



Agent DVR

User guide

2026-08-26 · ispyconnect.com/docs/agent

Contents

Agent DVR

- Welcome
- Troubleshooting
- Organizing Servers
- Connecting Remotely
- Connecting Locally
- Plugins
- Nest and Dropcam Cameras
- FAQ
- Windows Tray Application

User Interface

- Live Viewing Devices
- Layouts
- Time Line
- Recordings
- Playback
- Photos
- Floor Plans
- Virtual Reality

Configuration

- Adding Cameras
- Adding Microphones
- Editing Cameras
- Editing Microphones
- Motion Detection
- Video Sources
- Audio Sources
- Server Settings
- Actions
- Investigations
- Alerts
- Using MQTT
- Using Profiles
- Notifications
- Network Drives
- Permissions
- RTMP Streaming

- Setting up SSL
- Storage Management
- Themes
- Shortcut Keys
- Customizing Controls
- FFmpeg Install

Integrations

- API
- Integrations

AI

- Servers
- Configuration

Account Management

- Account Management
- 2 Factor Authentication
- Subscriptions
- Payment History
- Account Permissions

Agent DVR

Welcome

About Agent DVR

Agent DVR is video surveillance software that turns your computer into a full NVR: watch live security cameras, record footage and get motion detection alerts, all from a web browser.

Welcome to Agent DVR, the world's most advanced DVR! It runs smoothly as a service, consumes less CPU than iSpy, and offers a user-friendly web interface accessible from anywhere without any port forwarding hassles!

Friendly Reminder: It's best to use either iSpy **or** Agent DVR for optimal performance. Running both might lead to some hiccups with device drivers and network access.

Getting the Most Out of Agent DVR

Agent DVR boasts a sleek, browser-based interface, unlike iSpy's windows forms UI. Access it via the local portal, web portal, or our handy mobile apps.

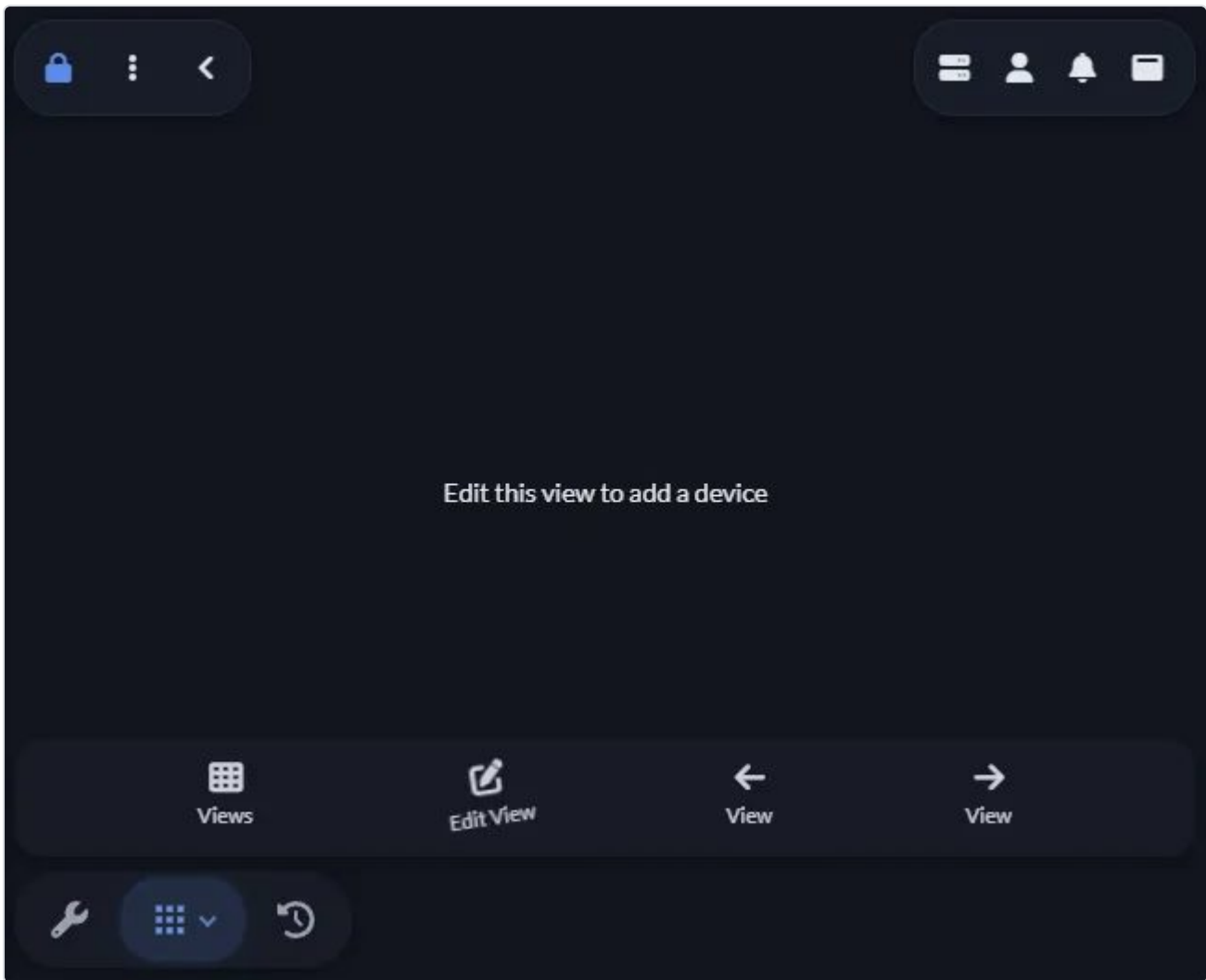
Agent DVR's own webserver is your gateway to convenience, usually found at <http://localhost:8090>[↗].

Remember, you can also access Agent DVR over your local network using private IP addresses or computer names (like <http://192.168.1.10:8090> or <http://nvr:8090>).

You might need to tweak your firewall settings for local network access - see the [Ports](#) list.

