NexTrack by NexSuite

Feature guide

Every feature of NexTrack, IT asset & endpoint management, one by one, with screenshots.

DECEMBER 2026 · GETNEXSUITE.COM

OVERVIEW

How NexTrack works

NexTrack runs on your own server. A small agent on each PC reports to it, and your team works in the browser.

1 · Your server

NexTrack and its database on a Windows Server (or Linux) you control, on-premises or in your cloud. Your data never passes through ours.

2 · The agent

Installed on each PC with Group Policy, Intune or by hand. It only connects out to your server over HTTPS; no ports are opened on the PCs.

3 · Your team

Signs in with their company account in any browser. Roles come from your directory groups.

Contents

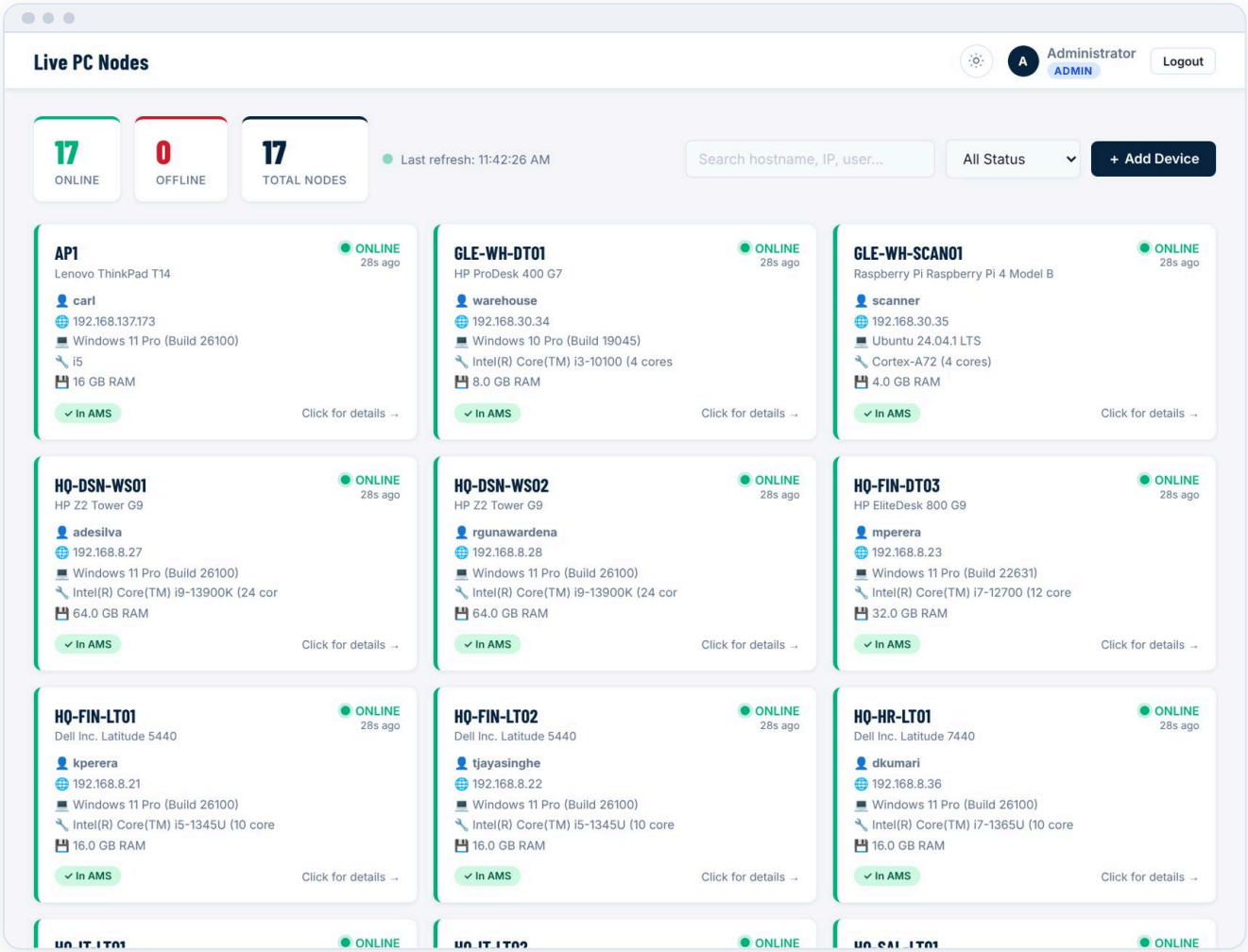
01 Live inventory — Discovery · 3
02 Device details — Discovery · 4
03 Device history — Discovery · 5
04 Coverage report — Discovery · 6
05 Dashboard — Overview · 7
06 Asset register — Assets · 8
07 QR asset labels — Assets · 9
08 Software licences — Assets · 10
09 Contracts and warranties — Assets · 11
10 Purchasing, vendors and locations — Assets · 12
11 Bulk import and reports — Assets · 13
12 Remote support — Support · 14
13 Company sign-in — Access · 15
14 Roles and audit log — Access · 16
15 Rolling out the agent — Deployment · 17
– Security and privacy — 18
– Editions and requirements — 19

Screenshots are from a NexTrack server with sample data. Names of people and computers are examples.

01 · DISCOVERY

Live inventory

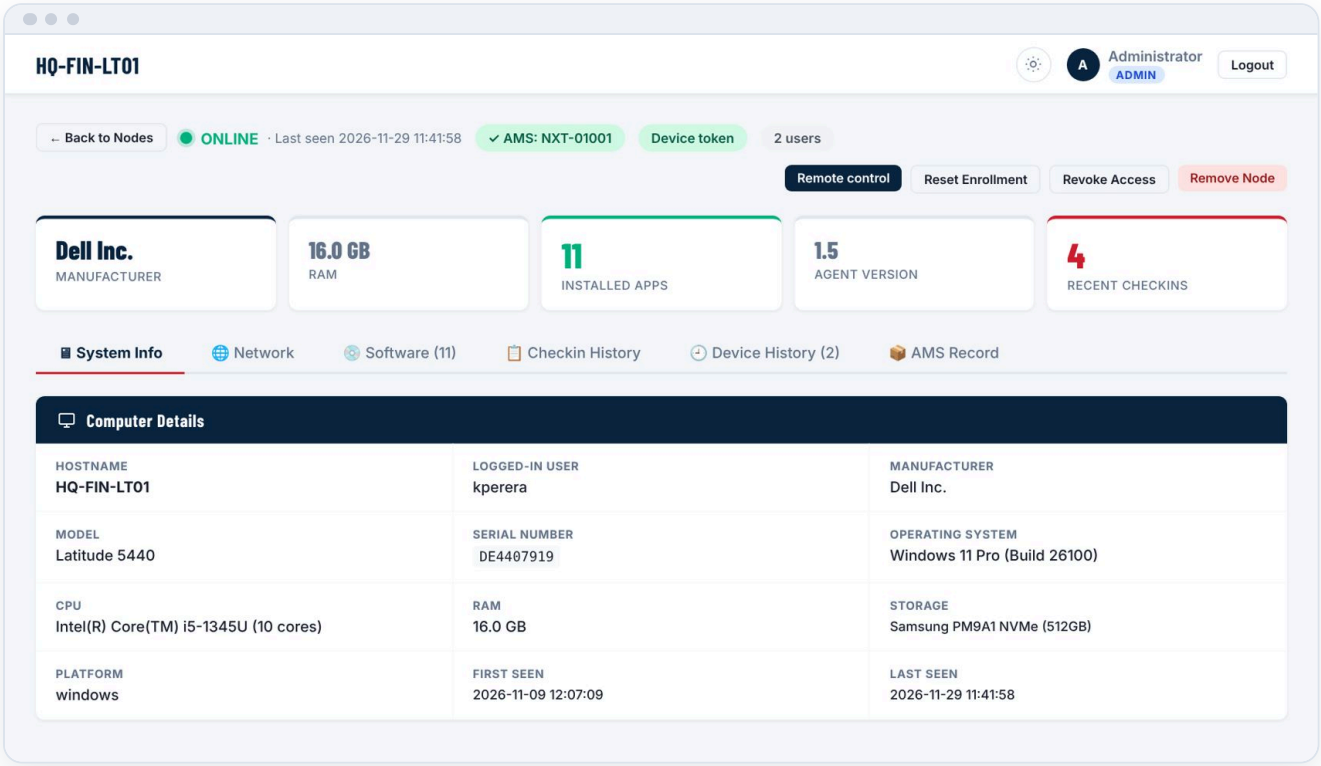
A small agent on every Windows and Linux PC reports in by itself. New machines appear within a minute; nobody types anything in.

