RTVCP Sparrow Self Hosted

User Manual

This manual explains how to install RTVCP Sparrow Self-Hosted, connect cameras, sign in to the local portal, and check that the system is operating. It is intended for the person setting up Sparrow and users reviewing camera activity.

Guide contents

Install and complete setup
Connect and verify cameras
Use Sparrow each day
Troubleshooting and support

Install and complete setup

Before you begin

Use the current system requirements published at rtvcp.com and the checks in the deployment tool to confirm compatibility. This guide covers the Windows installation workflow. Hardware suitability depends on the installed release and the number and quality of camera streams.

- Have Windows administrator access available for installation and service setup.
- Have your registration email address and any trial or license information ready.
- Connect the computer to the same reachable network as the cameras. Have the camera addresses, RTSP details, and camera login credentials available.
- Allow enough storage for Sparrow, its prerequisites, and model files. Keep the computer connected to power during setup.

Install Sparrow

1. Download the current RTVCP Sparrow installer from rtvcp.com.
2. Run rtvcp-setup.msi and follow the installation prompts. If Windows asks for administrator approval, approve it after verifying that the file came from RTVCP.
3. If the browser flags an uncommon download, check the source and filename before choosing to keep the installer. If Windows blocks execution and you cannot verify the publisher or source, contact support.
4. Continue into RTVCP Sparrow Deploy after installation. If it does not open, launch the installed deployment tool from the available application shortcut. On the welcome screen, select Next to continue.

Complete deployment

Figure 1. The RTVCP Sparrow Deploy welcome screen.

5. Review the system checks. Resolve failed checks before proceeding, then allow required components and model files to finish installing or downloading.

Depending on the release and existing software, setup may install runtime components, database components, and background services. Follow any restart request, then return to setup to finish the remaining steps.

Registration and licensing

Complete the registration or licensing steps offered by the deployment tool. When purchasing for the installed machine, use the purchase link generated by that tool so the request is associated with the correct computer. A trial is available for 7 days under the trial terms.

If the portal reports that a trial or license has expired, follow the purchase instructions it provides. Contact support before moving an existing installation or replacing hardware if you need help with its machine license.

Open the portal

After setup completes and the services are running, open http://localhost:18473/ on the installed computer. Sign in with the email address used for registration and the initial password password, unless it has already been changed.

Connect and verify cameras

Prepare camera access

Sparrow needs a reachable camera stream and valid credentials. The camera login is separate from your Sparrow portal login. Consult the camera manufacturer or your installer for the correct RTSP stream address and permission settings.

Discover and configure cameras

1. Use the deployment tool to scan the camera network. To review or change the scan range, open Tools > Scan Settings. Enter your camera network in Scan IP Block using CIDR notation, then select Scan. For example, 192.168.0.0/24 covers addresses in the 192.168.0.x network; use the range appropriate to your installation.

Figure 2. Scan Settings lets you specify the camera network before scanning.

2. Wait while Scanning for video streams is displayed. The IP Address line identifies the address currently being checked. Next may remain unavailable while the scan is running.

