden.
- Der Online-Abruf ist die einzige Funktion, die ins Internet geht – und nur auf Klick. Auf dem Scan-PC ohne Internet den Dateiweg nutzen.

So geht's

1. Advanced → ERGEBNISSE → „Splunk-Abgleich“ → Karte „Schwachstellen-Daten (Herstellermeldungen)“.
2. Index aktualisieren: „Online aktualisieren“ (nur auf einem PC mit Internet) oder „Datei übernehmen ...“ mit otsp_csaf_index.json.gz, die auf einem Internet-PC mit otsp_csaf_sync.py --aus <Ordner> erzeugt wurde.
3. Datenstand prüfen: Das Feld „erstellt“ zeigt das Datum des Index. Er liegt in %APPDATA%\OTScan3\csaf\otsp_csaf_index.json.gz.
4. Stufenlauf laufen lassen – der Abgleich passiert automatisch beim Erzeugen der Berichte. Nach einem Index-Update vorhandene Berichte neu erzeugen.
5. Lesen: Güte „exakt“ = Firmware liegt nachweislich im betroffenen Bereich; „Modell“ = Modell passt, Version offen – am Gerät prüfen; „Hersteller“ = nur schwacher Hinweis.
6. Maßnahmenliste <Bericht>_Massnahmen.xlsx öffnen: eine Zeile je unsicherem Dienst und je Herstellermeldung mit CMDB-Name, Ort, Gewerk, Dringlichkeit, Firewall-Verkehr und den Spalten Verantwortlich, Termin, Status und Bemerkung zum Abarbeiten.

Was trage ich wo ein?

Feld	Bedeutung
Datei übernehmen ...	Index-Datei otsp_csaf_index.json.gz von einem Internet-PC wählen.
Verantwortlich, Termin, Status, Bemerkung	Spalten der Maßnahmenliste zum Abarbeiten (Status als Auswahlliste).



Herstellermeldungen (CSAF) und Maßnahmenliste

Berichte: Maßnahmenliste (Excel)

Datei: `<Netzwerk>_<Zeit>_stufenlauf_Massnahmen.xlsx` · Muster ansehen: `assets/muster/Muster_05_Massnahmen.xlsx`

Wie erzeuge ich ihn?

1. Entsteht immer nach einem vollständigen Lauf.

Wie lese ich ihn?

- Eine Zeile je Gerät und Befund: Dringlichkeit, IP, Gerät, Hersteller, Modell/Firmware, Name/Ort/Gewerk aus der CMDB, Was, Verkehr über Firewall, Empfehlung.
- Die Spalten Verantwortlich bis Bemerkung sind zum Abhaken gedacht.

Woher kommen die Daten?

- Unsichere Dienste aus dem Scan, Herstellermeldungen aus dem CSAF-Bestand, Ort und Verantwortliche aus der CMDB, Verkehr aus Splunk.

Was sagt er nicht?

- Dringlichkeit sagt, wie schnell und leicht sich etwas abstellen lässt – nicht, wie groß das Risiko ist.

5.6 Berichte und Dokumente

Welche Berichte es gibt, wo sie liegen, wie Sie sie erzeugen, öffnen und lesen – mit dem Fenster „Berichte & Muster …“.

Wozu?

Nach jedem vollständigen Lauf erzeugt OTScan 3 Berichte für verschiedene Leser: PDF für Anlagenverantwortliche, Excel für die Technik, PowerPoint fürs Management, Maßnahmenliste für die Gewerke. Dazu kommen PDF-Berichte je Netzwerk (Netzwerk-Check, Geräte-Detailansicht), über alle

Netzwerke (Standortbericht, Geräteverzeichnis) und das Gesamtinventar als Excel. Im Fenster „Berichte & Muster …“ wählen Sie, welche Berichte entstehen, und sehen sich anonymisierte Muster an.

Achtung

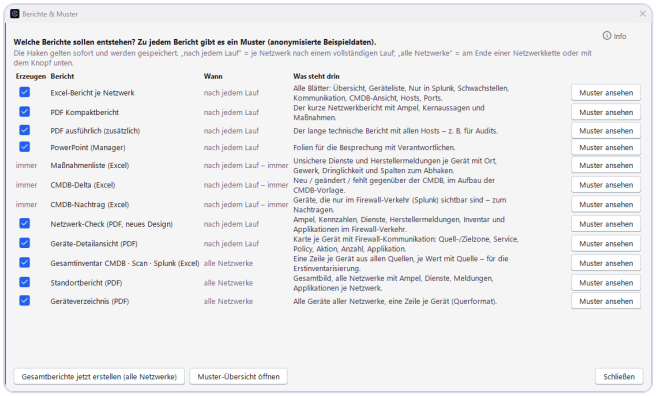
- Die neuen PDF-Berichte (Netzwerk-Check, Geräte-Detailansicht, Standortbericht, Geräteverzeichnis) erzeugt OTScan 3 im Hintergrund über Microsoft Edge.
- Alle Berichte sind vertraulich und enthalten IP- und MAC-Adressen. Nach außen nur Unterlagen ohne Adressen und Standort geben.
- Teilläufe (einzelne Stufen, Teil-A/B-Scans) erzeugen keinen Gesamtbericht. Es gibt genau einen Bericht je vollständigem Lauf.
- Während ein Bericht entsteht (bis zu einer Minute), die Dateien im Ausgabeordner nicht öffnen oder verschieben.

So geht's

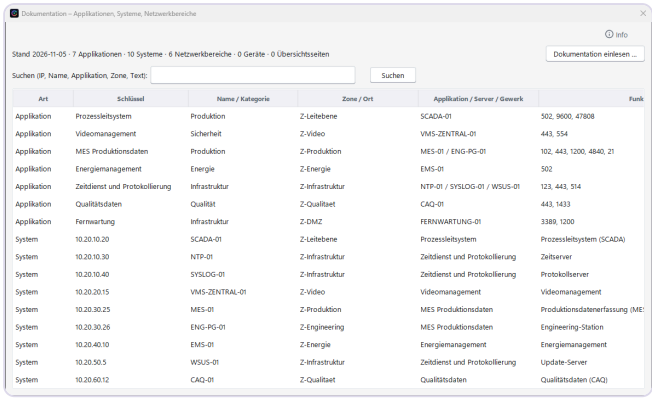
1. Advanced → SCANNEN → Scan-Zentrale → „Ausgabe und Berichte“ aufklappen. Ausgabeordner prüfen (Standard Dokumente).
2. Haken „Nach jedem Scan erzeugen“ für Excel, PDF und PowerPoint setzen; „PDF ausführlich zusätzlich“ nur bei Bedarf (für Audits).
3. „Berichte & Muster …“ öffnen: Alle Berichtsarten stehen mit Haken da. Haken setzen für Netzwerk-Check, Geräte-Detailansicht, Standortbericht, Geräteverzeichnis und Gesamtinventar.
4. „Muster ansehen“ zeigt zu jeder Berichtsart eine anonymisierte Beispieldatei – so sehen Sie vorher, was Sie bekommen.
5. Erzeugen: Die gewählten Berichte entstehen automatisch am Ende jedes Gesamtlaufs. Von Hand: Auftrag in der Warteschlange markieren → „Berichte für markierten Auftrag neu erzeugen“, oder „Berichte aus XML erzeugen“, oder „Gesamtinventar jetzt erstellen“.
6. Öffnen: Im Ausgabeordner tragen die Dateien Netzwerkname und Zeit im Namen, zum Beispiel Halle3_CAM_<Zeit>_stufenlauf.pdf. Im Schnellscan gibt es die Knöpfe „Bericht öffnen (PDF)“, „Excel“ und „Kurzbericht (HTML)“.
7. Weitere Ablagen: Inventar in Dokumente\OTScan3_Inventar, Splunk-Abgleich im Unterordner Splunk des Ausgabeordners, Erstinbetriebnahme-Pakete in Dokumente\OTScan3_Abnahmen\<Jahr>, Vorlagen in Dokumente\OTScan3_Vorlagen.
8. Lesen: Beim PDF zuerst Seite 1 (Ampel, das Wichtigste, was ist zu tun). Steht „UNVOLLSTAENDIG“ in der Fußzeile, den Scan wiederholen, bevor Sie Schlüsse ziehen.
9. Jeder Bericht ist im Info-Fenster beschrieben: „Info“ → Thema „Berichte und Dokumente“ – oder in diesem Handbuch im Teil Berichte.

Was trage ich wo ein?

Feld	Bedeutung
Ausgabeordner	Ordner für alle Berichte eines Laufs. Standard: Dokumente.
Nach jedem Scan erzeugen	Haken je Format: Excel, PDF, PowerPoint.
PDF ausführlich zusätzlich	Legt neben dem Kompaktbericht den langen Bericht ab.
Haken in „Berichte & Muster …“	Wählt Netzwerk-Check, Geräte-Detailansicht, Standortbericht, Geräteverzeichnis und Gesamtinventar.



Berichte und Dokumente



Berichte und Dokumente

Berichte: PDF-Kompaktbericht

Datei: `<Netzwerk>_<Zeit>_stufenlauf.pdf im Ausgabeordner (Standard: Dokumente)` · Muster ansehen: `assets/muster/Muster_02_PDF_Kompakt.pdf`

Wie erzeuge ich ihn?

1. Entsteht am Ende jedes vollständigen Laufs, wenn unter „Ausgabe und Berichte“ der Haken für PDF gesetzt ist.
2. Von Hand: Auftrag markieren → „Berichte für markierten Auftrag neu erzeugen“.

Wie lese ich ihn?

- Seite 1: Ampel, Kennzahlen, „Das Wichtigste“ und „Was ist zu tun?“ – das reicht für Anlagenverantwortliche.
- Danach die Tabelle „Unsichere Dienste“: je Dienst Anzahl Geräte, warum riskant, was tun.

Woher kommen die Daten?

- Scan-Ergebnis (nmap-XML) des Laufs, bewertet nach den Verkehrsregeln (HanselCraft-Voreinstellung, anpassbar).
- Splunk-Zeitraum und „nur im Firewall-Verkehr“ aus der Splunk-Ablage, CMDB-Bezug aus der hinterlegten CMDB.

Was sagt er nicht?

- Ein unsicherer Dienst ist eine offene Tür, kein Angriff.
- Verkehr innerhalb eines Netzwerks sieht Splunk nicht – „ohne Firewall-Verkehr“ heißt nicht „unbenutzt“.

Berichte: PDF ausführlich

Datei: `<Netzwerk>_<Zeit>_stufenlauf_ausfuehrlich.pdf` · Muster ansehen: `assets/muster/Muster_03_PDF_ausfuehrlich.pdf`

Wie erzeuge ich ihn?

1. Haken „PDF ausführlich (zusätzlich)“ im Fenster „Berichte & Muster …“.
2. Entsteht neben dem Kompaktbericht.

Wie lese ich ihn?

- Für Audits und Fachleute: Zusammenfassung, Heatmap nach Subnetz und Gerätetyp, kritische Hosts, vollständiges Host-Inventar.
- Kapitel „Technische Details“ nennt Profil, Portset und nmap-Version.

Woher kommen die Daten?

- Dieselbe Scan-XML wie der Kompaktbericht.

Was sagt er nicht?

- Lang (viele Seiten bei großen Netzwerken); für Besprechungen lieber Kompaktbericht oder PowerPoint.

Berichte: Excel-Bericht je Netzwerk

Datei: `<Netzwerk>_<Zeit>_stufenlauf.xlsx` · Muster ansehen: `assets/muster/Muster_01_Excel_Netzwerk.xlsx`

Wie erzeuge ich ihn?

1. Haken für Excel unter „Ausgabe und Berichte“; entsteht nach jedem vollständigen Lauf.

Wie lese ich ihn?

- Blätter: Übersicht, Geräteliste, Nur in Splunk, Schwachstellen, Kommunikation, CMDB-Ansicht, Shadow (nicht in der CMDB), Hosts, Ports, Scripts.
- Filter in der Geräteliste setzen, z. B. auf „Unsichere Dienste“ oder Hersteller.

Woher kommen die Daten?

- Scan-XML, Splunk-Ablage, CMDB und Herstellermeldungen (CSAF-Bestand).

Was sagt er nicht?

- Arbeitsdatei für die Technik; enthält alle Adressen – nicht nach außen geben.

Berichte: PowerPoint (Manager)

Datei: `<Netzwerk>_<Zeit>_stufenlauf_manager.pptx` · Muster ansehen: `assets/muster/Muster_04_PowerPoint_Manager.pptx`

Wie erzeuge ich ihn?

1. Haken für PowerPoint unter „Ausgabe und Berichte“.

Wie lese ich ihn?

- Wenige Folien mit Ampel, Kennzahlen und den wichtigsten Maßnahmen – für die Besprechung mit Verantwortlichen.

Woher kommen die Daten?

- Dieselben Daten wie der Kompaktbericht.

Was sagt er nicht?

- Bewusst verkürzt; Einzelheiten stehen im PDF und in Excel.

Berichte: Netzwerk-Check (PDF)

Datei: `<Netzwerk>_<Zeit>_stufenlauf_Netzwerk-Check.pdf` · Muster ansehen: `assets/muster/Muster_08_Netzwerk-Check.pdf`

Wie erzeuge ich ihn?

1. Haken „Netzwerk-Check“ im Fenster „Berichte & Muster …“; entsteht im Hintergrund nach jedem vollständigen Lauf.

Wie lese ich ihn?

- Deckblatt mit Ampel, dann „Auf einen Blick“, Dienste, Herstellermeldungen, Inventarstatus und Applikationen im Firewall-Verkehr.

Woher kommen die Daten?

- Lauf-Excel, Maßnahmenliste, Gesamtinventar, Splunk-Ablage und Dokumentations-Datenbank.

Was sagt er nicht?

- Braucht Microsoft Edge, Google Chrome oder Chromium für die PDF-Ausgabe; ohne Browser bleibt eine HTML-Datei.

Berichte: Standortbericht (PDF)

Datei: `OTScan3_Standortbericht_<Datum>.pdf` · Muster ansehen: `assets/muster/Muster_11_Standortbericht.pdf`

Wie erzeuge ich ihn?

1. Haken „Standortbericht“; entsteht am Ende einer Netzwerkkette oder mit „Gesamtberichte jetzt erstellen (alle Netzwerke)“.

Wie lese ich ihn?

- Gesamtbild aller Netzwerke mit Ampel, häufigste Dienste, Herstellermeldungen und Applikationen je Netzwerk.

Woher kommen die Daten?

- Neuester vollständiger Lauf je Netzwerk, Gesamtinventar, Splunk-Ablage, Dokumentations-Datenbank.

Was sagt er nicht?

- Ältere Läufe einzelner Netzwerke fließen mit ihrem Stand ein – Datum je Netzwerk beachten.

5.7 Nachweise & Fristen

Wiederkehrende Pflichten rund um die OT-Sicherheit mit Zyklus, nächster Fälligkeit und Ampel – z. B. als Gedächtnisstütze für Nachweise nach NIS-2 oder IEC 62443.

Wozu?

Viele Aufgaben im OT-Betrieb wiederholen sich: Inventur, Wiederholungsscan, Prüfung der Fernwartungszugänge, Firewall-Regeln, Firmwarestände, Sicherungen, Notfallübung, Unterweisung. Die Seite merkt sich für jede Pflicht, wann sie zuletzt erledigt wurde, berechnet die nächste Fälligkeit und zeigt, was überfällig (rot) oder in den nächsten 30 Tagen fällig ist (gelb). Jede Erledigung bleibt im Verlauf sichtbar – so können Sie zeigen, dass regelmäßig geprüft wurde.

