NETVANE

User Guide

The complete guide to NetVane

Document version 1.0

A doorvane project

NetVane v1.3.1 · August 27, 2026

See your network the way an outsider would.

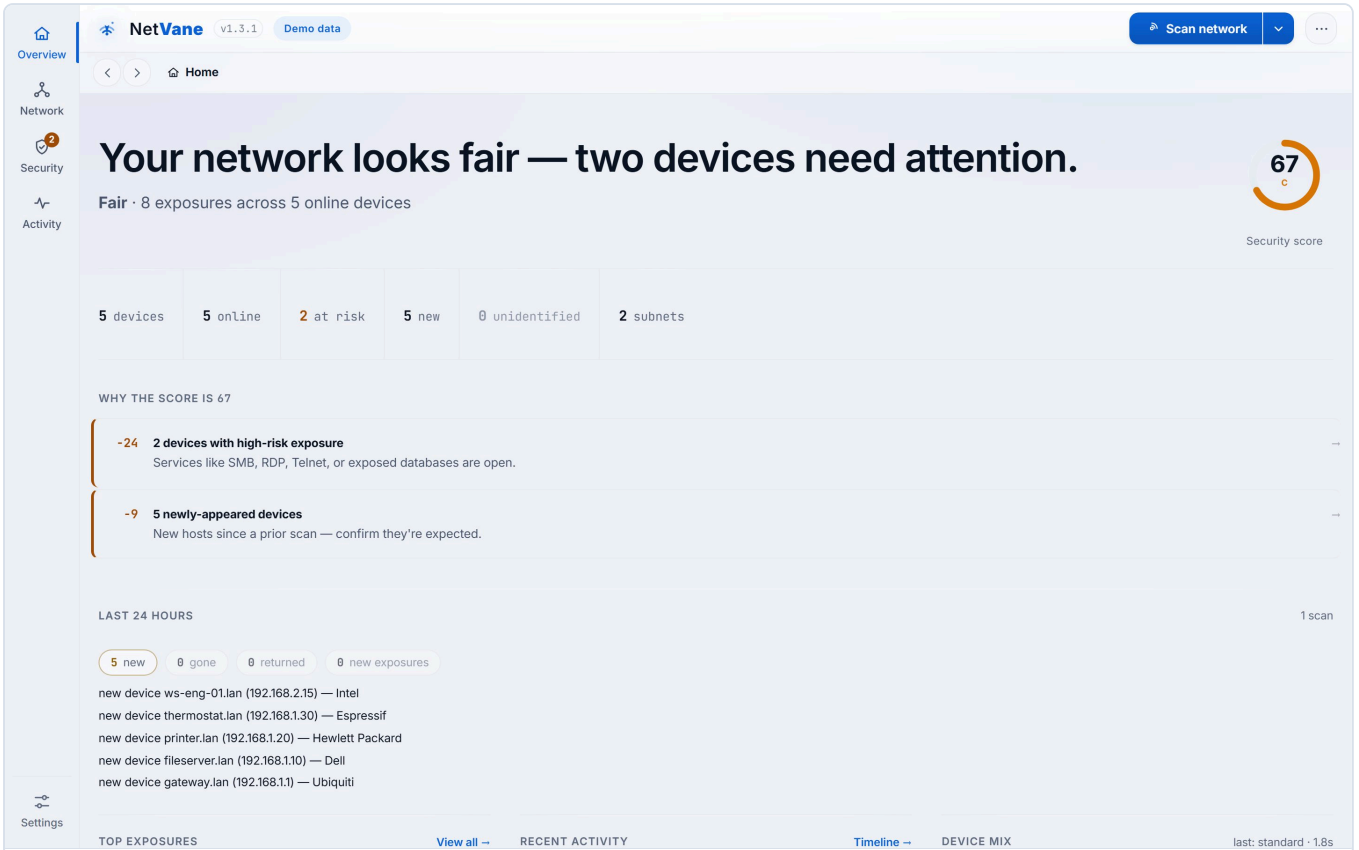
Contents

1. Introduction

NetVane shows you what is actually on your network — and what an outsider could reach — without anything about your network leaving your machine unless you ask it to.

Most people have no clear picture of their own network. Devices come and go: a new phone, a smart plug, a work laptop, a guest's tablet, a printer someone plugged in months ago. Each of those devices may be listening on the network — exposing services such as file shares, remote desktop, cameras, or databases — and there is rarely any single place to see all of it at once. The result is a quiet, growing blind spot: you cannot protect what you cannot see.

NetVane closes that gap. It is a **local, private network scanner and security monitor**. You run it on your own machine, it discovers the devices on your network, examines which services each one exposes, and presents everything in a clear dashboard in your browser at `http://127.0.0.1:8787`. It gives every network a transparent security score, explains exactly why the score is what it is, and shows you — in plain language — how to fix the things that matter.



The NetVane Overview. One screen summarising the whole network — score and grade, device counts, top exposures, recent activity, and device-type mix (demo data).

1.1 The problem NetVane solves

Home and small-office networks have quietly become as complex as small business networks used to be, but without any of the tooling. NetVane answers the questions that otherwise go unanswered: What is on my network right now? Which of these devices is exposing something risky, like remote desktop or an

unauthenticated database? Did a new device just appear that I do not recognise? Has anything changed since last week? And most importantly: what should I actually do about it?

1.2 Local-first and private by design

NetVane is not a cloud service and it is not SaaS. There is no account to create, no data about your network uploaded, and no telemetry — and nothing about your network ever leaves your machine. Nothing NetVane scans or monitors leaves your machine on its own. The only traffic that ever goes out is traffic you asked for: optional, integrity-checked update checks for the app, the CVE database, the device-fingerprint table and the network-owner data (none of which send anything about your network); a change-alert webhook, if you configure one; a support report, if you choose to send one; and the two internet-quality tools — the speed test and the DNS benchmark — which by their nature contact public internet services when you run them. NetVane loads no web fonts or external scripts. Everything runs on your computer, and all results are stored in a single local database file. The dashboard is served from your own machine to your own browser. If your machine is offline, NetVane still works. This is a deliberate design choice: a tool that inventories your network and its weaknesses should never be a tool that leaks that same information. Privacy is covered in full in section 12.

1.3 What NetVane is not

NetVane is primarily a **reachability** scanner: it tells you which services are reachable on which devices and helps you judge whether they should be. It also matches the service versions it detects against a **bundled, offline CVE database** (NVD + CISA-KEV) to flag likely-affected devices — but it is not a live or authenticated vulnerability scanner. It is **non-destructive toward other devices**: it never exploits a weakness, never writes to a device and never changes anyone's configuration. It does go a step beyond passive watching — to tell a real exposure from a harmless open port it speaks each service's own protocol read-only (see section 5.5, *Active risk validation*) — and it sends no credentials at all unless you deliberately switch on the optional credential check and authorize it for your own network. Section 5 explains this in detail.

1.4 Who this guide is for

This guide is written for anyone who wants a clear view of their own network — home users, hobbyists, and people responsible for a small office or lab. No prior security or networking expertise is assumed. Where a technical term is unavoidable, it is explained. More advanced readers can skim the introductory context and jump straight to the reference sections.

1.5 How to use this guide

If you are new, read sections 1 through 3 in order — they take you from installing NetVane to running your first scan. Section 4 tours the dashboard so you know where everything lives. Sections 5 through 11 explain each capability in depth; treat them as reference. Sections 12 and 13 cover privacy and responsible use, and are worth reading in full. Section 14 collects the common problems and their fixes, and section 15 lists the keyboard shortcuts. Section 16 records the revision history of this document.

1.6 Conventions used in this guide

- Instructions addressed to you use the second person ("open the dashboard", "click **Scan**").
- Things you type or filenames appear in `monospace`, for example `python run.py` or `netvane.db`.
- Keys appear as key caps, for example `Ctrl` `K`.
- Coloured callouts flag information worth pausing on: blue for a helpful note, amber for a caution.
- Figures throughout this guide show the dashboard populated with anonymised demo data, so you can see what each screen looks like before you run your own scan.

> **Keeping this guide current**
> This guide documents NetVane v1.3.1. NetVane updates itself, so if your copy of the app is newer than the version above, download the current guide from netvane.doorvane.com/docs/.

2. Installation

A quick per-user installer for most people, a portable single file for the rest — and never an administrator prompt.

NetVane never needs administrator rights or a separate runtime such as Python or .NET. It is a direct download from `netvane.doorvane.com/download` — no account and no sign-up. There are two builds: the **installer**, `NetVane-Setup-1.3.1.exe` (recommended), and the **portable** single-file build, `NetVane-Portable-1.3.1.exe`. They are about 19 MB and 17 MB respectively, and both are fully self-contained.

2.1 The Windows installer (recommended)

The installer sets NetVane up the way a normal Windows application should be: shortcuts, clean upgrades, and a proper uninstall entry — all per-user, so no administrator or UAC prompt ever appears.

1. Download `NetVane-Setup-1.3.1.exe` from `netvane.doorvane.com/download`.
2. Double-click it and follow the short wizard. The app installs under your own user profile (`%LocalAppData%\Programs\NetVane`) and adds Start-menu and desktop shortcuts. Installing a newer version automatically removes the older one first.
3. Launch **NetVane** from the Start menu.
4. NetVane starts its local server and opens the dashboard at `http://127.0.0.1:8787` in its **own app window** — a clean, chromeless window with no tabs or address bar. It prefers Brave, then Chrome or another Chromium-family browser for this window (Edge only as a last resort); if none is installed, it opens a tab in your default browser instead.
5. Closing the window stops NetVane — unless you have turned on the optional background mode (section 10.4), in which case it keeps running in the system tray.

