MTech ScanFind

Network Discovery Pro

Quick Start Guide

Get scanning in 10 minutes

First Edition · 2026

sales@mtpsite.com

About this guide

This Quick Start Guide gets you up and running with MTech ScanFind in about ten minutes. It walks through the four daily-use workflows that 90 % of users need:

- Running a network scan and reading the results.
- Watching a camera live with one click.
- Changing a camera's IP address — single camera and bulk.
- Changing camera passwords in bulk.

Every step is paired with a numbered illustration of what you should see on screen. For deeper material — every dialog, every setting, the full credential reference, ONVIF/RTSP internals, and troubleshooting — read the Comprehensive Manual that ships next to this guide.

> 💡 **Tip:** If you've never used MTech ScanFind before, read Chapter 1 first. Returning users can jump straight to whichever workflow they need.

Conventions used in this book

- **Bold text** — names a button, menu item, tab, or dialog field.
- **Right-click** — always means click with the right (or secondary) mouse button — it's how you reach most actions.
- **UPPER-CASE words** — in screenshots indicate status values (ONLINE / OFFLINE).
- 💡 **boxes** — are tips that make the workflow smoother.
- ⚠ **boxes** — are warnings — read these before clicking anything that changes a camera.

Contents

Chapter 1 — Installation and first launch

MTech ScanFind ships as a single Windows executable. There is no installer to run; you double-click MTech ScanFind.exe and the application starts.

System requirements

- **Operating system** — Windows 10 or 11 (64-bit). The app also runs on Windows Server 2019 / 2022.
- **Privileges** — Most features work as a standard user. A few — cross-subnet IP changes, port scans on privileged ports, network-adapter aliasing — require admin rights. The app tells you when and pops the UAC prompt.
- **Network** — Wired Ethernet is recommended for camera management. Wi-Fi works for discovery but IP-change reliability is much better over wired.
- **RAM** — 4 GB minimum; 8 GB recommended for large network maps.
- **Disk** — About 150 MB for the executable, plus a few megabytes for saved layouts and exports.

First launch

On the very first run, you'll see two things in quick succession.

1. The splash screen

A small dark popup appears in the centre of the screen with the word MTech bouncing around like a DVD-screensaver, cycling through seven brand colours. It tells you the app is loading.

Figure: The bouncing-MTech splash screen at startup

> **Tip:** The splash auto-closes after 3 seconds. Click anywhere on it or hit any key to dismiss it early.

2. The main window

After the splash, the main window opens with the Dashboard tab selected. The very top is a deep-navy header showing the app name on the left and your PC's local IP addresses on the right — Ethernet and Wi-Fi each appear in gold so the actual IP values stand out from the labels.

Figure: The top header — IP values rendered in gold so they're easy to read at a glance

Below the header is the toolbar (Run Scan, Stop, progress bar, and right-side action buttons), and below that the dashboard split into three vertically-stacked panes.

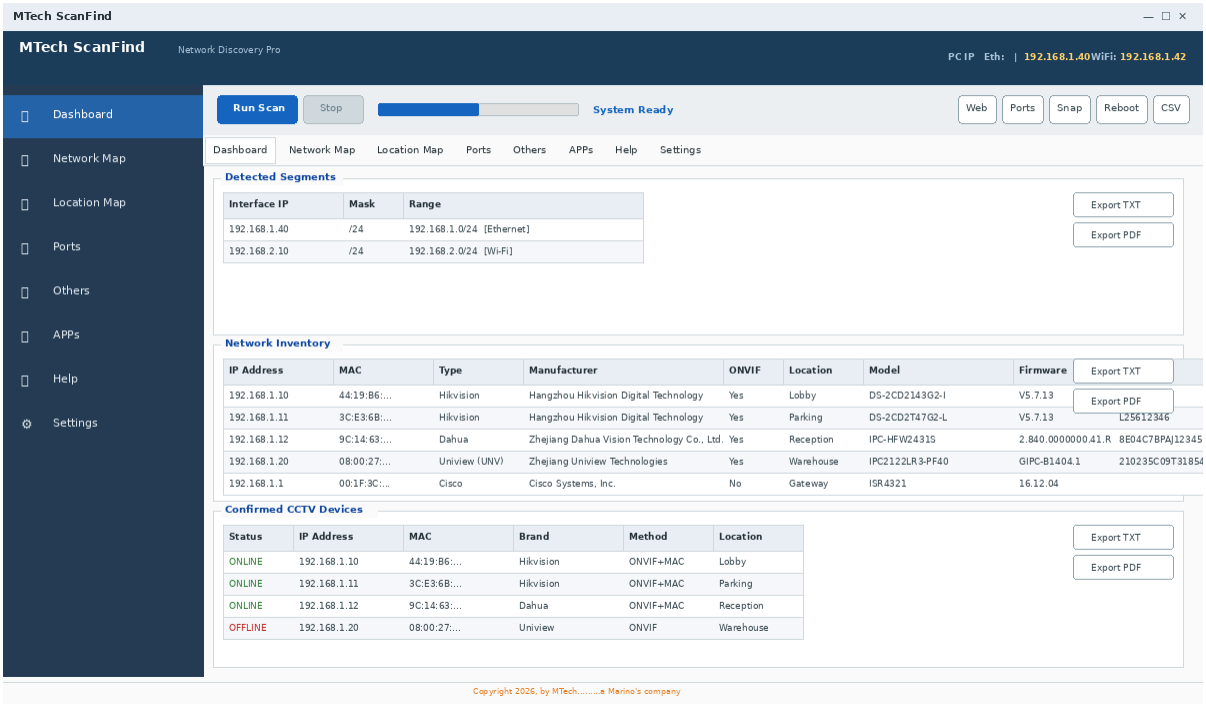

Figure: The full main window on first launch — sidebar nav on the left, three-pane Dashboard on the right

Licensing

If this is the first launch on this PC, the app opens in 30-day trial mode with full access. A yellow trial banner appears under the header. When the trial ends — or whenever you want a permanent license — click the trial banner and follow the instructions in ACTIVATION_README.pdf to email a hardware-ID and receive your license code.

Chapter 2 — Layout of the main window

Understanding the screen layout makes every other workflow easier.

Sidebar navigation (left)

The dark sidebar on the left of the window is the primary navigation. Click any item to switch tabs. The currently-selected tab is highlighted in blue.