Achtung

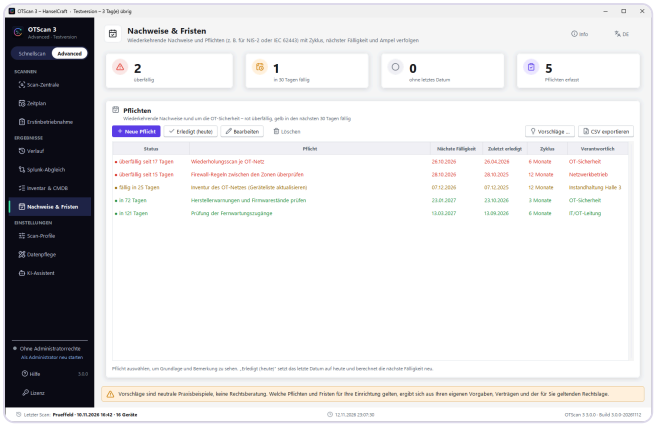
- Die Vorschläge sind neutrale Praxisbeispiele, keine Rechtsberatung. Welche Pflichten und Fristen für Ihre Einrichtung gelten (etwa nach NIS-2 bzw. BSI-Gesetz), ergibt sich aus Ihren eigenen Vorgaben, Verträgen und der für Sie geltenden Rechtslage.
- OTScan 3 erinnert nicht per Mail – die Ampel sehen Sie auf dieser Seite und über den KI-Assistenten.
- Die Pflichten liegen in der Datenbank von OTScan 3 und werden von der Datensicherung mitgenommen. „Löschen“ entfernt eine Pflicht samt Verlauf.

So geht's

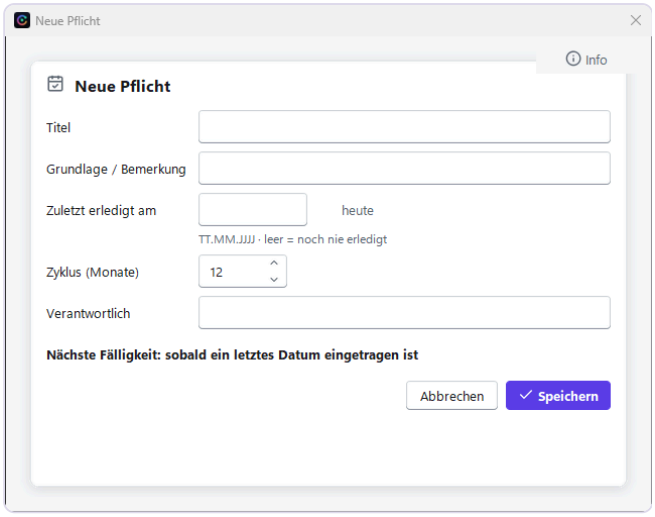
1. Advanced → ERGEBNISSE → „Nachweise & Fristen“ öffnen.
2. „Vorschläge …“ wählen, passende Praxisbeispiele anhaken und „Übernehmen“ – oder mit „Neue Pflicht“ eine eigene anlegen.
3. Pflicht doppelt anklicken (oder „Bearbeiten“) und Zyklus in Monaten, Verantwortlich und das Datum der letzten Erledigung eintragen. Die nächste Fälligkeit erscheint sofort im Dialog.
4. Nach getaner Arbeit die Pflicht markieren und „Erledigt (heute)“ wählen. Das Datum wird übernommen, die nächste Fälligkeit neu berechnet, das vorige Datum bleibt im Verlauf.
5. „CSV exportieren“ speichert die Liste mit allen bisherigen Daten für Excel, z. B. als Anlage zu einem Prüfbericht.

Was trage ich wo ein?

Feld	Bedeutung
Titel	Kurzname der Pflicht, z. B. „Prüfung der Fernwartungszugänge“.
Grundlage / Bemerkung	Woher die Pflicht kommt (eigene Richtlinie, Vertrag, Norm) und was zu tun ist.
Zuletzt erledigt am	Datum TT.MM.JJJJ; leer = noch nie erledigt (gelb, „noch kein Datum“).
Zyklus (Monate)	1 bis 120 Monate bis zur nächsten Fälligkeit.
Verantwortlich	Person oder Rolle, die die Pflicht erledigt.
Ampel	Rot = überfällig, Gelb = in den nächsten 30 Tagen fällig oder noch ohne Datum, Grün = später fällig.



Nachweise & Fristen



Nachweise & Fristen

6 Einstellungen

6.1 Datenpflege – alle Stammdaten selbst pflegen

Netzwerke, Scan-MAC-Liste, CMDB, Splunk, Profile, Verlauf und Abnahmen anlegen, ändern, löschen, importieren und exportieren – dazu Hersteller-Regeln, Splunk-Datenbank und Kamera-Zugangsdaten.

Wozu?

Alle Daten, die OTScan 3 braucht, pflegen Sie an einer Stelle selbst – ohne Dateien von Hand zu bearbeiten. Exporte haben das Importformat und lassen sich wieder einlesen. Löschen fragt immer nach; Dateien (Splunk-Exporte, Abnahme-Pakete) werden nur in einen Ordner _geloescht verschoben.

Achtung

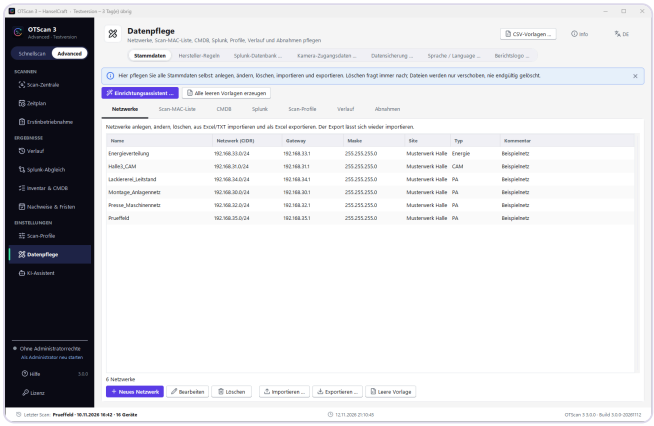
- Die Scan-MAC-Liste nicht ändern, während eine Netzwerkkette läuft.
- Ein Netzwerk zu löschen löscht keine Scan-Ergebnisse und keinen Verlauf.
- Standardprofile werden bei jedem Start neu angelegt und lassen sich deshalb nicht löschen.

So geht's

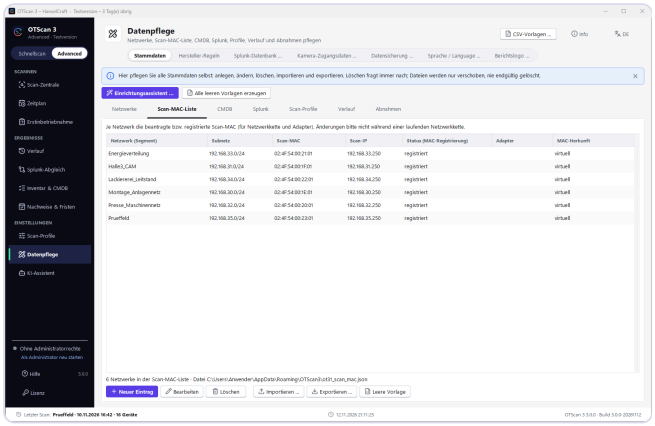
1. Advanced → EINSTELLUNGEN → „Datenpflege“. Oben stehen die Reiter „Stammdaten“, „Hersteller-Regeln“, „Splunk-Datenbank …“ und „Kamera-Zugangsdaten …“ (die letzten beiden öffnen Fenster).
2. Im Reiter „Stammdaten“ gibt es die inneren Reiter Netzwerke, Scan-MAC-Liste, CMDB, Splunk, Scan-Profile, Verlauf und Abnahmen.
3. Netzwerke: „Neues Netzwerk“, „Bearbeiten“ (oder Doppelklick), „Löschen“ (Mehrfachauswahl), „Importieren …“, „Exportieren …“, „Leere Vorlage“ – Einzelheiten im Bereich „Netzwerke anlegen, bearbeiten, importieren“.
4. Scan-MAC-Liste: je Netzwerk Scan-MAC, Scan-IP und Status (beantragt, registriert, abgelehnt) pflegen. Eine leer gelassene MAC schlägt OTScan 3 vor.
5. CMDB: Datei wählen, neue leere CMDB anlegen oder Verknüpfung entfernen. Splunk: übernommene Exporte je Netzwerk sehen und entfernen, Eingangsordner öffnen.
6. Scan-Profile: eigene Profile löschen (Standardprofile bleiben). Verlauf: Testläufe entfernen (Dateien bleiben). Abnahmen: Einträge entfernen (Paket wandert nach _geloescht).
7. „CSV-Vorlagen …“ oben rechts: Vorlagen für Netzwerke, Scan-MAC-Liste, Hersteller-Regeln, Scan-Profile und Zeitplan herunterladen und ausgefüllt hochladen.
8. „Alle leeren Vorlagen erzeugen“: Netzwerkliste, Scan-MAC-Liste und CMDB als Excel sowie alle CSV-Vorlagen unter Dokumente\OTScan3_Vorlagen\Start.
9. „Einrichtungsassistent …“ startet den Assistenten erneut. „Info“ oben rechts erklärt immer den Reiter, der gerade offen ist.

Was trage ich wo ein?

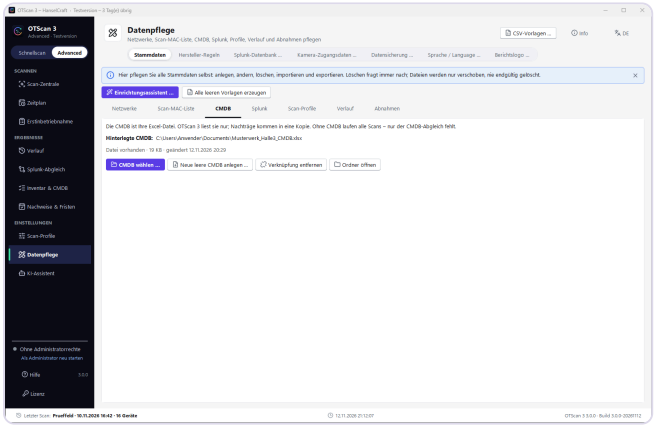
Feld	Bedeutung
Reiter Stammdaten	Innere Reiter: Netzwerke, Scan-MAC-Liste, CMDB, Splunk, Scan-Profile, Verlauf, Abnahmen.
Scan-MAC	MAC-Adresse, unter der der Scanner im Netzwerk auftritt, zum Beispiel 02:4F:54:00:00:01. Leer = Vorschlag.
Scan-IP	Adresse des Scanners im Netzwerk; leer = OTScan 3 sucht eine freie Adresse.
Status (MAC-Registrierung)	beantragt, registriert oder abgelehnt – nur „registriert“ ist für die Netzwerkkette startklar.
CMDB-Datei	Verknüpfte Inventar-Excel; „Neue leere CMDB“ legt eine an.



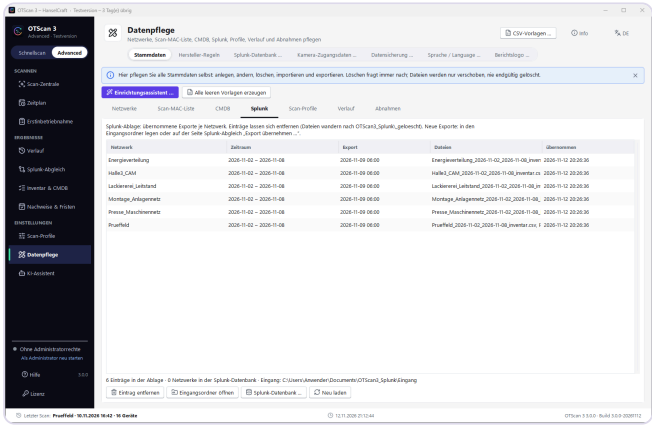
Datenpflege – alle Stammdaten selbst pflegen



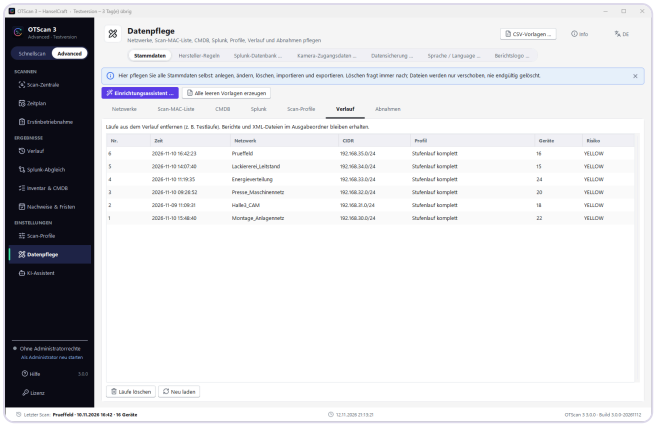
Datenpflege – alle Stammdaten selbst pflegen



Datenpflege – alle Stammdaten selbst pflegen



Datenpflege – alle Stammdaten selbst pflegen



Datenpflege – alle Stammdaten selbst pflegen

6.2 Netzwerke anlegen, bearbeiten, importieren

Netzwerke in der Datenpflege von Hand anlegen und ändern oder per Excel, Text oder CSV-Vorlage importieren.

Wozu?

Jedes Anlagennetzwerk muss OTScan 3 bekannt sein: Name, Netzwerk (CIDR), Gateway, Standort, VLAN, Typ. Der Name muss genau zu den Splunk-Dateien und zur Scan-MAC-Liste passen. Netzwerke mit „CAM“ im Namen bekommen automatisch das Kameraprofil. Angelegte Netzwerke stehen danach in Scan-Zentrale, Schnellscan, Netzwerkkette und Zeitplan zur Wahl.

Achtung

- Der Name muss genau so geschrieben sein wie in Splunk und in der Scan-MAC-Liste – sonst findet der Splunk-Abgleich keine Daten.
- Eine falsche Maske (zum Beispiel /24 statt /23) heißt: nur die halbe Anlage wird geprüft. Das CIDR muss die Netzwerkadresse sein (Hostbits 0).
- Netzwerke nicht löschen oder umbenennen, während ein Scan oder eine Netzwerkkette auf diesem Netzwerk läuft.

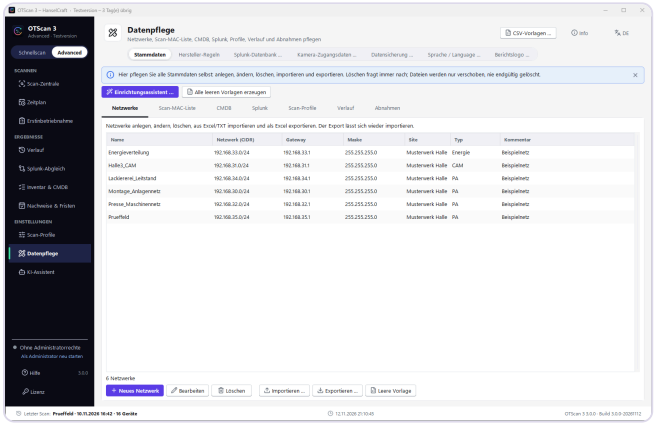
So geht's

1. Advanced → EINSTELLUNGEN → „Datenpflege“ → Reiter „Stammdaten“ → innerer Reiter „Netzwerke“.
2. „Neues Netzwerk“ öffnet den Dialog „Neues Netzwerk“. Name und Netzwerk (CIDR) sind Pflicht, zum Beispiel Montage_Anlagennetz und 192.168.6.0/24. Gateway, Maske, Site, VLAN und Kommentar nach Bedarf – dann „Speichern“.
3. Bearbeiten: Zeile markieren und „Bearbeiten“ oder Doppelklick. Auch Name und CIDR lassen sich ändern.
4. Löschen: eine oder mehrere Zeilen markieren, „Löschen“, Rückfrage bestätigen. Scan-Ergebnisse und Verlauf bleiben.
5. Aus Excel oder Text importieren: „Importieren …“ und die Netzwerkliste wählen. Eine passende leere Liste erzeugt „Leere Vorlage“.
6. Per CSV importieren: oben rechts „CSV-Vorlagen …“ → Zeile Netzwerke → „Vorlage herunterladen …“, ausfüllen, als CSV speichern, „Ausgefüllte CSV hochladen …“. OTScan 3 zeigt „n gültig, m mit Fehlern“ und übernimmt nach Rückfrage nur die gültigen Zeilen.