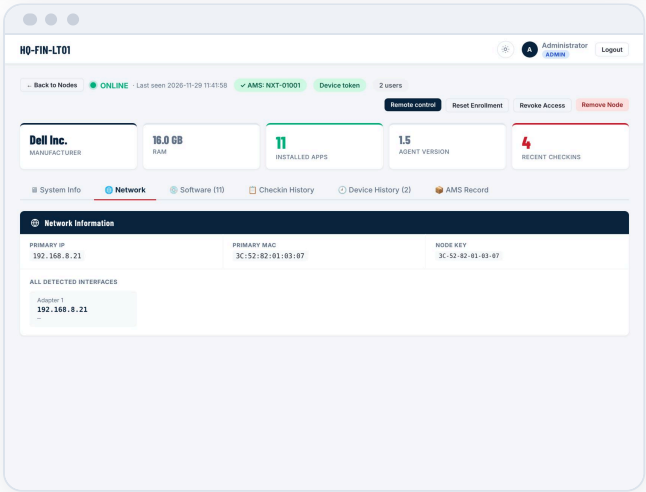


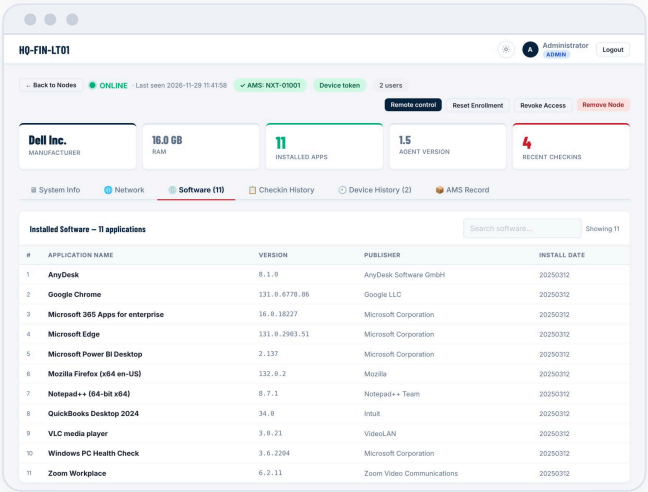
- Each PC reports its hardware, operating system, logged-in user, network and software every 10 minutes
- Online, offline and total counts at the top; offline machines are flagged after 20 minutes of silence
- Search by computer name, IP address or user, and filter by status
- Every new PC gets an asset tag (NXT-...) in the asset register automatically
- Windows 10/11 and Windows Server 2016+; Linux: Ubuntu, Debian, RHEL, Rocky, Alma, CentOS 7+, SUSE

Device details

One page per machine with everything IT needs to know, from serial number to installed software.





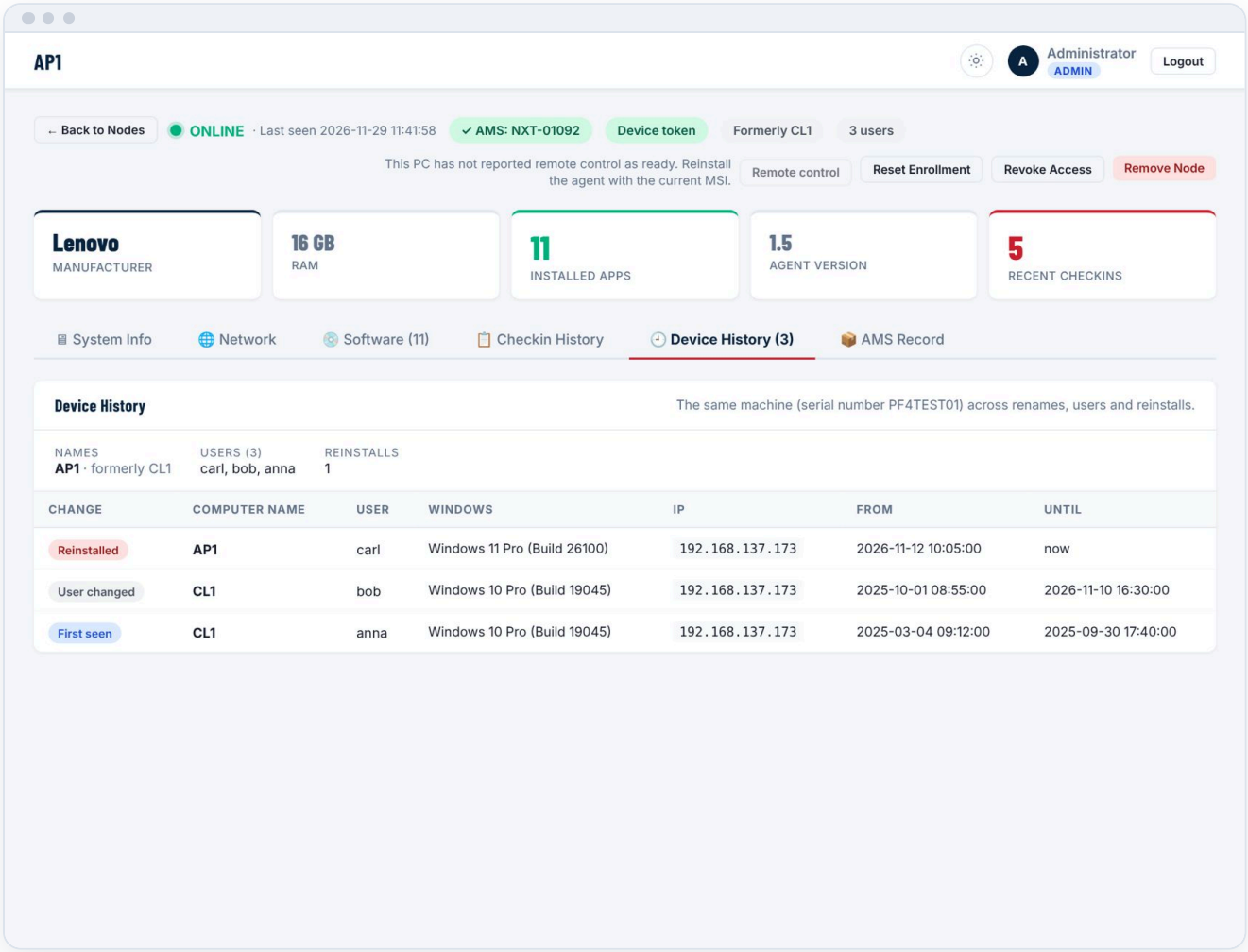


- Manufacturer, model, serial number, CPU, RAM, storage, operating system and build
- Network adapters with IP and MAC addresses
- The full list of installed applications with version, publisher and install date
- Check-in history, the linked asset record, and actions: remote control, reset enrollment, revoke access

03 · DISCOVERY

Device history

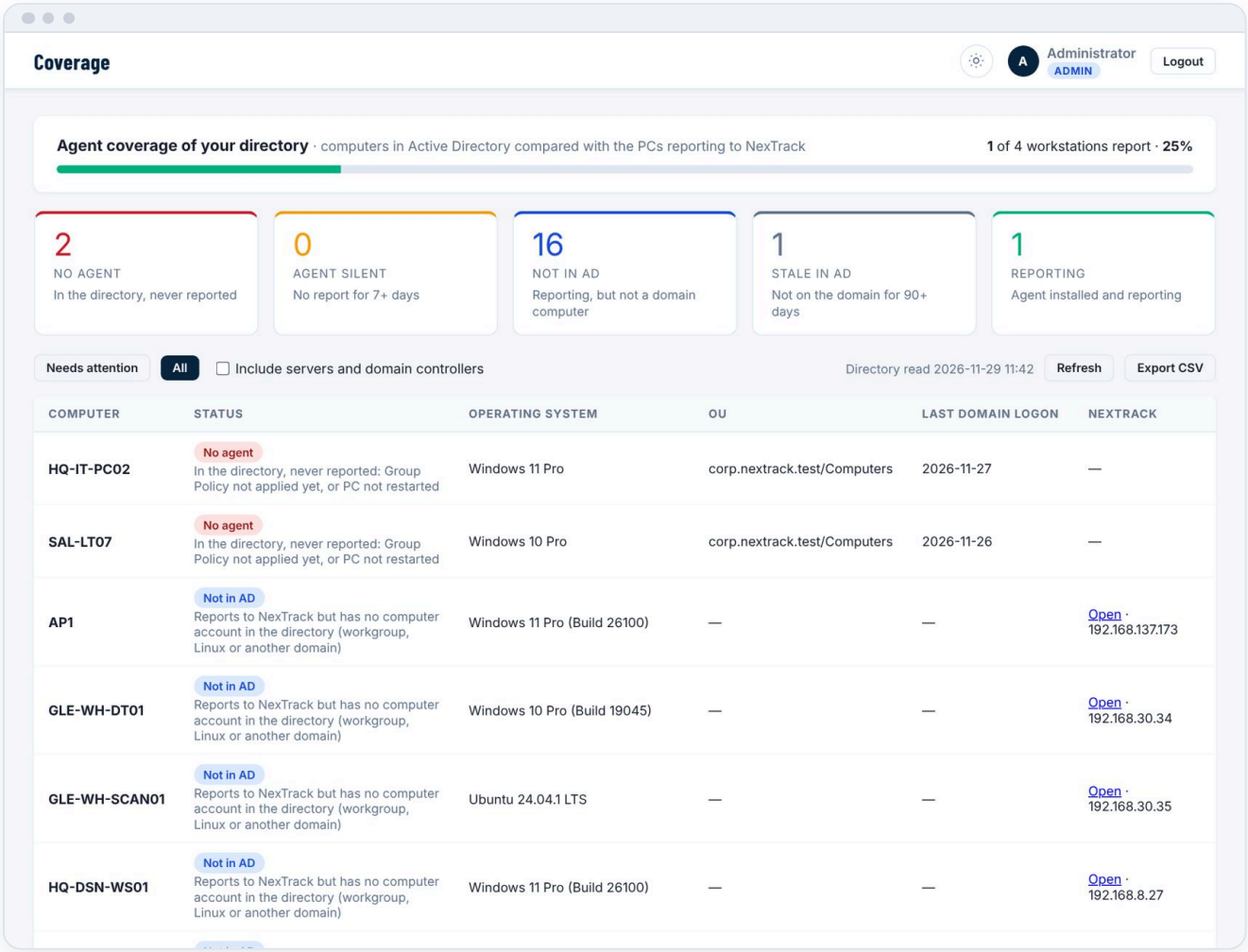
When a PC is formatted, renamed or handed to someone else, it stays one device. NexTrack recognises it by its serial number and network card.