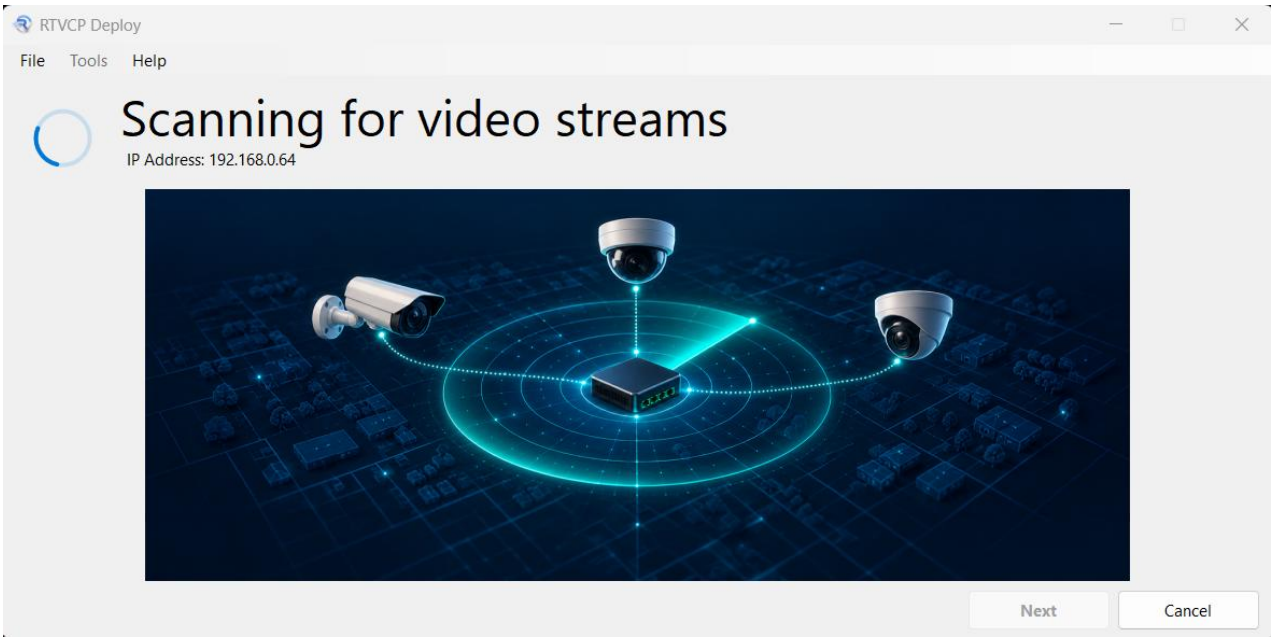
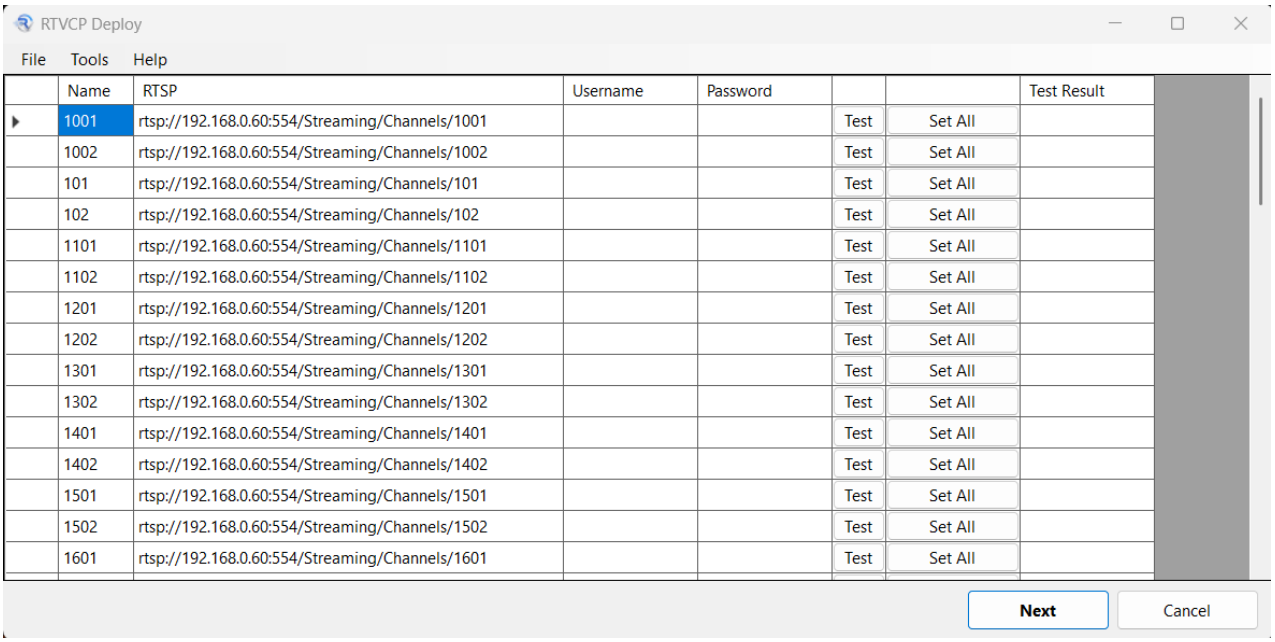


Figure 3. The deployment tool scans network addresses for video streams.

