QUICK GUIDE

OTScan 3 in 15 minutes

First start, user interface, quick scan and staged run, results, reports and master data – the essentials on a few pages.

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

1 What OTScan 3 does

OTScan 3 checks operational technology (OT) networks: it finds the devices, detects vendor, model, firmware and open services, and assesses which services are insecure. On request it compares the results with firewall traffic (e.g. from Splunk) and with your inventory (CMDB), and it creates reports for plant owners, engineers and management.

> 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.

2 First start

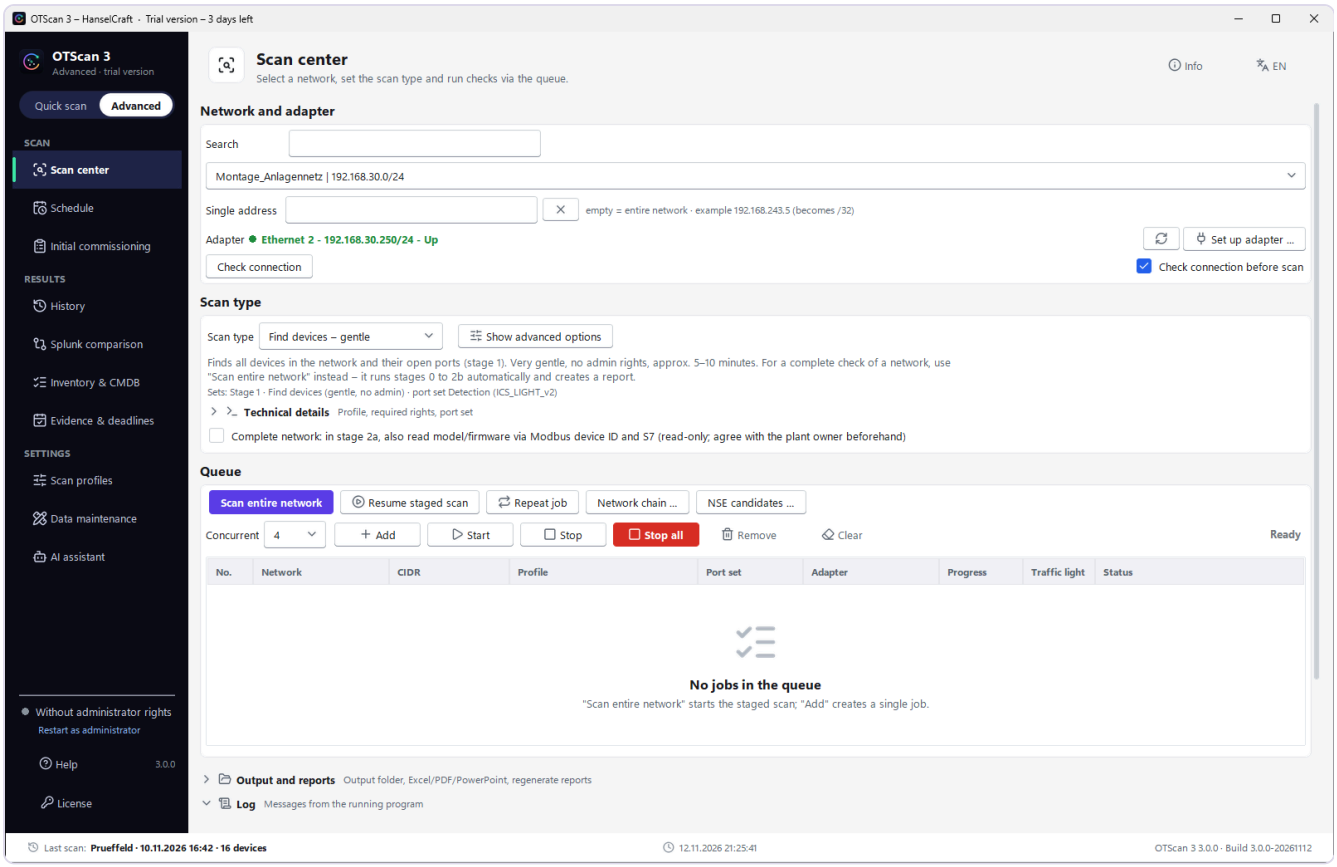
1. Start OTScan 3 from the desktop icon or the start menu entry **OTScan 3** (Linux: `/opt/otscan3/otscan3.sh`).
2. At the first start OTScan 3 asks for the language and shows the window **Activate OTScan 3**. Enter the licence key and click **Activate** – or **Later** for the trial version.
3. The **setup wizard** asks what you need: *Minimal – quick scan*, *Standard*, *Complete (OT security)* or *Detect automatically*. Then enter networks, optionally choose a CMDB and click **Finish**.

