MTech ScanFind

Network Discovery Pro

Comprehensive Manual

The complete reference

First Edition · 2026

sales@mtpsite.com

Disclaimer

Important — please read before using this application.

MTech ScanFind (the "Application") is provided "AS IS", WITHOUT WARRANTY OF ANY KIND, express or implied, including but not limited to the warranties of merchantability, fitness for a particular purpose, title, non-infringement, and the absence of latent or other defects, whether or not discoverable.

By installing, running, or otherwise using the Application you acknowledge and agree to the following terms:

- USE AT YOUR OWN RISK. The Application interacts directly with your network, your IP cameras, your NVRs / DVRs, and the operating system on the computer it runs on. Every action you perform with it — running a scan, changing a camera IP, changing a camera password, rebooting a device, modifying firmware-level settings, adding a temporary network alias, opening RTSP streams — is initiated by you and executed on your equipment at your sole risk.
- NO RESPONSIBILITY FOR LOSS OR DAMAGE. MTech, its officers, employees, contractors, partners, distributors and resellers shall NOT be liable for any direct, indirect, incidental, special, exemplary, punitive, or consequential damages whatsoever — including, without limitation, loss of profits, loss of data, loss of use, loss of recorded video, loss of business, business interruption, equipment damage, equipment lockout, account lockout, security exposure, downtime, personnel costs, replacement costs, or any other loss — arising out of or in any way connected with the use of, or inability to use, the Application, whether based on warranty, contract, tort (including negligence), strict liability, or any other legal theory, and whether or not MTech has been advised of the possibility of such damages.
- NO WARRANTY. MTech does not warrant that the Application will be uninterrupted, error-free, secure, compatible with every device or every firmware revision, free of viruses or other harmful components, or that defects will be corrected. MTech does not warrant the accuracy or completeness of any output the Application produces, including but not limited to scan results, vendor identification, manufacturer attribution, model / firmware / serial detection, online / offline status, port scan output, or any export or report file.
- DESTRUCTIVE OPERATIONS. Several Application features perform configuration changes on remote devices — Change IP, Bulk Change IP, Bulk Change Password, Reboot, switching cameras to DHCP, and similar — that are difficult or impossible to reverse without physical access to the affected device. You are solely responsible for verifying every parameter before applying any such change and for maintaining adequate backups, written records and offline recovery procedures for every device you manage with the Application.
- CREDENTIALS AND SECURITY. The Application stores camera credentials in plain text on the local file system (camera_creds.json) because ONVIF and HTTP digest authentication require the raw password to compute their hashes. You are solely responsible for protecting access to that file, for your network's overall security posture, and for any consequences arising from credential compromise.
- VENDOR DEFAULT CREDENTIALS. The Application bundles a reference list of factory-default credentials for many camera vendors. This list is provided strictly for legitimate administration of equipment you own or are authorised to manage. Unauthorised access to a device you do not own is illegal in most jurisdictions. You assume full responsibility for the lawful use of this information.
- NETWORK INTERACTIONS. The Application sends ARP, UDP broadcast, multicast, ICMP, and TCP traffic on every detected subnet, and may add temporary IP aliases to your network adapters when running as Administrator. These actions may trigger intrusion-detection, security-information-and-event-management (SIEM), or other monitoring systems. Coordinate with your network operations team and observe all applicable usage policies before running scans on networks you do not own.
- THIRD-PARTY EQUIPMENT. MTech is not the manufacturer of, and has no affiliation with, the camera vendors named in this Application (Hikvision, Dahua, Uniview, Axis, Hanwha / Samsung, Bosch, Sony, Pelco, and any other brand). Vendor names appear solely for the purpose of device identification and

interoperability. Each vendor's name and trademarks remain the property of their respective owners. The Application does not imply endorsement by or partnership with any vendor.

- ACCEPTANCE OF TERMS. By launching the Application even once you indicate that you have read, understood, and agreed to be bound by every term of this disclaimer. If you do not agree, you must uninstall the Application and discontinue all use immediately.

USE AT YOUR OWN RISK. NO WARRANTY. AS IS.

About this manual

This is the complete reference for MTech ScanFind — Network Discovery Pro. Every feature, dialog, button and setting in the application is documented here, organised in 10 parts.

If you're new to MTech ScanFind, start with the companion Quick Start Guide (MTech_ScanFind_Quick_Start_Guide.docx). That book gets you to your first useful scan in under ten minutes. This book is the long-form reference you keep open on the second monitor.

Who this book is for

- **Security integrators** — commissioning new sites and re-IPing groups of cameras.
- **IT operators** — managing a mixed estate of cameras, switches, and access controllers.
- **Installers** — auditing existing deployments before warranty renewals.
- **End users** — running a small CCTV install at home or in a small business.

How this book is organised

Part	Topic	Chapters
I	Getting started	1–3
II	Core workflows	4–7
III	Camera management	8–10
IV	Visualisation	11–12
V	Network analysis	13
VI	Help and database	14–16
VII	Apps and integration	17–18
VIII	Settings	19
IX	Advanced topics	20–21
X	Reference and troubleshooting	22–24

> **Tip:** Cross-references throughout the book point to chapter numbers, not page numbers, so they survive re-flow.

Contents

Part I — Getting started

The first three chapters cover everything a new user needs to be productive: installation, the splash and licensing, and a guided tour of the main window.

Chapter 1 — Installation

Distribution package

MTech ScanFind is delivered as a single 64-bit Windows executable ("MTech ScanFind.exe") plus two optional folders:

- **apps/** — drop in additional .exe tools you want to launch from inside MTech ScanFind. They appear on the APPs tab once enabled.
- **ext/** — drop in Python helper scripts renamed to .dll. They appear on the Others tab.

Both folders are created automatically next to the .exe on the first launch if they don't exist. No installer is needed — just copy the .exe to wherever you want it and double-click.

System requirements

Requirement	Minimum	Recommended
Operating system	Windows 10 64-bit	Windows 11 64-bit
CPU	Dual-core 2 GHz	Quad-core 2.5+ GHz
RAM	4 GB	8 GB or more
Disk	150 MB	1 GB (for exports / logs)
Network	100 Mbit Ethernet	Gigabit wired
Privileges	Standard user	Run as Administrator

> **Tip:** Run-as-Administrator is required for cross-subnet IP changes (the "subnet trick" alias), for port scans on privileged ports below 1024, and for any operation that modifies a network-adapter alias.

Files written next to the executable

The app keeps its state in the folder containing the .exe. After running a scan, you'll see these files appear:

File	Purpose
camera_creds.json	Per-camera username / password / port / device-type / channel.
custom_manufacturers.json	Your additions to the OUI brand database.
device_locations.json	Per-IP location labels.
floor_plans.json	Floor-plan image paths and pin positions.
apps_config.json	List of enabled apps for the APPs tab.
site_<gateway>_network_map_pos.json	Saved Network Map layout for each site.
change_ip_debug.log	Detailed log of every IP-change attempt.
change_ip_log.txt	Concise log of browser-mediated IP changes.
network_scan_log.txt	Scan history.

⚠ **Warning:** Back up these files before reinstalling or moving the app to a new PC. They contain all your site-specific configuration.

Chapter 2 — First launch and licensing

The splash screen

Every launch starts with a small dark popup window centred on the screen. Inside, the word "MTech" in 36-point bold bounces around the canvas DVD-screensaver style, cycling through seven brand colours (gold, mint, blue, pink, peach, teal, violet) every time it hits a wall.

Figure: The splash screen showing the bouncing MTech logo

The splash auto-closes after 3 seconds. Click anywhere on the popup or hit any key to dismiss it early. The main window is withdrawn during the splash, so you don't see it flicker.

Trial mode

On the very first launch on a new PC, the app starts in 30-day trial mode with full access to every feature. A yellow banner below the main header tracks the days remaining.

1. When the trial expires, the banner turns red and most actions are disabled (you can still read the database and view saved data).
2. Click the trial banner — or open the License panel from the Help menu — to copy your hardware ID and email it to sales@mtpsite.com.
3. Paste the returned license code into the activation panel and click Activate. The banner turns green and full access returns.

Full licensing details are in ACTIVATION_README.pdf next to the .exe.

Chapter 3 — Tour of the main window

The header (top)

The deep-navy strip across the top of the window shows the app branding on the left and your PC's local IP addresses on the right.

Figure: The header strip. The IP values are rendered in gold so they're easy to read at a glance.

Each network adapter appears with its type (Eth or WiFi) and its current IPv4 address. Labels use a muted blue-grey; IP values pop in gold. Double-click anywhere on the IP block to open the full ipconfig output in a popup window — useful for diagnosing multi-NIC machines.

The toolbar

Directly beneath the header is the toolbar — the same on every tab.

Button / Element	Description
Run Scan	Discover every device on every enabled subnet.
Stop	Cancel a scan in progress. Already-found devices are kept.
Progress bar	Tracks the scan as it moves through subnets.
Status text	Shows the current operation in blue.
Web	Open the selected device's HTTP page in Edge / Chrome.
Ports	Run a port scan on the selected device.
Snap	Capture a single RTSP frame from the selected camera.
Reboot	Send an ONVIF reboot to the selected camera(s).
CSV	Export the current Network Inventory to a CSV file.

The sidebar (left)

The dark sidebar is the primary navigation. Each item maps to one of the main tabs.

Icon	Tab	Chapter
▯	Dashboard	4-6
▯	Network Map	11
▯	Location Map	12
▯	Ports	13
▯	Others	17
▯	APPs	18
▯	Help	14-16

Icon	Tab	Chapter
⚙	Settings	19

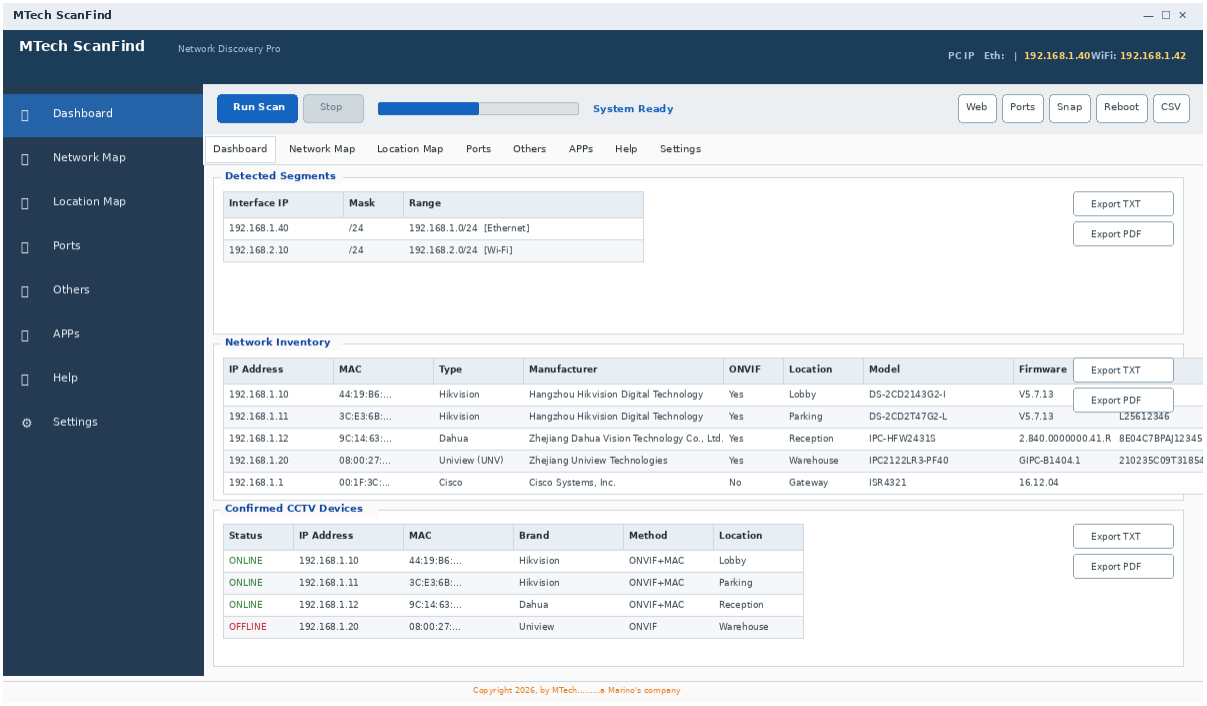


Figure: The main window — sidebar on the left, dashboard panes on the right, top toolbar, footer copyright

Part II — Core workflows

Part II is the meat of the application: scanning the network, reading and managing inventory rows, watching live video, and the right-click context menus.