- **Dashboard** — The main workspace with three stacked panes: Detected Segments, Network Inventory, Confirmed CCTV Devices.
- **Network Map** — Visual map of every device on every subnet.
- **Location Map** — Pin each camera to a floor-plan image.
- **Ports** — Detailed port scanning for any device.
- **Others** — Run Python helper scripts.
- **APPs** — Launch external tools (SADP, EZTools, etc.).
- **Help** — Contains three sub-tabs: IP Cameras Password reference, Cameras Brand database, and Support / Contact MTech.
- ⚙ **Settings** — Alerts, scan-segment management, database editor.

Top toolbar

Across the top of every tab is a fixed toolbar with the scan controls and per-row action buttons.

- **Run Scan** — Start a fresh scan of every enabled subnet.
- **Stop** — Cancel a scan in progress.
- **Progress bar** — Fills as the scan walks through subnets.
- **Status text** — Shows what the scan engine is doing right now.
- **Web / Ports / Snap / Reboot / CSV** — Right-side action buttons that act on the currently-selected device row in the dashboard.

Dashboard — the three panes

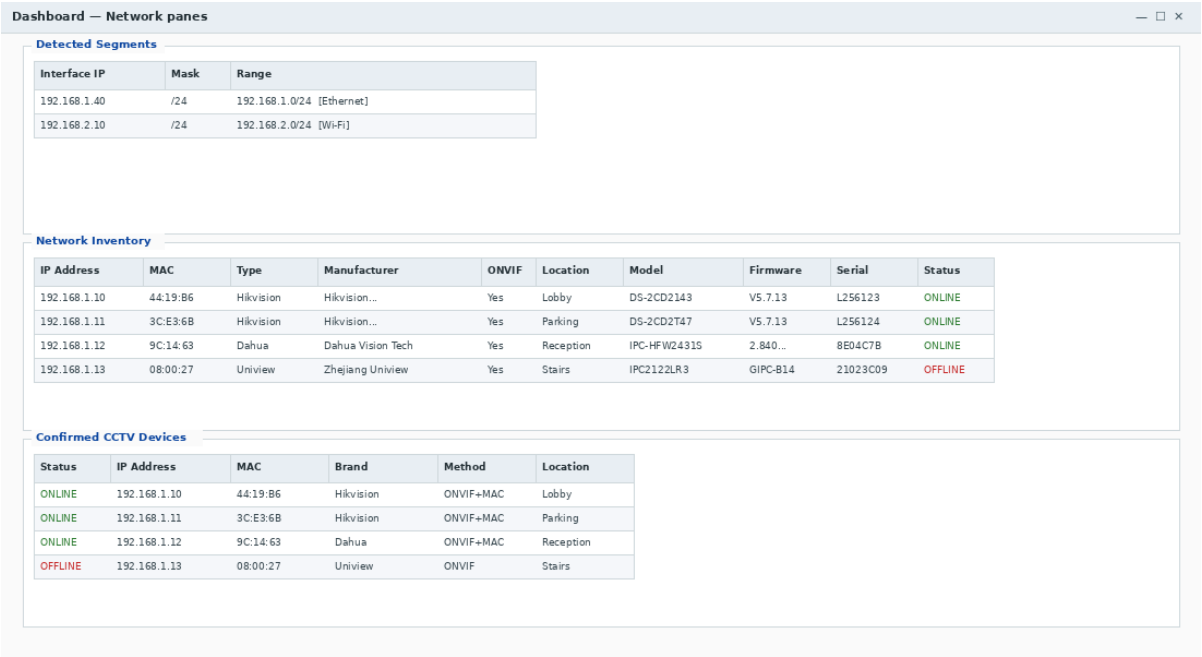

Figure: The dashboard always shows three resizable panels

The Dashboard is split into three panels with draggable dividers between them. From top to bottom:

- **Detected Segments** — Every subnet the app discovered on your network adapters.
- **Network Inventory** — Every device found, with brand, MAC, location, model, firmware, serial, and live status.
- **Confirmed CCTV Devices** — Filtered view containing only cameras / NVRs / encoders.

Drag the horizontal dividers to give one panel more room. Each panel has Export TXT and Export PDF buttons on its right side.

Chapter 3 — Your first scan

This is the workflow you'll run every time you arrive at a new site or whenever you want to refresh what's on the network.

Run the scan

1. Click the Run Scan button in the top toolbar.
2. The status bar shows which subnet is being probed right now ("Scanning 192.168.1.0/24 [Ethernet]").
3. The progress bar fills as the scan moves through your subnets.
4. Devices begin appearing in the Network Inventory and Confirmed CCTV Devices panes as soon as they're detected — you don't have to wait for the whole scan to finish.