First Steps

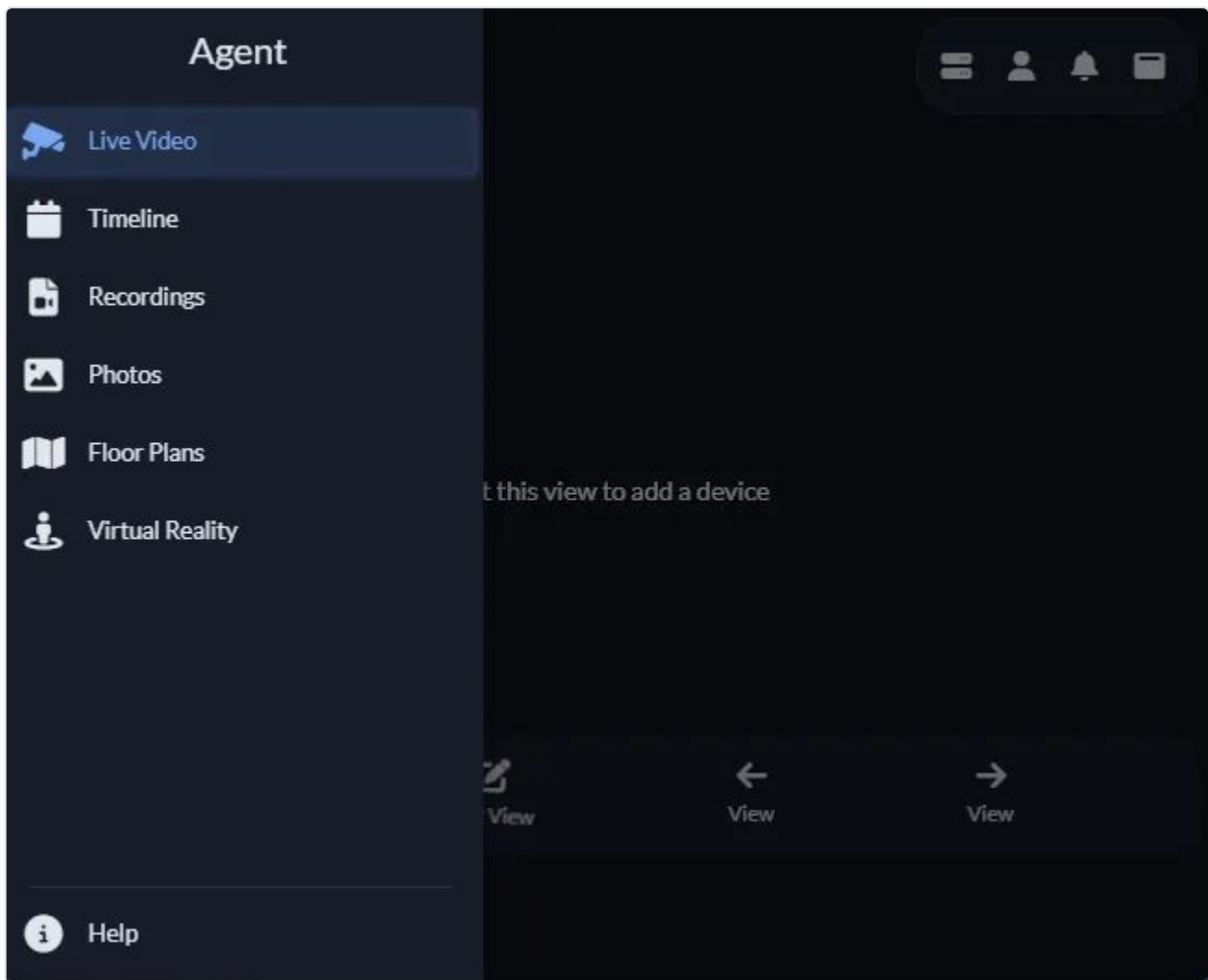
When you first open Agent DVR's main UI (usually at <http://localhost:8090>), you'll see something like this:



At the top left is the main Alerts icon. In this image, the system is currently **Armed** (green padlock icon), which means alerts are active. Click this icon to turn off this main alerts master switch (or apply a profile).

The menu with 3 dots on it to the right of the padlock is the main menu icon - this lets you access recordings, photos, VR and other views.

The arrow to the right of the main menu toggles the overlay of the UI - click this to show or hide the overlay controls.



Use this to navigate Agent DVR's various content views or to make the app go fullscreen.

At the top right is the **Server menu** (click this to configure your server settings), **Account menu** (for customization and profile settings), and the **Alerts view**, which provides a list of recent alerts.

At the bottom, you'll see a spanner icon - this is the **Controls menu**. At the moment, there are no devices added to the UI. To add a camera, click the *Edit View* button. This opens the view editor. Agent DVR has customizable views that let you arrange devices in what we call *slots*. The default slot is an automatic grid layout - just click the grid to select it, then click *New Device* at the bottom.

Once you've added your camera, it will connect and start playing video in the main UI:



You'll notice a new menu appears at the bottom left. With the camera selected in the UI, you can use this menu to control the camera: turn it on or off, edit it, start recording, and more.

Explore this user guide to discover all the amazing features Agent DVR has to offer!

Performance Tips

Ready to max out your PC's performance with Agent DVR? Here are some savvy tips to keep things running smoothly:

Disable HDR: If HDR's causing issues, turn it off in Windows Settings > System > Display.

Monitor CPU: Set a Max CPU value in Server Settings to avoid overloads.

Use Framerate Limits: Control max framerates for both live viewing and recording.

Use Raw Recording: Opt for a low-res URL for live viewing and a high-res URL for recording to save CPU (most effective!).

Use ONVIF Motion Detection: Let your ONVIF camera handle the motion detection.

Use the Scheduler: Turn off features like motion detection when they're not needed.

Set the Max Stream Size: Reduce resolution in Server Settings to ease CPU use.

Set Video FPS: Lower the framerate in Playback Settings to reduce CPU load.

Use the GPU: Decode video using your GPU for better performance.

Skip Decode: Choose 'None' for Decoder if live playback isn't essential.

Turn off Audio: Disable audio if it's not needed to save resources.

Use High Performance Resizing: A great option in Server Settings to save CPU, with a slight quality trade-off.

Utilise other Computers: Run heavy processes like AI servers on a different computer to keep things light.

Use the web UI on another computer: Access the web UI from a different computer to distribute the processing load.

Follow these steps, and you'll have Agent DVR running at top efficiency in no time!

Supported Languages

Agent DVR has been translated into the following languages: English, Arabic, Bengali, Czech, Danish, Dutch, Farsi, Finnish, French, German, Hindi, Hungarian, Indonesian, Italian, Japanese, Korean, Mandarin (Simplified Chinese), Norwegian, Polish, Portuguese, Russian, Spanish, Swedish, Taiwanese Mandarin (Traditional Chinese), Turkish, Ukrainian, Vietnamese.

To switch languages, simply click on Account  - Language and choose your preferred language.

Helping with Translations

Have you spotted an issue in our translations? You can make a difference! To contribute, please modify and make a pull request on our translations [GitHub Project](#) ↗.

Thanks for your help!

Installing

Ready to dive in? [Download Agent DVR](#) and launch the installer. Agent DVR operates as a service or a console application on a variety of platforms including Windows 10+, Linux X64 (Ubuntu), macOS (M1 included), and ARM-based systems like the Raspberry Pi.

Need guidance? Just follow the setup instructions tailored for your operating system on our [download page](#). We've got you covered!

Once Agent DVR is up and running, access it via most web browsers at `http://localhost:8090`

If port 8090 wasn't available when Agent was installed it will have started on a different port number - check the file `Agent/Media/XML/current_port.txt` for the port it's currently running on.

Installing Manually

Can't use the online installer? You can set up Agent DVR on Windows offline. Just make sure your computer has active network hardware to start the server. Follow these easy steps to get going:

First, grab the latest download link by calling our API here: [Download Location \(Windows\)](#)[↗]. Simply copy the link from the response and paste it into your browser's URL bar to begin the download.

