USER MANUAL

User manual

Everything about OTScan 3 in one place: installation, scanning, results, reports, master data and initial commissioning – illustrated with the Musterwerk Halle 3 sample plant.

Version 3.0.0 · 12 Nov 2026
HanselCraft · otscan.hanselcraft.de

Contents

1 About this manual 4

2 Basics 5

2.1 Overview and first steps 5

2.2 Installation under Windows and setup wizard 6

2.3 Installation under Linux 9

2.4 Help in the program: info and manual 11

2.5 Security and data protection 12

2.6 Security with administrator rights 14

3 New in OTScan 3 16

4 Scan 18

4.1 Quick scan – check network 18

4.2 Scan center and staged scan 19

4.3 Network chain – many networks one after the other 22

4.4 Schedule – recurring scans 25

4.5 Initial commissioning and initial acceptance 26

4.6 Direct connection to a machine 28

4.7 Acceptances 30

5 Results 32

5.1 History 32

5.2 Splunk comparison, Splunk storage and Splunk database 33

5.3 CMDB comparison 36

5.4 Inventory per network 37

5.5 Vendor advisories (CSAF) and action list 39

5.6 Reports and documents 41

5.7 Evidence & deadlines 45

6 Settings 47

6.1 Data maintenance – maintain all master data yourself 47

6.2 Create, edit and import networks 49

6.3 Set up adapter and Scan MAC 50

6.4 Download, fill in and upload CSV templates 52

6.5 Scan profiles and port sets 54

6.6 Vendor rules 56

6.7 Camera profile and camera credentials 57

6.8 Backup and moving to a new computer 59

6.9 Interface language / Language 61

6.10 Your own company logo in reports 63

6.11 AI assistant (Claude Desktop, MCP) 64

7 Reports and exports 67

7.1 PDF compact report 67

7.2 PDF detailed 67

7.3 Excel report per network 68

7.4 PowerPoint (management) 68
7.5 Action list (Excel) 68
7.6 CMDB delta (Excel) 69
7.7 CMDB addendum (Excel) 69
7.8 Network check (PDF) 69
7.9 Device detail view (PDF) 70
7.10 Overall inventory CMDB · scan · Splunk (Excel) 70
7.11 Site report (PDF) 71
7.12 Device directory (PDF) 71
7.13 Splunk comparison (CSV and report) 71
7.14 Inventory per network (HTML/CSV) 72
7.15 Initial commissioning: report and package 72

8 Reference 73
8.1 How is the data created? 73
8.2 Initial commissioning check questions 73
8.3 Glossary 76
8.4 Frequently asked questions 78

9 Documents in the package and help 80

1 About this manual

This manual is the print version of the user manual that OTScan 3 opens in the browser via "Info" → "Manual" (`handbuch/index_en.html`). It has the same chapters as the info help in the program; every chapter starts with "What for?", followed by "How it works", "What do I enter where?" and screenshots.

Published by HanselCraft (hanselcraft.de). Screenshots and samples come from the fictitious "Musterwerk Halle 3" sample plant (networks Montage_Anlagennetz, Halle3_CAM, Presse_Maschinennetz, Energieverteilung, Lackiererei_Leitstand, Prueffeld; 192.168.30.0/24 to 192.168.35.0/24). Device names, addresses and MAC addresses are examples.

> OTScan 3 only reads. It does not change devices, does not try passwords and does not use attack or load-test scripts. A scan is still network traffic: obtain the plant owner's approval before the first scan.

Button and menu labels are written as they appear in the program, e.g. **Info** . Some screenshots show the German user interface; the layout is the same in every language. Version 3.0.0, as of 12 Nov 2026.

2 Basics

2.1 Overview and first steps

What OTScan 3 is, how the interface is structured and how the first scan works.

What for?

OTScan 3 is a network scanner for plant networks (OT). It finds devices, detects their services and assesses them against adjustable traffic rules (HanselCraft default, based on IEC 62443). There are two editions in one program: the quick scan (one button, for all users) and the Advanced Edition (staged scan, network chain, comparisons, initial commissioning – for trained users). The program runs under Windows and under Linux with the same functions. This section is the starting point for new users.

Important

- OTScan 3 only reads: no write commands, no password attempts, no vulnerability tests. The only credentials in the standard run are the SNMP community "public" and – in CAM networks – a voluntarily stored, read-only ONVIF user.
- Only scan a network with the approval of the plant owner. Do not change or delete any files or settings during a run.
- The program only sees what responds, and only on the checked ports. A silent device is missing from the result.
- All data stays on the scan PC (no cloud, no telemetry). Database and settings are located in %APPDATA%\OTScan3, reports in the Documents folder.

How it works

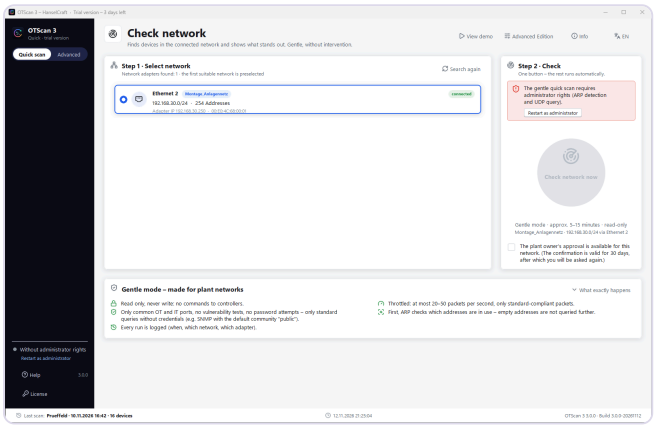
1. Start the program via the desktop icon "OTScan3" and confirm the prompt for administrator rights with "Yes".
2. Switch between "Quick scan" and "Advanced" at the top left. OTScan 3 remembers the edition and page for the next start.
3. The sidebar of the Advanced Edition has three groups: SCAN (Scan center, Schedule, Initial commissioning), RESULTS (History, Splunk comparison, Inventory & CMDB) and SETTINGS (Scan profiles, Data maintenance).
4. Merged sections have tabs at the top of the page header: Initial commissioning | Acceptances, CMDB comparison | Inventory per network and in Data maintenance Master data | Vendor rules | Splunk database ... | Camera credentials ....
5. On every page at the top right: "Info" opens the step-by-step help for the page. F1 also opens the info.
6. Before the first scan: obtain the approval of the plant owner, create the network in Data maintenance (Networks tab) or import it via CSV template, and set up the matching adapter.
7. Start the first scan: in the quick scan "Check network now" or in the Scan center "Scan entire network".
8. Reading the result: PDF page 1 (traffic light, the most important points, what to do), Excel for details, PowerPoint for meetings. Where each file is located is explained in the "Reports and documents"

section.

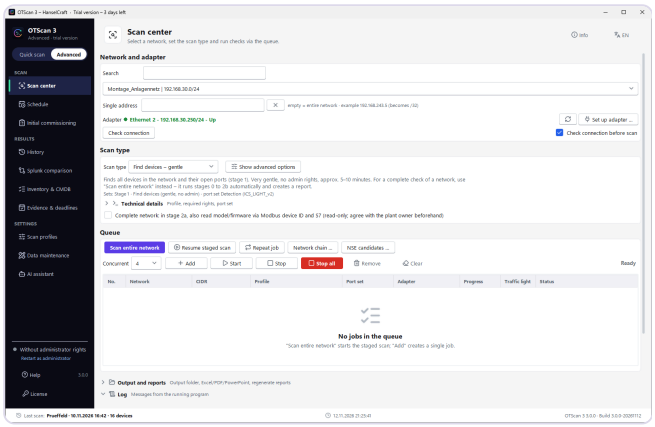
9. "Administrator rights active" is shown at the bottom left when OTScan 3 runs as administrator. Without administrator rights there is no quick scan, no ARP and no UDP queries. The build identifier is shown at the bottom right, for example "OTScan 3 3.0.0 · Build 3.0.0-20261112".

What do I enter where?

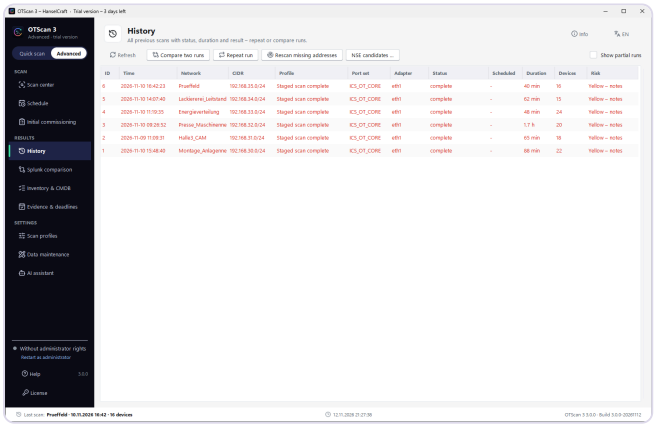
Field	Meaning
Quick scan | Advanced	Switch at the top left: simple check with one button or the full Advanced Edition.
Sidebar	Page selection: SCAN, RESULTS, SETTINGS.
Tabs in the page header	Switch between related parts of a page, for example CMDB comparison and Inventory per network.



Overview and first steps



Overview and first steps



Overview and first steps

2.2 Installation under Windows and setup wizard

Install OTScan 3 under Windows and set it up with the setup wizard at the first start.

What for?

Installation under Windows is done by INSTALL.bat: it asks once for administrator rights, checks whether nmap and Npcap are installed, copies the program to C:\Program Files\OTScan3 and creates the desktop

icon "OTScan3". On a new computer, OTScan 3 starts without data. The setup wizard then opens by itself and asks what you need: Minimal (quick scan only), Standard (network list, reports, CMDB comparison) or Complete (additionally Scan MAC list, network chain, Splunk, cameras, initial commissioning). "Detect automatically" searches for existing network lists, CMDB and Scan MAC lists and suggests the matching template.

Important

- "Set up later" closes the wizard. You can open it again at any time via Data maintenance → "Setup wizard ...".
- "Detect automatically" does not import anything without your click – found files are only suggested.
- While ERSTINSTALLATION_MIT_BILDERN.bat is running, do not use the mouse and keyboard (the script takes screenshots).
- A workstation that already has networks does not get the wizard automatically. Existing data in %APPDATA%\OTScan3 is kept during a reinstallation.

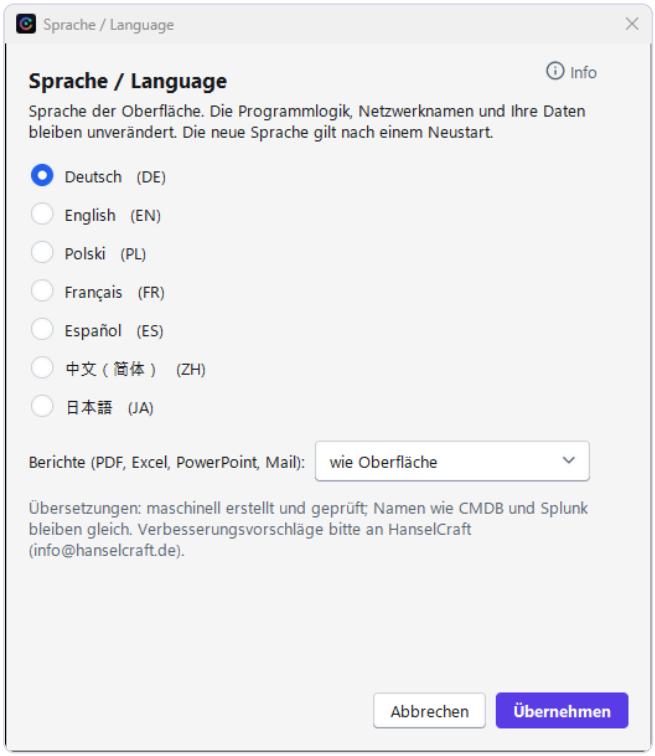
How it works

1. Unpack the ZIP package completely into a folder (do not start from within the ZIP).
2. Double-click INSTALL.bat and answer the prompt for administrator rights with "Yes". The window shows whether nmap and Npcap were found, sets up the program and reports the result at the end. nmap and Npcap are not part of the package: if they are missing, first run the nmap setup from https://nmap.org/download.html as administrator (install Npcap with it) and then start INSTALL.bat again.
3. For trying out without changing the system, there is TESTINSTALLATION.bat (separate folder, separate data). ERSTINSTALLATION_MIT_BILDERN.bat additionally creates an illustrated guide (PDF) for this computer.
4. Start OTScan 3 via the desktop icon and confirm the prompt for administrator rights with "Yes". Without data, the setup wizard opens after a few seconds.
5. Select the template: Minimal, Standard, Complete or "Detect automatically" – then "Next".
6. Enter networks: name, network (CIDR) and gateway, then "Add". Or "Import network list ..." or "Open empty template".
7. Standard and Complete: select the CMDB file, create an empty CMDB or skip the step.
8. Complete: import the Scan MAC list or accept the suggestions, create the Splunk input, store the camera credentials.
9. "Finish" – OTScan 3 opens the matching view. Again later: SETTINGS → Data maintenance → button "Setup wizard ...".
10. SELBSTTEST.bat checks the installation without scanning a network.

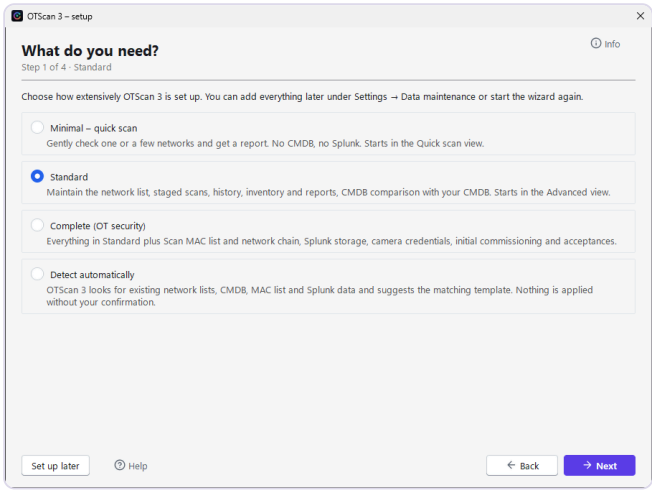
What do I enter where?

Field	Meaning
Template	Minimal, Standard, Complete or Detect automatically – determines which steps the wizard shows.
Name	Network name, for example Montage_Anlagennetz. Must be named exactly as in Splunk and in the Scan MAC list.

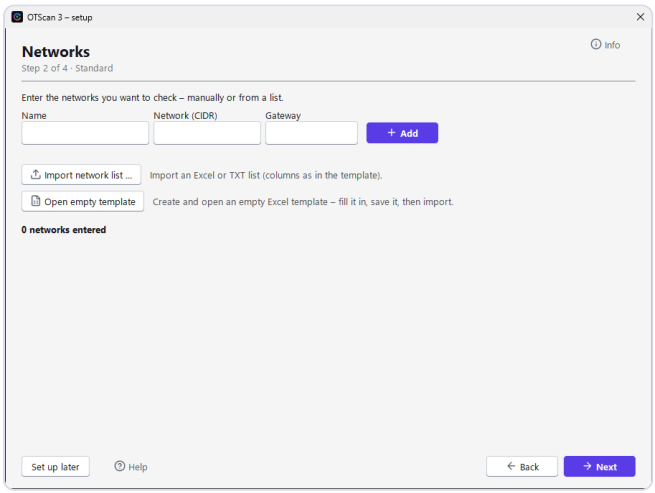
Field	Meaning
Network (CIDR)	Address range with mask, for example 192.168.6.0/24. The host bits must be 0.
Gateway	Address of the gateway in the network, for example 192.168.6.1 (optional).
CMDB file	Your inventory Excel file (sheet "CMDB"). Only read.
Scan MAC list	Excel or CSV list with Scan MAC and scan IP per network (Complete template only).
Camera credentials	Read-only ONVIF user and password for CAM networks (optional).



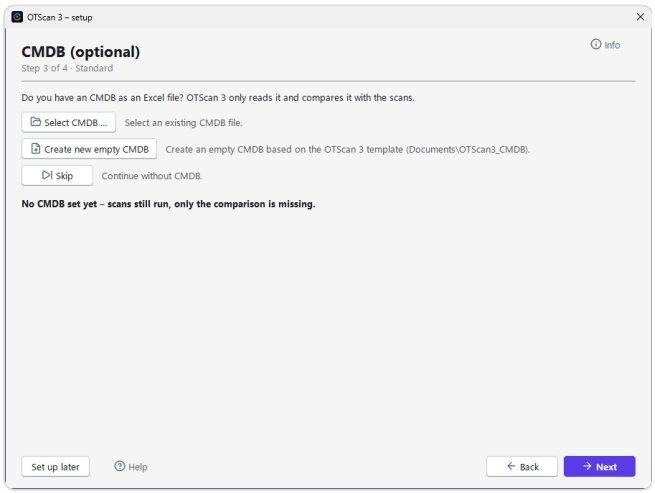
Installation under Windows and setup wizard



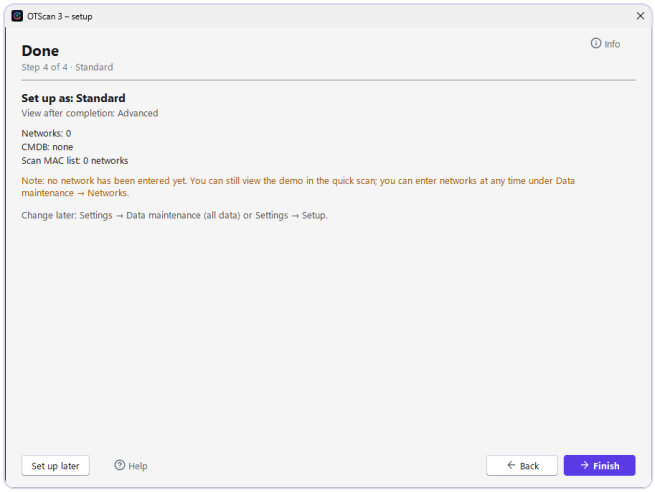
Installation under Windows and setup wizard



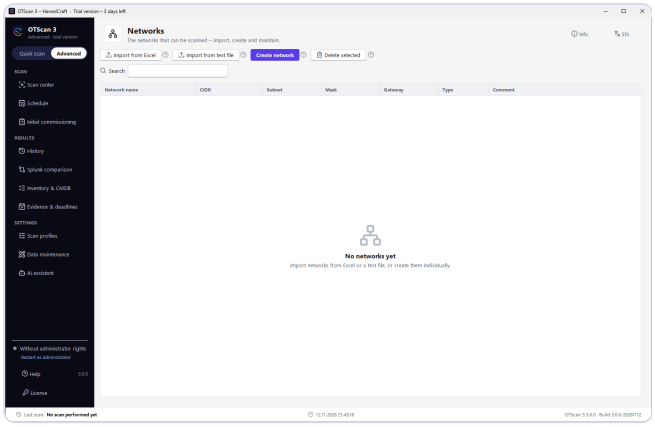
Installation under Windows and setup wizard



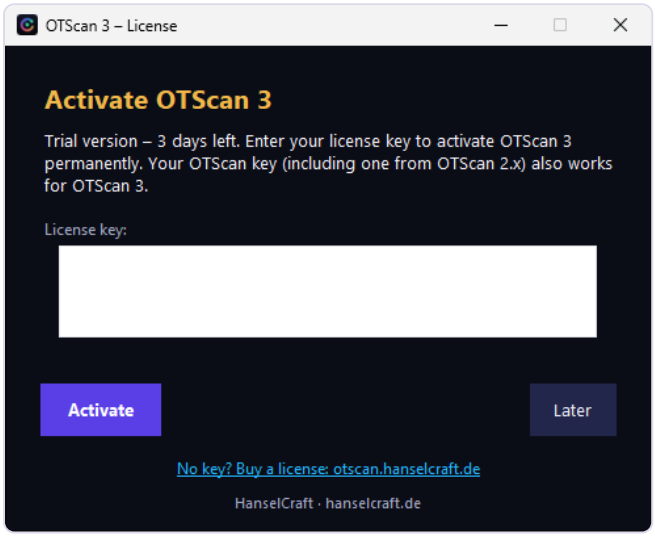
Installation under Windows and setup wizard



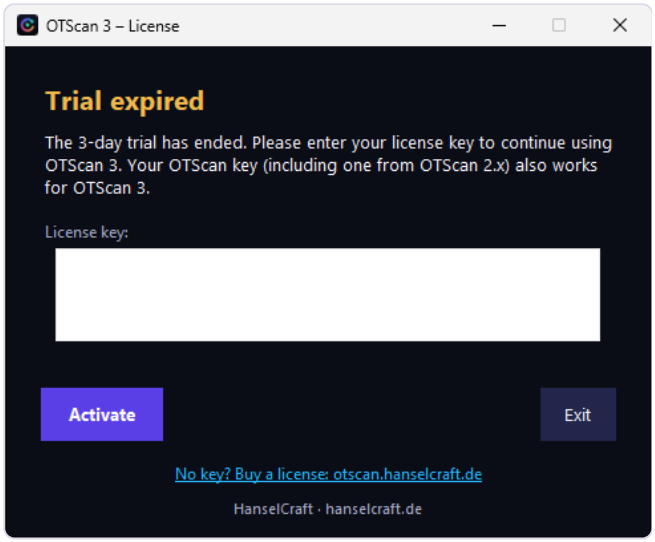
Installation under Windows and setup wizard



Installation under Windows and setup wizard



Installation under Windows and setup wizard



Installation under Windows and setup wizard

2.3 Installation under Linux

Set up, start, check OTScan 3 under Ubuntu, Debian or Fedora with install_linux.sh, transfer data and remove it again.

What for?

Under Linux, the install_linux.sh script sets up everything once: packages (nmap, python3-tk, iproute2, iputils-arping, cron, Chromium, secret-tool, mpg123), a Python environment in the ./venv subfolder, the nmap rights via setcap (scans without root) and the "otscan3" group with a sudo rule only for the network helper /usr/local/lib/otscan3/otsp-netz. The helper only executes the commands needed to switch the scan adapter (ip, arping, nmcli, dhclient, dhcpcd or networkctl), checks every argument and rejects everything else. After that you start OTScan 3 as a normal user.

Important

- Never start OTScan 3 with sudo. The required rights come via setcap (nmap) and the sudo rule of the "otscan3" group.
- Without the sudo rule (setup with OTSP_OHNE_SUDOREGEL=1), OTScan 3 scans normally, but switching the adapter (set up adapter, network chain, direct connection) is then locked – with a note.
- After an nmap update, the rights are lost. Then run install_linux.sh again or check the rights with getcap.
- PDF reports need Chromium, Google Chrome or Microsoft Edge. If Chromium is missing after installation, the script reports it with a note.

How it works

1. Unpack the package and copy the program folder to its fixed location, for example to /opt/otscan3. Open a terminal in the program folder.
2. Set up: enter sudo ./install_linux.sh <username>. As the user name, specify the login name of the person who will scan later.
3. The script works through six sections: "== 1. Pakete" (core packages separately; missing additional packages only as a note), "== 2. Python-Bibliotheken (./venv)" (rebuilt and only swapped on success), "== 3. nmap-Rechte" (shows the getcap line), "== 4. sudo-Regel ..." (shows "Gruppe otscan3: <benutzer>"), "== 5. Startmenü" and "== 6. Selbsttest". At the end it says "Fertig." ("Done").
4. Log out and log in again once. Only then does the "otscan3" group take effect.
5. Check the rights: getcap "$(readlink -f "$(command -v nmap)")" must show "cap_net_admin,cap_net_bind_service,cap_net_raw=eip"; sudo -n /usr/local/lib/otscan3/otsp-netz ip link show lo must respond without a password prompt; id must contain the group "otscan3".
6. Start: ./otscan3.sh in the program folder or start menu "OTScan3" – as a normal user, NOT with sudo. "Administrator rights active" must be shown at the bottom left. At the first start without data, the setup wizard opens.
7. Transferring data from Windows (optional): close OTScan 3 on both computers. Copy the Windows data folder OTScan 3 (in the user profile under AppData/Roaming) to ~/.local/share/OTScan3 and the folders Dokumente/OTScan3_* to the Documents folder (e.g. ~/Documents or ~/Dokumente). Then re-enter the camera passwords; check scheduled scans with crontab -l and re-create missing ones in the schedule.
8. Network adapter: if NetworkManager manages the scan adapter, OTScan 3 creates a dedicated connection profile "OTScan 3 <Netzwerk>" during setup (without default gateway, kept after a restart) – first only with the Scan MAC, after the address conflict check with the scan IP. If a step fails, OTScan 3 removes the profile again. "Reset" deletes this profile and reactivates the previous connection; if none was active, the adapter is released. If systemd-networkd manages the adapter, OTScan 3 aborts with a note.
9. Uninstalling: delete the program folder including the venv subfolder; sudo rm /etc/sudoers.d/otscan3; sudo rm -r /usr/local/lib/otscan3; remove the nmap rights with sudo setcap -r "$(readlink -f "$(command -v nmap)")"; delete the start menu entry ~/.local/share/applications/otscan3.desktop; remove scheduled scans with crontab -e. Your data in ~/.local/share/OTScan3 and the Documents folder (e.g. ~/Documents or ~/Dokumente) is kept until you delete it yourself.

What do I enter where?

Field	Meaning
<username>	Login name of the person who uses OTScan 3. They become a member of the "otscan3" group.
OTSP_OHNE_SUDOREGEL=1	Optionally set before the call: the script then does not create a sudo rule (no switching of the adapter).
Program folder	Fixed location of the program, for example /opt/otscan3. otscan3.sh and venv are located there.

2.4 Help in the program: info and manual

At the top right of every page "Info" (step-by-step help). F1 opens the info for the current page.

What for?

Help is where you work: "Info" opens the "Info – how it works" window to the right of the page with a short description, "What for?", the numbered steps "How to proceed", "What do I enter where?" and "Important". From there you can open the manual if needed. Everything runs offline, without internet.