3. Review the discovered streams in the grid. Confirm the Name and RTSP address, then enter the camera Username and Password. A device may expose several channels or stream variants, so multiple rows can refer to the same IP address. The IP address is included in the RTSP URL.



Name	RTSP	Username	Password			Test Result
1001	rtsp://192.168.0.60:554/Streaming/Channels/1001			Test	Set All	
1002	rtsp://192.168.0.60:554/Streaming/Channels/1002			Test	Set All	
101	rtsp://192.168.0.60:554/Streaming/Channels/101			Test	Set All	
102	rtsp://192.168.0.60:554/Streaming/Channels/102			Test	Set All	
1101	rtsp://192.168.0.60:554/Streaming/Channels/1101			Test	Set All	
1102	rtsp://192.168.0.60:554/Streaming/Channels/1102			Test	Set All	
1201	rtsp://192.168.0.60:554/Streaming/Channels/1201			Test	Set All	
1202	rtsp://192.168.0.60:554/Streaming/Channels/1202			Test	Set All	
1301	rtsp://192.168.0.60:554/Streaming/Channels/1301			Test	Set All	
1302	rtsp://192.168.0.60:554/Streaming/Channels/1302			Test	Set All	
1401	rtsp://192.168.0.60:554/Streaming/Channels/1401			Test	Set All	
1402	rtsp://192.168.0.60:554/Streaming/Channels/1402			Test	Set All	
1501	rtsp://192.168.0.60:554/Streaming/Channels/1501			Test	Set All	
1502	rtsp://192.168.0.60:554/Streaming/Channels/1502			Test	Set All	
1601	rtsp://192.168.0.60:554/Streaming/Channels/1601			Test	Set All	

Figure 4. Discovered streams with camera credentials and per-stream controls.

4. Select Test on a row and review Test Result. Use Set All only when the same credentials should apply across the camera list, then review every row. The Tools menu also offers Test All to check the listed streams and Remove Fail Streams to remove failed entries. Correct credentials and connectivity before removing entries you still need.