Next, download the zip file from the link provided in the API response.

Then, unzip this file into a folder on your target computer.

Run (double-click) 'agent-install-service.bat' to start the installation process.

Optionally, double-click 'AgentTray.exe' to start the tray app. For convenience, you can [add it to your startup folder](#)[↗].

To ensure smooth LAN access, [add an exception in your Windows firewall](#)[↗] for the Agent.exe application.

Finally, open a web browser and navigate to <http://localhost:8090> to launch Agent DVR.

Installing Older Versions

Downgrading Agent DVR isn't guaranteed to work smoothly - make sure you back everything up first!

Linux and Mac

To install older versions on Linux and Mac run the install script with a provided version number. For example, in terminal to install v5.8.0.0:

```
curl -sL "https://www.ispyconnect.com/install" | bash -s -- -v 5800
```

Windows

To install an older version on Windows you can grab the download by modifying the version number in the following location:

```
https://files.ispyconnect.com/downloads/Agent_Windows64_5_8_0_0.zip
```

Click the Start menu, type "services" and press enter. Find Agent in the list, right click it and click "Stop".

Unzip the download over the top of the existing install (usually C:\Program Files\Agent)

In services, right click Agent again and click "Start"

Please note that we sometimes purge older versions for security reasons so you may want to keep a copy of the installer locally for future use

Windows 7

To install on Windows 7 you can use the following files. You will need to unzip the application to a folder (Agent) and then manually install the ffmpeg files.

For 64 bit:

```
https://files.ispyconnect.com/downloads/Agent_Windows64_5_8_0_0.zip  
https://files.ispyconnect.com/downloads/ffmpeg6-win64.zip
```

You will need to unzip the application to a folder and then unzip the ffmpeg files to Agent\dlls\x64

For 32 bit:

```
https://files.ispyconnect.com/downloads/Agent_Windows_5_8_0_0.zip  
https://files.ispyconnect.com/downloads/ffmpeg6-win32.zip
```

You will need to unzip the application to a folder and then unzip the ffmpeg files to Agent\dlls\x86

When you have done that, run agent-install-service.bat, which should start the service on Windows. You can then open <http://localhost:8090/> in a web browser.

Importing Existing Content

Importing existing video, audio and image data into Agent DVR is easy. Just follow these steps (v7.1.5.0+):

Click on server menu - Import Content (under Devices)

Enter the local path to the content (local to the computer running Agent DVR). For example: C:\MyFiles

Select the camera or microphone device you want to attach the content to

Click OK

Agent DVR will scan the folder and import any compatible files it finds. Supported file types include: mp4, mp3, mkv and jpg. The importer will run in the background and copy the content to Agent's media storage locations. Imported content will be tagged with "Imported" and locked against file deletion by default. To unlock the files you'll need to select them in the UI and click unlock.

LAN (network) access

Agent DVR uses a few ports for network access. The ports you will need available are:

8090 (TCP/UDP) for the User Interface (may be different if you changed it)

3478 (TCP/UDP) for the STUN/TURN server (webrtc)

50000-50100 (TCP/UDP) for relay session connections. Optional in most setups - relay traffic normally travels through port 3478.

Uninstalling

If you installed Agent DVR using the installer, you'll find it in the add/remove programs list on Windows. You can uninstall it there, but if it's not listed there, no problem!

If Agent DVR is running as a service, you'll need to stop it to continue uninstalling:

For Windows: Just double-click **agent-uninstall-service.bat** in the Agent DVR directory (usually C:\Program Files\Agent). Don't forget to right-click and quit the AgentTray application in the taskbar.

For Linux: Open a terminal and run these commands:

```
sudo systemctl stop AgentDVR.service
sudo systemctl disable AgentDVR.service
```

. This will stop and disable the Agent DVR service.

For macOS: Open a terminal and run these commands:

```
launchctl bootout gui/$(id -u) ~/Library/LaunchAgents/com.ispy.agent.dvr.plist
rm -f ~/Library/LaunchAgents/com.ispy.agent.dvr.plist
```

On older installs Agent DVR was set up as a system service instead - if the file above doesn't exist, run:

```
sudo launchctl bootout system /Library/LaunchDaemons/com.ispy.agent.dvr.plist
sudo rm -f /Library/LaunchDaemons/com.ispy.agent.dvr.plist
```

This will stop and remove the Agent DVR service.

To completely remove the Agent DVR files, just delete the Agent DVR directory. On Windows, it's usually located at C:\Program Files\Agent. On macOS (installer-based installs), it's at ~/Library/Application Support/AgentDVR - also delete the launcher app at ~/Applications/Agent DVR.app. On Linux (and older script-based macOS installs), it's wherever you ran the install script.

Delete Account

To delete your account, including all data sent to us via the iOS Agent DVR application or the Android "Agent DVR Client" application, follow these steps:

Open the remote web portal on your mobile device at <https://www.ispyconnect.com/app> ↗ or use the remote portal in the app

Click on Account menu at top right and select **Account Settings**

Click **Delete** at the lower left and then confirm

All data will be deleted from your account apart from a one-way hash of your email address (to prevent future usage).

Updating Agent DVR

Before updating Agent DVR, make sure to back up your configuration - this can be done by either copying the files in Agent/Media/XML or exporting them via the web interface's server menu under backup/restore.

Keep up-to-date with the latest features and improvements! Check out the [update log](#) ↗ for all the newest update information.

If you have a license or a subscription, updating Agent DVR is a breeze! Just click on the server menu and select "Update Agent" at the top. This option will appear when an update is available.

For Linux or macOS users looking to update manually, all the instructions you need are on the [update instructions](#) page. Follow these steps to stay current with the latest version.

Windows users, to update manually re-run the installer from the [download page](#)

Troubleshooting

Accessing logs

Agent DVR makes it easy to keep an eye on what's happening under the hood with formatted live logs. You can find these logs right on the local server at /logs.html. For a default setup, that's <http://localhost:8090/logs.html>. Perfect for real-time insights!

From version 3.5.6.0 onwards, Agent DVR also stores the five most recent raw logs in .json format in your Media folder. On Windows, this is typically located at C:\Program Files\Agent\Media. These detailed logs are great for debugging and understanding the inner workings of Agent.

On macOS, the Agent DVR service also writes its console output to ~/Library/Logs/agentdvr.log and ~/Library/Logs/agentdvr.error.log - check these if the service fails to start.

A common issue with Agent DVR not working locally is VPN programs interfering with it. If you have problems with the local version of Agent DVR, try disabling your VPN and see if that resolves the issue. The "Stay Invisible on LAN" setting in NordVPN is known to also cause issues.

Need to access logs remotely? No problem! You can download these raw logs right from the server menu in the web portal. And if you have questions or need a helping hand, our [Community](#) ↗ boards are just a click away. Join the conversation and get the support you need!