Chapter 4 — Running a scan

The scan engine in detail

When you click Run Scan, MTech ScanFind starts six discovery methods in parallel, each in its own background thread:

1. Subnet enumeration

Every network adapter is queried for its assigned IPv4 addresses. Each address yields a /24 subnet (the most common case in CCTV installs). Loopback and link-local addresses are skipped.

Detected segments appear in the Detected Segments panel at the top of the dashboard. Segments you've disabled in Settings → Scan Segments don't appear at all.

2. ARP broadcast

For each enabled subnet, a series of ARP "who-has" packets is broadcast in 256-IP chunks. Every responsive host appears in the inventory with its MAC. ARP is L2 and bypasses ACLs, firewalls and routing — it's the fastest, most reliable discovery method on a flat LAN.

3. Passive Layer-2 sniff

In parallel with the active ARP probes, a 5-second packet sniff captures every ARP and IP frame seen on the wire. On managed switches that flood broadcast traffic, this catches devices on other VLANs that would otherwise be invisible. Source MACs are deduplicated against the ARP findings.

4. Proprietary vendor broadcasts

A UDP broadcast pass speaks the discovery dialects of every major CCTV brand: Hikvision SADP, Dahua/Amcrest/Lorex, Uniview EZTools, Reolink, Vivotek, TP-Link VIGI, Hanwha, Pelco, Axis VAPIX, Bosch / Sony / Panasonic SSDP, Mobotix, Avigilon.

Cameras that answer these proprietary probes are added with an OUI-matched brand even if ARP missed them (cameras with strict ACLs sometimes ignore ARP but reply to their vendor probe).

5. ONVIF WS-Discovery

A standards-compliant ONVIF multicast probe is sent on every interface that has an IPv4 address. Cameras that implement ONVIF (the vast majority of modern IP cameras) reply with their service URLs. This catches devices across routed boundaries since multicast may traverse VLAN routers.

6. TCP fallback probe

After the ARP / sniff / proprietary passes, every IP that did NOT respond gets a parallel TCP probe on the common camera ports (80, 443, 22, 23, 8080, 8443). A successful TCP connection forces the OS to ARP-resolve the host, so we then read the MAC from the OS ARP cache.

Final verification pass

After all six methods finish, a final ICMP / TCP verification pass pings every device. Devices that don't respond (and didn't come from a direct ONVIF unicast reply) are dropped. This eliminates phantom devices left over from stale ARP-cache entries.

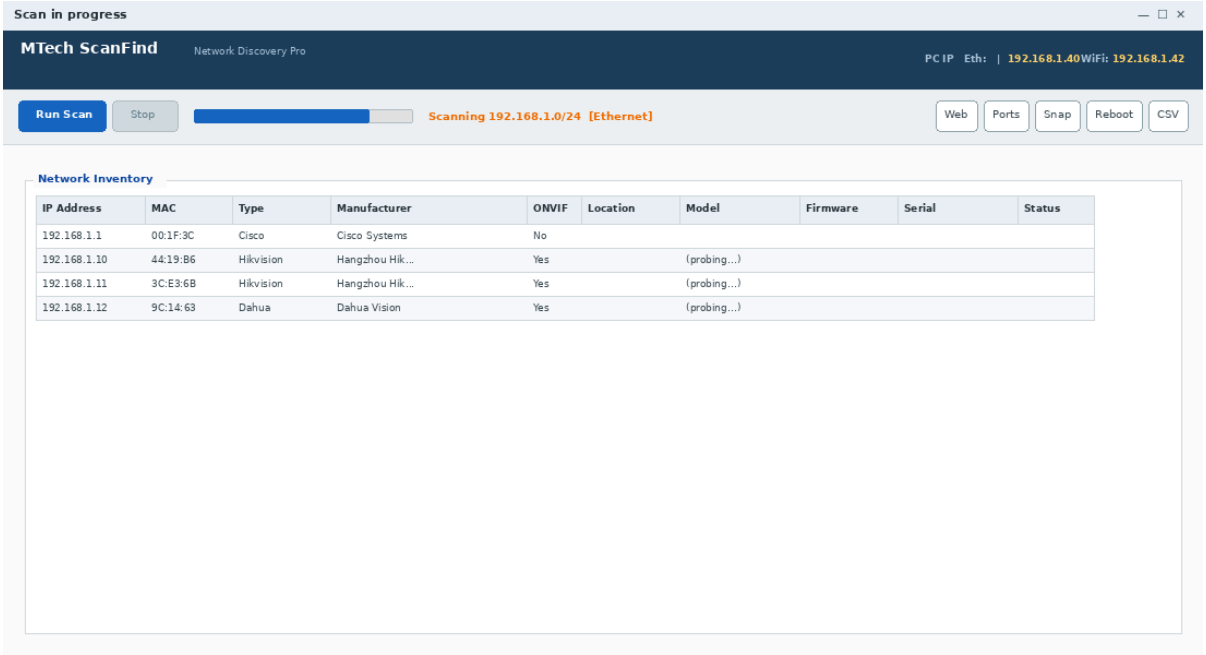


Figure: Mid-scan: devices appear as soon as they're found, Model / Firmware / Serial fill in afterwards

Background enrichment

Within 200 milliseconds of the scan finishing, a background enrichment task starts:

4. Phase 1 (~1 sec): Parallel ping + TCP probe of every device marks each row ONLINE (green) or OFFLINE (red). Status mirrors into both the Network Inventory and the Confirmed CCTV trees from the same ping result.
5. Phase 2 (varies): ONVIF GetDeviceInformation runs against every alive device, trying saved credentials first, then admin/blank. Successful responses fill the Model, Firmware and Serial columns.
6. Phase 3 (varies): For devices ONVIF couldn't authenticate, vendor-specific HTTP endpoints are tried. Hikvision/Annke/HiLook → /ISAPI/System/deviceInfo. Dahua/Amcrest/Lorex → magicBox.cgi. Axis → /axis-cgi/param.cgi.
7. Phase 4: As a last resort, the HTTP Server: header is read. The raw banner text ("Hikvision-Webs", "DNVRS-Webs", "App-webs/", "Mongoose/Dahua") lands in the Model column so even routers, switches and printers get some identifying string.

Tip: The enrichment never tries more than 6 credentials per host. This stays well below the 7-failures-in-30-minutes threshold that triggers Hikvision's user-lockout policy.

Timing expectations

Network size	Approximate scan time
< 20 devices	10–15 seconds
20–100 devices	30–60 seconds
100–250 devices	1–3 minutes
Multi-subnet, > 250	3–10 minutes

Warning: Slow scans on small networks usually mean a misbehaving NIC or a VPN adapter capturing traffic. Disable any active VPN before running CCTV scans.

Chapter 5 — The Dashboard panes in detail

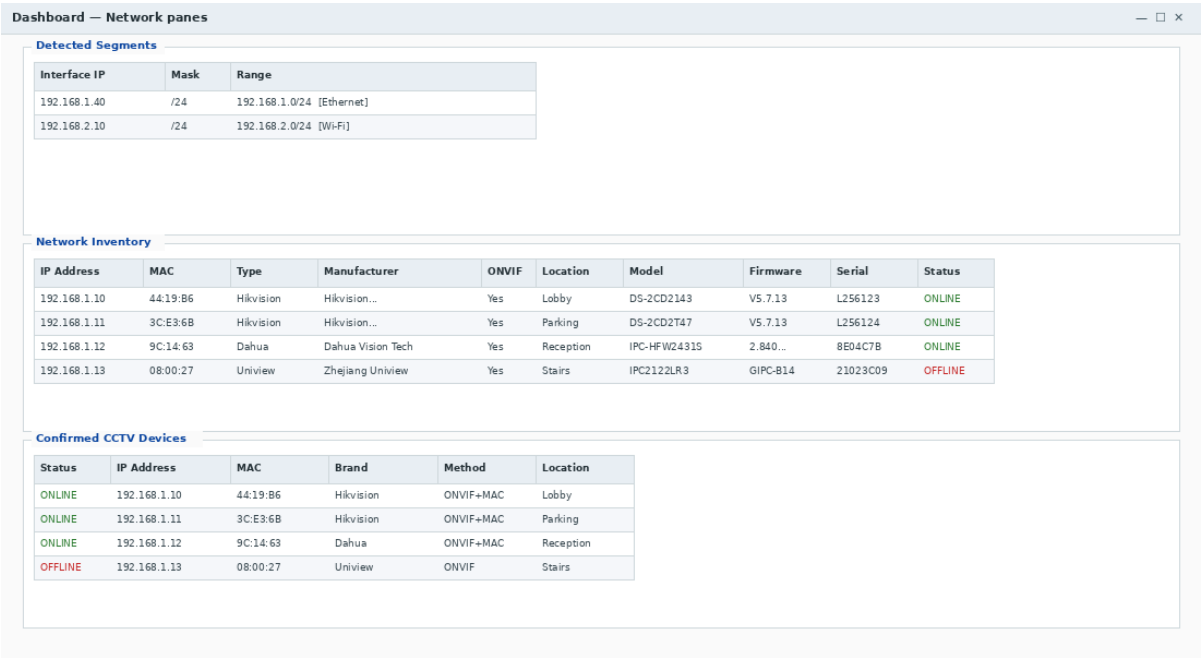


Figure: The dashboard's three panes, top to bottom

Pane 1: Detected Segments

Lists every subnet the scanner found on your network adapters. The columns are:

- **Interface IP** — Your PC's IP on this subnet.
- **Mask** — Subnet mask in CIDR notation (e.g. /24).
- **Range** — Full subnet in dotted-decimal with the interface name.

Right-click any segment to disable / re-enable it for future scans, or double-click to launch a sub-segment scan on a custom range within that subnet.

Pane 2: Network Inventory

The primary inventory list. Every device discovered, with full metadata. Ten columns:

Column	Source	When it fills
IP Address	Scan	Immediately
MAC Address	ARP / sniff	Immediately
Type	OUI brand match	Immediately
Manufacturer	IEEE OUI db	Immediately
ONVIF	ONVIF probe	End of scan
Location	User-assigned	Persistent
Model	ONVIF / vendor HTTP	Background
Firmware	ONVIF / vendor HTTP	Background

Column	Source	When it fills
Serial	ONVIF / vendor HTTP	Background
Status	Live ping monitor	Continuous

Every column is sortable — click the header to sort ascending, click again to reverse. Multi-select is supported (Ctrl + click for individual rows, Shift + click for a range).

Pane 3: Confirmed CCTV Devices

A filtered view containing only devices the scanner positively identified as cameras, NVRs, video encoders, or doorbells. Six columns: Status, IP, MAC, Brand, Method, Location.

The Method column tells you HOW the device was identified:

Method	Means
ONVIF+MAC	Both ONVIF discovery AND OUI match agreed.
ONVIF	Only ONVIF responded — vendor was generic / unknown.
MAC Match	Brand was identified by MAC OUI; ONVIF didn't respond.

The Status column is updated every 10 seconds by the live monitor (more details in Chapter 7).

Chapter 6 — Context menus

Every action you'll perform on a device starts with a right-click on its row. The context menus on the Network Inventory and Confirmed CCTV panes are similar but not identical.