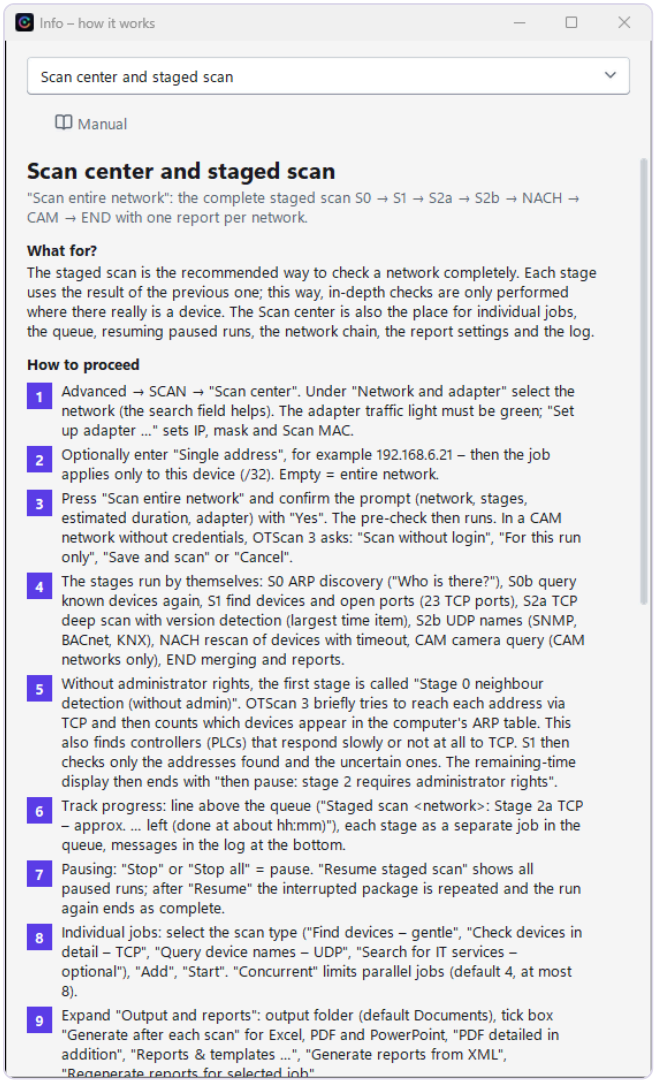
> **Important**
>
> - If no manual is installed, the manual buttons open the info on the matching topic instead.

How it works

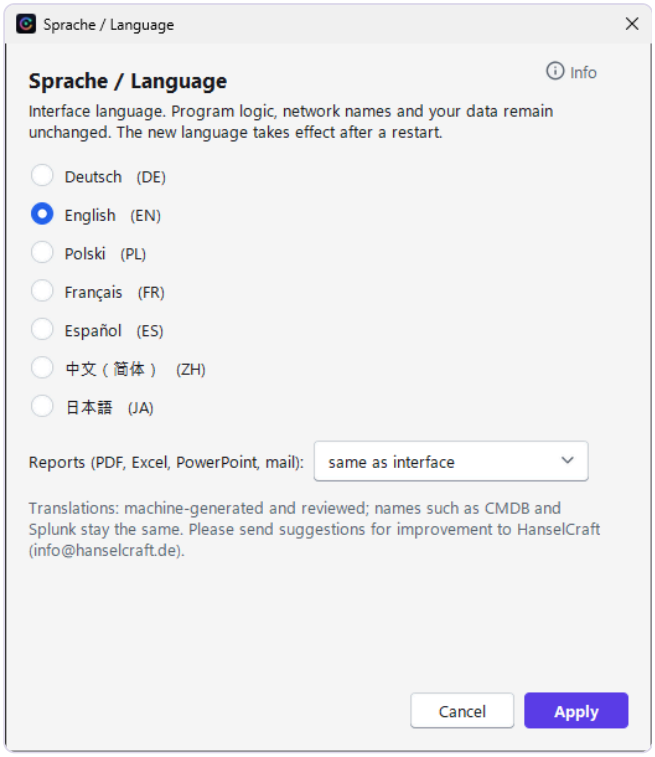
1. Click "Info" at the top right of the page – or press F1. "Info – how it works" opens on the right for the topic of the page.
2. Reading: title and short description, "What for?", "How to proceed" (numbered steps), "What do I enter where?" (every field explained) and "Important".
3. "Manual" opens this manual in the browser directly at the matching section.
4. At the top of the info window you can select any other topic – including "Reports and documents" and "CSV templates". In Data maintenance, the topic follows the open tab.
5. The important windows also have "Info" at the top right: Set up network adapter, Network chain, Direct connection, Splunk database, Camera credentials, Setup wizard, Reports & templates, CSV templates and the schedule dialogs.
6. Initial commissioning: the info point (i) in front of each check question explains "What is it? What for? Why?" with an example; "Read in manual" leads to the question in the manual.

What do I enter where?

Field	Meaning
Topic selection	List at the top of the info window: selects a topic other than that of the current page.



Help in the program: info and manual



Help in the program: info and manual

2.5 Security and data protection

What a scan does in the network, which data is created, where it is stored and which rules apply.

What for?

A scan is network traffic in a plant. This section explains what devices notice of the scan, which data is stored and which operating rules apply. Read it before the first scan and before passing results on to third parties.

Important

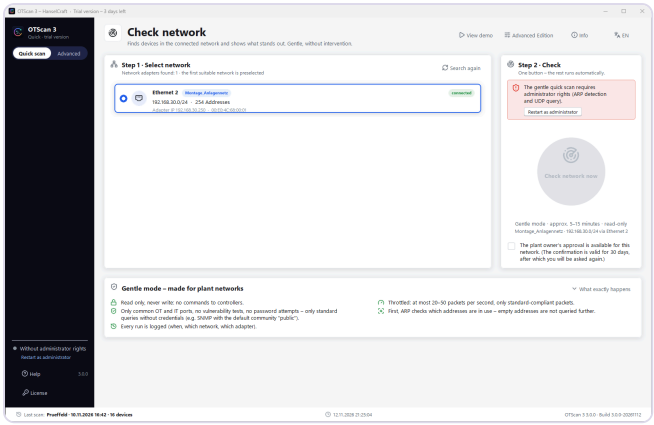
- What goes over the network: ARP requests (at most 20 packets per second), TCP connection setup to fixed port lists (at most 50 packets per second), a few standard UDP queries (SNMP GET with "public", BACnet, KNX), in stage 2a version probes to open ports; in CAM networks additionally WS-Discovery and ONVIF GetDeviceInformation (read-only).
- Not used: nmap scripts of the categories vuln, brute, exploit, dos; no operating system detection in the staged scan. Exception only on request: the option "model/firmware via Modbus device ID and S7" (read-only).
- The database is not encrypted. Protection is provided by the Windows user profile and drive encryption. All outputs contain network data and must be treated as confidential.
- Schedule and network chain run unattended – only with organisational approval. Inform network operations and the security team about Scan MACs and scan IPs.
- What OTScan 3 blocks when running with administrator rights and what the message "nmap blocked" means is explained in the topic "Security with administrator rights".

How it works

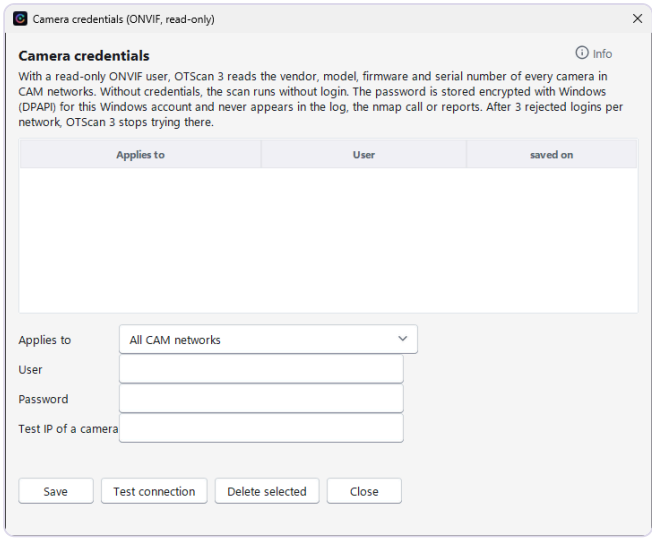
1. Obtain approval: before the first scan of a network, obtain the consent of the plant owner. The tick box in the program is a self-declaration, is valid for 30 days and does not replace a written approval.
2. Deep scans (stage 2a, initial commissioning "complete") preferably in the maintenance window. Older controllers sometimes react sluggishly to version detection.
3. One network, one scanner: never run two programs or computers on the same network at the same time. OTScan 3 warns about foreign nmap processes.
4. Use the right adapter: never scan via the office network. Pay attention to yellow notes such as "Adapter has a default gateway".
5. Only pass on reports to external parties (service providers, vendors) without IP addresses, MAC addresses and sites – the service provider PDF of the initial commissioning is made for this.
6. Camera passwords are only entered by the user in the program. They are encrypted with Windows DPAPI and never appear in logs, XML or reports.
7. Deleting data: the program does not delete anything automatically. To delete a network completely, exit the program, remove the files with the network name in the output folder, in Splunk\, Dokumente\OTScan3_Inventar and Dokumente\OTScan3_Splunk, delete the state files under %APPDATA%\OTScan3\stufenlauf and remove the network in Data maintenance.

What do I enter where?

Field	Meaning
Approval tick box	"The plant owner's approval is available for this network" – only tick it if the approval really exists. Valid for 30 days.



Security and data protection



Security and data protection

2.6 Security with administrator rights

What OTScan 3 allows and blocks with administrator rights – and what to do when the message "nmap blocked" appears.

What for?

With administrator rights (OTScan 3 (Admin), scheduled scans), a program may do almost anything on the computer. Other programs without administrator rights must not be able to exploit this by changing files that OTScan 3 later uses with administrator rights. That is why OTScan 3 with administrator rights only starts programs from protected folders and only accepts checked settings. In normal operation you will not notice any of this.

Important

- Restoring a backup only works without administrator rights. If a backup is queued and OTScan 3 starts with administrator rights, it restarts itself without administrator rights. If that fails, the backup is not restored – then start OTScan 3 via "OTScan 3 (ohne Admin)".
- OTScan 3 only creates Outlook drafts (e.g. emails to service providers) without administrator rights. If OTScan 3 runs with administrator rights, a notice appears; then create the drafts in "OTScan 3 (ohne Admin)".
- With administrator rights, OTScan 3 opens folders, reports and documents via Explorer without administrator rights. It does not open programs, scripts or shortcuts in this case.
- If the warning "OTScan 3 – Installation" appears, reinstall OTScan 3 with INSTALL.bat. Until then, scheduled scans from such a folder do not start nmap with administrator rights.
- Never create the folder %APPDATA%\nmap yourself and do not put your own scripts or files into the nmap program folder. New checks only come with a new OTScan 3 version.
- With administrator rights, OTScan 3 only starts known programs: Windows tools, nmap, its own Python and Edge/Chrome from "Program Files". It removes risky environment variables (e.g. NMAP_ARGS, OPENSSL_CONF) beforehand. If OTScan 3 reports "... is not started", have the scan profile or the computer checked by your IT contact.

How it works

1. Install: INSTALL.bat installs OTScan 3 in C:\Program Files\OTScan3. Only administrators can change this folder. INSTALL.bat moves an older installation from the user folder there: scheduled scans are switched to the new folder and the old program files are removed. Database and settings remain in %APPDATA%\OTScan3. Close OTScan 3 first: while it is running, INSTALL.bat does not move the installation.
2. Read the INSTALL.bat summary: scheduled tasks that would still start a program from a user folder (e.g. from older versions) are deactivated and listed there. If needed, plan these scans again in OTScan 3 under "Schedule".
3. For tasks that only work without administrator rights (restoring a backup, Outlook drafts), start OTScan 3 via the Start menu entry "OTScan 3 (ohne Admin)" (without administrator rights).
4. Message "OTScan 3 – nmap blocked": the scan was not started. The message states the reason – depending on the reason, proceed as described in the following steps.
5. Reason "the folder ... nmap exists": the message names the folder (usually %APPDATA%\nmap). Open exactly this folder in Explorer, check the contents and remove the folder. OTScan 3 does not need it. Then start the scan again. If it is unclear where the folder comes from, inform your IT contact first.
6. Reason "Option ...", "Script ...", "Script argument ..." or "Target ...": the scan profile contains something that is not permitted with administrator rights. Open the profile under "Scan profiles" and remove the item named; for a scheduled scan, check the profile used by the schedule. Only nmap options from a fixed list of permitted options and scripts installed in the nmap program folder are permitted (name or category, no file path).
7. Reason "no nmap installation ..." or "data folder ... incomplete": reinstall nmap (nmap setup from https://nmap.org/download.html) and run INSTALL.bat again.

What do I enter where?

Field	Meaning
Program folder	C:\Program Files\OTScan3 – only administrators can change it. Data and settings remain in %APPDATA%\OTScan3.
OTScan 3 (ohne Admin)	Start menu entry (or OTScan3_ohne_Admin.bat) for tasks that only work without administrator rights.
Message "nmap blocked"	nmap or another program was not started for security reasons; a scan then does not run. The message states the reason (see steps).
Warning "OTScan 3 – Installation"	Appears when starting with administrator rights if OTScan 3 runs from a folder that normal users can also change.

3 New in OTScan 3

What OTScan 3.0 can do that OTScan 2.3 could not – at a glance.

What for?

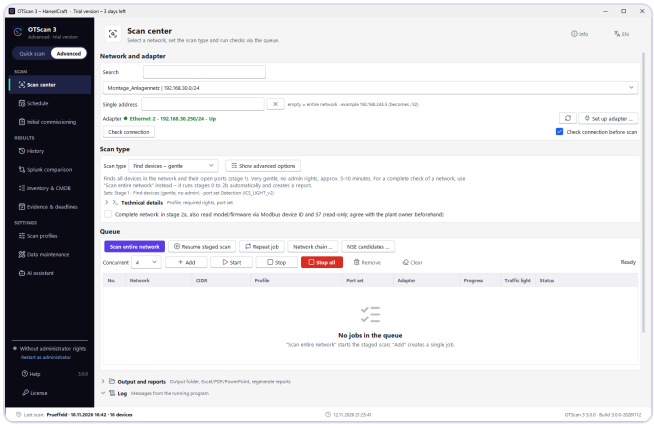
OTScan 3 is the successor of OTScan 2.3. The network scanner has become a tool for the whole workflow: check networks completely and gently in stages, compare results with firewall traffic (e.g. from Splunk) and your inventory (CMDB), match vendor advisories, accept devices at installation and create reports for every audience. The user interface is available in 7 languages; the program runs on Windows and Linux.

> **Important**
>
> - Data from OTScan 2.3 is not taken over automatically: OTScan 3 has its own data folder (OTScan3). Networks can be imported via the CSV templates or the setup wizard.
> - License keys from OTScan 2.x also work for OTScan 3 (same computer limit). After the trial period, activate OTScan 3 with your existing key or a new one (otscan.hanselcraft.de).
> - The traffic rules are a default, not a standard. Adapt them to your company's requirements before you pass reports on.

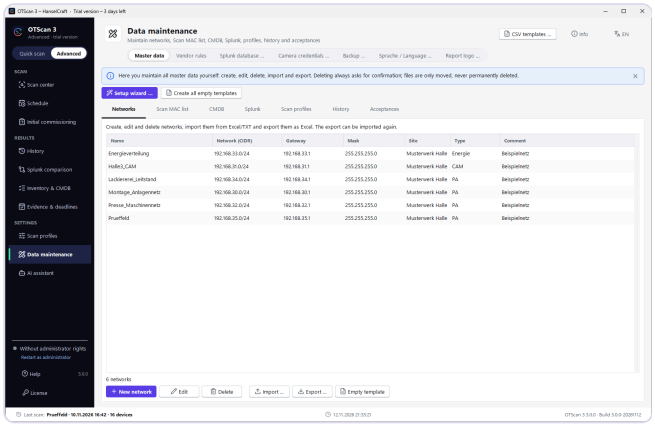
How it works

1. Two views in one program: "Quick scan" (one button, for all users) and "Advanced" (Scan center, Schedule, Initial commissioning, History, Splunk comparison, Inventory & CMDB, Scan profiles, Data maintenance).
2. Staged run "Scan entire network": stages 0 to 2b, follow-up scan and camera query run one after another, each stage uses the result of the previous one; without administrator rights the run starts with neighbour discovery. You can pause and resume at any time.
3. Network chain: scan many networks one after another through one adapter – with a scan MAC per network or via a trunk port with VLAN number.
4. Splunk comparison: import firewall exports (e.g. a Splunk search over FortiGate logs) and compare them with the scan – devices only seen in traffic, port gaps, follow-up scan suggestions; zones, services and policies appear in the reports.
5. Inventory & CMDB: comparison with your Excel device list, CMDB delta (new, changed, missing), CMDB addendum for devices that only appear in traffic, and an overall inventory across all sources. The CMDB is only read.
6. Vendor advisories: bundled offline data from public CSAF sources (vendor PSIRTs, CERT@VDE, CISA) instead of the 11 individual advisories of OTScan 2.3; updated only when you press "Update online".
7. Initial commissioning and acceptances: checklist with an explanation for every question, scan before/after at the device, direct connection, report and package for the service provider; adopt a target state and compare later scans against it.
8. New reports: Network check, Device detail view with firewall communication, Site report and Device directory (PDF), Action list (Excel), PowerPoint for meetings – with samples under "Reports & templates".

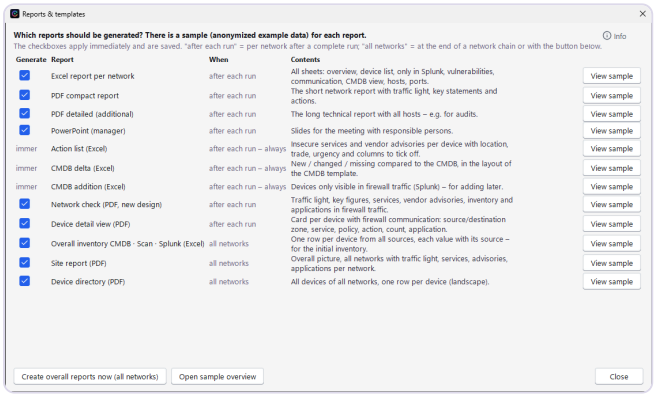
9. Assessment by traffic rules: a HanselCraft default based on IEC 62443 (zones and conduits) that you adapt to your own rules.
10. Camera profile and camera credentials (ONVIF, read-only), vendor rules, schedule, CSV templates for all master data, data backup including moving between Windows and Linux.
11. Help where you work: "Info" at the top right of every page (F1), setup wizard at first start, user manual in the program folder. User interface and reports in German, English, Spanish, French, Polish, Japanese and Chinese.



New in OTScan 3



New in OTScan 3



New in OTScan 3

4 Scan

4.1 Quick scan – check network

Check a network gently with one button – without deep scan, with report.

What for?

The quick scan is intended for all users, even without networking knowledge. It finds the devices of a directly connected network (up to /22), checks 23 common TCP ports and queries device names via SNMP, BACnet and KNX. It is suitable for ongoing operation (with approval) and for regular visual checks; the complete staged scan is handled by the Advanced Edition.

Important

- The quick scan needs administrator rights (ARP and UDP). Without them it does not start – restart OTScan 3 and confirm the prompt with "Yes".
- Screen findings (also Modbus, S7, BACnet) and the traffic light based on the traffic rules in the PDF are two different yardsticks: the screen may show "Modbus/TCP without login – Important" while the PDF is still GREEN. For actions, the report applies.
- Typical durations: /25 about 3 to 7 minutes, /24 about 5 to 15 minutes, /23 about 10 to 30 minutes. If there is no ARP response, step 3 checks all addresses – this takes considerably longer.
- If the netmask of the adapter does not match the stored network, OTScan 3 blocks the start with a red note. You set the mask in the Scan center via "Set up adapter ...".

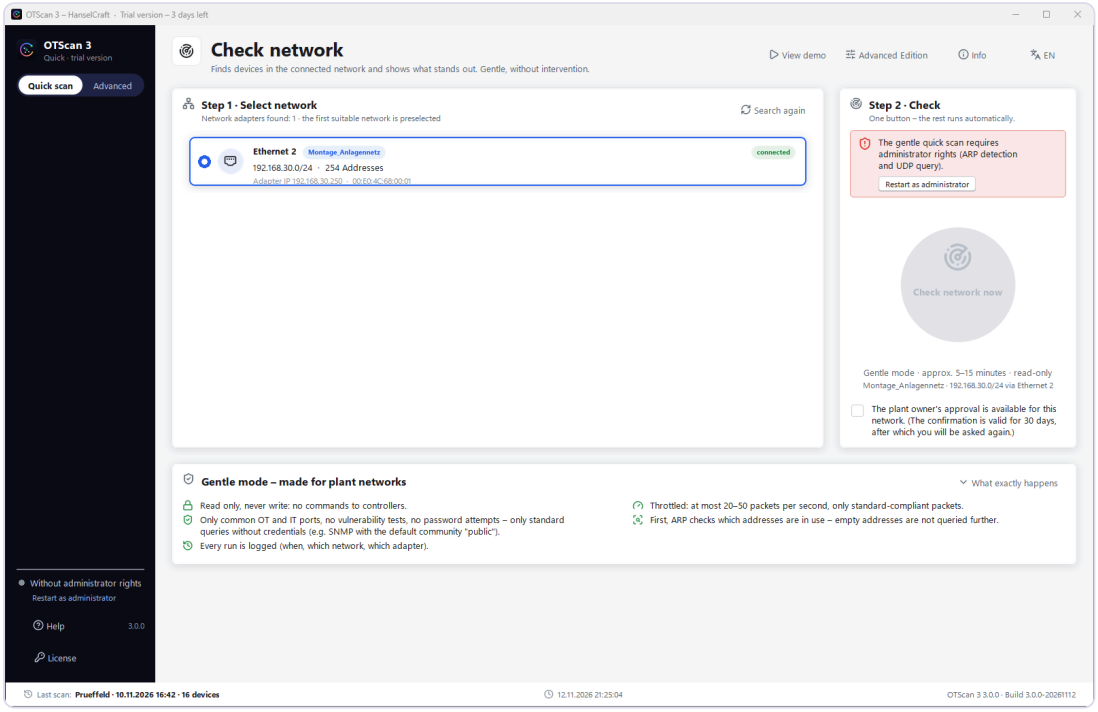
How it works

1. Select "Quick scan" at the top left. The "Check network" page lists all network adapters with a traffic light under "Step 1 · Select network": green "connected", yellow office network note, red "not connected", "unsuitable" for networks with more than 1022 addresses.
2. Click the adapter of the plant network. If the network is stored in OTScan 3, its name is shown next to it; OTScan 3 creates unknown networks automatically at the start.
3. On the right under "Step 2 · Check", tick "The plant owner's approval is available for this network" (valid for 30 days).
4. Press "Check network now". The pre-check reports foreign nmap scans, running jobs, Windows Update or restart and disconnected adapters – with "Start anyway" or "Cancel".
5. During the check, the step card shows five steps (detect network, find devices, check services, device type and vendor, create report) with remaining time; an interim status of the devices appears on the left.
6. "Pause check" pauses. Completed steps are kept, the current one is repeated when resuming. Resume: Advanced → Scan center → "Resume staged scan".
7. Result: key figures (devices, OT devices, notes, of which important), device cards or table with filter, findings with recommendation. Buttons "Open report (PDF)", "Excel", "Compact report (HTML)", "Open in Advanced", "New check".

8. "View demo" shows the procedure with fictitious data without network traffic. "Info" at the top right explains the page step by step.

What do I enter where?

Field	Meaning
Step 1 · Select network	Click the adapter of the plant network. Only adapters marked green are suitable right away.
Approval tick box	Confirms that the approval of the plant owner is available. Valid for 30 days per network.
Filter (result)	Restricts the device list, for example to devices with notes.



Quick scan – check network

4.2 Scan center and staged scan

"Scan entire network": the complete staged scan S0 → S1 → S2a → S2b → NACH → CAM → END with one report per network.

What for?

The staged scan is the recommended way to check a network completely. Each stage uses the result of the previous one; this way, in-depth checks are only performed where there really is a device. The Scan center is also the place for individual jobs, the queue, resuming paused runs, the network chain, the report settings and the log.

Important

- Without administrator rights, the run starts with "Stage 0 neighbour detection (without admin)" and S1. It stops before S2a ("Stage 2a TCP requires administrator rights ..." – stage 2a TCP needs administrator rights). Then restart OTScan 3 as administrator and click "Resume staged scan".
- Typical durations: /25 with about 30 devices a good hour, /23 with about 150 devices 6 to 7 hours. "Check devices in detail – TCP" on an entire network takes hours – that is what the staged scan is for.
- A restart during the run aborts it; the state remains in %APPDATA%\OTScan3\stufenlauf and can be reached via "Resume staged scan". Disable Windows Update and power saving beforehand.
- Several networks in parallel only with a separate adapter each. The option "additionally read model/firmware via Modbus device ID and S7 in stage 2a" is off by default – agree with the plant owner beforehand.
- Neighbour detection only works if the network is directly connected to the adapter. If it is behind a router, a VPN or a route, S1 checks all addresses individually as before.
- Large networks without administrator rights: from /20 (4094 usable addresses), OTScan 3 asks before starting ("Large network") and shows the estimated duration. From /18, it recommends splitting the network into smaller subnetworks (e.g. /22) or starting OTScan 3 as administrator.
- If neighbour detection gives no usable result in a very large network (from /21, i.e. more than 1024 usable addresses), the staged scan stops ("Staged run paused") instead of checking every address individually for days. Recommendation: start OTScan 3 as administrator and "Resume staged scan", or split the network. Choosing "Resume staged scan" without administrator rights deliberately starts S1 on all addresses.
- If very many addresses report the same MAC address (proxy ARP), a warning appears in the log; S1 then checks all reported addresses. Without administrator rights, S1 works through large hit lists in packages; after "Stop", "Resume staged scan" repeats the interrupted package.