Installation Issues

Running into issues with the Windows installer for Agent? If it fails to complete, or if Agent DVR doesn't start, or you need additional functionalities not available in the Windows service mode (like certain GPU drivers and desktop monitoring), here's a workaround using the command prompt:

First, stop the Agent DVR service if it's running. Go to Start, type "services.msc", and hit enter. Find "Agent" in the list, right-click it and select "Stop". To prevent it from auto-starting, right-click on "Agent", go to Properties, set the startup type to "Disabled", and apply the changes.

Next, open a console window. Click Start, type "cmd", right-click "Command Prompt" and select "Run as administrator".

Then, navigate to the Agent DVR directory, usually "cd C:\Program Files\Agent".

Finally, run Agent DVR as a console application by typing "Agent.exe" and hitting enter.

Agent DVR will inform you of any startup issues and the local port it's using. You can exit Agent DVR anytime by pressing enter. Running Agent DVR in the console enables more GPU device usage and desktop recording capabilities.

Facing an error like 'The type initializer for 'Emgu.CV.Cuda.CudaInvoke' threw an exception.' on Windows? You might need to install the [Windows Media Feature Pack](#) ↗ for your OS.

If an antivirus app or firewall is blocking Agent DVR's access to local ports, consider adding Agent.exe to the safe list or opening the necessary port in your firewall.

Using Windows N? You'll need the [media feature pack for Windows N](#) ↗.

On macOS, Linux, or Raspberry Pi, missing libraries can cause start-up failures (like a missing 'libcvaextn.so'). Use commands like 'ldd' or 'objdump -r --dylibs-used' to identify and install missing dependencies. If you encounter such issues, [contact us](#) so we can update our documentation and assist you better!

Glitchy Video

Experiencing glitchy video? Let's smooth things out! Agent DVR defaults to using UDP for quick, real-time video, but switching to TCP could solve any corruption issues at the cost of slight buffering. Here are some other tips and tricks you can try:

To modify these settings, edit the camera, select the General tab then click the "..." button next to video source and on that control choose FFmpeg or Advanced in the top right menu. These options are only available with file and network (IP) video sources.

Check "Prefer TCP" in the FFmpeg settings for a more stable connection.

Uncheck "Low Delay" in the FFmpeg settings. This might improve stability at the cost of a slight delay in the video feed.

Add options to FFmpeg settings. For high resolution streams you may need to adjust some buffering sizes. For example these might help:

```
reorder_queue_size=500  
  
buffer_size=4096000
```

Tip: Agent DVR logs the ffmpeg settings it's applying when cameras are connected. You can override these in the options panel. An example set of options is:

```
probesize=10485760  
analyzeduration=5000000  
max_delay=10000000  
overrun_nonfatal=1  
tcp_nodelay=1  
reorder_queue_size=16  
fifo_size=278876  
buffer_size=2100000  
rw_timeout=8000000  
timeout=8000000  
stimeout=8000000  
user_agent=Mozilla/5.0
```

Try CPU decoding on the Advanced tab if GPU decoding isn't cutting it. Sometimes the CPU will actually give you better performance than the GPU as transferring memory between the system and the GPU can actually take longer than just decoding it in place.

Consider using VLC as the Decoder on the Advanced tab if it's available. This should be a last option as it's not very efficient and there are some bugs in the VLC library

Reolink Cameras, in particular, might face issues with corrupted RTSP streams. A useful tip is to switch the encoder in the camera's settings to use H264 instead of H265, if available. Also, Reolink cameras may offer alternate video endpoints with the **RTMP://** protocol, rather than **RTSP://**. Use the 'Add Camera' wizard in Agent DVR to explore these **RTMP://** alternatives for potentially better results.

Stuttering Video? If you're noticing stuttering in live or recorded playback, especially with some Reolink cameras, here's a fix: edit the camera settings, go to the FFmpeg tab, and add `reorder_queue_size=500` to options at the bottom.

Resetting the Local Login

Forgot your local Agent DVR login? No worries, resetting it is a breeze and will revert it back to no login required:

First, let's stop Agent DVR:

Windows: Go to Start, type "services.msc", find Agent DVR in the list, right-click, and select 'Stop'.

Linux: Open a terminal and run

```
sudo systemctl stop AgentDVR.service
```

macOS: Open a terminal and run

```
launchctl bootout gui/$(id -u) ~/Library/LaunchAgents/com.ispy.agent.dvr.plist
```

On older installs the service runs as a system daemon instead - if that file doesn't exist, run

```
sudo launchctl bootout system /Library/LaunchDaemons/com.ispy.agent.dvr.plist
```

Note: don't just quit the Agent process - the service will automatically restart it.

Next, run the reset script. On Windows, it's **agent-reset-local-login.bat**. On Linux/macOS, use **agent-reset-local-login.sh**. Don't forget to make it executable with:

```
chmod +x agent-reset-local-login.sh
```

Finally, restart Agent DVR:

Windows: Open "services.msc", find Agent, right-click, and choose 'Start'.

Linux: In the terminal, run

```
sudo systemctl start AgentDVR.service
```

macOS: Use the terminal to run

```
launchctl bootstrap gui/$(id -u) ~/Library/LaunchAgents/com.ispy.agent.dvr.plist
```

(or on older system-service installs:

```
sudo launchctl bootstrap system /Library/LaunchDaemons/com.ispy.agent.dvr.plist
```

```
)
```

There you go! Your Agent DVR local login is reset and you can access it without needing to log in. Easy and secure!

Organizing Servers

Removing a Server from Your Account

Want to keep disconnected Agent DVR from your online account? Follow these steps to keep it running independently:

Sign in to ispyconnect.com/app

Choose your server then click on Account menu - Remove Server

Move to another Account

To transfer Agent DVR to another account, follow these steps:

[Remove Agent DVR from your current account.](#)

Click on the server icon, Remote Access and connect it to your new account.

Switching to a New Computer

Upgrading your hardware? You can move Agent DVR to a new machine and keep your camera configuration and recordings by copying the Media folder across. Follow the steps below for your operating system.

Windows

First, uninstall Agent DVR from your old computer using Add/Remove programs, or if it's not listed there, double-click **agent-uninstall-service.bat** in the Agent DVR directory (C:\Program Files\Agent).

Next, [download](#) and install Agent DVR on your new PC.

On your new PC, open 'services.msc' from the Run dialog, find Agent DVR in the list, right-click it, and click 'Stop' to pause the service momentarily.

Now, copy the /Media directory from your old Agent DVR directory to the new one. This directory might be large, so using a large USB drive could be handy. If you only need the configuration, just copy the Agent/Media/XML directory, excluding Media/XML/fileDB.db3.

Once everything's copied over, restart the Agent DVR service on your new PC through 'services.msc' - find Agent DVR, right-click it, and click 'Start' to get things rolling.

Optionally, you can delete the original Agent DVR directory from your old PC once you confirm everything is smooth sailing on your new setup.

Linux

On your old PC, open a terminal window and gracefully stop Agent DVR with these commands:

```
sudo systemctl stop AgentDVR.service
sudo systemctl disable AgentDVR.service
```

This ensures a clean shutdown.

Ready for a fresh start? [Download](#) and install Agent DVR on your new Linux PC. It's a new beginning!