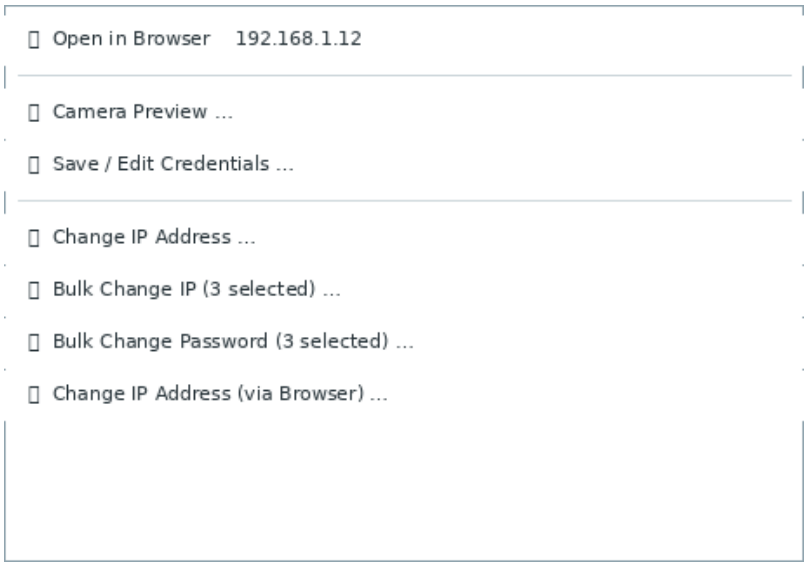


Figure: The right-click context menu on the Network Inventory

Inventory right-click menu

Item	Action
Open in Browser …	Launch the device's HTTP page in Edge.
Camera Preview …	Open live video preview window.
Save / Edit Credentials …	Open per-camera credentials dialog.
Change IP Address …	Single-camera IP-change dialog.
Bulk Change IP (N selected) …	Multi-camera IP change with auto-increment.
Bulk Change Password (N selected) …	Multi-camera password change.
Change IP Address (via Browser) …	Open camera's web admin in a dedicated browser window.

CCTV right-click menu

Same items as above, plus:

- **Open HTTP / Open HTTPS** — Two separate buttons for cameras that serve admin on different ports.
- **Copy IP / Copy MAC** — Clipboard helpers for site documentation.

Tip: Bulk Change IP and Bulk Change Password only appear in the context menu when 2 or more rows are selected — they're greyed out otherwise.

Chapter 7 — Live monitoring

How status is maintained

A background thread polls every camera in the Confirmed CCTV list every 10 seconds with a single ICMP ping. Results update the Status column in real time:

- **ONLINE** — Camera replied to ping within 500 ms. Row tag is green.
- **OFFLINE** — Camera failed to reply. Row tag is red.

The same monitor mirrors its results into the Network Inventory Status column, so both panes stay in sync.

Offline alerts

When the monitor detects a camera transitioning ONLINE → OFFLINE, and the alert is enabled in Settings → Alerts & Notifications, a popup appears listing every camera that just went offline. Cameras that were already offline at start-up don't trigger the alert (the monitor seeds its state cache from the post-scan ping pass to avoid false alarms).

Part III — Camera management

Part III covers the destructive workflows: changing camera IPs, changing passwords, and managing per-camera credentials.

Chapter 8 — Live camera preview

MTech ScanFind has a built-in live RTSP viewer. You don't need VLC, Smart PSS, IVMS-4200, or any other third-party tool.

Opening the preview

Right-click any camera and choose Camera Preview…. A new window opens, the body shows "Connecting…", and within 1–3 seconds live video starts streaming.

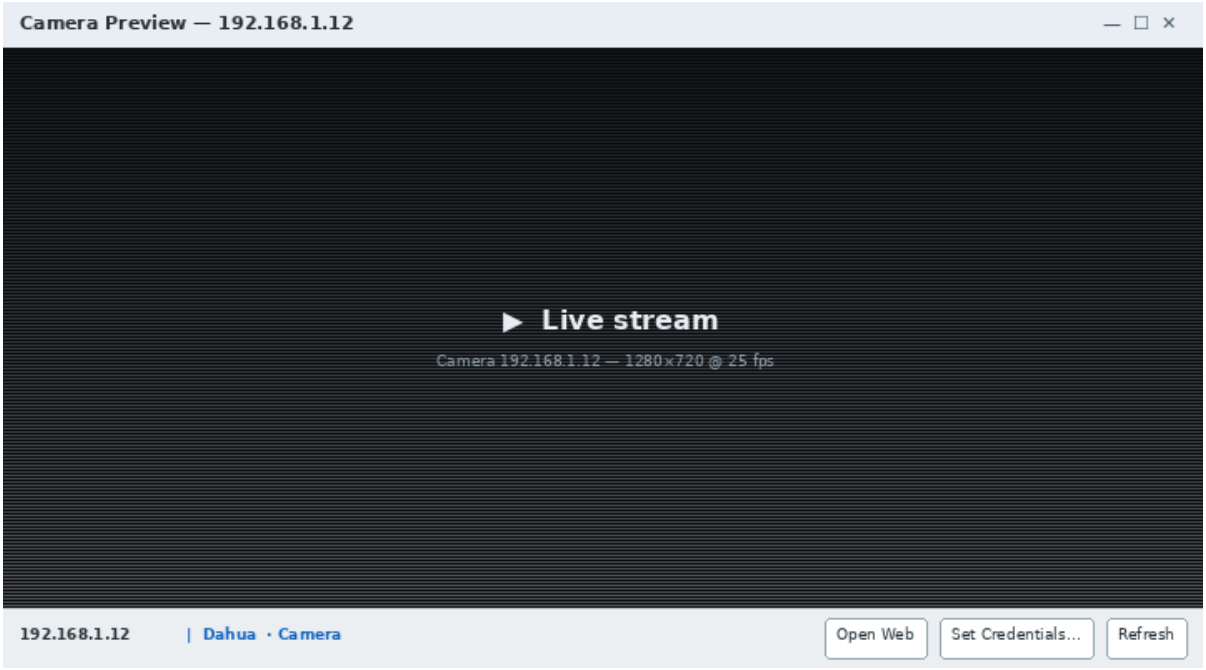


Figure: The Camera Preview window with a live stream running

Credential discovery

Before the stream starts, the worker thread runs through a credential discovery sequence:

8. Try the last known good RTSP URL (the working_url cached in camera_creds.json). If a frame returns, jump straight to streaming.
9. Try ONVIF GetProfiles using saved credentials, on each of the five common ONVIF ports (80, 8000, 8080, 2020, 8899).
10. Try ONVIF with vendor default credentials (see Chapter 14 for the full list).
11. Try the camera's RTSP server directly using vendor-known URL patterns (Hikvision /Streaming/Channels/101, Dahua /cam/realmonitor?channel=1&subtype=0, Axis /axis-media/media.amp, etc.)
12. If everything fails, the credentials dialog opens automatically.

The credentials dialog

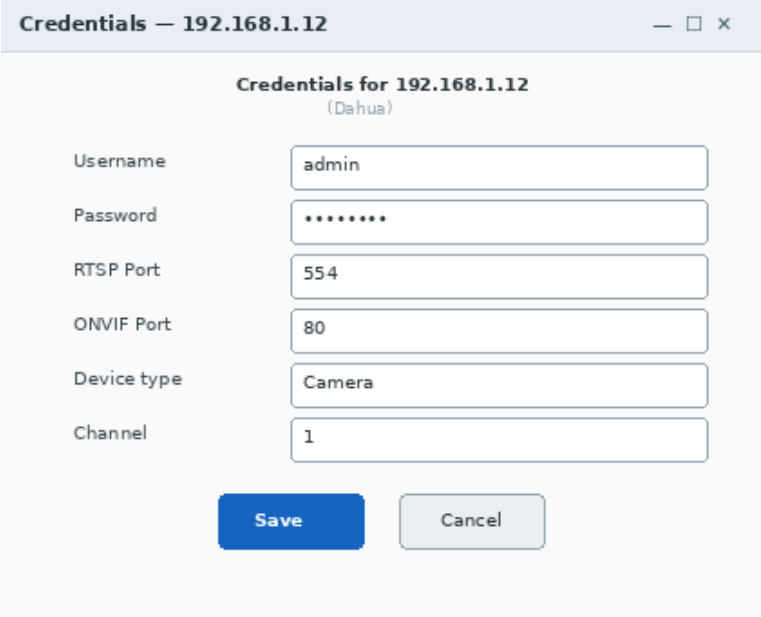


Figure: The per-camera credentials dialog

Fields:

Field	Purpose
Username	Camera admin account (usually "admin").
Password	Plain text. Stored RAW in camera_creds.json (ONVIF and HTTP digest need raw to compute hashes).
RTSP Port	TCP port for the RTSP server. Default 554.
ONVIF Port	TCP port for the ONVIF web service. Default 80.
Device Type	Camera or NVR. Auto-detected on first success but you can override.
Channel	For NVR/DVR — which channel to preview. 1-based.

Click Save and the preview re-runs with your credentials. Successful credentials are persisted to camera_creds.json.

> ⚠ **Warning:** Credentials are stored raw on disk. The file has standard Windows ACLs — readable only by your user account — but is not encrypted. Don't ship the file outside your organisation.

Stream rendering details

RTSP transport

Every RTSP connection is forced over TCP via the OPENCV_FFMPEG_CAPTURE_OPTIONS environment variable. UDP RTSP is silently dropped by most consumer routers and almost every corporate firewall, so the app always uses TCP even when the camera advertises UDP.

Profile selection

When the camera offers multiple profiles (main / sub stream), the app picks the one with the smallest pixel count. The sub stream is much lower bitrate and starts in a fraction of the time of the main stream — perfect for

preview-only use cases. The picked URL is then cached in camera_creds.json with a version tag, so subsequent connections skip the discovery.

Frame display

Frames are pushed at up to 20 fps (single cameras) or 15 fps (DVR streams). The display window is fixed at 720 × 400 pixels with a fixed-size body holder (pack_propagate disabled) so the Label can never grow the window beyond the bottom-bar buttons.

Every frame is stretched to fill the body exactly — so a 4:3 Dahua DVR sub-stream takes up the same screen area as a 16:9 Uniview IP camera. The slight horizontal stretch is the trade-off for uniform widescreen rendering.

DVR / NVR tuning

When the device is detected as an NVR/DVR, the streaming loop uses different parameters:

Parameter	Single camera	DVR / NVR
stimeout (µs)	5,000,000	15,000,000
max_delay (µs)	500,000	2,000,000
reorder_queue_size	default	1,000
CAP_PROP_BUFFERSIZE	1	3
DRAIN_MAX	4	1
UI fps cap	20	15
Reopen after fails	30	12

DVRs serialise multiple channels onto a single TCP socket, so packet jitter is higher and frame intervals are less regular. Larger buffers and gentler draining give cleaner playback at the cost of a slightly higher end-to-end latency.

Reconnection

If the camera stops sending frames for ~5 seconds (single camera) or ~2 seconds (DVR), the loop tears down the VideoCapture, opens a fresh one, and starts reading again. The last good frame stays on screen while the reconnect happens, so the user sees no black-out for brief network blips or camera reboots.

