BYSEC™
SECURITY SYSTEMS

USER MANUAL

CamVerifier
GDPR audit of camera systems

Professional tool for installers and administrators of camera systems · automatic network scan · 20+ GDPR tests · PDF report + certificate · tier model from trial to enterprise · support for Hikvision, Dahua, BYSEC™, Milesight and ONVIF devices.

VERSION	LANGUAGE	PAGES
V1.0 · 05 / 2026	EN	18

CONTENTS

Manual **contents**

BEFORE FIRST LAUNCH
Before installation make sure you have network access to the cameras (LAN or VPN) and know the admin passwords of the devices. CamVerifier runs entirely locally — no data leaves your computer. For Pro and Max tier you need a license key from BySec, s.r.o.

CHAPTER 1

Introduction and **tier model**

CamVerifier is a professional software tool for GDPR audit of camera systems. It automatically discovers IP cameras and NVRs on the network, runs more than 20 security and GDPR compliance tests, and generates a signed PDF report. Work that normally takes hours of manual verification and writing is done in minutes.

Who CamVerifier is for

Installers and integrators document project handover to the client. IT administrators audit their own CCTV systems from a GDPR perspective. Auditors and internal audit get verifiable technical evidence. Premium home CCTV owners can verify the security of their installation.

Four license tiers

CamVerifier is available in four tiers — from the free Trial for trying it out up to Max with unlimited devices and white-label branding in the PDF. The tier is set when the license key is issued and is baked into the key's signature (Ed25519). To move to a higher tier, contact BySec, s.r.o. via infomail@bysec.sk.

Tier	Price	Devices	PDF watermark	White-label
Trial	€0	4	TRIAL	—
Basic	€9.99/year	16	—	—
Pro	€19.99/year	64	—	—
Max	€49.99/year	unlimited	—	yes

BYSEC™ B2B PARTNERS
Installers who deliver BySec, s.r.o. camera systems get a Basic license for free as a benefit. Just contact infomail@bysec.sk with an invoice or order number.

Security and privacy principles

Local processing. CamVerifier runs exclusively on your computer. It does not communicate with BYSEC cloud or third parties; scan results and camera snapshots stay in the local file `app_state.json`.

No personal data. IP addresses and camera passwords are technical identifiers of devices, not personal data under GDPR. BySec, s.r.o. is neither a processor nor an intermediary of your client data.

Signed keys. License keys are signed with Ed25519 asymmetric cryptography. The application verifies signatures offline via an embedded public key — no internet required.

CHAPTER 2

Installation · **macOS and Windows**

CamVerifier is available as native applications for macOS (Apple Silicon and Intel) and Windows 10/11. The installer is self-contained — no system dependencies are installed. On first launch, the application downloads a supporting browser (~150 MB) needed for accessing some NVR APIs.

Installing on macOS

STEP 1 Open bysec.sk/software/camverifier in your browser and click Download for macOS. The file `BYSEC_Verifier.dmg` will download.

STEP 2 In Finder, double-click the downloaded DMG — a virtual disk will mount with the application and an Applications shortcut.

STEP 3 Drag the BYSEC Verifier.app icon into the Applications folder. When installing a newer version, confirm replacement.

STEP 4 Eject the virtual disk (right click → Eject) and open the application from Launchpad or Applications. On first launch macOS will display a security dialog — click Open.

Installing on Windows 10 / 11

STEP 1 Download `BYSEC_Verifier_Setup.exe` from bysec.sk/software/camverifier.

STEP 2 Run the installer. If Windows Defender SmartScreen displays a warning (the installer is not code-signed for Microsoft), click More info → Run anyway.

STEP 3 Walk through the installer: target folder, desktop shortcut, Start menu entry. By default it installs to `C:\Program Files\BYSEC Verifier`.

STEP 4 Launch the application from the Start menu or desktop. On first launch, Windows Firewall may ask for permission for a local port — allow Private networks.

CHROMIUM DOWNLOAD ON FIRST LAUNCH
On first launch the application automatically downloads an embedded Chromium browser (~150 MB) used for logging into some NVRs (BYSEC™ Raysharp OEM, Dahua). The download runs in the background and takes 1–3 minutes depending on connection speed. You can continue with other work — but camera testing won't start until it finishes.

CHAPTER 3

License and **activation**

Without a license key, the application runs in Trial mode with a 4-device limit and PDF reports marked TRIAL. For full functionality, activate the license via the License tab. Activation is offline — no internet required.