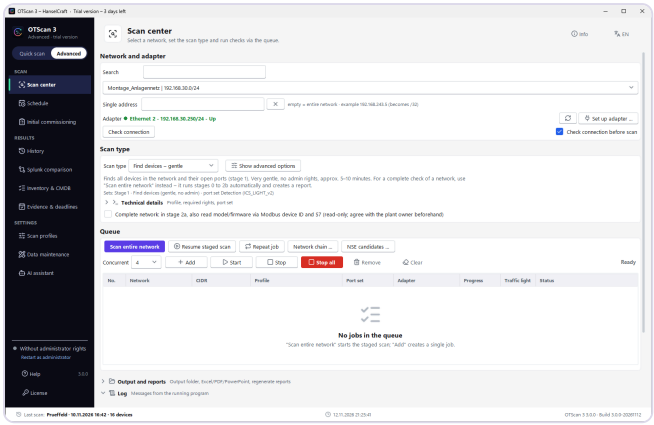
How it works

1. Advanced → SCAN → "Scan center". Under "Network and adapter" select the network (the search field helps). The adapter traffic light must be green; "Set up adapter ..." sets IP, mask and Scan MAC.
2. Optionally enter "Single address", for example 192.168.6.21 – then the job applies only to this device (/32). Empty = entire network.
3. Press "Scan entire network" and confirm the prompt (network, stages, estimated duration, adapter) with "Yes". The pre-check then runs. In a CAM network without credentials, OTScan 3 asks: "Scan without login", "For this run only", "Save and scan" or "Cancel".
4. The stages run by themselves: S0 ARP discovery ("Who is there?"), S0b query known devices again, S1 find devices and open ports (23 TCP ports), S2a TCP deep scan with version detection (largest time item), S2b UDP names (SNMP, BACnet, KNX), NACH rescan of devices with timeout, CAM camera query (CAM networks only), END merging and reports.
5. Without administrator rights, the first stage is called "Stage 0 neighbour detection (without admin)". OTScan 3 briefly tries to reach each address via TCP and then counts which devices appear in the computer's ARP table. This also finds controllers (PLCs) that respond slowly or not at all to TCP. S1 then checks only the addresses found and the uncertain ones. The remaining-time display then ends with "then pause: stage 2 requires administrator rights".

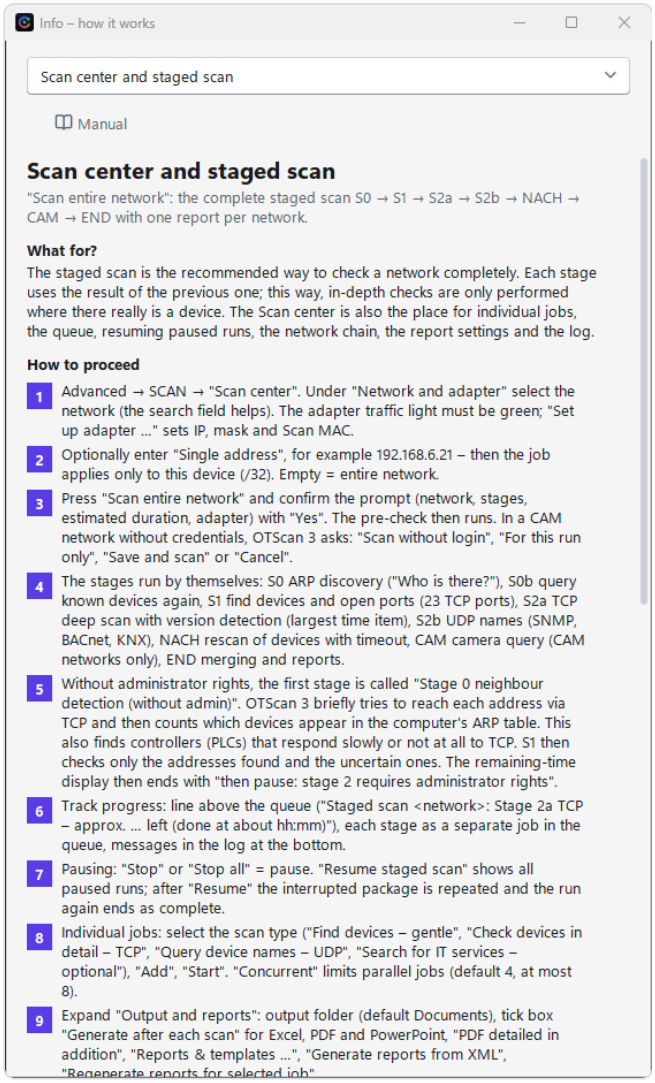
6. Track progress: line above the queue ("Staged scan <network>: Stage 2a TCP – approx. ... left (done at about hh:mm)"), each stage as a separate job in the queue, messages in the log at the bottom.
7. Pausing: "Stop" or "Stop all" = pause. "Resume staged scan" shows all paused runs; after "Resume" the interrupted package is repeated and the run again ends as complete.
8. Individual jobs: select the scan type ("Find devices – gentle", "Check devices in detail – TCP", "Query device names – UDP", "Search for IT services – optional"), "Add", "Start". "Concurrent" limits parallel jobs (default 4, at most 8).
9. Expand "Output and reports": output folder (default Documents), tick box "Generate after each scan" for Excel, PDF and PowerPoint, "PDF detailed in addition", "Reports & templates ...", "Generate reports from XML", "Regenerate reports for selected job".
10. After the run: it appears in the history as "Complete network (staged scan)". The reports are in the output folder (see "Reports and documents").

What do I enter where?

Field	Meaning
Search / network	Select the network from the list; the search field filters by name.
Single address	Empty = entire network. One address, for example 192.168.6.21, restricts the job to one device.
Adapter	Shows the adapter for the network with a traffic light. Change via "Set up adapter ...".
Scan type	Only for individual jobs: find devices, check devices in detail (TCP), query device names (UDP), search for IT services.
Concurrent	How many jobs may run in parallel (default 4, at most 8).
Modbus/S7 tick box	In stage 2a, additionally reads model and firmware via Modbus device ID and S7 (off by default).
Output folder	Where reports are written. Default: Documents.
Generate after each scan	Tick boxes for Excel, PDF and PowerPoint; "PDF detailed in addition" for audits.



Scan center and staged scan



Scan center and staged scan

4.3 Network chain – many networks one after the other

One adapter on a network socket scans all selected networks one after the other – with Scan MAC, cross-check, pause and start window. Via a trunk port, the chain sets the VLAN number for each network instead of the Scan MAC.

What for?

At many sites, network access control (for example MAC-based port approval) only enables a plant network for a registered MAC address. For each network, the network chain sets the registered Scan MAC and a free scan IP on one adapter, cross-checks the network, scans, pauses and moves on to the next network. This way night or weekend runs cover many networks without re-plugging. At sites without this access control, the switch port can instead be set up as a trunk: the chain then sets the VLAN number on the adapter for each network.

Important

- Only networks with a registered Scan MAC (Scan MAC list, column "MAC origin" or "MAC registration" = registered), scan IP and valid approval (30 days, no automatic extension) are ready to start. With a trunk port, each network instead needs a valid VLAN number (1–4094) in the network master data; an invalid number is shown in the list as "Trunk: not ready – VLAN invalid".
- If the cross-check fails (MAC, IP or gateway does not match), the network is not scanned. After 3 consecutive errors, the chain stops.
- OTScan 3 (as administrator) must remain open; disable power saving and Windows restarts. After a restart, the chain is set to "interrupted" and only continues after "Resume".
- Do not change the Scan MAC list while a chain is running. One separate chain per adapter; a network must not be in two chains. The chain never asks for camera credentials.
- Only use a trunk port if the network team has set up the switch port as a trunk with exactly the approved VLANs. If the adapter does not support VLAN, OTScan 3 stops before anything on the adapter is changed. In trunk mode the chain sets no Scan MAC; mixed chains (Scan MAC and VLAN) are not possible.
- "Finish + reset adapter" also restores the VLAN setting. If the chain reports "Reset not confirmed - check the adapter manually ('Set up adapter' -> Reset)" at the end, check the adapter manually via "Set up adapter" → "Reset". The log then shows "VLAN on the adapter not reset".

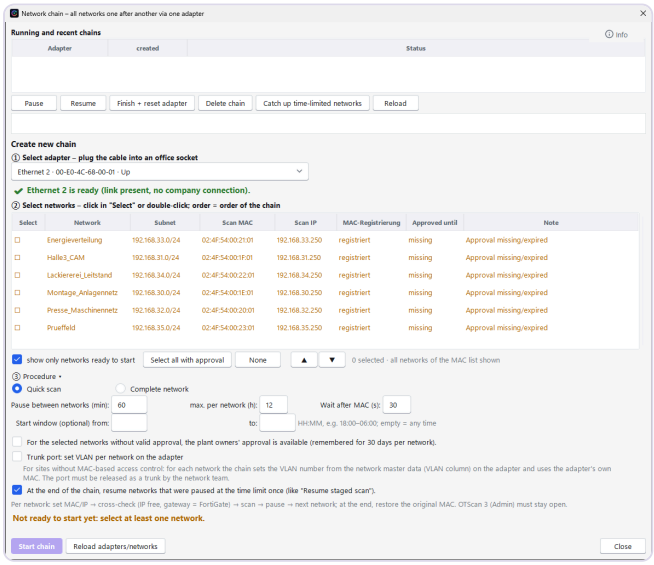
How it works

1. Advanced → SCAN → Scan center → Queue → "Network chain ...". At the top is "Running and recent chains" with adapter, created and status.
2. "Create new chain" – ① select the adapter (cable in a network socket). The matching adapter is usually preselected and green "ready"; red states the reason (wireless, company connection, no cable).
3. ② Select networks: click in the "Select" column or double-click. ☐ becomes ✔ 1, ✔ 2 ... (order of the chain). Columns: network, subnet, Scan MAC, scan IP, MAC registration, approval until, note. Aids: "show only networks ready to start", "Select all with approval", "None", arrows for reordering.
4. Trunk port (for sites without MAC-based access control): tick "Trunk port: set VLAN per network on the adapter". For each network, the chain then sets the VLAN number from the network master data (VLAN column) on the adapter and uses the adapter's own MAC – no Scan MAC. The list then also shows networks with a VLAN number from the master data; the Scan MAC column stays empty. Requirement: the adapter driver supports VLAN (property "VLAN ID"). OTScan 3 saves the setting beforehand and restores it at the end.
5. ③ Configure the sequence: "Quick scan" or "Complete network", pause between networks (default 60 minutes), maximum per network (hours), wait after MAC (seconds), optionally a start window, for example 18:00–06:00. With the "Trunk port" checkbox, the field is called "Wait after adapter restart (s)". On small screens (e.g. 1366×768), ③ is collapsed and shows a summary; clicking "③ Procedure" expands the fields.
6. Only tick the approval box for networks without a valid approval if the approvals really exist. The line above the buttons must show "Ready to start ..." in green – then "Start chain".
7. For each network: set Scan MAC and scan IP → wait for the network assignment → cross-check (IP free, gateway is a FortiGate) → run → pause → next network. With a trunk port: set the VLAN number instead of the Scan MAC and wait until the switch port passes traffic again.

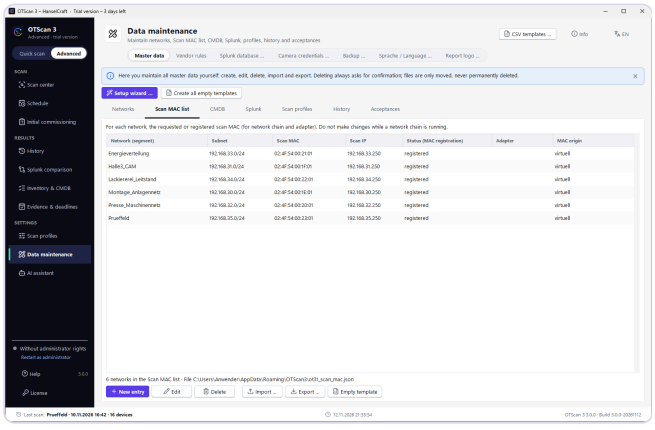
8. At the end OTScan 3 restores the original MAC and writes Netzkette_<Adapter>_<Zeit>.csv to the output folder.
9. Buttons at the top: "Pause" (after the current network), "Resume" (also after a program restart), "Finish + reset adapter", "Delete chain", "Reload".
10. "Delete chain": select one or more finished or aborted chains and confirm the prompt. The chain file is moved to %APPDATA%\OTScan3\netzkette_geloescht (recoverable); scans, reports and overview CSV are kept.

What do I enter where?

Field	Meaning
① Adapter	Adapter for the whole chain. Green "ready" = suitable; red states the reason.
② Select	Click or double-click selects a network; the number indicates the order.
Scan type	"Quick scan" (faster) or "Complete network" (staged scan) for all networks of the chain.
Pause between networks	Waiting time after each network in minutes (default 60).
max. per network (h)	Time limit per network in hours; after that the chain continues.
Wait after MAC (s)	Waiting time after setting the Scan MAC until the network assignment takes effect.
Start window	Optional, for example 18:00–06:00: networks only start within this period.
Approval tick box	Confirms the approval for the selected networks without a valid approval; remembered for 30 days per network.
Trunk port	Sets the VLAN number from the network master data on the adapter for each network (adapter's own MAC). Without the tick: access port, Scan MAC per network.
Wait after adapter restart (s)	Only with trunk port: waiting time after setting the VLAN number until the switch port passes traffic again.



Network chain – many networks one after the other



Network chain – many networks one after the other

4.4 Schedule – recurring scans

Run individual jobs daily, weekly or monthly via the Windows Task Scheduler.

What for?

The schedule creates a scheduled scan that runs automatically at the set time – even when the program is not open. For this, OTScan 3 enters it in the Windows Task Scheduler. Suitable for recurring visual checks with a fixed profile. For the complete check of several networks, the network chain is the better way.

Important

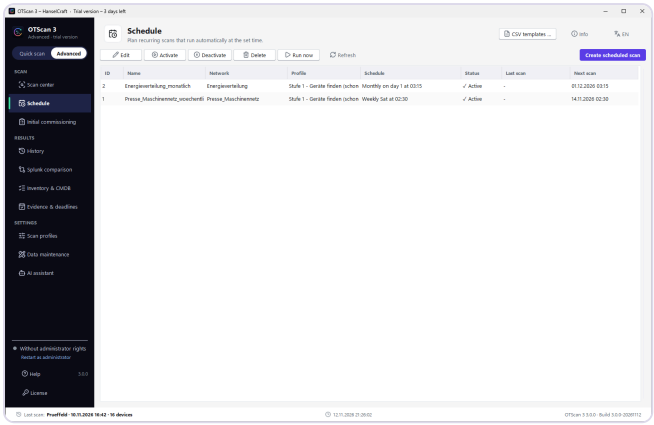
- A scheduled scan is a single job with the selected profile – no staged scan, no pre-check, no approval prompt. It produces Excel and PDF.
- The same approval requirement applies as for a manual scan: only schedule with the consent of the plant owner.
- The task runs unattended with highest privileges from the program folder. After removing a program version, delete orphaned tasks in the Task Scheduler.
- The scan runs via the adapter connected to the target network – a scheduled scan does not set a Scan MAC.

How it works

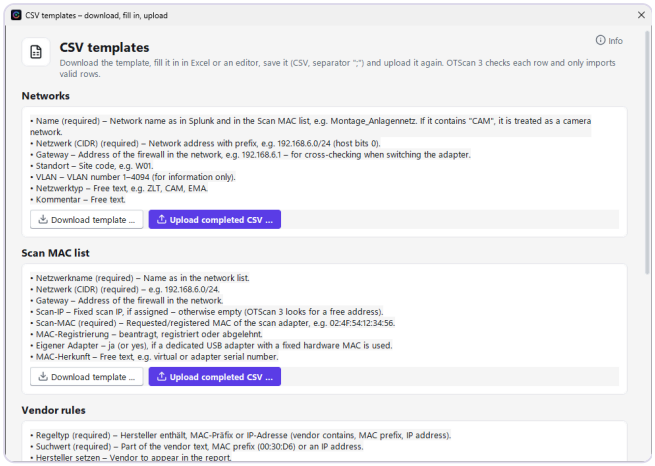
1. Advanced → SCAN → "Schedule".
2. "Create scheduled scan": select name, network, profile and port set, enter interval (daily, weekly, monthly), time (HH:MM) and for weekly the weekday or for monthly the day (1–28). "Info" at the top right of the dialog explains every field.
3. Save – OTScan 3 creates a task in the Windows Task Scheduler with elevated privileges.
4. The table shows ID, name, network, profile, schedule, status, last and next scan. "Next run" is now also correct for weekly schedules.
5. Further buttons: "Edit", "Activate", "Deactivate", "Delete", "Run now", "Refresh".
6. Many schedules at once: "CSV templates ..." at the top right → Schedule → "Download template ...", fill in, "Upload completed CSV ...".
7. Log of the scheduled runs: %APPDATA%\OTScan3\scheduler.log.

What do I enter where?

Field	Meaning
Name	Freely selectable name of the schedule (letters, digits, _ . -).
Network	A network created in OTScan 3, for example Montage_Anlagennetz.
Profile	Scan profile of the job, for example "Stage 1 · Find devices (gentle, no admin)".
Port set	List of checked ports; empty = default port set of the profile.
Interval	daily, weekly or monthly.
Time	Start time in the format HH:MM, for example 02:30.
Day	For weekly the weekday (Mon to Sun), for monthly the day 1 to 28.



Schedule – recurring scans



Schedule – recurring scans

4.5 Initial commissioning and initial acceptance

Check and document a new device during installation: Part A at the device, Part B in the target network, report and package.

What for?

When a service provider installs a new OT device (controller, camera, gateway) during initial commissioning, OTScan 3 checks it gently and read-only, compares type plate and scan, goes through the checklists with the service provider and creates an acceptance package with report, open items and checksums. Part A takes place directly at the device while the service provider is on site; Part B is the initial acceptance in the target network after installation.

Important

- Only scan with the consent of the plant owner. For safety controllers and sensitive devices, select the "gentle" mode.
- Part A/B scans are partial runs: no PDF scan report, no PowerPoint, no CMDB comparison, no entry as a full run in the history.
- Signature only by the service provider; no signature is required on the operator side. The ZIP stays local as long as no shared storage location is approved.
- Only the service provider version goes to external parties (without IP, MAC, site and network name; IPs and MACs masked in free texts) together with the open items. Check recipients and attachments before sending.

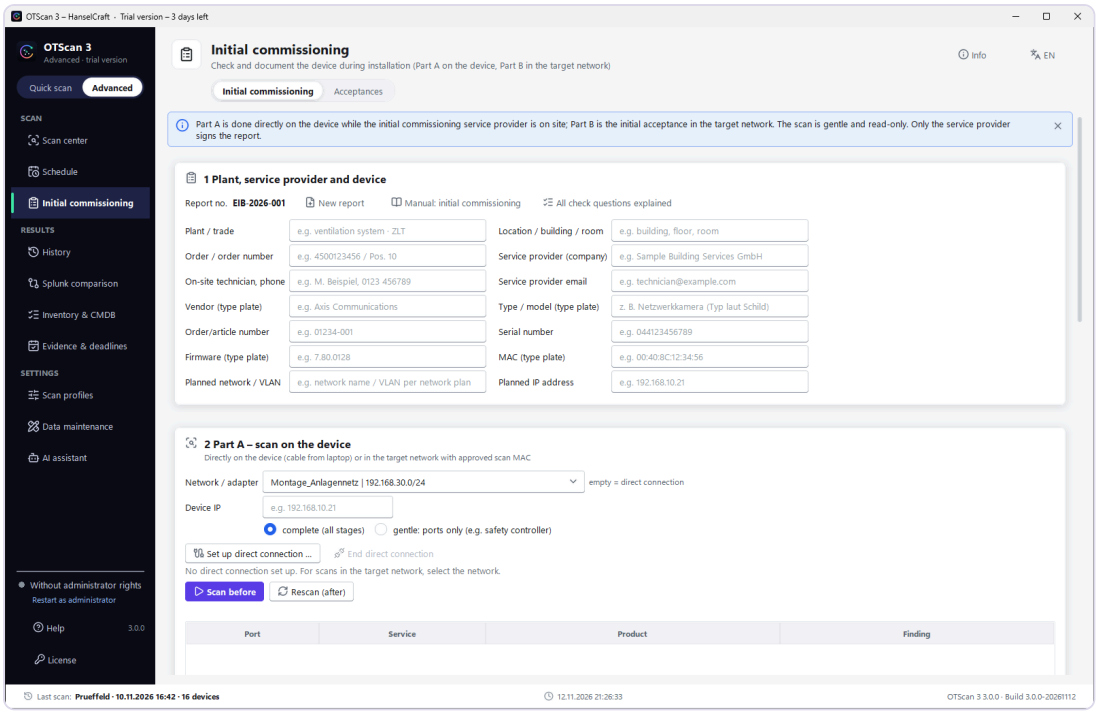
How it works

1. Advanced → SCAN → "Initial commissioning", tab "Initial commissioning" at the top. The report no. (EIB-JJJJ-NNN) is assigned automatically; "New report" starts a new one (with confirmation).
2. 1 Plant, service provider and device: enter the master data (see "What do I enter where?"). Grey example texts show what belongs in a field; they disappear when you click into the field and are never saved.
3. Directly at the device: enter the device IP and click "Set up direct connection ..." – OTScan 3 sets the laptop adapter to a free address in the device's network and later restores it (section "Direct connection").

4. 2 Part A – scan on the device: select "Network / adapter" (empty = direct connection), mode "complete (all stages)" or "gentle: ports only (e.g. safety controller)", then "Scan before". After the service provider's corrections, "Rescan (after)".
5. Read the status text and table: open services, findings, vendor, model, firmware, MAC and the comparison type plate ↔ scan (✓ or "≠ scan: ..."). For cameras, the ONVIF query follows automatically. Findings of the first scan are taken over as a suggestion into "Open items".
6. 3 Checklist with the service provider: for each question select yes, no or n/a and enter a remark; add the vendor documents (CRA conformity, IEC 62443, SBOM, end of support, hardening guide). The info point (i) explains each question.
7. 4 Part B – initial acceptance in the target network: select "Target network", then "Scan in the target network". The status text compares with Part A ("Additionally open in the target network: ..."). Answer checklist B.
8. 5 Open items: one line each "finding ; action ; deadline" – the service provider is responsible.
9. 6 Completion: "Create report and package" (folder and ZIP under Dokumente\OTScan3_Abnahmen\<Jahr>\EIB-JJJJ-NNN_<Typ>), "Email drafts (Outlook)" opens Outlook drafts – they are never sent automatically, "Apply target state" (appears in the "Acceptances" tab), "Open storage".
10. Forms (Word) "Herstellerauskunft" (vendor information) and "Erstinbetriebnahme/Erstabnahme" (initial commissioning/initial acceptance) are located in Dokumente\OTScan3_Vorlagen.

What do I enter where?

Field	Meaning
Plant / trade, site, order	Where the device is installed and which order it belongs to.
Service provider (company), technician, service provider email	Who installs the device; the email is used for the external email draft.
Vendor, type, article number, serial number, firmware, MAC	Data from the type plate; OTScan 3 compares MAC, firmware and vendor with the scan.
Planned network / VLAN, planned IP	Where the device is to be connected after installation, for example Halle3_CAM and 192.168.6.21.
Network / adapter	Network for Part A. Empty = direct connection by cable from the laptop.
Device IP	Address of the device, for example 192.168.6.21 (type plate, documentation or service provider).
Mode	"complete (all stages)" or "gentle: ports only" for sensitive devices.
Checklist	For each question yes / no / n/a and a remark, for example "Telnet and FTP off".
Target network	Network for Part B, to which the device is connected after installation.
Open items	One line per item: finding ; action ; deadline.



Initial commissioning and initial acceptance

Reports: Initial commissioning: report and package

File: `Documents/OTScan3_Abnahmen/<year>/<report no.>/ (ZIP, internal and external PDF, open items)`

How do I create it?

1. Page "Initial commissioning" → "Create report and package".

How do I read it?

- Internal report with all details; external PDF for the service provider without addresses; list of open items with due date.

Where does the data come from?

- Entries on the page, scan before/after at the device, checklist.

What does it not tell you?

- Only the external PDF is meant for third parties.

4.6 Direct connection to a machine

Laptop connected by cable directly to the device: OTScan 3 sets up the network adapter and restores it afterwards.

What for?

During initial registration, the device is often not yet connected to the target network. In that case the laptop is connected directly to the device. For the scan to work, the laptop needs an address in the device's network. OTScan 3 configures a free adapter for this – without a gateway, the old setting is backed up – and restores it afterwards. Company LAN, WLAN, VPN and the adapter of a running network chain are never touched.