Chapter 9 — Changing a single camera's IP

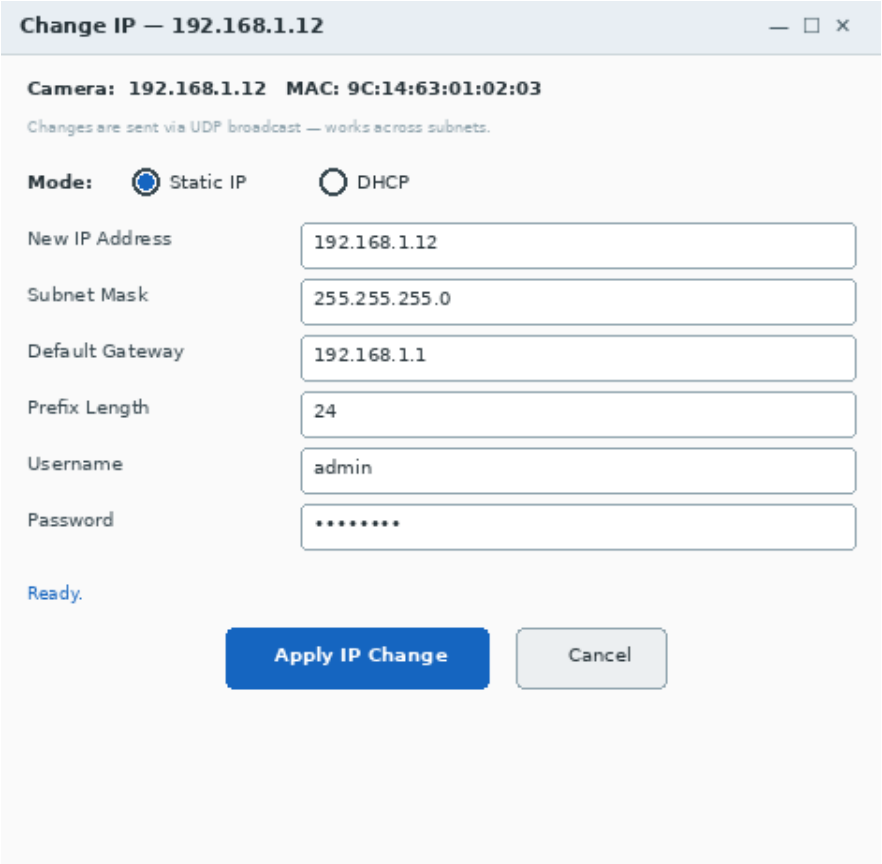


Figure: The single-camera Change IP dialog

Field reference

Field	Notes
Mode (Static / DHCP)	Top of dialog. Static (default) requires explicit IP/mask/gateway. DHCP greys those fields and tells the camera to use DHCP after reboot.
New IP Address	Target IPv4 address. Validated for syntax before sending.
Subnet Mask	Default 255.255.255.0. Used to compute the prefix length.
Default Gateway	Auto-fills as you type the New IP (mirrors first three octets + .1). Stops auto-filling once you click into the gateway field.
Prefix Length	Auto-derived from the mask. Override if you need a non-/24.
Username / Password	ONVIF admin credentials for the camera. Pulled from camera_creds.json if available.

Execution flow

When you click Apply IP Change, the worker thread:

13. Pre-check: confirms your PC is on the camera's subnet. If not, and you're running as Administrator, the app silently adds a temporary IP alias to one of your NICs via netsh (the "subnet trick") so ONVIF can reach the camera.
14. TCP probe: tests ports 80 / 8000 / 8080 / 2020 / 8899 to find which ones the camera has open.
15. Primary path: tries ONVIF SetNetworkInterfaces + SetNetworkDefaultGateway on each open port, with your credentials.
16. Reboot trigger: many cameras stage the config and only commit on reboot. The app issues an explicit SystemReboot to commit the change.
17. Verification: polls the OLD IP (waiting for it to go silent) and the NEW IP (waiting for it to start responding). On success, the inventory row updates to the new IP.
18. Uniview LAPI fallback: if ONVIF returned False or rejected the request, the app falls through to Uniview's LAPI HTTP API with four schema variants.
19. UDP broadcast fallback: as a last resort, vendor-specific UDP broadcasts (Hikvision SADP UDP 37020, Dahua UDP 37810, Uniview UDP 7373) are sent.
20. Cleanup: any temporary alias added in step 1 is removed.

Tip: Every step is logged in detail to change_ip_debug.log. Open this file when troubleshooting failures.

Switching a camera to DHCP

Selecting the DHCP radio button at the top of the dialog has these effects:

- IP / mask / gateway / prefix fields grey out.
- The ONVIF payload sends DHCP: True with no Manual array.
- SetNetworkDefaultGateway is skipped (DHCP provides one).
- Uniview LAPI fallback uses the DHCP-mode body variants.

⚠ **Warning:** After flipping to DHCP, you must re-scan to find the camera at its new address. The old IP will become unreachable as soon as the camera reboots and pulls a DHCP lease.

Chapter 10 — Bulk operations

Bulk Change IP

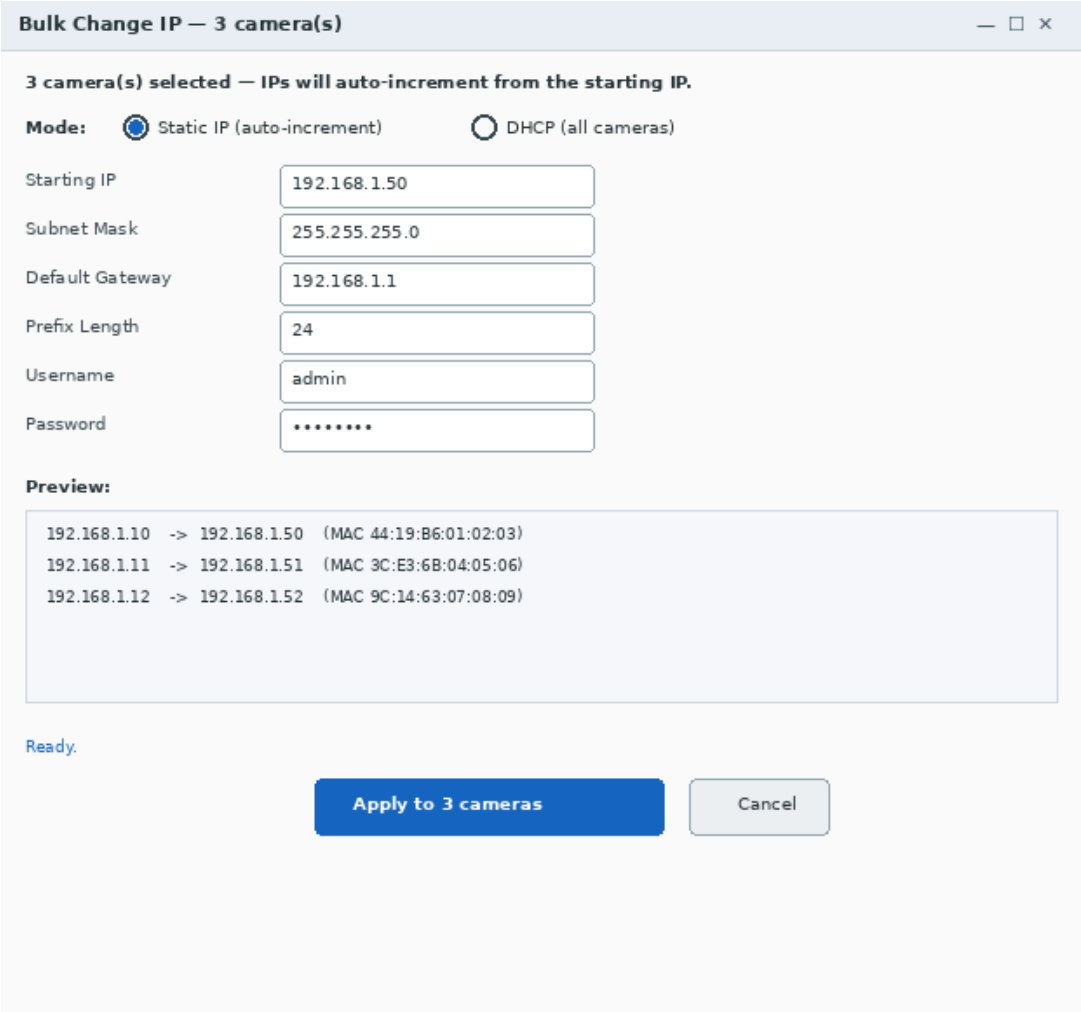


Figure: The Bulk Change IP dialog with live preview

The fastest way to commission a batch of newly-installed cameras.

21. Select 2+ cameras (Ctrl + click for individual, Shift + click for a range).
22. Right-click any selected row → Bulk Change IP (N selected)…
23. Enter the Starting IP. Every selected camera gets a sequential address: start, start+1, start+2, …
24. Set Mask, Gateway, Prefix as needed.
25. Username / Password — assumed to be the same on every selected camera.
26. Review the preview pane (shows every old → new mapping).
27. Click Apply to N cameras and confirm.

DHCP mode in bulk

Selecting the DHCP radio at the top of the bulk dialog flips every selected camera to DHCP in one pass. Useful when handing an install over to a managed network where DHCP reservations are in use.

Sequential execution

Each camera is processed one at a time, not in parallel. This keeps the bandwidth load reasonable and lets the progress bar report meaningful per-camera status.

Failure handling

After every camera has been attempted, a summary dialog lists the count of successes / failures and the per-camera error message for any failure. Common failures:

- Auth failure — credentials don't match.
- Account locked — too many wrong attempts hit Hikvision's policy. Wait 30 min for auto-unlock.
- Did not confirm success — the camera applied the change but the new IP didn't come up in 75 seconds (camera is on a routed boundary, or it needs longer to boot).

Bulk Change Password

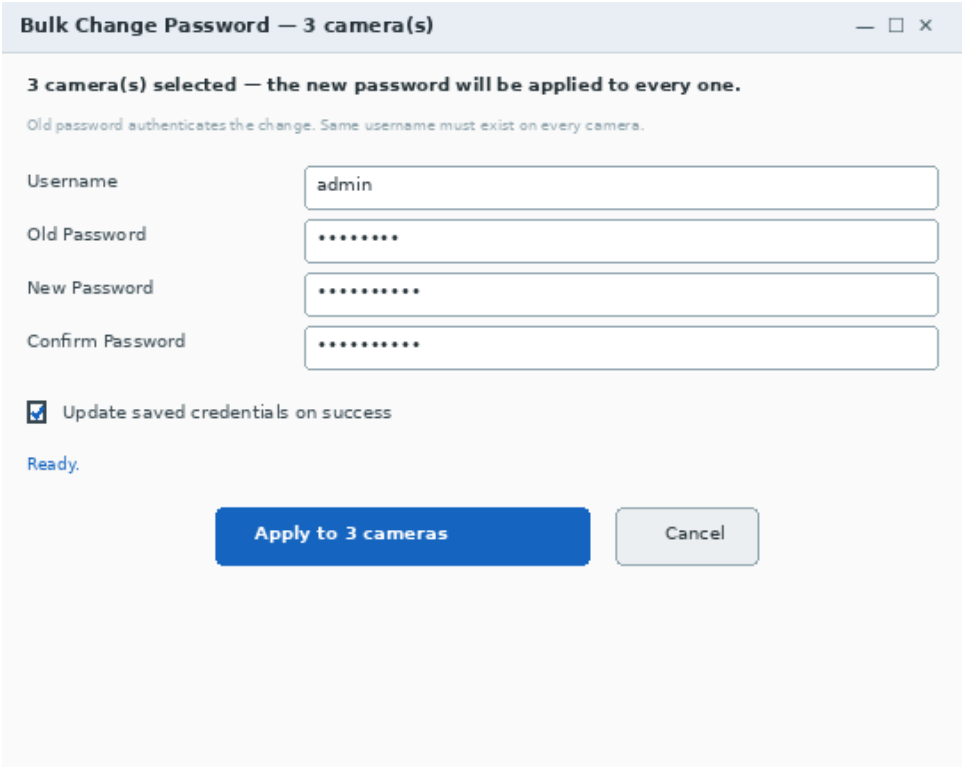


Figure: The Bulk Change Password dialog

Standardise admin credentials across a site in one pass.