Trial — no activation

Trial mode activates automatically on launch if no license is installed. The tier badge in the top-right of the topbar shows Trial · 4. Clicking the badge opens a dialog with a tier overview and a license purchase button.

Trial version allows you to:

- Scan the network and find all devices (but only the first 4 are listed)
- Run full GDPR tests on 4 devices
- Generate PDF reports with a TRIAL · bysec.sk watermark on every page
- Generate a GDPR certificate with watermark (not valid as proof)
- Test all features of the application before purchase

Full license activation

After purchasing via Stripe Checkout, you receive a key by email in the format `BYSEC1-eyJwYXlsb2FkIjp7...`. The key is a long string (about 400 characters) — copy it in full including the `BYSEC1-` prefix.

STEP 1 In the application, click the License tab in the top navigation.

STEP 2 In the Activate offline section, paste the full license key into the text field.

STEP 3 Click the Activate key button. The application verifies the key signature offline and stores it in the application data folder.

STEP 4 After successful activation, the tier badge in the top-right changes from Trial · 4 to your purchased tier (e.g. Pro · 64). The TRIAL watermark will disappear on next report generation.

TRANSFERRING THE LICENSE TO ANOTHER COMPUTER
The license key is not tied to a specific computer — you can transfer it to another machine. However, one license key allows simultaneous activation on only one installation. Before transfer we recommend removing the key from the old installation via License → Remove.

Tier badge and upgrade dialog

In the top-right corner of the application, a colored badge shows the current tier: orange Trial, blue Basic, green Pro, purple Max. Next to the label is the maximum number of devices (4 / 16 / 64 / ∞ for Max).

Clicking the Trial or Basic badge opens an upgrade dialog with a tier comparison and a direct link to purchase a license (bysec.sk/software/camverifier). The dialog also has an I have a key button which switches to the License tab and focuses the key input field.

White-label in the Max tier

The Max tier lets you replace BYSEC™ branding in PDF reports with your own company name. The client sees your report — you keep your primary brand without a third party. White-label is set when the license is issued via the parameter `--white-label-company "Your Company Ltd."` and is written into the license key. Once activated in the application, all generated reports are automatically branded with the new name — the BYSEC logo in the header is replaced with the company text, and the footer contains the company name instead of BySec, s.r.o. · www.bysec.sk.

WHITE-LABEL EXAMPLE
Installer AlphaSec Security Systems Ltd. delivers a camera system to client ABC Trade Ltd.. The Max license has white_label_company = AlphaSec Security Systems Ltd. The generated PDF report shows only the AlphaSec brand — the client never sees BYSEC anywhere. The installer sells the audit as their own service.

CHAPTER 4

Network **scan**

On launch, the application automatically detects your local network via the OS interface (netifaces) and pre-fills the scan range. For most home and small-business installations it's enough to click Start scan — the application finds all cameras and NVRs on the network in 1–3 minutes.

Network auto-detection

When you open the Scan tab, a green info banner appears with the detected network:

> Your network detected: `192.168.1.0/24` · router `192.168.1.1`

Detection works for standard ranges 192.168.x.x and 10.x.x.x. To manually enter a different range (e.g. a VPN tunnel or remote network), click the Other network… button and enter the range in CIDR format (e.g. `10.8.0.0/24`).

ONVIF WS-Discovery

Built-in support for ONVIF WS-Discovery finds cameras that announce themselves on the network via multicast (UDP port 3702). These cameras are discovered immediately, without scanning each IP address. WS-Discovery is enabled by default — in settings you can disable it if a firewall blocks it and you want only an IP scan.

Port scan

For IP addresses in range, ports 80, 443, 554 (RTSP), 37777 (Dahua), 8000 (Hikvision) and 9000 (BYSEC™ Raysharp OEM) are checked. An open port indicates that a camera device runs at the address. For speed the scan runs in parallel (10 threads) — a full /24 net (254 addresses) usually takes 30–60 seconds.

Fingerprint and identification

After discovering a device, the application runs fingerprinting — it sends HTTP requests to typical camera URLs and determines the brand (BYSEC™, Hikvision, Dahua, Milesight) and type (camera / NVR) from the response. Identified devices are added to the list in the Devices tab with pre-filled type and brand.

> **TIP — VPN INSTALLATIONS**
> If you scan a client's network over VPN, WS-Discovery may not work (multicast is not tunneled through most VPNs). In this case, disable WS-Discovery and use only IP scan for the specific range. Scans over VPN are slower due to latency — for 100+ cameras count on 5–15 min.