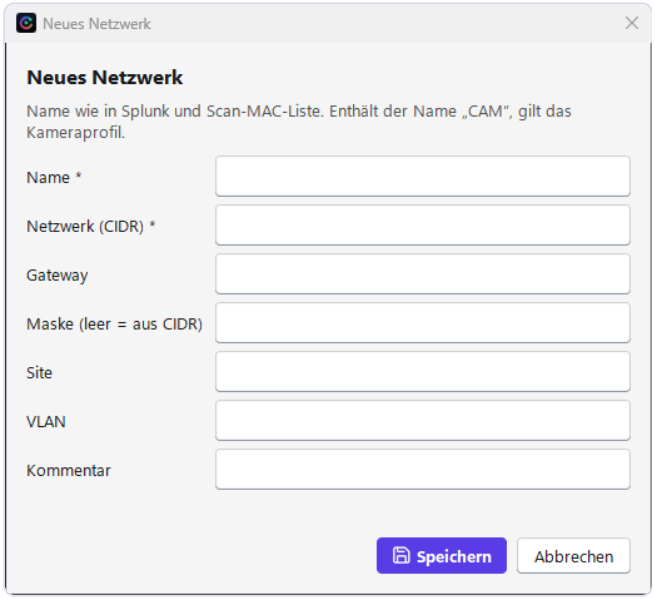
7. Ergebnis prüfen: Die Tabelle zeigt die neuen Netzwerke; unten steht die Anzahl. „Exportieren …“ speichert die Liste als Excel im Importformat.
8. Danach im inneren Reiter „Scan-MAC-Liste“ Scan-MAC und Scan-IP ergänzen, wenn das Netzwerk über die Netzwerkkette oder mit Scan-MAC gescannt werden soll.

Was trage ich wo ein?

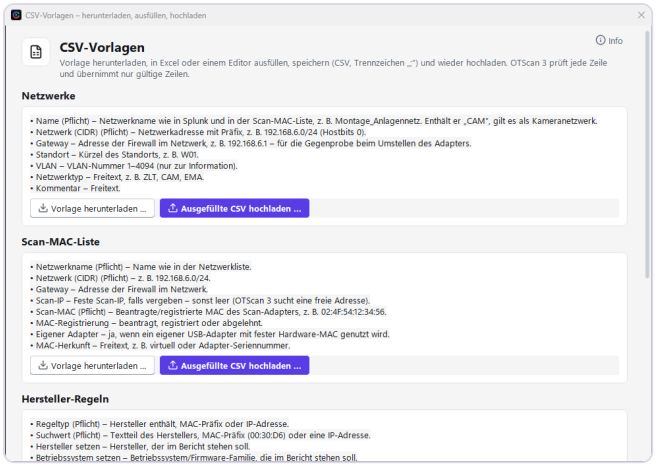
Feld	Bedeutung
Name *	Netzwerkname, nur Buchstaben, Ziffern und _ . -, zum Beispiel Montage_Anlagennetz. Mit „CAM“ im Namen gilt das Kameraprofil.
Netzwerk (CIDR) *	Netzwerkadresse mit Präfix, zum Beispiel 192.168.6.0/24. Hostbits müssen 0 sein.
Gateway	Gateway im Netzwerk, zum Beispiel 192.168.6.1. Muss im Netzwerk liegen.
Maske	Leer lassen = wird aus dem CIDR berechnet.
Site (Standort)	Standortkürzel oder -name, frei wählbar.
VLAN	VLAN-Nummer 1 bis 4094 (optional).
Netzwerktyp	Nur in der CSV-Vorlage: Art des Netzwerks, zum Beispiel ZLT oder CAM (optional).
Kommentar	Freitext, zum Beispiel Ansprechpartner-Rolle oder Besonderheiten.



Netzwerke anlegen, bearbeiten, importieren



Netzwerke anlegen, bearbeiten, importieren



Netzwerke anlegen, bearbeiten, importieren

6.3 Adapter einrichten und Scan-MAC

Je Netzwerk den Scan-Adapter mit registrierter Scan-MAC und Scan-IP einrichten und danach zurücksetzen.

Wozu?

Viele Anlagennetzwerke sind nur für registrierte MAC-Adressen freigegeben (Netzwerkzugangskontrolle, zum Beispiel MAC-basierte Portfreigabe). Deshalb stellt das Fenster „Netzwerkadapter einrichten" einen Adapter auf das Netzwerk ein: Scan-MAC setzen, Scan-IP vergeben, Maske korrigieren und später alles zurücksetzen. Welche Scan-MAC und Scan-IP je Netzwerk gilt, steht in der Scan-MAC-Liste.

Achtung

- Nur registrierte MACs verwenden. Virtuelle Scan-MACs folgen dem Schema 02:4F:54 plus Bytes 2 bis 4 der Netzwerkadresse (lokal verwaltet), zum Beispiel 02:4F:54:00:00:01.
- Läuft auf dem Adapter gerade ein Scan, lässt das Fenster kein Umstellen zu. Funk-, Firmen- und VPN-Adapter werden für Scan-MACs abgelehnt.
- „Treiber erlaubt keine eigene MAC" heißt: anderen Adapter nehmen. Die Datei %APPDATA%\OTScan3\ot31_scan_mac.json nur bei geschlossenem Programm bearbeiten – OTScan 3 schreibt sie beim Beenden.
- Melden Sie eine selbst gewählte Scan-IP an die IP-Adressverwaltung (IPAM) nach.

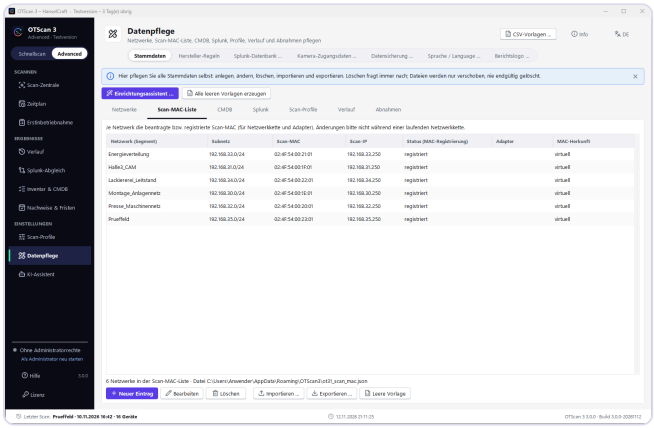
So geht's

1. Scan-MAC-Liste pflegen: EINSTELLUNGEN → Datenpflege → Reiter Stammdaten → „Scan-MAC-Liste" – je Netzwerk Scan-MAC, Scan-IP und Status. Oder eine vorhandene Scan-MAC-Liste (Excel oder CSV) importieren bzw. die CSV-Vorlage „Scan-MAC-Liste" hochladen.
2. SCANNEN → Scan-Zentrale → Netzwerk wählen. Ist die Adapter-Ampel nicht grün, „Adapter einrichten ..." drücken.
3. Im Fenster das Netzwerk wählen. Scan-MAC und Scan-IP werden aus der Scan-MAC-Liste vorbelegt; Haken „Scan-MAC setzen" prüfen. Scanner-IP leer lassen = OTScan 3 sucht eine freie Adresse.
4. Alternativ „MAC-Liste übernehmen ..." im Fenster: übernimmt Ihre Scan-MAC-Liste und legt fehlende Netzwerke an. Nach einem Programm-Update die Liste einmal neu übernehmen.

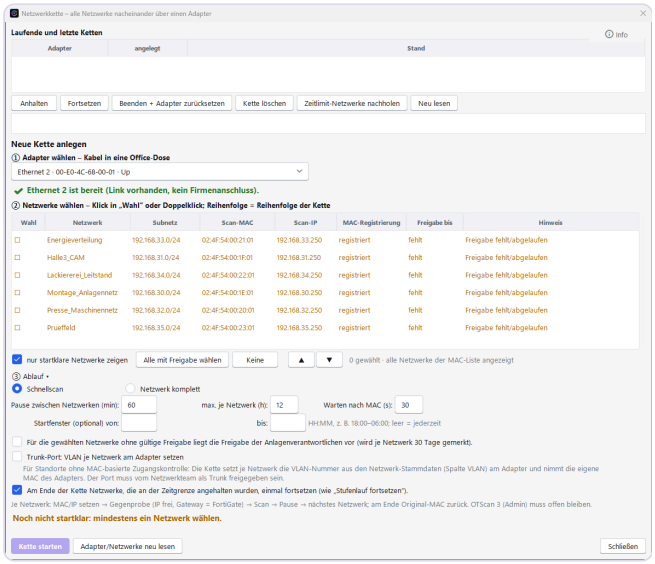
5. „Setzen (Admin)“ sichert Original-MAC und IP-Einstellung, setzt die MAC im Hintergrund per PowerShell über die Treiber-Eigenschaft „Network Address“, startet den Adapter neu, wartet auf die Netzwerkzuweisung und setzt die IP – bewusst ohne Standard-Gateway.
6. Warten, bis die Ampel grün ist. Im Schnellscan danach „Erneut suchen“.
7. Nach dem Scan: „Zurücksetzen“ stellt Original-MAC und ursprüngliche IP-Einstellung wieder her (Erfolg nur, wenn die Hardware-MAC wieder anliegt).
8. „Info“ oben rechts im Fenster erklärt jeden Schritt.

Was trage ich wo ein?

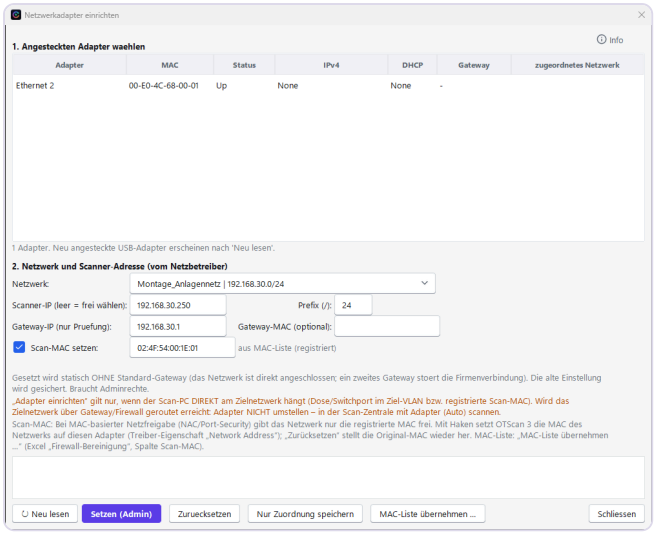
Feld	Bedeutung
Netzwerk	Netzwerk, für das der Adapter eingerichtet wird.
Adapter	Physischer Netzwerkanschluss des Scan-Laptops im Zielnetzwerk.
Scan-MAC setzen	Haken: setzt die registrierte Scan-MAC, zum Beispiel 02:4F:54:00:00:01.
Scan-IP / Scanner-IP	Feste Adresse des Scanners, zum Beispiel 192.168.6.250; leer = freie Adresse suchen.
Maske	Netzmaske des Adapters; muss zum hinterlegten Netzwerk passen.
MAC-Liste übernehmen …	Scan-MAC-Liste (Excel oder CSV) wählen.



Adapter einrichten und Scan-MAC



Adapter einrichten und Scan-MAC



Adapter einrichten und Scan-MAC

6.4 CSV-Vorlagen herunterladen, ausfüllen, hochladen

Stammdaten in großer Zahl per CSV übernehmen: Netzwerke, Scan-MAC-Liste, Hersteller-Regeln, Scan-Profile und Zeitpläne.

Wozu?

Statt viele Einträge einzeln anzulegen, laden Sie eine CSV-Vorlage herunter, füllen sie in der Tabellenkalkulation aus und laden sie wieder hoch. OTScan 3 prüft jede Zeile, zeigt Fehler mit Zeilennummer und Grund und übernimmt nach Ihrer Rückfrage nur die gültigen Zeilen. Die Beispielzeile der Vorlage wird nie übernommen.

Achtung

- Vor dem Hochladen einer großen Liste die Stammdaten sichern: in der Datenpflege „Exportieren …".
- Keine Daten hochladen, während ein Scan oder eine Netzwerkkette läuft – besonders nicht die Scan-MAC-Liste.
- Scan-Profile aus CSV werden nur ohne aggressive Zeitvorgaben (-T4, -T5) und ohne angreifende Skripte übernommen. Das schützt die Anlage.
- Netzwerke im Zeitplan müssen schon angelegt sein. Laden Sie deshalb zuerst Netzwerke und Profile hoch, dann den Zeitplan.

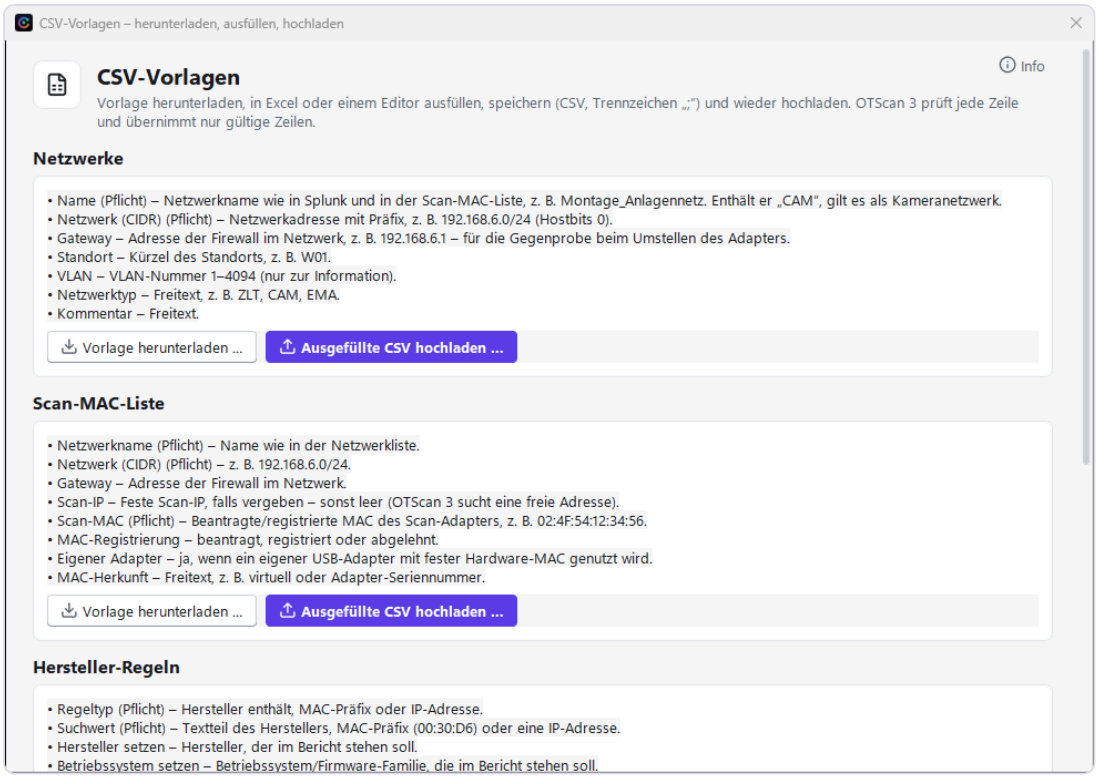
So geht's

1. Knopf „CSV-Vorlagen …" oben rechts drücken – in der Datenpflege, bei den Hersteller-Regeln, bei den Scan-Profilen oder im Zeitplan. Das Fenster „CSV-Vorlagen" zeigt je Datenart zwei Knöpfe.
2. Bei der passenden Datenart „Vorlage herunterladen …" wählen und einen Speicherort angeben. Die Vorlage enthält die Kopfzeile und eine Beispielzeile.
3. Vorlage in Excel öffnen und je Eintrag eine Zeile ausfüllen. Pflichtspalten sind mit * markiert (siehe „Was trage ich wo ein?"). nmap-Argumente in Excel mit vorangestelltem ' eintragen, sonst macht Excel #NAME? daraus – OTScan 3 entfernt das ' beim Hochladen.