To remove NetVane later, uninstall it from Windows **Settings** → **Apps** as you would any application.

> **First run: SmartScreen or antivirus may warn you**
> The binary is **signed as GRCSAC**, so Windows names the publisher. A new certificate can still draw a SmartScreen prompt, and antivirus may show a warning the first time you run it — typically "Windows protected your PC". A prompt on a recently issued certificate does not indicate a problem with the file — check that it names GRCSAC. To proceed, click **More info** and then **Run anyway**. NetVane still needs no administrator rights.

2.2 Portable build and running from source

The **portable build**, `NetVane-Portable-1.3.1.exe`, is a single self-contained file: download it, save it anywhere convenient, and double-click it. Nothing is installed and no shortcuts are created; to remove it, delete the file. It behaves identically to the installed app, including opening its own app window.

Running from source is for developers. Note that NetVane targets **Windows only** — the source uses Windows-native APIs, so macOS and Linux are not supported.

1. Ensure you have **Python 3.10 or newer** installed. Python 3.12 is recommended, as it matches the version the release is built and tested against.
2. Obtain the source. (NetVane's source is not currently public — the prebuilt installer and portable builds above are the supported way to run it.)
3. Install the dependencies: `pip install -r requirements.txt`.
4. Start the application: `python run.py`.
5. Open `http://127.0.0.1:8787` in your browser if it does not open automatically.

```
python --version          # confirm 3.10+ (3.12 recommended)
pip install -r requirements.txt
python run.py             # serves the dashboard on http://127.0.0.1:8787
```

2.3 Requirements at a glance

Operating system	Windows 10 or 11, 64-bit. Running from source also targets Windows (it uses Windows-native APIs); macOS and Linux are not supported.
Downloads	`NetVane-Setup-1.3.1.exe` (per-user installer, recommended) or `NetVane-Portable-1.3.1.exe` (single file). Each ~20 MB; no admin, no Python/.NET/drivers.
Browser	Nothing to set up — NetVane opens its own app window (Brave or Chrome preferred; Edge only as a last resort; falls back to a tab in your default browser).
Disk space	~200 MB free (the app plus a small SQLite database that grows slowly over time).
From source	Python 3.10+ (3.12 recommended); `pip install -r requirements.txt`; `python run.py`.
nmap	Optional. Adds OS fingerprinting and richer version detection when you select the nmap engine.
Npcap / WinPcap	Not required.

> **nmap is optional**
> NetVane includes its own built-in scan engine written in pure Python, so it works fully out of the box with nothing else installed. If you want deeper operating-system fingerprinting and more detailed service-version detection, install **nmap** and select the nmap engine in Settings — it is a power-user option, never a requirement, and NetVane never switches to it on its own (section 5.1).

3. Getting started

From a standing start to your first complete picture of the network in a couple of minutes.

Once NetVane is running and its window is open, you are ready to scan. The first time in, a short **guided tour** points out the essentials — the network map, the scan-target box, the Scan button, the view rail, and the **…** overflow menu. Step through it or skip it; you can replay it any time from **…** → **Take the guided tour**. The dashboard opens on **Overview**, which stays quiet until NetVane has looked at your network; over in **Network**, the map starts empty with a "Scan to build your map" prompt. A single scan fills both in.

3.1 Your first scan

1. Open the dashboard (it opens automatically; if you ever need it by hand, it is at `http://127.0.0.1:8787`).
2. Start a scan. You can click the **Scan** control, or simply press `s` anywhere in the dashboard.
3. **Confirm you are authorized.** Before your very first scan, NetVane shows a one-time authorization prompt: tick the box to confirm the network is yours (or that you have explicit permission to examine it) and continue. You are never asked again on this machine.
4. NetVane detects your local network range automatically and begins discovering devices. You do not need to know or type an IP range for a normal home or office network.
5. For your first run, the **Standard** profile is the recommended choice — it balances thoroughness and speed (see section 5). If you simply want to see what is alive as fast as possible, choose **Discovery**.
6. Watch the Map populate live as results arrive. NetVane streams updates as it works, so devices and findings appear progressively rather than all at the end.

3.2 What happens during a scan

A scan proceeds in stages. NetVane first discovers which hosts on your network are alive. For each live host it then checks which ports are open, attempts to identify the service behind each open port, and works out what kind of device it is — router, camera, phone, printer, workstation, and so on — using a combination of the open ports, the hardware vendor (from a bundled offline vendor registry), the hostname, and, if available, the operating system. It reads MAC addresses from your system's ARP table to map devices to vendors, resolves names via reverse DNS, and grabs service banners where offered. As it goes, it calculates your security score and records everything to the local database so you can track changes later.

> **Scans look, they never meddle**
> A NetVane scan finds which services are reachable and gathers what those services volunteer, then confirms whether an exposure is real by talking to the service in its own protocol — read-only. It never exploits anything, never writes to a device and never changes another device's configuration or state, and it sends no credentials unless you have explicitly enabled the optional credential check (section 5.5). Scanning is safe to run against your own network, and section 13 covers when it is appropriate to run it at all.

3.3 Your first results

When the scan finishes, head to the **Overview** view for the summary. This is what you can expect to see: a headline security score and grade, cards counting the devices found, how many are online, how many are at risk, and how many remain unidentified, a feed of what changed in the last 24 hours, the top exposures ranked by severity, and a breakdown of the mix of device types on your network. From here every figure is a click-through into the detail behind it, so the Overview is both a summary and a launchpad. Explore the other views described next.

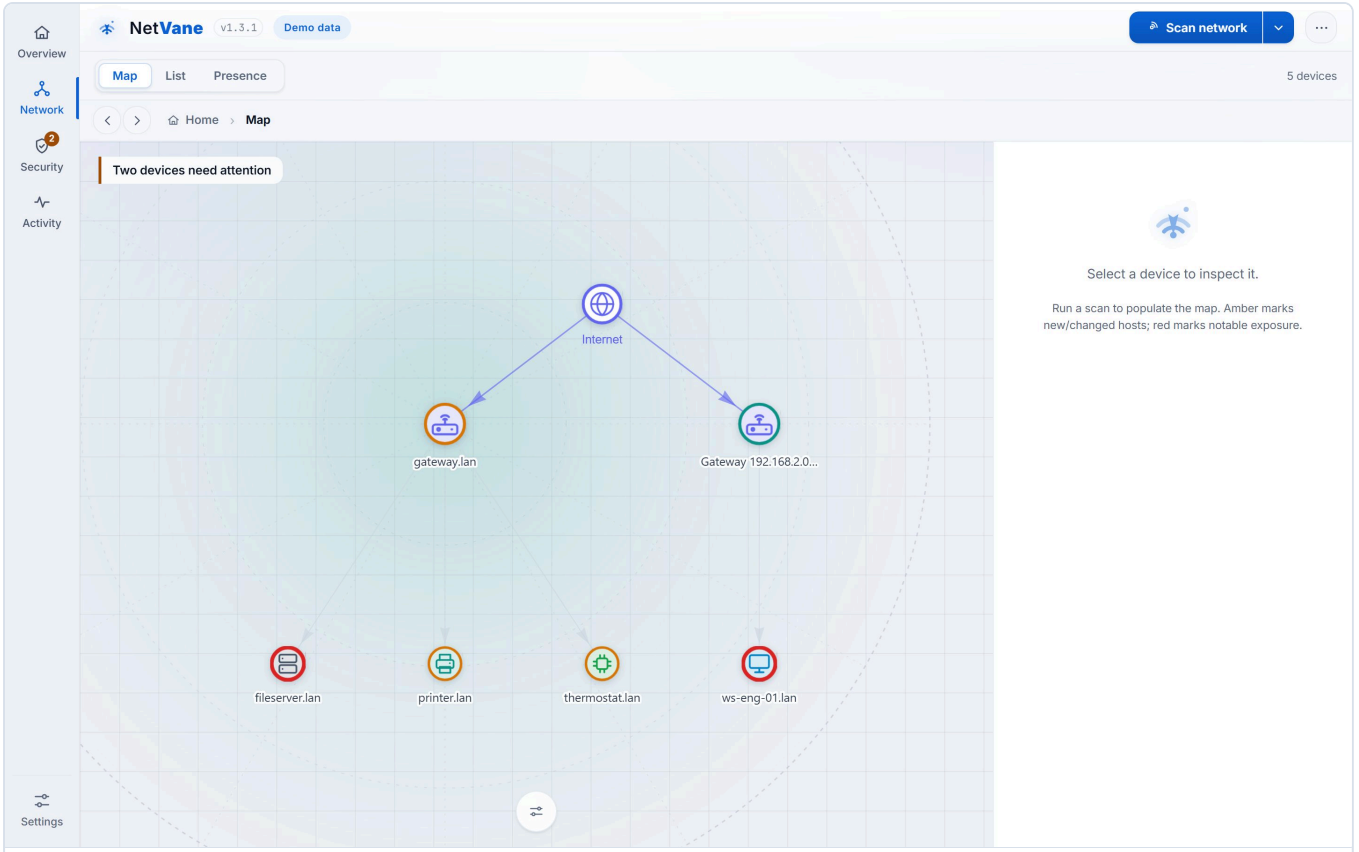
4. The dashboard

Four views, one network, everything a click away.

