ProVife User Manual

This manual covers version 2.4.41 of the ProVife video management platform: installing and starting the server, adding cameras and NVRs, user permissions, recording and storage, live monitoring, playback and search, AI scenarios, Store Analytics, license plate recognition and under-vehicle scanning, smart building, notifications and integrations, remote access and maintenance. Each section proceeds step by step using the button and field names on screen. Which screens you see depends on your account's permissions and your license; if you cannot find a page, use the Search menu box on the Control panel.

Contents

Getting started

Devices

Users and security

Recording and storage

Live monitoring

Playback and search

AI

Store Analytics

Plates and under-vehicle

Smart building

Notifications and integration

Remote access

Maintenance

Common issues

Getting started

Quick start

Follow the steps below to get to your first live view.

1. Install the main setup package (ProVife-2.4.41-Setup) on the server computer. Enter your company information, accept the agreement and check the network and storage pages.
2. Open Service Manager, create the initial administrator (admin) password with at least 12 characters and click Start.
3. Open ProVife Administrator, enter the server address (e.g., 192.168.1.10:7443), compare the certificate fingerprint using Verify server, then click SIGN IN.
4. Add cameras and NVRs from Control panel → Device Management.
5. Turn on the recording schedule on the Local Recording page; server recording is off by default for newly added channels.
6. Create separate accounts for operators in Account Management and grant camera permissions.
7. Install ProVife Surveillance on the monitoring computers and connect to the same server.

Applications: Administrator, Surveillance, Service Manager

The three applications are parts of the same system and serve different purposes.

Application	What it does
ProVife Administrator	Configures devices, users, roles, recording, storage, AI, integrations and maintenance. It appears as “Administrator Client” in the window title. Requires an account with administrative permission.

Application	What it does
ProVife Surveillance	The operator client: permitted live views, recordings, events, plate and store screens, PTZ. Installed with a separate setup package and does not include the server or AI components. The window title reads “Surveillance Client.”
Service Manager	Starts, stops and restarts the ProVife service on the server computer; shows the IP, HTTPS port, camera stream network, data folder and certificate fingerprint. Closing its window does not stop the service.

Pre-installation preparation

Plan hardware and network according to the number of cameras, resolution and analytics load.

- Operating system: 64-bit desktop or server edition. Installing the service requires operating system administrator rights.
- Network: The server computer must be able to reach the cameras and NVRs. Enable ONVIF and RTSP services on the devices and give the ONVIF user sufficient permissions.
- Time: Keep camera, NVR and server clocks consistent; use the same NTP server if possible.
- Storage: Check the free space and write speed of the recording drive. Make sure the service account can access this drive; network drives mapped only to a user session may not be visible to the service.
- Port: The default HTTPS port is 7443. Allow this TCP port in the firewall on the computers that clients will connect to.

The number of supported cameras depends on hardware, codec, frame rate and concurrent analytics; no fixed number is guaranteed. Measure with your real load during the trial period and monitor resource usage on the System information screen.

Installation

The main package is installed on the server computer, and the Surveillance package on the monitoring computers.

The main setup package includes the server, Service Manager and ProVife Administrator. The full setup wizard opens even if an existing installation is found; if the existing folder is selected, it installs over it and data is preserved.

1. Run the ProVife-2.4.41-Setup file. On the “Company information and installation agreement” page, enter the Company / organization name and email address, then read and accept the agreement. Installation does not proceed until it is accepted.
2. Check the Setup contents and Installation folder pages. The folder must be empty or be the existing ProVife application folder.
3. On the Network and time zone page, view the computer’s IPv4 addresses and time zone. The wizard does not change these settings; if needed, it opens the operating system’s network settings.
4. On the Server network page, select the Server listening address. If there is a second network adapter, a Second address and an optional Stream receive address can be selected.
5. On the Storage page, check the Data directory and retention period, then click Finish. Approve the permission prompt if it appears.

On the monitoring computers, run the ProVife-Surveillance-2.4.41-Setup package. This package asks only for the agreement page and installs into its own folder.

Starting the server: Service Manager

The server service is managed from the Service Manager window.

1. Open Service Manager with the operating system account that owns the data. The server data folder is found automatically; it appears on screen as “Server data and recording folder.”

2. On a new installation, type a password of at least 12 characters in the Initial admin password field. This password is created only once.
3. From the Server IP address list, select the network adapter that clients can reach. The HTTPS port is 7443 by default.
4. In the Camera stream network field, select a specific adapter or the “Balanced — all suitable network adapters” option.
5. Click Start. The database and service are prepared; the “Client connection: https://...” line and the SERVER CERTIFICATE · SHA-256 fingerprint appear.

The service runs under a restricted service account; no account password is requested. Stop waits for open recording segments to finish. Restart applies setting changes. While the server is stopped, recording selection and disk settings are changed from this window; while it is running, from ProVife Administrator.

First connection to the server and certificate

On first connection, the server’s identity is verified by its fingerprint.

1. Open ProVife Administrator or ProVife Surveillance. Type the IP and port in the Server address field (e.g., 192.168.1.10:7443).
2. If you will connect remotely, fill in the Remote address (optional) field; on the local network you can leave it blank.
3. Click Verify server. Compare the fingerprint in the Verify server identity window that opens, character by character, with the SERVER CERTIFICATE · SHA-256 value in Service Manager.
4. If the values are the same, click It matches, trust this server. If they differ, exit with Cancel and notify your system administrator.
5. Fill in the User and Password fields and click SIGN IN. Optionally, check the Remember password box.

The fingerprint is verified only once and is stored on this computer for that server address. If the server is reinstalled and its certificate changes, verification is requested again. If the server is on the same computer, the client uses the local loopback address in the background, so video does not drop even if the network adapter goes to sleep.

Menus and Control panel

Screens are reached from the top menu, and settings pages from the Control panel.

The top menu contains working screens such as Main View (live monitoring), Playback, AI Playback, Video Wall, AI Monitoring, License Plate Recognition, Store Analytics, Under-Vehicle Monitor and Time Lapse. Which buttons appear depends on the account's menu permissions.

In ProVife Administrator, the Control panel lists settings pages in groups:

- Basic configuration: devices, recording and storage, users and security.
- Application configuration: AI, alarms and notifications, Store Analytics.
- System configuration: system settings, time, updates, remote access, maintenance.
- Smart Home and Building Management: smart devices, scenarios, MQTT, Home Assistant, building plans.

The fastest way to find the page you need is the Search menu box at the top of the Control panel; type the page name or a word from its description. In the Surveillance client, the same field appears as Monitoring tools.

License and trial period

The trial period starts when the server is first launched; the license file is uploaded from the License screen.

On a new installation, a 15-day initial trial period starts when the server is first started. During this period all channels, analytics and under-vehicle scanning are enabled. Updating or reinstalling does not reset the period. When it ends, live streaming, new recording and analytics stop; camera settings, users and recording files are not deleted.

License type	Scope
Perpetual (lifetime)	Base package of 32, 64, 128 or 256 channels; additional channels per camera above 256. Each AI analytic is licensed separately by the number of channels it will run on.
Annual	One year; unlimited cameras and analytics.
Under-vehicle scanning	Separate for both types, by number of stations (under-vehicle + plate camera).

1. Open the Control panel → License page and copy the SERVER ID code.
2. Request your license file by sending the code to sales@provife.com.
3. Select the file you receive with Upload license file, then click Refresh status and check the scope.

> The license is tied to the server installation and the computer's hardware; it does not work in a data folder copied to another computer. Do not change the system date.

Devices

Device discovery on the network

Device Management automatically finds ONVIF devices on the network.

1. Open Control panel → Device Management and click + Add camera / recorder.
2. In the Devices found on the network section, open Search options. Choose Recording server's network or This computer's network; if needed, enter an IP / network range and ONVIF ports.
3. Click Search devices. Each device found is listed with its Model and Added status.
4. Check the devices to add and click Add selected. The same user name and password are used for the selected devices.