3 The user interface

At the top left you switch between **Quick scan** (one button, for everyone) and **Advanced**. The Advanced sidebar has three areas:

Area	Pages	Purpose
SCAN	Scan center · Schedule · Initial commissioning	Check networks, plan runs, accept new devices
RESULTS	History · Splunk comparison · Inventory & CMDB	Review runs, compare with firewall traffic and inventory
SETTINGS	Scan profiles · Data maintenance	Profiles, networks, scan MAC list, CMDB, vendor rules

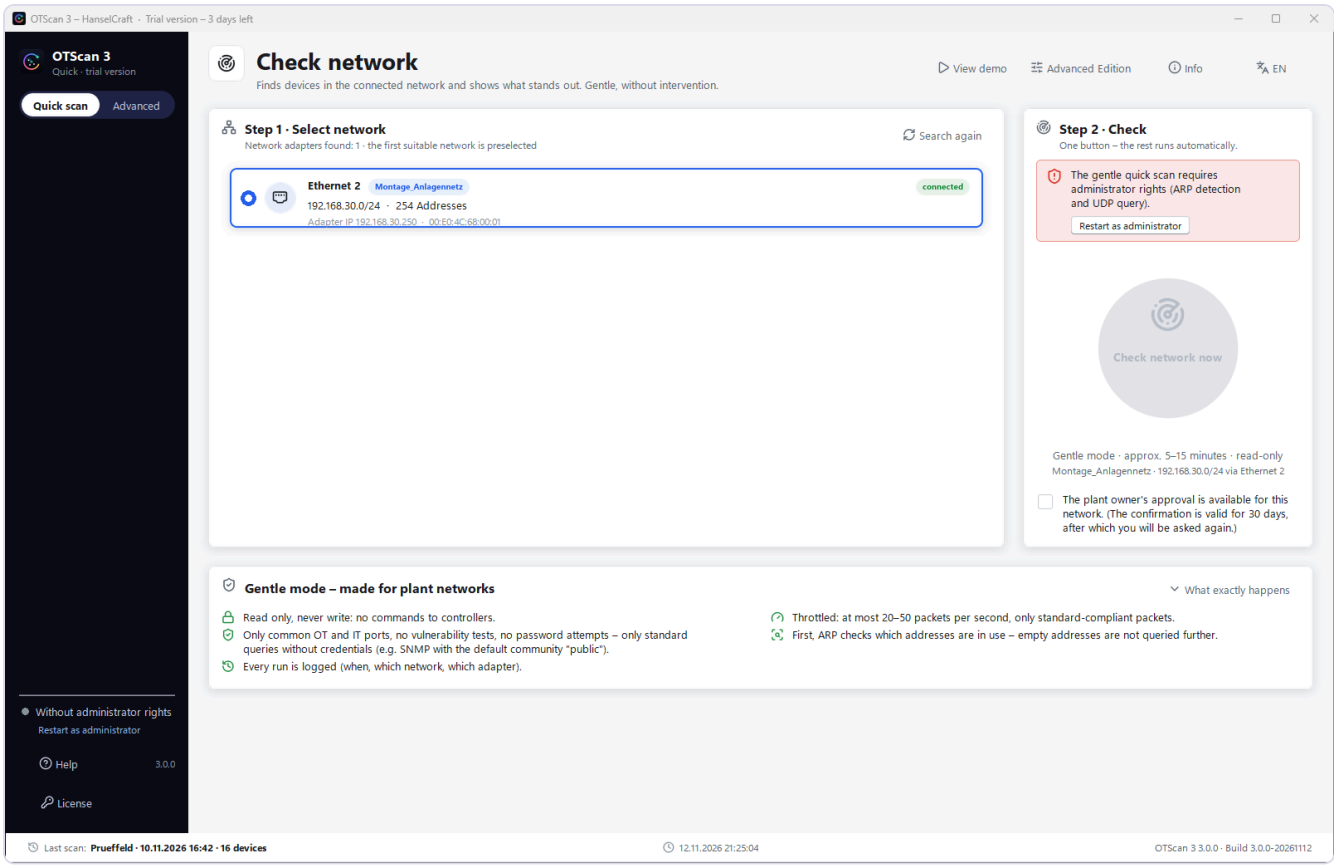
At the top right of every page: **Info** (step-by-step help, also F1) and the language button. At the bottom left: administrator rights, **Help** and **License**; the footer shows the last scan and the version.