The dashboard is a single-page application served entirely from your machine. It is organised into four views — **Overview**, **Network**, **Security**, and **Activity** — which you can reach from the navigation rail down the left edge, by pressing the number keys `1` through `4` in that order, or through the command palette (`Ctrl` `K`). **Network** shows your devices three ways, switched with a lens control — an interactive **Map**, a searchable device **List**, and **Presence** ("who's on your network", grouping devices into here-now / recently-seen / away) — and **Activity** combines the **Timeline** of changes with a **Scans & trends** section. Settings keep everyday options up front with an optional **Advanced** mode for power & beta features. Every view uses real URLs, so browser **back** and **forward** work as you would expect, breadcrumbs show where you are, and you can bookmark or share a deep link to a specific device or scan. Nearly every figure and item is a live link: clicking a number on the Overview takes you to the filtered list behind it. A header pill appears when the optional nmap engine is in use, and you can switch between dark and light themes at any time with `t`. IP and MAC addresses are click-to-copy throughout.

4.1 Network — your devices, three ways (Map, List & Presence)

The **Map** is the Network view's default lens (NetVane itself opens on the Overview) — an interactive diagram of your network, rendered with a vendored graph library so nothing is loaded from the internet. Devices are laid out around the network so you can see the shape of things — the gateway, and the devices hanging off it — at a glance. It is the most intuitive way to spot something that does not belong. Before your first scan it shows a simple "Scan to build your map" prompt; after that, click any node to jump to that device's detail, or navigate it entirely from the keyboard (focus the map, then use the arrow keys to pan and `+`/`-` to zoom).



The Map view. Your network as a topology graph — internet to gateway to devices, each node carrying a device-type icon. Click a node to open its detail (demo data).

Placing a device under its switch or access point. A network scan can't see the wiring inside an Ethernet switch, so by default every device is drawn one hop under the gateway. If you know a device is actually connected through a particular switch or access point, open the device and set **"Connected via"** to that switch/AP — the Map redraws the real physical hierarchy (for example, a laptop under its desk switch, under the router). It's a per-device choice that persists; the picker only lists network gear on that device's own subnet, and pick "Directly on the gateway" to clear it. A manual placement like this always wins over anything NetVane guesses on its own.

Two best-effort guesses, always marked as guesses. When exactly one Wi-Fi access point is visible on your network, NetVane guesses that nearby camera and smart-home devices connect to it over Wi-Fi rather than drawing them under the gateway — shown as a dashed line with a note explaining it's a guess, never a confirmed fact, and instantly overridden the moment you set "Connected via" yourself. Separately, on a **Deep scan**, if traceroute data from multiple devices agrees that one of your networks' own gateway sits upstream of another (a double-NAT setup, e.g. an ISP router feeding your own router), the Map nests the second network under the first — again dashed and noted as a guess, not asserted as fact.

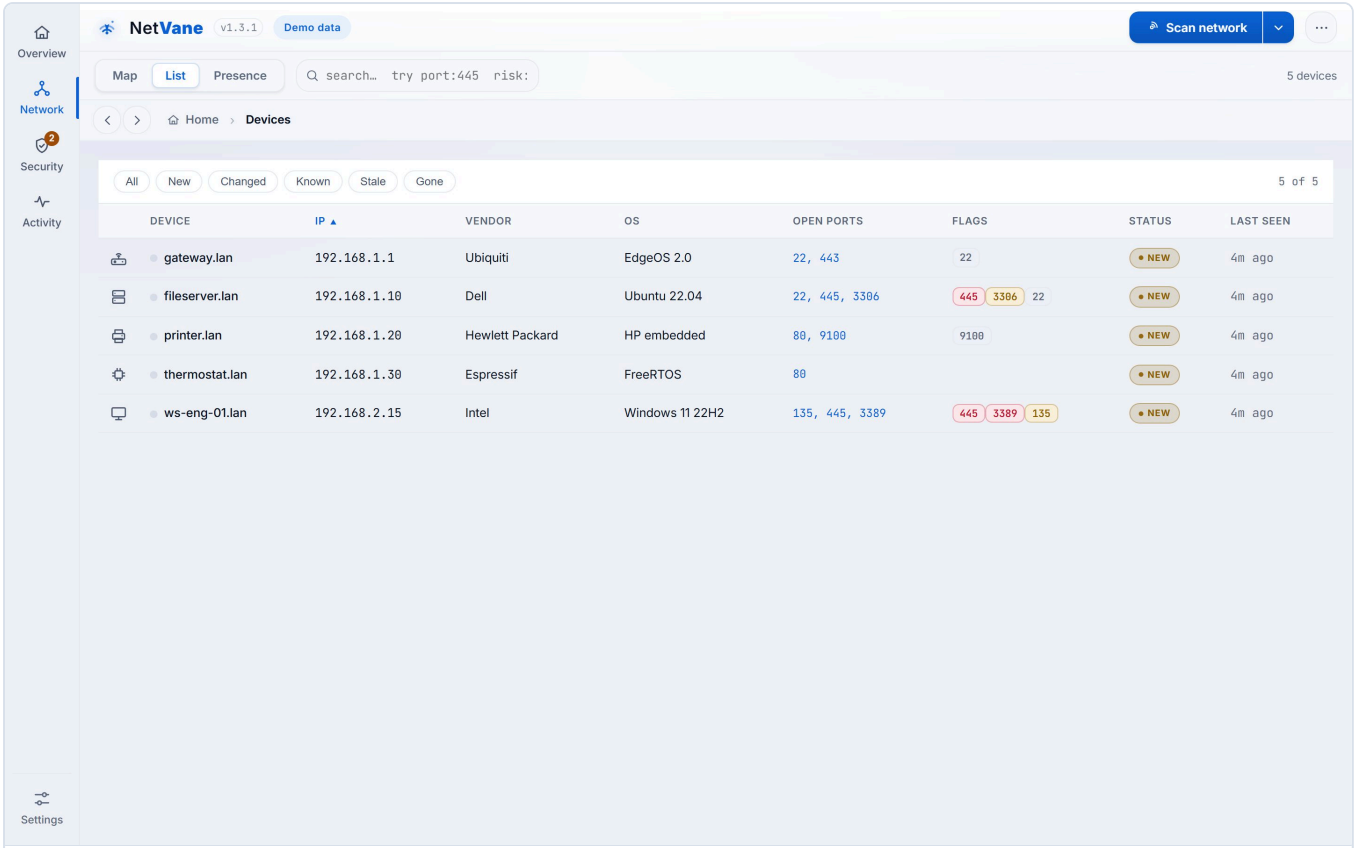
4.2 Overview

The Overview is the summary screen — the whole network's state on one page. It shows your current security score and grade, the number of devices found, how many exposures exist and at what risk level, and what has changed since your last scan. Every figure is a click-through: clicking the device count opens the Devices list, clicking a high-risk figure takes you straight to those exposures, and so on. Open

it after each scan to see at a glance whether anything needs attention — the figure in section 1 shows the KPI cards, activity feed, top exposures, and device-type mix all visible on the one screen.

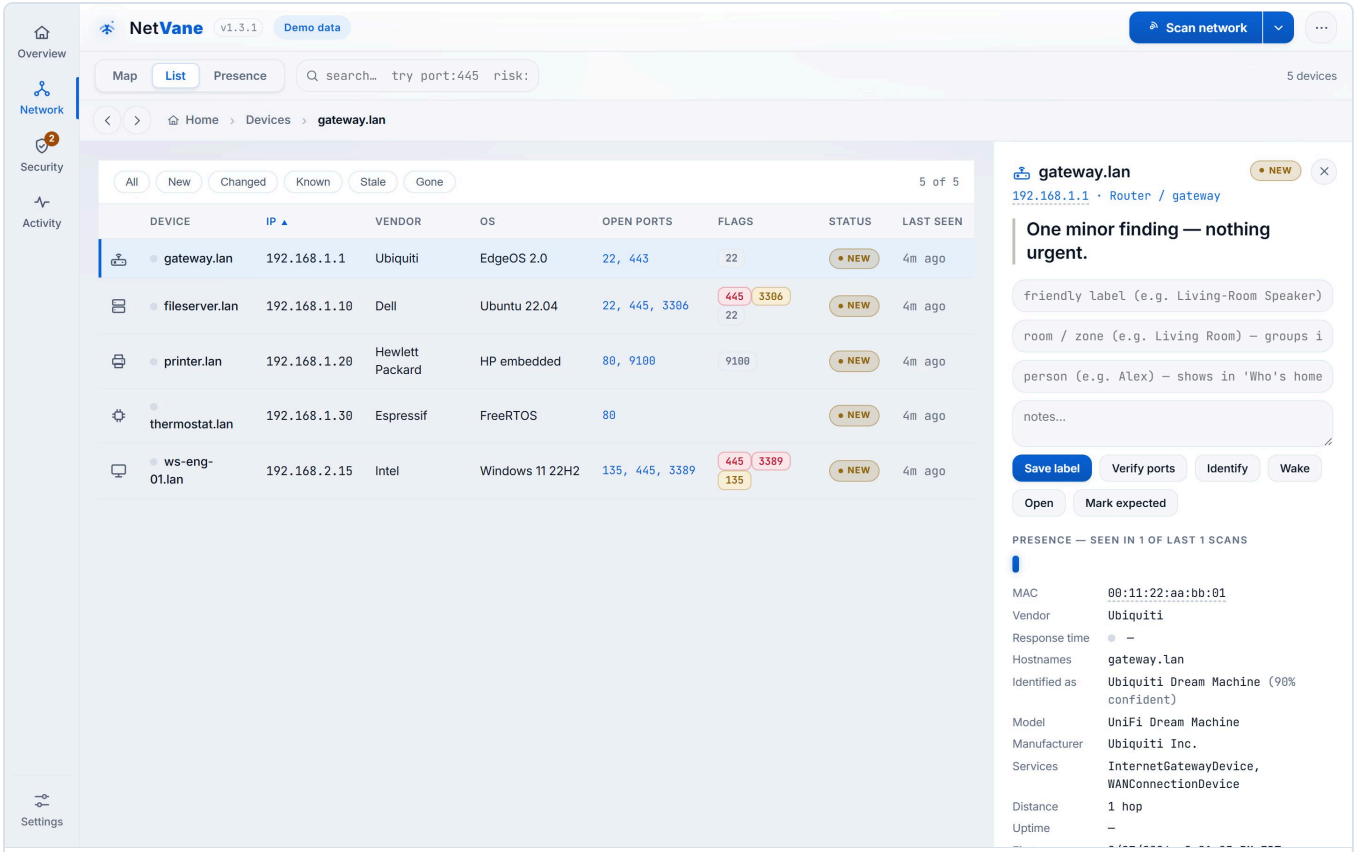
4.3 Network — the List lens (devices)