Important

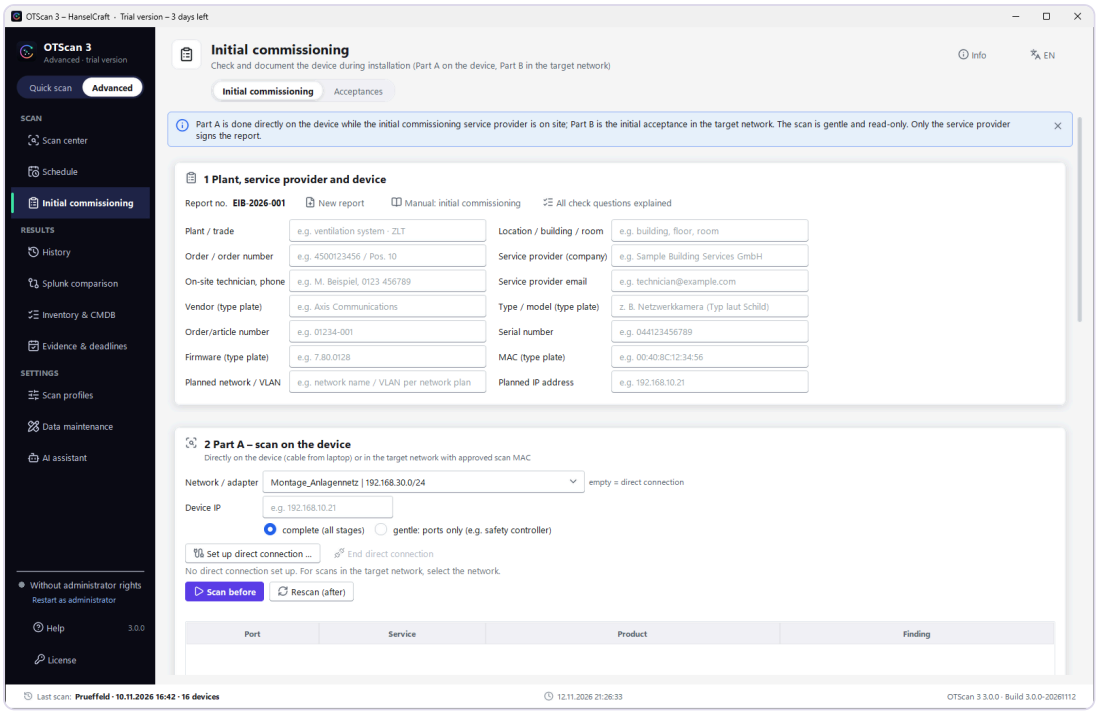
- OTScan 3 must run with administrator rights to switch the adapter.
- Only adapters without an address or with 169.254.x.x, without a gateway, without a network chain and without assignment to an OT network can be selected; never WLAN, VPN or virtual adapters.
- If the device network overlaps with the network of another adapter, OTScan 3 does not set anything up – otherwise company or chain traffic would run over the direct cable.
- A registered Scan MAC is not required – there is no company network between the laptop and the device.

How it works

1. Connect the laptop directly to the device with a network cable (preferably via a separate USB network adapter).
2. SCAN → Initial commissioning, Part A: leave "Network / adapter" empty and enter the "Device IP" (type plate, documentation or service provider).
3. "Set up direct connection ...": select the adapter (only suitable ones can be selected), check the prefix (usually /24), "Set up". "Info" at the top right of the window explains every point.
4. OTScan 3 searches for a free address via ARP, configures the adapter in the background with PowerShell and reports whether the device responds and whether its MAC matches the type plate.
5. "Scan before" – corrections by the service provider – "Rescan (after)". With the tick box, OTScan 3 automatically restores the adapter after the rescan.
6. Otherwise "End direct connection". "New report" and closing OTScan 3 also restore the adapter; after a crash, a note with a button appears the next time the program is opened.
7. For each part the report states "Anschluss: Direktanschluss über <Adapter> mit <Adresse>" (connection: direct connection via <adapter> with <address>) – in the version for the service provider without addresses.

What do I enter where?

Field	Meaning
Device IP	Address of the device, for example 192.168.6.21.
Adapter	Free network adapter of the laptop; only suitable ones can be selected.
Prefix	Netmask of the device network, usually 24.
Tick box "Restore after the rescan"	Automatically restores the adapter after "Rescan (after)".



Direct connection to a machine

4.7 Acceptances

List of all saved initial commissionings and target states with access to the package – "Acceptances" tab of Initial commissioning.

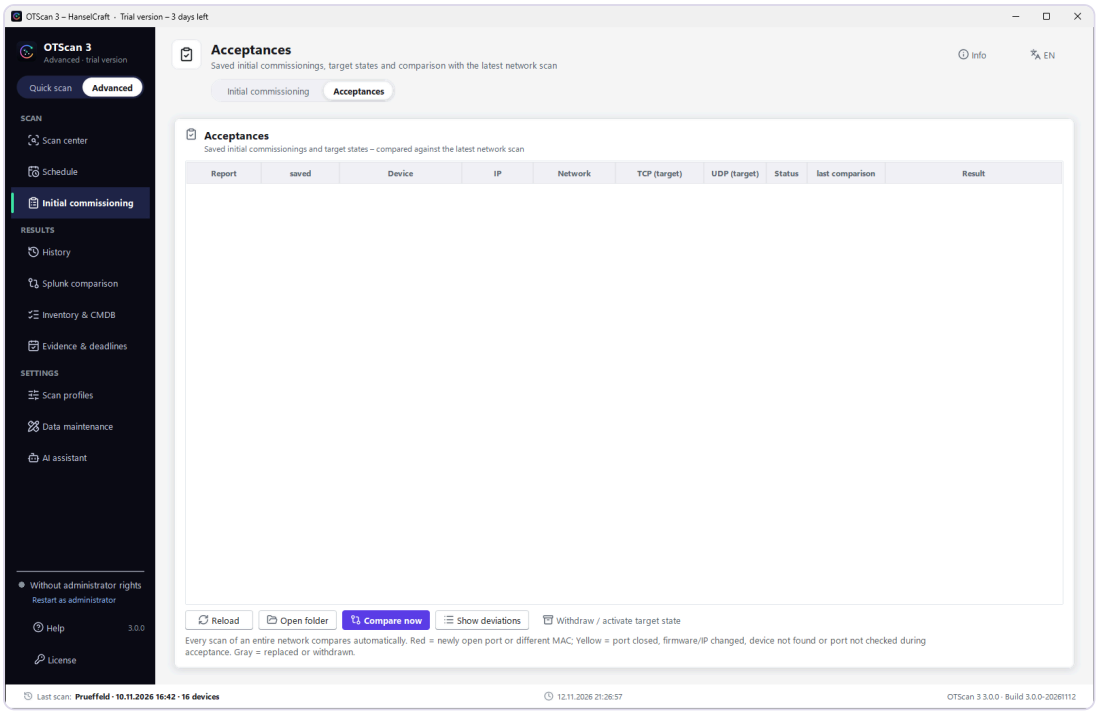
What for?

The "Acceptances" tab shows every initial commissioning report whose target state has been applied: number, date, device, IP, network, the accepted TCP and UDP ports (target) and the status (Part A or Part B). From here you open the package folder. The target state is the reference for later comparisons.

> **Important**
>
> - An entry is only created via "Apply target state" – not automatically with the package.
> - "Für diesen Eintrag wurde noch kein Paket gespeichert" (no package has been saved for this entry yet) appears if the target state was applied before "Create report and package".
> - Target states are not removed automatically when a network is deleted.

How it works

1. Advanced → SCAN → "Initial commissioning" and select the "Acceptances" tab at the top.
2. Reading the columns: report, saved, device, IP, network, TCP (target), UDP (target), status.
3. Select an entry → "Open folder" shows the package folder under Dokumente\OTScan3_Abnahmen\<Jahr>. Without a selection, the base folder opens.
4. "Reload" refreshes the list, for example after "Apply target state" was pressed in the "Initial commissioning" tab.
5. Removing entries: SETTINGS → Data maintenance → Master data tab → "Acceptances", select the entry, "Delete" and confirm the prompt. The package is moved to the _geloescht folder.



Acceptances

5 Results

5.1 History

All previous runs with status, duration, devices and traffic light – repeat, compare, rescan.

What for?

The history is the program's memory: every run is listed with ID, time, network, CIDR, profile, port set, adapter, status, planned and actual duration, number of devices and risk. Here you identify incomplete runs, compare two runs and create repeats.

Important

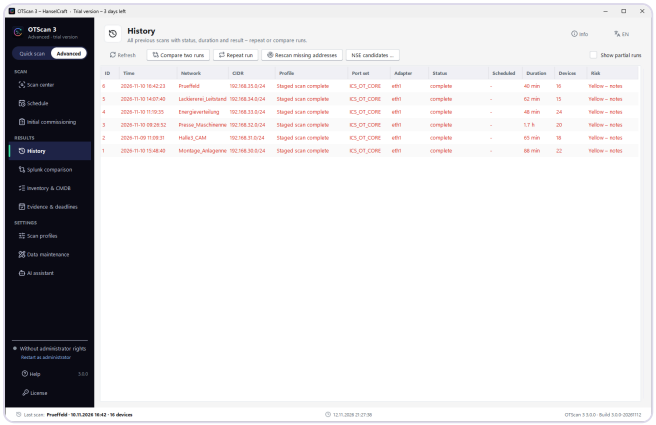
- Risk shows "Green – normal" or "Yellow – notes". Very old runs may still show "Red – critical" from an earlier assessment; today's traffic light has no red.
- The history comparison window uses an older choice of previous run (including partial runs). The "Change since the last scan" in the report is authoritative.
- Database and history are located in %APPDATA%\OTScan3\otscan3.db and are shared by all program versions of this user.

How it works

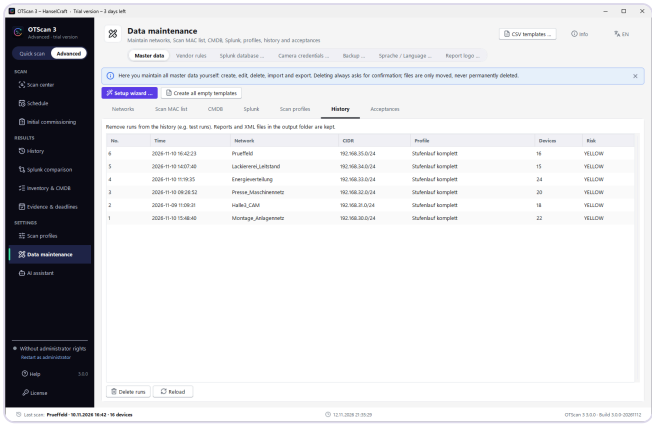
1. Advanced → RESULTS → "History". "Refresh" reloads the list.
2. Reading the columns: profile "Complete network (staged scan)" = staged scan, "Quick scan" = quick scan. Status: complete (possibly "(1 host timeout)"), aborted, stopped, start error. Incomplete runs are shown in red.
3. "Compare two runs": select exactly two runs – shows new, disappeared and changed devices.
4. "Repeat run": creates a new job with network, CIDR, targets, adapter, profile and port set of the selected run.
5. "Rescan missing addresses": for aborted individual jobs – scans the remainder after the last processed address. Instead, continue paused staged scans in the Scan center with "Resume staged scan".
6. The "Show partial runs" tick box shows the individual steps of a staged scan (S0, S0b, S1, S2a, S2b, NACH, initial commissioning); by default they are hidden.
7. Remove test runs: Data maintenance → Master data tab → "History". The report files are kept.

What do I enter where?

Field	Meaning
Show partial runs	Tick box: also shows the individual steps of a staged scan.
Selection	One row for "Repeat run" or "Rescan missing addresses", exactly two rows for "Compare two runs".



History



History

5.2 Splunk comparison, Splunk storage and Splunk database

Hold firewall traffic from Splunk against the scan: devices visible only in Splunk, port gaps and targeted rescans.

What for?

The OT firewall (for example FortiGate) logs to a log system (for example Splunk) which devices communicate via the firewall. The scan sees what responds. The comparison brings both together: devices the scan missed (K3, K4, K6), ports missing in the scan (K2a, K2b) and phantom targets (K3b). The comparison runs automatically with every network report as soon as Splunk data is in the storage. The Splunk storage is the data store for this, the Splunk database a window for specialists.

Important

- Scan first, then compare: the comparison uses up to three of the most recent complete full runs of the network. Without such a run, all Splunk devices end up in K3, K3b, K4 or K6.
- Splunk only sees traffic via the firewall, not within the network. "Open, but not used via the firewall" does not mean that a service is unused – clarify with the plant owner before disabling it.
- Splunk data older than 45 days is not compared in the network report; exports older than 14 days trigger a warning. If Splunk data is missing, a service does not count as "insecure without firewall traffic".
- Pay attention to warnings: "keine abgewiesene Verbindung (deny)" (no rejected connection), "Zeiträume überschneiden sich / Lücke" (periods overlap / gap), "n Zeilen, laut _index.csv m" (file changed – export again).

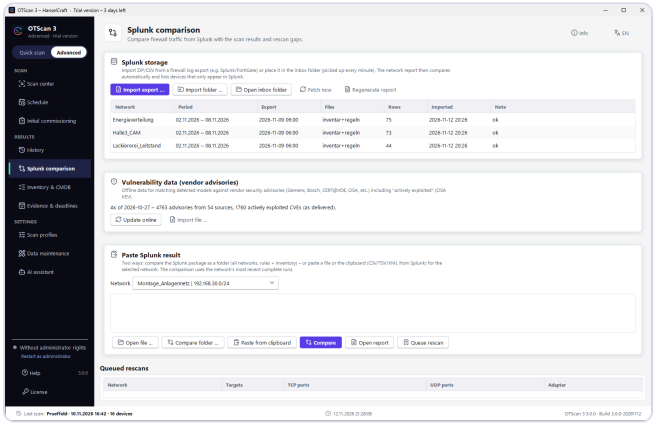
How it works

1. Advanced → RESULTS → "Splunk comparison".
2. Feeding in data – card "Splunk storage": place the export (ZIP or CSV in the format "#FW-EXPORT v2") in Dokumente\OTScan3_Splunk\Eingang – it is collected roughly every 15 seconds. Or "Import export ..." or "Import folder ..."; "Fetch now" collects immediately.
3. The storage table shows for each network the period, export, files, rows, imported and note. The data is located under Dokumente\OTScan3_Splunk\Ablage\<Netzwerk>.
4. Network names in OTScan 3 must be named exactly as in the Splunk files (for example Montage_Anlagennetz), otherwise the network is skipped.

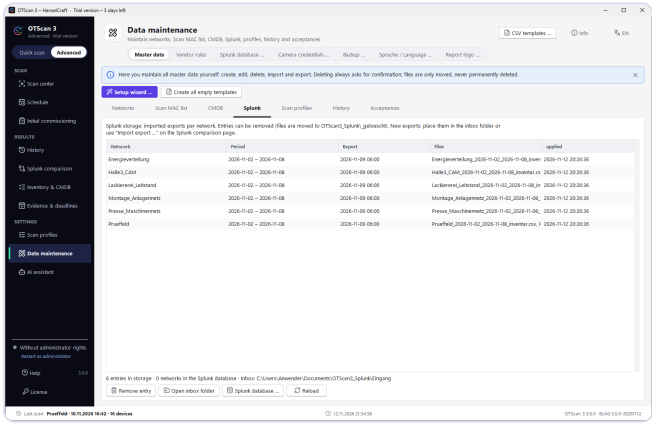
5. Manual comparison – card "Paste Splunk result": "Open file ...", "Compare folder ..." (all networks) or "Paste from clipboard", then "Compare".
6. "Open report" shows the report per network. "Queue rescan" takes over targets and ports; "Start all queued rescans" queues the jobs – only in agreement with the plant owner.
7. "Regenerate report" (select the network in the storage): regenerates PDF, Excel, PowerPoint and CMDB supplement of the most recent complete run with the current Splunk data.
8. Splunk database: SETTINGS → Data maintenance → tab "Splunk database ..." opens the window with the stored firewall exports per network (network, CIDR, flows, uploaded, age). Maintain about once a year.

What do I enter where?

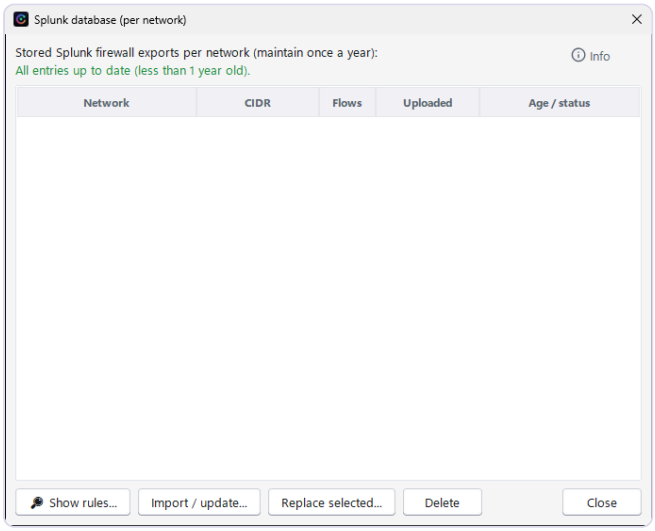
Field	Meaning
Import export ... / Import folder ...	Select a Splunk export (ZIP or CSV, format #FW-EXPORT v2) or a folder with exports.
Open file ... / Compare folder ...	Rule file of a network or a folder with all networks for manual comparison.
Paste from clipboard	Paste copied Splunk result lines directly.
Queued rescans	List of targets and ports for targeted rescans; only start after agreement.



Splunk comparison, Splunk storage and Splunk database



Splunk comparison, Splunk storage and Splunk database



Splunk comparison, Splunk storage and Splunk database

Reports: CMDB addendum (Excel)

File: `<network>_<time>_stufenlauf_CMDB-Nachtrag.xlsx` · View sample: `assets/muster/en/Muster_07_CMDB-Nachtrag_EN.xlsx`

How do I create it?

1. Created when Splunk shows devices that are neither in the scan nor in the CMDB.

How do I read it?

- Sheet "CMDB" in the template layout with the addresses found, sheet "Suchhilfe" with partners, ports and period.

Where does the data come from?

- Splunk inventory and firewall traffic of the network.

What does it not tell you?

- These devices do not answer the scan: find them on site (MAC, switch port) before adding them to the CMDB.

Reports: Device detail view (PDF)

File: `<network>_<time>_stufenlauf_Geraete-Details.pdf` · View sample: `assets/muster/en/Muster_09_Geraete-Detailansicht_EN.pdf`

How do I create it?

1. Tick "Device detail view" in the "Reports & templates" window.

How do I read it?

- One card per device: scan data, name and location from the CMDB, critical ports in plain text, firewall communication with source/destination zone, service, policy, action and count.
- Risk value: 2 points per critical port (maximum 8), +2 for a vendor advisory with CVSS ≥ 7.

Where does the data come from?

- Scan, CMDB, Splunk export (zones, services, policies) and documentation database.

What does it not tell you?

- Per direction only the 5 most frequent allowed connections and all blocked ones.

Reports: Splunk comparison (CSV and report)

File: `Subfolder Splunk of the output folder: <network>_splunkabgleich_<time>.csv, _bericht.md, _ziele.txt, _nachscan.bat or .sh`

How do I create it?

1. Page "Splunk comparison": paste the export or choose a file/folder and click "Compare".

How do I read it?

- One class K1–K6 per IP: confirmed, port gap, only Splunk (server/client), only scan, only denied.
- The follow-up scan file checks the missing ports specifically.

Where does the data come from?

- Firewall export (e.g. Splunk search over FortiGate logs) and the scan XML of the network.

What does it not tell you?

- Splunk only sees traffic through the firewall.

5.3 CMDB comparison

Compare scan results with the inventory Excel file (CMDB) – OK, MAC changed, IP changed, offline, new. Tab "CMDB comparison" in "Inventory & CMDB".

What for?

The inventory (CMDB) is the self-maintained inventory Excel file in the format of the OTScan 3 template. The comparison shows which devices match in the scan and in the CMDB, where MAC or IP differ, which CMDB entries do not respond (offline) and which devices are new. The CMDB file is only read, never changed. After every full run the comparison runs automatically; the tab is for viewing and exporting.

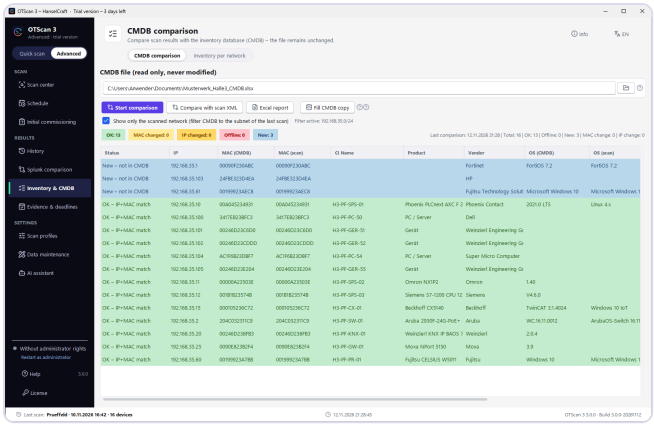
> **Important**
>
> - The original CMDB always remains unchanged. You apply changes yourself from the generated copies and delta files.
> - "Offline" only means: not found in the scan – switched off, relocated or silent. "New" = in the scan, not in the CMDB – check and add.
> - Firmware is compared as a whole word; whitespace and a "V" or "Version" prefix are normalised. Cameras supply firmware to the comparison via ONVIF.

How it works

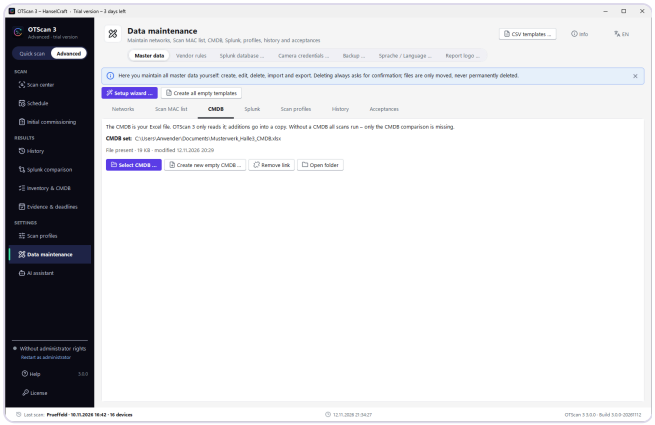
1. Advanced → RESULTS → "Inventory & CMDB" and select the "CMDB comparison" tab at the top.
2. Select the CMDB file with "...": Excel with sheet "CMDB", data from row 18 (IP in column AB, MAC in column AF, CI name in column B).
3. "Start comparison" compares the last saved scan; "Compare with scan XML" takes any result file.
4. The "Show only the scanned network" tick box hides CMDB entries of other networks.
5. Reading: counters at the top (OK, MAC changed, IP changed, offline, new); the table shows per device the status (coloured), IP, MAC according to CMDB and scan, CI name, product, vendor, operating system, building/room, trade and open ports.
6. "Excel report" saves the colour-coded comparison with the "Statistics" sheet. "Fill CMDB copy" creates a copy of the CMDB in the original format with scan data in empty fields.
7. Automatically after each complete "Complete network" run, <Bericht>_CMDB-Delta.xlsx and – with Splunk data – <Bericht>_CMDB-Nachtrag.xlsx are also created.

What do I enter where?

Field	Meaning
CMDB file	Path to the inventory Excel file (sheet "CMDB", data from row 18).
Show only the scanned network	Tick box: filters the CMDB to the subnet of the last scan.



CMDB comparison



CMDB comparison

Reports: CMDB delta (Excel)

File: `<network>_<time>_stufenlauf_CMDB-Delta.xlsx` · View sample: `assets/muster/en/Muster_06_CMDB-Delta_EN.xlsx`

How do I create it?

1. Always created after a complete run if a CMDB is configured.

How do I read it?

- Sheet "Delta-Übersicht": new (green), changed (orange), missing in the scan (grey), notes (blue).
- Sheet "CMDB" has the layout of the CMDB template – copy checked rows into your own CMDB.

Where does the data come from?

- Scan of the network against the configured CMDB file (read only).

What does it not tell you?

- Different open ports depend on the port selection of the run and are only notes.

5.4 Inventory per network

All devices found in a network in one list – with name, vendor, MAC and open services. Tab "Inventory per network" in "Inventory & CMDB".

What for?

The inventory combines the scan results of a network into one row per device. It is created automatically at the end of every staged scan and quick scan and can be rebuilt manually from all scans of a network. It is the basis for CMDB maintenance and the overall inventory across all networks.

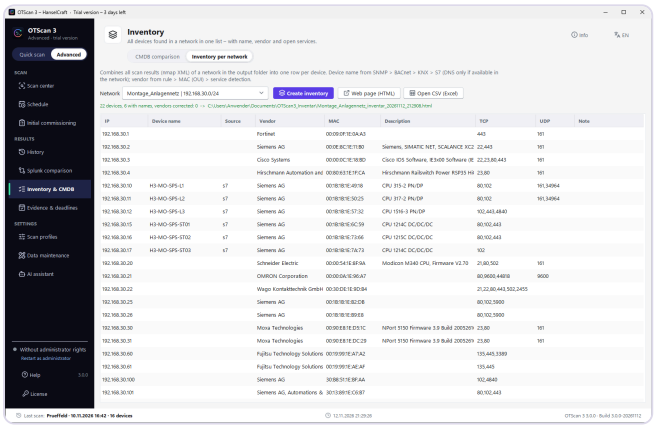
> **Important**
>
> - Device names only come from SNMP, BACnet and KNX; plant networks usually have no DNS. Devices without these services remain nameless.
> - The scan laptop's own adapter addresses are excluded. Cameras appear as "IP camera (ONVIF)" if the CAM stage has run.
> - The inventory summarises what responded – it is not an assessment and not a substitute for the CMDB.

How it works

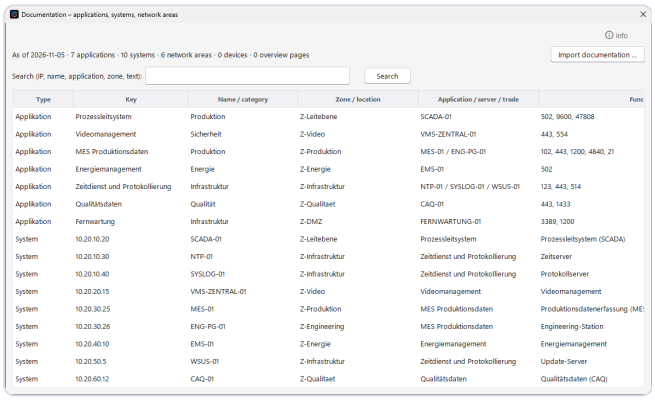
1. Advanced → RESULTS → "Inventory & CMDB" and select the "Inventory per network" tab at the top.
2. Select the network and press "Create inventory" – combines all scan results of this network in the output folder.
3. Reading the columns: IP, device name, source of the name (SNMP before BACnet before KNX before S7 before DNS), vendor (rule before MAC OUI before service detection), MAC, description, TCP, UDP, note.
4. "Web page (HTML)" opens the inventory in the browser, "Open CSV (Excel)" in the spreadsheet application. Storage: Dokumente\OTScan3_Inventar (CSV and HTML per network).
5. Correct wrongly detected vendors permanently via the vendor rules (Data maintenance → "Vendor rules" tab) and rebuild the inventory.
6. Overall inventory across all networks: Scan center → "Output and reports" → "Create overall inventory now" (see "Reports and documents").