Discovery runs through the network adapter the server is connected to. If the cameras are on a different subnet, enter the range manually or add the device by its address. A device showing "… channels added" in the list is already in the system.

Adding cameras and NVRs

Add the device by IP address; NVR channels are imported automatically.

1. In the Add device window, enter an optional name (e.g., Main NVR) and the IP address / domain name.
2. Fill in the Port, User name and Password fields with the device's ONVIF credentials.
3. Click Add. All available NVR channels are added along with their names; existing channels are preserved.
4. Check that the status is Online in the channel list. Test the main stream and substream on a single camera first.

For a device without ONVIF support, use the Add via RTSP button: enter the Channel name, RTSP address, User and Password. An RTSP address adds a single channel; it does not provide features such as PTZ, device archive and events.

> Server recording is off for newly added channels. If you want recording, turn on the schedule using the steps in the Recording and storage section.

Device list and bulk actions

The Device Management list works with search, a status filter and bulk selection.

Each NVR and camera appears on a single row in the list: DEVICE / IP ADDRESS, status (Online, Connecting, Offline), event service status and SERVER RECORDING / ANALYTICS information.

- Search: Type in the Search device name, IP address or group box.
- Filter: Select All statuses, Online or Offline / connecting.
- Name and group: Select the row, click the Name / Group button and edit in the Device name and group window. This change does not interrupt live streaming or recording.
- Camera settings: Double-click the row.

1. Check the devices to remove, or use Select all.
2. Click Remove selected and check the number of channels in the confirmation window.
3. Confirm with Remove. Existing recording files are preserved; live monitoring, new recording and analytics stop for these channels.

Camera settings (ONVIF)

Encoder and image settings are applied to the camera via ONVIF.

1. Select the camera in Device Management and double-click it, or open Control panel → Camera Settings.
2. Select the profile to edit from the Stream profile list. Watch for the “Selected profile is used for ProVife recording” warning.
3. In the Video stream section, change the resolution, frame rate, bitrate and codec values.

4. In the Image and Color section, adjust settings such as brightness, contrast, white balance and wide dynamic range.
5. Click Apply to camera; use Read again to view the values again.

Setting limits are read from the device. If the device does not report a setting, the row appears as “The device did not report this setting” or as read-only. During a stream change, recording briefly stops and restarts, and other connections using the same encoder may be affected.

Organization tree and camera groups

A tree of sites, buildings, floors and sections keeps cameras organized.

1. Open the Control panel → Organization page.
2. Build the site > building > floor > section tree with New organization by entering an Organization name and selecting a Parent organization.
3. Search for cameras in the list on the right; use Select listed or check them one by one.
4. Select the target node in the tree and click Move selected.

The camera list on the left of the live monitoring screen is a tree: camera groups, NVRs and other cameras sit under headings. Create a camera group with + Group by typing a Group name (e.g., Parking lot) and selecting cameras. A camera can belong to only one group. Right-click a group heading and choose Edit group or Delete group; when deleted, its cameras move to “General.”

Graphical network topology

The Topology page reads switches and maps which port each camera is connected to.

1. Open the Control panel → Topology page.
2. Type the main switch’s IP address in the Switch address field and the SNMP v2c community name in the SNMP community name field, then save.
3. Click Scan network. Other switches connected via LLDP are found and read automatically.

4. On the map, the switch appears in the center with devices around it; the port number is written above the connection line.

View options can show IP, port, MAC or ProVife cameras only. Clicking a device opens its details; the Scan summary gives the numbers of open ports and of cameras found and not found. Cameras not found on a switch appear in a separate list. The list view gives a table with switch, port, IP and MAC columns.

Users and security

Creating a user account

Create a separate ProVife account for each person.

1. Open Control panel → Account Management and click New user.
2. Enter a user name and a password of at least 12 characters; select the role and click Create.
3. Select the new user from the list. Edit the Camera permissions and Menu access tabs.
4. Click Save permissions.

The user name can be 1–64 characters and may contain only A–Z, a–z, 0–9, periods, underscores and hyphens; spaces and accented characters are not allowed. Example: maria.smith.

New accounts cannot view video until camera permission is granted. You can temporarily disable an account without deleting it by unchecking the Account enabled box. Saved changes are also applied to open Surveillance sessions.

Roles and custom roles

The role determines which actions the account can perform.

Role	Permission
Viewer	View permitted cameras.
Operator	PTZ control and event acknowledgment in addition to viewing.
System administrator	All cameras and administrative actions.
Integration	Send events from external systems.

1. In Account Management, click Create custom role.

2. Enter a Role code (e.g., shift_supervisor) and a Display role name.
3. In the Camera actions section, check Live view, Recording view, Export, Event acknowledgment, Camera settings, Recording settings, Edit AI and Turn AI on/off.
4. In the Administrative actions section, select what is needed: Add devices, Users, Audit log, System monitoring, Person gallery, Smart Home use.
5. Click Save role and assign it to the user.

> Smart Home use (arming alarms, opening doors, operating devices, announcements) is not included in the Operator role by default; if needed, create a custom role that includes this permission.

Camera and menu permissions

Camera permissions, menu access and account status are applied together.

On the Camera permissions tab, live and recording permissions are granted separately for each camera. Narrow the list with the Search camera, NVR or IP address box.

- Enable live for all: turns on live view for the listed cameras.
- Enable recording for all: turns on recording view for the listed cameras.
- Disable live / recording: removes permissions for the listed cameras.
- Additional permissions: per-camera actions such as export and event acknowledgment.

Bulk actions apply only to the cameras currently shown in the list and are not sent to the server until you click Save permissions.

From the Surveillance Client menus list on the Menu access tab, select the screens the operator will see; the Enable all and Disable all buttons allow quick selection. Enabling a menu does not grant camera permission. Disabled menus are removed from the top menu and from the Control panel.

Password and session rules

Protect accounts with strong passwords and sign-in limits.

- For new accounts and the initial admin account, the password must be at least 12 characters.
- Failed password attempts are limited per client address: at most 10 attempts in 5 minutes.
- Camera passwords and email and MQTT passwords are stored encrypted on the server and never shown in plain text on any screen. A password field left blank keeps the saved value.
- The Remember password option stores sign-in information only on that computer; do not check it on shared computers.
- External sign-in rules are set on the Remote access page; rejected sign-ins are written to the audit log.

Password expiration, complexity rules and two-step verification are not available in this version. For this reason, keep passwords long, issue them per person and renew them when roles change.

> If you forget the administrator password, do not edit recording or database files manually; contact support@provife.com.

Audit log

Administrative actions on the server are logged with who performed them and when.

The Control panel → Audit Log page lists actions such as adding and removing devices, user and permission changes, saving settings, generating reports, keyword search, opening the barrier manually, bypass and alarm mode changes. The same records also appear on the Admin log tab of the AI Playback screen.

1. Open Control panel → Audit Log.
2. On each row, read the date and time of the action, the user who performed it, the action name and its target (camera, user, setting).
3. When investigating a specific incident, review the rows from the same time together with events on the AI Playback → Admin log tab.

To view the log, the account must have the Audit log administrative permission. Records are kept on the server; they are not lost even if the client is closed.

Recording and storage

Recording schedule

Recordings are written to the server's disk; recording must be turned on separately for each camera.

1. Open the Control panel → Local Recording page.
2. Select the camera and turn on server recording.
3. In the weekly schedule table, paint the hours to record with Draw mode; clear wrong areas with Erase mode.
4. After completing one day, copy it to the other days with Copy this day to the whole week.
5. For special days such as holidays, enter a date (YYYY-MM-DD) with Add exception; optionally select Off that day.
6. Click Save recording schedule.

The schedule determines at which hours a channel with recording turned on writes files. The client computer does not keep recordings; video opening on the client does not mean it is being recorded.

Time templates and bulk recording schedule

Apply the same schedule to many cameras at once.