- A timeline of every computer name, user and Windows version the machine has had, with dates
- "Formerly CL1" and "3 users" badges on the device page
- A reinstalled PC is accepted again automatically, without an admin resetting it; the change is audited
- Placeholder serial numbers (such as "To be filled by O.E.M.") never merge two machines

Coverage report

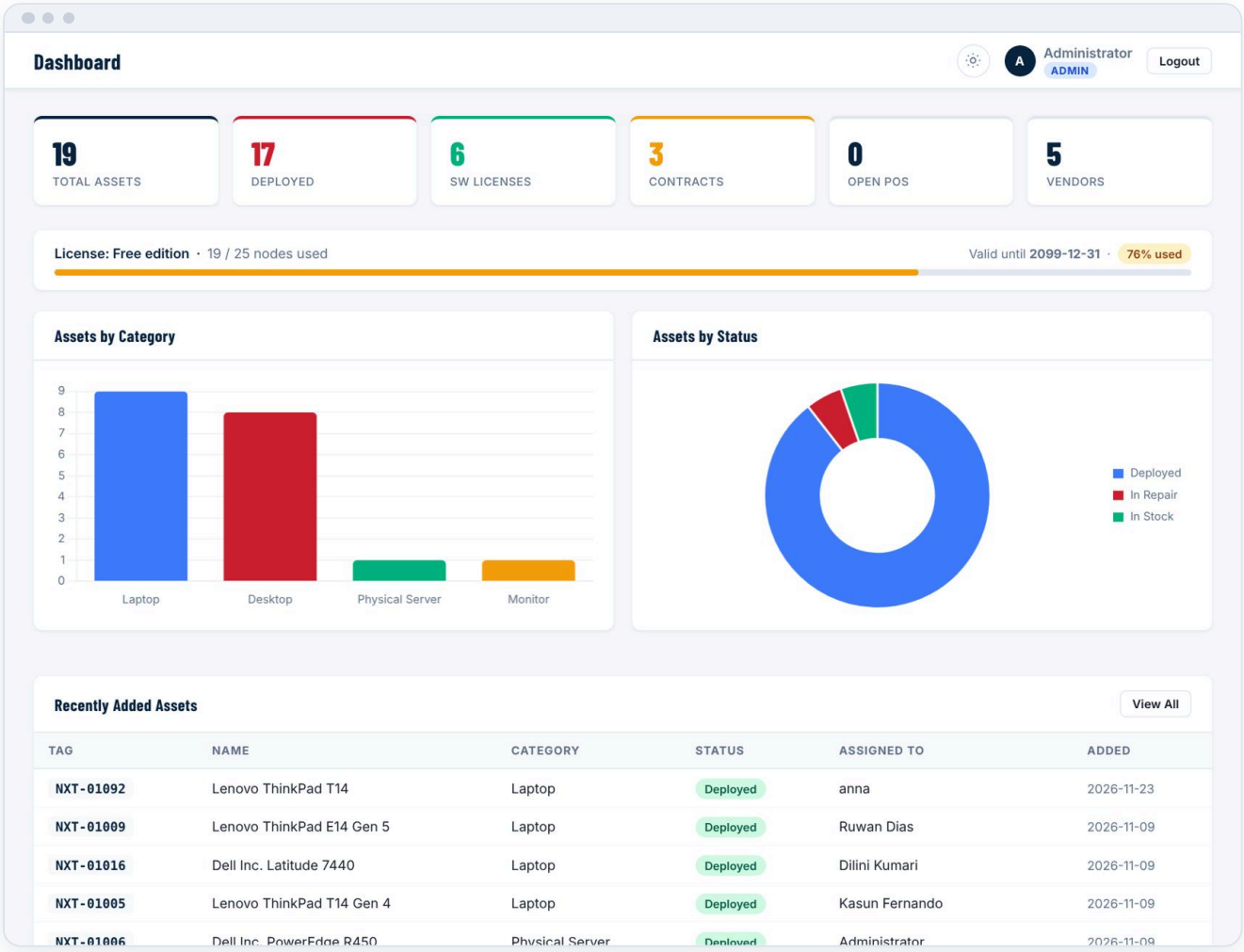
Compares the computers in your Active Directory with the PCs that actually report, so you see exactly where the agent is missing.



- No agent: in the directory but never reported (for example, Group Policy not applied yet)
- Agent silent: no report for 7+ days. Not in AD: reporting but not a domain computer
- Stale in AD: computer accounts unused for 90+ days, usually retired PCs
- Coverage percentage, OU and last domain logon per PC, advice for each status, CSV export

Dashboard

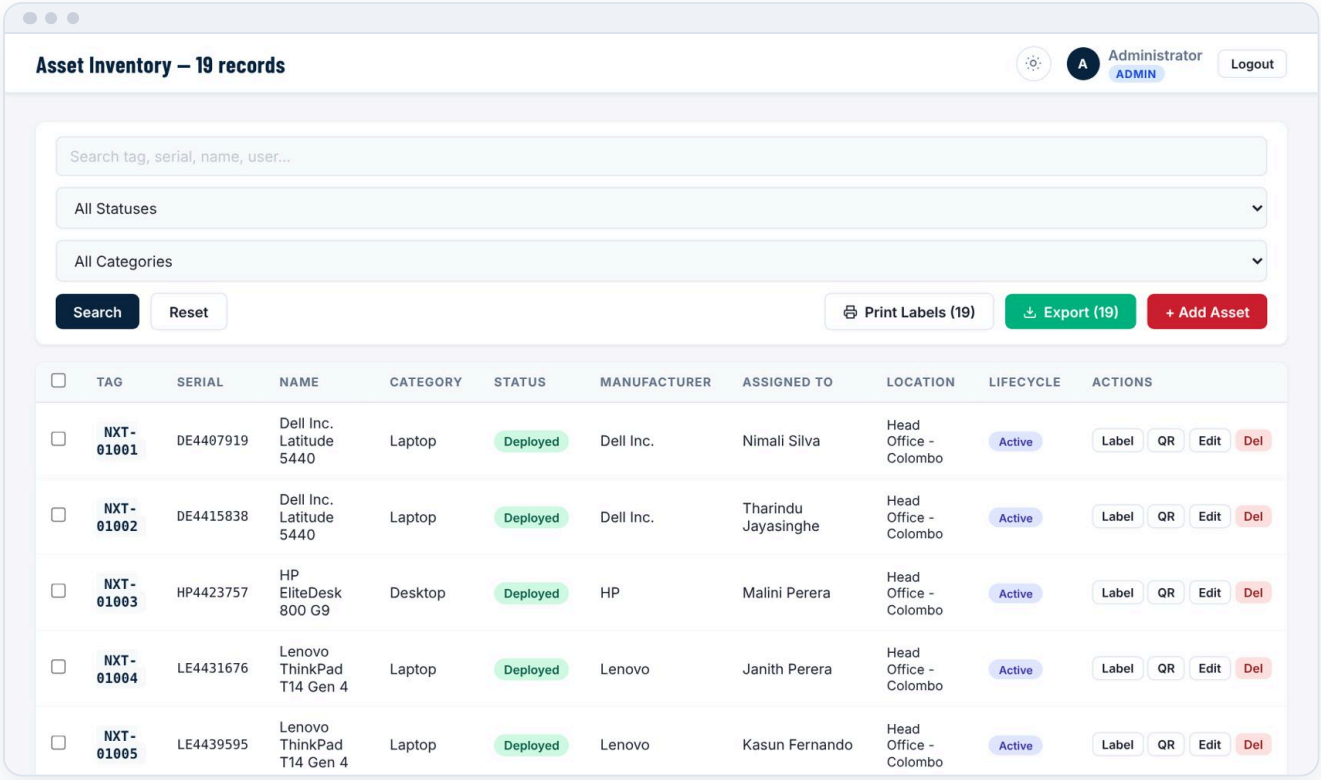
The whole estate on one screen: assets, licences, contracts, purchasing and your licence usage.

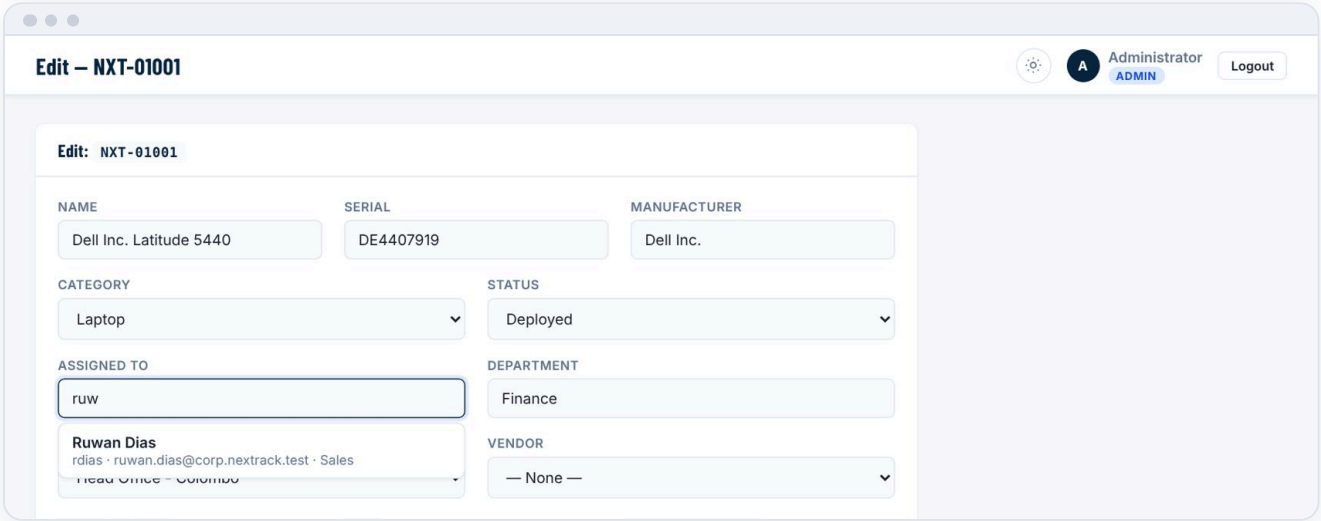


- Totals for assets, deployed devices, software licences, contracts, open purchase orders and vendors
- Charts by category and by status
- Licence usage bar showing how many devices your edition allows
- Recently added assets with their owners

Asset register

Every device and its owner, location, cost and lifecycle stage, kept current by the agents.