What do I enter where?

Field	Meaning
Network	The network whose scans are combined.



Inventory per network



Inventory per network

Reports: Overall inventory CMDB · scan · Splunk (Excel)

File: `OTScan3_Gesamtinventar_<date>.xlsx in the output folder` · View sample: `assets/muster/en/Muster_10_Gesamtinventar_EN.xlsx`

How do I create it?

1. Tick "Overall inventory" in the "Reports & templates" window or "Create overall inventory now".

How do I read it?

- Sheet "Übersicht": count per inventory status with "Was tun?" (what to do). Sheet "Gesamtinventar": one row per device, every value with its source (CMDB, SCAN, SPLUNK).

Where does the data come from?

- CMDB, newest complete staged run per network and newest Splunk inventory per network.

What does it not tell you?

- Networks without a complete run appear as "network open".

Reports: Device directory (PDF)

File: `OTScan3_Geraeteverzeichnis_<date>.pdf` · View sample: `assets/muster/en/Muster_12_Geraeteverzeichnis_EN.pdf`

How do I create it?

1. Tick "Device directory"; created together with the site report.

How do I read it?

- All devices of all networks, one row per device (landscape), with inventory status.

Where does the data come from?

- Overall inventory.

What does it not tell you?

- Contains all addresses – treat as confidential.

Reports: Inventory per network (HTML/CSV)

File: `Documents/OTScan3_Inventar/<network>_inventar_<time>.html and .csv`

How do I create it?

1. Inventory & CMDB → tab "Inventory per network" → "Create inventory"; also created at the end of every staged run.

How do I read it?

- One row per device with name, source of the name, vendor, MAC, description and open ports.

Where does the data come from?

- All scan files of the network in the output folder, vendor rules.

What does it not tell you?

- Without CMDB comparison – use the CMDB delta or the overall inventory for that.

5.5 Vendor advisories (CSAF) and action list

Compare detected models and firmware versions offline against vendor security advisories and output them as actions.

What for?

Models and firmware versions detected in the staged scan (S7, BACnet, KNX, CODESYS, SNMP, ONVIF for cameras) are compared with an offline index of security advisories (CSAF 2.0) from Siemens ProductCERT, CERT@VDE, Bosch PSIRT, CISA ICS and others, supplemented by "actively exploited" (CISA KEV) and the exploit probability (EPSS). The result appears in the PDF section "Known vulnerabilities", in the Excel sheet "Vulnerabilities" and in the action list.

Important

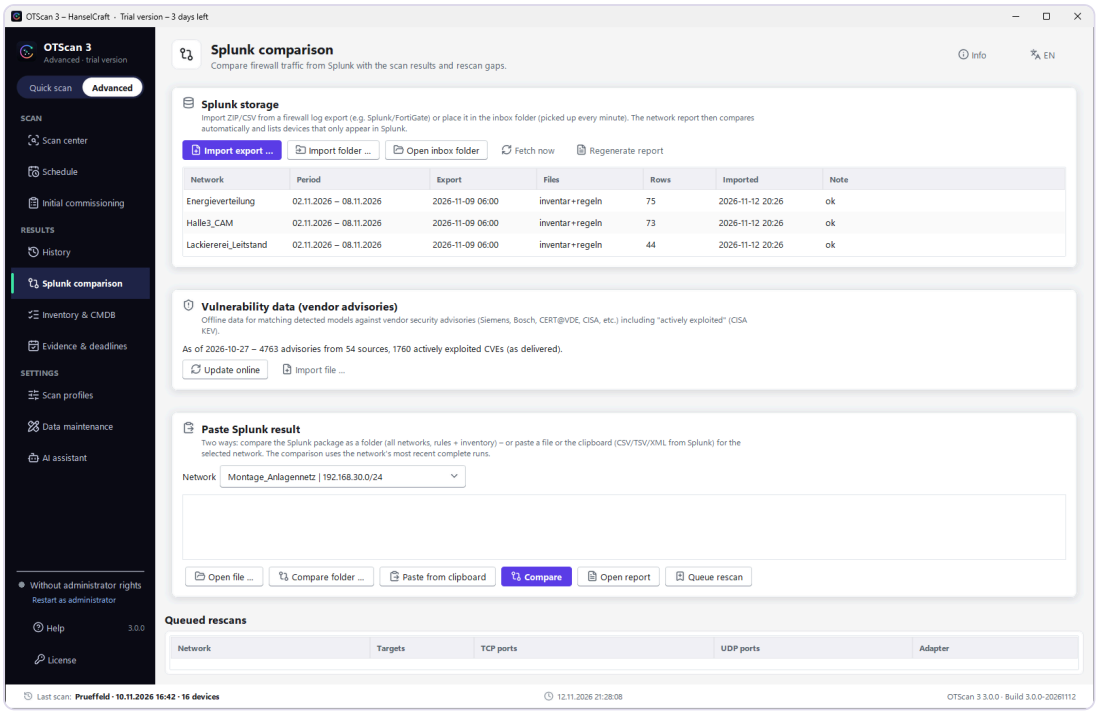
- Urgency in the action list indicates how easily something can be remedied – not the risk.
- Always check "Model" and "Vendor" matches at the device; the index does not replace the original advisory (link in the Excel file). Without a detected model, a device cannot be checked.
- The online retrieval is the only function that accesses the internet – and only on click. On a scan PC without internet, use the file route.

How it works

1. Advanced → RESULTS → "Splunk comparison" → card "Vulnerability data (vendor advisories)".
2. Update the index: "Update online" (only on a PC with internet) or "Import file ..." with otsp_csaf_index.json.gz created on an internet PC with otsp_csaf_sync.py --aus <Ordner>.
3. Check data status: the "created" field shows the date of the index. It is located in %APPDATA%\OTScan3\csaf\otsp_csaf_index.json.gz.
4. Let the staged scan run – the comparison happens automatically when the reports are generated. After an index update, regenerate existing reports.
5. Reading: quality "exact" = firmware is demonstrably in the affected range; "Model" = model matches, version open – check at the device; "Vendor" = only a weak indication.
6. Open the action list <Bericht>_Massnahmen.xlsx: one row per insecure service and per vendor advisory with CMDB name, location, trade, urgency, firewall traffic and the columns Responsible, Date, Status and Remark for working through.

What do I enter where?

Field	Meaning
Import file ...	Select the index file otsp_csaf_index.json.gz from an internet PC.
Responsible, date, status, remark	Columns of the action list for working through (status as a selection list).



Vendor advisories (CSAF) and action list

Reports: Action list (Excel)

File: `<network>_<time>_stufenlauf_Massnahmen.xlsx` · View sample: `assets/muster/en/Muster_05_Massnahmen_EN.xlsx`

How do I create it?

1. Always created after a complete run.

How do I read it?

- One row per device and finding: urgency, IP, device, vendor, model/firmware, name/location/trade from the CMDB, what, traffic via firewall, recommendation.
- The columns from "Responsible" to "Remark" are meant for ticking off.

Where does the data come from?

- Insecure services from the scan, vendor advisories from the CSAF data, location and owners from the CMDB, traffic from Splunk.

What does it not tell you?

- Urgency says how quickly and easily something can be fixed – not how big the risk is.

5.6 Reports and documents

Which reports exist, where they are located, how to generate, open and read them – with the "Reports & templates …" window.

What for?

After every complete run, OTScan 3 generates reports for different readers: PDF for plant owners, Excel for engineering, PowerPoint for management, action list for the trades. In addition there are PDF reports per network (network check, device detail view), across all networks (site report, device directory) and

the overall inventory as Excel. In the "Reports & templates ..." window you choose which reports are generated and view anonymised samples.

Important

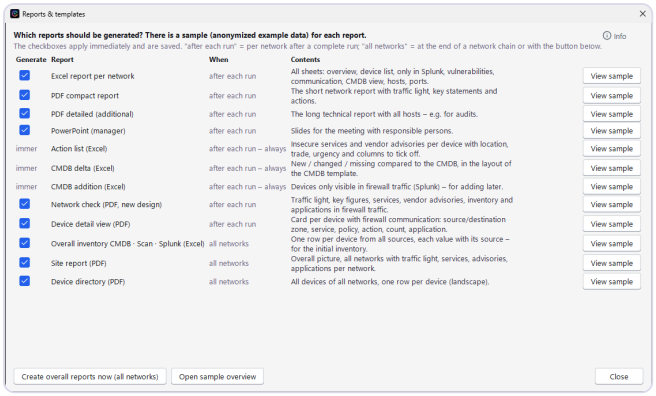
- OTScan 3 generates the new PDF reports (network check, device detail view, site report, device directory) in the background via Microsoft Edge.
- All reports are confidential and contain IP and MAC addresses. Only pass on documents without addresses and site to external parties.
- Partial runs (individual stages, Part A/B scans) do not produce an overall report. There is exactly one report per complete run.
- While a report is being created (up to one minute), do not open or move the files in the output folder.

How it works

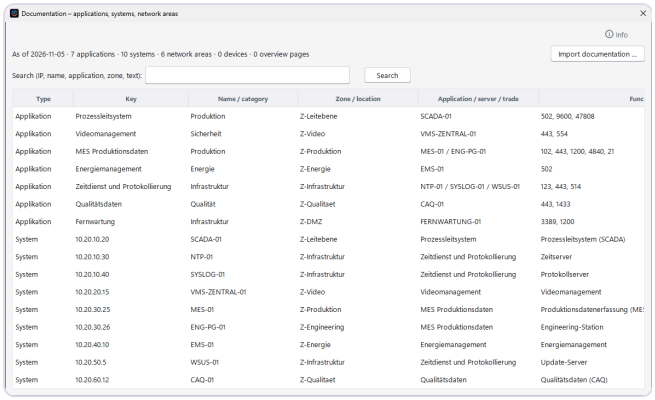
1. Advanced → SCAN → Scan center → expand "Output and reports". Check the output folder (default Documents).
2. Tick "Generate after each scan" for Excel, PDF and PowerPoint; "PDF detailed in addition" only if required (for audits).
3. Open "Reports & templates ...": all report types are listed with tick boxes. Tick network check, device detail view, site report, device directory and overall inventory.
4. "View sample" shows an anonymised example file for each report type – so you can see beforehand what you will get.
5. Generating: the selected reports are created automatically at the end of every full run. Manually: select the job in the queue → "Regenerate reports for selected job", or "Generate reports from XML", or "Create overall inventory now".
6. Opening: in the output folder, the file names contain the network name and time, for example Halle3_CAM_<Zeit>_stufenlauf.pdf. In the quick scan there are the buttons "Open report (PDF)", "Excel" and "Compact report (HTML)".
7. Other storage locations: inventory in Dokumente\OTScan3_Inventar, Splunk comparison in the Splunk subfolder of the output folder, initial commissioning packages in Dokumente\OTScan3_Abnahmen\<Jahr>, templates in Dokumente\OTScan3_Vorlagen.
8. Reading: in the PDF, start with page 1 (traffic light, the most important points, what to do). If "UNVOLLSTAENDIG" (incomplete) appears in the footer, repeat the scan before drawing conclusions.
9. Every report is described in the info window: "Info" → topic "Reports and documents" – or in this manual in the Reports part.

What do I enter where?

Field	Meaning
Output folder	Folder for all reports of a run. Default: Documents.
Generate after each scan	Tick box per format: Excel, PDF, PowerPoint.
PDF detailed in addition	Stores the long report next to the compact report.
Tick box in "Reports & templates ..."	Selects network check, device detail view, site report, device directory and overall inventory.



Reports and documents



Reports and documents

Reports: PDF compact report

File: `<network>_<time>_stufenlauf.pdf in the output folder (default: Documents)` · View sample: `assets/muster/en/Muster_02_PDF_Kompakt_EN.pdf`

How do I create it?

1. Created at the end of every complete run if the PDF tick is set under "Output and reports".
2. Manually: select the job → "Regenerate reports for selected job".

How do I read it?

- Page 1: traffic light, key figures, "Key points" and "What needs to be done?" – enough for the plant owner.
- Then the table "Insecure services": per service the number of devices, why it is risky, what to do.

Where does the data come from?

- Scan result (nmap XML) of the run, assessed against the traffic rules (HanselCraft default, adjustable).
- Splunk period and "only in firewall traffic" from the Splunk store, CMDB reference from the configured CMDB.

What does it not tell you?

- An insecure service is an open door, not an attack.
- Splunk does not see traffic inside a network – "no firewall traffic" does not mean "unused".

Reports: PDF detailed

File: `<network>_<time>_stufenlauf_ausfuehrlich.pdf` · View sample: `assets/muster/en/Muster_03_PDF_ausfuehrlich_EN.pdf`

How do I create it?

1. Tick "PDF detailed (additional)" in the "Reports & templates" window.
2. Created next to the compact report.

How do I read it?

- For audits and specialists: summary, heatmap by subnet and device type, critical hosts, complete host inventory.
- Chapter "Technical details" names profile, port set and nmap version.

Where does the data come from?

- The same scan XML as the compact report.

What does it not tell you?

- Long for large networks; for meetings use the compact report or PowerPoint.

Reports: Excel report per network

File: `<network>_<time>_stufenlauf.xlsx` · View sample: `assets/muster/en/Muster_01_Excel_Netzwerk_EN.xlsx`

How do I create it?

1. Excel tick under "Output and reports"; created after every complete run.

How do I read it?

- Sheets: overview, device list, only in Splunk, vulnerabilities, communication, CMDB view, shadow (not in the CMDB), hosts, ports, scripts.
- Use filters in the device list, e.g. on insecure services or vendor.

Where does the data come from?

- Scan XML, Splunk store, CMDB and vendor advisories (CSAF data).

What does it not tell you?

- Working file for engineers; contains all addresses – do not pass on externally.

Reports: PowerPoint (management)

File: `<network>_<time>_stufenlauf_manager.pptx` · View sample: `assets/muster/en/Muster_04_PowerPoint_Manager_EN.pptx`

How do I create it?

1. PowerPoint tick under "Output and reports".

How do I read it?

- A few slides with traffic light, key figures and the most important actions – for meetings with the people responsible.

Where does the data come from?

- The same data as the compact report.

What does it not tell you?

- Deliberately short; details are in the PDF and in Excel.

Reports: Network check (PDF)

File: `<network>_<time>_stufenlauf_Netzwerk-Check.pdf` · View sample: `assets/muster/en/Muster_08_Netzwerk-Check_EN.pdf`

How do I create it?

1. Tick "Network check" in the "Reports & templates" window; created in the background after every complete run.

How do I read it?

- Cover page with traffic light, then "At a glance", services, vendor advisories, inventory status and applications in firewall traffic.

Where does the data come from?

- Run Excel, action list, overall inventory, Splunk store and documentation database.

What does it not tell you?

- Needs Microsoft Edge, Google Chrome or Chromium for the PDF; without a browser an HTML file remains.

Reports: Site report (PDF)

File: `OTScan3_Standortbericht_<date>.pdf` · View sample: `assets/muster/en/Muster_11_Standortbericht_EN.pdf`

How do I create it?

1. Tick "Site report"; created at the end of a network chain or with "Create overall reports now (all networks)".

How do I read it?

- Overall picture of all networks with traffic light, most frequent services, vendor advisories and applications per network.

Where does the data come from?

- Newest complete run per network, overall inventory, Splunk store, documentation database.

What does it not tell you?

- Older runs of individual networks are included with their state – check the date per network.

5.7 Evidence & deadlines

Recurring obligations around OT security with cycle, next due date and traffic light – e.g. as a reminder for evidence under NIS2 or IEC 62443.

What for?

Many tasks in OT operations recur: inventory, repeat scan, review of remote maintenance access, firewall rules, firmware versions, backups, emergency drill, training. For each obligation the page remembers when it was last done, calculates the next due date and shows what is overdue (red) or due within the next 30 days (yellow). Every completion stays visible in the history – so you can show that checks were carried out regularly.

> **Important**
>
> - The suggestions are neutral practical examples, not legal advice. Which obligations and deadlines apply to your organisation (e.g. under NIS2 or the German BSI Act) follows from your own requirements, contracts and the law applicable to you.
> - OTScan 3 does not send e-mail reminders – you see the traffic light on this page and via the AI assistant.
> - The obligations are stored in the OTScan 3 database and are included in the data backup. "Delete" removes an obligation together with its history.

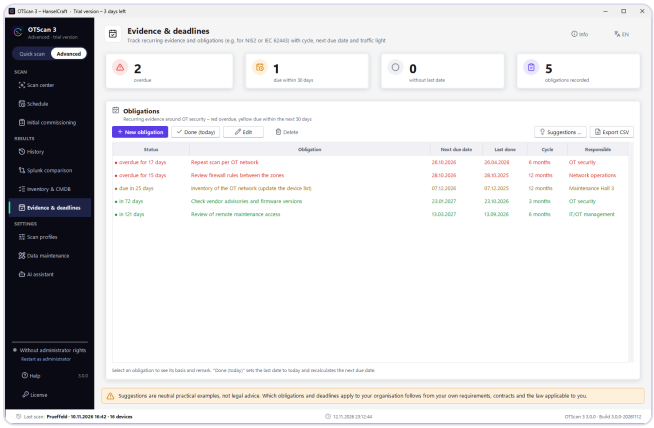
How it works

1. Advanced → RESULTS → open "Evidence & deadlines".

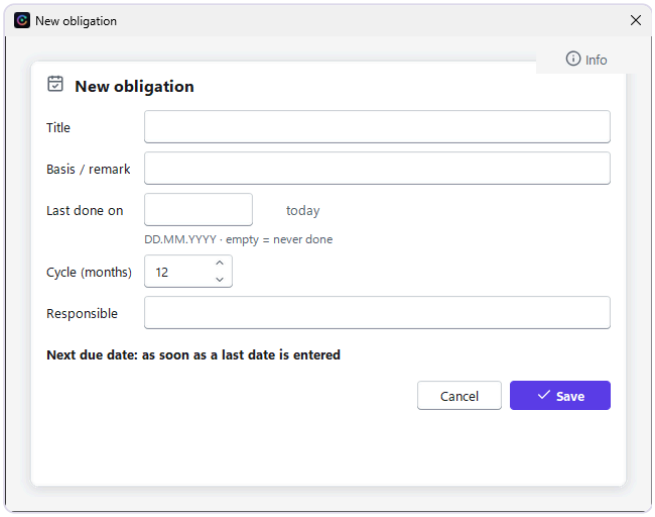
2. Choose "Suggestions ...", tick the suitable practical examples and click "Apply" – or create your own with "New obligation".
3. Double-click an obligation (or "Edit") and enter the cycle in months, the person responsible and the date it was last done. The next due date appears immediately in the dialog.
4. Once the work is done, select the obligation and choose "Done (today)". The date is taken over, the next due date is recalculated, the previous date stays in the history.
5. "Export CSV" saves the list with all previous dates for Excel, e.g. as an appendix to an audit report.

What do I enter where?

Field	Meaning
Title	Short name of the obligation, e.g. "Review of remote maintenance access".
Basis / remark	Where the obligation comes from (own policy, contract, standard) and what has to be done.
Last done on	Date DD.MM.YYYY; empty = never done (yellow, "no date yet").
Cycle (months)	1 to 120 months until the next due date.
Responsible	Person or role who carries out the obligation.
Traffic light	Red = overdue, yellow = due within the next 30 days or no date yet, green = due later.



Evidence & deadlines



Evidence & deadlines

6 Settings

6.1 Data maintenance – maintain all master data yourself

Create, edit, delete, import and export networks, Scan MAC list, CMDB, Splunk, profiles, history and acceptances – plus vendor rules, Splunk database and camera credentials.

What for?

You maintain all data OTScan 3 needs in one place yourself – without editing files by hand. Exports have the import format and can be imported again. Deleting always asks for confirmation; files (Splunk exports, acceptance packages) are only moved to a _geloescht folder.

> **Important**
>
> - Do not change the Scan MAC list while a network chain is running.
> - Deleting a network does not delete any scan results or history.
> - Default profiles are re-created at every start and therefore cannot be deleted.

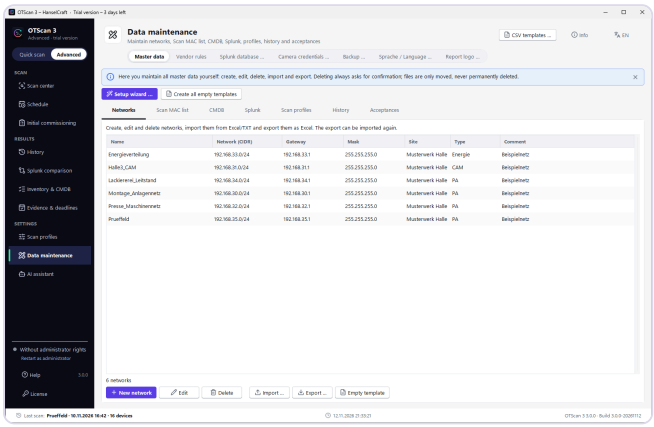
How it works

1. Advanced → SETTINGS → "Data maintenance". At the top are the tabs "Master data", "Vendor rules", "Splunk database ..." and "Camera credentials ..." (the last two open windows).
2. The "Master data" tab contains the inner tabs Networks, Scan MAC list, CMDB, Splunk, Scan profiles, History and Acceptances.
3. Networks: "New network", "Edit" (or double-click), "Delete" (multiple selection), "Import ...", "Export ...", "Empty template" – details in the section "Create, edit and import networks".
4. Scan MAC list: maintain scan MAC, scan IP and status (requested, registered, rejected) per network. If the MAC is left empty, OTScan 3 suggests one.
5. CMDB: select a file, create a new empty CMDB or remove the link. Splunk: view and remove imported exports per network, open the inbox folder.
6. Scan profiles: delete custom profiles (standard profiles remain). History: remove test runs (files remain). Acceptances: remove entries (package is moved to _geloescht).
7. "CSV templates ..." at the top right: download templates for networks, Scan MAC list, vendor rules, scan profiles and schedule, and upload them filled in.
8. "Create all empty templates": network list, Scan MAC list and CMDB as Excel as well as all CSV templates under Dokumente\OTScan3_Vorlagen\Start.
9. "Setup wizard ..." starts the wizard again. "Info" at the top right always explains the tab that is currently open.

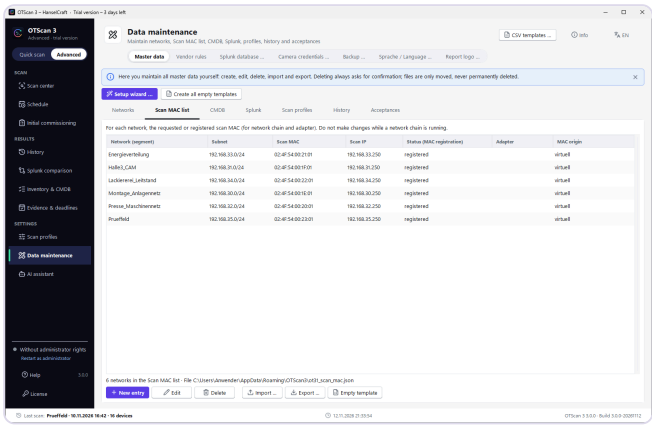
What do I enter where?

Field	Meaning
Master data tab	Inner tabs: Networks, Scan MAC list, CMDB, Splunk, Scan profiles, History, Acceptances.

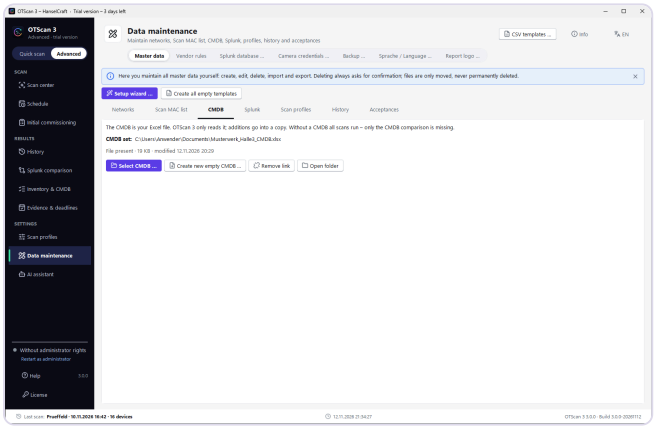
Field	Meaning
Scan MAC	MAC address under which the scanner appears in the network, for example 02:4F:54:00:00:01. Empty = suggestion.
Scan IP	Address of the scanner in the network; empty = OTScan 3 searches for a free address.
Status (MAC registration)	requested, registered or rejected – only "registered" is ready to start for the network chain.
CMDB file	Linked inventory Excel file; "New empty CMDB" creates one.