1. Open the Control panel → Time Templates page and click + New template.
2. Enter a template name, draw the weekly hours and add special date exceptions if needed. Save the template.
3. In the Apply to cameras section, search for cameras or locations; check them with Select listed.
4. If you also want recording turned on where it is off, check the Turn on recording if off box.

5. Click Apply schedule and check the number of cameras that will change in the confirmation window.

Applying writes a copy of the schedule to the selected cameras. Changing the template later does not change the cameras automatically; you need to apply the new schedule again. Deleting a template keeps the schedules already applied.

Retention period and disk reserve

The retention period and reserve keep disk filling under control.

The retention period and disk reserve are changed in the Server / Storage Settings section of the Local Recording page or on the System Settings → FILE SETTINGS tab.

Setting	Description
Recording retention period (days)	1–3650 days. Expired recordings are deleted automatically.
Free disk space to reserve (GB)	When free space drops below this value, new recording stops while live monitoring continues.
Segment duration (seconds)	How often recording files are split; applied the next time the camera starts.
Maximum file size (bytes)	0 splits by duration only.
File type	Recording and export use the Matroska (mkv) format.

The Storage and disk status card at the top of the screen shows free space, retention days and the recording folder. If you see the “Below disk reserve. New recording stopped” warning, export old recordings, review the reserve or increase disk capacity.

Encryption and data protection

Know which data is kept encrypted and how to protect recording files.

ProVife encrypts all traffic between the client and the server (sign-in, live video, playback, events) with TLS. The server's identity is verified by its certificate fingerprint.

- Camera passwords and email, MQTT and smart device credentials are stored encrypted on the server.
- Face templates and small face images in the face gallery are stored encrypted; deleting a person deletes both.
- The topology community name is stored encrypted and is never returned in any response.

In this version, video recording files are not encrypted on disk; they are stored as mkv. To protect recordings:

1. Encrypt the recording drive using the operating system's disk encryption feature.
2. Make sure only the service account and authorized administrators can access the recording folder.
3. Review access permissions before sharing exported files; grant the Export permission only to those who need it.

Video archive backup

Copy recordings from selected cameras to another folder.

1. Open Control panel → Video Archive Backup.
2. Select the backup folder. It cannot be inside the recording folder; a separate drive is recommended.
3. In the Cameras field, select the cameras to back up. If left empty, all recorded cameras are copied.
4. To limit network or disk load, enter a Bandwidth limit (KB/s); 0 means no limit.
5. Click Save to store the setting and Copy to start copying. Click Cancel to stop if needed.

Copying is started manually; source recordings are not deleted. The result line shows copied files and errors. The copy stays in the folder and is not linked back to the system; the files can be opened with a media player when needed.

A video archive backup is not a configuration backup or a standby server. To protect your settings, see “Configuration backup” in the Maintenance section.

Live monitoring

Layouts and camera list

Arrange cameras in the layout you want on the Main View screen.

1. Open Main View from the top menu.
2. Choose the number of tiles from the layout strip: 1, 4, 9, 16, 25, 36, 49 or 64.
3. Drag a camera from the camera tree on the left onto a tile, or double-click it.
4. Drag one tile onto another to swap them; “Swapping…” appears briefly and the connection is not interrupted.
5. Double-click a tile to enlarge it; double-click again to return to the split view.

Tile format can be set to Fill, Fit all, 16:9 or 4:3. Multi-tile layouts use the substream, and an enlarged tile uses the main stream; the threshold is set by Stream switch threshold in System Settings. When the layout changes, tiles that stay the same keep streaming without interruption.

Right-clicking a tile shows Enlarge, Open in separate window, Full screen, Reconnect live, Unmute / Mute, Save image, Watch instant recording and Camera settings. You can restore closed tiles with Restore closed tiles.

Custom views and camera tour

Save the layout you use most and cycle through pages automatically.

1. Arrange the cameras in the layout you want.
2. In the CUSTOM VIEWS section, click Save custom view and enter a name (e.g. Factory entrances).
3. If you like, check Include all cameras in the visible list.
4. Enter seconds in Tour interval (0: off); if set, pages change automatically at that interval.
5. Save. After making changes, refresh the view with Update selected view.

The view is saved on this computer for this user and server. To use the same view on another computer, save it again there. The Reopen last grid at next session option in System Settings restores the last layout at the next sign-in.

Camera controls and notification panel

The right panel shows actions for the selected camera and incoming alarms.

The right panel has two tabs:

- Camera control: PTZ direction buttons, ZOOM, Go to preset, Saved tours, Fisheye, Camera Settings and Time Lapse buttons, with a storage and disk status card below.
- Notifications: The list of incoming alarms. The saved frame of the selected alarm is shown large; Open camera switches to live video, and Seen dismisses the notification.

Alarm notifications show the event frame as a thumbnail, with the scenario area outlined in yellow and the target in a red box. The smart event notification window opens at the bottom of the screen; in intercom scenarios it also includes an Open door button.

PTZ, presets and patrol

PTZ functions depend on the camera's capabilities and the account's permissions.

1. Select the PTZ camera in live view and open the Camera control tab.
2. Press and hold the direction buttons to move the camera; it stops when you release them. Use the ZOOM buttons to zoom in and out.
3. Select a preset number and click Go to preset.
4. Select a tour under Saved tours and click Start.

For a new tour, click New tour in the tour editor, enter a Tour name, add presets in order with Add step and click Save changes. The tour is stored on the camera. Tours that contain coordinate steps can only be started and stopped.

The Control panel → Patrol Settings page manages ONVIF preset tours: click Get tours, enter a Tour name and Preset tokens (comma-separated), click Create tour, then Start.

The PTZ auto tracking scenario (AI Settings → Camera) keeps the object in the center of the image; when the object is lost, the camera returns to the Home position preset. Tracking stops when an operator uses PTZ.

Fisheye dewarping

Fisheye camera images are dewarped in the client.

1. Select the camera and click Fisheye on the Camera control tab.
2. Check Enable fisheye dewarping.
3. From the Mounting / starting direction list, select how the camera is mounted (ceiling, wall, desk).
4. For the view, select Original, 360° panorama, 2 × 180° panorama, Virtual PTZ or 4 views.
5. Save an angle you use often by entering a Favorite view name and clicking Add view to favorites; then click Save settings.

Dewarping is done in the client; the original recording is unchanged, and the same setting can also be used in playback. AI overlays and analytics run on the original camera image, so analytics layers may be hidden in dewarp mode.

Video wall

Spread camera layouts across up to four monitors.

1. In the operating system’s display settings, set the monitors to extended desktop.
2. Open Video Wall from the top menu. The number of connected monitors is shown at the top.
3. Select a monitor and set Display mode to Camera grid or AI Monitoring.
4. For a camera grid, select a Layout and pick cameras from the list; they are placed in the order you select them. Drag cells to swap them.

5. Click Save and open.

Auto-fill 4 screens distributes authorized cameras across the first four connected monitors. Open saved screens opens saved layouts, and Close all closes every wall window. Apply to all screens applies the selected layout to every camera grid screen.

A monitor in AI Monitoring mode shows a single camera, the selected scenario, live boxes and lines, and counters in full screen. This requires the AI menu permission and live, event and AI read permissions on the camera.

Map

Show camera locations on a floor plan or site layout image.

1. Open Control panel → Map Settings.
2. Enter a Map name and select the plan image.
3. Select a camera from the list and place it on the map; drag the marker to position it. Delete a misplaced marker with Remove marker.
4. On a camera with a heat map scenario, click Mark heat area and click the corners of the analytics area in order (top left, top right, bottom right, bottom left).
5. Save.

The Map button on the live monitoring screen opens the saved plan; clicking a camera marker selects that camera. Show heat map draws the camera’s heat grid over the plan.

Playback and search

Playing back server recordings

Playback → Local opens video recorded by the ProVife server.

1. Open Playback from the top menu and select the Local button.
2. Select the camera and pick a day from the calendar. Days with recordings are marked on the calendar.
3. Click the recording bar on the TIMELINE; playback starts from that moment.
4. Change the speed from the Playback speed menu; use the 30 seconds back and 30 seconds forward buttons to move through the recording.