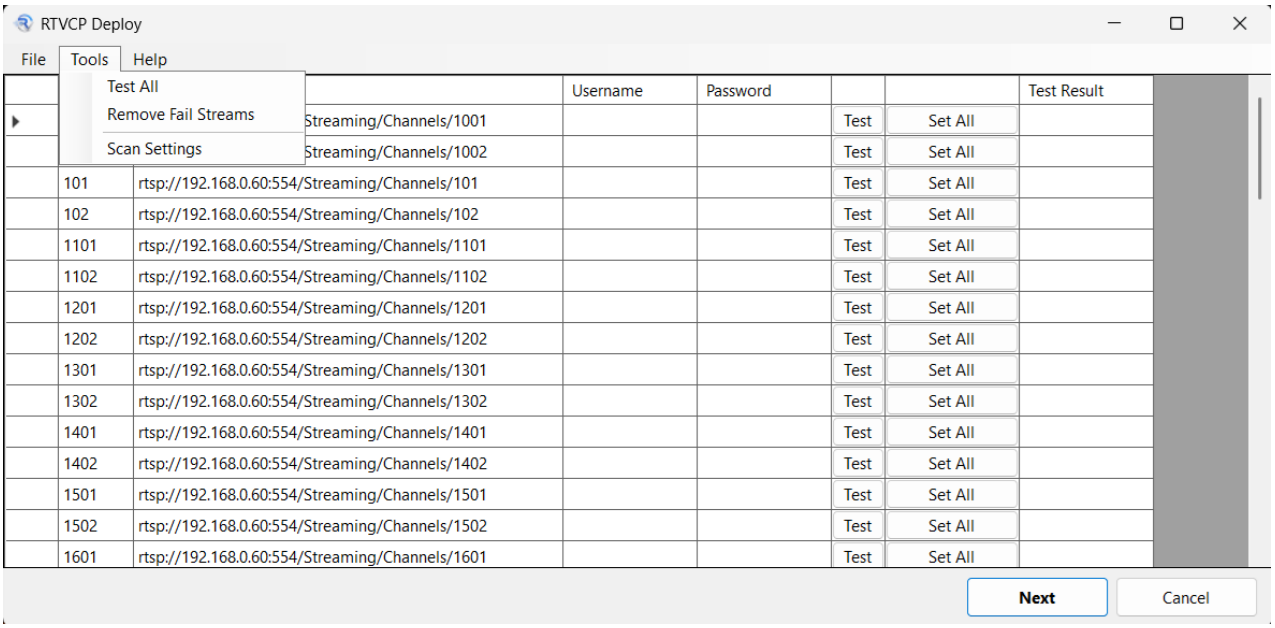


Figure 5. Tools provides batch testing, failed-stream removal, and scan settings.

5. After reviewing and testing the intended streams, select Next and finish the remaining deployment steps. Open the portal and check each configured camera before relying on monitoring.

Choose a useful stream

A camera may offer a main stream and a lower resolution substream. Choose a stream that shows the activity you need to understand while remaining within the computer's capacity. If processing is slow, reduce the workload gradually and verify that important details are still visible.

A successful stream test confirms access at the time of testing. Also check that the displayed view is current, correctly aimed, and usable in normal daytime and nighttime lighting.

Validate the completed setup

- Confirm that each camera has a clear, recognizable name and the expected view.
- Walk through a monitored area and verify that Sparrow reports the activity after allowing time for processing.
- Check for stale views, repeated connection failures, or summaries that do not match visible activity.
- If you enable email alerts in your installed release and plan, confirm the recipient and verify delivery with a controlled test. Check the spam folder if needed.

When a camera will not connect

Recheck its IP address, RTSP path, port, username, and password. Confirm that RTSP access is enabled on the camera and that the network permits the connection. A camera working in its manufacturer's app does not by itself confirm that its RTSP stream is accessible to Sparrow.

Use Sparrow each day

Sign in to the monitoring console

Open http://localhost:18473/ on the computer running Sparrow. If the portal shows a Login button, select it to reach the sign-in screen. The computer must be awake and connected to the camera network.