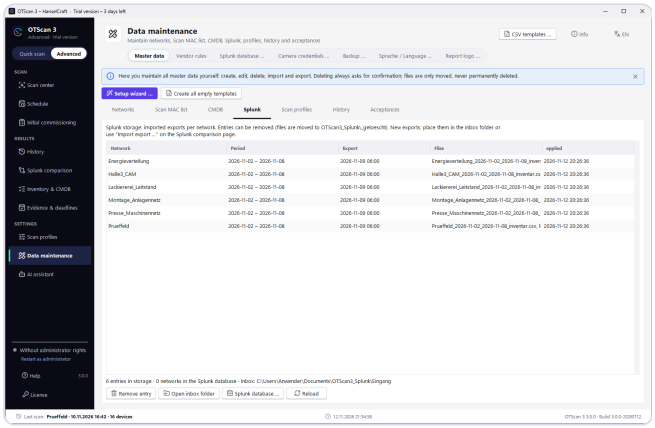
Data maintenance – maintain all master data yourself



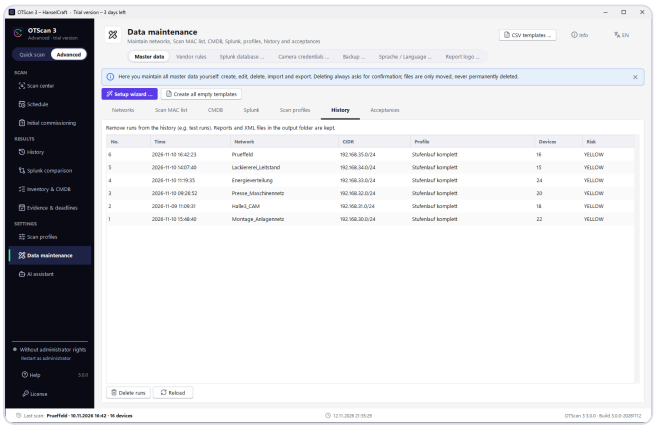
Data maintenance – maintain all master data yourself



Data maintenance – maintain all master data yourself



Data maintenance – maintain all master data yourself



Data maintenance – maintain all master data yourself

6.2 Create, edit and import networks

Create and change networks manually in Data maintenance or import them via Excel, text or CSV template.

What for?

Every plant network must be known to OTScan 3: name, network (CIDR), gateway, site, VLAN, type. The name must exactly match the Splunk files and the Scan MAC list. Networks with "CAM" in their name automatically get the camera profile. Created networks are then available for selection in the Scan center, quick scan, network chain and schedule.

> **Important**
>
> - The name must be spelled exactly as in Splunk and in the Scan MAC list – otherwise the Splunk comparison finds no data.
> - A wrong mask (for example /24 instead of /23) means: only half of the plant is checked. The CIDR must be the network address (host bits 0).
> - Do not delete or rename networks while a scan or a network chain is running on this network.

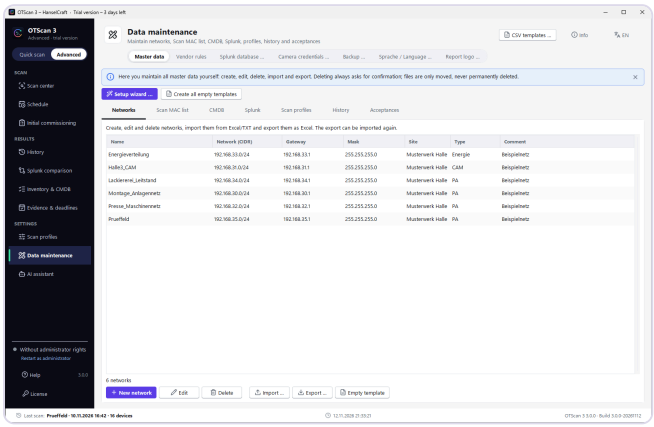
How it works

1. Advanced → SETTINGS → "Data maintenance" → "Master data" tab → inner tab "Networks".
2. "New network" opens the "New network" dialog. Name and network (CIDR) are mandatory, for example Montage_Anlagennetz and 192.168.6.0/24. Gateway, mask, site, VLAN and comment as required – then "Save".
3. Edit: select the row and click "Edit" or double-click. Name and CIDR can also be changed.
4. Delete: select one or more rows, "Delete", confirm the prompt. Scan results and history are kept.
5. Import from Excel or text: "Import ..." and select the network list. "Empty template" creates a matching empty list.
6. Import via CSV: at the top right "CSV templates ..." → row Networks → "Download template ...", fill in, save as CSV, "Upload completed CSV ...". OTScan 3 shows "n valid, m with errors" and, after confirmation, imports only the valid rows.
7. Check the result: the table shows the new networks; the number is shown at the bottom. "Export ..." saves the list as Excel in the import format.
8. Then, in the inner tab "Scan MAC list", add Scan MAC and scan IP if the network is to be scanned via the network chain or with Scan MAC.

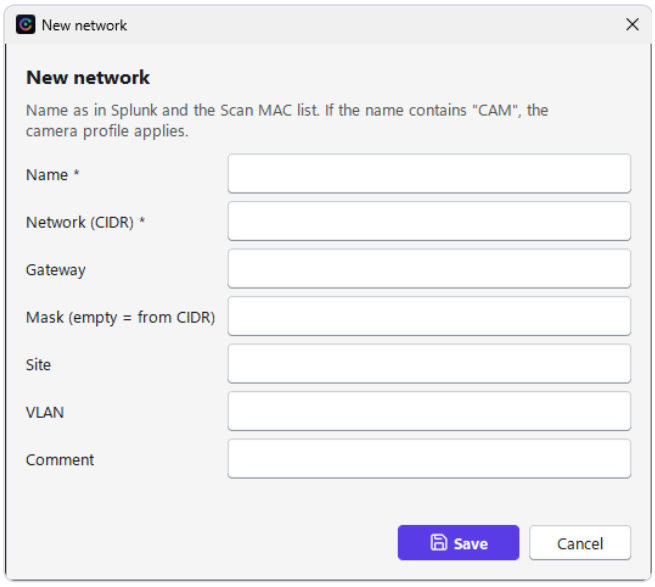
What do I enter where?

Field	Meaning
Name *	Network name, only letters, digits and _ . -, for example Montage_Anlagennetz. With "CAM" in the name, the camera profile applies.
Network (CIDR) *	Network address with prefix, for example 192.168.6.0/24. Host bits must be 0.
Gateway	Gateway in the network, for example 192.168.6.1. Must be within the network.
Mask	Leave empty = calculated from the CIDR.

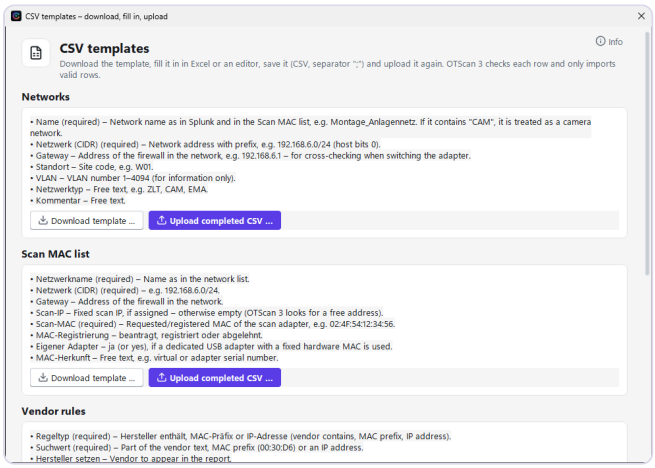
Field	Meaning
Site	Site code or name, freely selectable.
VLAN	VLAN number 1 to 4094 (optional).
Network type	Only in the CSV template: type of network, for example ZLT or CAM (optional).
Comment	Free text, for example contact person role or special features.



Create, edit and import networks



Create, edit and import networks



Create, edit and import networks

6.3 Set up adapter and Scan MAC

For each network, set up the scan adapter with registered Scan MAC and scan IP and reset it afterwards.

What for?

Many plant networks are only enabled for registered MAC addresses (network access control, for example MAC-based port approval). That is why the "Set up network adapter" window configures an adapter for the network: set the Scan MAC, assign the scan IP, correct the mask and reset everything later. Which Scan MAC and scan IP applies to each network is stored in the Scan MAC list.

Important

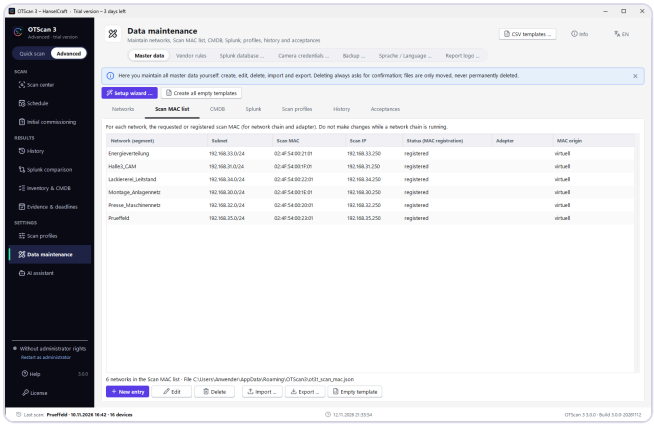
- Only use registered MACs. Virtual Scan MACs follow the scheme 02:4F:54 plus bytes 2 to 4 of the network address (locally administered), for example 02:4F:54:00:00:01.
- If a scan is currently running on the adapter, the window does not allow switching. Wireless, company and VPN adapters are rejected for Scan MACs.
- "Treiber erlaubt keine eigene MAC" (driver does not allow its own MAC) means: use a different adapter. Only edit the file %APPDATA%\OTScan3\ot31_scan_mac.json while the program is closed – OTScan 3 writes it on exit.
- Report a self-selected scan IP to the IP address management (IPAM) afterwards.

How it works

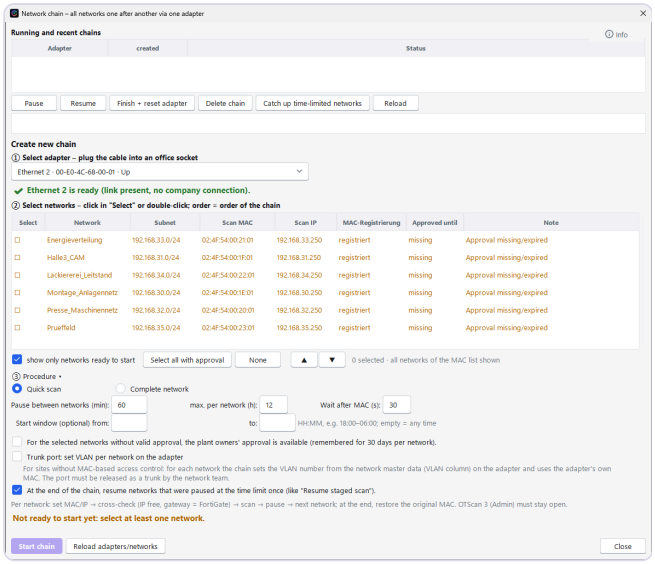
1. Maintain the Scan MAC list: SETTINGS → Data maintenance → Master data tab → "Scan MAC list" – for each network Scan MAC, scan IP and status. Or import an existing Scan MAC list (Excel or CSV) or upload the CSV template "Scan MAC list".
2. SCAN → Scan center → select the network. If the adapter traffic light is not green, press "Set up adapter ...".
3. In the window, select the network. Scan MAC and scan IP are pre-filled from the Scan MAC list; check the "Set Scan MAC" tick box. Leave the scanner IP empty = OTScan 3 searches for a free address.
4. Alternatively "Import MAC list ..." in the window: imports your Scan MAC list and creates missing networks. After a program update, import the list again once.
5. "Set (admin)" backs up the original MAC and IP setting, sets the MAC in the background via PowerShell using the driver property "Network Address", restarts the adapter, waits for the network assignment and sets the IP – deliberately without a default gateway.
6. Wait until the traffic light is green. In the quick scan, then "Search again".
7. After the scan: "Reset" restores the original MAC and the original IP setting (success only if the hardware MAC is active again).
8. "Info" at the top right of the window explains every step.

What do I enter where?

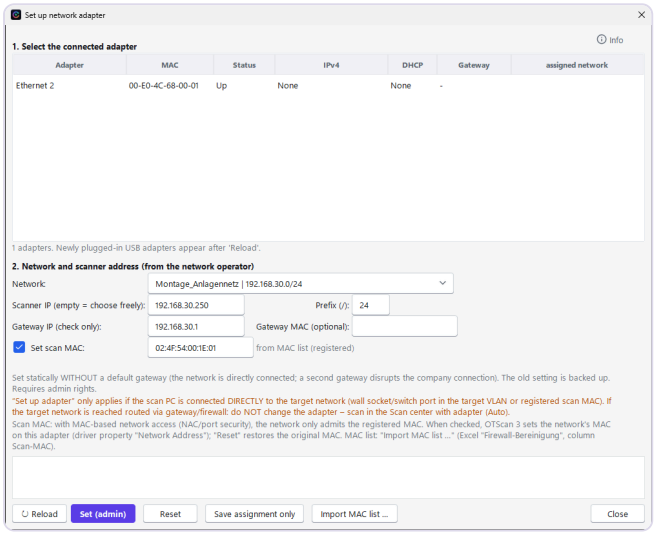
Field	Meaning
Network	Network for which the adapter is set up.
Adapter	Physical network port of the scan laptop in the target network.
Set Scan MAC	Tick box: sets the registered Scan MAC, for example 02:4F:54:00:00:01.
Scan IP / scanner IP	Fixed address of the scanner, for example 192.168.6.250; empty = search for a free address.
Mask	Netmask of the adapter; must match the stored network.
Import MAC list ...	Select the Scan MAC list (Excel or CSV).



Set up adapter and Scan MAC



Set up adapter and Scan MAC



Set up adapter and Scan MAC

6.4 Download, fill in and upload CSV templates

Import master data in bulk via CSV: networks, Scan MAC list, vendor rules, scan profiles and schedules.

What for?

Instead of creating many entries individually, download a CSV template, fill it in in the spreadsheet application and upload it again. OTScan 3 checks each row, shows errors with row number and reason and, after your confirmation, imports only the valid rows. The example line of the template is never imported.

Important

- Before uploading a large list, back up the master data: in Data maintenance, "Export ...".
- Do not upload any data while a scan or a network chain is running – especially not the Scan MAC list.
- Scan profiles from CSV are only imported without aggressive timing (-T4, -T5) and without attacking scripts. This protects the plant.
- Networks in the schedule must already have been created. Therefore upload networks and profiles first, then the schedule.

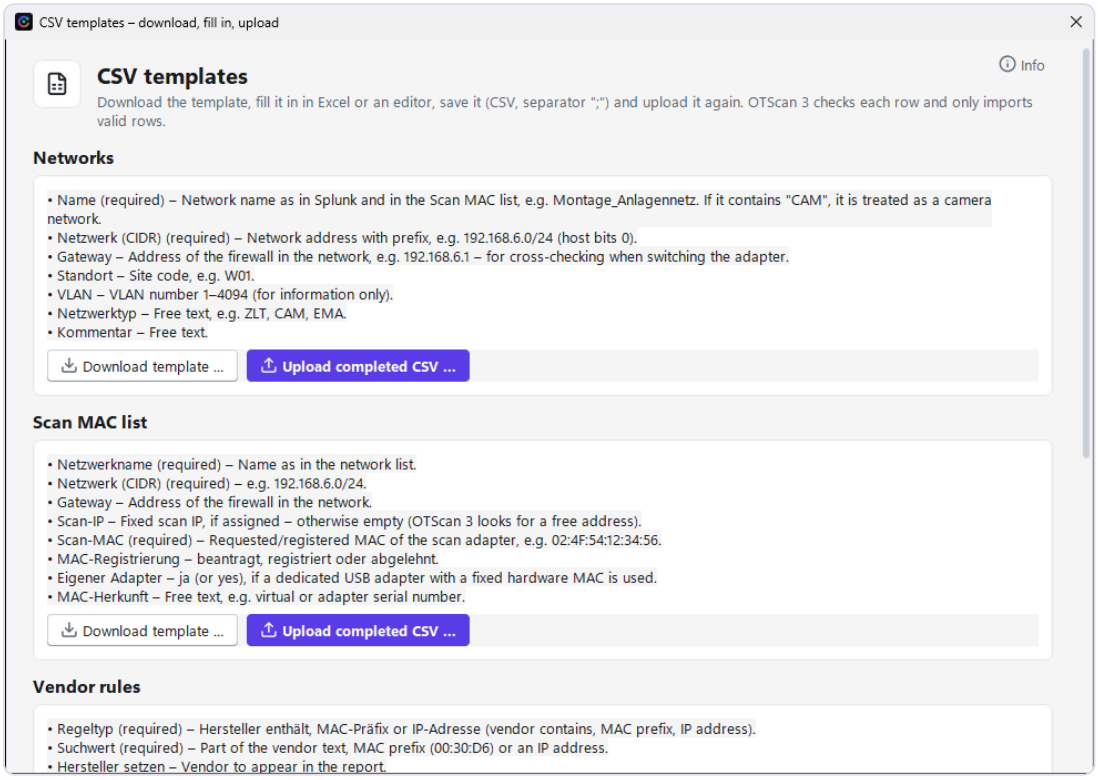
How it works

1. Press the "CSV templates ..." button at the top right – in Data maintenance, in Vendor rules, in Scan profiles or in Schedule. The "CSV templates" window shows two buttons per data type.
2. For the matching data type, select "Download template ..." and specify a storage location. The template contains the header line and an example line.
3. Open the template in Excel and fill in one row per entry. Mandatory columns are marked with * (see "What do I enter where?"). Enter nmap arguments in Excel with a leading ', otherwise Excel turns them into #NAME? – OTScan 3 removes the ' when uploading.
4. Save as CSV: separator semicolon, character set UTF-8 (in Excel "CSV UTF-8"; Windows-1252 also works). You may leave the example line in place.
5. Back in the window, for the same data type select "Upload completed CSV ..." and choose the file.
6. OTScan 3 checks each row and reports "n valid, m with errors", below that the row number and the reason for each faulty row.
7. Typical reasons and remedies: CIDR without /prefix or with host bits (192.168.6.5/24 instead of 192.168.6.0/24); existing network name with a different CIDR or existing network under a different name (renaming only in Data maintenance); gateway or scan IP not in the network; MAC not 12 hex characters, multicast, duplicate or already assigned to another network; more than one row per network in the Scan MAC list; VLAN outside 1–4094; invalid characters in the name; free text starts with = + @ or contains an Excel error value such as #NAME?.
8. Further reasons: profile with -T4/-T5 (also -T 4, aggressive, insane), -oX, -oS, -iL, -iR, --datadir, --resume, --excludefile, --script all or * or scripts vuln, exploit, brute, dos, intrusive; schedule name already exists or is duplicated in the file; network or profile in the schedule unknown; day of the month outside 1–28; time not HH:MM. If the Windows task could not be created, the message names the entries – they are then deactivated.
9. Confirm the prompt: only the valid rows are imported. Correct faulty rows in the file and upload the file again.
10. All empty templates at once: Data maintenance → "Create all empty templates" places them in Dokumente\OTScan3_Vorlagen\Start. They are also in the package in the "vorlagen" folder.

What do I enter where?

Field	Meaning
Networks	Name*, network (CIDR)*, gateway, site, VLAN, network type, comment.
Scan MAC list	Network name*, network (CIDR)*, gateway, scan IP, Scan MAC*, MAC-Registrierung (beantragt/registriert/abgelehnt), own adapter (ja/nein), MAC origin.

Field	Meaning
Vendor rules	Rule type* (Hersteller enthält | MAC-Präfix | IP-Adresse), search value*, set vendor, set operating system, active, note.
Scan profiles	Name*, description, nmap arguments* (in Excel with a leading ', for example '-sT), port set.
Schedule	Name*, network*, profile*, port set, interval* (täglich/wöchentlich/monatlich), time* (HH:MM), day (Mo...So or 1–28).
Format	Separator ";", UTF-8 (Excel "CSV UTF-8") or Windows-1252; first line = header line.



Download, fill in and upload CSV templates

6.5 Scan profiles and port sets

View, duplicate and create technical nmap profiles – only needed for individual jobs and schedules.

What for?

A profile is a set of nmap parameters (scan type, throttling, scripts), a port set is the list of checked ports. The four active profiles correspond to the stages of the staged scan; all others are shown greyed out at the bottom as "Archive · ...". You do not need this page for regular checks – the staged scan selects everything itself.

Important

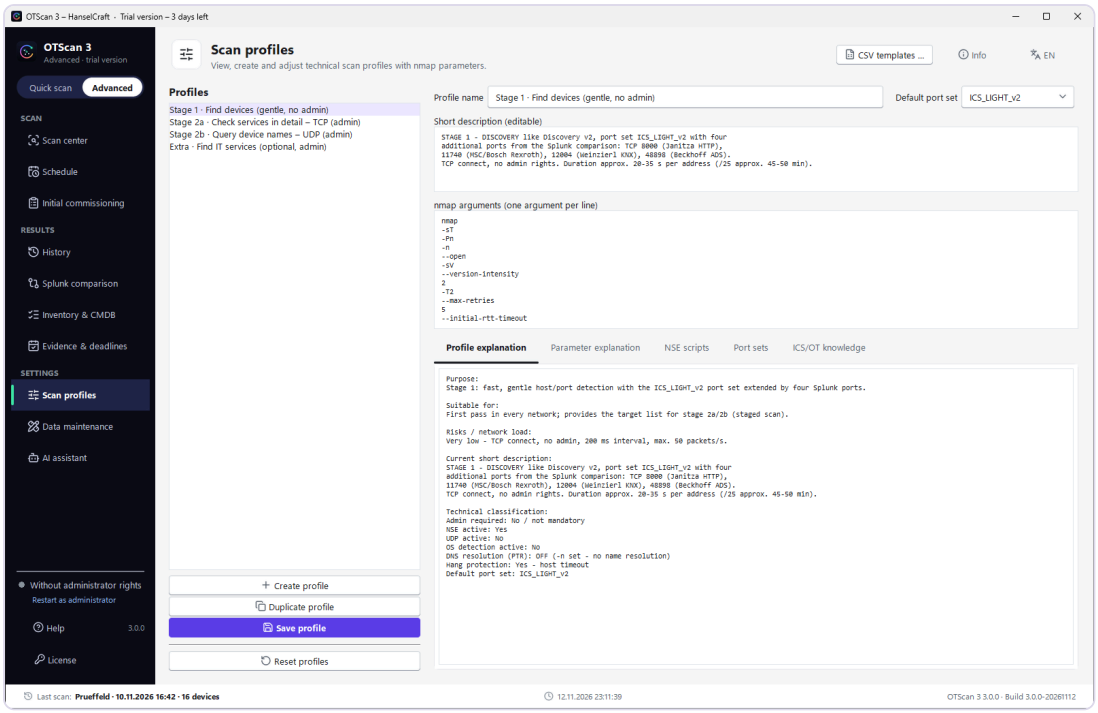
- Default profiles are reset to the program version at every program start. Your own changes are only kept under a new name.
- Do not change technical profile names – history, time estimation and staged scan depend on them.
- None of the active profiles uses operating system detection (-O) or scripts of the categories vuln, brute, exploit, intrusive. The CSV import rejects own profiles with -T4/-T5 or such scripts – scan gently.

How it works

1. Advanced → SETTINGS → "Scan profiles". On the left the profiles: "Stage 1 · Find devices (gentle, no admin)", "Stage 2a · Check services in detail – TCP (admin)", "Stage 2b · Query device names – UDP (admin)", "Extra · Search for IT services (optional, admin)", below them archive profiles.
2. On the right: profile name, default port set, short description, nmap arguments (one argument per line) and the tabs profile explanation, parameter explanation, NSE scripts, port sets, ICS/OT knowledge.
3. Own profile: "Duplicate profile", change the name, adjust the arguments, "Save profile". "Create profile" starts empty; "Reset profiles" restores the default profiles.
4. Many profiles at once: "CSV templates ..." at the top right → Scan profiles → download the template, fill it in, upload it.
5. Port sets: discovery (ICS_LIGHT_v2: 23 TCP + 5 UDP), OT depth (ICS_OT_CORE: about 60 TCP + 19 UDP), IT services (ICS_IT_SWEEP: 27 TCP + 4 UDP), none. In CAM networks, OTScan 3 adds camera ports.

What do I enter where?

Field	Meaning
Profile name	Technical name; save your own profiles under a new name.
Default port set	Port list the profile uses if nothing else is specified.
Short description	One sentence describing what the profile is intended for.
nmap arguments	One argument per line, for example -sT or --max-rate 50. Without -T4/-T5 and without -oX.



Scan profiles and port sets

6.6 Vendor rules

Your own corrections for vendor and operating system that apply when reading in every scan – "Vendor rules" tab in Data maintenance.

What for?

Vendors recognised from the MAC address are sometimes misleading – for example "MSC Vertriebs" instead of "Bosch Rexroth". With vendor rules you permanently override vendor and operating system by vendor text, MAC prefix or IP address. The rules apply to reports, inventory and comparisons.

> **Important**
>
> - Rules apply when reading in every scan from the moment they are saved. Reports already generated do not change – regenerate reports.
> - IP rules are bound to the network – for relocated devices an IP rule loses its meaning. MAC prefix rules are more robust.
> - After camera queries, ONVIF supplies the vendor directly; a rule is rarely needed there.