To find motion in a specific area, click Search motion. In the Search motion in recording window, drag on the image to draw the area to search, or select Entire image. Up to 24 hours can be scanned; matching intervals appear in the list and on the timeline, and clicking one plays the recording from there.

> If no intervals appear on the timeline, check the camera's recording schedule, the drive's reserve status and the service's access to the recording folder. Live video alone does not create a recording you can go back to.

NVR and remote playback

Recordings on NVR or camera storage are searched and played back via ONVIF.

1. On the Playback screen, select the Device button.
2. Expand the NVR in the device tree and check up to four cameras among its channels.
3. Select the Start and End date and time (less than 31 days).
4. For Stream type, select Main stream or Substream.
5. Click Search and play. Times appear above the playback bar; drag and release the bar to start playback from that time.

The Remote Playback (Device archive) window uses the device's recording and replay services for a single camera. If there is no automatic match, select the recording channel with Match to this camera, then click Fetch device recording and play.

> Try a single channel and a short interval first. A substream recording is found only if the NVR actually records that stream. The NVR and the server must be in the same time zone.

Synchronized playback

Watch the same time range on multiple cameras together.

To watch several cameras at once on the same timeline, use the four-channel NVR playback under Playback → Device. Up to four selected channels open at the same start time and move together on a shared time bar.

1. Select the channels to watch (up to four) under the same NVR.
2. Set a short interval that covers the time before and after the event.
3. Open all four channels together with Search and play.
4. Drag the time bar to move all four channels to the moment you want; the speed menu applies to all four channels together.

In this version, server recordings (Local) do not support multi-camera playback on a shared timeline; each camera is played separately. To compare the same moment across cameras, note the time and go to it on each camera, or open the recording from the event time in AI Playback.

AI Playback

List and review analytics events, and open the related recording.

The AI Playback screen (AI event center) shows events generated on the ProVife server and on cameras. The tabs at the top are Event list, Administration log and AI Monitoring.

1. Open AI Playback from the top menu.

2. For the filter, select All events, Person / vehicle detection or System and other; narrow the source to All sources, ProVife analytics or External analytics engine.
3. Type text in the Search plate, person, camera or event box; select Pending acknowledgment to see only events that require acknowledgment.
4. Use Details on an event row to see the event frame and values.
5. Use Open related recording to play the recording at the time of the event; acknowledge the event if needed.

> For an event to be recorded, the related scenario must be enabled and saved at that time. Temporary analysis run with the Test button does not write events.

Keyword search

Find recorded events by person name, plate, analytic name, color and time words.

You can type in everyday language in the search bar at the top of the AI Playback screen. Search ignores Turkish special characters and tolerates minor typos.

Example search	What it finds
Maria Smith	This person in face recognition events, or the driver in this plate's record.
7ABC123	Passes where this plate was read.
yellow hard hat	Events where the hard hat check scenario required a yellow hard hat and did not find one.
red car yesterday	Red vehicle events recorded yesterday.

1. Type words in the search bar and select a period: Last 7 days, Last 30 days, Last 90 days or Last 1 year.
2. Matching scenes are listed with thumbnails; tags show how the search was understood.

3. Play the recording of that moment with Open recording; return to the list with Close search.

> Search covers recorded events only: situations that follow the rules do not generate events, so they are not found. If there are no results, extend the period or try different words.

Time Lapse

A daily fast-view archive is built by capturing one frame per hour from a camera.

1. Click Time Lapse on the Camera control tab, or open the Time Lapse screen from the top menu.
2. Select the camera and turn on Hourly recording on this camera.
3. Enter the Retention (days) value.
4. To view, select a day and click Show; return to the current day with Today.

Recording runs independently of the client while the server is running. The first frame is captured within the hour you turn it on, and subsequent frames each new hour. On the hourly chart, "● Recorded" and "— No image" markers show which hours have frames.

Export and snapshots

Save recording segments as mkv files and frames as images.

1. In Control panel → System Settings → FILE SETTINGS, choose the Exported videos and Image folder paths with Browse and click Save.
2. In Playback → Local, select the camera and the recording segment on the timeline.
3. Click Export recording. The file is written to the selected folder as mkv.
4. For a snapshot, right-click a live or recorded frame and select Save image.

Exporting requires the Export permission on the camera. The output is an unwatermarked mkv; no mask, password or integrity file is added. Before sharing the file with others, review any personal data it contains and the access permissions.

AI

Setting up a scenario: camera and analytic type

Scenarios are created on the AI Settings screen; analytics run on the server.

1. Open Control panel → AI Settings and select the camera from the top strip.
2. If analytics are off for the camera, click Enable analytics.
3. Click + New and select the scenario type from the categorized list that opens.
4. Enter a descriptive name in the Scenario name field and check Enable detection.

Category	Scenario types
Lines and areas	Line crossing, Zone intrusion, Wrong-way detection, Conveyor object counting, Occupancy / heat map
Person	People counting, Crowd gathering, Queue detection, Loitering, Running / fast movement, Fight analysis, Fall analysis, Posture detection
Recognition	Face detection, Face recognition, Approximate age range, License plate recognition
Vehicle	Speed measurement (radar), Vehicle color and type, Vehicle make / model / year
Object	Abandoned object, Missing object, Empty shelf detection
Workplace safety	Hard hat check, Workwear color, Mask check, Workstation check
Fire / Camera	Flame detection, Smoke detection; Camera tampering, PTZ auto tracking

Human, vehicle and animal classification is not a separate scenario; it is set with the Detection object option in Line crossing and Zone intrusion. Types marked “License required” are not included in your license.

Area, line and detection settings

Define where and under what conditions the scenario generates events.

1. Use Capture frame to get a current image from the camera. Frames can be captured for drawing even when analytics are off.
2. For types that need a line, use Draw line (1 → 2) to drag the line from point 1 to point 2. For types that need an area, use Draw area (drag) or select Entire image.
3. Delete an incorrect drawing with Clear line or Clear zone.
4. Select values in the Detection settings section. Hover over the i icon next to each setting to see its description.
5. Check the result with Test, then click Create scenario. If you changed an existing scenario, click Apply.

Setting	What it does
Direction	Which crossing direction counts as an event (A → B, B → A, Both directions).
Detection object	Human, Vehicle (all), Animal (all) or a specific object.
Confidence threshold %	A lower value detects more but increases false alarms.
Repeat interval (s)	Minimum time between two notifications for the same object.
Camera view	Front-facing or Overhead; determines the counting method.

Schedule and actions

Choose when the scenario runs and what happens on an event.

- Analytics hours: The weekly hours when the scenario runs (e.g. after hours).
- Notification hours: The hours when events are notified; limits notifications while analytics keep running.
- Severity: Warning or critical.

- Repeat alert interval (s): The interval between consecutive notifications from the same scenario.

Select one or more actions in the Alert method section:

- Smart event notification on the main screen
- Show the related camera in a pop-up window and Audible alert
- Send to WhatsApp group with image (optional message text, e.g. “An announcement has been made”)
- Trigger smart device: relay, siren or light; optional “revert after (s)” time
- Call Home Assistant service

> Schedules and alerts are saved to the server with the Create scenario / Apply button. If you see a version warning when saving, get the current record with Reload from server; with your confirmation, this discards unsaved changes in the form.

Analytics speed and diagnostics

The analytics frame rate sets the balance between server load and detection performance.

The camera’s analytics rate is shown in the top strip of the AI Settings screen. It can be set to By scenario, Upper limit or Automatic (stable). A scenario requests its own rate in Advanced settings → Scenario frames/s; this value cannot exceed the camera’s analytics rate.

- If the screen shows the warning “This scenario will analyze … frames per second”, click Set to recommended rate.
- The motion pre-filter does not rerun the object model when there is no motion in the area; the savings rate is shown on screen.
- Speed measurement requires at least 6 frames/s (10 recommended); fight detection requires about 3 frames/s.