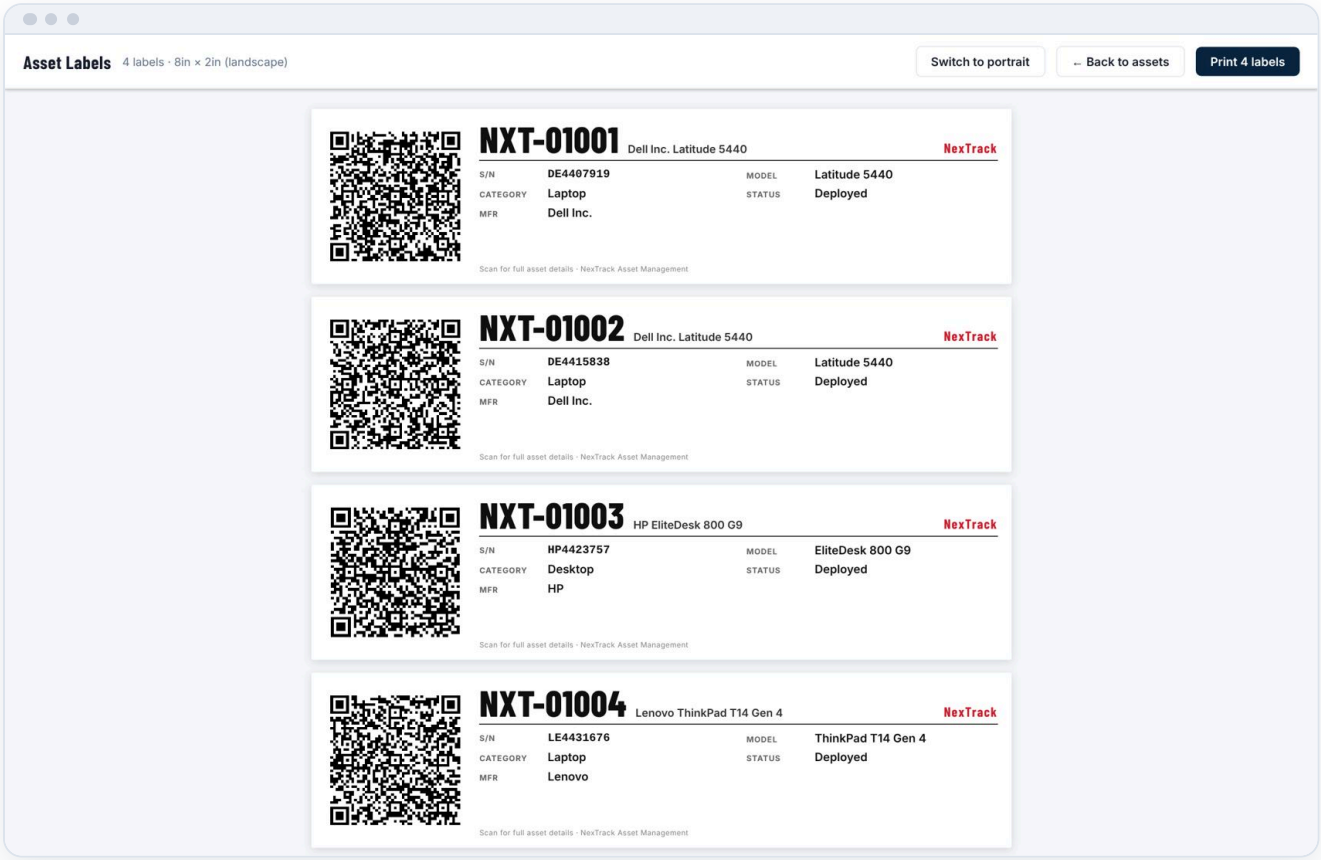




- Asset tag, serial, category, status, manufacturer, model, department and assignee
- Search and filter by status and category; export to Excel
- Assign a device to a person picked from Active Directory or Entra ID: name, email and department fill in
- Purchase date, cost, vendor, warranty end and lifecycle stage from purchase to retirement

QR asset labels

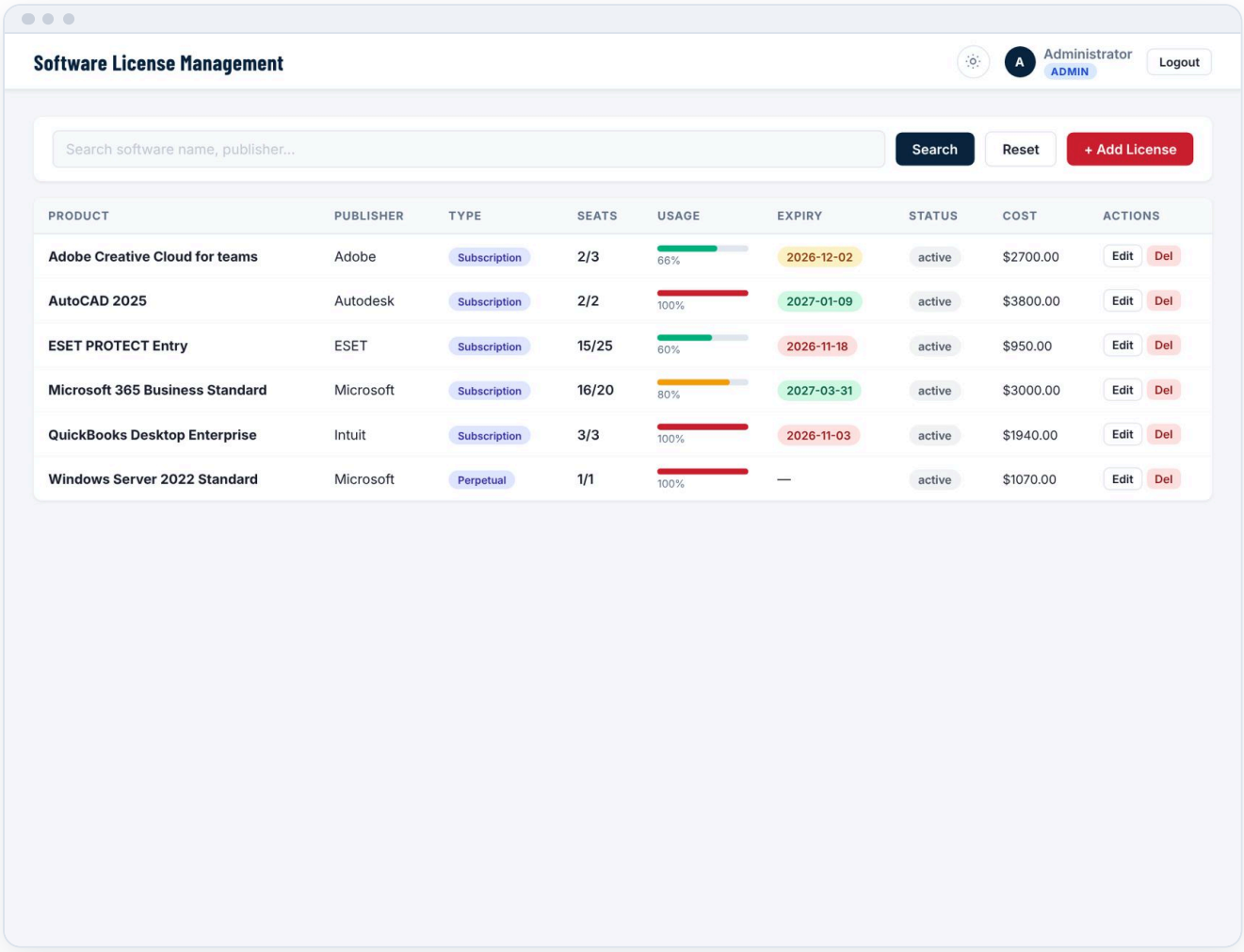
Print labels for any selection of assets. Any phone camera reads the QR code; no app is needed.



- Asset tag, serial number, model, category, status and manufacturer on each label
- Choose assets by ticking them or by filter; landscape or portrait layout
- Prints from the browser on standard label stock