28. Select 2+ cameras.
29. Right-click → Bulk Change Password (N selected)…
30. Enter Username (same on every selected camera), Old Password (authenticates the change), New Password, and Confirm.
31. Leave "Update saved credentials on success" checked — this rewrites camera_creds.json for every camera that succeeds.
32. Click Apply. Each camera receives an ONVIF SetUser request with UserLevel: Administrator on the first responsive ONVIF port.

⚠ **Warning:** A bad new password locks every selected camera simultaneously. Read the confirmation dialog carefully — the cost of a typo scales with how many cameras you've selected.

Part IV — Visualisation

Two tabs in MTech ScanFind exist purely to show your network graphically: the Network Map (logical topology) and the Location Map (physical floor plan).

Chapter 11 — The Network Map

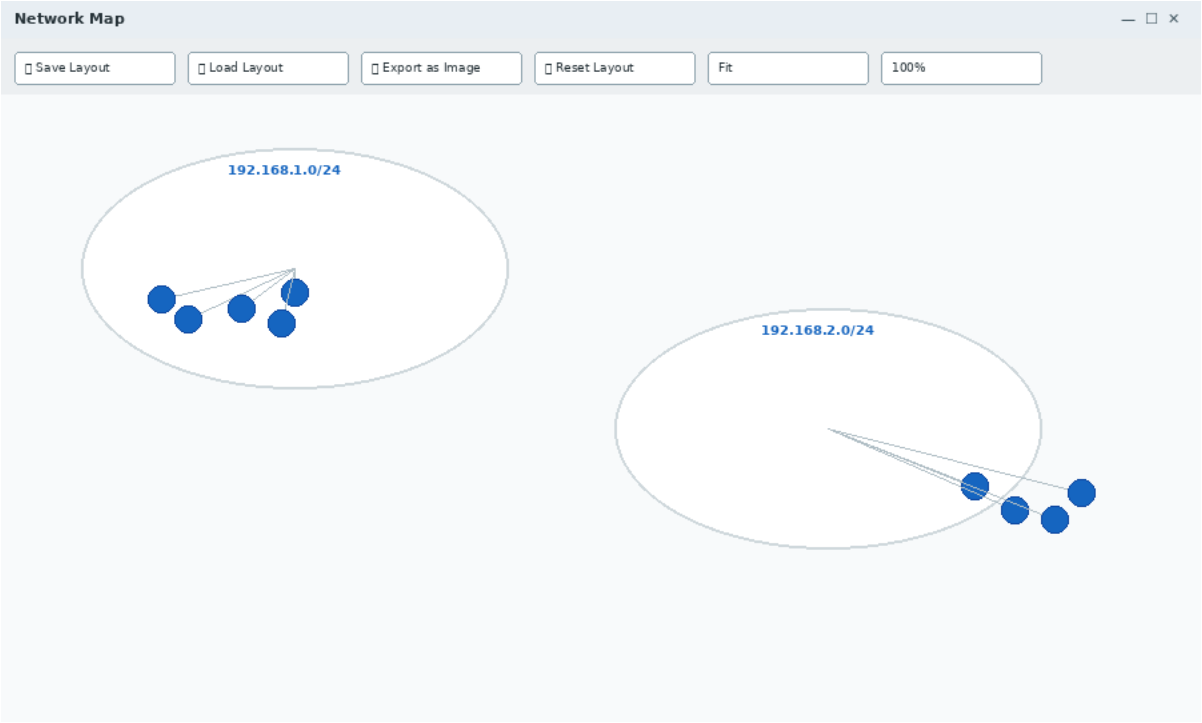


Figure: The Network Map showing devices grouped into subnet bubbles

What it shows

Every discovered subnet appears as a labelled bubble. Inside the bubble, each device shows as a dot connected to the bubble's centre. Drag any device to reposition. Drag a bubble to move the whole subnet.

Toolbar

- **Save Layout** — Persists the current arrangement to site_<gateway>_network_map_pos.json next to the .exe. Each site you visit keeps its own layout.
- **Load Layout** — Restores a previously-saved arrangement. Pick from the list if multiple sites are saved.
- **Export as Image** — Renders the current view to a PNG file.
- **Reset Layout** — Re-runs the auto-arrangement algorithm.
- **Fit / 100%** — Zoom controls. Mouse wheel also zooms; Shift+wheel scrolls horizontally.

Switches and trunks

If your network has managed switches, you can register them so the map shows a proper port-to-device topology rather than a simple bubble:

33. Right-click empty map space → Add Switch.
34. Enter the switch's IP and the number of ports.
35. Drag cameras into the switch box. Each camera shows on a numbered port.

Bulk switch management is in Settings → Switches.

Chapter 12 — The Location Map (Floor Plans)

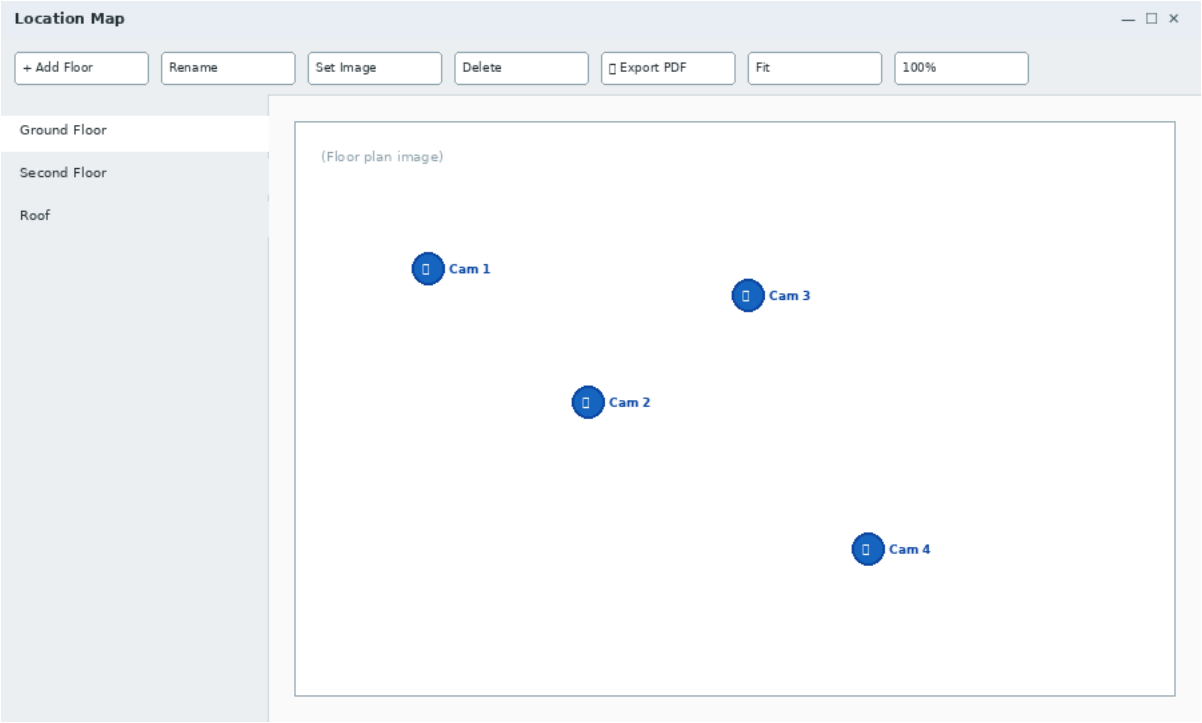


Figure: The Location Map with a floor plan and camera pins

Workflow

36. Click + Add Floor in the toolbar and give the floor a name ("Ground Floor", "Roof", etc.).
37. Click Set Image and pick a JPG / PNG of the floor plan.
38. On the Dashboard, right-click any camera → Set Location Name..., and pick the floor.
39. Switch back to the Location Map tab. The camera appears as a pin somewhere on the floor.
40. Drag the pin to its real-world position on the floor plan.
41. Positions auto-save to floor_plans.json — no Save button needed.

Exporting to PDF

Click Export PDF in the toolbar to render every floor as a page in a single PDF. Each page shows the floor plan with every pinned camera labelled by its IP and friendly name. Useful for site documentation, audits, or handoff to facility management.

Part V — Network analysis

Chapter 13 — The Ports tab

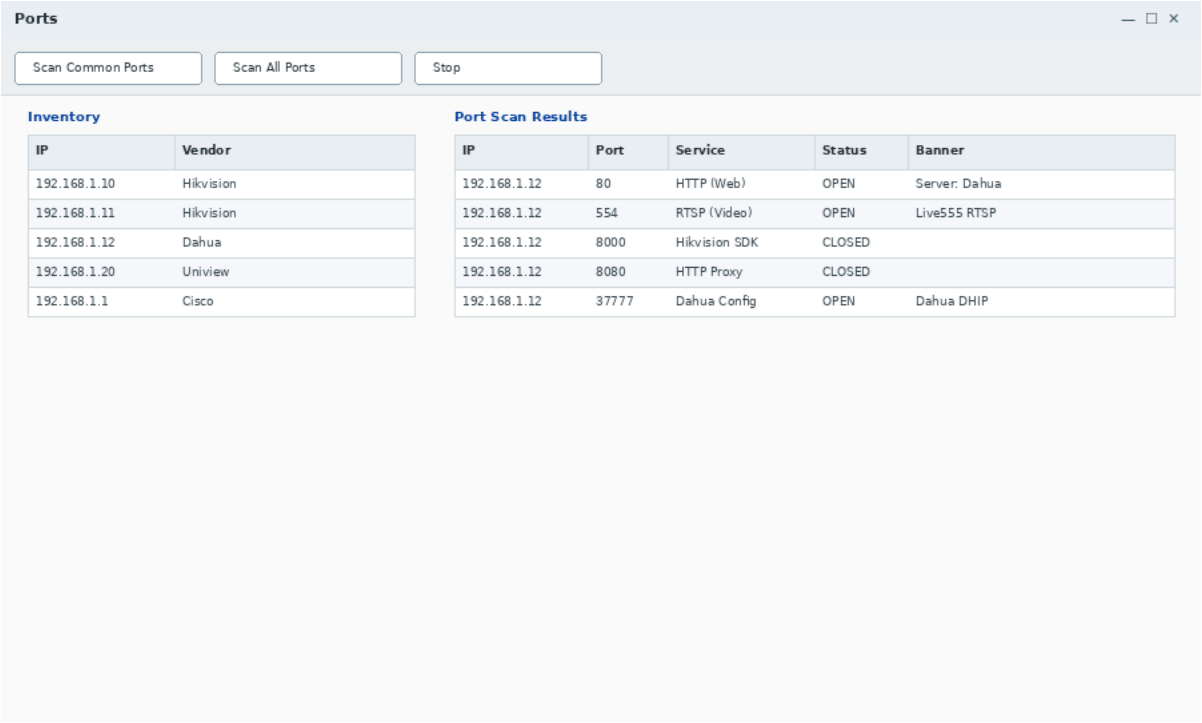


Figure: The Ports tab — pick a target on the left, see scan results on the right

Scope

The Ports tab does deeper port scanning than the Dashboard's quick probe. Two scan modes are available:

- **Scan Common Ports** — Tests a curated list of CCTV-relevant ports (21, 22, 23, 53, 80, 81, 443, 554, 1935, 3702, 5000, 8000, 8080, 8200, 9000, 34567, 37777, 37778). Fast — seconds per host.
- **Scan All Ports** — Tests all 65,535 TCP ports. Slow — several minutes per host. Use with care on production networks.

Results table

Columns: IP, Port, Service, Status, Banner. The Service column maps the port number to its common service name. The Banner column shows any text the server returned during the connection (server header, OS hint, protocol version).

> ⚠ **Warning:** Aggressive port scans can trigger IDS / IPS alerts on managed networks. Coordinate with your network operations team before running Scan All Ports during business hours.

Part VI — Help and database

The Help tab is a self-contained reference hub: vendor default credentials, the OUI brand database, and direct contact links to MTech support.