The **List** lens (Network → List) is the full inventory: every device NetVane has seen, with its IP address, MAC address and vendor, inferred device type, operating system where known, open ports, risk level, and status. Columns are sortable, addresses are click-to-copy, and a powerful structured search box lets you filter the list precisely (see section 9). NetVane also flags devices using randomized or private MAC addresses here, since those can make a device harder to identify reliably.



The List lens (Network → List). A sortable table of every device — hostname, vendor, OS, open ports, flags, and status — with a structured search box above it (demo data).

Click any device to open its detail page, where you will find its open ports and services, its identification, its presence history and response time, its notable exposures, its per-device security timeline, and the actions you can take on it — Verify, Fix, Accept risk, Identify, and Acknowledge (see section 7). Drag the panel's left edge to resize it — your chosen width is remembered across restarts; **Settings → Appearance → Restore default** resets it.



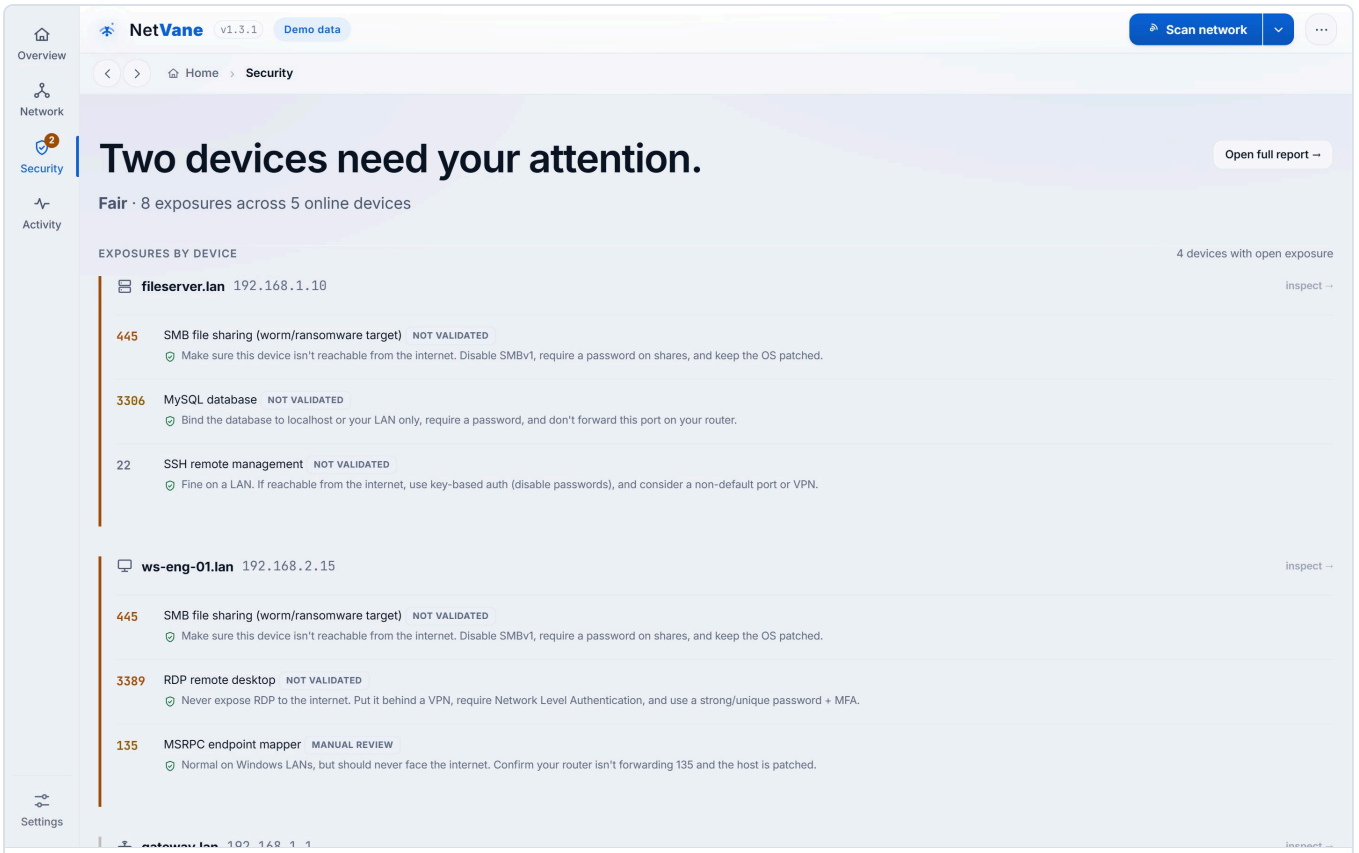
A device detail drawer. Everything about one device in one place: presence history, response time, notable exposure, and the device's own security timeline (demo data).

4.4 Security

The Security view is where your score is explained in full. It breaks the 0–100 score down factor by factor, showing exactly how many points each issue deducts and why, and charts the score over time so you can see whether your posture is improving or slipping. It also leads with a "Since last scan" delta and groups exposures by device, each paired with a plain-English fix, so you can drill into any contributing exposure and act on it. This is the view to open when you want to understand the score, not just see it.

Alongside the score, the Security view carries a set of **insight cards** that read what NetVane has already gathered — all computed locally, none of them changing your score, and nothing to turn on: **"Is your smart home contained?"** tells you whether your cameras, speakers and plugs share a network with your computers and phones (and, if so, walks you through setting up a separate guest/IoT network); **Router & gateway health** folds your DNS trust, gateway identity, risky remote-admin services and firmware currency into one plain-language verdict; **DNS speed** benchmarks your resolver(s) against reputable public ones; and **Network behavior watch** — device behavior analytics — learns your network's normal and flags meaningful drift a scan alone misses, such as a sudden sustained upload spike (read from your router's own counters), a new internet port-forward, or a long-stable smart-home device that suddenly opens a port. These signals are deliberately tuned against false alarms. An **opt-in per-device flow collector** extends this analytics *per device*: if you point your router's NetFlow v5/v9, IPFIX or sFlow export at NetVane (Settings → Advanced; per-router setup steps for UniFi, pfSense, OPNsense, MikroTik and OpenWrt are in the online guide at netvane.doorvane.com/docs/), it baselines which external destinations each device normally talks to

and flags a device that suddenly sends real volume to a brand-new destination — the classic exfiltration signature that a switched-LAN scan cannot see on its own. The collector is receive-only and accepts flow records only from the router IP you configure — a first-line filter against stray or accidental injection (a UDP source address is forgeable on the local segment, so these alerts are advisory indicators); it is off by default. A companion card, **How much data your network used**, charts daily upload and download for the last two weeks from the router's own counters — the same local samples the behavior watch already records. Days when NetVane was not running are faded and labelled, because a day it only half-watched genuinely saw less data, and drawing it as an equal would invent a usage drop that never happened.



The Security view. A "Since last scan" delta up top, then exposures grouped by device — each with a plain-English fix you can act on (demo data).

4.5 Activity

The Activity view is a chronological timeline of everything that has changed on your network: ports opening and closing, services or operating systems or hostnames changing, and devices appearing, returning, or going away. It turns a series of point-in-time scans into a running history, so you can answer questions like "when did that device first show up?" or "when did port 3389 open on the media PC?". Section 8 covers change tracking in depth.

4.6 Activity — Scans & trends

The **Scans & trends** section of Activity lists every scan you have run, with its profile, timing, and results. From here you launch new scans and pick a profile, review past scans, and **compare any two**

scans to see precisely what changed between them. It is also where recurring scheduled scans are managed (see section 10). Think of it as the control room for scanning itself.

5. Scanning

Two engines and five profiles let you trade speed for depth — and none of them touch the devices they examine.

Scanning is the heart of NetVane. Understanding the engine that does the work and the profile that decides how much work is done lets you get exactly the picture you need, whether that is a ten-second sweep or a deep one-off audit.

5.1 The two scan engines

NetVane can scan using either of two engines. The default is deliberate and simple: the built-in engine does the work unless you explicitly choose otherwise.