Software licences

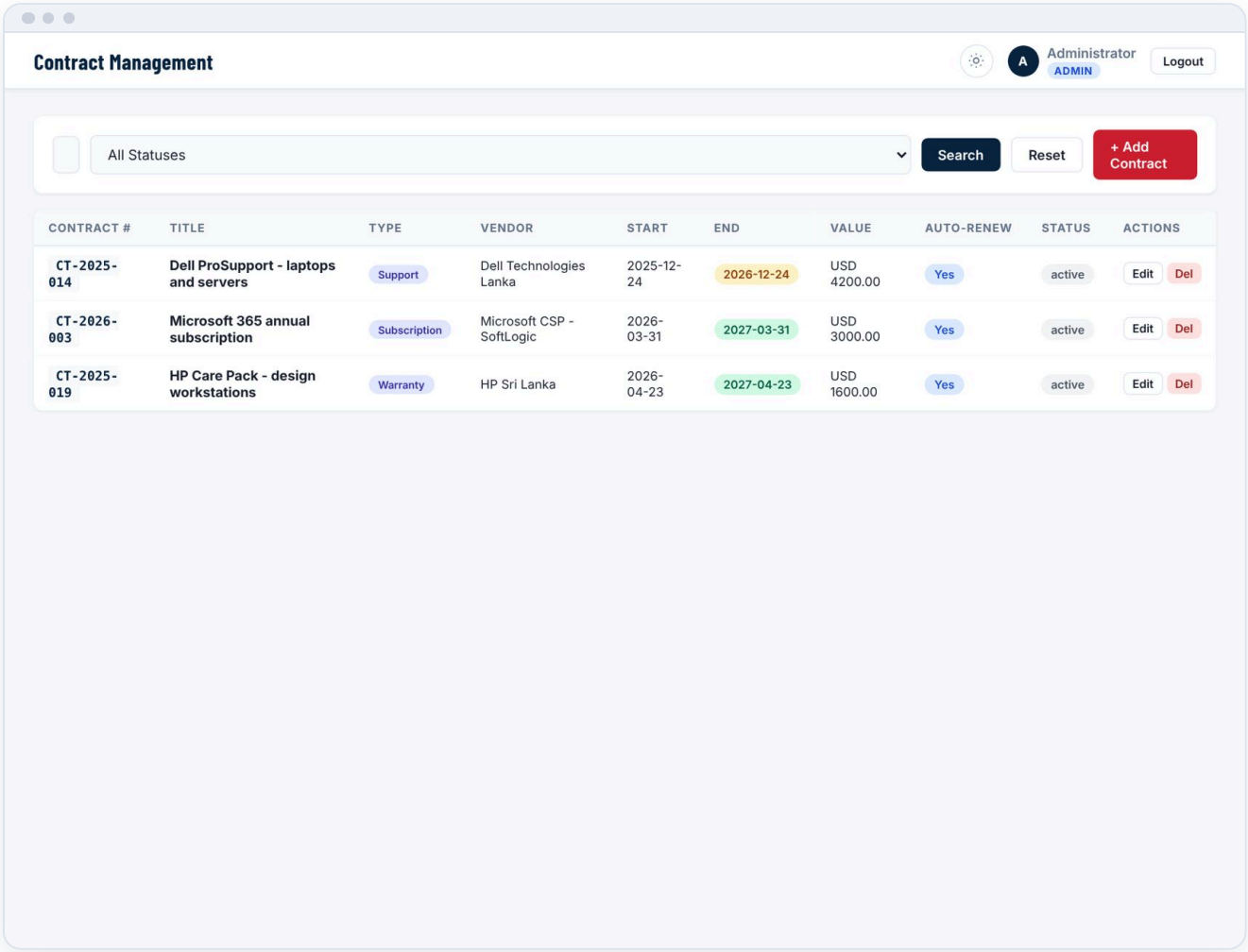
Know what you bought, what is in use and what renews next.



- Seats purchased versus seats in use, with a usage bar per product
- Full and over-used licences flagged in red
- Expiry dates highlighted as they approach; subscription or perpetual; cost per licence

Contracts and warranties

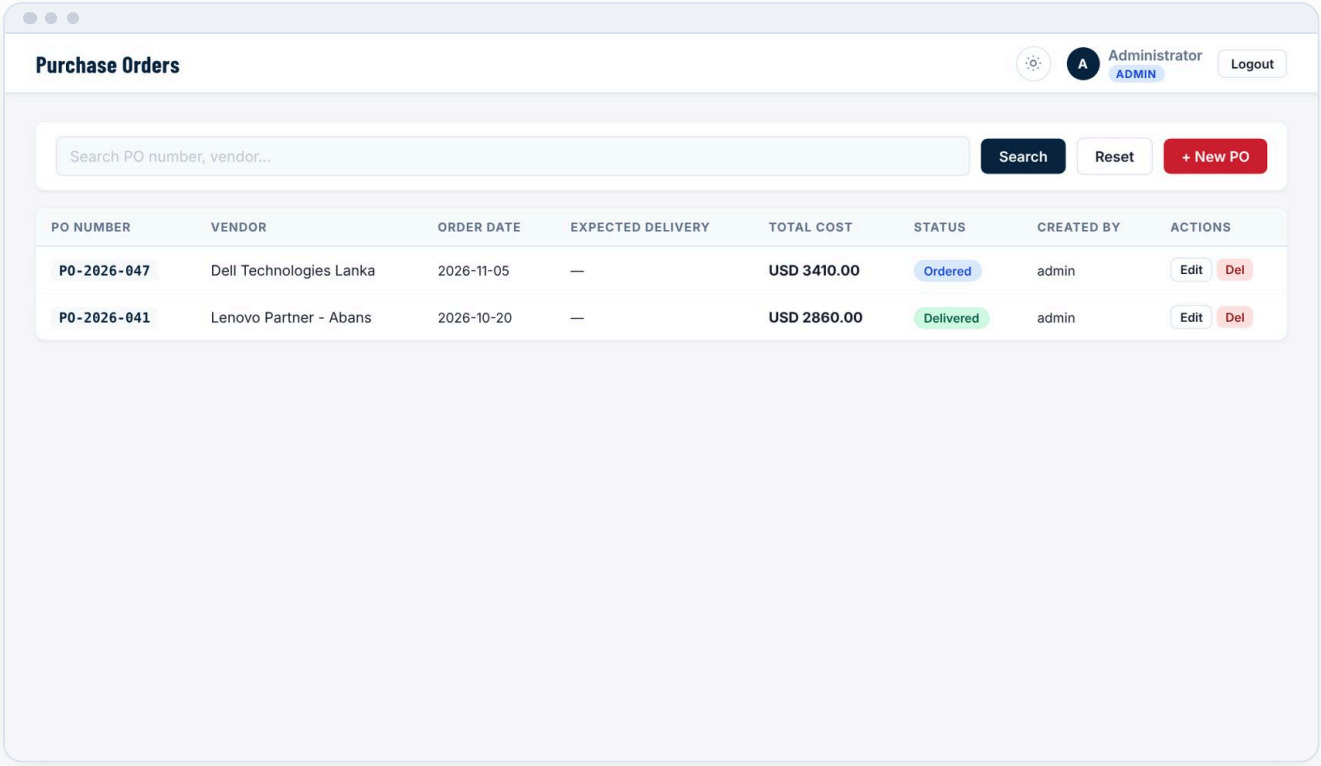
Support, maintenance and warranty contracts with their end dates, so renewals are planned instead of discovered.

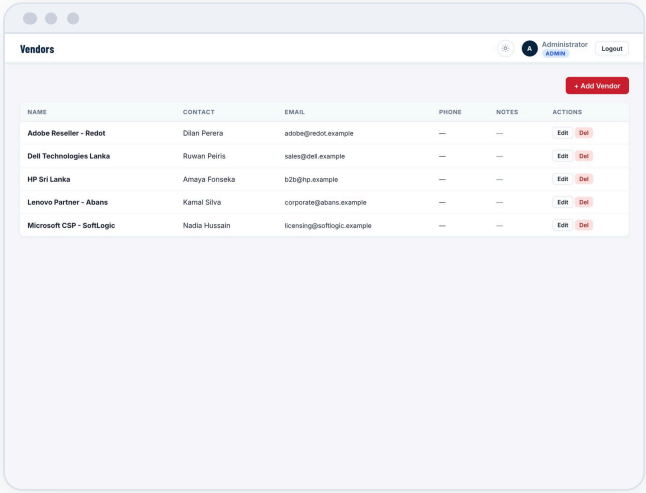


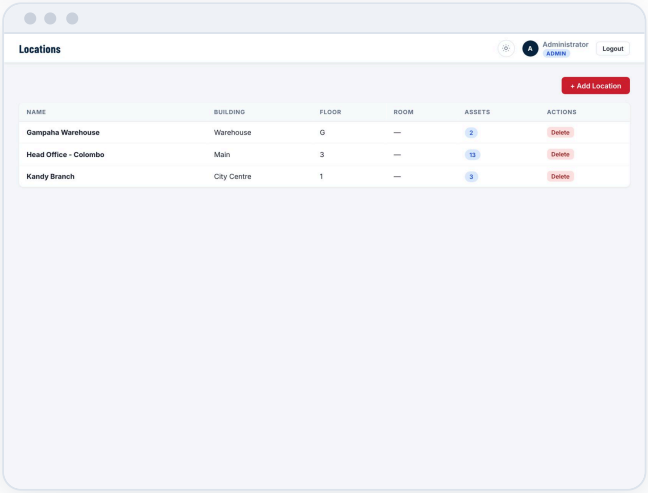
- Type, vendor, start and end dates, value and auto-renew setting
- Contracts ending soon highlighted
- Linked to the vendors you buy from

Purchasing, vendors and locations

Where every asset came from, what it cost and where it is.