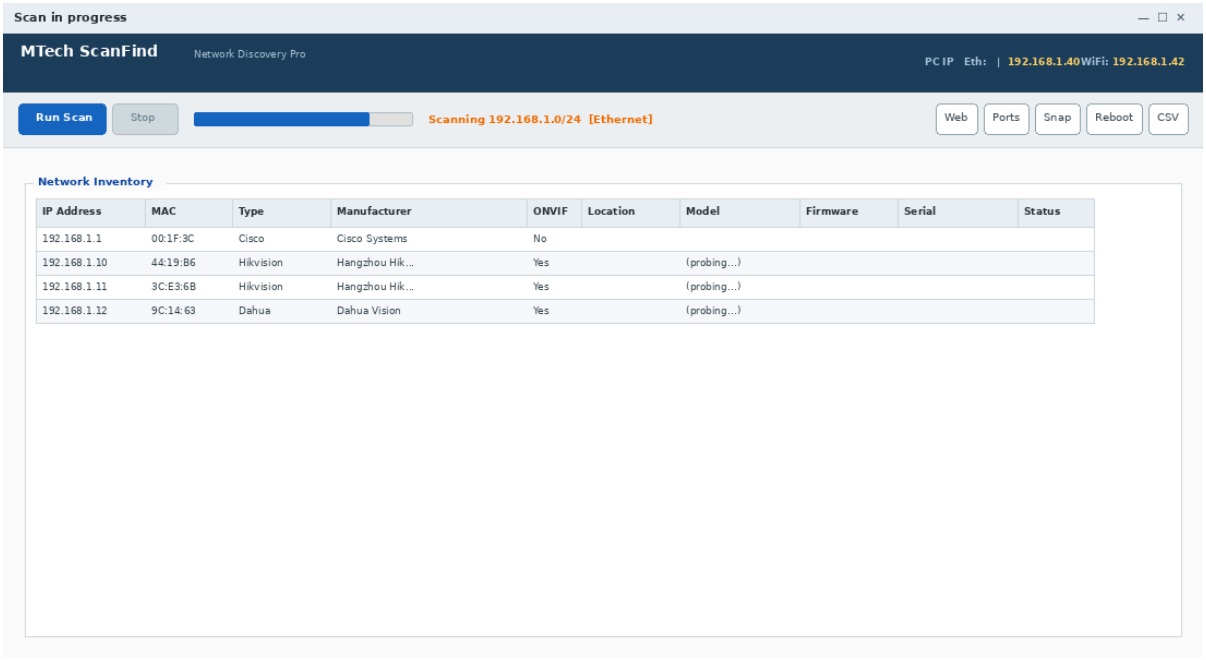

Figure: A scan mid-flight — devices appear as soon as they're found

Tip: A typical office network (50–100 devices) takes 30–60 seconds. Larger networks or networks with many silent devices take a couple of minutes.

What just happened

Behind the scenes, MTech ScanFind ran six discovery methods in parallel so it catches every kind of device:

- ARP broadcast on every detected subnet (catches every responsive host).
- Passive packet sniff on each interface (catches devices that send traffic but won't reply to ARP).
- Vendor UDP broadcasts (Hikvision SADP, Dahua, Uniview, Reolink, Axis, Bosch, Sony — about 15 manufacturers).
- ONVIF WS-Discovery multicast (finds standards-compliant cameras even across VLANs).
- TCP fallback probe on common camera ports (catches managed switches and locked-down devices).
- A final ICMP / TCP verification pass to drop stale ARP-cache entries — so disconnected devices don't keep showing up.

Reading the Network Inventory

Each row is one device. The columns are:

Column	What it means
IP Address	The device's IPv4 address.
MAC Address	The hardware address (used for vendor lookup).
Type	Brand identified from the MAC's OUI prefix.
Manufacturer	Full IEEE manufacturer name.
ONVIF	Yes if the device answered the ONVIF probe.
Location	Friendly label you assign (Lobby, Roof, etc.).
Model	Camera model — auto-filled by the enrichment pass.
Firmware	Firmware version — auto-filled.
Serial	Serial number — auto-filled.
Status	ONLINE / OFFLINE — colour-coded green / red.

Click any column header to sort by that column. Click the same header again to reverse the sort.

How the Model, Firmware, and Serial cells get filled in

As soon as the scan finishes, a background enrichment task probes every alive device:

5. Phase 1 — Parallel ping/TCP probes mark every device ONLINE or OFFLINE. Status updates within ~1 second.
6. Phase 2 — For each alive device, ONVIF GetDeviceInformation is called with your saved credentials, then vendor defaults picked from the Type column (Hikvision / Dahua / Axis etc.).
7. Phase 3 — If ONVIF doesn't answer, vendor-specific HTTP endpoints are tried (Hikvision ISAPI, Dahua magicBox, Axis VAPIX).
8. Phase 4 — As a last resort, the HTTP Server: header is read so even non-camera gear (routers, switches, printers) gets some identifying text in the Model column.

> **Tip:** The enrichment pass uses at most 6 credential attempts per device, well below typical lockout thresholds.

Saving the results

Each pane has Export TXT and Export PDF buttons on its right edge. Click either one to save the visible rows.

To export everything as a single CSV, use the CSV button in the top toolbar.

Chapter 4 — Live camera preview

MTech ScanFind streams live video from any ONVIF or RTSP camera. You don't need a separate viewer.

Open the preview

9. Right-click a camera row in either the Network Inventory or Confirmed CCTV Devices pane.
10. Choose Camera Preview … from the context menu.
11. A new window opens. While the app discovers credentials, the body says "Connecting…" — usually 1–3 seconds.
12. Live video begins streaming as soon as the connection succeeds.