CHAPTER 5

Devices · list and passwords

The Devices tab contains a list of all discovered or manually added cameras and NVRs. For each device you set login credentials, type, edit or remove. Without correct passwords, tests fail with unauthorized.

Manually adding a device

If a scan didn't find a device (e.g. it's in another segment or blocks SYN scan), add it manually via the Add device button. Fill in:

- IP address — required (e.g. `192.168.1.151`)
- Port — default 80 (HTTP), 443 for HTTPS
- Username — admin account, usually `admin`
- Password — admin password of the device
- Type — camera or NVR (decides which tests run)

TRIAL LIMIT ON THE 5TH DEVICE
Trial mode allows a maximum of 4 devices. Attempting to add a fifth shows the upgrade dialog with a tier comparison and a purchase button. The existing 4 devices remain intact — for a larger limit, activate Basic (16), Pro (64) or Max (∞) license.

Bulk credentials check

To quickly verify all passwords at once, click Verify passwords in the Devices tab. The application tests login on each camera in parallel and marks the rows:

- Green — password OK, device ready for testing
- Red — password wrong or device rejected login
- Gray — device unreachable (timeout, network error)

For red rows directly in the list, fix the password and click Save — a green flash confirms saving. The feature saves significant time in large installations (50+ cameras), where you can have many different passwords from clients or default manufacturer passwords.

Editing and removal

Clicking a device row in the list opens an edit dialog. You can change IP, port, login credentials, type, or completely remove the device with the Delete button. Removal also discards the device's test results.

CHAPTER 6

Testing · **process and results**

After setting passwords, click Start testing in the Devices tab. The application runs 20+ GDPR tests in parallel on each device. Testing one camera takes 5–30 seconds, an NVR 30–90 seconds (depending on number of channels and connection speed).

Test modes

When starting tests you choose a mode:

- All devices — retests every device in the list from scratch
- Only new — tests only devices without results yet (added since last test)
- Only failed — retests devices with errors (error, unreachable) after fixing password or network

Incremental testing (Only new / Only failed) saves time significantly in large installations. With 117 HYZA cameras, initial testing takes 30 minutes, retesting a fixed segment after a few days 3 minutes.

Progress monitoring

During testing the following is shown:

- Progress bar — number completed of total devices
- Current device — IP address and test phase
- Test log — line-by-line event output (success, error, warning)
- Preliminary results — Results tab updates live, you can watch the score during the test

STOPPING A TEST
You can stop the test at any time via the button in the progress section. Already completed results are kept — when restarting in Only new mode, the application continues with the untested devices.

Results tab

The Results tab shows a summary of all devices with color-coded GDPR scores:

- Green 80–100 — device meets GDPR requirements
- Yellow 50–79 — partially, weak points should be fixed
- Red 0–49 — serious shortcomings, GDPR not met
- Gray ? — not tested (unreachable / error)

CHAPTER 7

GDPR tests **in detail**

CamVerifier performs 20+ automated tests grouped into three categories: security (passwords, encryption, ports), configuration (firmware, NTP, retention period) and additional (privacy zones, AI detection, audio). Each test has a weight in the final GDPR score.

Security tests

Password strength. Tests length, complexity and matches against the HIBP database of known breached passwords. Default passwords like admin/admin or 12345 score 0 points.

HTTPS interface. Verifies whether the camera supports HTTPS for the admin interface. Unencrypted HTTP is a GDPR risk.

RTSP without authentication. Checks whether the RTSP stream is available anonymously. Open RTSP allows anyone on the network to view the recording.

Open ports. Identifies risky ports (Telnet 23, FTP 21, SSH 22 with default passwords) and classifies them by risk.

P2P connection. Cloud P2P services of cameras (e.g. Hikvision Hik-Connect, Dahua P2P) transmit stream via Chinese servers. For GDPR compliance it should be disabled.

UPnP and port forwarding. Automatic port opening on the router via UPnP is a serious GDPR risk — cameras become publicly accessible on the internet without the owner's knowledge.

Configuration tests

Firmware age. Compares the current firmware version with the online database of manufacturers, which the application automatically synchronizes. Firmware older than 2 years is aging, older than 4 years outdated. CVE vulnerabilities are flagged automatically.

NTP synchronization. Tests whether the camera has an NTP server set and time is synchronized. Wrong time means unusable video evidence in case of an incident.