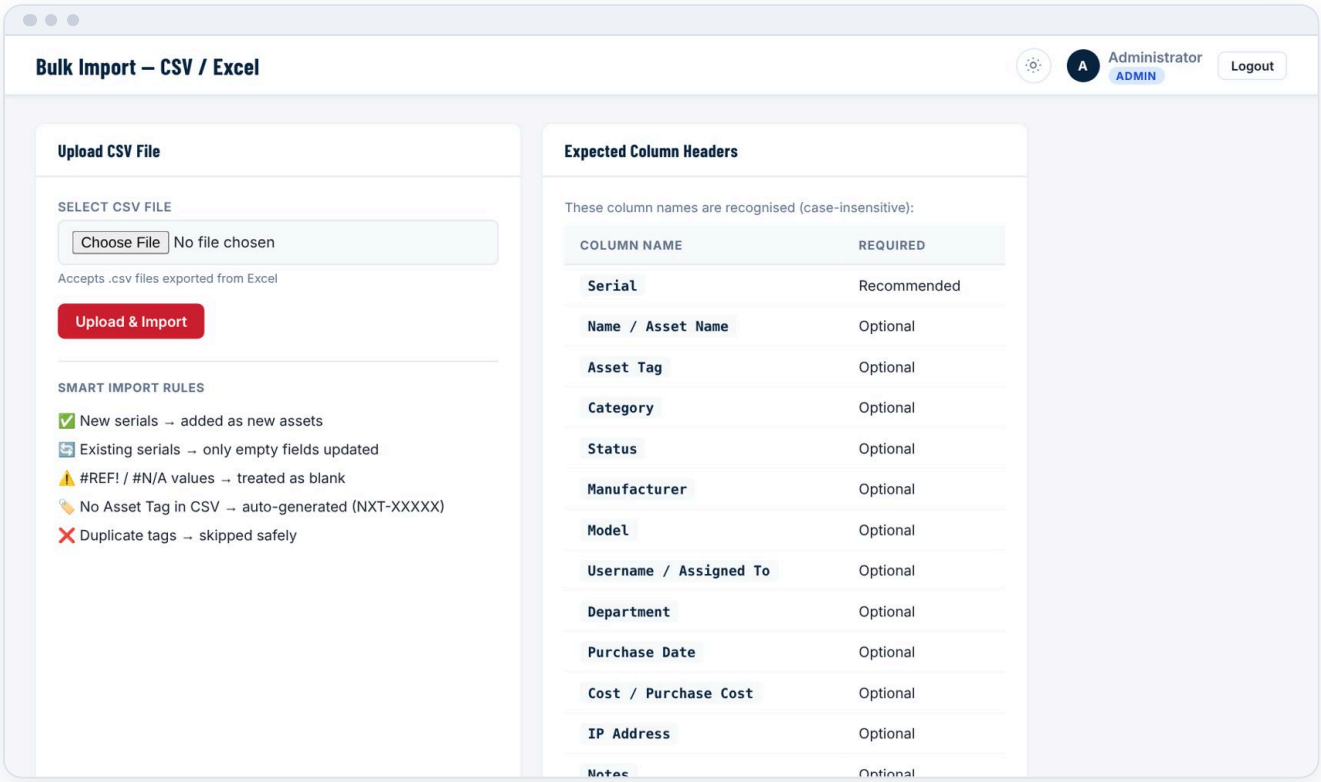


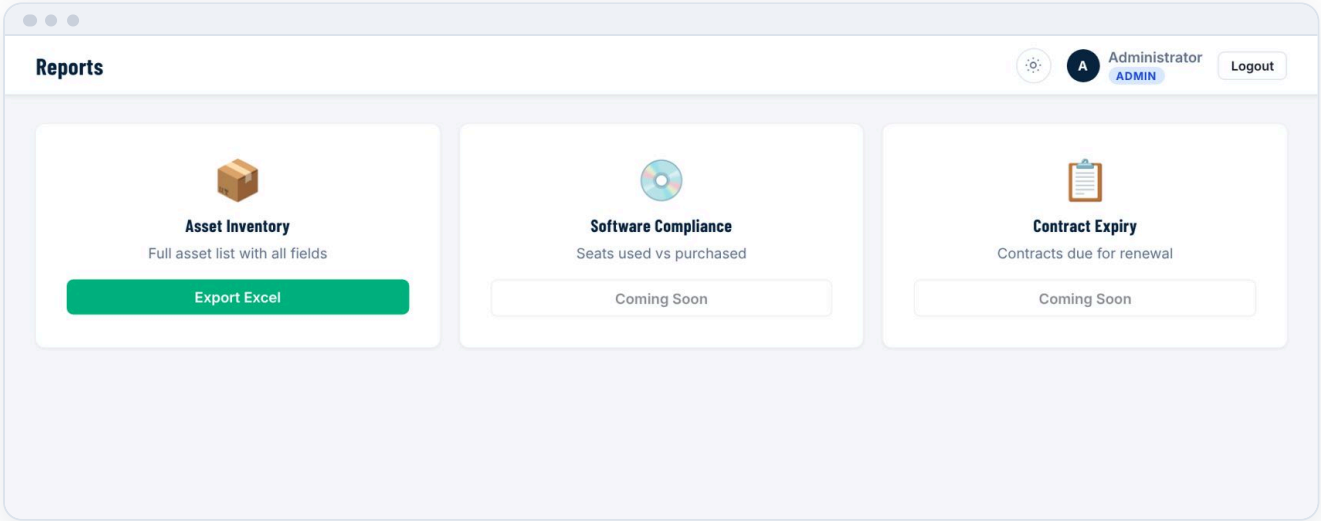


- ✓ Purchase orders with vendor, dates, total and status
- ✓ Vendor list with contacts
- ✓ Locations (warehouses, offices, branches) with the number of assets at each

Bulk import and reports

Bring in the spreadsheet you use today, and take reports out.

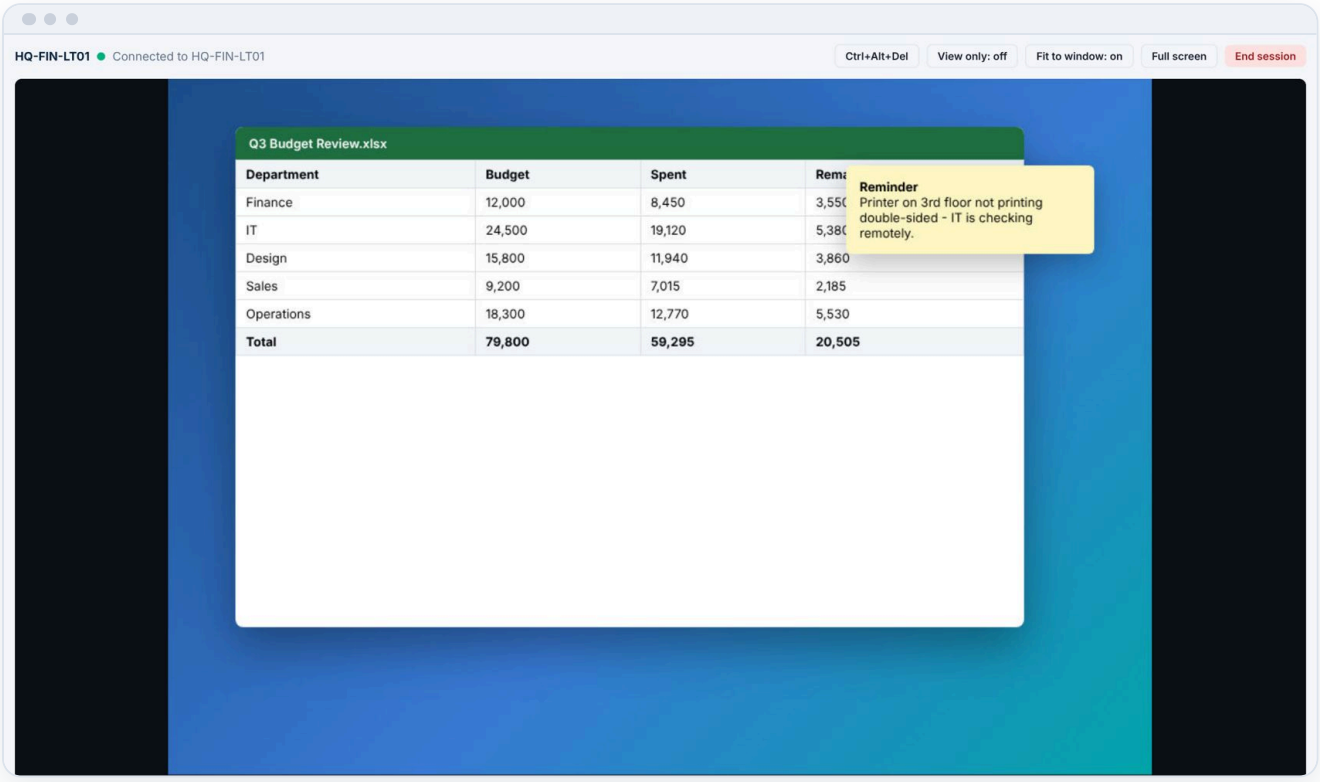


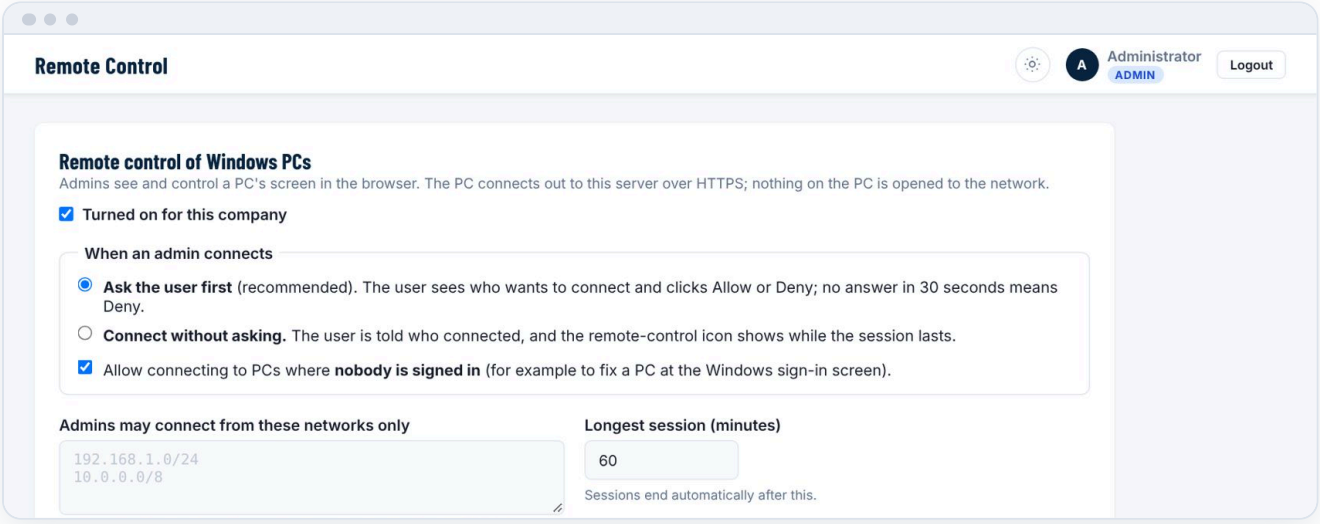


- Import a CSV or Excel file; existing serial numbers are updated, not duplicated
- Clear column guide and a summary of what was added, updated and skipped
- Asset inventory export to Excel

Remote support

Open any online Windows PC's screen from its page, in a browser tab. Nothing to install on the technician's PC.