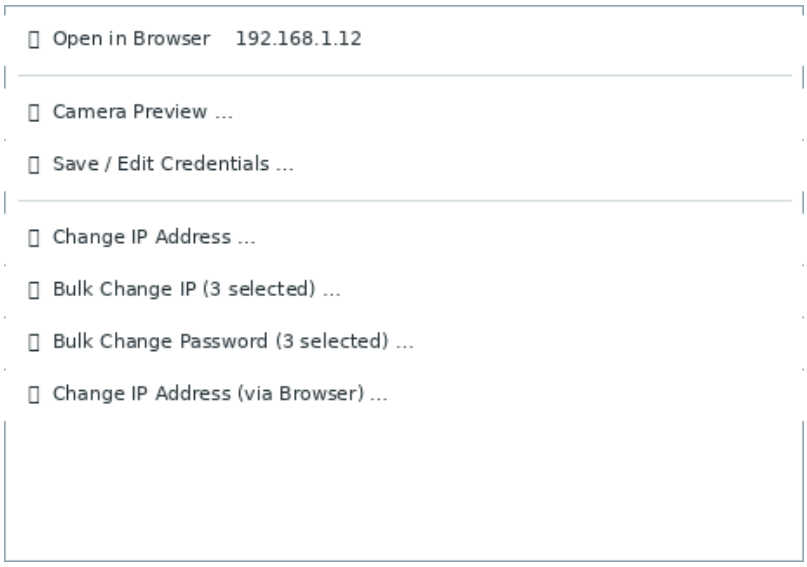

Figure: The right-click context menu on the Network Inventory

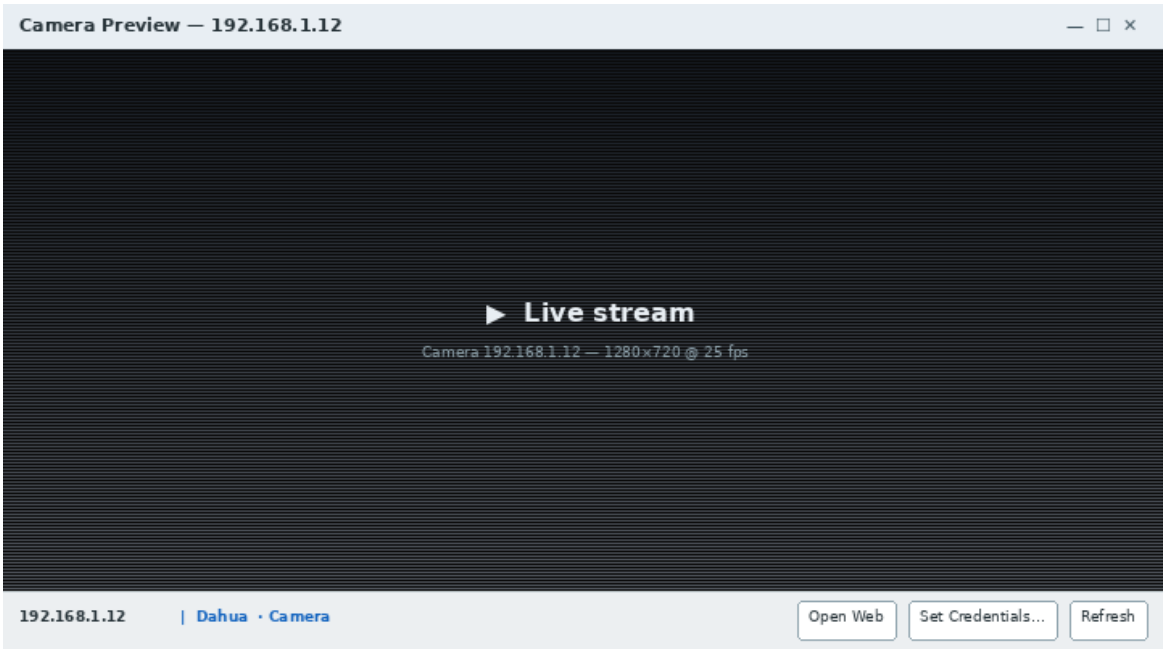

Figure: The preview window with a live stream running

Inside the preview window

- **Channel (NVR only)** — If the device is an NVR/DVR, a Channel dropdown appears at the top. Switch channels live.
- **Bottom bar — IP and brand** — Shows the camera's IP and vendor for quick reference.
- **Refresh** — Reconnect to the camera (useful after a power cycle).
- **Set Credentials...** — Open the credentials dialog if the auto-discovery fell back to default creds and you want to lock it to your real ones.
- **Open Web** — Launch the camera's web admin in your default browser.

Setting credentials manually

If MTech ScanFind couldn't authenticate using saved credentials or any vendor defaults, the credentials dialog pops automatically.

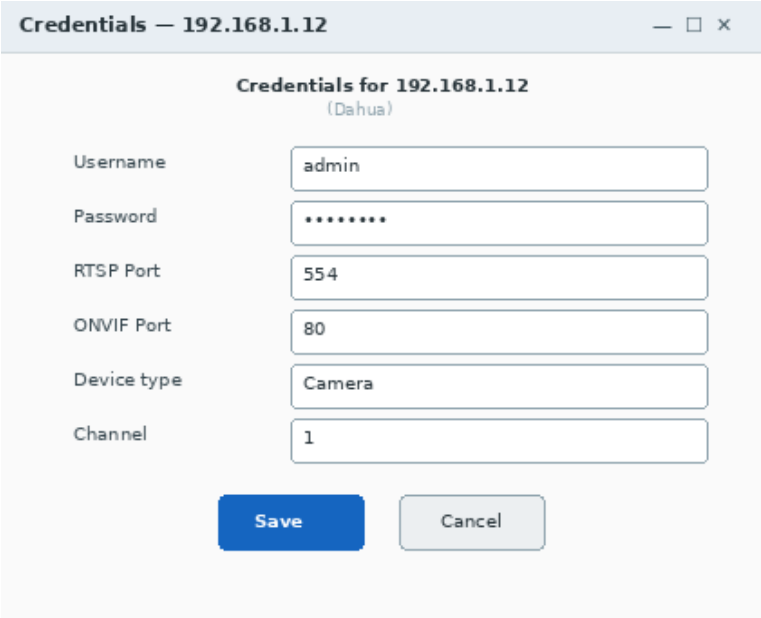

Figure: The per-camera credentials dialog

13. Type the camera's Username and Password.
14. Adjust RTSP Port (usually 554) or ONVIF Port (usually 80) only if your camera is non-standard.
15. Click Save. The preview re-runs with your credentials. On success, the credentials are remembered for next time.

Tip: Credentials are stored in camera_creds.json next to the .exe. Back this file up if you want to move the app to another PC without re-typing every password.

Stream quality and rendering

All previews render at the same widescreen size (720 × 400). The streaming loop:

- Forces RTSP over TCP (UDP is silently dropped by most routers).
- Picks the camera's sub-stream when available (lower bitrate / faster start).
- Drains stale buffered frames so the picture stays at the live edge.
- For DVR/NVR streams: uses a slightly larger jitter buffer and doesn't skip frames — DVRs serialize multiple channels onto one socket and need gentler handling.

- Stretches every source to fill the widescreen body so a 4:3 Dahua DVR stream takes up the same screen area as a 16:9 Uniview IP camera.

⚠ **Warning:** Closing the preview window stops the stream and frees the camera's RTSP session slot. Many doorbells and budget cameras only allow 1–2 concurrent RTSP connections, so leaving previews open can block other apps.

Chapter 5 — Changing a camera's IP address

MTech ScanFind can change a camera's IP via ONVIF (the standard way) and via vendor-specific HTTP fallbacks. For Uniview, it also speaks LAPI directly.

Single-camera change

16. Right-click the camera in the Dashboard.
17. Choose Change IP Address … from the context menu.
18. The Change IP dialog opens — pre-filled with the camera's current IP, the default mask (255.255.255.0), and a gateway guessed from the first three octets of the IP plus ".1".
19. Type the new IP. As you type, the Gateway field auto-fills to mirror the new IP's first three octets, ending in ".1" — until you click into the Gateway field and edit it manually.
20. Enter your camera's Username and Password.
21. Click Apply IP Change.