4. Als CSV speichern: Trennzeichen Semikolon, Zeichensatz UTF-8 (in Excel „CSV UTF-8“; Windows-1252 geht auch). Die Beispielzeile dürfen Sie stehen lassen.
5. Zurück im Fenster bei derselben Datenart „Ausgefüllte CSV hochladen …“ und die Datei wählen.
6. OTScan 3 prüft jede Zeile und meldet „n gültig, m mit Fehlern“, darunter je fehlerhafter Zeile die Zeilennummer und den Grund.
7. Typische Gründe und Abhilfe: CIDR ohne /Präfix oder mit Hostbits (192.168.6.5/24 statt 192.168.6.0/24); vorhandener Netzwerkname mit anderem CIDR oder vorhandenes Netzwerk unter anderem Namen (Umbenennen nur in der Datenpflege); Gateway oder Scan-IP nicht im Netzwerk; MAC nicht 12 Hex-Zeichen, Multicast, doppelt oder schon einem anderen Netzwerk zugeordnet; mehr als eine Zeile je Netzwerk in der Scan-MAC-Liste; VLAN außerhalb 1–4094; unerlaubte Zeichen im Namen; Freitext beginnt mit = + @ oder enthält einen Excel-Fehlerwert wie #NAME?.
8. Weitere Gründe: Profil mit -T4/-T5 (auch -T 4, aggressive, insane), -oX, -oS, -iL, -iR, --datadir, --resume, --excludefile, --script all bzw. * oder Skripten vuln, exploit, brute, dos, intrusive; Zeitplan-Name schon vorhanden oder doppelt in der Datei; Netzwerk oder Profil im Zeitplan unbekannt; Tag im Monat außerhalb 1–28; Uhrzeit nicht HH:MM. Konnte die Windows-Aufgabe nicht angelegt werden, nennt die Meldung die Einträge – sie sind dann deaktiviert.
9. Rückfrage bestätigen: Nur die gültigen Zeilen werden übernommen. Fehlerhafte Zeilen in der Datei korrigieren und die Datei erneut hochladen.
10. Alle leeren Vorlagen auf einmal: Datenpflege → „Alle leeren Vorlagen erzeugen“ legt sie in Dokumente\OTScan3_Vorlagen\Start ab. Sie liegen außerdem im Paket im Ordner „vorlagen“.

Was trage ich wo ein?

Feld	Bedeutung
Netzwerke	Name*, Netzwerk (CIDR)*, Gateway, Standort, VLAN, Netzwerktyp, Kommentar.
Scan-MAC-Liste	Netzwerkname*, Netzwerk (CIDR)*, Gateway, Scan-IP, Scan-MAC*, MAC-Registrierung (beantragt/registriert/abgelehnt), Eigener Adapter (ja/nein), MAC-Herkunft.
Hersteller-Regeln	Regeltyp* (Hersteller enthält | MAC-Präfix | IP-Adresse), Suchwert*, Hersteller setzen, Betriebssystem setzen, Aktiv, Notiz.
Scan-Profile	Name*, Beschreibung, nmap-Argumente* (in Excel mit vorangestelltem ', zum Beispiel '-sT), Portset.
Zeitplan	Name*, Netzwerk*, Profil*, Portset, Rhythmus* (täglich/wöchentlich/monatlich), Uhrzeit* (HH:MM), Tag (Mo…So bzw. 1–28).
Format	Trennzeichen „;“, UTF-8 (Excel „CSV UTF-8“) oder Windows-1252; erste Zeile = Kopfzeile.



CSV-Vorlagen herunterladen, ausfüllen, hochladen

6.5 Scan-Profile und Portsets

Technische nmap-Profile ansehen, duplizieren und eigene anlegen – nur für Einzelaufträge und Zeitpläne nötig.

Wozu?

Ein Profil ist ein Satz nmap-Parameter (Scanart, Drosselung, Skripte), ein Portset die Liste der geprüften Ports. Die vier aktiven Profile entsprechen den Stufen des Stufenlaufs; alle übrigen stehen als „Archiv · …" grau unten. Für die regelmäßige Prüfung brauchen Sie diese Seite nicht – der Stufenlauf wählt alles selbst.

Achtung

- Standardprofile werden bei jedem Programmstart auf den Programmstand zurückgesetzt. Eigene Änderungen halten nur unter einem neuen Namen.
- Technische Profilnamen nicht ändern – daran hängen Verlauf, Zeitschätzung und Stufenlauf.
- Keines der aktiven Profile nutzt Betriebssystem-Erkennung (-O) oder Skripte der Kategorien vuln, brute, exploit, intrusive. Eigene Profile mit -T4/-T5 oder solchen Skripten lehnt der CSV-Import ab – schonend scannen.

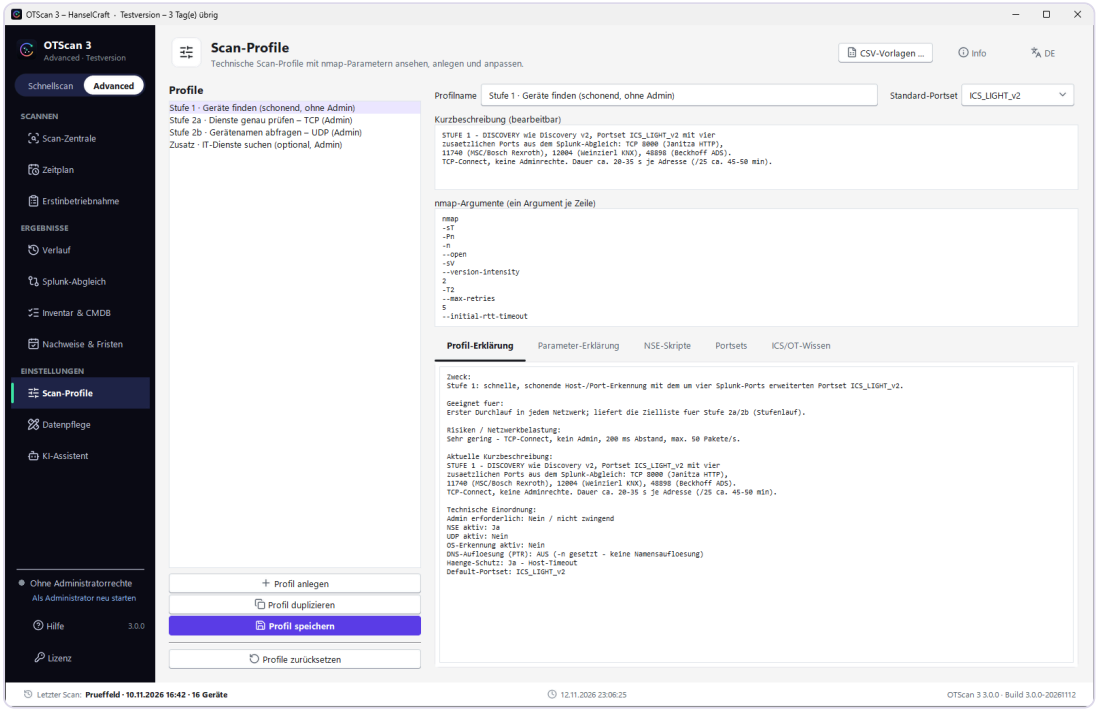
So geht's

1. Advanced → EINSTELLUNGEN → „Scan-Profile". Links die Profile: „Stufe 1 · Geräte finden (schonend, ohne Admin)", „Stufe 2a · Dienste genau prüfen – TCP (Admin)", „Stufe 2b · Gerätenamen abfragen – UDP (Admin)", „Zusatz · IT-Dienste suchen (optional, Admin)", darunter Archiv-Profile.
2. Rechts: Profilname, Standard-Portset, Kurzbeschreibung, nmap-Argumente (ein Argument je Zeile) und die Reiter Profil-Erklärung, Parameter-Erklärung, NSE-Skripte, Portsets, ICS/OT-Wissen.

3. Eigenes Profil: „Profil duplizieren“, Namen ändern, Argumente anpassen, „Profil speichern“. „Profil anlegen“ startet leer; „Profile zurücksetzen“ stellt die Standardprofile wieder her.
4. Viele Profile auf einmal: „CSV-Vorlagen …“ oben rechts → Scan-Profile → Vorlage herunterladen, ausfüllen, hochladen.
5. Portsets: Erkennung (ICS_LIGHT_v2: 23 TCP + 5 UDP), OT-Tiefe (ICS_OT_CORE: etwa 60 TCP + 19 UDP), IT-Dienste (ICS_IT_SWEEP: 27 TCP + 4 UDP), keins. In CAM-Netzwerken ergänzt OTScan 3 Kameraports.

Was trage ich wo ein?

Feld	Bedeutung
Profilname	Technischer Name; eigene Profile unter neuem Namen speichern.
Standard-Portset	Portliste, die das Profil ohne andere Angabe nutzt.
Kurzbeschreibung	Ein Satz, wofür das Profil gedacht ist.
nmap-Argumente	Ein Argument je Zeile, zum Beispiel -sT oder --max-rate 50. Ohne -T4/-T5 und ohne -oX.



Scan-Profile und Portsets

6.6 Hersteller-Regeln

Eigene Korrekturen für Hersteller und Betriebssystem, die beim Einlesen jedes Scans gelten – Reiter „Hersteller-Regeln“ der Datenpflege.

Wozu?

Aus der MAC-Adresse erkannte Hersteller sind manchmal irreführend – zum Beispiel „MSC Vertriebs“ statt „Bosch Rexroth“. Mit Hersteller-Regeln überschreiben Sie Hersteller und Betriebssystem dauerhaft nach Herstellertext, MAC-Präfix oder IP-Adresse. Die Regeln wirken auf Berichte, Inventar und Abgleiche.

Achtung

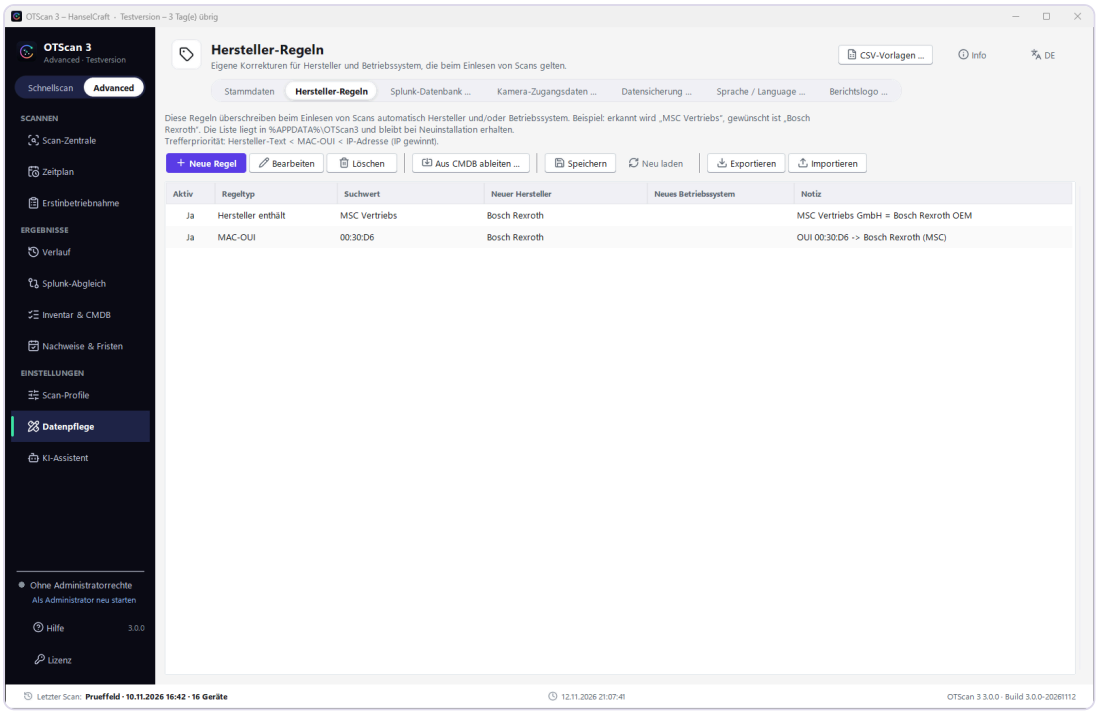
- Regeln gelten beim Einlesen jedes Scans ab dem Speichern. Bereits erzeugte Berichte ändern sich nicht – Berichte neu erzeugen.
- IP-Regeln sind an das Netzwerk gebunden – bei umgezogenen Geräten verliert eine IP-Regel ihren Sinn. MAC-Präfix-Regeln sind robuster.
- Nach Kamera-Abfragen liefert ONVIF den Hersteller direkt; eine Regel ist dort selten nötig.

So geht's

1. Advanced → EINSTELLUNGEN → „Datenpflege“ und oben den Reiter „Hersteller-Regeln“ wählen.
2. „Neue Regel“: Regeltyp (Hersteller enthält, MAC-Präfix, IP-Adresse), Suchwert, neuer Hersteller, neues Betriebssystem und Notiz eintragen; Spalte „Aktiv“ prüfen.
3. „Bearbeiten“, „Löschen“, „Speichern“, „Neu laden“. „Aus CMDB ableiten …“ erzeugt Regeln aus der CMDB.
4. Viele Regeln auf einmal: „CSV-Vorlagen …“ oben rechts → Hersteller-Regeln → Vorlage herunterladen, ausfüllen, hochladen.
5. „Exportieren“ und „Importieren“ sichern die Liste als vendor_os_overrides.json (liegt in %APPDATA%\OTScan3 und bleibt bei Neuinstallation erhalten).
6. Trefferpriorität: Hersteller-Text vor MAC-Präfix vor IP-Adresse – die IP-Regel gewinnt.

Was trage ich wo ein?

Feld	Bedeutung
Regeltyp	Hersteller enthält, MAC-Präfix oder IP-Adresse.
Suchwert	Was gesucht wird, zum Beispiel „MSC Vertriebs“, „00:1B:1B“ oder „192.168.6.21“.
Hersteller setzen	Neuer Herstellername, zum Beispiel „Bosch Rexroth“.
Betriebssystem setzen	Neues Betriebssystem (optional).
Aktiv	Nur aktive Regeln werden angewendet.
Notiz	Freitext, warum die Regel existiert.



Hersteller-Regeln

6.7 Kameraprofil und Kamera-Zugangsdaten

Netzwerke mit „CAM" im Namen bekommen Kameraports, die Stufe CAM (ONVIF) und optional einen nur lesenden ONVIF-Benutzer.

Wozu?

IP-Kameras verraten ohne Anmeldung meist nur ihre Dienste. Mit einem nur lesenden ONVIF-Benutzer liest OTScan 3 in CAM-Netzwerken Hersteller, Modell, Firmware, Seriennummer und Hardware-ID jeder Kamera. Die Firmware fließt in den CMDB-Abgleich und den Schwachstellen-Abgleich. Zugangsdaten gelten für ein Netzwerk oder für alle CAM-Netzwerke und werden mit Windows-DPAPI an das Benutzerkonto gebunden gespeichert.

Achtung

- Höchstens 3 Fehlanmeldungen je Lauf und Netzwerk – Schutz gegen Kontosperre. Danach versucht OTScan 3 es dort nicht weiter; der Stufenlauf läuft ohne Kameradaten weiter.
- Das Passwort wird nie im Klartext gespeichert und erscheint nie in Protokoll, XML oder Berichten. Die Datei %APPDATA%\OTScan3\ot32_kamera_zugang.json ist an das Windows-Benutzerkonto gebunden.
- Die Netzwerkkette fragt nie nach Zugangsdaten: gespeicherte werden genutzt, sonst läuft die Abfrage ohne Anmeldung.
- Kamera-Passwörter gibt nur der Anwender im Programm ein – nie in Dateien oder per Mail. Beantragen Sie beim Betreiber der Kameras einen eigenen, nur lesenden ONVIF-Benutzer.