On the Model and Diagnostics tab, the AI runtime status section shows image age, processed and skipped frames, processing latency and model status (Running,

Loading, Model error). If there is a problem, use Restart analytics process; for support, generate a report with Save analytics diagnostic report.

AI Monitoring and PDF report

Watch the selected camera's scenario live and get a report with images.

1. Open AI Monitoring from the top menu.
2. Select the camera and a scenario saved for that camera from the Select scenario list.
3. Watch the area, line and detection boxes on the live scenario view. Counting scenarios show the PERSISTENT CROSSING COUNTER and CURRENT OBSERVATION COUNT; speed scenarios show the number of VEHICLES OVER THE LIMIT.
4. Open recent events from the NOTIFICATIONS list on the right.

For a report, enter dates and times in the Start and End fields (YYYY-MM-DD HH:MM:SS), select a single scenario or All scenarios, and click Get PDF report with images. The report is saved as A4 in the Documents folder with a dated name and then opens; targets are marked on event frames.

Boxes come from the latest analyzed frame, so there may be a slight delay compared to live video. The approximate age result is not a verified age; speed measurement is indicative only and is not a calibrated, legally valid radar measurement.

AI event search

Filter face, person, vehicle and plate events.

AI event search uses the filters on the AI Playback screen. Unlike the keyword search bar, here you narrow the event list by category and source.

1. Open the AI Playback screen.
2. Select the Person / vehicle detection filter.
3. Type a plate (7ABC123), person name (Maria Smith), camera name or event type in the search box.

4. Select ProVife analytics or External analytics engine as the source.
5. Open a row to review the event frame, and go to the recording with Open related recording.

Events generated by the cameras themselves also appear in the list. In the Camera event mappings section (AI Settings), map the event topic coming from the camera to an analytics category so these events appear under the right filter.

Face gallery

Enroll people in the gallery for face recognition.

1. On the AI Settings screen, open the Person gallery tab.
2. Choose a clear face photo with Upload photo, or mark a face in live video with Select from camera.
3. Enter the first and last name below the face (e.g. Maria Smith).
4. Click Save to gallery.
5. Add a Face recognition scenario to the camera and set the Face similarity threshold % value.

The face template and the small face image are stored encrypted on the server. Delete person deletes both. The gallery is also used in Store Analytics to exclude staff from counts.

> Adding people to the gallery requires the Person gallery permission. Complete the privacy notice and consent processes required by personal data regulations within your organization. Similarity is not proof of identity.

Face attendance

A daily check-in and check-out list is created from face recognition events.

1. Enable the Face recognition scenario on the entrance and exit cameras and add staff to the face gallery.
2. Open Control panel → Face Attendance.

3. Select the entrance or exit camera from the camera list, enter the date (YYYY-MM-DD) in the day field and click Refresh.
4. The list shows that day's face recognition events with their time and the matched person's name; the total number of face events is shown at the top.
5. To find a person's first and last pass, search for their name in the list; for details, open the event in AI Playback.

Attendance is generated only from events written by the face recognition scenario; no detections are invented. If the list is empty for the selected day, check that the face recognition scenario is enabled on the camera and that the analytics process is writing matches.

Store Analytics

Adding a store

Store Analytics counts people crossing a line on entrance cameras.

Store Analytics is a separate menu, independent of AI scenarios. Its settings are kept only on this screen; editing scenarios does not affect counting.

1. Open Store Analytics from the top menu and click Add store.
2. Enter a Store name and the Daily reset time (HH:MM, e.g. 00:00).
3. In the Entrance and exit doors section, select the camera for the first door.
4. Draw the counting line and an optional counting area with Draw area and line.
5. Save. If analytics are off for the camera, click Enable analytics.

The screen shows In, Out, Inside, Shoppers, Left without buying and Conversion rate counters for each store. In live view, all of the store's cameras are shown with their counting area, line and A/B sides; on the live store map, people move as dots entering and leaving through the doors.

Entry and exit doors

For each door, set the camera, line, direction and camera view.

1. In the Edit store window, click Add entrance or Add exit.
2. Enter the door name and select its camera.
3. With Draw area and line, click to draw the line with 2–12 points; drag points to move them. Add at least 3 corners for the counting area; if left empty, the entire image is used.
4. Select the door type: Entrance and exit, Entrance only or Exit only.
5. Select the direction (e.g. A → B entrance) and set Camera view to Overhead or Front-facing.

At overhead doors, counting uses a motion-based method; at front-facing doors, it uses person detection. In front-facing view, the foot point is tracked while feet are visible, and the body center when the person is very close to the camera.

> Draw the line where people actually cross in the image. If people walk toward the camera and exit to the side, draw the line vertically. A door pointing to a removed camera shows the red warning “Camera removed, select again”.

Checkout, staff and repeat entries

Conversion rate and people to exclude from counts are set in the Options section.

For conversion rate, check “Conversion rate: people crossing the checkout line count as shoppers” in the Options section, select the Checkout camera, draw the line with Draw checkout line and set the direction (e.g. A → B purchase).

To exclude staff and customers who re-enter within a short time:

1. Add staff faces to AI Settings → Person gallery.
2. Check “Exclude staff” and select the staff to exclude.
3. Check “Exclude re-entries” and enter a Duration (minutes).
4. In the Face camera (facing the entrance) field, select the camera that sees the faces of people entering.

A face is excluded from the count only if an entry has recently crossed the line; a face seen at the door that does not enter does not change the count. The screen also shows separate Excluded staff and Excluded re-entries counts.

> Customer face templates are not written to disk and no images are taken; they are held only in memory for the selected duration. If the server restarts during this time, re-entries may be counted again.

Overview camera and heat map

A camera that sees the whole store shows the map live and keeps a heat map.

1. Click Add Store Overview above the store map.
2. From the Store overview camera list, select the camera that sees the whole store. Instead of a camera, you can also use a PNG/JPG plan with Upload plan image.
3. Check Keep heat map.
4. Click Place doors; drag the doors and checkout to their positions in the image and click Save layout.

The Heat map button on screen shows today's heat map over the live video; red areas are where people spend the most time. Data is aggregated hourly and kept for 400 days. If there is no data yet, "Heat map waiting for today's data" is shown.

Use Change overview to change the overview and Remove overview to remove it; counts and records are not deleted.

Reports

Get store counts as a PDF or Excel report.

1. Click Get report on the store row.
2. Select the range: Today, Yesterday, Last 7 days, This month, Last month, or Start–End dates (up to 92 days).
3. For a store with an overview camera, you can check Add heat map to report.
4. Click Save as PDF or Save as Excel.

Format	Contents
PDF	Summary boxes (in, out, peak inside, busiest hour and day, conversion rate, excluded staff / re-entries), charts by day or hour, daily, door and hourly tables, a day-of-week table for seven days or more, and an optional heat map page.
Excel	Summary, Daily, Hourly, Hourly average, Doors, Days of the week and optional Heat map sheets; numbers are written as numeric values.

Each day starts at the store's daily reset time. Images of people are not included in the report; only counts are. Every report is written to the Audit Log and can also be generated from the Surveillance client.

Daily WhatsApp and email report

The day’s report is sent automatically at the set time.

1. Connect the account and select the group on the WhatsApp notifications page; for email, fill in the Email settings page.
2. In the Daily report section of the Edit store window, check Send report automatically every day.
3. Enter the send time (default 22:00).
4. Select WhatsApp and/or Email. If email recipients are left empty, the recipients in the email settings are used.
5. Save, and test the setting with Send today’s report now in the Get report window.

The WhatsApp group receives the summary text and a chart image, and for stores with a heat map, the heat map image as a second message. Emails include the summary text with PDF, Excel and heat map image attachments.

For the report, it is enough to have the group selected in WhatsApp. If WhatsApp is not connected, the report is retried every 5 minutes for 12 hours; if the server is off at the send time, the report is sent when it starts up the same day. The result appears on the “Last daily report” line in the Get report window.

> Automatic sending is off by default.