Chapter 14 — IP Cameras Password reference

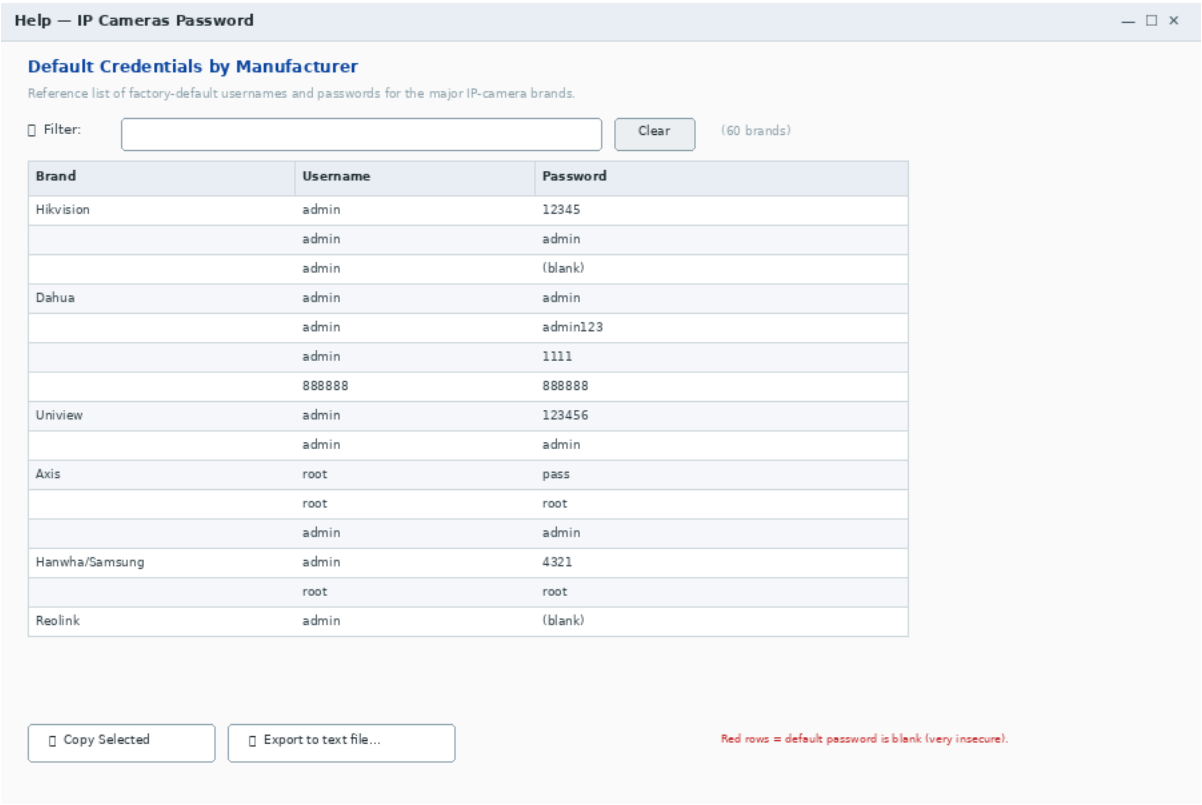


Figure: The IP Cameras Password reference sub-tab

A live, searchable table of factory-default usernames and passwords for every brand the credential discovery uses (60+ brands, 150+ credential pairs).

Features

- Live filter — typing anything in the Filter box narrows the list by brand, username, or password text.
- Alternating row shading by brand makes it easy to scan visually.
- Red text on the Password column marks credentials where the default is BLANK — these are extremely insecure and should be changed immediately.
- Copy Selected copies the highlighted rows to clipboard as tab-separated values (paste into Excel).
- Export to text file… writes the entire list as plain text for printing / sharing.

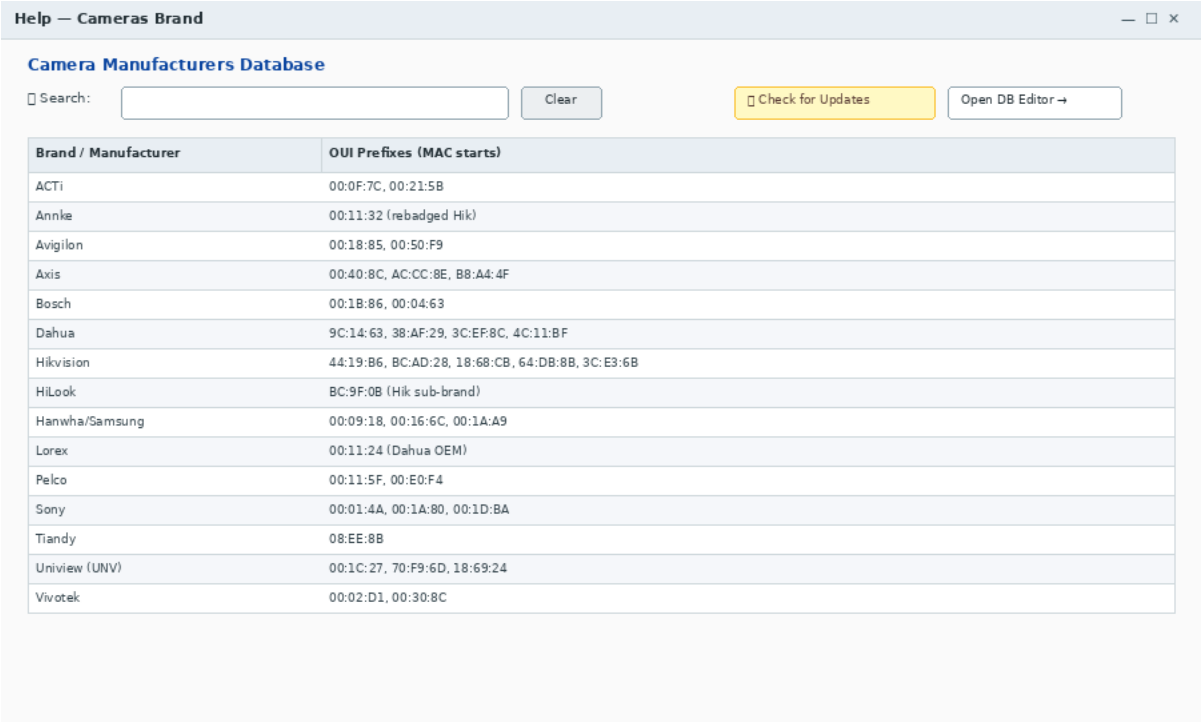
Sample of the most-common defaults

Brand	Username	Default password
Hikvision	admin	12345 (older) / Admin12345 (newer)
Dahua	admin	admin
Uniview (UNV)	admin	123456
Axis	root	pass
Hanwha/Samsung	admin	4321

Brand	Username	Default password
Vivotek	root	(blank)
Reolink	admin	(blank)
Bosch	service	service
Sony	admin	admin
Panasonic	admin	12345
Pelco	admin	admin
Mobotix	admin	meinsm
Lorex	admin	000000
Avigilon	administrator	(blank)
TP-Link VIGI	admin	admin
Foscam	admin	(blank)
Wyze	admin	(blank)

⚠ **Warning:** Any camera still on its factory-default password is an open door to your network. The Bulk Change Password feature (Chapter 10) standardises them across a whole site in one pass.

Chapter 15 — Cameras Brand database



Brand / Manufacturer	OUI Prefixes (MAC starts)
ACTi	00:0F:7C, 00:21:5B
Annke	00:11:32 (rebadged Hik)
Avigilon	00:18:85, 00:50:F9
Axis	00:40:8C, AC:CC:8E, B8:A4:4F
Bosch	00:1B:86, 00:04:63
Dahua	9C:14:63, 3B:AF:29, 3C:EF:8C, 4C:11:BF
Hikvision	44:19:B6, BC:AD:28, 18:68:CB, 64:DB:8B, 3C:E3:6B
HiLook	BC:9F:0B (Hik sub-brand)
Hanwha/Samsung	00:09:18, 00:16:6C, 00:1A:A9
Lorex	00:11:24 (Dahua OEM)
Pelco	00:11:5F, 00:E0:F4
Sony	00:01:4A, 00:1A:80, 00:1D:BA
Tiandy	08:EE:8B
Uniview (UNV)	00:1C:27, 70:F9:6D, 18:69:24
Vivotek	00:02:D1, 00:30:8C

Figure: The Cameras Brand sub-tab — searchable OUI → brand database

This is the database the scan engine uses to map MAC addresses to vendor names. When you see "Hikvision" in the Type column of the inventory, it's because the device's MAC starts with one of Hikvision's registered OUI prefixes (44:19:B6, BC:AD:28, etc.).

Search and browse

Type any brand name or MAC prefix in the search box. The table filters in real time. Double-click a brand row to open the DB editor pre-loaded with that brand for quick edits.

Chapter 16 — Check for Updates

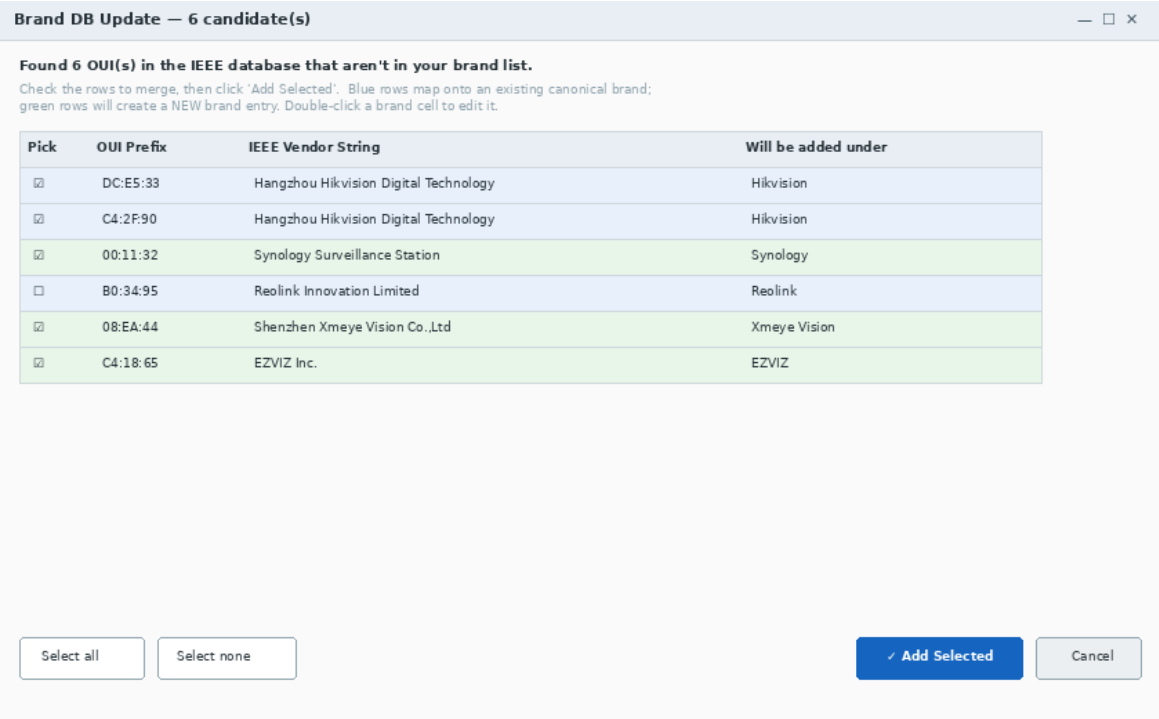


Figure: The Check for Updates dialog

What it does

Clicking the ⟳ Check for Updates button (top right of the Cameras Brand tab) does the following:

42. Refreshes the IEEE OUI database cache (force re-download if older than 7 days), running in a background thread.
43. Walks every OUI in the IEEE database, normalising the prefix to XX:XX:XX, and skips anything already in your brand list.
44. For each unknown OUI: runs the vendor string through the _resolve_vendor_key matcher (the same one used by the credential picker). Hits get proposed under the canonical brand.
45. OUIs whose vendor string contains camera/surveillance keywords ("camera", "cctv", "surveillance", "vision", "imaging", "video", "security", "nvr", "dvr", "webcam", "ip cam", "ptz", "alarm", "intercom") but no canonical match are proposed as new brands.