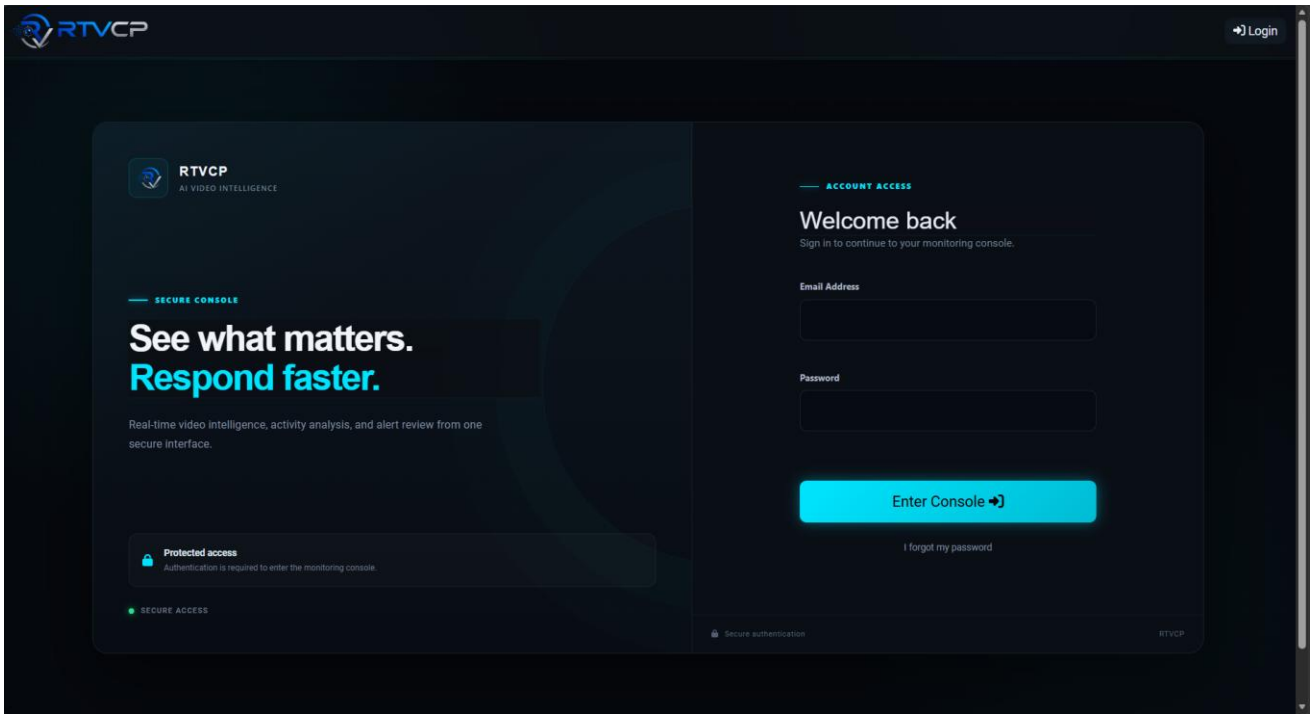


Figure 6. Sign in with your registered email address and current password.

1. Enter the email address used during registration in Email Address.

2. Enter your current Password. For the first login, the initial password is password, all lowercase and without quotation marks.

3. Select Enter Console. After signing in, review Video Log and confirm that recent activity is available for the expected cameras.

If you have forgotten a changed password, select I forgot my password and follow the instructions shown. Contact support if you cannot recover access. Replace the initial password through the available account controls; the account menu is at the upper right after sign-in.

Read and search the Video Log

Video Log lists camera activity and its AI-generated descriptions. Use the table view when you need to compare event details, alert status, and times. The screenshots show example records; their dates and camera names are not installation defaults.