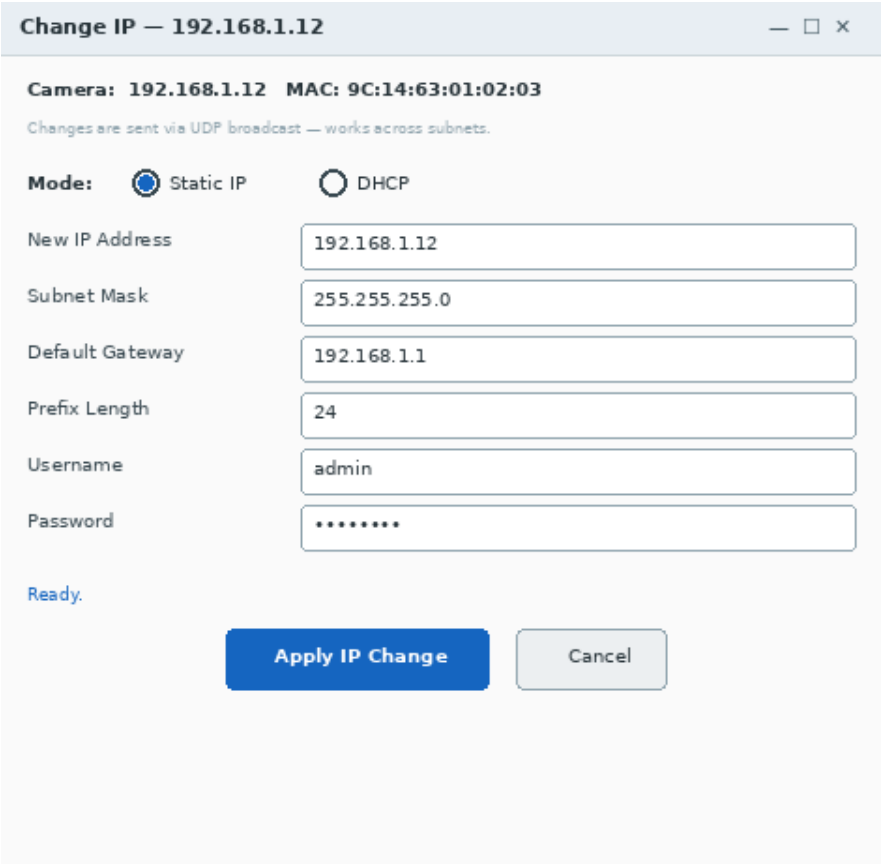

Figure: The single-camera Change IP dialog with the Static / DHCP toggle

Static vs DHCP

At the top of the dialog is a Mode selector with two radio buttons:

- **Static IP** — (default) — the new IP, mask, gateway and prefix fields are active. The camera is told to use exactly these values.
- **DHCP** — — the IP/mask/gateway/prefix fields grey out. The camera is told to switch to DHCP and will pick up a new address from your DHCP server on reboot.

⚠ **Warning:** After switching a camera to DHCP, you need to re-scan to find it again at its new address. The status bar will show the rebooting and reconnecting steps as they happen.

Bulk IP change (auto-increment)

To re-IP a whole group of cameras at once, use the Bulk Change IP dialog. This is the workflow most installers use when commissioning a new install.

22. Hold Ctrl and click each camera you want to re-IP in the Network Inventory or Confirmed CCTV Devices pane. (Or Shift-click to select a range.)
23. Right-click any selected row and choose Bulk Change IP (N selected) … — the menu item only appears once 2 or more rows are selected.
24. Type the Starting IP (e.g. 192.168.1.50). Every selected camera gets a sequential address: .50, .51, .52, …
25. Adjust Mask / Gateway / Prefix as needed.
26. Type the Username and Password (assumes all selected cameras share the same login).
27. Review the preview pane — it shows exactly which old IP will become which new IP.
28. Click Apply to N cameras and confirm the warning dialog.

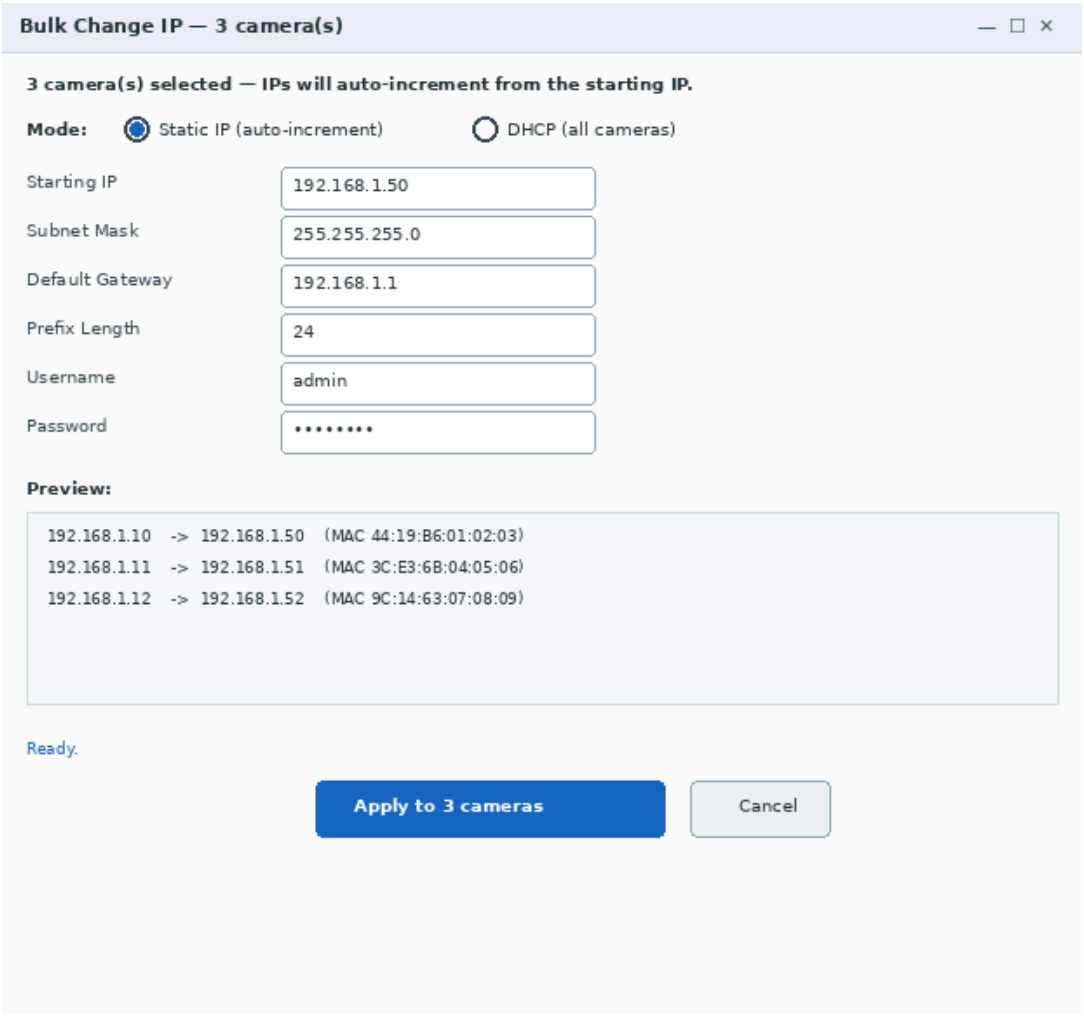

Figure: The Bulk Change IP dialog with auto-increment preview

 Tip: Switch the Mode to DHCP at the top to flip every selected camera to DHCP in one pass — handy when commissioning to a site where DHCP will assign reserved addresses.