Plates and under-vehicle

License plate recognition scenario and speed measurement

A pass point is created by adding a License plate recognition scenario to a camera.

1. In AI Settings, select the entrance or exit camera, then choose + New → Recognition → License plate recognition.
2. Get an image with Capture frame and limit the reading area to the lane.
3. Enter the Confidence threshold % value; 80 or higher is recommended to prevent misreads.
4. Select the Plate format and Plates to notify: All plates, Block list only, Not on allow list or Allow list only.
5. For parking duration, select the Entrance camera or Exit camera role and save the scenario.

For speed, check Also measure speed when reading plates. Use Draw line A and Draw line B to draw lines at two known points on the road, then enter the Distance between lines (m) and Speed limit (km/h). If the limit is 0, only the speed is recorded. A separate Speed measurement (radar) scenario is also available in the Vehicle category.

> For fast-moving vehicles, the camera must deliver at least 10 frames/s. Speed is indicative only and is not a calibrated, legally valid measurement.

License Plate Recognition screen

Monitor live plate passes, the driver, list status and barrier result.

Open License Plate Recognition from the top menu. The screen is also available in the Surveillance client and appears with camera event permission.

- In the center, the selected or latest pass: large image, plate, driver, list (Allow list, Block list, Registered, Unregistered), barrier result and parking duration.

- On the right, Recent passes: the last 60 passes, filtered with the Search plate or person box.
- At the top, Today's counts: total, allow list, block list, unregistered and barrier opened.
- Pass points: each plate recognition scenario on each camera is a separate pass point, with Watch live and Watch last pass buttons.
- Open barrier: opens manually; the action is written to the Audit Log.

> Opening the barrier manually requires camera control permission or Smart Home use permission.

Plate lists and logbook

Allow list, block list and registered plates are shared across all pass points.

1. On the License Plate Recognition screen, click Plate lists.
2. Select the Allow list, Block list or Registered plate tab.
3. Enter the plate (e.g. 7ABC123), the driver (e.g. Maria Smith) and an optional description.
4. Click Save lists.

The person name is shown in plate events, on the live plate label, in notifications, in analytics and under-vehicle PDF reports, and below the plate on the under-vehicle screen. The new name also appears on events recorded before it was added.

List	Effect
Allow list	If a barrier is configured, it opens when the plate is read.
Block list	Generates an event and notification according to the scenario settings; the barrier does not open.
Registered plate	Only the person name and description are matched; it does not affect the barrier.

Barrier setup

When an allow-listed plate is read, the pass point's barrier opens.

1. On the License Plate Recognition screen, select the pass point and click Barrier settings (the same setting can also be edited in the scenario in AI Settings).
2. Select the barrier type: Smart relay, Camera relay (ONVIF) or No barrier.
3. For a smart relay, select the relay and Data point from the list; for a camera relay, select the Relay output.
4. Enter the Open duration (s).
5. Choose the event recording option: All plates, Block list only, Not on allow list or Allow list only. Save.

The barrier opens for every allow-listed plate, regardless of the event recording option. For example, at an entrance set to "Not on allow list", the barrier also opens for staff, but staff passes are not recorded as events. The smart relay also works over the local network without internet.

> If the smart relay is not in the list, first add it on the Smart device connection page. If the relay is not connected, "Barrier could not be opened" appears on the pass and a system event is created. Configuring this requires AI edit permission on the camera.

Under-vehicle scanning settings

Under-vehicle scanning uses a plate camera and a camera facing the underside of the vehicle.

1. Open Control panel → Under-Vehicle Scanning and create a Scanning station.
2. Select the Under-vehicle camera and the Plate camera; configure Retention (days), Scan line (%) and Image motion (Down / forward, Up / backward).
3. In the TRIGGER section, select the Start method: When plate is read (delayed) or When plate is read + under-vehicle motion; enter the delay and vehicle wait times.
4. For ending, select Fixed duration or When the vehicle has passed (motion ends); enter the time limits.

5. Set Motion sensitivity, Plate confidence, Read count and Same plate repeat times, then click Save settings.

The screen describes what your settings will do in a plain sentence (e.g. “The scan takes 8 s”). The camera must be fixed, facing the vehicle’s underside and well lit; duration, sensitivity and direction are tuned by testing on site.

> Under-vehicle scanning requires a separate license. Without a license, new scans do not start and station settings cannot be changed; past scans can still be viewed.

Under-vehicle monitoring and reports

Each live scan is automatically compared with the previous scan of the same plate.

Open Under-Vehicle Monitor from the top menu. The status light turns green while scanning and shows SCAN STARTING; SCAN COMPLETE appears when it ends. Preparation and vehicle wait are shown in yellow, and errors in red with the reason.

- The live pass is at the top and the Previous pass (reference) below. Differences are marked with numbered red boxes on the live scan and yellow dashed outlines on the reference.
- Zoom both images together with the mouse wheel, dragging, double-clicking, Zoom and Fit; click a marker number to zoom to that spot.
- On the Under-Vehicle Scanning screen, select a pass, enter Correct plate, vehicle information, Operator: OK / needs check and a Review note, then click Save review; set the reference with Pin reference.

For a report, enter a date range and an optional plate filter, then click Get PDF report; up to 31 days and 100 passes are included. Recording viewing and export permissions are required on both cameras.

> Under-vehicle images are for operator review. No automatic weapon, explosive or contraband detection is performed.

Smart building

Smart device connection

Relays, sirens, switches and sensors connect to ProVife events over the local network.

1. Open Control panel → Smart Home → Smart device connection and check Smart device connection enabled.
2. In the 1 · DEVICES section, click Search network (local); the ID, IP address and version of discovered devices are listed.
3. Enter the Local key for each device. The ProVife technical team provides this information; the key is stored masked.
4. Add a device that is not found with Add device manually by entering the Device ID, IP and Local key. For wireless sub-devices connected to a gateway, fill in the Gateway and Node fields.
5. In the 3 · MONITORED SENSORS section, use Add sensor to enter the Data point and Trigger value; click Connect / retry.

The connection runs in a separate process; if it fails, recording and analytics are not affected. When Local network priority (work offline) is on, commands are sent even without internet. The 2 · CLOUD section is optional and is used only to retrieve local keys automatically.

Smart Home scenarios

Respond to events automatically with if–then scenarios.

1. On the Smart Home scenarios page, click New scenario, or choose a ready-made scenario with Add from template….
2. Enter a Scenario name and optionally select a Section. A scenario linked to a section listens only to that section’s cameras.
3. IF (trigger): Camera / AI event, Device status, Time, When alarm mode changes, or People counting zone full.

4. CONDITIONS (optional): Only in these alarm modes, Only within a time range, Repeat cooldown (s).
5. THEN (actions, in order): + Device command, + Notification, + Alarm mode, + Announcement. Up to 10 actions can be added. Save.

If a duration (s) is given for a device command, the command is reverted after that many seconds; 0 makes it permanent. For a notification action, you can select Open camera in pop-up window, Audible alert and Open door button in notification. If one action fails, the others still run; the result appears in the Recent runs list.

> The device status trigger fires the moment the value changes to the set value; a sensor that is already on at startup does not generate an alarm. To trigger with MQTT messages, enter “mqtt” in the event trigger.

Alarm and fire detection

Arm home or section alarms; manage detectors and fire scenarios.

The Alarm page shows door, window and motion sensors and sirens. The Home alarm section has Arm home, Arm away and Disarm buttons. The General alarm (entire site) and Section alarms can be armed separately.

1. On the Alarm page, use Add from template… to select the “Alarm if a door opens while armed” template.
2. Select the sensor that triggers it and the siren that sounds, then save.
3. Arm the alarm with Arm away. If the door opens, the scenario sounds the siren and sends a notification.

The Fire Detection page lists smoke, gas and carbon monoxide detectors. The “Fire alarm on smoke detection” template links the detector to a siren and a notification. The camera’s Fire and Smoke analytics can also be selected as event triggers.

> Only scenarios can set the “Alarm!” state. Alarm mode changes are written to the audit log. Camera fire analytics do not replace a certified fire detection system.