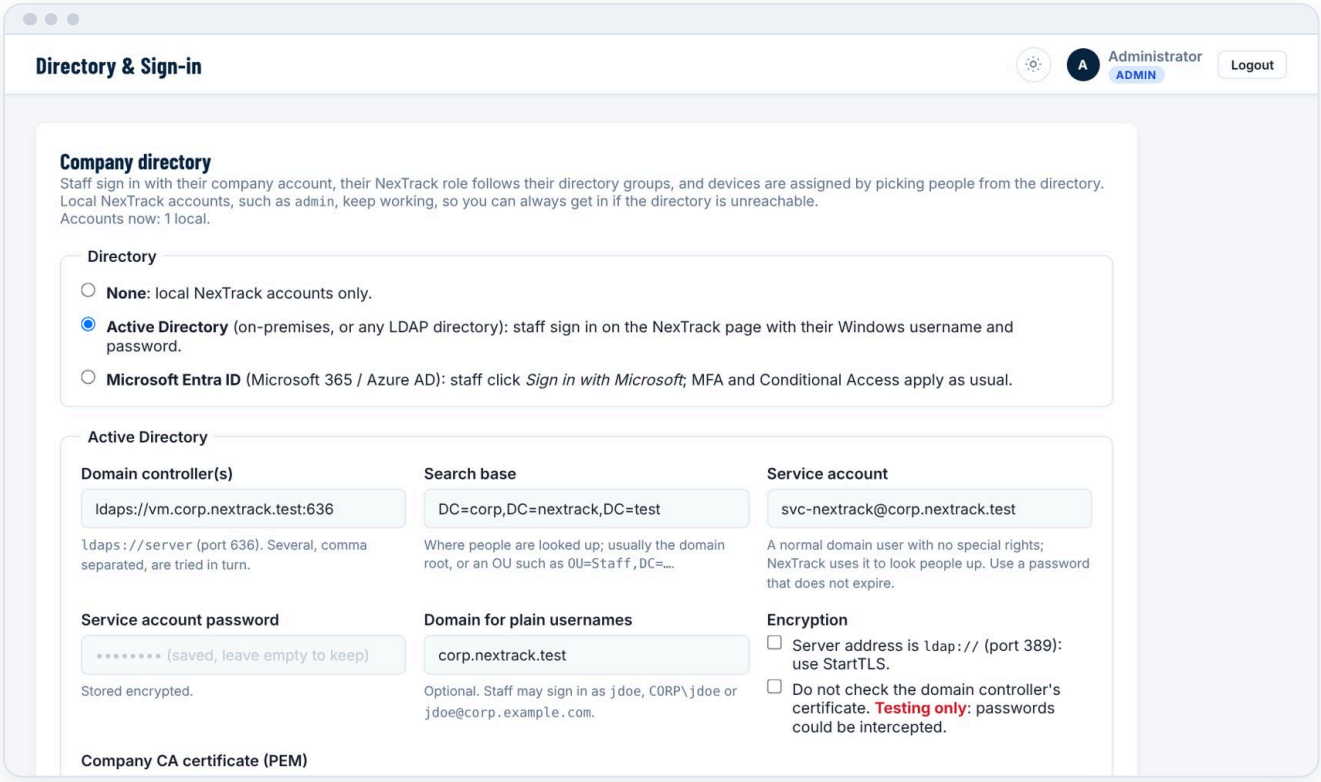


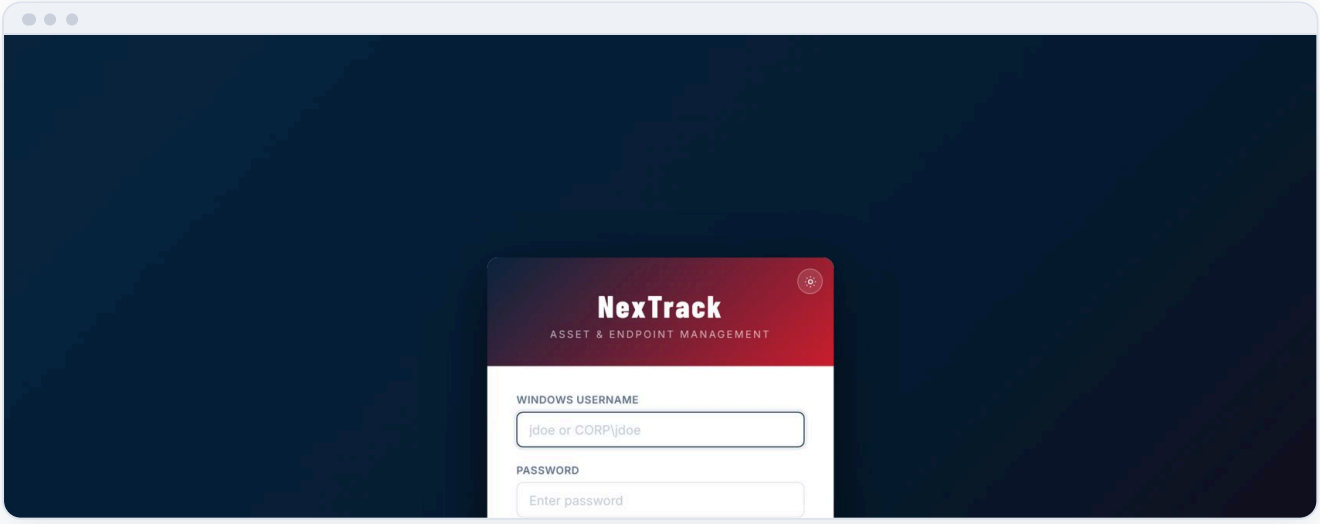


- Encrypted through your own NexTrack server over HTTPS; the PC opens no inbound ports
- Your company decides: the user accepts each session, or sessions start without a prompt for unattended PCs
- Ctrl+Alt+Del, view-only mode, full screen; sessions end automatically after a time limit
- Admins can be limited to connecting from chosen networks; every session is in the audit log

Company sign-in

Staff sign in with their Windows or Microsoft 365 account; NexTrack follows your directory.

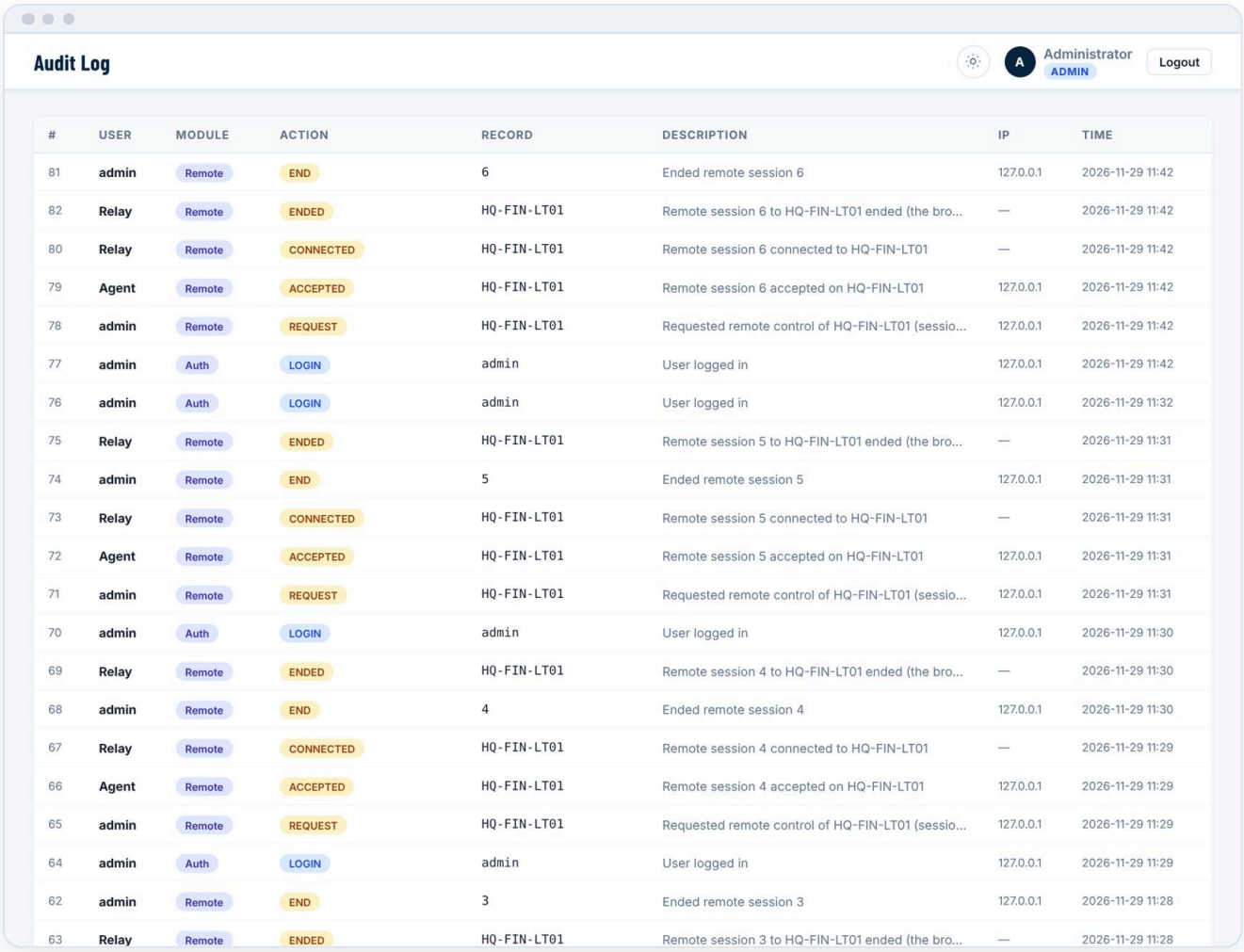




- Active Directory over encrypted LDAPS, or Microsoft Entra ID with "Sign in with Microsoft" (MFA applies)
- Roles from directory groups: Administrators, Staff, Read-only; nested groups count
- Accounts disabled in the directory lose access within 15 minutes
- Connection test checks the server, certificate, service account and each group; a local admin always works

Roles and audit log

Who did what, and when.