On your new PC, open a terminal and run

```
sudo systemctl stop AgentDVR.service
```

to pause the service for setup.

Time to transfer your data! Copy the /Media directory from your old Agent DVR setup to the new one. If it's quite large, consider using a large USB drive. Just need the settings? Copy only the Agent/Media/XML directory (leave out Media/XML/fileDB.db3).

In the terminal of your new PC, run

```
sudo systemctl start AgentDVR.service
```

to restart the Agent DVR service. Your surveillance system is now up and running!

If everything's working perfectly, feel free to clean up by deleting the original Agent DVR directory on your old PC.

Mac OS

On your old Mac, start by opening a terminal window and run these commands to stop and remove the Agent DVR service:

```
launchctl bootout gui/${id -u} ~/Library/LaunchAgents/com.ispy.agent.dvr.plist
rm -f ~/Library/LaunchAgents/com.ispy.agent.dvr.plist
```

On older installs the service is a system daemon instead - if that file doesn't exist, run:

```
sudo launchctl bootout system /Library/LaunchDaemons/com.ispy.agent.dvr.plist
sudo rm -f /Library/LaunchDaemons/com.ispy.agent.dvr.plist
```

This ensures a smooth departure.

Ready for a fresh setup? [Download](#) and install Agent DVR on your new Mac.

On your new Mac, open a terminal and pause the Agent DVR service with

```
launchctl bootout gui/${id -u} ~/Library/LaunchAgents/com.ispy.agent.dvr.plist
```

It's moving time! Transfer the /Media directory from the old Agent DVR setup to the new one (on macOS the Agent DVR directory is at ~/Library/Application Support/AgentDVR). If you have a lot of data, a large USB drive might come in handy. Just need the settings? Copy over the Agent/Media/XML directory (excluding Media/XML/fileDB.db3).

In the terminal of your new Mac, bring Agent DVR to life by running

```
launchctl bootstrap gui/${id -u} ~/Library/LaunchAgents/com.ispy.agent.dvr.plist
```

Your surveillance setup is now good to go!

Feel free to clean up and delete the original Agent DVR directory from your old Mac once everything is confirmed to be working seamlessly on your new setup.

Important

Got a subscription? Time to link your new Agent DVR setup to your account. Simply click on the Server icon in the local UI and select Remote Access to pair it with your online account. Stay connected, effortlessly!

If you're a license holder, remember to [transfer your license](#) to the new PC.

Using a basic subscription with two Agent DVR instances? Remember, only one can be active on the web portal at a time. To switch, just stop the first instance, and the other will connect seamlessly.

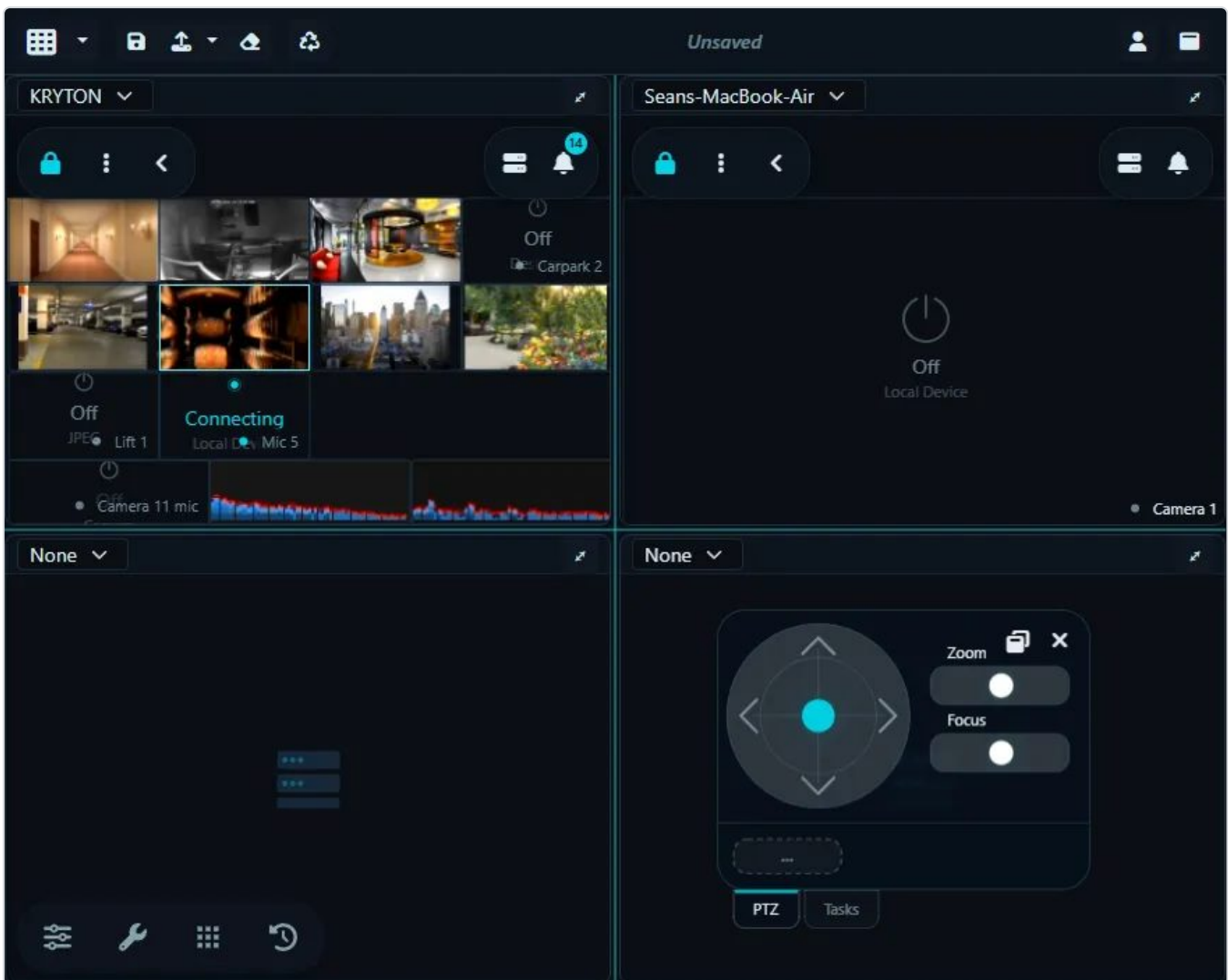
If you've customized drives and storage directories on your old PC, dive into the settings on your new PC to tweak the storage settings to match your new environment. Keep everything organized just the way you like it!

Multi View

If you have more than one Agent DVR server linked to your account, Multi-View provides a single, unified interface to monitor and control all of them at once. This is especially useful for users managing cameras across multiple sites, departments, or locations.

To open Multi-View, choose **"Multi View"** from the server selection dialog (desktop browsers only). Agent DVR will then display every server you have access to in a fully customizable, resizable grid.