Intercom and access control

Open the camera when the doorbell rings; open the door with one tap.

1. On the Intercom page, use Add from template… to select the “Camera on doorbell + Open door button” template.
2. Select the doorbell device, the camera to show and the door relay, then save.
3. When the doorbell rings, the camera appears in a pop-up window; open the door with the Open door button in the notification.

The Access Control page lists locks, garden/garage gates and door release relays. Use the Unlock, Open door and Hold open buttons on each row; for scheduled locking, use the “Lock the door every night at 23:00” template.

- The door relay sends a short pulse to release the electric lock.
- The Home Assistant lock is unlocked and left to its own auto-lock.
- Garden or garage gates close on their own; ProVife does not close them.

Audio control and announcements

Make announcements over speakers and sound the siren.

1. Open the Audio Control page.
2. Select the speaker in the Make announcement section.
3. Type the announcement in the Text to speak field (leave it empty for the siren) and adjust the Volume.
4. Send. If siren is selected, the siren plays instead of the text.

Speakers are Home Assistant media players; text is spoken by the text-to-speech service in Home Assistant. Announcements can also be used in scenarios with the + Announcement action, for example the “evacuation announcement on fire” in the school template.

Frequently used announcements are added in the Preset announcements section of the Graphical monitoring page by entering an Announcement name (e.g. Evacuation)

and the Text to read. They play with one click by selecting Preset announcement in the device window.

Building management: home, business, school

Alarms, devices and cameras for every section of a building are managed from one central point.

1. On the Organization page, build the site > block > floor > unit / business / school section tree and assign cameras to sections.
2. In the Sections and plans list on the Home management, Business management or School management page, mark nodes with their type.
3. Upload the section's plan (PNG, JPG or the first page of a PDF) with Upload plan; place devices and cameras with Add to plan and drag them into position.
4. Place smart devices by selecting a Section in their rows on the Alarm, Fire Detection… pages.
5. Select a template and click Apply to all sections in this building; each section gets its own scenario with its own sensor, siren and camera.

Each section and common area has its own alarm mode; a neighboring unit's camera does not trigger another section. The section card shows alarm buttons, devices reporting alerts, cameras, scenarios and the plan.

Graphical monitoring

Monitor live device status and send commands on building, floor and section plans.

The Building Management → Graphical monitoring page has the organization tree on the left, the selected section's plan in the center, the scenario panel on the right and the command bar at the bottom. Tree and plan zones are colored by their worst state: Fire, Alarm, Active, Bypass, Disconnected, Normal. Zones flash during fire and alarm.

- Device window: Open temporarily (1–60 s) or Hold open and lock for doors; Sound (60 s) or silence for sirens; Preset announcement for speakers; Watch live for cameras.

- Bypass: for maintenance or faults, a device, camera or entire heading (General bypass) does not start scenarios. The bypass list records who and when; remove an entry with Resolve.
- Scenario panel: Arm home, Arm away, Disarm; Run the scenarios that cover the section.

Command	Result
Manual alarm	After confirmation, the alarm mode becomes “Alarm!”, sirens in the section sound for 5 minutes and a critical notification is sent.
Silence sirens	Sirens stop; the mode does not change.
Reset system	Sections in alarm return to their previous mode and sirens stop; bypasses are unchanged.

People counting zones

Track the number of people inside areas such as entrances, cafeterias or floors.

1. First create a People counting scenario (Line entry / exit or People seen in area) on the relevant cameras in AI Settings.
2. On the Building Management → People counting zones page, click Add zone.
3. Name the zone and enter the Capacity (0 = unlimited), Daily reset time and an optional Section.
4. Add the cameras’ counting scenarios from the Counting scenarios list. If a camera faces the other way, check Reverse direction.
5. Save.

On a line, A → B counts as entry and B → A as exit; inside = in − out. A zone made up only of occupancy scenarios shows the “Number of people currently seen”. Line crossing counts crossings, not unique people.

When the number inside reaches capacity, a single “People counting zone full” event and notification is generated; this event can be selected as a trigger in Smart Home scenarios.

Notifications and integration

WhatsApp connection and group

Alarms are sent with images to a selected WhatsApp group.

1. Open Control panel → WhatsApp notifications.
2. In the 1 · CONNECT WHATSAPP ACCOUNT section, click Connect WhatsApp; a QR code appears.
3. On the phone registered to the account that will send notifications, go to WhatsApp → Settings → Linked devices → Link a device and scan the code.
4. After the message “Phone paired; opening connection…”, the status changes to Connected.
5. In the 2 · NOTIFICATION GROUP section, click Get groups, select the group and check Send alarms to this group.
6. Enter the maximum number of messages per minute (1–30) and try it with Send test message.

If the code expires, click Get new QR code. In scenarios, Alert method → Send to WhatsApp group with image must be selected. The message includes the event frame (area in yellow, target in red), camera, event, rule and time. Alarms older than ten minutes are not sent.

> Use a separate number and your own team’s group; accounts that send automated messages may be restricted. Remove connection removes the server from linked devices; camera and alarm data are not deleted.

Email (SMTP)

Email settings are used to send store reports by email.

1. Open Control panel → Email settings and check Enable notification.
2. Enter the SMTP server and Port (usually 587); select STARTTLS, SSL or None for Secure connection.

3. Enter the Username and Password. If a password is saved, leaving the field empty keeps the saved value.
4. Enter the Sender address and the Recipients list (comma-separated).
5. Click Test Connection and check the result line.

In this version, email is used for Store Analytics daily reports and delivery tests. AI alarms are delivered via main screen notifications, WhatsApp, smart devices, Home Assistant and MQTT. SMS and push notifications are not supported.

Notification preferences and alarm sounds

Set how notifications appear on this computer.

The Notification preferences page (Control panel → Alarms and notifications) affects only that computer, and changes are saved immediately.

- Show action alert at bottom: shows the result of actions such as saving or deleting in a bubble at the bottom.
- Show notification with thumbnail when an alarm arrives: turns the alarm window on or off.
- Mute notification sounds: turns off sounds in this client.
- Recent action notifications: the list of action notifications in this session.

On the Control panel → Alarm Settings page, sound files are assigned to motion, input, video loss, infrared and analytics alarms and stored with Save alarm sounds. Sounds play in this client; other clients use their own sound files.

MQTT

Send ProVife events to an MQTT broker and turn monitored topics into alarms.

1. On the Control panel → Smart Home → MQTT page, check Enable MQTT connection.
2. Enter the Server and Port; for an encrypted connection, select TLS (encrypted).
3. Enter the Username, Password, Client ID and Topic prefix.

4. Events to send: All analytics events or Alarms only (warning and critical). For QoS, select 0 · at most once or 1 · at least once (acknowledged).
5. In the Monitored topics section, use Add topic to enter a topic (e.g. building/+/door), a Name (e.g. Back door), an optional Value and severity. Save and click Send test message.

Events are published as JSON to the <prefix>/events/<camera>/<event type> topic; images are not sent. “online” is published to the <prefix>/status topic while connected, and “offline” when the connection drops. A matching message on a monitored topic becomes a ProVife alarm and triggers Smart Home scenarios; each row generates at most one alarm every 5 seconds.

Home Assistant

Connect your own Home Assistant server with an access token.

1. In Home Assistant, create a long-lived access token from your user profile.
2. On the Control panel → Smart Home → Home Assistant page, enter the Server address and Access token in the 1 · SERVER CONNECTION section.
3. If Home Assistant runs over https, leave Verify TLS certificate (https) on; enter the Commands per minute limit.
4. Check Home Assistant integration enabled and click Connect / retry.
5. List entities with Get entities; in the 2 · MONITORED ENTITIES section, use Add entity to select the sensors that will generate alarms.

When a monitored entity reaches the specified state (e.g. sensor “on”, door “open”), a ProVife event is created and notified like any other alarm. In the 3 · TEST SERVICE section, you can test a service with Call.