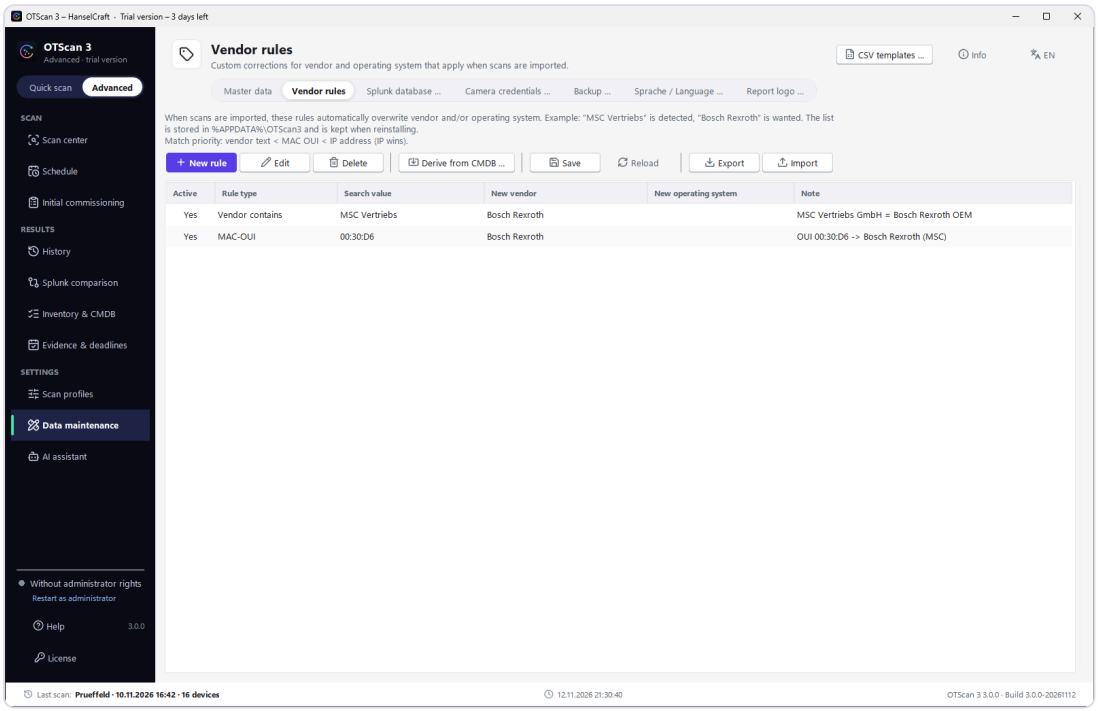
How it works

1. Advanced → SETTINGS → "Data maintenance" and select the "Vendor rules" tab at the top.
2. "New rule": enter rule type (vendor contains, MAC prefix, IP address), search value, new vendor, new operating system and note; check the "Active" column.
3. "Edit", "Delete", "Save", "Reload". "Derive from CMDB ..." creates rules from the CMDB.
4. Many rules at once: "CSV templates ..." at the top right → Vendor rules → download the template, fill it in, upload it.
5. "Export" and "Import" save the list as vendor_os_overrides.json (located in %APPDATA%\OTScan3 and kept during reinstallation).

6. Match priority: vendor text before MAC prefix before IP address – the IP rule wins.

What do I enter where?

Field	Meaning
Rule type	Vendor contains, MAC prefix or IP address.
Search value	What is searched for, for example "MSC Vertriebs", "00:1B:1B" or "192.168.6.21".
Set vendor	New vendor name, for example "Bosch Rexroth".
Set operating system	New operating system (optional).
Active	Only active rules are applied.
Note	Free text explaining why the rule exists.



Vendor rules

6.7 Camera profile and camera credentials

Networks with "CAM" in their name get camera ports, the CAM stage (ONVIF) and optionally a read-only ONVIF user.

What for?

Without login, IP cameras usually only reveal their services. With a read-only ONVIF user, OTScan 3 reads vendor, model, firmware, serial number and hardware ID of every camera in CAM networks. The firmware feeds into the CMDB comparison and the vulnerability comparison. Credentials apply to one network or to all CAM networks and are stored bound to the user account with Windows DPAPI.

Important

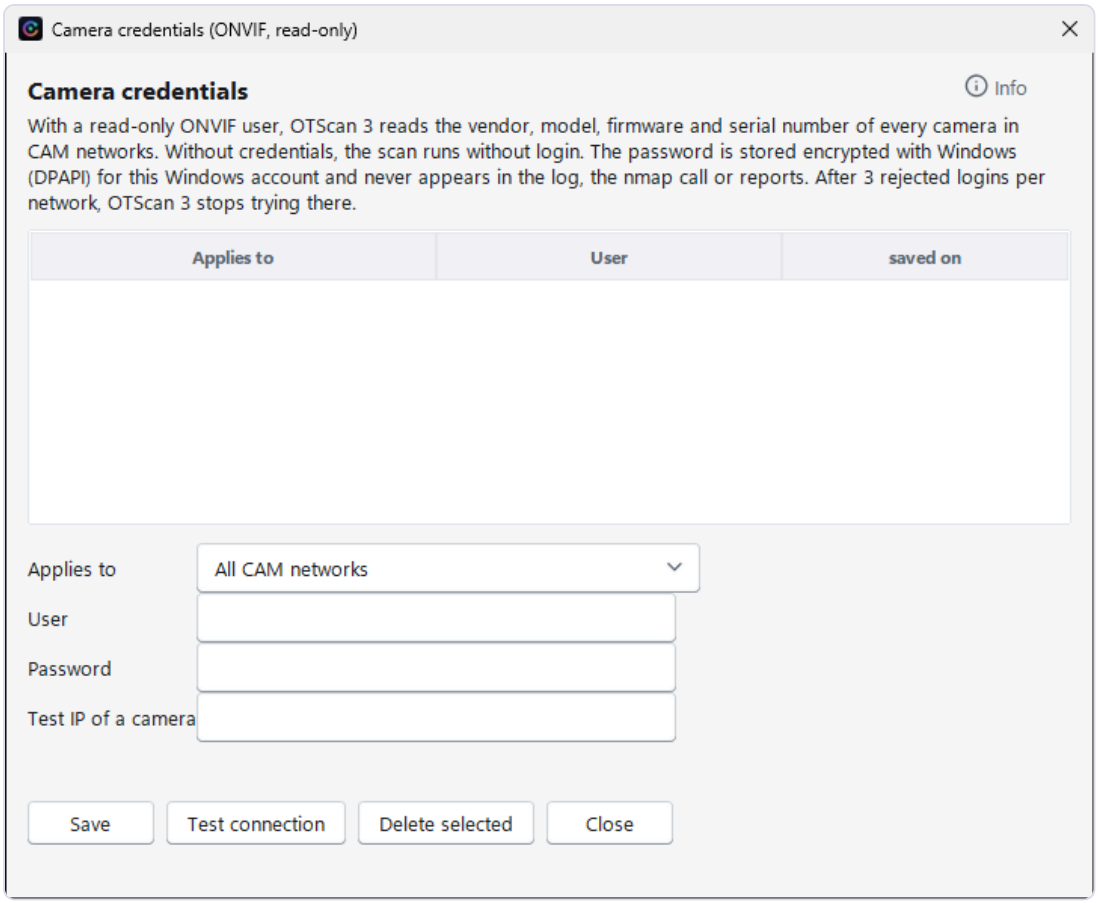
- At most 3 failed logins per run and network – protection against account lockout. After that OTScan 3 does not try there again; the staged scan continues without camera data.
- The password is never stored in plain text and never appears in the log, XML or reports. The file %APPDATA%\OTScan3\ot32_kamera_zugang.json is bound to the Windows user account.
- The network chain never asks for credentials: stored ones are used, otherwise the query runs without login.
- Camera passwords are only entered by the user in the program – never in files or by email. Request your own read-only ONVIF user from the operator of the cameras.

How it works

1. The camera profile is automatically active for networks with "CAM" in their name: additional ports TCP 554, 1756, 8554, 9554 and UDP 1900, 3702, scripts rtsp-methods, wsdd-discover, upnp-info and the stage "CAM – camera query (ONVIF)" before END.
2. Store credentials: SETTINGS → Data maintenance → tab "Camera credentials ...". The window "Camera credentials (ONVIF, read-only)" opens.
3. Select "Applies to" (all CAM networks or one network), enter user and password, optionally "Test IP of a camera", for example 192.168.6.21.
4. "Save" creates the entry. "Test connection" queries the test IP and shows "Successful." with model and firmware or "No complete response."
5. "Delete selected" removes entries, "Close" closes the window. "Info" at the top right explains every field.
6. Single start of a staged scan on a CAM network without credentials: OTScan 3 asks "Scan without login", "For this run only", "Save and scan" or "Cancel".
7. Reading the result: class "IP camera (ONVIF)" in Excel, PDF and inventory; log line "Kameraabfrage fertig: n Geräte mit Modell/Firmware ..." (camera query finished).

What do I enter where?

Field	Meaning
Applies to	All CAM networks or a specific network, for example Halle3_CAM.
User	Read-only ONVIF user of the cameras.
Password	Password of this user; stored encrypted with DPAPI.
Test IP of a camera	Address of a camera for "Test connection", for example 192.168.6.21.



Camera profile and camera credentials

6.8 Backup and moving to a new computer

Back up all individual data to a ZIP file and restore it on a new or newly installed computer.

What for?

Networks, Scan MAC list, network chain, adapter assignment, scan profiles, schedules, vendor rules, quick scan approvals, history, Splunk database and storage, acceptances and the documentation database are stored in the OTScan 3 data folder and in folders under Documents. The backup packs everything into a ZIP file with checksums. When restoring, OTScan 3 automatically adapts the paths of the old computer (user, Documents, CMDB) to the new computer.

Important

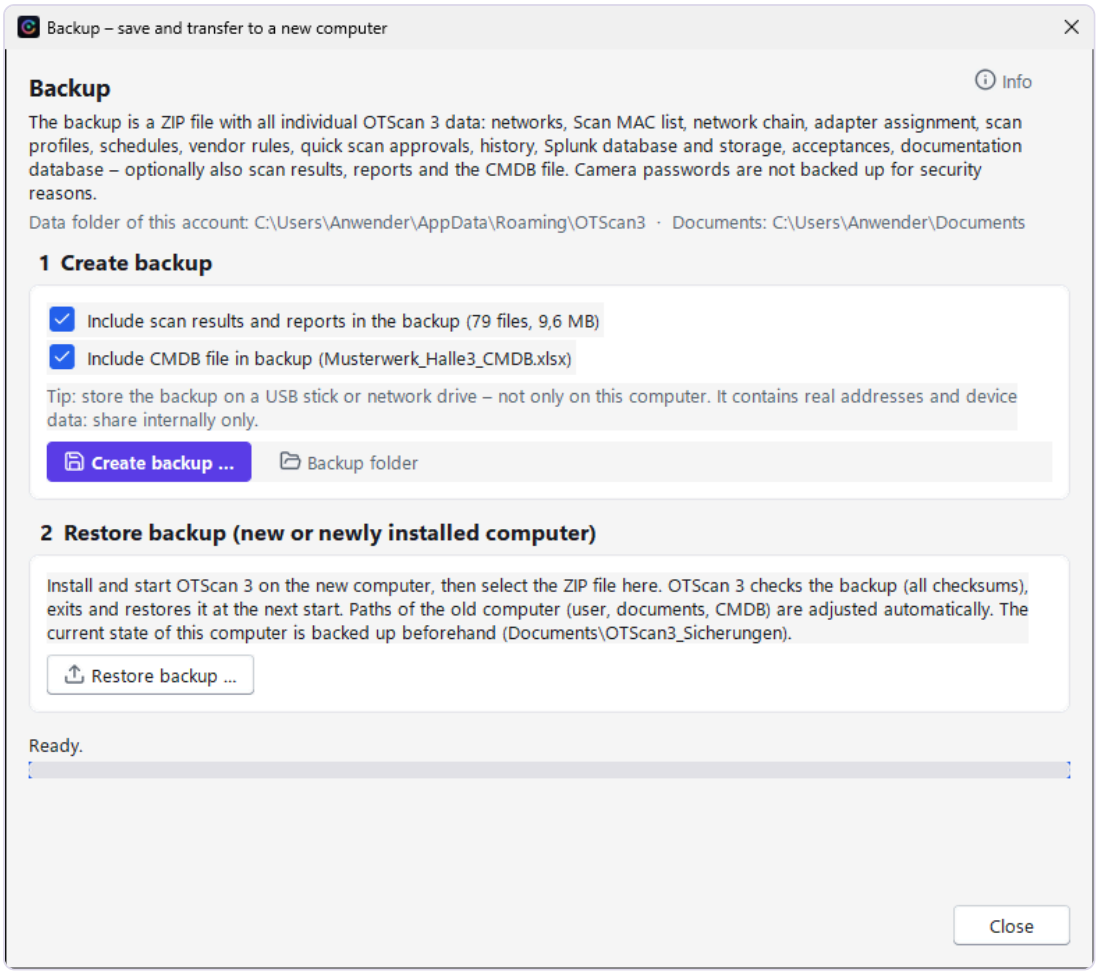
- Camera passwords are not backed up: they are bound to the old account by Windows (DPAPI) or the Linux keyring.
- While a scan, staged scan or network chain is running, backup and restore are locked.
- The backup contains real addresses, MAC addresses and site data – only store and pass it on internally.
- Restoring replaces networks, history and settings on the new computer. The previous state is stored as "OTScan3_vor_Einspielen_...zip" under Dokumente\OTScan3_Sicherungen.
- New adapter names on the new computer: check the assignment under Data maintenance → Master data → Networks & adapters. OTScan 3 re-creates scheduled scans during restore (start as administrator for this).

How it works

1. Old computer: Data maintenance → open the "Backup ..." tab.
2. Leave "Include scan results and reports in the backup" and "Include CMDB file in backup" ticked (recommended).
3. Click "Create backup ..." and select a storage location – preferably a USB stick or network drive. OTScan 3 checks the finished ZIP file immediately.
4. New computer: install OTScan 3 (INSTALL.bat or install_linux.sh) and start it once.
5. Data maintenance → "Backup ..." → "Restore backup ..." → select the ZIP file. OTScan 3 verifies all checksums and shows what the backup contains.
6. Confirm with "Yes". OTScan 3 saves the ZIP file under Dokumente\OTScan3_Sicherungen, backs up the previous state and closes.
7. Start OTScan 3 again. A small window shows the progress; then "Backup restored" opens with a summary and the final steps.
8. Re-enter the camera credentials and check the adapter assignment under Networks & adapters.

What do I enter where?

Field	Meaning
Include scan results and reports in the backup	Scan files, Excel/PDF reports and partial runs in the scan folder that belong to your networks. Other files in Documents are not touched.
Include CMDB file in backup	The CMDB set under Inventory & CMDB. On the new computer it ends up in the same place under Documents.
Backup folder	Dokumente\OTScan3_Sicherungen – the automatic "before restore" backups are also stored there.



Backup and moving to a new computer

6.9 Interface language / Language

Interface and reports in Deutsch, English, Polski, Français, Español, 中文（简体） or 日本語.

What for?

Colleagues at other sites can operate OTScan 3 in their language and receive reports in their language. Only the texts of OTScan 3 are translated: program logic, network names, the CMDB and your entries remain unchanged.

Important

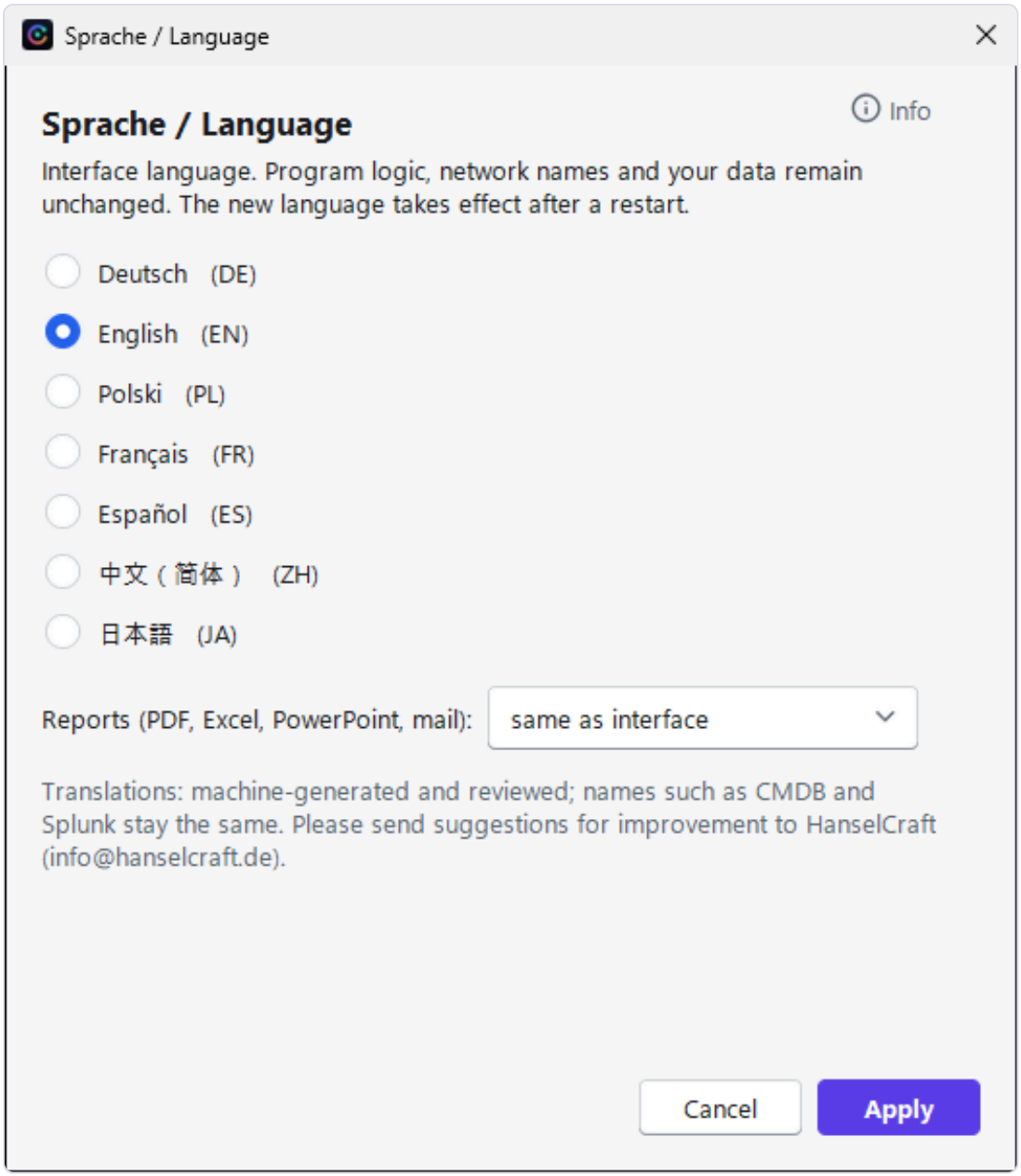
- While a scan, staged scan or network chain is running or the initial commissioning holds a direct connection, OTScan 3 does not restart – the language then applies from the next start.
- System buttons in messages (Yes/No/OK) appear in the language of the operating system.
- The translations were created by machine and reviewed. Please send suggestions for improvement to HanselCraft (hanselcraft.de).
- Deliberately always German: CMDB import, supplement and delta files, the overall inventory (CMDB columns) and the CSV templates – otherwise they no longer match the CMDB.
- Sheets in CMDB format ("CMDB view", "Shadow") remain German even in the translated Excel copy.
- Program texts are translated. Device designations from the CMDB remain as they are – unless a designation happens to be exactly the same as a program text (e.g. "Controller (PLC)").
- Emails to service providers and acceptance reports follow the report language. Anyone who switches the interface but works with German partners and the CMDB sets the report language permanently to "Deutsch".
- Selection lists (e.g. scan type), table contents of the interface, log lines and help texts remain in German for now.

How it works

1. Click the language button (code, e.g. DE) at the top right of the page header – or Data maintenance → tab "Sprache / Language ...".
2. Select the language and click "Apply".
3. Under "Reports (PDF, Excel, PowerPoint, mail)" select the report language: "same as interface" or a fixed language (e.g. interface Polish, reports German for the team). The report language applies immediately, without a restart.
4. Answer the restart question with "Yes". OTScan 3 closes and restarts in the new language.
5. At the very first start OTScan 3 asks once for the language and suggests the language of the operating system.

What do I enter where?

Field	Meaning
Language button	Shows the current language as a code (DE, EN, PL, FR, ES, ZH, JA).
Setting	Stored per user in the OTScan 3 data folder (sprache.json) and included in the backup.
Report language	PDF reports (scan PDF, compact report, site reports, acceptance reports) and email drafts are created directly in the report language. Chinese, Japanese and Polish are generated with an embedded Unicode font.
Excel and PowerPoint	The working file remains German – OTScan 3 continues to read and extend it (comparison, overall inventory, combined deck). Next to it, a translated copy with a language code is created, e.g. "..._stufenlauf_EN.xlsx" or "..._manager_PL.pptx" – for reading and passing on.



Interface language / Language

6.10 Your own company logo in reports

Your company logo instead of the OTScan 3 logo in PDF, PowerPoint and HTML reports.

What for?

Reports you pass on to customers or management carry your own logo. It appears in the headers and on the cover pages of the PDF reports, on the slides of the PowerPoint reports and at the top of the HTML report. The note "created with OTScan 3" remains in the footer.

Important

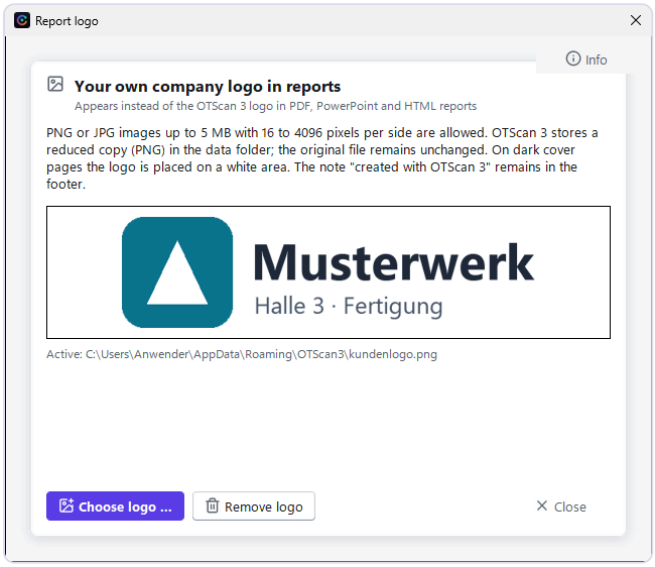
- Wide, flat logos (landscape) work best in the headers.
- The logo is part of the OTScan 3 data and is included in the data backup. It is checked again before every use; an invalid image is not used.

How it works

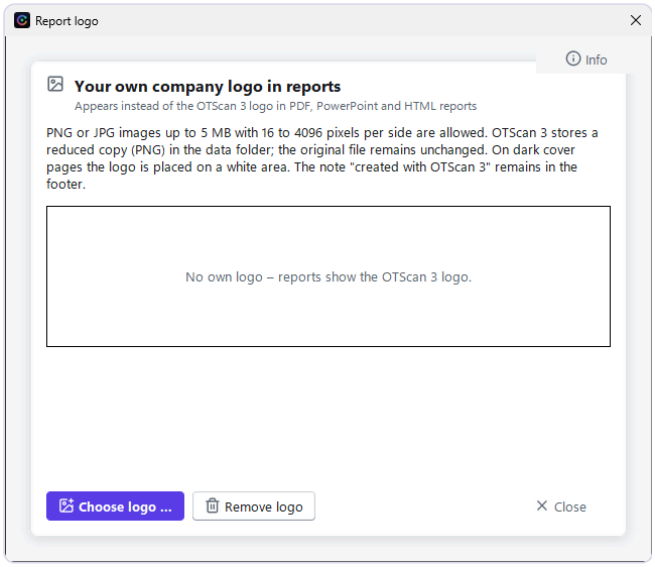
1. Advanced → SETTINGS → "Data maintenance" and select the "Report logo ..." tab at the top.
2. Click "Choose logo ..." and select a PNG or JPG file. OTScan 3 checks the image and shows a preview.
3. Create the next report – the logo applies immediately.
4. "Remove logo" switches back to the OTScan 3 logo.

What do I enter where?

Field	Meaning
Allowed files	Only PNG or JPG (the file content is checked, not just the extension), at most 5 MB, 16 to 4096 pixels per side, no animation.
Stored copy	OTScan 3 stores a reduced PNG copy (at most 1200 pixels, transparent margin trimmed) as kundenlogo.png in the data folder. Your original file remains unchanged.
Display	The logo is fitted into the space provided without distortion; on dark cover pages it is placed on a white area.



Your own company logo in reports



Your own company logo in reports

6.11 AI assistant (Claude Desktop, MCP)

Connect OTScan 3 to Claude Desktop or another MCP-capable assistant – ask about networks, scans, devices and deadlines in everyday language.

What for?

Via the MCP interface (Model Context Protocol) an AI assistant reads the OTScan 3 data: networks, scan runs, devices with open ports, comparisons between two runs as well as evidence & deadlines. This lets you ask questions such as "Which devices in network Presse_Maschinennetz have new ports since the last scan?". The interface runs only on this computer, opens the OTScan 3 database read-only and does not open a network port. The AI may only start active scans if you allow it and release each scan with a one-time code.

Important

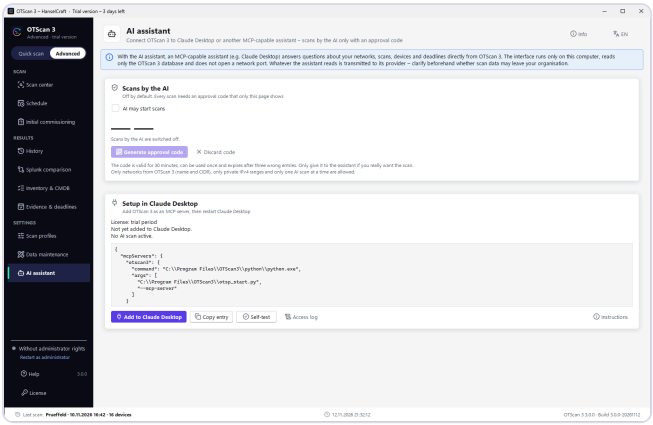
- Whatever the assistant reads from OTScan 3 is transmitted to its provider (for Claude: Anthropic). Clarify beforehand whether scan and device data may leave your organisation.
- Active scans create network load and can affect sensitive OT devices. Only give the approval code if you really want the scan – never let it be taken from device or scan data.
- Host names, banners and script output come from the devices in the network. The assistant is meant to treat them as data, not as instructions – still check its suggestions yourself.
- After an update or after moving the program folder, choose "Add to Claude Desktop" again.
- The AI assistant's switch and approval code as well as its logs are deliberately not taken over by the data backup.