⚠ **Warning:** Triple-check the preview pane before clicking Apply. Bulk IP changes are irreversible without going camera-to-camera.

Chapter 6 — Changing camera passwords in bulk

Standardising the admin password across every camera on a site is a common security-hygiene job. The Bulk Change Password dialog does it in one pass.

29. Multi-select 2 or more cameras in the Dashboard (Ctrl + click).
30. Right-click and choose Bulk Change Password (N selected) …
31. Type the Username, the current Old Password (must be the same on every selected camera), the New Password, and Confirm it.
32. Leave "Update saved credentials on success" checked — this automatically rewrites camera_creds.json for every camera that succeeds, so Camera Preview / Change IP / etc. keep working without manual re-saving.
33. Click Apply to N cameras and confirm.

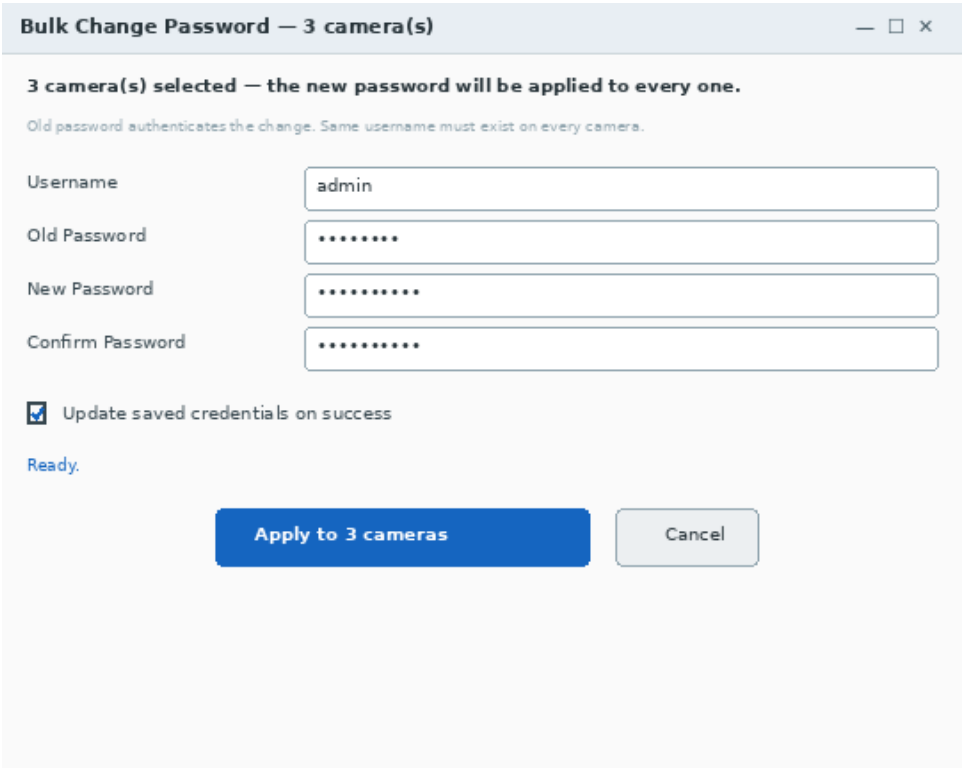

Figure: The Bulk Change Password dialog

⚠ **Warning:** A bad new password locks all of the selected cameras simultaneously. Read the confirmation dialog carefully before clicking Yes.

What happens behind the scenes

- For each camera, the app issues an ONVIF SetUser request with UserLevel: Administrator, trying common ONVIF ports (80, 8000, 8080, 2020, 8899) until one responds.
- If "Update saved credentials on success" is checked, the new password is written into camera_creds.json immediately on success — so the next preview / IP-change call uses it.
- Failures (auth fail, account locked, no ONVIF) are listed at the end with the underlying error so you can retry one-by-one.

Chapter 7 — Help and support

The Help tab in the sidebar contains everything you need to look up vendor defaults, manage the brand database, and reach MTech directly.