The proposal dialog

- **Blue rows** — An existing canonical brand (e.g. a new Hikvision OUI). The new OUI will be added to that brand's list.
- **Green rows** — A brand-new entry. The cleaned-up vendor string becomes the brand name.
- **Pick checkbox** — Toggle to include / exclude each row.
- **Brand cell** — Double-click to edit the suggested brand name before merging.
- **Select all / Select none** — Bulk toggles at the bottom.
- **✓ Add Selected** — Merges everything checked into self.manufacturers and saves via save_custom_manufacturers.

Tip: After Add Selected, both the Brand tab list and the Settings → Database Manager refresh automatically with the new entries.

Chapter 16 — Contacting MTech (Support sub-tab)

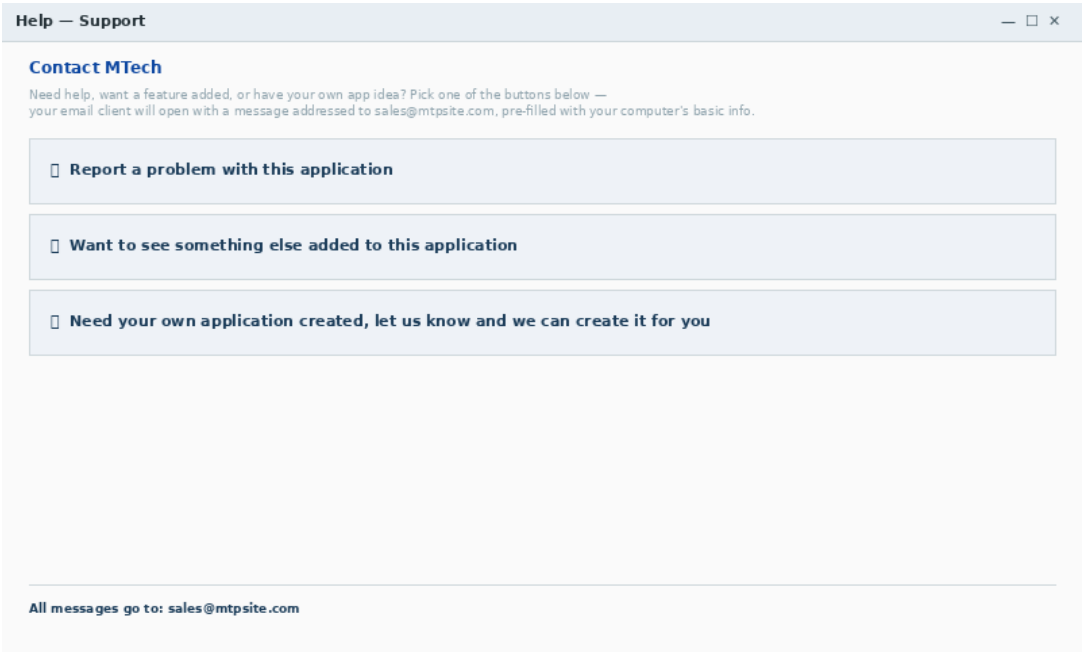


Figure: The Support sub-tab — three direct-contact links

Three link-styled buttons under Help → Support open your default mail client with a pre-addressed email to sales@mtpsite.com.

Button	Use it when…
Report a problem with this application	You found a bug, the app crashes, a feature doesn't work as documented.
Want to see something else added to this application	You have a feature request, you want a new vendor's defaults added, you'd like a tweak to an existing workflow.
Need your own application created, let us know and we can create it for you	You have an idea for a custom tool, internal utility, or industry-specific app you want MTech to build.

Each button's text is used as both the email Subject AND the first body line, so every request arrives self-classified.

Sender context auto-attached

To save round-trips, the message body is pre-filled with a block of sender information:

- Computer name (platform.node())
- OS / version (platform.system / release / version)
- Username (USERNAME / USER environment variable)
- Active local IPs (the same data shown in the header)
- Timestamp

If your default mail client isn't set up (mailto blocked by policy, etc.), an error toast appears with the destination address spelled out so you can compose manually.

Part VII — Apps and integration

Chapter 17 — The Others tab

Run third-party Python scripts from inside MTech ScanFind. Useful for site-specific utilities — an exporter to your CMMS, a custom RTSP test tool, a one-off firmware-upgrade batch job.

How it works

46. Drop your .py file into the ext/ folder next to MTech ScanFind.exe.
47. Rename the file from .py to .dll. This is a security measure — stops Windows or third-party launchers from accidentally running the file outside of MTech ScanFind.
48. Click ⍰ Refresh on the Others tab.
49. A button appears for each script. Click ▶ Run.
50. MTech ScanFind hides the main window, runs your script in a subprocess, and re-shows the main window when the script exits.

Why the .dll rename?

Python scripts with .py extensions can be opened by IDEs, explorer's preview pane, or Windows' default Python handler. The rename to .dll stops any of that from happening accidentally — the file becomes opaque to everything except MTech ScanFind, which knows to load it as Python code.

Chapter 18 — The APPs tab

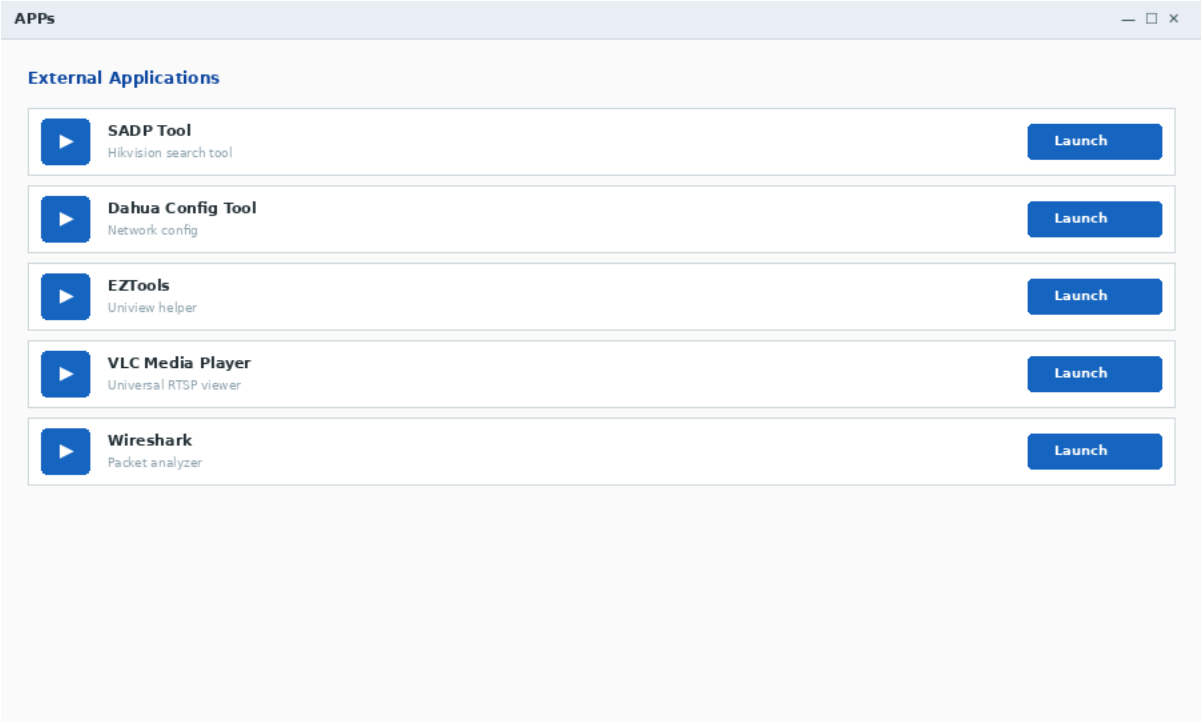


Figure: The APPs tab — every enabled .exe gets a Launch button

Like the Others tab, but for pre-built .exe tools. Drop SADP, EZTools, the Dahua Config Tool, your favourite RTSP viewer, Wireshark — anything you launch frequently — into the apps/ folder and they appear here.

Setup

51. Drop your .exe into the apps/ folder next to MTech ScanFind.exe.
52. Open Settings → APPs and click ⍰ Scan for Apps.
53. Tick the checkbox next to each .exe you want visible.
54. Switch to the APPs tab. Each enabled app appears as a button with a Launch action.

Run as Administrator

Some camera tools (Hikvision SADP, Dahua Config Tool) need admin rights to access raw sockets or change adapter settings. Right-click a Launch button and choose Launch as Administrator — a UAC prompt appears, the app launches elevated.

Part VIII — Settings

Chapter 19 — The Settings tab

The Settings tab is a notebook with four sub-tabs.

Alerts & Notifications

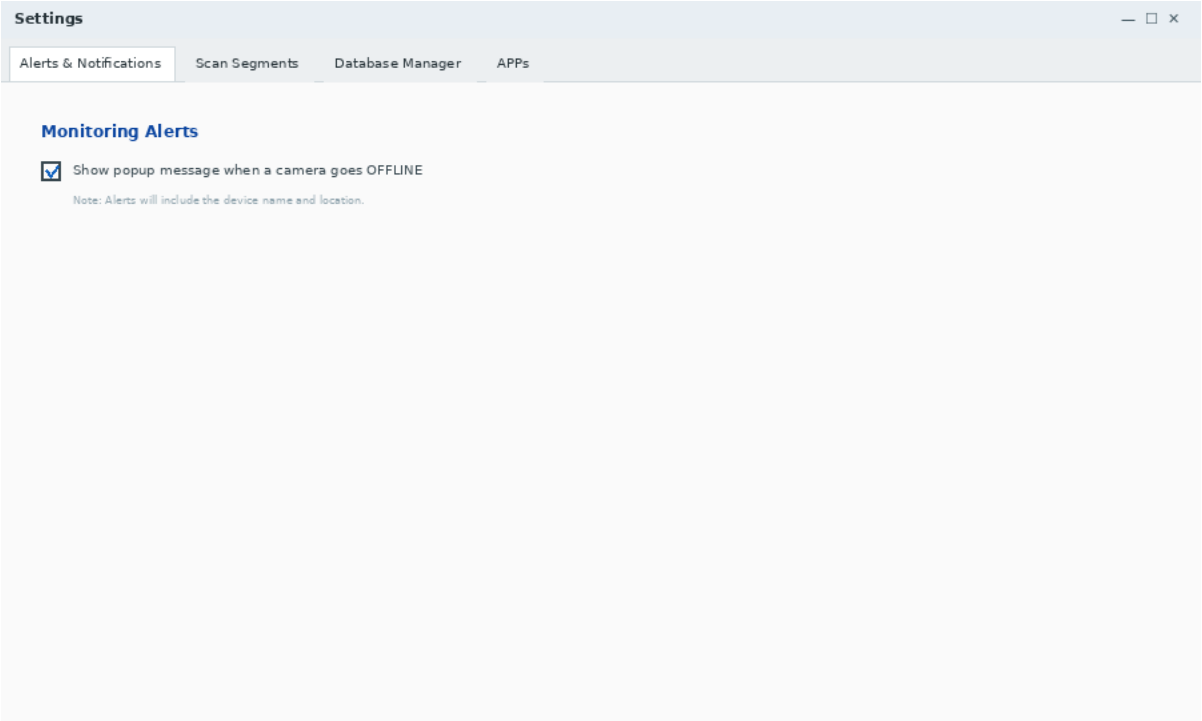


Figure: Settings → Alerts & Notifications

A single checkbox controls the offline-alert popup.