The **built-in native engine** is pure Python and needs nothing installed. It performs a TCP-connect port scan, reads your system's ARP table to map MAC addresses to hardware vendors, resolves reverse-DNS names, grabs service banners where they are offered, and measures TCP-connect latency (round-trip time). It runs unprivileged — no administrator rights required — discovers a home network in seconds, and works everywhere NetVane runs.

The **nmap engine** is a power-user option you select explicitly. It adds operating-system fingerprinting and richer service-version detection on top of what the native engine provides, at the cost of speed and of nmap being installed. NetVane never switches to nmap on its own — not even when nmap is present on the system.

Settings offers the choice as two options: **Built-in — fast & reliable** (the default) and **Deep scan (nmap)**, which is the only way nmap ever runs. When the nmap engine is active a pill appears in the dashboard header, so a deep scan is never a surprise; the built-in default shows no pill.

5.2 The five scan profiles

A profile decides how deep a scan goes. None of the five attack, exploit, or change anything on the devices they examine — they differ only in how much they look at. Choose a lighter profile for speed and a heavier one for depth.

Profile	What it does	Speed	When to use
Discovery	Finds live hosts only; no port scanning.	Fastest	A quick "who is on the network right now" sweep.
Quick	Scans roughly the top 100 ports with light service detection.	Fast	A rapid check of the most common services.
Standard	Top 1,000 ports plus service versions and an OS guess.	Moderate	The recommended default for regular scans.
Thorough	All 65,535 ports with full version and OS detection.	Slow (minutes per host)	When you want to leave nothing unchecked.
Aggressive	All ports plus full OS/version detection, safe discovery scripts, and traceroute.	Slowest	A one-off deep audit of the network.

For day-to-day use, Standard is the sweet spot. Reach for Discovery when you just want a fast headcount, and reserve Thorough or Aggressive for occasional deep audits, since they can take minutes per host.

5.3 Experimental scanning (opt-in)

Settings includes an **Experimental scanning** toggle, off by default while the features behind it are validated. Turning it on changes two things:

- **Two-phase deep scans.** When the nmap engine runs a deep profile, NetVane first sweeps the range for live hosts, then points nmap's slow, detailed scan only at the hosts that answered — dramatically faster on a mostly-empty range than probing every possible address in depth.
- **Multi-subnet auto-targeting.** On a fresh configuration, NetVane detects *all* the local networks your machine is attached to (up to five) and targets each of them, instead of assuming a single network — useful in homes with separate main, guest, and IoT networks.

With the toggle off, scanning behaves exactly as described in sections 5.1 and 5.2. The toggle lives in Settings alongside the other preferences, and you can turn it off again at any time.

5.4 Experimental features (opt-in)

A separate **Experimental features** group in Settings holds two newer capabilities, each **off by default** and toggled independently while they are validated:

- **IPv6 device discovery.** Alongside the normal IPv4 scan, NetVane also lists IPv6-only devices it finds in your computer's IPv6 neighbour cache — showing each one's address, manufacturer, and name. Your IPv4 scan is unchanged; these extra devices are shown for awareness but are not port-scanned.
- **SNMP switch topology.** If you have managed switches, NetVane can ask each one (over SNMP, read-only, without anything leaving your network) which devices are connected to which port, and use that to draw each device under the correct switch on the Map. Enter your switches' IP addresses

and read community, save, then click *Sync now*. Anything you've set by hand with *Connected via* always wins over what SNMP reports.

Both are off until you enable them, so nothing changes unless you opt in.

5.5 Active risk validation

An open port is not automatically a problem. Port 445 answering on a file server with signing enforced is normal; the same port on a device that will talk to anyone is not. To tell those apart, NetVane follows each scan with **active risk validation**: it connects to the notable open ports it found and speaks each service's own protocol, read-only, to see how the service actually behaves.

This is what lets the Security view separate *Confirmed active* findings from ones it can mark **Checked & cleared** — and clearing a finding removes it from your action list and lifts your score. Without validation every open port would sit in the same undifferentiated pile.

The behaviour is a single setting, **Settings → Active risk validation**, with three choices:

- **Safe — non-destructive checks (recommended).** The default. Read-only protocol handshakes and banner reads only: NetVane never sends a credential at this level, never writes anything, and never changes a device's configuration. For a few services that answer anyone without authentication at all (an exposed Redis or Elasticsearch, for example), confirming the exposure means issuing one harmless read-only command such as a status query — which is precisely the evidence that the service is open to the whole network.
- **Off — don't validate.** No probing at all. Findings stay unverified, so nothing is ever cleared from your action list automatically.
- **Authenticated — also try default/blank credentials.** Off unless you choose it, and deliberately hard to switch on by accident. This is the only level at which NetVane attempts a login, using a short list of well-known default and blank credentials to find devices still shipping with them. It stays inert until you additionally tick *I am authorized to actively test <your network>*, that authorization is tied to the exact network range you granted it for and is revoked automatically if the range changes, and it runs only on the Aggressive profile. Attempts are capped per service to avoid tripping account lockouts.

Every level is bounded by per-host and overall time budgets, and validation never breaks a scan: if it cannot finish, the scan keeps whatever it confirmed and the rest stays unverified.

6. The security score

A single transparent number from 0 to 100, with a letter grade — and every point of it explained.

NetVane distils the state of your network into one figure: a security score from **0 to 100**, paired with a letter grade from **A to F**. The point of the score is not the number itself but the fact that it is fully transparent. Every factor that affects it is shown, along with the exact number of points it costs you, so the score is never a black box — you can always see why it is what it is and what you would gain by fixing something.

6.1 What deducts points

The score deducts points for three broad things:

- **High-risk exposures** — reachable services that carry real risk, such as remote desktop, unauthenticated databases, or cleartext protocols (see section 7 and Appendix A).
- **Unidentified devices** — devices NetVane cannot confidently identify, since an unknown device on your network is itself a small risk.
- **Unexpected new devices** — devices that have appeared and that you have not acknowledged as expected.

Because each factor is shown with its point impact, the score doubles as a prioritised to-do list: fix the item that deducts the most points first, and watch the score rise.

6.2 Score history and drop alerts

NetVane charts your score over time on the Security view, so you can see the trend across many scans rather than just today's value. When the score **drops** — for example because a new high-risk exposure appeared — NetVane raises an alert so you find out promptly rather than at your next casual glance. Alerts are delivered as described in section 10.

7. Finding and fixing exposures

NetVane does not just point at problems — it explains them and walks you through fixing them, then confirms the fix worked.

An **exposure** is a reachable service that may warrant attention. NetVane groups exposures into meaningful categories, explains the risk of each in plain language, and gives you a set of actions to resolve or triage them. Crucially, it flags what is *reachable* — it is not claiming a specific known vulnerability exists. The Security view (section 4.4) is the natural starting point: it groups exposures by device and pairs each one with a plain-English fix, as shown in that view's figure above.

> **Reachable services, not CVEs**
> NetVane flags which services are reachable on your devices, and matches their versions against a bundled offline CVE database (NVD + CISA-KEV). An exposure means "this service can be reached from the network" — whether that is acceptable depends on your situation, which is exactly the judgement the Fix panel and the Accept-risk action help you make.

7.1 Notable exposure categories

Category	Typical services / ports
Cleartext protocols	Telnet, FTP
File sharing	SMB / NetBIOS (445, 139)
Windows RPC	135
Remote desktop	RDP (3389), VNC (5900)
Databases	MySQL 3306, Postgres 5432, MSSQL 1433, Redis 6379, MongoDB 27017, Elasticsearch 9200, memcached 11211
Containers	Docker (2375)
SSH	22
Printers	9100
UPnP	1900, 5000
Admin panels	8080, 8443

7.2 The Fix panel

When you open an exposure, the Fix panel explains **why** the service is flagged, **what the risk** is if it is left reachable, and gives **step-by-step remediation** instructions. To make acting on it painless, the

panel can **open the device's admin page** directly and lets you **copy the steps** so you have them to hand while you work. The guidance is written to be followed by someone who is not a security specialist.

7.3 Verify — the closed loop

After you have made a change, use **Verify**. This performs a closed-loop re-scan of that single host to confirm whether the exposure is genuinely resolved or still open. You do not have to re-scan your whole network to check one fix, and you get an unambiguous answer rather than having to guess whether the change took effect.

7.4 Accept risk

Sometimes an exposure is intentional and acceptable — you know that SSH is open on that server and you want it that way. Use **Accept risk** to triage it: the exposure is then excluded from your score and recorded with a note and a date, so your score reflects reality and there is a clear audit trail of decisions you have made. Accepted risks are collected together (and appear in reports, see section 11).

7.5 Acknowledge and Identify

When a new device appears, **Acknowledge** marks it as expected, so it stops counting against your score as an unexpected arrival. If a device is hard to identify, the opt-in **Identify** action performs a deeper name lookup using mDNS and NetBIOS to try to put a name to it — this is opt-in because it reaches out to the device a little more actively than a passive read.

7.6 Device intelligence (fingerprints)

NetVane also names the **make and model** of common home devices (“Ring doorbell”, “Sonos speaker”, “HP OfficeJet”) by matching what a device already reveals — its SSDP/UPnP identity, hostname, hardware vendor, and service banners — against a **built-in fingerprint table**. Matching happens entirely on your machine; the device detail shows the result as *Identified as*, always with a confidence percentage, because a fingerprint is an inference rather than a fact. The table updates over the air via **…** → **Update intelligence** (its Device intelligence tab) — verified before install and recorded in the locality panel, exactly like the CVE tab's updates — so identification keeps improving without an app update, and your existing devices re-identify instantly with no rescan.