Multi-View gives you complete flexibility in how your servers are arranged. A typical layout looks like this:



The toolbar at the top of Multi-View includes several layout and management options:

- Configure Grid:** Adjust the number of rows and columns. This lets you display as many servers as you need in the arrangement you prefer.
- Save Layout:** Store your current layout as a preset so you can quickly return to it at any time.
- Load Preset:** Apply a previously saved layout to instantly switch between different monitoring configurations.
- Clear Selection:** Remove the current set of servers from the grid so you can start fresh.
- Reset Layout:** Restore the grid splitter sizes to their defaults.

Multi-View automatically remembers your layout, so once you've configured it the way you want, it will be ready for you every time you log in. This makes it ideal for ongoing monitoring, control rooms, and multi-site management.

Connecting Remotely

Website Remote Access

Remote access lets you view and control your security cameras from anywhere - at work, travelling, or on your phone - through the ispyconnect.com web portal or the mobile apps.

Agent DVR leverages WebRTC for setting up remote connections, meaning no hassle with port forwarding, and it even works smoothly over mobile internet! For remote access you'll need a subscription. Click the server icon  in the local web interface and select "Remote Access" to get started.

Important: No need to install Agent DVR on other devices or fiddle with port forwarding for remote access. Just navigate to [/app](#) on any web browser once Agent DVR is connected. Remember, remote access to Agent DVR is part of a [subscription service](#).

Subscription not applied? Typically, payment notifications are instant, but occasionally there might be a delay. When your order is processed we'll send you an email, or you can check the [manage licenses](#) page to see if your order has been processed. Any issues? Just [contact us](#) for assistance.

Connection troubles? If you're struggling to connect, especially over a VPN, check your content filtering settings. Make sure to whitelist *.ispyconnect.com and *.azurewebsites.net.

Why use the website? Agent DVR's use of WebRTC means you can bypass most firewall and port forwarding complexities. Direct connections work on your local network, but for secure remote access, browsers require SSL, STUN, TURN, and relay servers, all of which we provide through ispyconnect.com.

Port Forward Remote Access

Looking to enable port forwarding in Agent DVR? With the free version, port forwarding is disabled, but don't worry! You can unlock this feature by purchasing any annual or multi-year [license](#). Just a heads-up: port forwarding success isn't always guaranteed as some networks and firewalls might block necessary traffic for WebRTC connections.

If you're encountering issues with accessing Agent DVR via port forwarding, make sure to check your firewall settings. Ensure the application isn't blocked and that the following ports are forwarded and unblocked on both your firewall and antivirus:

8090 TCP/UDP for the web interface - the gateway to your Agent DVR.

3478 TCP/UDP for the STUN/TURN server - the critical one for remote viewing. Make sure it's forwarded for both TCP and UDP and points at the Agent machine's current internal IP.

50000-50100 TCP/UDP for WebRTC relay connections - optional in most setups, as relay traffic normally travels through port 3478. If remote viewing isn't working, focus on 8090 and 3478 first.

Set these up correctly, and you're all set for a smoother remote access experience with Agent DVR!

Connecting Locally

Local Connections

Planning to access Agent DVR over your Local Area Network (LAN)? You might need to tweak some settings in your firewall or antivirus, as Agent DVR utilizes WebRTC for its connections. Here's a quick guide to ensure a smooth LAN experience:

8090 TCP/UDP for the web interface - This is your primary gateway for accessing Agent DVR within your network.

3478 TCP/UDP for the STUN/TURN server - Essential for helping your devices find each other and establish a connection.

50000-50100 TCP/UDP for WebRTC relay connections - Usually not needed on a local network, but worth unblocking if you're troubleshooting connection issues.

By ensuring these ports are open and not blocked by your firewall or antivirus, you're setting the stage for seamless LAN access to Agent DVR.

To enhance the security of your LAN access, it's a great idea to set up a login. You can do this under Server Settings - Users in Agent DVR. Secure and simple!

Forgot your password? No sweat! Just stop Agent DVR and reset it. On Windows, use "Agent.exe reset-local-login", and on macOS or Linux, run "agent-reset-local-login.sh". This way, you're back in control in no time.

Facing connection issues locally? Sometimes browser extensions can be the culprits. If you're having trouble, try switching your browser to Safari, Chrome, Firefox, or the latest version of Edge. Consider disabling any troublesome extensions and clearing your cache to ensure smooth access.

Customizing with Parameters

Want to tailor the Agent DVR UI to your liking? It's easy to add parameters to the URL for customization! Here's how you can do it:

Set the default UI size (also available under account menu - UI Settings):

?large=true - Start with a larger UI scale.

Want to auto-play audio on load? (Note: version 3.7.7.0+ may require additional browser settings adjustments):

?playaudio=true - Set your UI to be heard right from the start.

Prefer a more minimalistic approach? Start in minimized mode (top and bottom UI bars hidden) from version 3.8.7.0+:

?mini=true - For a cleaner, distraction-free interface.

For quick access, pass in your local username and password for auto-login (from version 4.7.6.0+). Caution: This will expose your credentials to the network:

?un=username&pwd=password - Enter your details for faster login.

Want to jump straight to a specific view or select a device (version 4.9.8.0+)? Check this out:

?viewIndex=1&oid=2&ot=1&max=true#Live - Directly navigate to your desired view and device.

Pass a language in for the UI:

?lang=en - Specify the 2 letter language code.

Explore these options to make Agent DVR work just the way you want it.

No Local ICE

Can't connect to cameras?

Your browser may be blocking local connections. Common causes and solutions:

Recommended Solutions

1. **Use our desktop app shortcut** - automatically loads a WebRTC extension
2. Run agent.exe openBrowser
3. Try a different browser (Chrome, Edge, Brave, Vivaldi)

Privacy & Security Software

4. Temporarily disable your VPN (NordVPN, ExpressVPN, Surfshark, etc.)
5. Check VPN browser extensions for "WebRTC leak protection"
6. Disable antivirus "web protection" features temporarily
7. Turn off "Secure DNS" or "DNS over HTTPS" in browser settings

Corporate/Enterprise Environment

8. Contact your IT department - they may have restricted WebRTC
9. Try using a personal device on the same network
10. Check if you're on a "guest" WiFi network with restrictions
11. **Enterprise/managed devices:** Contact your IT department - WebRTC may be locked by company policy
12. **Domain-joined computers:** Your system administrator may need to whitelist localhost WebRTC

Browser Settings

- 11. Disable browser extensions temporarily (especially privacy-focused ones)
- 12. Clear browser cache and reload the page

Firewall & Network

- 13. Temporarily disable Windows/macOS firewall
- 14. Check router firewall settings
- 15. Ensure you're on the same WiFi network as the camera system
- 16. Try connecting from a mobile device on the same network

Mobile Issues

- 17. Try Firefox mobile instead of Chrome mobile
- 18. Disable mobile VPN apps
- 19. Check if you're using mobile data instead of WiFi

Advanced Troubleshooting

- 20. Open browser developer tools and check for errors
- 21. Follow our manual setup instructions
- 22. Restart Agent DVR and try again

Plugins

Installing Plugins

Plugins are optional add-on modules that extend Agent DVR with extra audio and video processing features, such as barcode scanning, weather overlays and audio filters.