- **Show popup message when a camera goes OFFLINE** — When checked, the live monitor pops a system alert whenever a previously-online camera fails to ping. The alert lists every camera in the current transition (one alert can cover many cameras).

Scan Segments

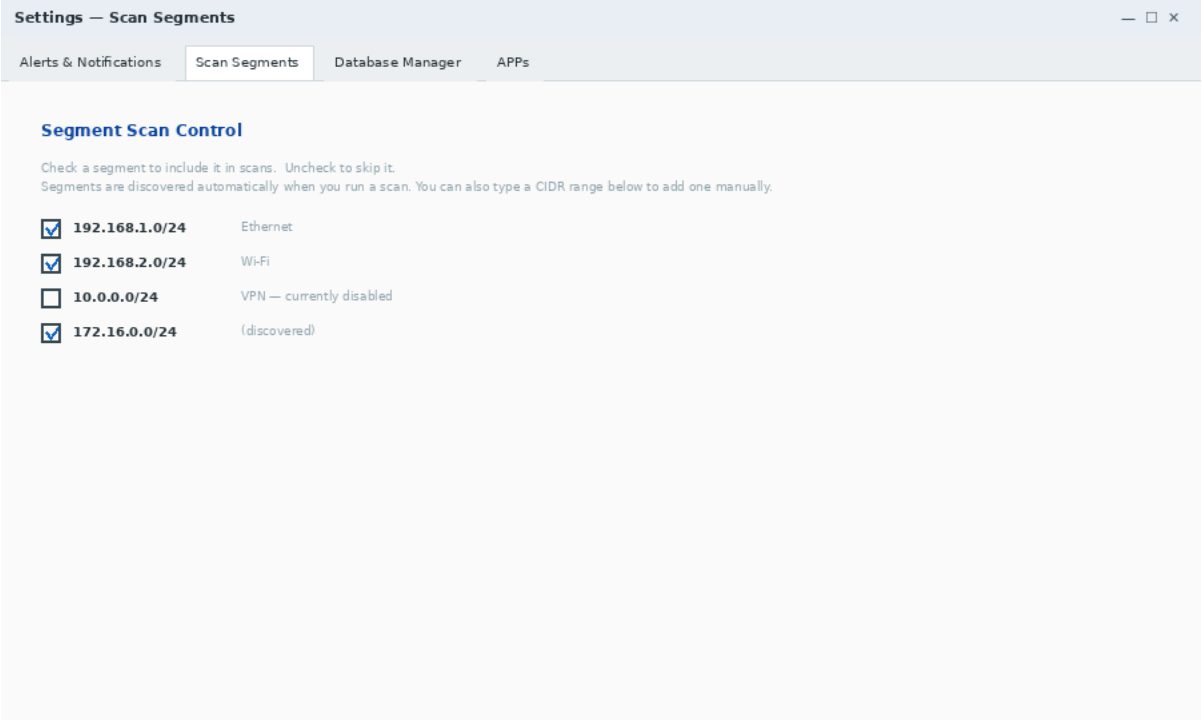


Figure: Settings → Scan Segments

Lists every subnet MTech ScanFind has discovered. Each row has a checkbox; unchecking the box excludes that subnet from future scans.

- Useful for excluding guest VLANs you don't manage.
- Useful for excluding a VPN subnet that shouldn't be scanned.
- Manually-added segments (typed CIDR) appear here alongside the auto-discovered ones.

Disabled segments are persisted to a JSON file next to the .exe and survive app restarts.

Database Manager

Same editor as the Cameras Brand tab, but with the full set of import / export controls. Used to:

- Add a brand-new manufacturer mapping (brand name → list of OUI prefixes).
- Bulk import a JSON file of vendor entries (format documented in the bundled database).
- Manage duplicate OUIs — some MAC prefixes have been reassigned by IEEE over the years, and this dialog lets you pick the preferred mapping.
- Export the entire database to text or PDF for backup.

APPs sub-tab

- **Scan for Apps** — Re-enumerate the apps/ folder.
- **Enable All** — Tick every app's checkbox.
- **Disable All** — Untick every app's checkbox.
- Per-app checkbox — control which apps appear on the APPs tab.

Part IX — Advanced topics

Chapter 20 — ONVIF, RTSP, and the discovery stack

ONVIF in 60 seconds

ONVIF (Open Network Video Interface Forum) is a SOAP-based industry standard that lets IP cameras and NVRs expose a uniform API regardless of manufacturer. MTech ScanFind uses the onvif-zeep Python library to speak this API.

Key ONVIF operations the app calls:

Operation	Used by	Purpose
WS-Discovery	Scanner	Find ONVIF devices on the network.
GetDeviceInformation	Enrichment	Read Model / Firmware / Serial.
GetProfiles	Preview	List available video profiles.
GetStreamUri	Preview	Get the RTSP URL for a profile.
SetNetworkInterfaces	Change IP	Set static IP / mask / DHCP mode.
SetNetworkDefaultGateway	Change IP	Set the default gateway.
SystemReboot	Change IP	Commit staged changes.
SetUser	Bulk Pwd	Change user password.

RTSP transport choice

The Real Time Streaming Protocol can run over either UDP or TCP. MTech ScanFind always forces TCP via the ffmpeg env var:

- UDP is silently dropped by most consumer / SoHo routers.
- UDP is blocked by virtually every corporate firewall.
- Uniview cameras in particular almost never serve usable video over UDP.
- TCP adds a small overhead but works everywhere RTSP is allowed.

The subnet trick

When you change a camera's IP and your PC isn't on the camera's subnet, ONVIF can't reach the camera. The "subnet trick" (also used by SADP and EZTools) is to temporarily add a secondary IP alias to one of your NICs in the camera's subnet, use that for the duration of the operation, and remove it afterwards.

On Windows, this requires Administrator rights (netsh interface ipv4 add address). The app handles add and removal automatically and logs the action to change_ip_debug.log.

Chapter 21 — File formats

camera_creds.json

Per-camera credentials and connection state, indexed by IP.

Field	Type	Description
user	string	Username for ONVIF / RTSP / HTTP digest.
pass	string	Password (raw — see warning below).
port	int	RTSP port. Default 554.
onvif_port	int	ONVIF web service port. Default 80.
device_type	string	"camera" or "nvr".
channel	int	For NVR — which channel to preview.
working_url	string	Cached RTSP URL that returned a frame.
preview_version	int	Cache version for invalidation.

> ⚠ **Warning:** Passwords are stored raw on disk. ONVIF and HTTP digest auth both need the raw password to compute their hashes — encrypting the stored value would break authentication.

custom_manufacturers.json

Your additions to the OUI brand database. Schema: a JSON object mapping brand name to an array of OUI prefix strings.

device_locations.json

IP → friendly location label mapping.

floor_plans.json

List of floor objects. Each floor has a name, an image path, and an array of pin positions (IP, x, y).

site_<gateway>_*.json

Per-site state files (network map positions, disabled segments, device locations). The filename includes the gateway IP (underscored) so multiple sites can coexist.

Part X — Reference and troubleshooting

Chapter 22 — Troubleshooting

Scanning

Symptom	Likely cause and fix
Scan returns no devices	PC isn't on the camera LAN, or a VPN is hijacking the route. Disable VPN, re-check Settings → Scan Segments.
Some cameras missing	ICMP-silent cameras or strict ACLs. Try a second scan — passive sniff and proprietary broadcast pick up stragglers. Check OUI database (Help → Cameras Brand).
Status column stuck on Pinging…	Background ping pass takes 1–2 sec on small networks. If stuck >15 sec, device is blocking ICMP — TCP probe should still work.
Same IP appears twice	Duplicate IP on the network (two devices configured with the same address). Use the MAC to identify which is which.

Live preview

Symptom	Likely cause and fix
Won't connect	Wrong credentials, or RTSP disabled on the camera. Open Set Credentials and verify.
503 Service Unavailable	Camera has hit its max concurrent RTSP sessions. Close other viewers (DMSS, web UI, browser tabs) and Refresh.
Picture lags or stutters (single camera)	Network jitter. The loop drains stale frames automatically — if it's still bad, check Wi-Fi signal or move to wired.
Picture pixelated or 4:3 instead of 16:9	Source is 4:3. Every preview stretches to widescreen, so 4:3 sources show slightly wider than reality. This is intentional (uniform display across mixed brands).

IP and password changes

Symptom	Likely cause and fix
"ONVIF returned False" in log	Camera staged the change and is waiting for reboot. Wait 30 sec then re-scan.
Cross-subnet IP change fails	Run MTech ScanFind as Administrator so the subnet-trick alias can be installed.
Bulk password — some succeed, some fail	Camera doesn't support ONVIF SetUser, or has a different user model. Read the summary dialog for per-camera errors.
Account locked	Too many wrong attempts hit the camera's lockout threshold. Wait 30 min for auto-unlock, or use the camera's web UI to force unlock.

Chapter 23 — Glossary

Term	Definition
ARP	Address Resolution Protocol — L2 mapping of IP to MAC.
CIDR	Classless Inter-Domain Routing — IP/prefix notation (192.168.1.0/24).
DHCP	Dynamic Host Configuration Protocol — automatic IP assignment.
LAPI	Uniview's proprietary HTTP API.
MAC	Media Access Control address — 48-bit hardware identifier.
NVR	Network Video Recorder — multi-channel CCTV recorder.
DVR	Digital Video Recorder — usually multi-channel, often analog inputs converted to digital.
ONVIF	Open Network Video Interface Forum — SOAP-based camera API standard.
OUI	Organizationally Unique Identifier — first 24 bits of a MAC, identifies the vendor.
RTSP	Real-Time Streaming Protocol — control protocol for video streams.
SADP	Hikvision's Search Active Devices Protocol (UDP 37020).
SOAP	Simple Object Access Protocol — XML-based RPC, used by ONVIF.
SSDP	Simple Service Discovery Protocol — UPnP discovery via UDP 1900.
VLAN	Virtual LAN — broadcast-domain partition inside a managed switch.
VAPIX	Axis Communications' proprietary HTTP API.
WS-Discovery	Web Services Dynamic Discovery — ONVIF's discovery layer over multicast UDP 3702.

Chapter 24 — Index of features added in this release

For installers familiar with earlier builds, the major changes in the current release are:

Area	What changed
Header bar	Local IP values now render in a distinct gold accent so they stand out from the labels.
Dashboard	Network Inventory gained four new columns: Model, Firmware, Serial, Status. All auto-populate in the background.
Scanner	Final live-verification pass prevents stale ARP-cache entries from appearing as phantom devices.
Camera preview	Now a continuous live stream (was single snapshot). DVR/NVR streams get tuned buffering. All sources stretch to widescreen for uniform display.
IP change	Gateway field auto-fills as you type the new IP. New Static / DHCP toggle. New Bulk Change IP with auto-increment.
Password change	New Bulk Change Password dialog. ONVIF SetUser across the selected cameras with credential-update-on-success.
Enrichment	Background ONVIF GetDeviceInformation + vendor HTTP fallbacks (Hikvision ISAPI, Dahua magicBox, Axis VAPIX) + Server-header read populate Model / Firmware / Serial for most devices.
Credentials	Expanded vendor default library to 60+ brands. Brand is auto-detected from Type and Manufacturer columns to pick the right credential set.
Help tab	New top-level Help tab with three sub-tabs: IP Cameras Password reference, Cameras Brand (moved out of sidebar), Support.
Brand database	New Check for Updates button — scans IEEE OUI database for camera-vendor OUIs not in your brand list.
Splash	Animated MTech bouncing-text splash window on app startup.

Closing notes

MTech ScanFind is actively developed. If you have feature ideas, bug reports, or want a custom application built, use the Support sub-tab (Chapter 16) or email sales@mtpsite.com directly.