8. Tracking change over time

A network is never static. NetVane remembers every scan so you can see not just the present, but the story of how you got here.

Individual scans are snapshots. NetVane's real strength is stringing those snapshots together so you can see change — the new device that appeared overnight, the port that opened last week, the score that quietly slipped. Several features work together to do this.

8.1 The activity timeline

The Activity view (section 4.5) records every change chronologically: ports opened and closed, service, OS and hostname changes, and devices that are new, that have returned, or that have gone. It is your network's history book.

8.2 "Since last scan" delta

After each scan, NetVane summarises exactly what is different from the previous scan: which exposures opened and which were resolved, which devices arrived and which departed, and how the score moved. This delta appears prominently on the Overview and at the top of the Security view (section 4.4), so the first thing you see is what changed.

8.3 Per-device security timeline

Each device has its own security timeline on its detail page, so you can follow the history of a single device — when it first appeared, when its ports or services changed, and how its risk has evolved — without wading through the whole network's history. You can see this timeline in the device-detail figure in section 4.3.

8.4 Security-score history

The Security view charts your overall score across all past scans, turning your posture into a trend line. A steadily rising line is reassuring; a dip is a prompt to look at what changed.

8.5 Compare any two scans

From the Scans & trends section of Activity you can pick any two scans and compare them directly to see precisely what changed between those two points in time. This is ideal for confirming the effect of a deliberate change — scan, make your changes, scan again, and compare.

9. Searching your inventory

Find exactly the devices you mean with structured field terms — combinable, and mixable with free text.

Once you have more than a handful of devices, scrolling the device list stops being practical. The search box on the **List** lens (Network → List) understands structured **field terms** that let you filter with precision. Each term is `field:value`, the terms combine (they narrow the results together), and you can add plain free text alongside them.

port:	Match devices with a given open port, e.g. `port:3389`.
vendor:	Match by hardware vendor, e.g. `vendor:ubiquiti`.
risk:	Match by risk level — `high`, `medium`, `info`, or `any`.
type:	Match by inferred device type, e.g. `type:camera`.
os:	Match by operating system, e.g. `os:linux`.
ip:	Match by IP address.
mac:	Match by MAC address.
status:	Match by device status.

9.1 Example queries

- `risk:high type:camera` — high-risk cameras only: a great first thing to check.
- `port:3389` — everything with remote desktop reachable.
- `vendor:raspberry os:linux` — combine terms to zero in on a specific class of device.

Because the terms combine and can be mixed with free text, you can build up a query as specific as you need without any special syntax to memorise beyond the field names above.

10. Scheduling and alerts

Set NetVane to watch your network for you, and be told when something changes.

Scanning once tells you the state today; scanning regularly tells you when something changes. NetVane can run scans on a recurring schedule and notify you when it finds something worth knowing about.

10.1 Recurring scans

You can schedule scans to run automatically on a recurring basis, managed from the Scans & trends section of Activity. This means your inventory and score stay current without you having to remember to press `s`, and change tracking (section 8) has a steady stream of snapshots to work from.

10.2 Desktop notifications

When something changes — most importantly when your security score drops (section 6.2) — NetVane raises a **native Windows notification** so you find out at the time rather than at your next visit to the dashboard. With background mode on (section 10.4), these notifications keep arriving even while the NetVane window is closed.

10.3 The optional webhook

For users who want alerts to reach another system — a chat channel or a home-automation hub, for example — NetVane can call an **optional webhook** that you configure. Because alert payloads include device details from your network, NetVane requires the webhook URL to be `https://` — a cleartext `http://` address is refused when you save it.

Beside the URL, **Alert format** chooses how the alert is written. A raw JSON payload is the right thing for your own automation and the wrong thing for a phone: **ntfy** would display it as a block of JSON, and **Discord** and **Slack** reject it outright. So pick the service you are sending to and NetVane writes the alert in that service's shape — a readable one-line headline, then the findings, highest severity first so the one that matters is never the one trimmed off the end. The four options are:

- **NetVane (raw JSON)** — the default, and unchanged from every previous version, so existing automations keep working exactly as before.
- **ntfy** — a plain-text push notification. The best choice for a phone; works with the public ntfy.sh service or your own self-hosted server.
- **Discord** — posts into a channel via an incoming webhook.
- **Slack** — also accepted by Mattermost and Rocket.Chat.

Send test, next to the format, posts one sample alert immediately so you can confirm it arrives before you rely on it. Delivery is deliberately fire-and-forget — a flaky webhook must never be able to slow or block a scan — so the button confirms that NetVane sent the request, not that the far end accepted it; any delivery failure appears in *Diagnostics* with the reason.

A hosted alert service sees your device names
Alerts carry hostnames, IP addresses and what NetVane found exposed. Send them to ntfy.sh, Discord or Slack and that company can see them. That may well be a fair trade for you — but it is a real disclosure, so make it deliberately. A **self-hosted ntfy** gives you the same phone notifications with nothing leaving your own infrastructure. Either way, every send is counted by destination in the **Local-only** panel.

The only traffic that carries your network's data — and only if you set it
The webhook is the main path by which information *about your network* can leave your machine, and it exists only because you explicitly asked for it. The one other path is a support report you choose to send from *Report a problem* (section 14), which carries recent logs with device IPs and MAC addresses stripped out. Configure no webhook and send no support report, and nothing about your network is transmitted anywhere. (NetVane's optional update checks, described in section 12, send nothing about your network.)

10.4 Background mode and start at login

By default, closing the NetVane window quits the app. For continuous monitoring, **Settings → Background & startup** offers two independent toggles, both **off by default**:

- **Run in the background.** With this on, closing the window minimizes NetVane to the **system tray** instead of quitting. Scheduled scans keep running and Windows notifications keep arriving while the window is closed. Reopen the dashboard, or quit NetVane completely, from the tray icon's menu (or **…** → **Exit** in the dashboard's overflow menu).
- **Start automatically at login.** With this on, NetVane starts when you sign in to Windows, minimized to the tray, so monitoring resumes without you doing anything. It uses a standard per-user startup entry — no administrator rights — and turning the toggle off removes it.

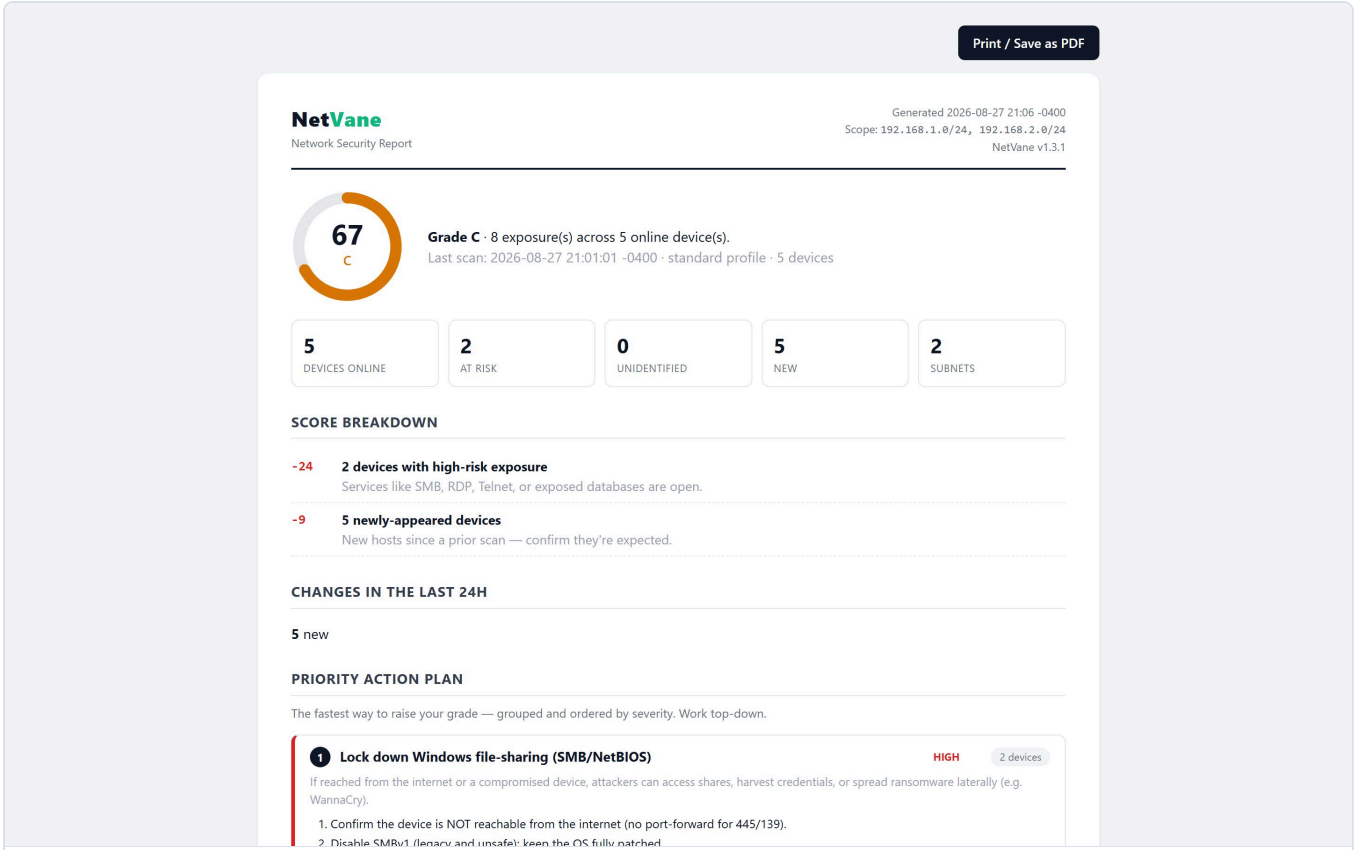
Together with scheduled scans (section 10.1), these turn NetVane from a tool you run into a monitor that watches the network for you.