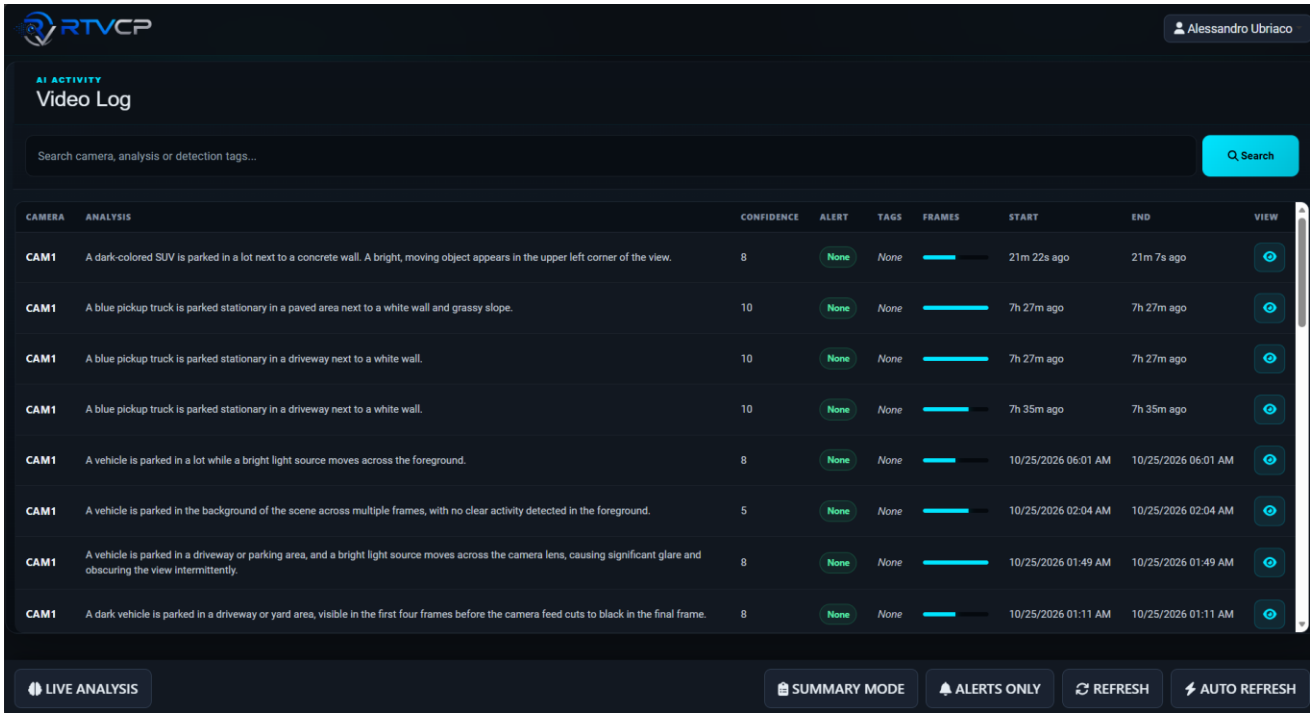


Figure 7. Video Log in table view with search and review controls.

Camera identifies the configured camera. Analysis contains the generated description. Always check the associated camera evidence before acting on a description.

Confidence is the score reported for the analysis. A higher displayed value is not a guarantee that the description is correct and should not be treated as a calibrated probability.

Alert indicates whether an entry is flagged. Tags provides detection labels when available; None means no labels are displayed for that record. An alert or tag alone does not establish that a threat occurred.

Frames shows a visual indicator associated with the entry. Start and End identify the activity interval. Recent entries can show relative times, while older entries can show dates and times. Check these fields before treating an item as current.

To find an entry, type a camera name, analysis term, or detection tag in the search field and select Search. Clear the field and search again to return to the unfiltered search results.

Use the eye icon in View to open an entry for closer review. Select Refresh to reload the results, or use Auto Refresh for automatic updates. Live Analysis provides access to the live analysis view. Available controls may vary by installed release.

Use Summary Mode

Select Summary Mode to switch to a simpler list of camera names, times, and descriptions. This view helps you scan activity quickly. Select it again to return to the table and its detailed fields. The highlighted button in the example indicates that Summary Mode is active.