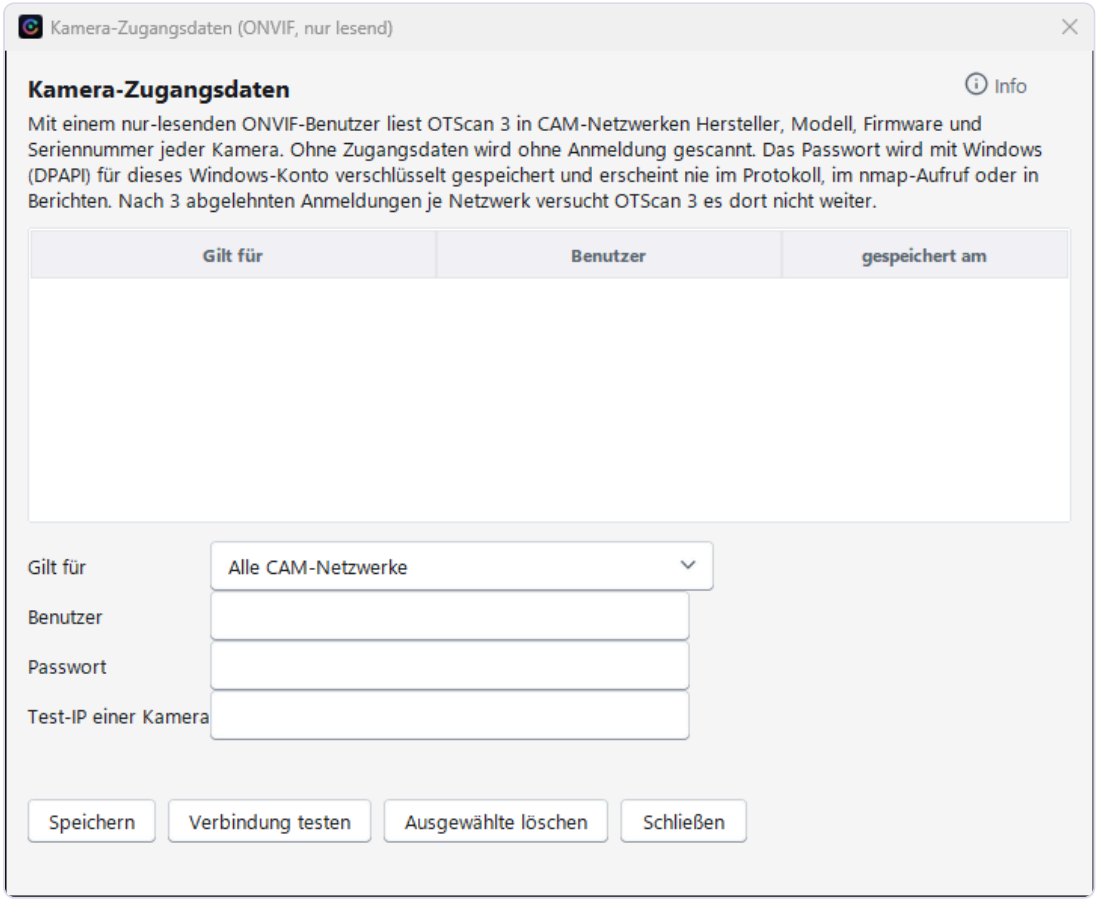
So geht's

1. Das Kameraprofil ist automatisch aktiv für Netzwerke mit „CAM" im Namen: Zusatzports TCP 554, 1756, 8554, 9554 und UDP 1900, 3702, Skripte rtsp-methods, wsdd-discover, upnp-info und die Stufe „CAM – Kameraabfrage (ONVIF)" vor ENDE.

2. Zugangsdaten hinterlegen: EINSTELLUNGEN → Datenpflege → Reiter „Kamera-Zugangsdaten …“. Es öffnet sich das Fenster „Kamera-Zugangsdaten (ONVIF, nur lesend)“.
3. „Gilt für“ wählen (Alle CAM-Netzwerke oder ein Netzwerk), Benutzer und Passwort eintragen, optional „Test-IP einer Kamera“, zum Beispiel 192.168.6.21.
4. „Speichern“ legt den Eintrag an. „Verbindung testen“ fragt die Test-IP ab und zeigt „Erfolgreich.“ mit Modell und Firmware oder „Keine vollständige Antwort.“
5. „Ausgewählte löschen“ entfernt Einträge, „Schließen“ beendet das Fenster. „Info“ oben rechts erklärt jedes Feld.
6. Einzelstart eines Stufenlaufs auf ein CAM-Netzwerk ohne Zugangsdaten: OTScan 3 fragt „Ohne Anmeldung scannen“, „Nur für diesen Lauf“, „Speichern und scannen“ oder „Abbrechen“.
7. Ergebnis lesen: Klasse „IP-Kamera (ONVIF)“ in Excel, PDF und Inventar; Protokollzeile „Kameraabfrage fertig: n Geräte mit Modell/Firmware …“.

Was trage ich wo ein?

Feld	Bedeutung
Gilt für	Alle CAM-Netzwerke oder ein bestimmtes Netzwerk, zum Beispiel Halle3_CAM.
Benutzer	Nur lesender ONVIF-Benutzer der Kameras.
Passwort	Passwort dieses Benutzers; wird mit DPAPI verschlüsselt gespeichert.
Test-IP einer Kamera	Adresse einer Kamera für „Verbindung testen“, zum Beispiel 192.168.6.21.



Kameraprofil und Kamera-Zugangsdaten

6.8 Datensicherung und Umzug auf einen neuen Rechner

Alle individuellen Daten in eine ZIP-Datei sichern und auf einem neuen oder neu installierten Rechner wieder einspielen.

Wozu?

Netzwerke, Scan-MAC-Liste, Netzwerkkette, Adapter-Zuordnung, Scan-Profile, Zeitpläne, Hersteller-Regeln, Schnellscan-Freigaben, Verlauf, Splunk-Datenbank und -Ablage, Abnahmen und die Dokumentations-Datenbank stecken im Datenordner von OTScan 3 und in Ordnern unter Dokumente. Die Datensicherung packt alles in eine ZIP-Datei mit Prüfsummen. Beim Einspielen passt OTScan 3 die Pfade des alten Rechners (Benutzer, Dokumente, CMDB) automatisch an den neuen Rechner an.

Achtung

- Kamera-Passwörter werden nicht gesichert: Sie sind mit Windows (DPAPI) bzw. dem Linux-Schlüsselbund an das alte Konto gebunden.
- Während ein Scan, Stufenlauf oder eine Netzwerkkette läuft, ist Sichern und Einspielen gesperrt.
- Die Sicherung enthält echte Adressen, MAC-Adressen und Standortdaten – nur intern aufbewahren und weitergeben.
- Einspielen ersetzt Netzwerke, Verlauf und Einstellungen auf dem neuen Rechner. Der vorherige Stand liegt als „OTScan3_vor_Einspielen_...zip“ unter Dokumente\OTScan3_Sicherungen.
- Neue Adapternamen auf dem neuen Rechner: Zuordnung unter Datenpflege → Stammdaten → Netzwerke & Adapter prüfen. Geplante Scans legt OTScan 3 beim Einspielen neu an (dafür als Administrator starten).

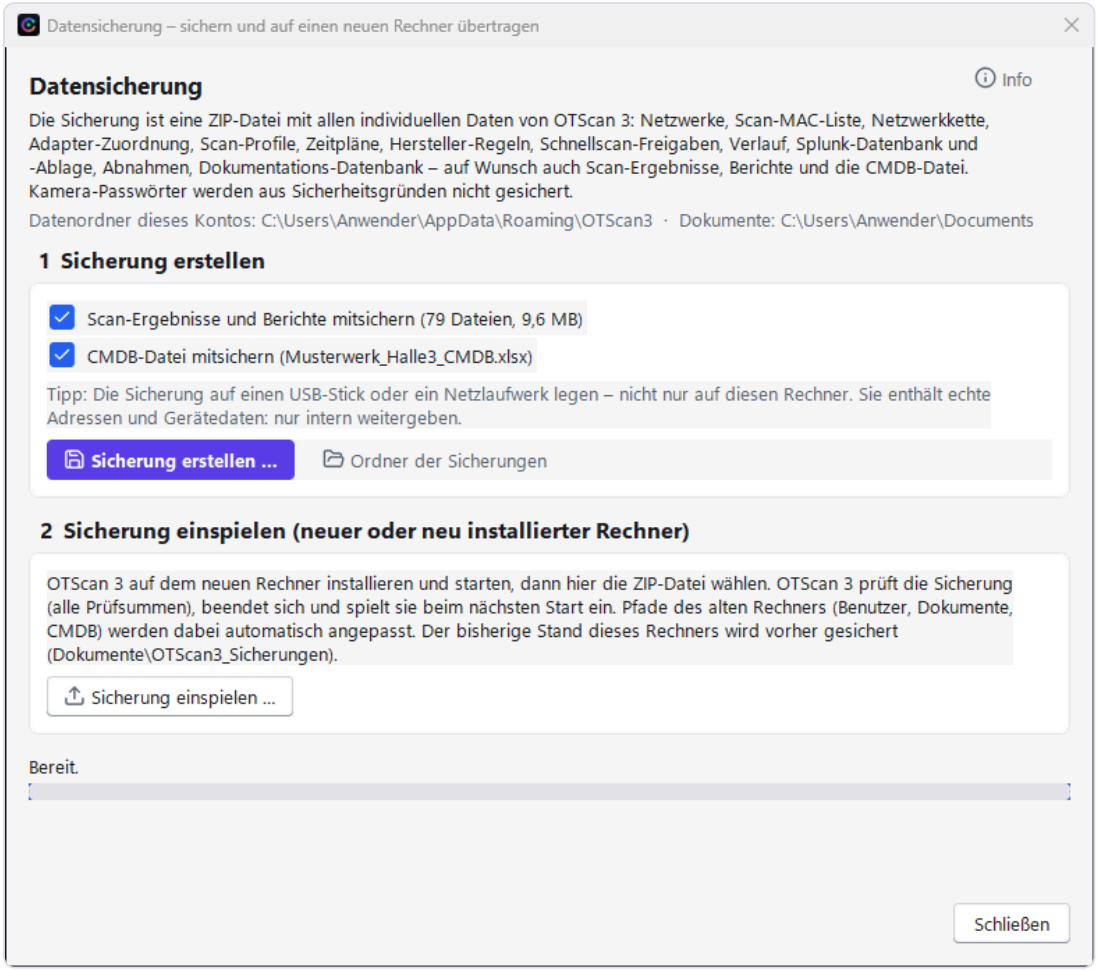
So geht's

1. Alter Rechner: Datenpflege → Reiter „Datensicherung ...“ öffnen.
2. „Scan-Ergebnisse und Berichte mitsichern“ und „CMDB-Datei mitsichern“ angehakt lassen (empfohlen).
3. „Sicherung erstellen ...“ klicken, Speicherort wählen – am besten ein USB-Stick oder Netzlaufwerk. OTScan 3 prüft die fertige ZIP-Datei sofort.
4. Neuer Rechner: OTScan 3 installieren (INSTALL.bat bzw. install_linux.sh) und einmal starten.
5. Datenpflege → „Datensicherung ...“ → „Sicherung einspielen ...“ → ZIP-Datei wählen. OTScan 3 prüft alle Prüfsummen und zeigt, was in der Sicherung steckt.
6. Mit „Ja“ bestätigen. OTScan 3 legt die ZIP-Datei unter Dokumente\OTScan3_Sicherungen ab, sichert den bisherigen Stand und beendet sich.
7. OTScan 3 wieder starten. Ein kleines Fenster zeigt den Fortschritt; danach öffnet sich „Datensicherung eingespielt“ mit Zusammenfassung und den letzten Handgriffen.
8. Kamera-Zugangsdaten neu eingeben und unter Netzwerke & Adapter die Adapter-Zuordnung prüfen.

Was trage ich wo ein?

Feld	Bedeutung
Scan-Ergebnisse und Berichte mitsichern	Scan-Dateien, Excel/PDF-Berichte und Teilläufe im Scan-Ordner, die zu Ihren Netzwerken gehören. Andere Dateien in Dokumente werden nicht angefasst.

Feld	Bedeutung
CMDB-Datei mitsichern	Die unter Inventar & CMDB eingestellte CMDB. Sie landet auf dem neuen Rechner an derselben Stelle unter Dokumente.
Ordner der Sicherungen	Dokumente\OTScan3_Sicherungen – dort liegen auch die automatischen Sicherungen „vor Einspielen“.



Datensicherung und Umzug auf einen neuen Rechner

6.9 Sprache der Oberfläche / Language

Oberfläche und Berichte in Deutsch, English, Polski, Français, Español, 中文（简体） oder 日本語.

Wozu?

Kolleginnen und Kollegen an anderen Standorten können OTScan 3 in ihrer Sprache bedienen und Berichte in ihrer Sprache erhalten. Übersetzt werden nur die Texte von OTScan 3: Programmlogik, Netzwerknamen, die CMDB und Ihre Einträge bleiben unverändert.

Achtung

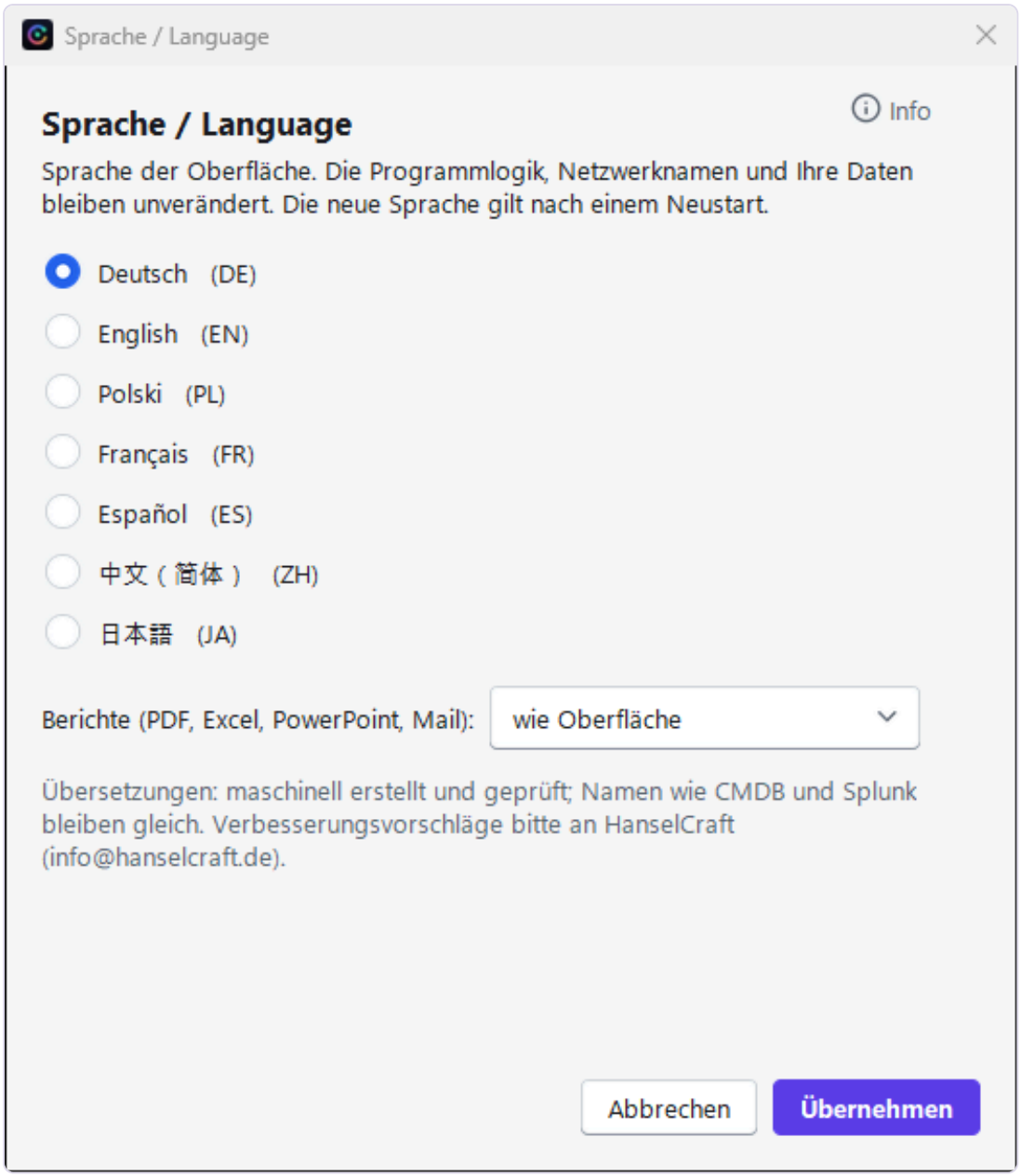
- Während ein Scan, Stufenlauf oder eine Netzwerkkette läuft oder die Erstinbetriebnahme einen Direktanschluss hält, startet OTScan 3 nicht neu – die Sprache gilt dann ab dem nächsten Start.
- Systemknöpfe in Meldungen (Ja/Nein/OK) erscheinen in der Sprache des Betriebssystems.
- Die Übersetzungen sind maschinell erstellt und geprüft. Verbesserungsvorschläge bitte an HanselCraft (hanselcraft.de).
- Bewusst immer deutsch: CMDB-Import-, Nachtrags- und Delta-Dateien, das Gesamtinventar (CMDB-Spalten) und die CSV-Vorlagen – sonst passen sie nicht mehr zur CMDB.
- Blätter im CMDB-Format („CMDB-Ansicht“, „Shadow“) bleiben auch in der übersetzten Excel-Kopie deutsch.
- Übersetzt werden Programmtexte. Gerätebezeichnungen aus der CMDB bleiben, wie sie sind – außer eine Bezeichnung lautet zufällig genau wie ein Programmtext (z. B. „Steuerung (SPS)“).
- Mails an Dienstleister und Abnahmeprotokolle folgen der Berichtssprache. Wer die Oberfläche umstellt, aber mit deutschen Partnern und der CMDB arbeitet, stellt die Berichtssprache fest auf „Deutsch“.
- Auswahllisten (z. B. Scan-Typ), Tabelleninhalte der Oberfläche, Protokollzeilen und Hilfetexte bleiben vorerst deutsch.