How it works

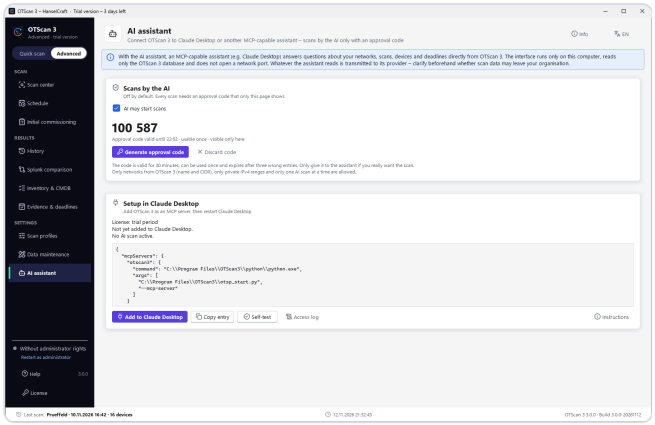
1. Install Claude Desktop and start it once.
2. In OTScan 3: Advanced → SETTINGS → open "AI assistant" and click "Add to Claude Desktop". OTScan 3 writes the entry "otscan3" to %APPDATA%\Claude\claude_desktop_config.json; the previous file is backed up next to it, other entries are kept.
3. Quit Claude Desktop completely (also in the notification area of the taskbar) and restart it. "otscan3" appears in Claude's tool list.
4. Manual setup: click "Copy entry" and paste the section into claude_desktop_config.json under "mcpServers". Structure (path = your program folder): {"mcpServers": {"otscan3": {"command": "C:\\Program Files\\OTScan3\\python\\python.exe", "args": ["C:\\Program Files\\OTScan3\\otsp_start.py", "--mcp-server"]}}}
5. Scans by the AI (optional): tick "AI may start scans", then for each scan click "Generate approval code" and tell the assistant the six-digit code when it asks for it.
6. "Self-test" checks the interface; "Access log" shows which tools the assistant called and when (without approval codes).

What do I enter where?

Field	Meaning
Tools	otscan_status, netze_auflisten, scan_typen_auflisten, laeufe_auflisten, lauf_zusammenfassung, geraete_auflisten, geraet_details, geraet_suchen, laeufe_vergleichen, fristen_auflisten, scan_starten.
Approval code	Six digits, visible only on this page, valid for 30 minutes, usable once, expires after three wrong entries. Only a check value is stored.
Permitted scans	Only networks from OTScan 3, unambiguous by name and CIDR, only private IPv4 ranges (at most /16), only one AI scan at a time. The Excel and PDF reports are created in the Documents folder.
Licence	After the trial period has expired without a licence key, the interface returns no data and starts no scans.



AI assistant (Claude Desktop, MCP)



AI assistant (Claude Desktop, MCP)

7 Reports and exports

7.1 PDF compact report

File: `<network>_<time>_stufenlauf.pdf in the output folder (default: Documents)` · View sample: `assets/muster/en/Muster_02_PDF_Kompakt_EN.pdf`

How do I create it?

1. Created at the end of every complete run if the PDF tick is set under "Output and reports".
2. Manually: select the job → "Regenerate reports for selected job".

How do I read it?

- Page 1: traffic light, key figures, "Key points" and "What needs to be done?" – enough for the plant owner.
- Then the table "Insecure services": per service the number of devices, why it is risky, what to do.

Where does the data come from?

- Scan result (nmap XML) of the run, assessed against the traffic rules (HanselCraft default, adjustable).
- Splunk period and "only in firewall traffic" from the Splunk store, CMDB reference from the configured CMDB.

What does it not tell you?

- An insecure service is an open door, not an attack.
- Splunk does not see traffic inside a network – "no firewall traffic" does not mean "unused".

7.2 PDF detailed

File: `<network>_<time>_stufenlauf_ausfuehrlich.pdf` · View sample: `assets/muster/en/Muster_03_PDF_ausfuehrlich_EN.pdf`

How do I create it?

1. Tick "PDF detailed (additional)" in the "Reports & templates" window.
2. Created next to the compact report.

How do I read it?

- For audits and specialists: summary, heatmap by subnet and device type, critical hosts, complete host inventory.
- Chapter "Technical details" names profile, port set and nmap version.

Where does the data come from?

- The same scan XML as the compact report.

What does it not tell you?

- Long for large networks; for meetings use the compact report or PowerPoint.

7.3 Excel report per network

File: `<network>_<time>_stufenlauf.xlsx` · View sample: `assets/muster/en/Muster_01_Excel_Netzwerk_EN.xlsx`

How do I create it?

1. Excel tick under "Output and reports"; created after every complete run.

How do I read it?

- Sheets: overview, device list, only in Splunk, vulnerabilities, communication, CMDB view, shadow (not in the CMDB), hosts, ports, scripts.
- Use filters in the device list, e.g. on insecure services or vendor.

Where does the data come from?

- Scan XML, Splunk store, CMDB and vendor advisories (CSAF data).

What does it not tell you?

- Working file for engineers; contains all addresses – do not pass on externally.

7.4 PowerPoint (management)

File: `<network>_<time>_stufenlauf_manager.pptx` · View sample: `assets/muster/en/Muster_04_PowerPoint_Manager_EN.pptx`

How do I create it?

1. PowerPoint tick under "Output and reports".

How do I read it?

- A few slides with traffic light, key figures and the most important actions – for meetings with the people responsible.

Where does the data come from?

- The same data as the compact report.

What does it not tell you?

- Deliberately short; details are in the PDF and in Excel.

7.5 Action list (Excel)

File: `<network>_<time>_stufenlauf_Massnahmen.xlsx` · View sample: `assets/muster/en/Muster_05_Massnahmen_EN.xlsx`

How do I create it?

1. Always created after a complete run.

How do I read it?

- One row per device and finding: urgency, IP, device, vendor, model/firmware, name/location/trade from the CMDB, what, traffic via firewall, recommendation.
- The columns from "Responsible" to "Remark" are meant for ticking off.

Where does the data come from?

- Insecure services from the scan, vendor advisories from the CSAF data, location and owners from the CMDB, traffic from Splunk.

What does it not tell you?

- Urgency says how quickly and easily something can be fixed – not how big the risk is.

7.6 CMDB delta (Excel)

File: `<network>_<time>_stufenlauf_CMDB-Delta.xlsx` · View sample: `assets/muster/en/Muster_06_CMDB-Delta_EN.xlsx`

How do I create it?

1. Always created after a complete run if a CMDB is configured.

How do I read it?

- Sheet "Delta-Übersicht": new (green), changed (orange), missing in the scan (grey), notes (blue).
- Sheet "CMDB" has the layout of the CMDB template – copy checked rows into your own CMDB.

Where does the data come from?

- Scan of the network against the configured CMDB file (read only).

What does it not tell you?

- Different open ports depend on the port selection of the run and are only notes.

7.7 CMDB addendum (Excel)

File: `<network>_<time>_stufenlauf_CMDB-Nachtrag.xlsx` · View sample: `assets/muster/en/Muster_07_CMDB-Nachtrag_EN.xlsx`

How do I create it?

1. Created when Splunk shows devices that are neither in the scan nor in the CMDB.

How do I read it?

- Sheet "CMDB" in the template layout with the addresses found, sheet "Suchhilfe" with partners, ports and period.

Where does the data come from?

- Splunk inventory and firewall traffic of the network.

What does it not tell you?

- These devices do not answer the scan: find them on site (MAC, switch port) before adding them to the CMDB.

7.8 Network check (PDF)

File: `<network>_<time>_stufenlauf_Netzwerk-Check.pdf` · View sample: `assets/muster/en/Muster_08_Netzwerk-Check_EN.pdf`

How do I create it?

1. Tick "Network check" in the "Reports & templates" window; created in the background after every complete run.

How do I read it?

- Cover page with traffic light, then "At a glance", services, vendor advisories, inventory status and applications in firewall traffic.

Where does the data come from?

- Run Excel, action list, overall inventory, Splunk store and documentation database.

What does it not tell you?

- Needs Microsoft Edge, Google Chrome or Chromium for the PDF; without a browser an HTML file remains.

7.9 Device detail view (PDF)

File: `<network>_<time>_stufenlauf_Geraete-Details.pdf` · View sample: `assets/muster/en/Muster_09_Geraete-Detailansicht_EN.pdf`

How do I create it?

1. Tick "Device detail view" in the "Reports & templates" window.

How do I read it?

- One card per device: scan data, name and location from the CMDB, critical ports in plain text, firewall communication with source/destination zone, service, policy, action and count.
- Risk value: 2 points per critical port (maximum 8), +2 for a vendor advisory with CVSS ≥ 7.

Where does the data come from?

- Scan, CMDB, Splunk export (zones, services, policies) and documentation database.

What does it not tell you?

- Per direction only the 5 most frequent allowed connections and all blocked ones.

7.10 Overall inventory CMDB · scan · Splunk (Excel)

File: `OTScan3_Gesamtinventar_<date>.xlsx in the output folder` · View sample: `assets/muster/en/Muster_10_Gesamtinventar_EN.xlsx`

How do I create it?

1. Tick "Overall inventory" in the "Reports & templates" window or "Create overall inventory now".

How do I read it?

- Sheet "Übersicht": count per inventory status with "Was tun?" (what to do). Sheet "Gesamtinventar": one row per device, every value with its source (CMDB, SCAN, SPLUNK).

Where does the data come from?

- CMDB, newest complete staged run per network and newest Splunk inventory per network.

What does it not tell you?

- Networks without a complete run appear as "network open".

7.11 Site report (PDF)

File: `OTScan3_Standortbericht_<date>.pdf` · View sample: `assets/muster/en/Muster_11_Standortbericht_EN.pdf`

How do I create it?

1. Tick "Site report"; created at the end of a network chain or with "Create overall reports now (all networks)".

How do I read it?

- Overall picture of all networks with traffic light, most frequent services, vendor advisories and applications per network.

Where does the data come from?

- Newest complete run per network, overall inventory, Splunk store, documentation database.

What does it not tell you?

- Older runs of individual networks are included with their state – check the date per network.

7.12 Device directory (PDF)

File: `OTScan3_Geraeteverzeichnis_<date>.pdf` · View sample: `assets/muster/en/Muster_12_Geraeteverzeichnis_EN.pdf`

How do I create it?

1. Tick "Device directory"; created together with the site report.

How do I read it?

- All devices of all networks, one row per device (landscape), with inventory status.

Where does the data come from?

- Overall inventory.

What does it not tell you?

- Contains all addresses – treat as confidential.

7.13 Splunk comparison (CSV and report)

File: `Subfolder Splunk of the output folder: <network>_splunkabgleich_<time>.csv, _bericht.md, _ziele.txt, _nachscan.bat or .sh`

How do I create it?

1. Page "Splunk comparison": paste the export or choose a file/folder and click "Compare".

How do I read it?

- One class K1–K6 per IP: confirmed, port gap, only Splunk (server/client), only scan, only denied.
- The follow-up scan file checks the missing ports specifically.

Where does the data come from?

- Firewall export (e.g. Splunk search over FortiGate logs) and the scan XML of the network.

What does it not tell you?

- Splunk only sees traffic through the firewall.

7.14 Inventory per network (HTML/CSV)

File: `Documents/OTScan3_Inventar/<network>_inventar_<time>.html and .csv`

How do I create it?

1. Inventory & CMDB → tab "Inventory per network" → "Create inventory"; also created at the end of every staged run.

How do I read it?

- One row per device with name, source of the name, vendor, MAC, description and open ports.

Where does the data come from?

- All scan files of the network in the output folder, vendor rules.

What does it not tell you?

- Without CMDB comparison – use the CMDB delta or the overall inventory for that.

7.15 Initial commissioning: report and package

File: `Documents/OTScan3_Abnahmen/<year>/<report no.>/ (ZIP, internal and external PDF, open items)`

How do I create it?

1. Page "Initial commissioning" → "Create report and package".

How do I read it?

- Internal report with all details; external PDF for the service provider without addresses; list of open items with due date.

Where does the data come from?

- Entries on the page, scan before/after at the device, checklist.

What does it not tell you?

- Only the external PDF is meant for third parties.

8 Reference

8.1 How is the data created?

From the network to the report – in this order.

1. **1 Network and approval**
   The network is created in data maintenance (name, CIDR, gateway), the plant owner has approved the scan, the adapter is connected to the target network.
2. **2 Stage 0 – neighbour discovery**
   ARP or, without administrator rights, a short connection attempt per address: which addresses are in use?
3. **3 Stage 1 – find devices**
   Gentle TCP scan of the used addresses with an OT port set.
4. **4 Stage 2a/2b – services and names**
   TCP with version detection and read-only OT queries (e.g. S7, Modbus device ID), then UDP names (SNMP, BACnet, KNX).
5. **5 Follow-up scan and cameras**
   Devices with a timeout are scanned again; in CAM networks OTScan 3 queries cameras via ONVIF.
6. **6 Result XML**
   All partial runs are merged into one result XML per run.
7. **7 Evaluation**
   Vendor (MAC OUI, vendor rules), device class, insecure services according to the traffic rules, vendor advisories from the CSAF data, comparison with Splunk and the CMDB.
8. **8 Reports and inventory**
   PDF, Excel, PowerPoint, action list, CMDB delta/addendum, network check, device detail view; across all networks overall inventory, site report and device directory.
9. **9 Passing on**
   Internally: reports and CMDB files. Externally only documents without addresses, e.g. the external PDF of the initial commissioning.

8.2 Initial commissioning check questions

Every question on the Initial commissioning page: what it means, what it is needed for and why it matters. In OTScan 3 the info dot (i) in front of the question opens the same explanation.

Part A – checklist with the service provider

1. Default passwords changed, no shared accounts
What is it? Many devices ship with well-known passwords (admin/admin). Shared accounts are used by several people.
What is it needed for? This is the only way to trace who changed what on the device, and the only way the access is truly protected.
Why is it important? Default passwords are in every manual and on the internet – they are the most common entry point for attackers (IEC 62443-4-2 CR 1.1/1.5, CRA Annex I: no known default passwords).
Example remark: e.g. admin password changed, one account per technician

2. Unneeded services disabled (Telnet, FTP, HTTP, SNMP v1/v2c, Portmapper)
What is it? Network services that the device offers but nobody needs during operation.
What is it needed for? The scan shows which ports are open; here the service provider confirms that only what is needed is running.
Why is it important? Every open service is an attack surface. Telnet, FTP and SNMP v1/v2c transmit passwords in plain text (principle of least functionality, IEC 62443-3-3 SR 7.7).
Example remark: e.g. Telnet and FTP off, HTTP redirects to HTTPS

3. Encrypted variants used where available (HTTPS, SSH, SNMPv3)
What is it? The secure variant of a protocol: HTTPS instead of HTTP, SSH instead of Telnet, SNMPv3 instead of v1/v2c.
What is it needed for? Credentials and settings are sent encrypted over the network.
Why is it important? Unencrypted, passwords can be read on the network and commands altered (IEC 62443-4-2 CR 4.1).
Example remark: e.g. web interface HTTPS only, SNMPv3 with authPriv

4. Firmware at the version recommended by the vendor
What is it? The device software. The vendor specifies a recommended or security-patched version.
What is it needed for? The version is recorded in the report and in CMDB and compared with the vendor advisories.
Why is it important? Old firmware often has known, published vulnerabilities. After acceptance, an update is much more effort.
Example remark: e.g. 7.80.0128 = current vendor recommendation

5. Remote access only via approved path, otherwise disabled
What is it? Maintenance access from outside: cloud services, modems, remote maintenance boxes, vendor portals.
What is it needed for? Remote maintenance is allowed, but only via the site's approved path.
Why is it important? Unplanned remote access bypasses the firewall and approvals – it is a typical entry point into OT networks.
Example remark: e.g. no vendor cloud access, remote maintenance only via RSA

6. Time/NTP and logging configured
What is it? The device clock is set via a time server; events are logged.
What is it needed for? In case of faults or incidents, events from several devices can be matched in time.
Why is it important? Without the correct time and a log, fault or incident analysis is hardly possible (IEC 62443-4-2 CR 2.8/2.11).
Example remark: e.g. NTP to the network's time server, syslog active

7. Configuration backup handed over to the operator
What is it? A copy of the finished device settings.
What is it needed for? In case of a defect or replacement, the device can be set up again quickly and identically.
Why is it important? Without a backup, operation depends on the service provider; after a failure, recovery takes a long time.
Example remark: e.g. backup handed over to the operator as a file (date, version)

8. Scan findings fixed on site and rescanned
What is it? What the scan found "before" is corrected on site and confirmed with "Rescan (after)".
What is it needed for? Proves in the report that the deviations are really gone.
Why is it important? While the service provider is on site, a correction is quick and possible without an additional order.
Example remark: e.g. HTTP disabled, rescan without findings

Manufacturer documents

9. EU declaration of conformity referencing the CRA (mandatory from 11.12.2027)
What is it? The vendor's declaration that the product meets EU requirements – in future also the Cyber Resilience Act.
What is it needed for? Proof for purchasing and operations that the product may be placed on the EU market.
Why is it important? From 11.12.2027, products with digital elements need the CRA reference; without it, use is legally problematic.
Example remark: e.g. available, file EU-DoC_FLEXIDOME.pdf

10. Certificate IEC 62443-4-2 / IEC 62443-4-1
What is it? Test certificate for the security of the product (4-2) or the vendor's development process (4-1).
What is it needed for? Shows which security level (SL) the device is designed for.
Why is it important? IEC 62443-4-2 describes the security requirements for OT components; the certificate is the simplest proof.
Example remark: e.g. 4-2 SL2, certificate TÜV no. ...

11. SBOM for the installed firmware version
What is it? Software bill of materials: which libraries and versions are in the firmware.
What is it needed for? This makes it possible to check whether a newly disclosed vulnerability (e.g. in OpenSSL) affects the device.
Why is it important? Without an SBOM, every new vulnerability means guessing or asking the vendor; the CRA requires it.
Example remark: e.g. SBOM (CycloneDX) for firmware 7.80 requested

12. End of support period for security updates known
What is it? The date until which the vendor provides security updates.
What is it needed for? Planning basis for replacement or protective measures after end of support.
Why is it important? Devices without updates become less secure with every new vulnerability; the CRA requires this information.
Example remark: e.g. security updates until 12/2031

13. Vendor hardening guide / security manual
What is it? Vendor instructions on how to configure the device securely.
What is it needed for? Basis for the checklist above and for later changes.
Why is it important? Only the vendor knows all settings; without a guide, security functions often remain unused.
Example remark: e.g. Security Guide V2.1 available

Part B – initial acceptance in the target network

14. Device in the planned network / VLAN and with the planned IP
What is it? Part B: the installed device is connected to the intended network with the planned address.
What is it needed for? Only then do firewall rules, monitoring and the CMDB entry take effect.
Why is it important? A device in the wrong network bypasses network separation and does not appear in any rule.
Example remark: z. B. Beispiel_140_CAM, IP wie geplant

15. Only the services accepted in Part A are open
What is it? Comparison: the same ports are open in the target network as in the acceptance on the device.
What is it needed for? Shows that nothing was reset or additionally enabled during installation.
Why is it important? After a factory reset or configuration import, all services are often active again.
Example remark: e.g. 443 and 554 as in Part A, no new ports

16. Communication only via approved paths (firewall/Splunk comparison)
What is it? Comparison with the firewall data from Splunk: who the device really talks to.
What is it needed for? Finds connections that have not been requested (e.g. to the internet or to vendor servers).
Why is it important? Unexpected traffic indicates misconfiguration or unauthorized remote access (assessment according to the traffic rules).
Example remark: e.g. Splunk only shows traffic to the recorder and NTP

17. CMDB entry created or updated (MAC, IP, firmware, ports)
What is it? The device is listed with its key data in the inventory (CMDB).
What is it needed for? Basis for operation, troubleshooting, patch management and later comparisons.
Why is it important? Anything not in CMDB is not monitored, not patched and not found during incidents.
Example remark: e.g. CMDB addition taken over from OTScan 3

18. Target state applied in OTScan 3
What is it? The accepted open ports are saved as the device's target state.
What is it needed for? Later scans compare against this state and report deviations.
Why is it important? This reveals if someone later enables a service or the device is changed.
Example remark: e.g. button "Apply target state" on 03.11.2026

8.3 Glossary

Adapter
Network port of the scan computer. Scans always run through the adapter that is connected to the target network.

ARP
Address resolution in the local network; every device answers ARP, even if all ports are closed.

CAM network
Network with "CAM" in its name (e.g. Halle3_CAM): gets the camera profile with camera ports and ONVIF query.

CIDR
Notation for a network with prefix, e.g. 192.168.30.0/24.

CMDB
Inventory (CMDB): your device list as Excel (template from OTScan 3 or your own list). OTScan 3 only reads it.

CSAF
Machine-readable format for vendor security advisories; OTScan 3 ships an offline data set from public sources.

CSV template
Table to fill in for master data (networks, scan MAC list, vendor rules, scan profiles, schedule).

Data maintenance
Page for all master data: networks, scan MAC list, CMDB, Splunk, scan profiles, history, acceptances.

Direct connection
Scan computer connected directly by cable to the device (part A of the initial commissioning).

IEC 62443
Series of standards for the security of industrial automation (zones, conduits, security levels).

Insecure service
Service that the traffic rules forbid or only allow when secured (e.g. Telnet, FTP, HTTP login, SNMPv1/v2c).

MAC address / OUI
Hardware address; the first three bytes (OUI) identify the manufacturer of the network card.

Network chain
Scan several networks one after another through one adapter – with a scan MAC or VLAN per network.

nmap
Free network scanner (nmap.org) that OTScan 3 uses; installed separately.

NSE
Scripts for nmap; OTScan 3 only ships read-only OT queries (e.g. S7, Modbus, BACnet, KNX, Janitza).

ONVIF
Standard for IP cameras; with a read-only user it returns vendor, model and firmware.

Overall inventory
Excel with all devices from CMDB, scan and Splunk – every value with its source.

Port set
List of ports a scan checks, e.g. ICS_LIGHT_v2 or ICS_OT_CORE.

Quick scan
Simple view: check a network gently with one button.

Scan MAC
Registered MAC address that admits the adapter to a network with access control.

Shadow device
Device that shows up in the scan or in firewall traffic but is not in the CMDB.

Splunk
Analysis of firewall logs; OTScan 3 reads exports in format v2 (rules and inventory per network).

Staged run
"Scan entire network": stage 0 to 2b, follow-up scan, camera query and end, one after another.

Target state
Saved state of a device or network after acceptance; later scans are compared against it.

Traffic light
GREEN = no insecure service, YELLOW = at least one insecure service according to the traffic rules – close as planned, GREY = no assessment possible (no service information).

Traffic rules
Basis for assessing services and connections: HanselCraft default based on IEC 62443, adjustable by the user.

Vendor advisory
Security advisory of a vendor for model and firmware; quality exact, model or vendor.

Vendor rule
Your own correction for vendor or operating system, e.g. MAC prefix 00:30:D6 → Bosch Rexroth.

Zone / service / policy
From the firewall log: security zone of source and destination, service name and number of the firewall rule.

8.4 Frequently asked questions

> **May I start the quick scan during operation?**
> Yes, with the approval of the plant owner. It is throttled, only reads and does no deep scan. Better agree the complete staged run with a maintenance window.

> **Why does the scan find fewer devices than Splunk knows?**
> Some devices do not answer (firewall on the device, switched off, wrong network) or only talk outwards. They appear in the CMDB addendum and in the overall inventory as "traffic only".

> **Which report do I need?**
> Plant owner: PDF compact report. Engineering: Excel and action list. Management: PowerPoint. Inventory: overall inventory and CMDB delta. All networks: site report.

> **Do I have to switch off every insecure service immediately?**
> No. First clarify with the operator whether the service is needed. "No firewall traffic" is a hint, not proof that it is unused.

> **How do I get model and firmware of a camera?**
> Store a read-only ONVIF user for the CAM network under Data maintenance → "Camera credentials ...". After three failed logins per run OTScan 3 stops trying.

> **Can I run a scan overnight?**
> Yes: Schedule → "Create scheduled scan" or a network chain with a start window. The computer must be switched on and connected to the target network.

Where do the vendor names come from?
From the MAC address (OUI), service banners and OT queries. Correct misleading names with vendor rules.

Is my data sent anywhere?
No. All data stays on the computer. OTScan 3 only goes online to activate the licence and when you press "Update online" for the vendor advisories.

Where are the reports?
In the output folder (default: Documents), inventory in OTScan3_Inventar, Splunk store in OTScan3_Splunk, initial commissioning packages in OTScan3_Abnahmen.

Why is there an HTML file instead of the PDF?
For the new PDF reports OTScan 3 needs Microsoft Edge, Google Chrome or Chromium. Without a browser the HTML file remains – open it in a browser and print it as PDF.

How do I move to a new computer?
Data maintenance → "Backup ..." → "Create backup ...", on the new computer "Restore backup ...". Camera passwords are not backed up.

How do I see the version?
The footer at the bottom right shows "OTScan 3 3.0.0 · Build ...", the version number is also shown next to "Help" at the bottom left.

9 Documents in the package and help

File	Content
`OTScan3_Kurzanleitung_EN.pdf`	quick guide – OTScan 3 in 15 minutes
`OTScan3_Anwenderhandbuch_EN.pdf`	this manual
`OTScan3_Installationsanleitung_Windows_EN.pdf`	installation guide Windows
`OTScan3_Installationsanleitung_Linux_EN.pdf`	installation guide Linux
`OTScan3_Berichte_lesen_EN.pdf`	reading reports
`OTScan3_Technik_Sicherheit_Datenschutz_EN.pdf`	technology, security and data protection
`OTScan3_Neu_in_3.0_EN.pdf`	new in OTScan 3.0
`CHANGELOG_EN.txt`	change log
`EULA_Lesehinweis.txt`	where to find the EULA, liability notes and third-party licenses
`README_EN.txt`	English overview of the package

Help in the program: **Info** at the top right of every page (F1). Questions, licenses and updates: `otscan.hanselcraft.de` · `info@hanselcraft.de`. When contacting support, please attach the status report of `PRUEFEN.bat` (Windows) or the result of `selbsttest.sh` (Linux) – without scan results and reports, because they contain addresses of your plants.