The easiest way to install plugins is through the remote web portal. Once connected, click on the Server icon at the top right and navigate to 'Plugins' under System. Here, you can select the plugin you wish to use from the drop-down menu at the top-right and click 'Install' to get started.

Prefer to install manually? No problem! You can build the plugins [from source](#) and then copy the built output to Agent/Plugins/PLUGINNAME. This method gives you more control over the installation process.

Available Plugins

Agent DVR comes packed with advanced video processing features like CodeProject AI integration, along with advanced object tracking, audio recognition and counting detectors. To further enhance your experience, we offer a range of plugins you can use in AgentDVR to extend its functionality.

Plugin List

Barcodes

Scan pretty much any barcode from a camera (windows only).

Raised Events: Barcode Recognized

Supports: Video

[screenshot](#)

Gain

Apply live band filters on audio coming from audio devices.

Raised Events: None

Supports: Audio

[screenshot](#)

Live Delay

Adds a delay to live audio and video (useful for sports analysis).

Raised Events: None

Supports: Video, Audio

[screenshot](#)

Weather

Adds a weather status overlay to live video based on your location. Raise events if the weather changes - for example if a storm is coming or if wind gusts or temperature limits are exceeded. You can customise the layout and display mode of the weather data from just an icon to full detail.

Weather configuration takes a format string to layout the information. Here are some example format strings you can use:

Full information:

```
{icon}{main}: {description}  
Wind: {wind} Gust: {gust}  
Temp: {temp} Feels Like: {feelsLike}  
Humidity: {humidity} UVI: {uvi}
```

Icon Only:

```
{icon}
```

One Line:

```
{main} {wind} {temp} {humidity} UVI: {uvi}
```

Raised Events: High Temp, Gust, Status

Supports: Video

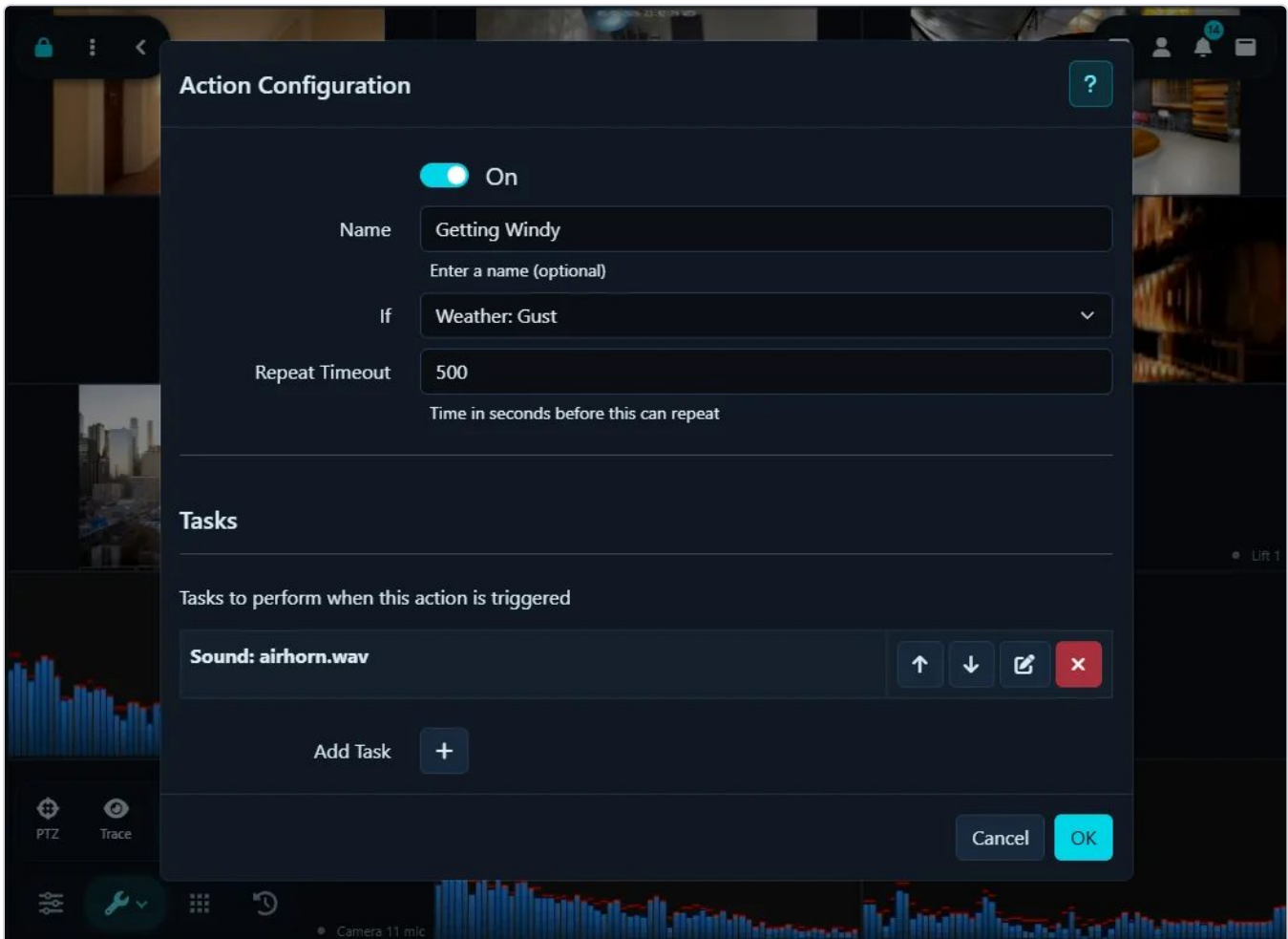
[screenshot](#)

If you are using an audio plugin like [Listen](#) on a camera you will need to edit the camera, select the Audio tab and click to configure the microphone. From there you can access the Plugins tab for audio devices. Alternatively you can click the Server Icon, Edit Devices and edit the microphone from that list.

Configuring Plugins

Ready to harness the power of plugins? Simply add a device (camera and/or microphone) and go into its edit settings. Look for the Plugins tab in the drop-down at the top right. Here, you can select your desired plugin and click the "... " button to configure it to your needs.

Some plugins raise events that you can attach actions to. The Weather plugin, for example, raises a Gust event when gusting winds exceed a specified value (configurable in the plugin). Editing the camera and navigating to the Actions tab gives you options to respond to this - sounding an alarm or starting a recording for example. Simply select the plugin name: event (e.g. Weather: Gust) in the If select box and assign an action.



Create your own Plugin

Plugins are dynamic modules you can add to Agent DVR to enhance its audio and video processing capabilities. With plugins, apply real-time effects, overlays, raise events, and trigger alerts in Agent DVR, allowing for advanced custom actions.

To start creating plugins for Agent DVR, begin by cloning our open-source plugins at <https://github.com/ispysoftware/AgentDVR-Plugins>. You'll need a recent version of Visual Studio to build them.