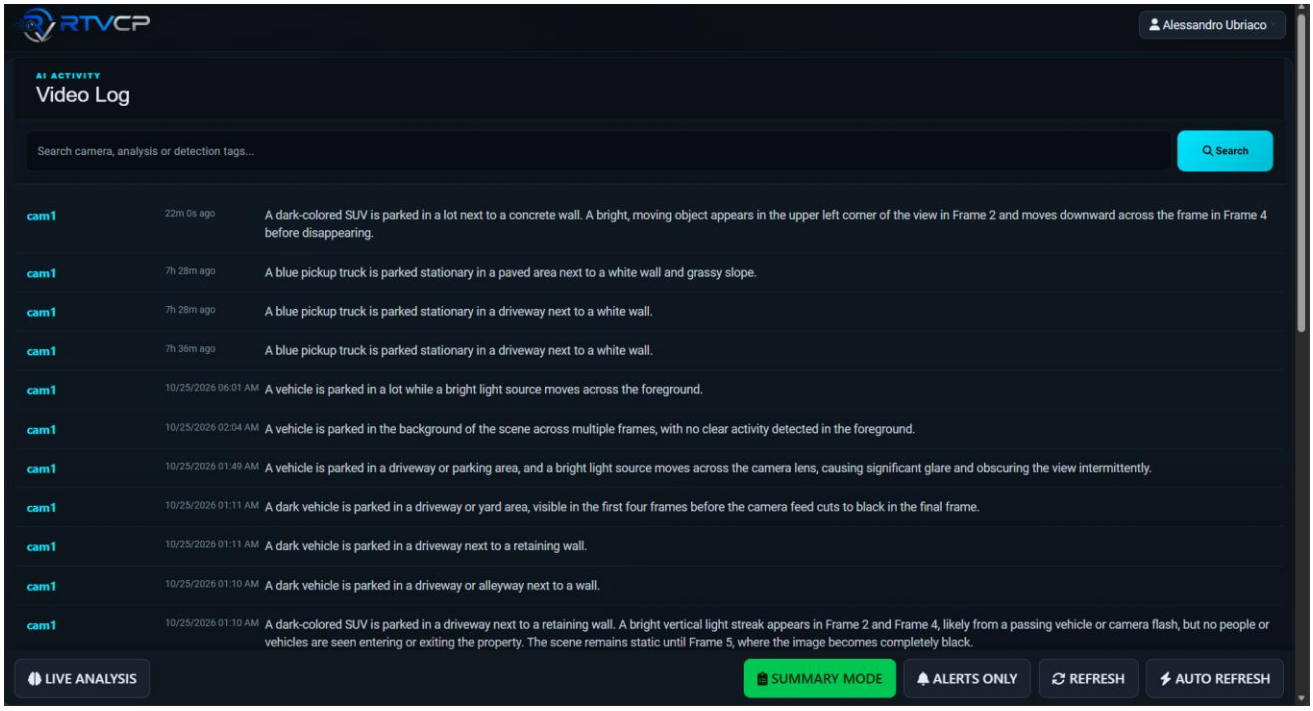


Figure 8. Summary Mode presents activity in a compact reading view.

Plan for interruptions

Stopping services, restarting Windows, disconnecting cameras, or shutting down the computer interrupts processing. Notify anyone relying on the system before planned maintenance and verify camera operation when it is complete.

Filter and review alerts

Select Alerts Only to restrict the list to flagged records. Select it again to restore the broader list. If no records appear, review the search text as well as the alert filter before concluding that camera activity is missing.