11. Reports and exports

Take your findings with you: a polished printable report and a plain CSV of your inventory.

11.1 The printable security report

NetVane can generate a self-contained, printable HTML security report. Because it is self-contained, you can open it, print it, or use your browser's **Print → Save as PDF** to produce a shareable document.



The printable report. Led by a Priority Action Plan — a ranked, de-duplicated to-do list with steps and the devices each fix affects (demo data).

The report is led by a **Priority Action Plan** — a ranked, de-duplicated to-do list grouped by fix, with the affected devices and ports listed against each item. This puts the highest-value work first and avoids repeating the same fix once per device. After the action plan, the report lays out exposures by device, an **accepted-risks ledger** (the risks you triaged in section 7.4), the full **score breakdown**, and a complete **inventory**. It is designed to be handed to someone else or filed as a record of a point in time.

11.2 CSV inventory export

For working with your data elsewhere — a spreadsheet, a script, or another tool — NetVane can export your device inventory as a **CSV** file.

12. Privacy and your data

Your network map never leaves your machine, because there is nowhere for it to go.

NetVane's privacy model is simple because it is absolute: the tool is **fully local**. There is no cloud service behind it, no account to sign in to, and no telemetry; nothing about your network ever leaves your machine, and it does not fetch web fonts or scripts. Nothing NetVane scans or monitors leaves your machine on its own. What can go out, and only because you asked for it: optional, integrity-checked update checks for the app, the CVE database, the device-fingerprint table and the network-owner data, none of which send anything about your network; a change-alert webhook, if you configure one (section 10.3); a support report, if you choose to send one (section 14); and the speed test and DNS benchmark, which contact public internet services by design when you run them. With none of those in use, NetVane works completely offline.

12.1 What is stored, and where

All of your data — every device, scan, exposure, note, and score — lives in a single local **SQLite database file named** `netvane.db` on your machine. The installed app keeps it, together with the settings file and a small local **troubleshooting log** (see section 14), in your per-user data folder at `%LocalAppData%\NetVane`; the portable build keeps the same three things in a `NetVane-Data` folder beside the executable, so it writes nothing to your user profile and the whole app travels with the file; running from source keeps them in the working directory. That folder, plus any reports or CSV exports you deliberately save, is the entirety of what NetVane keeps. Nothing is stored anywhere else, and the only things about your network that can leave the machine are ones you set up or ask for yourself: the outbound webhook of section 10.3, and a support report you choose to send (section 14).

12.2 How long your history is kept

NetVane keeps your history for a long time, but not forever — a database that only ever grew would eventually become a burden on your disk. The window is deliberately generous, and it has two halves that work together: **everything from the last 180 days is kept** (roughly six months), and **your 120 most recent scans are always kept**, together with the device detail and the changes recorded alongside them, however old they are. A scan is removed only once it is **both** older than six months **and** outside those 120 most recent scans, so whichever of the two is more generous for you is the one that applies. If you scan once a week, 120 scans is more than two years of history; once a month, it is a decade; several times a day, you keep a full six months. Alerts and notices that do not belong to a particular scan — a scheduled digest, a behaviour-watch alert — simply age out after six months.

What ages out is the scan-by-scan detail: individual scan records, the per-scan observations behind them, and the older entries in the Activity timeline (section 8). What never ages out is everything you would actually miss: your **device inventory**, the labels and notes you have written, the risks you have accepted, your zones and people, and your settings. Those stay until you remove them yourself.

Both halves of that window are **defaults, and both are yours to change** in **Settings → Data & backup**: *Keep history for* sets the number of days, and *always keep this many recent scans* sets the

count. Raise them if you want deeper history and have the disk for it; lower them if you would rather keep the database small.

> **Lowering the window never deletes history you already have**
> Every scan carries the retention window it was recorded under, so lowering the setting changes only what is kept from that point forward — it cannot reach back and remove records you already hold. That is a property of how the data is stored, not a promise about how the app behaves, and it holds regardless of anything to do with licensing. If you genuinely want old records gone, take a backup from **Settings → Data & backup → Download backup** first, then close NetVane and move `netvane.db` aside; the app creates a fresh database on the next launch.

A few of the live charts keep a deliberately shorter window, because a short window is all they are for. Internet and gateway quality samples cover the **last 7 days**; the data-volume samples behind behaviour watch cover the **last 14 days**; the speed test keeps your **last 50 results**; and if you switch on the optional flow collector, an external destination a device has not contacted for **60 days** drops out of that device's learned-normal list and has to be learned again.

The tidying happens quietly on your own machine, at the end of a scan. Nothing is sent anywhere when it runs, nothing is reported to anyone, and there is nothing for you to configure or approve. If you want to keep history beyond these windows, save a copy before it ages out: **Settings → Data & backup → Download backup** writes a single file holding your history and settings, or you can copy `netvane.db` somewhere safe while the app is closed.

12.3 Deleting your data

Because everything lives in one folder, removing your data is straightforward: **stop the application and delete the `%LocalAppData%\NetVane` folder** (or just `netvane.db` inside it to keep your settings), along with any exports you saved. That is all — there is no cloud copy to also delete, no account to close, and no residual data elsewhere. Uninstalling the app itself is a separate, normal Windows uninstall (section 2.1).

13. Licence and editions

What is free, what NetVane Pro adds, and what a licence never takes away.

13.1 Free, and what Pro adds

Free is not a trial and not a crippled version. Scanning whenever you like, every device, the network map, the security score, every finding explained, known-exploited vulnerability matching, read-only confirmation that an exposure is genuine, reports you export yourself, presence history, internet connection quality, local backup and the egress ledger are all free — on a single network, permanently, with no account and no time limit.

Vulnerability and device-fingerprint updates are free as well. NetVane tells you it is checking your network against known problems, and doing that against a database that had stopped being updated would be giving you a worse answer rather than a smaller feature set. Accuracy is not something you buy.

NetVane Pro is the automation. Scheduled unattended scanning, alerts to your phone or chat, running in the background from the tray, multiple subnets and VLANs, extended history retention, credential checks that find devices still on default logins, and one-click fixes for what NetVane finds. It is a perpetual licence for one person on every computer they use — bought once, not a subscription, and it does not expire.

NetVane Business is for organisations. Everything in Pro, licensed for one organisation and up to 3 administrators, plus two exports built for assessments, both in the **…** overflow menu: the **compliance evidence report** — a printable document stating what was scanned and how, what was found, which risks were explicitly accepted and why, and every change NetVane made with its audit trail — and the machine-readable **evidence pack**, which carries its own integrity hash so whoever receives it can prove the contents were not edited after export. The report states in its own words that it is evidence to support an assessment, not a certification.

Settings → Licence shows what you are entitled to, including who a Business licence covers. Where a setting needs Pro or Business, it stays visible and says so rather than disappearing.

13.2 The 14-day trial

From the moment you install it, NetVane runs with everything unlocked for **14 days**. There is no account to create, no card to enter and nothing to cancel. The trial exists to show you what the product does, not a shorter list of it.

The countdown starts at first run and is anchored in three places on your own machine, so reinstalling does not restart it. When it ends, NetVane tells you plainly, drops to Free, and lists what still works.

13.3 Activating a licence

A licence is a short block of signed text. Paste it into **Settings → Licence** and click Activate.

Activating sends nothing. Your licence is checked entirely on your own machine, against a key built into the application — it works on a computer that has never been connected to the internet, and it generates no network traffic at all. NetVane has no licence server to call, and adding one would undermine the thing that makes it worth running.

Remove, next to the licence, removes only the licence. It does not touch your scan history, your devices, your labels or your notes.

13.4 What expiry does, and does not, do

If a licence lapses, NetVane steps down to Free and says so. That is the whole of it. Specifically:

- **Nothing is deleted.** Your history, device names, notes and accepted risks stay exactly where they are.
- **Findings stay visible.** You can always see what NetVane has found about your own network. What a licence buys is acting on it, watching it and keeping the intelligence fresh — never the right to know.
- **It tells you.** Anything that pauses says that it has paused. A monitoring tool that quietly stops monitoring is worse than one that never offered.

The full terms are in the licence agreement at **netvane.doorvane.com/eula/**, and the editions are described at **netvane.doorvane.com/pricing/**.

14. Responsible use

Powerful visibility comes with a simple responsibility: only look at what is yours to look at.

NetVane gives you a clear view of a network and the services on it. That is exactly the kind of visibility that must be used responsibly. The rule is simple and firm: **only scan networks you own or are explicitly authorized to test**. Scanning networks you do not own or have permission to examine can be intrusive and, in many places, unlawful — even though NetVane changes nothing.