Advanced → Scan center

4 Quick check of a network (Quick scan)

1. Choose **Quick scan** at the top left.
2. Select the network (the adapter must be connected to the target network) and confirm the approval.
3. Start the scan. After a few minutes the traffic light and the result appear; the buttons open PDF, Excel and short report.



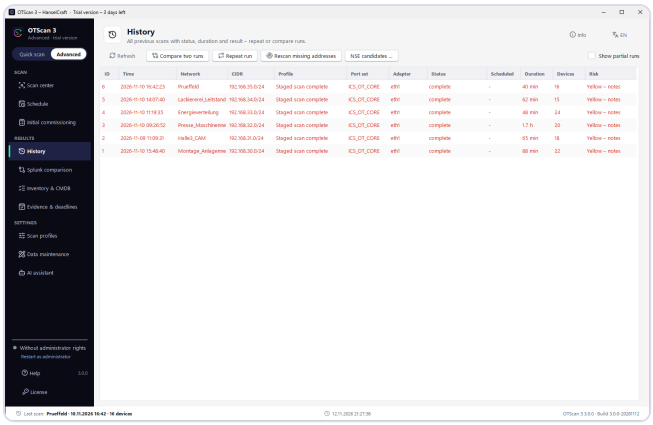
Quick scan

5 Complete check of a network (staged run)

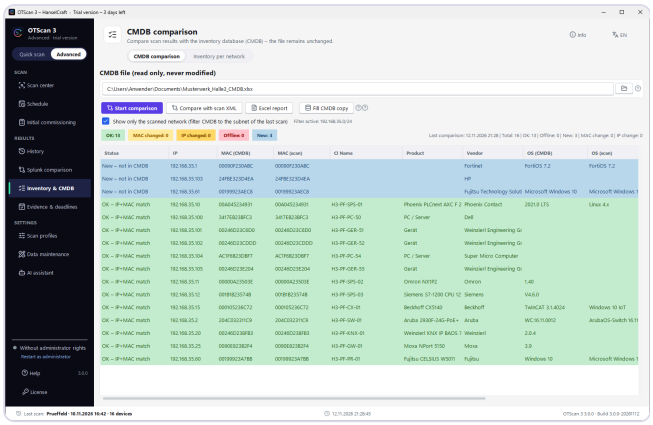
1. Advanced → SCAN → **Scan center**. Under "Network and adapter" search for and select the network.
2. Check the adapter (green = ready). If necessary use **Set up adapter …** – fixed scan IP without default gateway, optionally with scan MAC.
3. Click **Scan entire network** and confirm the prompt (network, stages, estimated duration).
4. The stages run one after another: stage 0 (who is there?), stage 1 (devices and ports), stage 2a (services and versions), stage 2b (UDP names), follow-up scan and, in CAM networks, the camera query. **Stop** pauses, **Resume staged scan** continues.
5. At the end the reports are created in the output folder (default: Documents).

6 Results

- **History**: all runs with status, duration, devices and traffic light; **Compare two runs**, **Repeat run**.
- **Splunk comparison**: import the firewall export with **Import export …**, then click **Compare** per network. Devices that only appear in traffic go into the CMDB addendum.
- **Inventory & CMDB**: choose the CMDB file, click **Start comparison**. Green = matches, red = not in the scan, blue = new.