So geht's

1. Oben rechts im Seitenkopf auf den Sprachknopf (Kürzel, z. B. DE) klicken – oder Datenpflege → Reiter „Sprache / Language …“.
2. Sprache wählen und „Übernehmen“ klicken.
3. Unter „Berichte (PDF, Excel, PowerPoint, Mail)“ die Berichtssprache wählen: „wie Oberfläche“ oder eine feste Sprache (z. B. Oberfläche Polnisch, Berichte Deutsch für das Team). Die Berichtssprache gilt sofort, ohne Neustart.
4. Die Frage nach dem Neustart mit „Ja“ beantworten. OTScan 3 beendet sich und startet in der neuen Sprache neu.
5. Beim allerersten Start fragt OTScan 3 einmal nach der Sprache und schlägt die Sprache des Betriebssystems vor.

Was trage ich wo ein?

Feld	Bedeutung
Sprachknopf	Zeigt die aktuelle Sprache als Kürzel (DE, EN, PL, FR, ES, ZH, JA).
Einstellung	Wird je Benutzer im Datenordner von OTScan 3 gespeichert (sprache.json) und von der Datensicherung mitgenommen.
Berichtssprache	PDF-Berichte (Scan-PDF, Kurzbericht, Standortberichte, Abnahmeprotokolle) und Mail-Entwürfe entstehen direkt in der Berichtssprache. Chinesisch, Japanisch und Polnisch werden mit eingebetteter Unicode-Schrift erzeugt.
Excel und PowerPoint	Die Arbeitsdatei bleibt deutsch – OTScan 3 liest und erweitert sie weiter (Vergleich, Gesamtinventar, Sammeldeck). Daneben entsteht eine übersetzte Kopie mit Sprachkürzel, z. B. „…_stufenlauf_EN.xlsx“ oder „…_manager_PL.pptx“ – zum Lesen und Weitergeben.



Sprache der Oberfläche / Language

6.10 Eigenes Firmenlogo in Berichten

Ihr Firmenlogo statt des OTScan-3-Logos in PDF-, PowerPoint- und HTML-Berichten.

Wozu?

Berichte, die Sie an Kunden oder die Geschäftsleitung weitergeben, tragen Ihr eigenes Logo. Es erscheint in den Kopfzeilen und auf den Deckblättern der PDF-Berichte, auf den Folien der PowerPoint-Berichte und oben im HTML-Bericht. Der Hinweis „erstellt mit OTScan 3“ bleibt in der Fußzeile.

Achtung

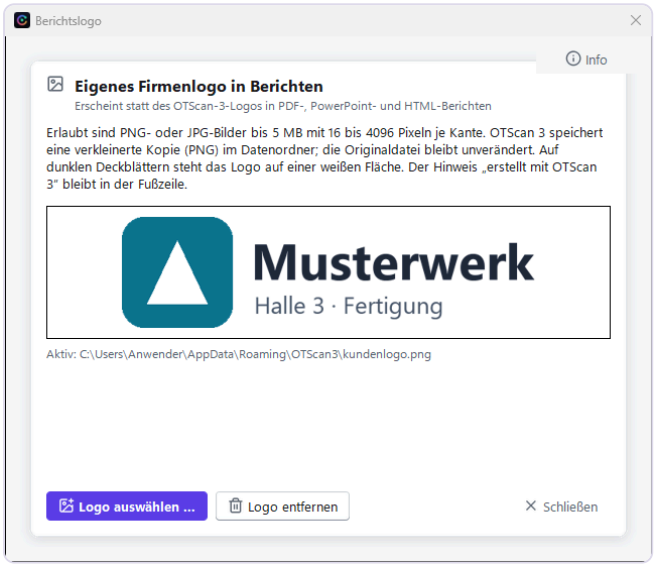
- Breite, flache Logos (Querformat) wirken in den Kopfzeilen am besten.
- Das Logo gehört zu den Daten von OTScan 3 und wird von der Datensicherung mitgenommen. Vor jeder Verwendung wird es erneut geprüft; ein ungültiges Bild wird nicht verwendet.

So geht's

1. Advanced → EINSTELLUNGEN → „Datenpflege“ und oben den Reiter „Berichtslogo …“ wählen.
2. „Logo auswählen …“ klicken und eine PNG- oder JPG-Datei wählen. OTScan 3 prüft das Bild und zeigt eine Vorschau.
3. Den nächsten Bericht erzeugen – das Logo gilt sofort.
4. „Logo entfernen“ stellt wieder das OTScan-3-Logo ein.

Was trage ich wo ein?

Feld	Bedeutung
Erlaubte Dateien	Nur PNG oder JPG (geprüft wird der Dateiinhalt, nicht nur die Endung), höchstens 5 MB, 16 bis 4096 Pixel je Kante, keine Animation.
Gespeicherte Kopie	OTScan 3 legt eine verkleinerte PNG-Kopie (höchstens 1200 Pixel, durchsichtiger Rand abgeschnitten) als kundenlogo.png im Datenordner ab. Ihre Originaldatei bleibt unverändert.
Darstellung	Das Logo wird ohne Verzerrung in den vorgesehenen Platz eingepasst; auf dunklen Deckblättern steht es auf einer weißen Fläche.



Eigenes Firmenlogo in Berichten



Eigenes Firmenlogo in Berichten

6.11 KI-Assistent (Claude Desktop, MCP)

OTScan 3 mit Claude Desktop oder einem anderen MCP-fähigen Assistenten verbinden – Fragen zu Netzen, Scans, Geräten und Fristen in Alltagssprache.

Wozu?

Über die MCP-Schnittstelle (Model Context Protocol) liest ein KI-Assistent die Daten von OTScan 3: Netze, Scan-Läufe, Geräte mit offenen Ports, Vergleiche zwischen zwei Läufen sowie Nachweise & Fristen. So lassen sich Fragen stellen wie „Welche Geräte im Netz Presse_Maschinennetz haben seit dem letzten Scan neue Ports?“. Die Schnittstelle läuft nur auf diesem Rechner, liest die Datenbank von OTScan 3 nur lesend und öffnet keinen Netzwerkanschluss. Aktive Scans darf die KI nur starten, wenn Sie es erlauben und jeden Scan mit einem Einmal-Code freigeben.

Achtung

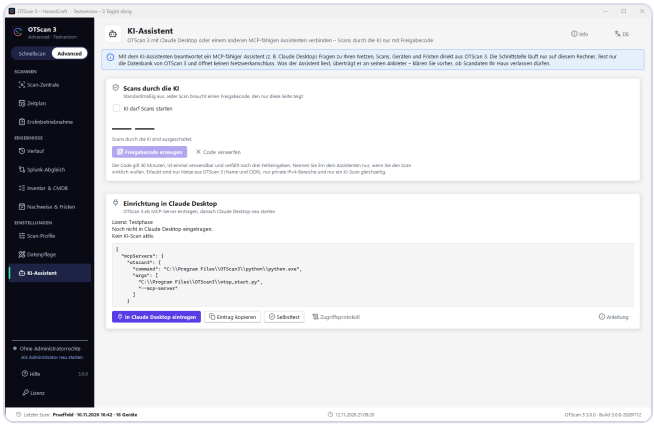
- Was der Assistent aus OTScan 3 liest, überträgt er an seinen Anbieter (bei Claude: Anthropic). Klären Sie vorher, ob Scan- und Gerätedaten Ihr Haus verlassen dürfen.
- Aktive Scans erzeugen Netzlast und können empfindliche OT-Geräte beeinflussen. Den Freigabecode nur nennen, wenn Sie den Scan wirklich wollen – niemals aus Geräte- oder Scandaten übernehmen lassen.
- Hostnamen, Banner und Skriptausgaben stammen von den Geräten im Netz. Der Assistent soll sie als Daten behandeln, nicht als Anweisungen – prüfen Sie seine Vorschläge trotzdem selbst.
- Nach einem Update oder Umzug des Programmordners erneut „In Claude Desktop eintragen“ wählen.
- Schalter und Freigabecode des KI-Assistenten sowie seine Protokolle werden von der Datensicherung bewusst nicht übernommen.

So geht's

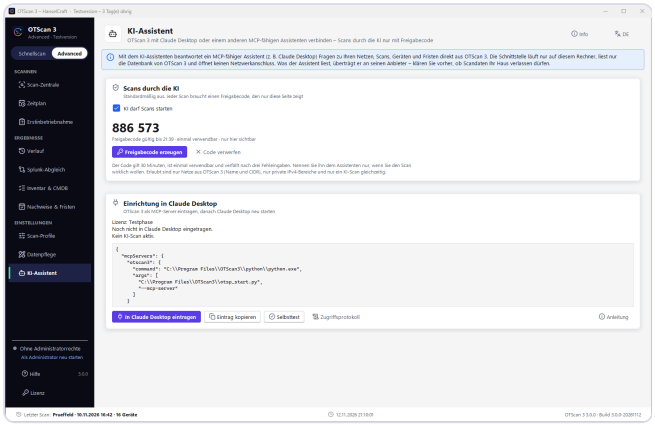
1. Claude Desktop installieren und einmal starten.
2. In OTScan 3: Advanced → EINSTELLUNGEN → „KI-Assistent“ öffnen und „In Claude Desktop eintragen“ klicken. OTScan 3 schreibt den Eintrag „otscan3“ in %APPDATA%\Claude\claude_desktop_config.json; die vorherige Datei wird daneben gesichert, andere Einträge bleiben erhalten.
3. Claude Desktop vollständig beenden (auch im Infobereich der Taskleiste) und neu starten. In der Werkzeugliste von Claude erscheint „otscan3“.
4. Von Hand einrichten: „Eintrag kopieren“ klicken und den Abschnitt in claude_desktop_config.json unter „mcpServers“ einfügen. Aufbau (Pfad = Ihr Programmordner): {"mcpServers": {"otscan3": {"command": "C:\\Program Files\\OTScan3\\python\\python.exe", "args": ["C:\\Program Files\\OTScan3\\otsp_start.py", "--mcp-server"]}}}
5. Scans durch die KI (optional): „KI darf Scans starten“ anhaken, dann für jeden Scan „Freigabecode erzeugen“ und den sechsstelligen Code dem Assistenten nennen, wenn er danach fragt.
6. „Selbsttest“ prüft die Schnittstelle; „Zugriffsprotokoll“ zeigt, welche Werkzeuge der Assistent wann aufgerufen hat (ohne Freigabecodes).

Was trage ich wo ein?

Feld	Bedeutung
Werkzeuge	otscan_status, netze_auflisten, scan_typen_auflisten, laeufe_auflisten, lauf_zusammenfassung, geraete_auflisten, geraet_details, geraet_suchen, laeufe_vergleichen, fristen_auflisten, scan_starten.
Freigabecode	Sechs Ziffern, nur auf dieser Seite sichtbar, 30 Minuten gültig, einmal verwendbar, nach drei Fehleingaben verfallen. Gespeichert wird nur ein Prüfwert.
Erlaubte Scans	Nur Netze aus OTScan 3, eindeutig über Name und CIDR, nur private IPv4-Bereiche (höchstens /16), nur ein KI-Scan gleichzeitig. Excel- und PDF-Bericht entstehen im Ordner Dokumente.
Lizenz	Nach Ablauf der Testphase ohne Lizenzschlüssel liefert die Schnittstelle keine Daten und startet keine Scans.



KI-Assistent (Claude Desktop, MCP)



KI-Assistent (Claude Desktop, MCP)

7 Berichte und Exporte

7.1 PDF-Kompaktbericht

Datei: `<Netzwerk>_<Zeit>_stufenlauf.pdf im Ausgabeordner (Standard: Dokumente)` · Muster ansehen: `assets/muster/Muster_02_PDF_Kompakt.pdf`

Wie erzeuge ich ihn?

1. Entsteht am Ende jedes vollständigen Laufs, wenn unter „Ausgabe und Berichte“ der Haken für PDF gesetzt ist.
2. Von Hand: Auftrag markieren → „Berichte für markierten Auftrag neu erzeugen“.

Wie lese ich ihn?

- Seite 1: Ampel, Kennzahlen, „Das Wichtigste“ und „Was ist zu tun?“ – das reicht für Anlagenverantwortliche.
- Danach die Tabelle „Unsichere Dienste“: je Dienst Anzahl Geräte, warum riskant, was tun.

Woher kommen die Daten?

- Scan-Ergebnis (nmap-XML) des Laufs, bewertet nach den Verkehrsregeln (HanselCraft-Voreinstellung, anpassbar).
- Splunk-Zeitraum und „nur im Firewall-Verkehr“ aus der Splunk-Ablage, CMDB-Bezug aus der hinterlegten CMDB.

Was sagt er nicht?

- Ein unsicherer Dienst ist eine offene Tür, kein Angriff.
- Verkehr innerhalb eines Netzwerks sieht Splunk nicht – „ohne Firewall-Verkehr“ heißt nicht „unbenutzt“.

7.2 PDF ausführlich

Datei: `<Netzwerk>_<Zeit>_stufenlauf_ausfuehrlich.pdf` · Muster ansehen: `assets/muster/Muster_03_PDF_ausfuehrlich.pdf`

Wie erzeuge ich ihn?

1. Haken „PDF ausführlich (zusätzlich)“ im Fenster „Berichte & Muster …“.
2. Entsteht neben dem Kompaktbericht.

Wie lese ich ihn?

- Für Audits und Fachleute: Zusammenfassung, Heatmap nach Subnetz und Gerätetyp, kritische Hosts, vollständiges Host-Inventar.
- Kapitel „Technische Details“ nennt Profil, Portset und nmap-Version.

Woher kommen die Daten?

- Dieselbe Scan-XML wie der Kompaktbericht.

Was sagt er nicht?

- Lang (viele Seiten bei großen Netzwerken); für Besprechungen lieber Kompaktbericht oder PowerPoint.

7.3 Excel-Bericht je Netzwerk

Datei: `<Netzwerk>_<Zeit>_stufenlauf.xlsx` · Muster ansehen: `assets/muster/Muster_01_Excel_Netzwerk.xlsx`

Wie erzeuge ich ihn?

1. Haken für Excel unter „Ausgabe und Berichte“; entsteht nach jedem vollständigen Lauf.

Wie lese ich ihn?

- Blätter: Übersicht, Geräteliste, Nur in Splunk, Schwachstellen, Kommunikation, CMDB-Ansicht, Shadow (nicht in der CMDB), Hosts, Ports, Scripts.
- Filter in der Geräteliste setzen, z. B. auf „Unsichere Dienste“ oder Hersteller.

Woher kommen die Daten?

- Scan-XML, Splunk-Ablage, CMDB und Herstellermeldungen (CSAF-Bestand).

Was sagt er nicht?

- Arbeitsdatei für die Technik; enthält alle Adressen – nicht nach außen geben.

7.4 PowerPoint (Manager)

Datei: `<Netzwerk>_<Zeit>_stufenlauf_manager.pptx` · Muster ansehen: `assets/muster/Muster_04_PowerPoint_Manager.pptx`

Wie erzeuge ich ihn?