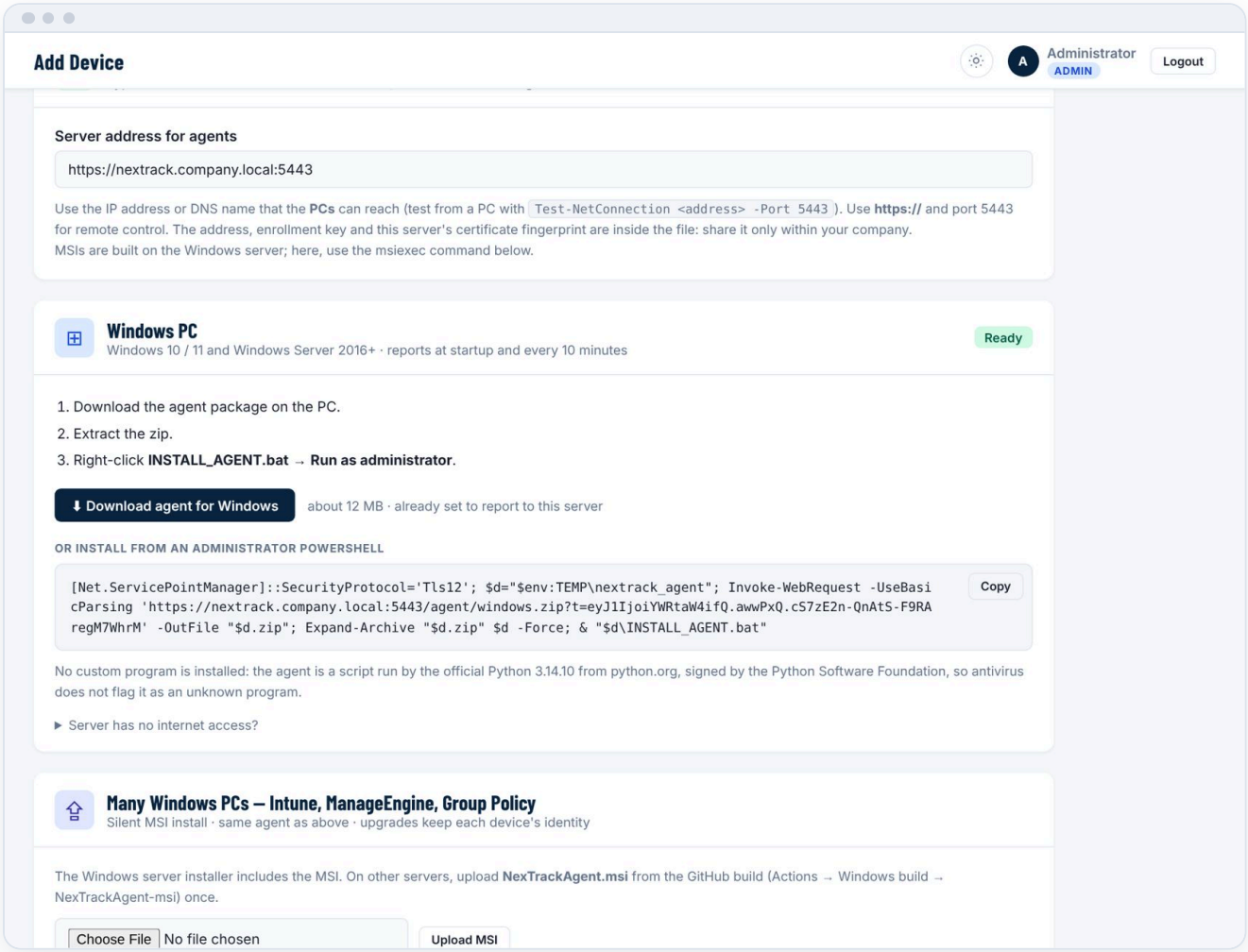


#	USER	MODULE	ACTION	RECORD	DESCRIPTION	IP	TIME
81	admin	Remote	END	6	Ended remote session 6	127.0.0.1	2026-11-29 11:42
82	Relay	Remote	ENDED	HQ-FIN-LT01	Remote session 6 to HQ-FIN-LT01 ended (the bro...	—	2026-11-29 11:42
80	Relay	Remote	CONNECTED	HQ-FIN-LT01	Remote session 6 connected to HQ-FIN-LT01	—	2026-11-29 11:42
79	Agent	Remote	ACCEPTED	HQ-FIN-LT01	Remote session 6 accepted on HQ-FIN-LT01	127.0.0.1	2026-11-29 11:42
78	admin	Remote	REQUEST	HQ-FIN-LT01	Requested remote control of HQ-FIN-LT01 (sessio...	127.0.0.1	2026-11-29 11:42
77	admin	Auth	LOGIN	admin	User logged in	127.0.0.1	2026-11-29 11:42
76	admin	Auth	LOGIN	admin	User logged in	127.0.0.1	2026-11-29 11:32
75	Relay	Remote	ENDED	HQ-FIN-LT01	Remote session 5 to HQ-FIN-LT01 ended (the bro...	—	2026-11-29 11:31
74	admin	Remote	END	5	Ended remote session 5	127.0.0.1	2026-11-29 11:31
73	Relay	Remote	CONNECTED	HQ-FIN-LT01	Remote session 5 connected to HQ-FIN-LT01	—	2026-11-29 11:31
72	Agent	Remote	ACCEPTED	HQ-FIN-LT01	Remote session 5 accepted on HQ-FIN-LT01	127.0.0.1	2026-11-29 11:31
71	admin	Remote	REQUEST	HQ-FIN-LT01	Requested remote control of HQ-FIN-LT01 (sessio...	127.0.0.1	2026-11-29 11:31
70	admin	Auth	LOGIN	admin	User logged in	127.0.0.1	2026-11-29 11:30
69	Relay	Remote	ENDED	HQ-FIN-LT01	Remote session 4 to HQ-FIN-LT01 ended (the bro...	—	2026-11-29 11:30
68	admin	Remote	END	4	Ended remote session 4	127.0.0.1	2026-11-29 11:30
67	Relay	Remote	CONNECTED	HQ-FIN-LT01	Remote session 4 connected to HQ-FIN-LT01	—	2026-11-29 11:29
66	Agent	Remote	ACCEPTED	HQ-FIN-LT01	Remote session 4 accepted on HQ-FIN-LT01	127.0.0.1	2026-11-29 11:29
65	admin	Remote	REQUEST	HQ-FIN-LT01	Requested remote control of HQ-FIN-LT01 (sessio...	127.0.0.1	2026-11-29 11:29
64	admin	Auth	LOGIN	admin	User logged in	127.0.0.1	2026-11-29 11:29
62	admin	Remote	END	3	Ended remote session 3	127.0.0.1	2026-11-29 11:28
63	Relay	Remote	ENDED	HQ-FIN-LT01	Remote session 3 to HQ-FIN-LT01 ended (the bro...	—	2026-11-29 11:28

- ✓ Admin, Staff and Read-only roles
- ✓ Every sign-in, change, agent enrollment and remote session written to the audit log
- ✓ Each PC has its own credential: one lost or retired device can be revoked without touching the others

Rolling out the agent

One ready-made installer with your server inside, deployed the way your company already deploys software.



- Build MSI: enter your server address and download an agent with the address, key and certificate inside
- Group Policy installs it on every domain PC at start-up; no ports opened on the PCs. Intune and ManageEngine also work
- Domain Deployer app (optional): finds the PCs of your domain and installs the agent where it is missing
- Linux: one command from the Add Device page

SECURITY

Security and privacy

Built for the people who answer to auditors: your data stays with you, and every machine and every action is accounted for.

Your data stays on your server

Inventory, users and remote sessions are stored only on the NexTrack server you run. Nothing is sent to NexSuite.

Encrypted everywhere

Agents, browsers and remote sessions use HTTPS. Agents check the server by its certificate fingerprint, built into the ready-made MSI.

One credential per PC

After its first report, each PC gets its own token. A lost or retired PC can be revoked on its own; a revoked PC cannot enroll again.

No inbound ports on PCs

Agents only connect out to your server. Remote control runs through the server too, so no PC listens on the network for it.

Directory-backed access

Sign-in with Active Directory (LDAPS) or Entra ID; roles from groups; disabled accounts lose access within 15 minutes.

Full audit trail

Sign-ins, changes, enrollments and remote sessions are logged with user, time and address. Secrets are stored encrypted.

What the agent collects: hardware details, serial number, network addresses, the logged-in user and the list of installed software. It does not read documents, browsing history or keystrokes.

EDITIONS

Editions and requirements

Every edition includes every feature in this guide. Editions differ only by the number of devices.

Free	Starter	Business	Enterprise
$0	**$29**/month	**$99**/month	**Custom**
up to 25 devices	up to 100 devices	up to 500 devices	unlimited devices

Prices in US dollars, excluding local taxes. Upgrading is a licence key: nothing is reinstalled and no data is lost.

Requirements

Server	Windows Server 2019 or 2022 (physical or virtual), or Ubuntu Linux. The installer sets up the database, HTTPS and the service.
Windows PCs	Windows 10, Windows 11 and Windows Server 2016 or later, 64-bit. Remote support for Windows PCs.
Linux machines	Ubuntu, Debian, RHEL, Rocky, Alma, CentOS 7+ and SUSE (inventory).
Network	PCs reach the server on HTTPS (port 5443 on Windows). No ports are opened on the PCs.
Directory (optional)	Active Directory with LDAPS, or Microsoft Entra ID (Microsoft 365).
Browser	Any current browser: Edge, Chrome, Firefox or Safari.

Try it on your own network

Free for up to 25 devices, or book a 30-minute demo.

getnexsuite.com
sales@getnexsuite.com