IP Cameras Password sub-tab

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

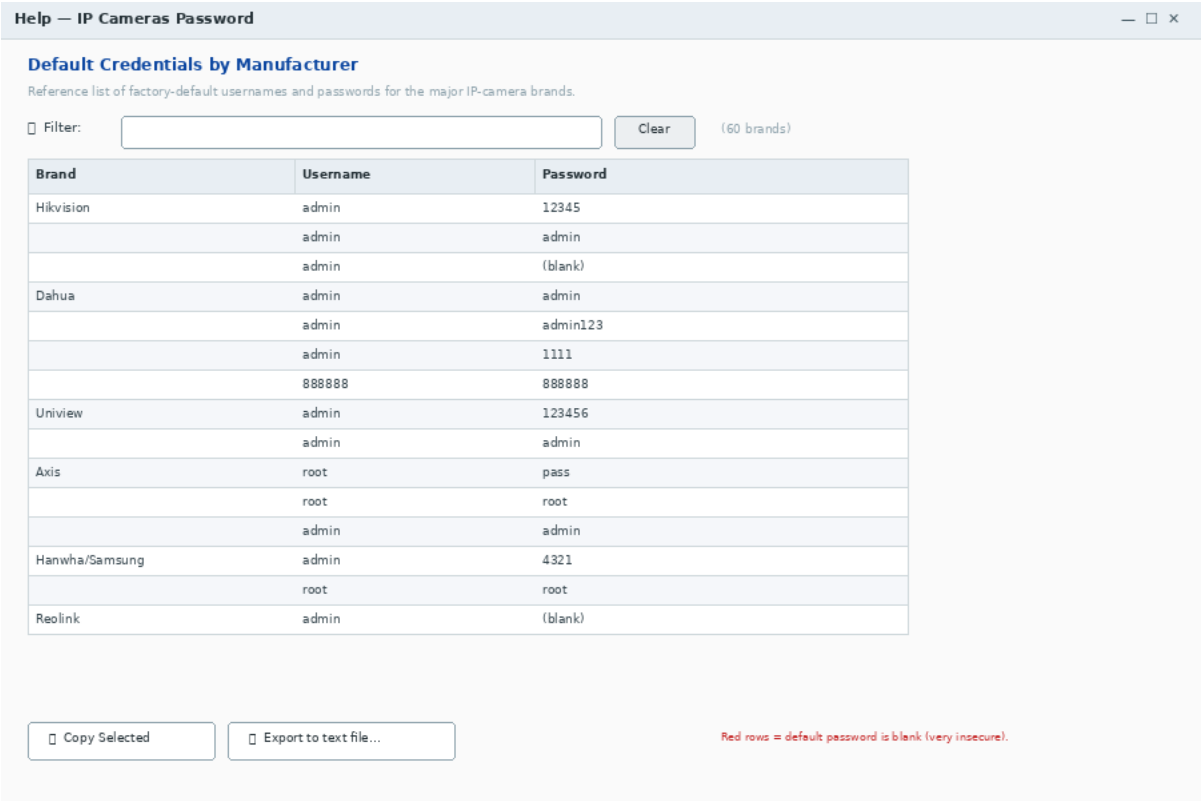

Figure: The IP Cameras Password reference table

- Type any text into the filter box to narrow the list by brand, username, or password.
- Red rows mark credentials where the default password is BLANK (extremely insecure — change immediately).
- Copy Selected copies the highlighted rows to the clipboard as tab-separated values (paste straight into Excel).
- Export to text file… saves the whole list as a plaintext reference you can email or print.

Cameras Brand sub-tab

The OUI-to-vendor database used by the scan engine to identify every device on the wire. Search any brand or MAC prefix to see the mapping.

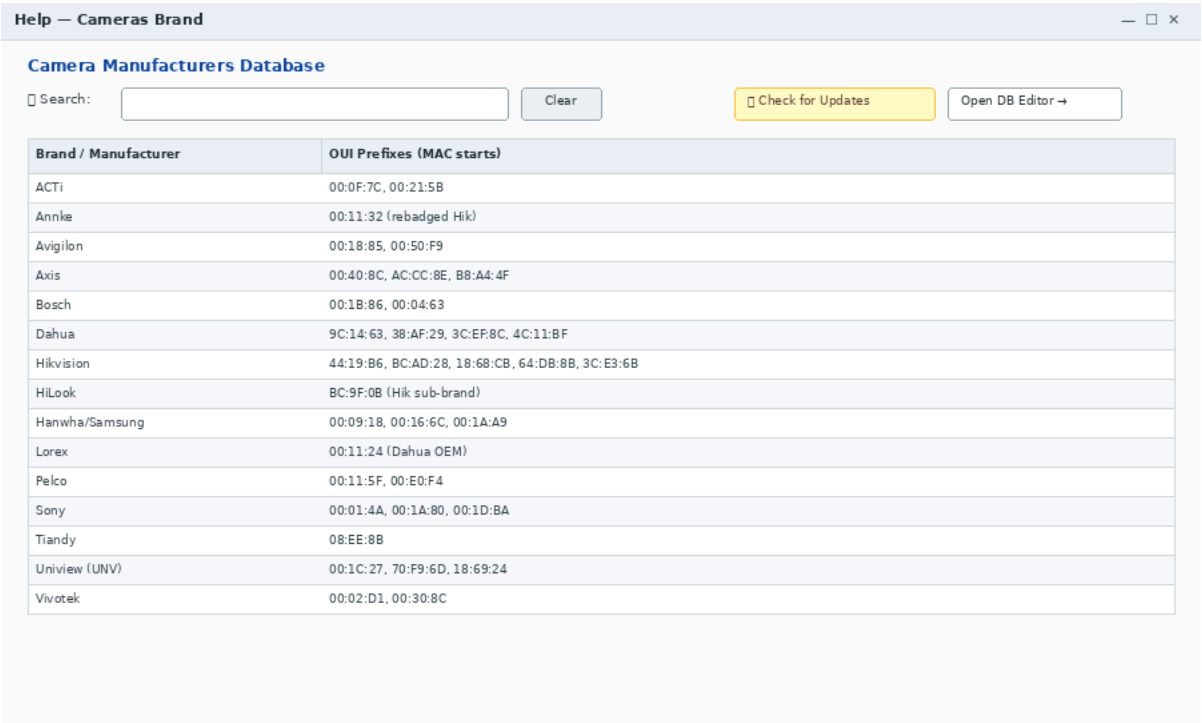

Figure: The Cameras Brand database — sortable, searchable

Check for Updates

The Check for Updates button (top right of the Cameras Brand tab) refreshes the IEEE OUI database in the background, then shows you any NEW camera-vendor OUIs that aren't yet in your brand list.