Retention period (NVR). For NVRs, the actual recording length is tested from HDD capacity and channel bitrates. GDPR requires a purpose for retention — typically 7–30 days.

HDD status (NVR). Disk status: SMART status, temperature, fill level. A full disk means new recordings overwrite old ones faster than planned retention.

OSD camera name. Visual overlay in the recording (camera name, time). GDPR requires that it be clear from the video who/when and where is recorded.

Privacy zones. Checks whether the camera supports and has active privacy zones (masking of areas that may not be recorded — e.g. neighbors' windows, private spaces).

Additional tests

Audio recording. A microphone in the camera is usually at odds with GDPR (audio recording is far more invasive than video and requires a stronger legal basis). The test detects whether the camera has audio active.

AI person/vehicle detection (PVD). Person/Vehicle/Detection — for GDPR this means the camera profiles subjects. Requires DPIA and a specific legal basis.

Clock drift. Time drift of the camera vs NTP. A drift greater than 5 minutes means video timestamps are not trustworthy for forensic analysis.

IR cut-filter (test). Active test of switching between day and night modes — a camera with broken IR cut-filter produces unusable video at a certain time of day.

Image snapshot. Visual check of a live snapshot — verifies the camera is actually capturing and the image is readable (not black, white, or corrupted).

ADAPTIVE TESTING
Not every test runs on every device. The application detects the type (camera vs NVR), brand (BYSEC™, Hikvision, Dahua, ONVIF) and selects relevant tests accordingly. For example, HDD status is tested only for NVRs, Privacy zones only for cameras that support it. The total number of tests is therefore slightly different on each device (15–22 tests).

CHAPTER 8

Report **generation**

After testing is complete, go to the Report tab. Fill in client and installer information, choose language and export type, and click Generate PDF. The application creates a professional document with a cover page, one page per device, summary, and an optional GDPR certificate.

Project information

Before generation, fill in the Report tab:

- Customer — company name or person (client)
- Site — installation address (building, city)
- Installer — your name or company (entity generating the audit)
- Notes — free text for specific info (order number, client contact…)
- Language — SK or EN (also switches text in the PDF)

PDF report structure

Cover page. BYSEC™ branding (or white-label in Max tier), project name, audit date, number of devices tested, summary GDPR score, installer identification.

One page per device. Identification (model, FW, IP, MAC), snapshot from the camera, test table with OK/FAIL/N/A status, GDPR score with breakdown by category, open ports, password strength, recommendations for fixing.

NVR channel pages. NVRs additionally get a 4×N grid with mini-snapshots of all channels, retention period, HDD status.

Summary page. Table of all devices with GDPR scores, total statistics (number OK / aging firmware / open ports), diff vs previous report (if any), GDPR checklist (manual questions for the installer).

GDPR certificate

A separate PDF document in A4 landscape format, designed as a compliance certificate with a decorative frame in BYSEC™ colors. Serves as an internal record of the audit. Generated via the Generate certificate button in the Report tab and contains:

- Identification of the client and site
- Audit date and report number
- Number of devices tested and average GDPR score
- Result: COMPLIANT (score ≥ 70) or NON-COMPLIANT
- Identification of the installer and a signature field (you can print and sign manually)

Excel and CSV export

For further data processing (analysis in your own spreadsheets, import to CMDB, audit log), CSV and XLSX exports are also available. They contain a list of devices with identifiers, test results and GDPR scores in columns. For large installations (100+ devices) Excel contains color-coded rows by score.

CHAPTER 9

History **and diff**

On repeat audits (e.g. yearly check of a camera system), CamVerifier compares the current state with the previous report and adds a Changes since last audit section to the new PDF. Very useful for continuous GDPR monitoring.

Report history

Every generated PDF report is automatically saved to `reports_history.json` in the application data folder. The history contains:

- Report ID — unique identifier in form `R-2026-0042`
- Report version — increments on repeated audits of the same project
- Timestamp — when the report was generated
- Device snapshot — state at audit time (firmware, ports, score)
- PDF path — where the file is stored

Diff between audits

On the second audit of the same project, a section Diff since previous audit is added to the PDF with a table of changes:

- Devices added — new cameras or NVRs on the network
- Devices removed — devices that were in the previous audit but not now
- Firmware change — camera has a newer/older version
- GDPR score change — improvement or worsening by ≥ 10 points
- Open ports change — added/closed ports
- Password change — password was changed (strength is rechecked, but content is not)

DIFF FILTER — IGNORE GDPR SCORE NOISE
The diff ignores minor GDPR score fluctuations (< 10 points) — these can arise from test variance (network latency, timeouts). Real changes are firmware, channel count, open ports and passwords — these are always flagged regardless of change size.