It helps to remember that NetVane is **non-destructive toward the devices it examines**. It sees which services are reachable, reads what those services volunteer, and confirms an exposure by speaking the service's own protocol read-only; it never exploits anything, never writes to a device and never changes one — and it logs in to nothing unless you switch on the optional credential check of section 5.5 yourself. That keeps NetVane safe to run on your own network, but it does not change the boundary of *where* it is appropriate to run it: your own networks, or those you have clear authorization to test. When in doubt, do not scan.

15. Troubleshooting

The handful of things that occasionally trip people up, and how to get past each one.

SmartScreen or antivirus warns on first run

Check that it names **GRCSAC**. A newly issued certificate builds SmartScreen reputation over time, so a prompt is not a sign of a problem with the file. Click **More info** and then **Run anyway**. NetVane still needs no administrator rights. (See section 2.1.)

Port 8787 is already in use, or "NetVane is already running"

NetVane serves its dashboard on `http://127.0.0.1:8787`. Only one copy runs at a time: launching a second copy simply hands you over to the one already running. If a dialog tells you NetVane is already running but its dashboard is not responding, a previous copy may not have closed cleanly — close it (check the system tray first) and launch again. If a *different* application is holding port 8787, stop it, then start NetVane again.

Slow first start

A cold start can take **10 to 40 seconds** the first time, especially from the prebuilt binary as it unpacks. This is normal — give it up to a minute before assuming something is wrong, then open `http://127.0.0.1:8787`.

No devices found

If a scan finds nothing, check that you are scanning the right network range and that a local firewall is not blocking NetVane's traffic. Confirm your machine is actually connected to the network you expect, then run the scan again.

nmap is installed but not being used

That is by design (section 5.1): NetVane never switches to nmap on its own. The default engine is the built-in scanner; if you want nmap's OS fingerprinting and richer version detection, open **Settings** and set the scan engine to `nmap` explicitly. When nmap is the active engine, the header pill says so.

Scans feel slow

Scan time depends heavily on the profile. Thorough and Aggressive scan every port and can take minutes per host. If a scan is taking longer than you want, choose a lighter profile — **Standard**, **Quick**, or **Discovery** (section 5.2).

Getting a shareable diagnostics report

For anything you cannot resolve from this list, open **…** → **Report a problem** from the dashboard's overflow menu. It assembles a **redacted** report — version, platform, engine, CVE-database status, and the recent log tail, with every IP and MAC address scrubbed — that you can copy with one click and safely include when reporting a problem. Nothing in the report identifies your devices, and nothing is ever sent automatically; you decide where it goes. The same dialog's **Open logs folder** button takes you straight to the log described below.

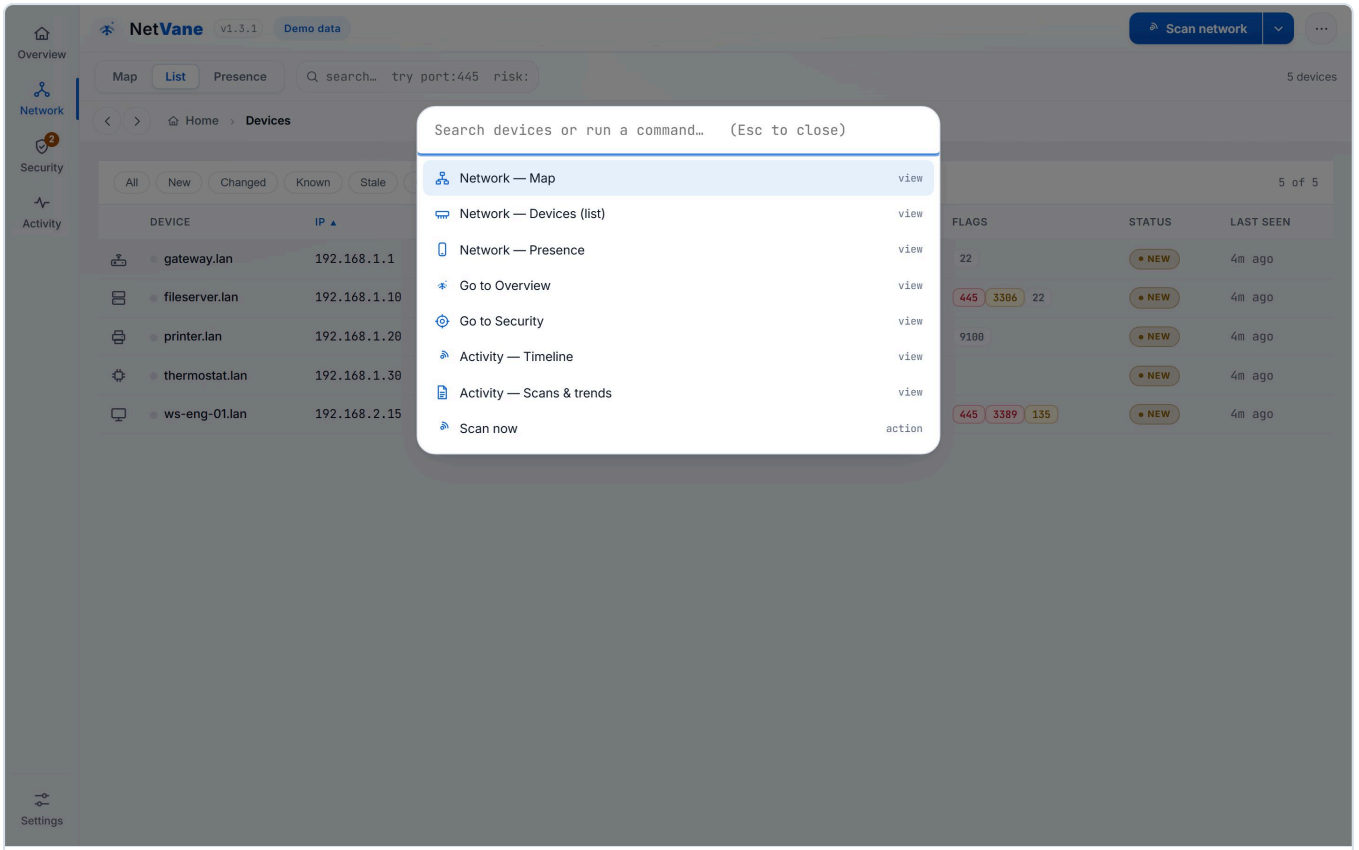
Where NetVane keeps its log

NetVane writes a small rotating troubleshooting log to `%LOCALAPPDATA%\NetVane\logs\netvane.log`, recording startup, scan failures, and any unexpected errors. If something goes wrong, that file is the first place to look — and useful to include when reporting a problem. Like everything else NetVane keeps, it is **local-only and never uploaded**.

16. Keyboard shortcuts

NetVane is built to be driven from the keyboard. These are the shortcuts worth learning.

Almost anything you can click, you can also reach without leaving the keyboard. The fastest way in is the **command palette**: press `Ctrl` `K` to open an overlay with a search box and quick actions, then type to jump to a view, a device, or an action. The number keys and single-letter shortcuts below are the direct routes for the things you do most often.



The command palette. Press `Ctrl` `K` to open it, then type to search views, devices, and quick actions (demo data).

Shortcut	Action
`1` – `4`	Jump to a view: Overview, Network, Security, Activity.
`Ctrl` `K`	Open the command palette.
`/`	Focus the search box.
`s`	Start a scan.
`t`	Toggle dark / light theme. (The three-way *System / Light / Dark* choice lives in **Settings** → **Appearance**.)
`?`	Open help.
`Esc`	Close the current panel or dialog / step back.

17. Revision history

A record of the changes made to this document across its revisions.

This table is updated with each revision of this document, so you can see at a glance which version you are reading and what changed.

Version	Date	Summary
1.0	July 30, 2026	Initial release.
1.2	August 24, 2026	NetVane Business added to Licence and editions (the compliance evidence report and the tamper-evident evidence pack); the data-usage card added to the dashboard tour; the flow collector now lists sFlow among its accepted formats.
1.1	August 20, 2026	Licence and editions rewritten for the release of NetVane Pro: what stays free, what Pro adds, and what a licence never takes away.

Appendix A — Notable ports reference

The service categories NetVane flags as notable exposures, and the ports behind them.

This table collects the notable exposure categories described in section 7, as a quick reference. Remember that NetVane flags these because they are *reachable*, not because a specific vulnerability is known to exist — whether a given exposure is acceptable is a judgement for you to make, with the help of the Fix panel and the Accept-risk action.

Category	Ports	What it is
Cleartext	Telnet, FTP	Protocols that carry data (including credentials) unencrypted.
File share	445, 139	SMB / NetBIOS file sharing.
Windows RPC	135	Windows remote procedure call endpoint mapper.
Remote desktop	3389, 5900	RDP (3389) and VNC (5900) remote-control services.
Database — MySQL	3306	MySQL database server.
Database — PostgreSQL	5432	PostgreSQL database server.
Database — MSSQL	1433	Microsoft SQL Server.
Database — Redis	6379	Redis in-memory data store.
Database — MongoDB	27017	MongoDB document database.
Database — Elasticsearch	9200	Elasticsearch search/analytics engine.
Database — memcached	11211	memcached caching service.
Container	2375	Docker remote API (unencrypted).
SSH	22	Secure Shell remote access.
Printer	9100	Raw printing (JetDirect) service.
UPnP	1900, 5000	Universal Plug and Play service endpoints.
Admin panel	8080, 8443	Web-based administration interfaces.

NetVane v1.3.1 · User Guide · Document version 1.0 · August 27, 2026 · A doorvane project.