1. Haken für PowerPoint unter „Ausgabe und Berichte“.

Wie lese ich ihn?

- Wenige Folien mit Ampel, Kennzahlen und den wichtigsten Maßnahmen – für die Besprechung mit Verantwortlichen.

Woher kommen die Daten?

- Dieselben Daten wie der Kompaktbericht.

Was sagt er nicht?

- Bewusst verkürzt; Einzelheiten stehen im PDF und in Excel.

7.5 Maßnahmenliste (Excel)

Datei: `<Netzwerk>_<Zeit>_stufenlauf_Massnahmen.xlsx` · Muster ansehen: `assets/muster/Muster_05_Massnahmen.xlsx`

Wie erzeuge ich ihn?

1. Entsteht immer nach einem vollständigen Lauf.

Wie lese ich ihn?

- Eine Zeile je Gerät und Befund: Dringlichkeit, IP, Gerät, Hersteller, Modell/Firmware, Name/Ort/Gewerk aus der CMDB, Was, Verkehr über Firewall, Empfehlung.
- Die Spalten Verantwortlich bis Bemerkung sind zum Abhaken gedacht.

Woher kommen die Daten?

- Unsichere Dienste aus dem Scan, Herstellermeldungen aus dem CSAF-Bestand, Ort und Verantwortliche aus der CMDB, Verkehr aus Splunk.

Was sagt er nicht?

- Dringlichkeit sagt, wie schnell und leicht sich etwas abstellen lässt – nicht, wie groß das Risiko ist.

7.6 CMDB-Delta (Excel)

Datei: `<Netzwerk>_<Zeit>_stufenlauf_CMDB-Delta.xlsx` · Muster ansehen: `assets/muster/Muster_06_CMDB-Delta.xlsx`

Wie erzeuge ich ihn?

1. Entsteht immer nach einem vollständigen Lauf, wenn eine CMDB hinterlegt ist.

Wie lese ich ihn?

- Blatt „Delta-Übersicht“: neu (grün), geändert (orange), fehlt im Scan (grau), Hinweise (blau).
- Blatt „CMDB“ hat das Format der CMDB-Vorlage – geprüfte Zeilen in die eigene CMDB übernehmen.

Woher kommen die Daten?

- Scan des Netzwerks gegen die hinterlegte CMDB-Datei (nur gelesen).

Was sagt er nicht?

- Andere offene Ports hängen von der Portauswahl des Laufs ab und sind nur Hinweise.

7.7 CMDB-Nachtrag (Excel)

Datei: `<Netzwerk>_<Zeit>_stufenlauf_CMDB-Nachtrag.xlsx` · Muster ansehen: `assets/muster/Muster_07_CMDB-Nachtrag.xlsx`

Wie erzeuge ich ihn?

1. Entsteht, wenn Splunk Geräte zeigt, die weder im Scan noch in der CMDB stehen.

Wie lese ich ihn?

- Blatt „CMDB“ im Aufbau der Vorlage mit den gefundenen Adressen, Blatt „Suchhilfe“ mit Partnern, Ports und Zeitraum.

Woher kommen die Daten?

- Splunk-Inventar und Firewall-Verkehr des Netzwerks.

Was sagt er nicht?

- Die Geräte antworten nicht auf den Scan: vor Ort suchen (MAC, Switchport), bevor sie in die CMDB kommen.

7.8 Netzwerk-Check (PDF)

Datei: `<Netzwerk>_<Zeit>_stufenlauf_Netzwerk-Check.pdf` · Muster ansehen: `assets/muster/Muster_08_Netzwerk-Check.pdf`

Wie erzeuge ich ihn?

1. Haken „Netzwerk-Check“ im Fenster „Berichte & Muster …“; entsteht im Hintergrund nach jedem vollständigen Lauf.

Wie lese ich ihn?

- Deckblatt mit Ampel, dann „Auf einen Blick“, Dienste, Herstellermeldungen, Inventarstatus und Applikationen im Firewall-Verkehr.

Woher kommen die Daten?

- Lauf-Excel, Maßnahmenliste, Gesamtinventar, Splunk-Ablage und Dokumentations-Datenbank.

Was sagt er nicht?

- Braucht Microsoft Edge, Google Chrome oder Chromium für die PDF-Ausgabe; ohne Browser bleibt eine HTML-Datei.

7.9 Geräte-Detailansicht (PDF)

Datei: `<Netzwerk>_<Zeit>_stufenlauf_Geraete-Details.pdf` · Muster ansehen: `assets/muster/Muster_09_Geraete-Detailansicht.pdf`

Wie erzeuge ich ihn?

1. Haken „Geräte-Detailansicht“ im Fenster „Berichte & Muster …“.

Wie lese ich ihn?

- Eine Karte je Gerät: Scan-Angaben, Name und Ort aus der CMDB, kritische Ports im Klartext, Firewall-Kommunikation mit Quell-/Zielzone, Service, Policy, Aktion und Anzahl.
- Risk-Wert: 2 Punkte je kritischem Port (höchstens 8), +2 bei Herstellermeldung mit CVSS ≥ 7.

Woher kommen die Daten?

- Scan, CMDB, Splunk-Export (Zonen, Services, Policies) und Dokumentations-Datenbank.

Was sagt er nicht?

- Je Richtung nur die 5 häufigsten erlaubten Verbindungen und alle geblockten.

7.10 Gesamtinventar CMDB · Scan · Splunk (Excel)

Datei: `OTScan3_Gesamtinventar_<Datum>.xlsx im Ausgabeordner` · Muster ansehen: `assets/muster/Muster_10_Gesamtinventar.xlsx`

Wie erzeuge ich ihn?

1. Haken „Gesamtinventar“ im Fenster „Berichte & Muster …“ oder Knopf „Gesamtinventar jetzt erstellen“.

Wie lese ich ihn?

- Blatt „Übersicht“: Anzahl je Inventar-Status mit „Was tun?“. Blatt „Gesamtinventar“: eine Zeile je Gerät, je Wert mit Quelle (CMDB, SCAN, SPLUNK).

Woher kommen die Daten?

- CMDB, neuester vollständiger Stufenlauf je Netzwerk und neuestes Splunk-Inventar je Netzwerk.

Was sagt er nicht?

- Netzwerke ohne vollständigen Lauf erscheinen als „Netzwerk offen“.

7.11 Standortbericht (PDF)

Datei: `OTScan3_Standortbericht_<Datum>.pdf` · Muster ansehen: `assets/muster/Muster_11_Standortbericht.pdf`

Wie erzeuge ich ihn?

1. Haken „Standortbericht“; entsteht am Ende einer Netzwerkkette oder mit „Gesamtberichte jetzt erstellen (alle Netzwerke)“.

Wie lese ich ihn?

- Gesamtbild aller Netzwerke mit Ampel, häufigste Dienste, Herstellermeldungen und Applikationen je Netzwerk.

Woher kommen die Daten?

- Neuester vollständiger Lauf je Netzwerk, Gesamtinventar, Splunk-Ablage, Dokumentations-Datenbank.

Was sagt er nicht?

- Ältere Läufe einzelner Netzwerke fließen mit ihrem Stand ein – Datum je Netzwerk beachten.

7.12 Geräteverzeichnis (PDF)

Datei: `OTScan3_Geraeteverzeichnis_<Datum>.pdf` · Muster ansehen: `assets/muster/Muster_12_Geraeteverzeichnis.pdf`

Wie erzeuge ich ihn?

1. Haken „Geräteverzeichnis“; entsteht zusammen mit dem Standortbericht.

Wie lese ich ihn?

- Alle Geräte aller Netzwerke, eine Zeile je Gerät (Querformat), mit Inventar-Status.

Woher kommen die Daten?

- Gesamtinventar.

Was sagt er nicht?

- Enthält alle Adressen – vertraulich behandeln.

7.13 Splunk-Abgleich (CSV und Bericht)

Datei: `Unterordner Splunk des Ausgabeordners: <Netzwerk>_splunkabgleich_<Zeit>.csv, _bericht.md, _ziele.txt, _nachscan.bat bzw. .sh`

Wie erzeuge ich ihn?

1. Seite „Splunk-Abgleich“: Export einfügen oder Datei/Ordner wählen und „Abgleichen“.

Wie lese ich ihn?

- Je IP eine Klasse K1–K6: bestätigt, Port-Lücke, nur Splunk (Server/Client), nur Scan, nur abgewiesen.
- Die Nachscan-Datei prüft gezielt die fehlenden Ports.

Woher kommen die Daten?

- Firewall-Export (z. B. Splunk-Suche über FortiGate-Logs) und die Scan-XML des Netzwerks.

Was sagt er nicht?

- Splunk sieht nur Verkehr über die Firewall.

7.14 Inventar je Netzwerk (HTML/CSV)

Datei: `Dokumente/OTScan3_Inventar/<Netzwerk>_inventar_<Zeit>.html und .csv`

Wie erzeuge ich ihn?

1. Inventar & CMDB → Reiter „Inventar je Netzwerk“ → „Inventar erstellen“; entsteht auch am Ende jedes Stufenlaufs.

Wie lese ich ihn?

- Eine Zeile je Gerät mit Namen, Quelle des Namens, Hersteller, MAC, Beschreibung und offenen Ports.

Woher kommen die Daten?

- Alle Scan-Dateien des Netzwerks im Ausgabeordner, Hersteller-Regeln.

Was sagt er nicht?

- Ohne CMDB-Abgleich – dafür CMDB-Delta oder Gesamtinventar nutzen.

7.15 Erstinbetriebnahme: Protokoll und Paket

Datei: `Dokumente/OTScan3_Abnahmen/<Jahr>/<Protokoll-Nr.>/ (ZIP, internes und externes PDF, offene Punkte)`

Wie erzeuge ich ihn?

1. Seite „Erstinbetriebnahme“ → „Protokoll und Paket erzeugen“.

Wie lese ich ihn?

- Internes Protokoll mit allen Angaben; externes PDF für den Dienstleister ohne Adressen; Liste offener Punkte mit Termin.

Woher kommen die Daten?

- Eingaben der Seite, Scan vorher/nachher am Gerät, Prüfliste.

Was sagt er nicht?

- Nur das externe PDF ist für Dritte gedacht.

8 Nachschlagen

8.1 Wie entstehen die Daten?

Vom Netzwerk bis zum Bericht – in dieser Reihenfolge.

1. **1 Netzwerk und Freigabe**
   Das Netzwerk ist in der Datenpflege angelegt (Name, CIDR, Gateway), die Freigabe des Anlagenverantwortlichen liegt vor, der Adapter steckt im Zielnetzwerk.
2. **2 Stufe 0 – Nachbar-Erkennung**
   ARP bzw. ohne Administratorrechte ein kurzer Verbindungsversuch je Adresse: Welche Adressen sind belegt?
3. **3 Stufe 1 – Geräte finden**
   Schonender TCP-Scan der belegten Adressen auf ein OT-Portset.
4. **4 Stufe 2a/2b – Dienste und Namen**
   TCP mit Versionserkennung und nur lesenden OT-Abfragen (z. B. S7, Modbus-Geräte-ID), danach UDP-Namen (SNMP, BACnet, KNX).
5. **5 Nachscan und Kameras**
   Geräte mit Zeitüberschreitung werden nachgescannt; in CAM-Netzwerken fragt OTScan 3 Kameras per ONVIF ab.
6. **6 Ergebnis-XML**
   Alle Teilläufe werden zu einer Ergebnis-XML je Lauf zusammengeführt.
7. **7 Auswertung**
   Hersteller (MAC-OUI, Hersteller-Regeln), Geräteklasse, unsichere Dienste nach Verkehrsregeln, Herstellermeldungen aus dem CSAF-Bestand, Abgleich mit Splunk und CMDB.
8. **8 Berichte und Inventar**
   PDF, Excel, PowerPoint, Maßnahmenliste, CMDB-Delta/-Nachtrag, Netzwerk-Check, Geräte-Detailansicht; über alle Netzwerke Gesamtinventar, Standortbericht und Geräteverzeichnis.
9. **9 Weitergabe**
   Intern: Berichte und CMDB-Dateien. Nach außen nur Unterlagen ohne Adressen, z. B. das externe PDF der Erstinbetriebnahme.

8.2 Prüffragen der Erstinbetriebnahme

Jede Frage der Seite Erstinbetriebnahme: was sie bedeutet, wofür sie gebraucht wird und warum sie wichtig ist. In OTScan 3 öffnet der Info-Punkt (i) vor der Frage dieselbe Erklärung.

Teil A – Prüfliste mit dem Dienstleister

1. Standardpasswörter geändert, keine gemeinsamen Konten
Was ist das? Ab Werk haben viele Geräte bekannte Kennwörter (admin/admin). Gemeinsame Konten nutzen mehrere Personen.
Wofür wird es benötigt? Nur so lässt sich nachvollziehen, wer was am Gerät geändert hat, und nur so ist der Zugang wirklich geschützt.
Warum ist es wichtig? Standardpasswörter stehen in jedem Handbuch und im Internet – sie sind der häufigste Einstieg für Angreifer (IEC 62443-4-2 CR 1.1/1.5, CRA Anhang I: keine bekannten Standardpasswörter).
Beispiel für die Bemerkung: z. B. admin-Passwort geändert, je Techniker ein Konto

2. Nicht benötigte Dienste abgeschaltet (Telnet, FTP, HTTP, SNMP v1/v2c, Portmapper)
Was ist das? Netzwerkdienste, die das Gerät anbietet, im Betrieb aber niemand braucht.
Wofür wird es benötigt? Der Scan zeigt, welche Ports offen sind; hier bestätigt der Dienstleister, dass nur Benötigtes läuft.
Warum ist es wichtig? Jeder offene Dienst ist eine Angriffsfläche. Telnet, FTP und SNMP v1/v2c übertragen Passwörter im Klartext (Grundsatz der minimalen Funktionalität, IEC 62443-3-3 SR 7.7).
Beispiel für die Bemerkung: z. B. Telnet und FTP aus, HTTP leitet auf HTTPS um

3. Verschlüsselte Varianten genutzt, wo vorhanden (HTTPS, SSH, SNMPv3)
Was ist das? Die sichere Variante eines Protokolls: HTTPS statt HTTP, SSH statt Telnet, SNMPv3 statt v1/v2c.
Wofür wird es benötigt? Zugangsdaten und Einstellungen gehen verschlüsselt über das Netzwerk.
Warum ist es wichtig? Unverschlüsselt können Kennwörter im Netzwerk mitgelesen und Befehle verändert werden (IEC 62443-4-2 CR 4.1).
Beispiel für die Bemerkung: z. B. Weboberfläche nur HTTPS, SNMPv3 mit authPriv

4. Firmware auf dem vom Hersteller empfohlenen Stand
Was ist das? Die Gerätesoftware. Der Hersteller nennt einen empfohlenen bzw. sicherheitsgepatchten Stand.
Wofür wird es benötigt? Der Stand wird im Protokoll und in der CMDB festgehalten und mit den Herstellermeldungen abgeglichen.
Warum ist es wichtig? Alte Firmware hat oft bekannte, veröffentlichte Schwachstellen. Nach der Abnahme ist ein Update viel aufwendiger.
Beispiel für die Bemerkung: z. B. 7.80.0128 = aktuelle Empfehlung laut Hersteller

5. Fernzugang nur über freigegebenen Weg, sonst abgeschaltet
Was ist das? Wartungszugänge von außen: Cloud-Dienste, Modems, Fernwartungsboxen, Hersteller-Portale.
Wofür wird es benötigt? Fernwartung ist erlaubt, aber nur über den freigegebenen Weg des Standorts.
Warum ist es wichtig? Ungeplante Fernzugänge umgehen Firewall und Freigaben – sie sind ein typischer Einfallsweg in OT-Netzwerke.
Beispiel für die Bemerkung: z. B. kein Hersteller-Cloud-Zugang, Fernwartung nur über RSA

6. Uhrzeit/NTP und Protokollierung eingestellt
Was ist das? Die Uhr des Geräts wird über einen Zeitserver gestellt; Ereignisse werden protokolliert.
Wofür wird es benötigt? Bei Störungen oder Vorfällen lassen sich Ereignisse mehrerer Geräte zeitlich zuordnen.
Warum ist es wichtig? Ohne richtige Uhrzeit und Protokoll ist eine Fehler- oder Vorfallsanalyse kaum möglich (IEC 62443-4-2 CR 2.8/2.11).
Beispiel für die Bemerkung: z. B. NTP auf Zeitserver des Netzwerks, Syslog aktiv