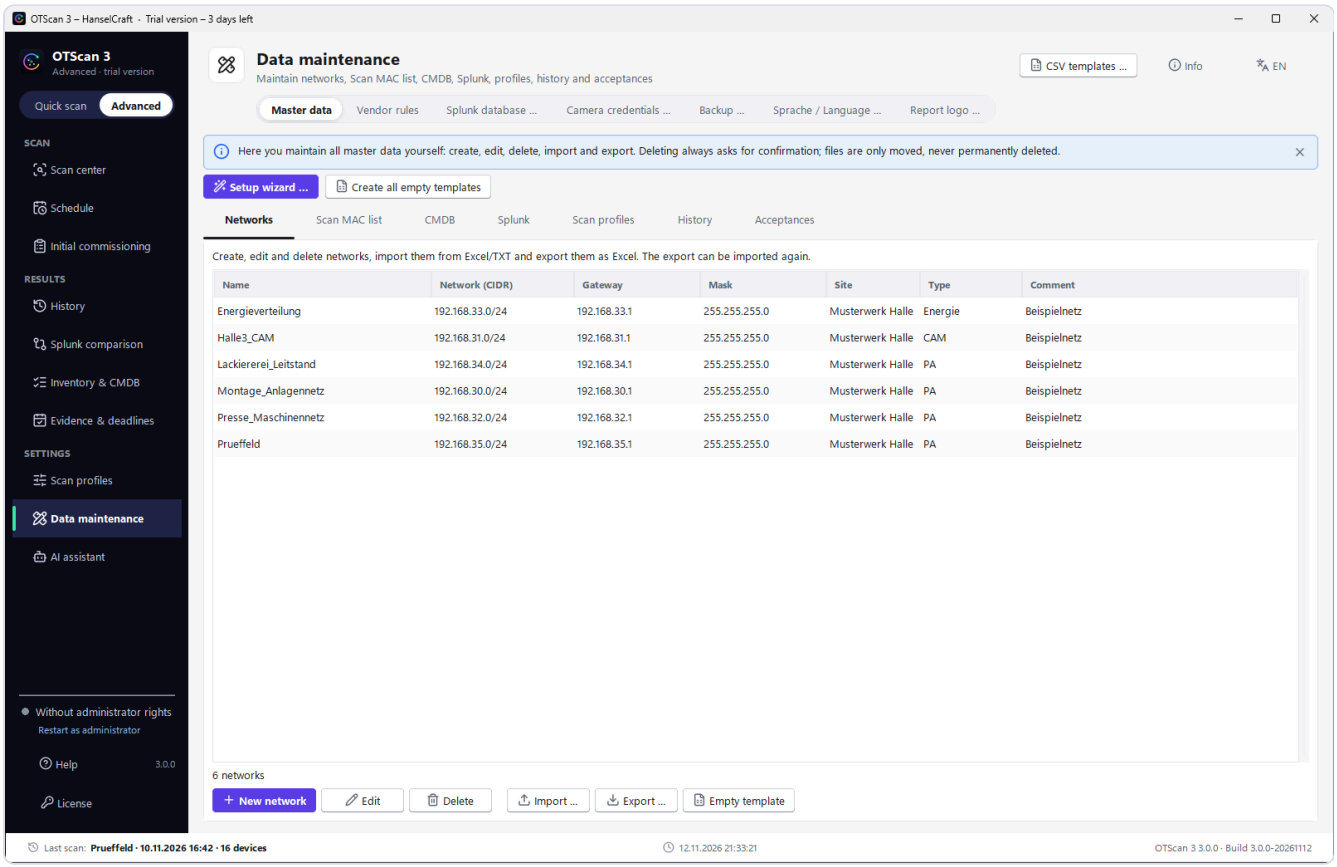
History



CMDB comparison

7 Reports and master data

Under "Output and reports" in the scan center set the ticks for Excel, PDF and PowerPoint. **Reports & templates ...** lists every report type with a tick and **View sample**. Master data lives in **Data maintenance**; for many entries at once use **CSV templates ...**.



Data maintenance → Master data → Networks

8 If something does not work

Message / observation	What to do
Adapter red or yellow	Cable in the target network? Scan MAC registered? Use **Set up adapter ...**.
Stage paused "needs administrator rights"	Start OTScan 3 from the desktop icon (with administrator rights) and click **Resume staged scan**.
"nmap blocked"	The message names the reason. Info → topic "Security with administrator rights".
HTML instead of PDF	Install Microsoft Edge, Google Chrome or Chromium for the new PDF reports.

More help: **Info** on every page (F1) and the user manual in the program folder (`handbuch/index_en.html`).