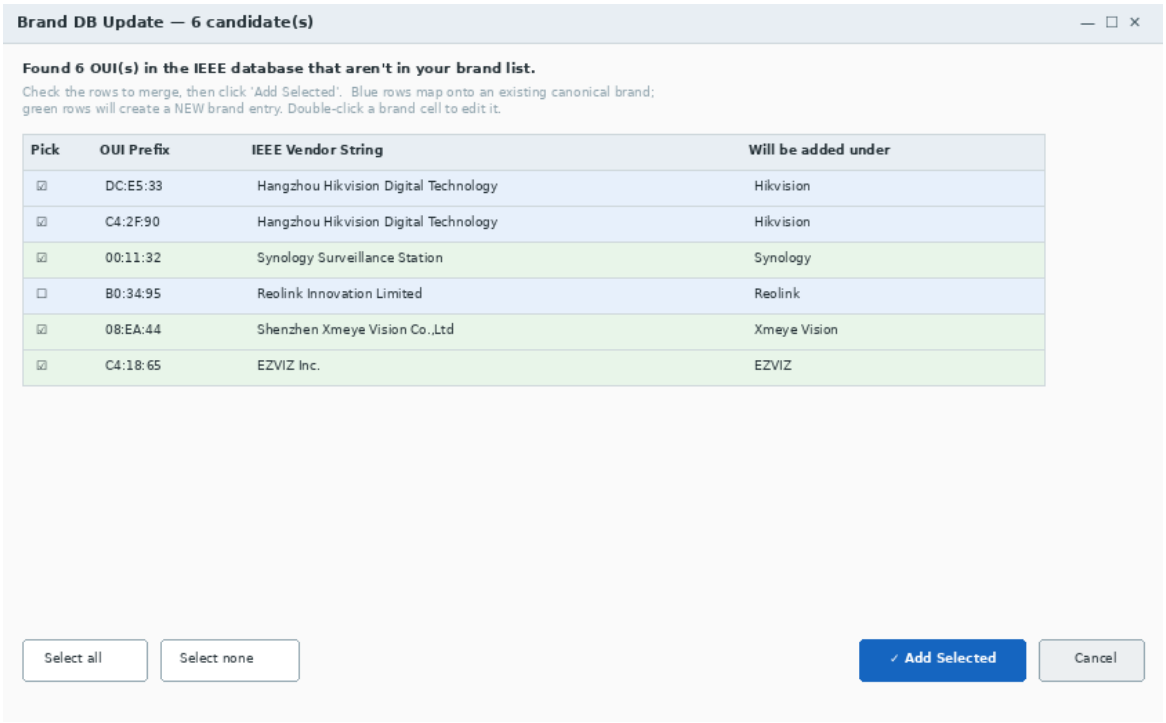

Figure: The Check for Updates dialog with discovered OUIs

34. Blue rows map onto an existing canonical brand (e.g. a new Hikvision OUI). Green rows propose a brand-new entry.
35. Toggle the ☑ in the Pick column to include / exclude rows.

36. Double-click the rightmost cell to edit the brand name before merging.
37. Click ✓ Add Selected. The new entries are saved to your custom brand database and used by every subsequent scan.

Support sub-tab

Three one-click email links go straight to sales@mtpsite.com:

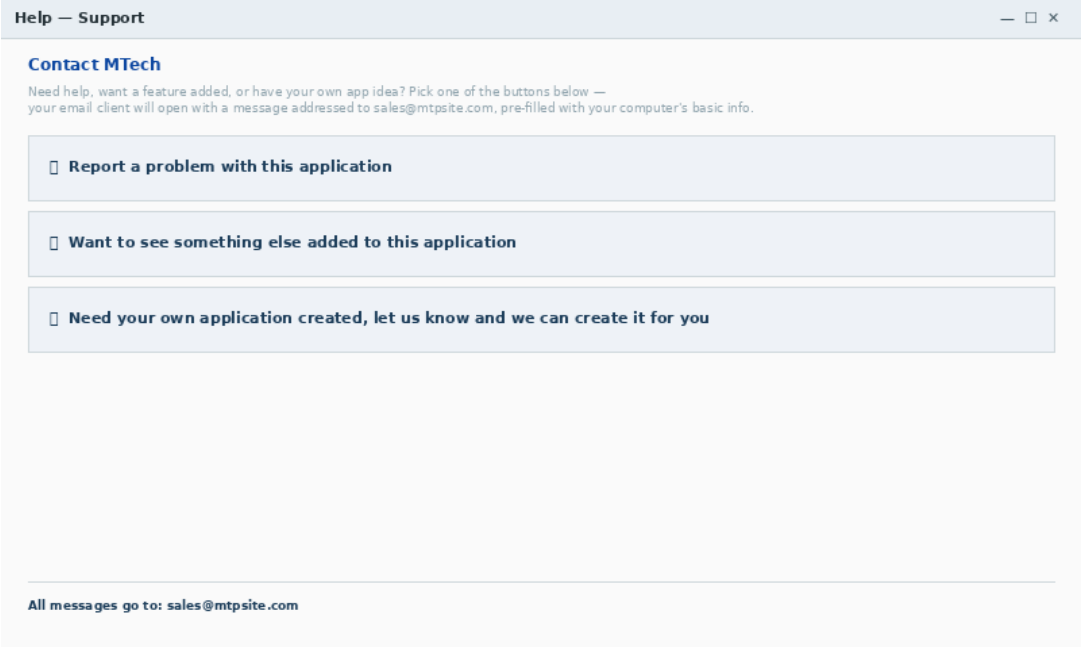

Figure: The Support sub-tab — three direct-contact links

- Report a problem with this application
- Want to see something else added to this application
- Need your own application created, let us know and we can create it for you

Each link opens your default mail client with the To, Subject and a body pre-filled with your computer's basic info (OS, username, local IPs, timestamp) so the MTech support team can follow up without a back-and-forth.

Chapter 8 — Troubleshooting cheat sheet

Scan finds fewer devices than expected

- Make sure your PC is on the same physical LAN as the cameras. VPNs and virtual Hyper-V adapters can hijack the default route.
- Open Settings → Scan Segments and confirm every subnet you care about has its checkbox ticked.
- Click Run Scan a second time — passive sniff and proprietary broadcast take a few seconds to catch silent devices.

Camera Preview won't connect

- Click Set Credentials… and enter the real username and password.
- Make sure the camera's web UI isn't open in another tab — doorbells and budget cameras often only allow one connection at a time.
- If port 554 is closed on the camera (RTSP disabled in its settings), enable it via the camera's web admin first.

Change IP says "ONVIF returned False"

- Some cameras stage the change and only commit on reboot — wait 30 seconds, then re-scan.
- Run MTech ScanFind as Administrator. Cross-subnet IP changes need the subnet-trick alias which requires admin rights.
- Open change_ip_debug.log next to the .exe — every attempt is logged in detail with the exact HTTP / ONVIF responses.

Live preview is slow or laggy

- Click Refresh to force a fresh connection. The sub-stream discovery may need re-running if the camera was just rebooted.
- Check your network. RTSP-over-TCP needs steady bandwidth; on Wi-Fi, move the PC closer to the AP.
- Confirm the camera's sub-stream is enabled in its web UI. Many cameras ship with the sub-stream disabled by default.

Status column stuck on "Pinging…"

- The first ping pass runs immediately after the scan — usually 1–2 seconds. If status stays "Pinging…" for more than 15 seconds, the device is blocking ICMP. Open the Set Credentials dialog and the TCP probe should confirm it's reachable.

Need more detail

Every feature, dialog, and setting is documented in depth in the Comprehensive Manual that ships alongside this guide (MTech_ScanFind_Comprehensive_Manual.docx).