CHAPTER 10

Tips and **troubleshooting**

The most common scenarios that occur in real audits and their solutions. For a specific problem not in this chapter, contact support via infomail@bysec.sk.

Scan finds no devices.

Check that you are connected to the same network as the cameras (LAN, not WAN). Test ping to a known camera IP from terminal. If ping works but scan doesn't find anything, the issue is with WS-Discovery (firewall) — disable WS-Discovery and use only IP scan. WS-Discovery also doesn't work over VPN.

Scan finds fewer cameras than expected.

Check the scan range — cameras may be in a different subnet (e.g. 192.168.10.0/24 instead of 192.168.1.0/24). Enter multiple ranges separated by comma. Or some cameras have ONVIF discovery disabled and standard ports closed — add them manually by IP.

Login fails with 401 or 403.

Most common cause is wrong password. Check that you use the admin account (not a limited user). Some cameras require two-factor (captcha or security questions) — these Verifier doesn't support, disable them in the camera's admin interface. For Raysharp OEM (BYSEC™ TM) check the password doesn't have special characters outside ASCII.

Test takes disproportionately long.

Some cameras respond slowly or don't implement all ONVIF endpoints and Verifier waits for timeout (usually 10s/test). For faster testing you can temporarily disable problematic devices and test them separately later.

PDF report can't be generated / crashes.

Most common cause is a damaged snapshot from a camera. If the Base64 snapshot is too large or corrupted, ReportLab can crash the process. In the Report tab disable Include snapshots and generate PDF without snapshots — this usually helps. Snapshots are missing but other data is preserved.

Key activation fails.

Check that you copied the full key including the `BYSEC1-` prefix without spaces or line breaks. The key must be on a single line. If you copied from email, open it in a plain-text editor (TextEdit, Notepad) and paste from there — rich text can add invisible characters.

Auto-update doesn't work.

The application checks for updates every 24 hours automatically. If the server is unavailable (firewall, VPN), the check silently fails and retries later. For manual check, click the version badge in the top-right of the topbar.

Useful commands for dev and debug

CamVerifier doesn't need a terminal for normal work, but for advanced users and troubleshooting:

Clear application state: close the app, delete `app_state.json` in the app data folder (Mac: `~/Library/Application Support/BYSEC/Verifier/`, Win: `%APPDATA%\BYSEC\Verifier\`). The application starts with empty state.

Open log: all app events are written to `verifier.log` in the same folder. For issues, send this file via infomail@bysec.sk.

Reset license: in the License tab → Remove or manually delete `license.key` from the app folder. The application switches to Trial mode.

Security info: the license key is signed with Ed25519, verified offline. The application sends no usage telemetry — only during the auto-update check it downloads a small JSON manifest.

CHAPTER 11

Warranty, **support and contact**

The CamVerifier license includes technical support and lifetime updates within main version 1.x. For any issues, contact us — Pro and Max licenses have priority support.

Warranty and license lifecycle

The license is lifetime for all 1.x versions of the application. After payment, no renewal is needed — the key works forever within the main version. Version 2.0 (planned for 2027+) will require a license upgrade with preferential pricing for existing customers.

On return within 14 days (EU consumer protection law) the license will be deactivated and payment refunded. For B2B contracts, contractual terms apply.

Technical support

Email: infomail@bysec.sk
Phone: +421 902 290 965
Hours: Monday–Friday, 08:00–17:00 CET

Response times:

- Trial: no guarantee
- Basic: 5 business days
- Pro: 24 hours on business days
- Max: 4 hours on business days + chat availability

Online resources

Product page: bysec.sk/software/camverifier
Download and license: directly from the product page
Demo PDF and documentation: available in the Materials section of the product page
Auto-update: the application notifies you of new versions — click the version badge in the top-right of the topbar
Firmware database: synchronized automatically every 24 h

Company identification

BySec, s.r.o.
Slovak technology company — security and IT solutions.

Reg. No.: 50 518 526
Tax ID: 2120353114
VAT ID: SK2120353114
Web: bysec.sk

FEEDBACK
Found a bug in the documentation, or have a suggestion for improving the application? Email us at infomail@bysec.sk with subject [CamVerifier Feedback]. Every feedback is valuable — the best ideas are reflected in upcoming versions. Max customers also get a roadmap call once a year, where you can directly influence the product direction.