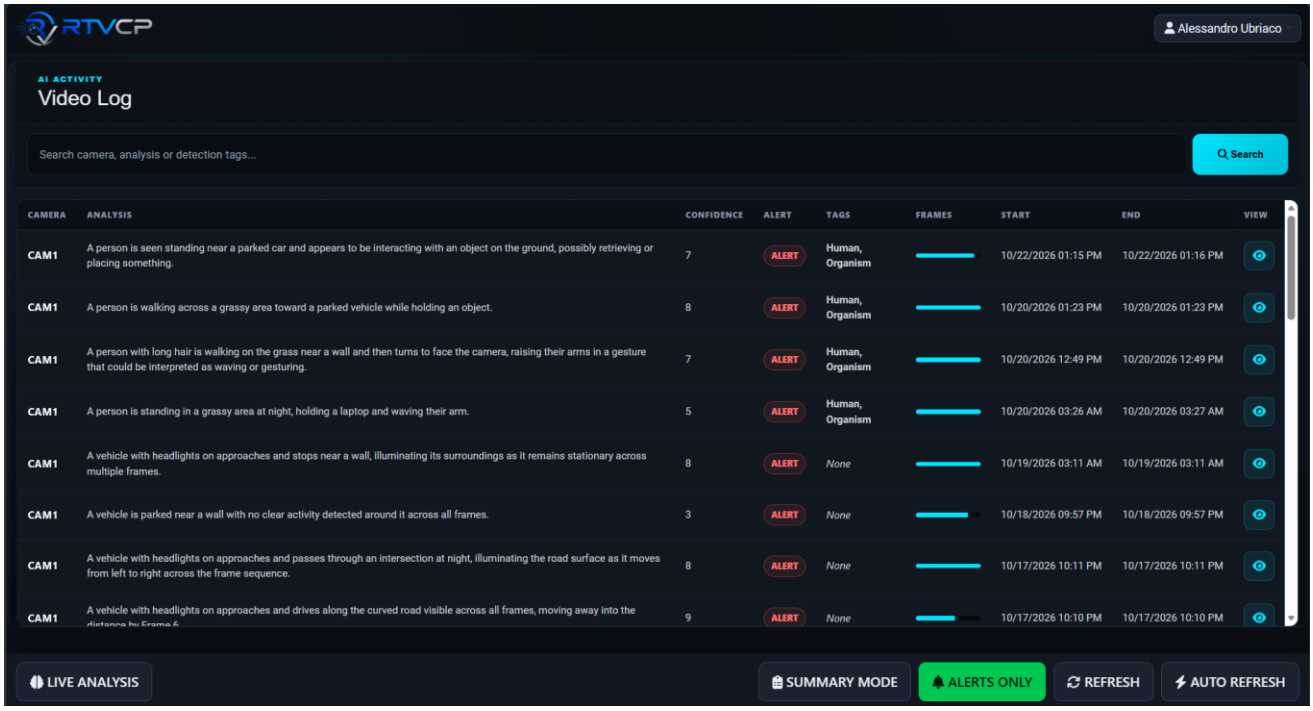


Figure 9. Alerts Only is active and the table shows flagged records.

For a flagged record, check Camera, Start, End, and Analysis, then use View to inspect the entry. Confirm significant events using the available camera evidence and your established response procedures. AI analysis can miss activity or describe it incorrectly, particularly with rain, glare, poor lighting, obstructions, or distant subjects.

Keep monitoring available

Closing the browser ends your viewing session; it does not serve as a stop command for the background services. Monitoring depends on the Sparrow services running and the computer remaining powered on, awake, and connected. Configure Windows power settings appropriately for the intended operating hours.

After a restart, update, power interruption, or camera change, reopen the portal and confirm that current activity is being processed. Do not assume that a successful login means every camera is connected.

Protect access and maintain the installation

- Replace the initial password and keep camera credentials private. Sign out after using a shared computer.
- Keep the local portal restricted to trusted access. Ask your administrator to configure secure remote access if you need to connect from outside the installation computer.
- Follow the update instructions for your installed release. Schedule maintenance when an interruption is acceptable, then verify operation afterward.
- Before reinstalling or making major changes, ask support for the supported backup and restore procedure. Do not delete database or configuration folders as a troubleshooting step.

Troubleshooting and support

The portal does not open

On the installed computer, enter the full address http://localhost:18473/ using HTTP. Confirm that setup has completed and allow time for startup. If you are using another device, localhost will refer to that device; ask your administrator for the correct network address and permitted access method.

If the portal still does not respond, open Windows Services and check RTVCP-Overlord. Also check RTVCP-Update when investigating update problems. Use an administrator account when required. Do not change service accounts or installation permissions without guidance.

Sign in fails

Use the exact email address entered during registration. The initial password is password, all lowercase, without quotation marks. Remove accidental spaces and check Caps Lock. If the password was changed, use the replacement password. Select I forgot my password on the sign-in screen and follow the displayed instructions if needed. Contact support if you cannot regain access; do not reinstall to reset a login.

Camera information is missing or outdated

Check camera power, network connectivity, and the configured RTSP credentials. Retest the stream in the deployment tool. If several cameras fail at once, check the network and the Sparrow computer first. After restoring a connection, allow processing time and confirm that the activity time advances.

Processing is slow or descriptions are inaccurate

Confirm that setup completed all required model downloads and that no hardware checks remain unresolved. Review CPU, memory, and GPU usage in Windows Task Manager. Reduce the number or workload of streams and test again. For inaccurate descriptions, check camera position, focus, lighting, obstructions, and stream quality.

Restart background services

Restarting services interrupts processing. In Windows Services, locate RTVCP-Overlord and choose Restart if it is running, or Start if it is stopped. Check RTVCP-Update separately if updates are failing. Afterward, reopen the portal and verify current camera activity. If a service immediately stops again, collect the error and contact support.

Contact RTVCP

Website: https://rtvcp.com
Email: info@rtvcp.com

Include the installed Sparrow version, Windows version, CPU and GPU models, memory, number of cameras, the exact error message, and the steps that produced the problem. State whether the portal opens locally and whether camera tests succeed. Remove passwords, license secrets, and sensitive camera content from screenshots or logs before sharing them.