7. Konfigurationssicherung an den Betreiber übergeben
Was ist das? Eine Kopie der fertigen Geräteeinstellungen.
Wofür wird es benötigt? Bei Defekt oder Austausch lässt sich das Gerät schnell und gleich wieder einrichten.
Warum ist es wichtig? Ohne Sicherung hängt der Betrieb am Dienstleister; nach einem Ausfall dauert die Wiederherstellung lange.
Beispiel für die Bemerkung: z. B. Sicherung als Datei an den Betreiber übergeben (Datum, Version)

8. Befunde des Scans vor Ort behoben und nachgescannt
Was ist das? Was der Scan „vorher" gefunden hat, wird vor Ort korrigiert und mit „Nachscan (nachher)" bestätigt.
Wofür wird es benötigt? Belegt im Protokoll, dass die Abweichungen wirklich weg sind.
Warum ist es wichtig? Solange der Dienstleister vor Ort ist, ist eine Korrektur schnell und ohne Zusatzauftrag möglich.
Beispiel für die Bemerkung: z. B. HTTP abgeschaltet, Nachscan ohne Befund

Unterlagen des Herstellers

9. EU-Konformitätserklärung mit CRA-Bezug (Pflicht ab 11.12.2027)
Was ist das? Die Erklärung des Herstellers, dass das Produkt die EU-Anforderungen erfüllt – künftig auch den Cyber Resilience Act.
Wofür wird es benötigt? Nachweis für Einkauf und Betrieb, dass das Produkt in der EU in Verkehr gebracht werden darf.
Warum ist es wichtig? Ab 11.12.2027 brauchen Produkte mit digitalen Elementen den CRA-Bezug; ohne ihn ist ein Einsatz rechtlich problematisch.
Beispiel für die Bemerkung: z. B. liegt vor, Datei EU-DoC_FLEXIDOME.pdf

10. Zertifikat IEC 62443-4-2 / IEC 62443-4-1
Was ist das? Prüfzertifikat zur Sicherheit des Produkts (4-2) bzw. des Entwicklungsprozesses beim Hersteller (4-1).
Wofür wird es benötigt? Zeigt, für welches Sicherheitsniveau (SL) das Gerät ausgelegt ist.
Warum ist es wichtig? IEC 62443-4-2 beschreibt die Sicherheitsanforderungen an OT-Komponenten; das Zertifikat ist der einfachste Nachweis.
Beispiel für die Bemerkung: z. B. 4-2 SL2, Zertifikat TÜV Nr. ...

11. SBOM für den installierten Firmware-Stand
Was ist das? Software-Stückliste: welche Bibliotheken und Versionen in der Firmware stecken.
Wofür wird es benötigt? Damit lässt sich prüfen, ob eine neu bekannt gewordene Schwachstelle (z. B. in OpenSSL) das Gerät betrifft.
Warum ist es wichtig? Ohne SBOM bleibt bei jeder neuen Schwachstelle nur Raten oder Nachfragen beim Hersteller; der CRA fordert sie.
Beispiel für die Bemerkung: z. B. SBOM (CycloneDX) zu Firmware 7.80 angefordert

12. Ende des Supportzeitraums für Sicherheitsupdates bekannt
Was ist das? Das Datum, bis zu dem der Hersteller Sicherheitsupdates liefert.
Wofür wird es benötigt? Planungsgrundlage für Austausch oder Schutzmaßnahmen nach Supportende.
Warum ist es wichtig? Geräte ohne Updates werden mit jeder neuen Schwachstelle unsicherer; der CRA verlangt die Angabe.
Beispiel für die Bemerkung: z. B. Sicherheitsupdates bis 12/2031

13. Härtungsleitfaden / Sicherheitshandbuch des Herstellers
Was ist das? Anleitung des Herstellers, wie das Gerät sicher eingestellt wird.
Wofür wird es benötigt? Grundlage für die Prüfliste oben und für spätere Änderungen.
Warum ist es wichtig? Nur der Hersteller kennt alle Einstellungen; ohne Leitfaden bleiben Sicherheitsfunktionen oft ungenutzt.
Beispiel für die Bemerkung: z. B. Security Guide V2.1 liegt vor

Teil B – Erstabnahme im Zielnetzwerk

14. Gerät im geplanten Netzwerk / VLAN und mit geplanter IP
Was ist das? Teil B: Das eingebaute Gerät hängt im vorgesehenen Netzwerk mit der geplanten Adresse.
Wofür wird es benötigt? Nur dann greifen Firewall-Regeln, Überwachung und CMDB-Eintrag.
Warum ist es wichtig? Ein Gerät im falschen Netzwerk umgeht die Netzwerktrennung und taucht in keiner Regel auf.
Beispiel für die Bemerkung: z. B. Beispiel_140_CAM, IP wie geplant

15. Nur die in Teil A abgenommenen Dienste offen
Was ist das? Vergleich: Im Zielnetzwerk sind dieselben Ports offen wie bei der Abnahme am Gerät.
Wofür wird es benötigt? Zeigt, dass beim Einbau nichts zurückgestellt oder zusätzlich eingeschaltet wurde.
Warum ist es wichtig? Nach Werksreset oder Konfigurationsimport sind oft wieder alle Dienste aktiv.
Beispiel für die Bemerkung: z. B. 443 und 554 wie in Teil A, keine neuen Ports

16. Kommunikation nur über freigegebene Wege (Firewall-/Splunk-Abgleich)
Was ist das? Abgleich mit den Firewall-Daten aus Splunk: mit wem das Gerät wirklich spricht.
Wofür wird es benötigt? Findet Verbindungen, die nicht beantragt sind (z. B. ins Internet oder zu Hersteller-Servern).
Warum ist es wichtig? Unerwarteter Verkehr ist ein Hinweis auf Fehlkonfiguration oder unerlaubte Fernzugänge (Bewertung nach Verkehrsregeln).
Beispiel für die Bemerkung: z. B. Splunk zeigt nur Verkehr zum Rekorder und NTP

17. CMDB-Eintrag angelegt bzw. aktualisiert (MAC, IP, Firmware, Ports)
Was ist das? Das Gerät wird mit seinen Kenndaten im Inventar (CMDB) geführt.
Wofür wird es benötigt? Grundlage für Betrieb, Störungsbearbeitung, Patch-Management und spätere Abgleiche.
Warum ist es wichtig? Was nicht in der CMDB steht, wird nicht überwacht, nicht gepatcht und bei Vorfällen nicht gefunden.
Beispiel für die Bemerkung: z. B. CMDB-Nachtrag aus OTScan 3 übernommen

18. Sollzustand in OTScan 3 übernommen
Was ist das? Die abgenommenen offenen Ports werden als Sollzustand des Geräts gespeichert.
Wofür wird es benötigt? Spätere Scans vergleichen gegen diesen Stand und melden Abweichungen.
Warum ist es wichtig? So fällt auf, wenn später jemand einen Dienst einschaltet oder das Gerät verändert wird.
Beispiel für die Bemerkung: z. B. Knopf „Sollzustand übernehmen“ am 03.11.2026

8.3 Glossar

Adapter
Netzwerkanschluss des Scan-Rechners. Gescannt wird immer über den Adapter, der im Zielnetzwerk steckt.

Ampel
GRÜN = kein unsicherer Dienst, GELB = mindestens ein unsicherer Dienst nach den Verkehrsregeln – geplant schließen, GRAU = keine Bewertung möglich (keine Angaben zu Diensten).

ARP
Adressauflösung im lokalen Netzwerk; jedes Gerät beantwortet ARP, auch wenn alle Ports zu sind.

CAM-Netzwerk
Netzwerk mit „CAM“ im Namen (z. B. Halle3_CAM): bekommt das Kameraprofil mit Kameraports und ONVIF-Abfrage.

CIDR
Schreibweise für ein Netzwerk mit Präfix, z. B. 192.168.30.0/24.

CMDB
Inventar (CMDB): Ihre Geräteliste als Excel (Vorlage aus OTScan 3 oder eigene Liste). OTScan 3 liest sie nur.

CSAF
Maschinenlesbares Format für Sicherheitsmeldungen von Herstellern; OTScan 3 bringt einen Offline-Bestand öffentlicher Quellen mit.

CSV-Vorlage
Tabelle zum Ausfüllen für Stammdaten (Netzwerke, Scan-MAC-Liste, Hersteller-Regeln, Scan-Profile, Zeitplan).

Datenpflege
Seite für alle Stammdaten: Netzwerke, Scan-MAC-Liste, CMDB, Splunk, Scan-Profile, Verlauf, Abnahmen.

Direktanschluss
Scan-Rechner direkt per Kabel am Gerät (Teil A der Erstinbetriebnahme).

Gesamtinventar
Excel mit allen Geräten aus CMDB, Scan und Splunk – je Wert mit Quelle.

Hersteller-Regel
Eigene Korrektur für Hersteller oder Betriebssystem, z. B. MAC-Präfix 00:30:D6 → Bosch Rexroth.

Herstellermeldung
Sicherheitsmeldung eines Herstellers zu Modell und Firmware; Güte exakt, modell oder hersteller.

IEC 62443
Normenreihe für die Sicherheit industrieller Automatisierung (Zonen, Conduits, Sicherheitsniveaus).

MAC-Adresse / OUI
Hardware-Adresse; die ersten drei Bytes (OUI) nennen den Hersteller der Netzwerkkarte.

Netzwerkkette
Mehrere Netzwerke nacheinander über einen Adapter scannen – mit Scan-MAC oder VLAN je Netzwerk.

nmap
Freier Netzwerkscanner (nmap.org), mit dem OTScan 3 scannt; wird separat installiert.

NSE
Skripte für nmap; OTScan 3 bringt nur lesende OT-Abfragen mit (z. B. S7, Modbus, BACnet, KNX, Janitza).

ONVIF
Standard für IP-Kameras; mit einem nur lesenden Benutzer liefert er Hersteller, Modell und Firmware.

Portset
Liste der Ports, die ein Scan prüft, z. B. ICS_LIGHT_v2 oder ICS_OT_CORE.

Scan-MAC
Registrierte MAC-Adresse, mit der der Adapter in einem Netzwerk mit Zugangskontrolle zugelassen ist.

Schnellscan
Einfache Ansicht: ein Netzwerk mit einem Knopf schonend prüfen.

Shadow-Gerät
Gerät, das im Scan oder im Firewall-Verkehr auftaucht, aber nicht in der CMDB steht.

Sollzustand
Gespeicherter Stand eines Geräts oder Netzwerks nach der Abnahme; spätere Scans vergleichen dagegen.

Splunk
Auswertung von Firewall-Logs; OTScan 3 liest Exporte im Format v2 (Regeln und Inventar je Netzwerk).

Stufenlauf
„Netzwerk komplett scannen“: Stufe 0 bis 2b, Nachscan, Kameraabfrage und Ende nacheinander.

Unsicherer Dienst
Dienst, den die Verkehrsregeln verbieten oder nur abgesichert erlauben (z. B. Telnet, FTP, HTTP-Anmeldung, SNMPv1/v2c).

Verkehrsregeln
Bewertungsgrundlage für Dienste und Verbindungen: HanselCraft-Voreinstellung, angelehnt an IEC 62443, vom Anwender anpassbar.

Zone / Service / Policy
Aus dem Firewall-Log: Sicherheitszone von Quelle und Ziel, Dienstname und Nummer der Firewall-Regel.

8.4 Häufige Fragen

Darf ich den Schnellscan im laufenden Betrieb starten?
Ja, mit Freigabe des Anlagenverantwortlichen. Er ist gedrosselt, liest nur und macht keinen Tiefenscan. Den vollständigen Stufenlauf stimmen Sie besser mit einem Wartungsfenster ab.

Warum findet der Scan weniger Geräte als Splunk kennt?
Manche Geräte antworten nicht (Firewall am Gerät, ausgeschaltet, falsches Netzwerk) oder sprechen nur nach außen. Sie stehen im CMDB-Nachtrag und im Gesamtinventar als „nur Verkehr“.

Welchen Bericht brauche ich?
Anlagenverantwortliche: PDF-Kompaktbericht. Technik: Excel und Maßnahmenliste. Management: PowerPoint. Inventarisierung: Gesamtinventar und CMDB-Delta. Alle Netzwerke: Standortbericht.

Muss ich jeden unsicheren Dienst sofort abschalten?
Nein. Erst mit dem Betreiber klären, ob der Dienst gebraucht wird. „Ohne Firewall-Verkehr“ ist ein Hinweis, aber kein Beweis, dass er unbenutzt ist.

Wie bekomme ich Modell und Firmware einer Kamera?
Für das CAM-Netzwerk unter Datenpflege → „Kamera-Zugangsdaten …“ einen nur lesenden ONVIF-Benutzer hinterlegen. Nach drei falschen Anmeldungen je Lauf versucht OTScan 3 es nicht weiter.

Kann ich einen Scan über Nacht laufen lassen?
Ja: Zeitplan → „Geplanten Scan anlegen“ oder eine Netzwerkkette mit Startfenster. Der Rechner muss eingeschaltet und im Zielnetzwerk sein.

Woher kommen die Herstellernamen?
Aus der MAC-Adresse (OUI), aus Dienstkennungen und OT-Abfragen. Irreführende Namen korrigieren Sie mit Hersteller-Regeln.

Werden meine Daten irgendwohin gesendet?
Nein. Alle Daten bleiben auf dem Rechner. Ins Internet geht OTScan 3 nur beim Aktivieren der Lizenz und wenn Sie „Online aktualisieren“ für die Herstellermeldungen drücken.

Wo liegen die Berichte?
Im Ausgabeordner (Standard: Dokumente), Inventar in OTScan3_Inventar, Splunk-Ablage in OTScan3_Splunk, Erstinbetriebnahme-Pakete in OTScan3_Abnahmen.

Warum fehlt das PDF und es liegt eine HTML-Datei da?
Für die neuen PDF-Berichte braucht OTScan 3 Microsoft Edge, Google Chrome oder Chromium. Ohne Browser bleibt die HTML-Datei – im Browser öffnen und als PDF drucken.

Wie ziehe ich auf einen neuen Rechner um?
Datenpflege → „Datensicherung …“ → „Sicherung erstellen …“, auf dem neuen Rechner „Sicherung einspielen …“. Kamera-Passwörter werden nicht gesichert.

Woran erkenne ich die Version?
Unten rechts in der Fußzeile steht „OTScan 3 3.0.0 · Build …“, links unten unter „Hilfe“ die Versionsnummer.

9 Dokumente im Paket und Hilfe

Datei	Inhalt
`OTScan3_Kurzanleitung.pdf`	OTScan 3 in 15 Minuten
`OTScan3_Anwenderhandbuch.pdf`	dieses Handbuch
`OTScan3_Installationsanleitung_Windows.pdf`	nmap/Npcap, INSTALL.bat, Lizenz, Umzug
`OTScan3_Installationsanleitung_Linux.pdf`	install_linux.sh, Rechte, Selbsttest
`OTScan3_Berichte_lesen.pdf`	welcher Bericht für wen, Ampel, Verkehrsregeln
`OTScan3_Technik_Sicherheit_Datenschutz.pdf`	für IT-Sicherheit und Datenschutz
`OTScan3_Neu_in_3.0.pdf`	Neuerungen gegenüber OTScan 2.3
`CHANGELOG.txt`	Änderungsprotokoll
`EULA_Lesehinweis.txt`	wo Lizenzvertrag, Haftungshinweise und Drittlizenzen liegen
`Dateinamen mit _EN`	englische Fassungen (README_EN.txt, *_EN.pdf, CHANGELOG_EN.txt)

Hilfe im Programm: **Info** oben rechts auf jeder Seite (F1). Fragen, Lizenzen und Aktualisierungen: `otscan.hanselcraft.de` · `info@hanselcraft.de`. Bitte bei Rückfragen den Lagebericht von `PRUEFEN.bat` (Windows) bzw. das Ergebnis von `selbsttest.sh` (Linux) beilegen – ohne Scan-Ergebnisse und Berichte, denn diese enthalten Adressen Ihrer Anlagen.