To have a scenario call a Home Assistant service, check Call Home Assistant service in the scenario’s Alert section in AI Settings. The connection stays on the local network; no cloud account is required.

Remote access

Port forwarding

Forwarding the server's single HTTPS port on your router is all you need for remote access.

Sign-in, live video, playback, events and images all go through the server's single HTTPS port (default 7443). Camera ports do not need to be exposed to the internet.

1. Open Control panel → Remote access; note the Server port and Local address.
2. In the router interface, open the Port Forwarding (NAT / Virtual Server) section.
3. Add a rule with external port 7443, protocol TCP and target <server's local IP address>:7443.
4. Fix the server's local IP address with a DHCP reservation on the router; if the address changes, forwarding stops working.
5. If you do not have a static public IP address, set up DDNS on the router (e.g. example.ddns.net).

The This connection line on the page shows whether the current session was opened from the Local network or from Outside (remote). The port can be changed in Service Manager; if you change it, update the router rule too.

Remote address field

The Surveillance client switches between the local and remote address automatically.

1. On the ProVife Surveillance sign-in screen, enter the server's local address (e.g. 192.168.1.10:7443).
2. In the Remote address (optional) field, enter the external address and port (e.g. example.ddns.net:7443).
3. Check the fingerprint with Verify server and click SIGN IN.

The client first tries the local address for about 4 seconds; if it cannot connect, it switches to the remote address. The working path is kept for the duration of the connection, and if it drops, the other one is tried. Live video uses the same path. When connected via the remote address, "· remote" appears on the bottom line. The remote address is stored on this computer for each server address.

The server certificate fingerprint must be the same for both addresses. If the remote address leads to a different server, the connection is not established; this protects against an intercepting device.

Remote sign-in permissions

Restrict who can sign in from outside and with which client.

The Remote sign-in permissions section on the Remote access page has two options:

Option	Default	Effect
Allow sign-in from outside the local network	On	If turned off, sign-in is possible only from local network addresses.
Allow the administration client to connect from outside	Off	When off, only the Surveillance client can connect from outside; administration stays on the local network.

Private IPv4 ranges (10.x, 172.16–31.x, 192.168.x), the loopback address, link-local addresses and IPv6 local addresses are treated as the local network. Rejected sign-ins are written to the audit log; because the rejection happens after the password check, it gives no separate hint about a wrong password. The failed password limit (10 attempts per 5 minutes per address) also applies to connections from outside.

> If you are currently connected from outside, you may not be able to reconnect with this client after saving; change this setting from the local network.

Maintenance

Software updates

Upload the signed installation package to the server and update the server and clients from within the software.

1. Open Control panel → Software update in ProVife Administrator.
2. In the 1 · UPLOAD PACKAGE TO SERVER section, click Select and upload package…; select the ProVife-x.y.z-Setup file and the .pvsig signature file next to it. Upload the monitoring package the same way.
3. The package is verified first on this computer, then on the server; check for the “signature verified” message. An interrupted upload resumes where it left off when the same package is selected.
4. On the server computer, click Update this computer in the 2 · UPDATE section, or select Apply software update in Service Manager.
5. Approve the administrator prompt and accept the license agreement. The service stops, files are updated, and the service and client restart.

Recording pauses for 1–3 minutes during the update. Once the server is on the new version, a “ProVife x.y.z ready · Update” banner appears at the top on other computers; the package is downloaded from the server and installed the same way.

> Modified or older packages are not accepted. Uploading a package requires device management permission. Camera, user and recording data are not deleted during updates.

Configuration backup

Back up regularly to protect your settings and database.

This version does not include a one-click configuration backup and restore tool. Installation and update processes check existing data and create an automatic migration backup; Service Manager shows its location on the “Pre-migration backup” line.

To back up manually:

1. In Service Manager, note the path of the server data folder (Server data and recording folder).
2. Stop the server safely with Stop and wait for the “Stopped” status.
3. Copy the entire data folder to an external drive or network location.
4. Restart the server with Start and check that the cameras are online.

To copy video recordings, use the Video Archive Backup page; the two backups do not replace each other.

> Do not manually copy backup files over a running system; recording indexes created afterward may be lost. If you need to restore, contact support@provife.com. Because the license is tied to the hardware, data moved to another computer requires relicensing.

Data analysis and resource monitoring

Monitor server resources, network traffic and disk status.

The Control panel → System information (Data Analysis) page shows Bandwidth and Storage charts:

- Machine network (Mbps): total traffic to and from the server; VMS OUTBOUND is video streamed to clients.
- DISK READ and DISK WRITE: the current load on the recording drive.
- Used and free space; an estimate of how long the drive will last at the current recording rate.

CPU, GPU and memory usage are always visible in the main window. If you enter a value in the CPU warning (%) field in System Settings, you get a warning when the CPU exceeds that level (0 is off).

For AI load, watch processing latency and skipped frame counts on the AI Settings → Model and Diagnostics tab. If skipped frames keep increasing, lower the analytics rate or reduce the number of scenarios.

Time and NTP

Recording timestamps come from the server clock; keep clocks in sync.

1. Open Control panel → Time and NTP (Time Synchronization).
2. Select the time zone. Daylight saving time follows this time zone's rules; there is no separate daylight saving switch.
3. Enter the NTP servers; if no port is given, 123 is used.
4. Enter the Clock offset warning (seconds) value.
5. Click Test Connection, check the result and save.

ProVife does not change the operating system clock; it only measures the offset and warns if the threshold is exceeded. Correct the server computer's clock in the operating system's time synchronization settings. Set cameras and NVRs to the same NTP server as well.

Clock offset can cause problems such as NVR recordings not being found, shifted event times, rejected PTZ commands and trial period validation issues.

Common issues

Connection and video issues

First narrow the problem down to a single device and a short time range.

Problem	Solution
Server does not start	Check that the selected IP exists on the computer and that the port is free. Review the error text in Service Manager and the service log; do not select the client profile folder as the data folder.
Client cannot connect to the server	Check the address and port (7443), and allow the TCP port in the firewall. If the fingerprint does not match, the server may have been reinstalled; verify the value in Service Manager.
Cannot connect from outside	Check the TCP 7443 forwarding, DHCP reservation and DDNS address on the router. Make sure external sign-in is allowed on the Remote access page.
Substream not showing	Check that the substream is enabled on the device and check the ONVIF profile. The main stream opening does not mean a substream exists.
Video stutters or freezes	Compare the main stream and substream on a single camera; check for network loss, CPU and memory load, and the number of open cameras. Try Reconnect live.

Recording, analytics and notification issues

First check that the setting was saved and that permissions are correct.

Problem	Solution
Recording not found	Check that server recording and the schedule are enabled for the camera and that the drive is not below its reserve.

Problem	Solution
NVR recording not found	Verify in the device's own interface that there is a recording at the same time; select the correct channel and stream, and check the time zone.
No analytics results	Check that the scenario was saved (Test is temporary), that analytics are enabled and that the license shows no "License required" warning. Review the status in Model and Diagnostics.
Overhead camera counts no one	Set Camera view to Overhead; the object model must be Motion (overhead counting).
WhatsApp groups not loading	After connecting, click Get groups again. If the QR code has expired, use Get new QR code.
Daily report not sent	Read the "Last daily report" line in the Get report window; check the WhatsApp group and email settings, then try Send today's report now.
Barrier does not open	Check that the plate is on the allow list, and check the barrier type and the smart relay connection.

Support and contact

For problems not answered here, contact the support team.

For technical support, write to support@provife.com; for licensing and purchasing, write to sales@provife.com.

To help us resolve the issue quickly, include the following in your message:

- ProVife version (client and server version in the About ProVife window).
- Device type and model, and only the relevant channel count.
- The error text on screen and when the problem started.
- Steps that reproduce the problem.
- If needed, the Diagnostic report from Device Management or the Analytics diagnostic report from Model and Diagnostics.

Do not share passwords, access tokens or personal camera footage. For license requests, send the SERVER ID code from the License screen.