We recommend starting with the demo plugin as your base. Ensure you have the latest version of [Agent](#) installed. After building the demo plugin, copy all files from the output folder to Agent\Plugins\Demo\. Restart Agent DVR, edit a camera, and head to the **Plugins** tab. Enable the plugin, select **Demo** from the dropdown, and click the "..." button to configure it.

The Demo plugin is fully cross-platform compatible and showcases the extensive functionality you can build with plugins. It includes live video effects, graphic overlays, live volume control, and integration with Agent DVR's Events subsystem. The plugin menu provides insights into how various input controls operate.

Plugin Notes for Developers:

Configuration: Agent DVR uses JSON and a class file for settings storage. To configure settings edit the config.cs file.

Agent DVR's configuration rendering relies on .json files. Edit config_en.json in the json directory for UI display, where you can add multiple sections rendered as tabs. The key 'bindto' fields in json link to the config fields. Agent DVR automates control rendering, settings storage, and updates.

Adding `"live": true` to json entries enables immediate updates without waiting for the OK button click, which is great for live tuning. The 'converter' field utilizes 'PopulateResponse' in Utils.cs for value formatting.

Media Support: Choose to process "video", "audio", or both. The 'Supports' field in Main.cs can be hardcoded.

Continuous Processing: Every video and audio frame from the device is sent to the plugin for analysis or processing, as demonstrated in the demo.

Motion/Alert Processing: Process frames on motion or alerts by utilizing the 'ProcessEvent' method in the demo plugin. This allows frame processing only during these events.

Custom Events: 'GetCustomEvents' method in your plugin should return a list of custom events it generates. These events then appear under Actions in Agent DVR UI's 'If' list. Trigger these events with a 'Result' item, specifying action name and optional MSG, Tag, Filename, and AIJSON.

Alert, Detect, and Tag: Raise alerts or detect events by adding a Result with "alert" or "detect" eventName. Tag ongoing recordings with a 'tag' eventName and set Tags as needed.

API Calls: Agent DVR initializes plugins with device info and local server port, useful for API commands for the device. The properties AppDataPath and AppPath are also set for display or file saving locations.

Distribution: Created a cool or useful plugin? [Share it with us](#) and contribute to the community!

Nest and Dropcam Cameras

About

Google has discontinued Dropcam and is phasing out public video sharing on legacy Nest cameras. This integration only works with older Nest cameras that can still share a public feed at video.nest.com. Newer Google Nest cameras do not provide a public stream that Agent DVR can use.

To use a legacy Nest or Dropcam camera with [Agent DVR](#) you need to make the video feed public. As long as you don't share the URL of the camera with anyone else this shouldn't be a problem. Use the generator below to create a source URL.

Add the camera in Agent DVR by adding a new device and choosing [NEST](#) as the source type on the General tab.

Generator

Public URL

FAQ

No Remote Connection

No need to install Agent DVR on other computers for remote access. If you've done so, it might confuse the portal. Simply follow the "Uninstalling" instructions above to remove Agent DVR from other PCs. Then, restart the computer running Agent DVR and ensure it's active (check the local web interface).

Remember, Agent DVR needs to be running on a computer for remote access - don't shut down your PC! Also, adjust your power settings to prevent the PC from entering sleep mode.

Possibly there is a temporary outage on our servers, check the logs in the local UI (under the server menu) or our [Service Status](#) page.

A PC restart might also help.

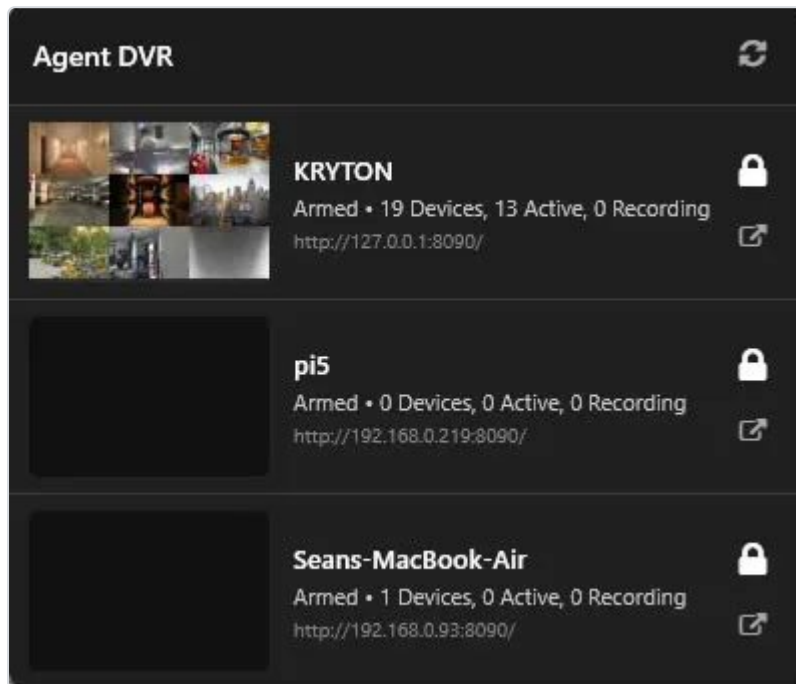
Lost Configuration

If Agent DVR encounters a problem with loading the configuration, it might reset it, but usually, it backs up the file first (e.g., "C:\Program Files\Agent\Media\XML\objects_(numbers).xml"). Try restoring this backup via the server menu. If that fails, [reach out to us](#) for help.

Windows Tray Application

About

Discover the ease of monitoring with the Windows version of Agent DVR! Our Tray Application automatically finds Agent DVR instances on your network. Enjoy quick access, stats, and live thumbnails of your cameras, all in one place!



Get started effortlessly with the Tray application, included in the Agent DVR Windows Install. Install Agent DVR from our [download page](#). It's pre-set to spring into action at startup.

Want to use the Tray application on other computers in your network? Simply copy AgentTray.exe from the Agent DVR directory to another computer and run it. You can even set it up to [start automatically](#) for convenience.

Using the Tray App

The main tray icon colorfully informs you: red indicates a local Agent DVR instance isn't found, and blue signals its presence.

Right-click the icon for options: start/stop the local service, exit the tray app, or manually add new Agent DVR Servers if needed.

A simple left click reveals connected Agent DVR instances, with details like camera previews, server names, armed status, and a device summary. Local instances show in green, remote ones in black. Click on a Server to launch it in your web browser.

If your server requires a login, the summary will prompt "Needs Login." This is not your iSpyConnect.com login, but the one set in your local server settings.

The summary like "Armed, 2 dev, 2 on, 0 rec" gives a quick snapshot: Agent DVR is armed, two devices are connected, both active, and none recording.

Hit the refresh icon at the top right to reinitiate network discovery, automatically locating new Agent DVR instances on your network.

Removing the Tray App

To uninstall the tray app, right-click it, select Quit, and remove AgentTray.exe from the Agent DVR directory. Alternatively, you can [disable its auto-start](#) at startup.

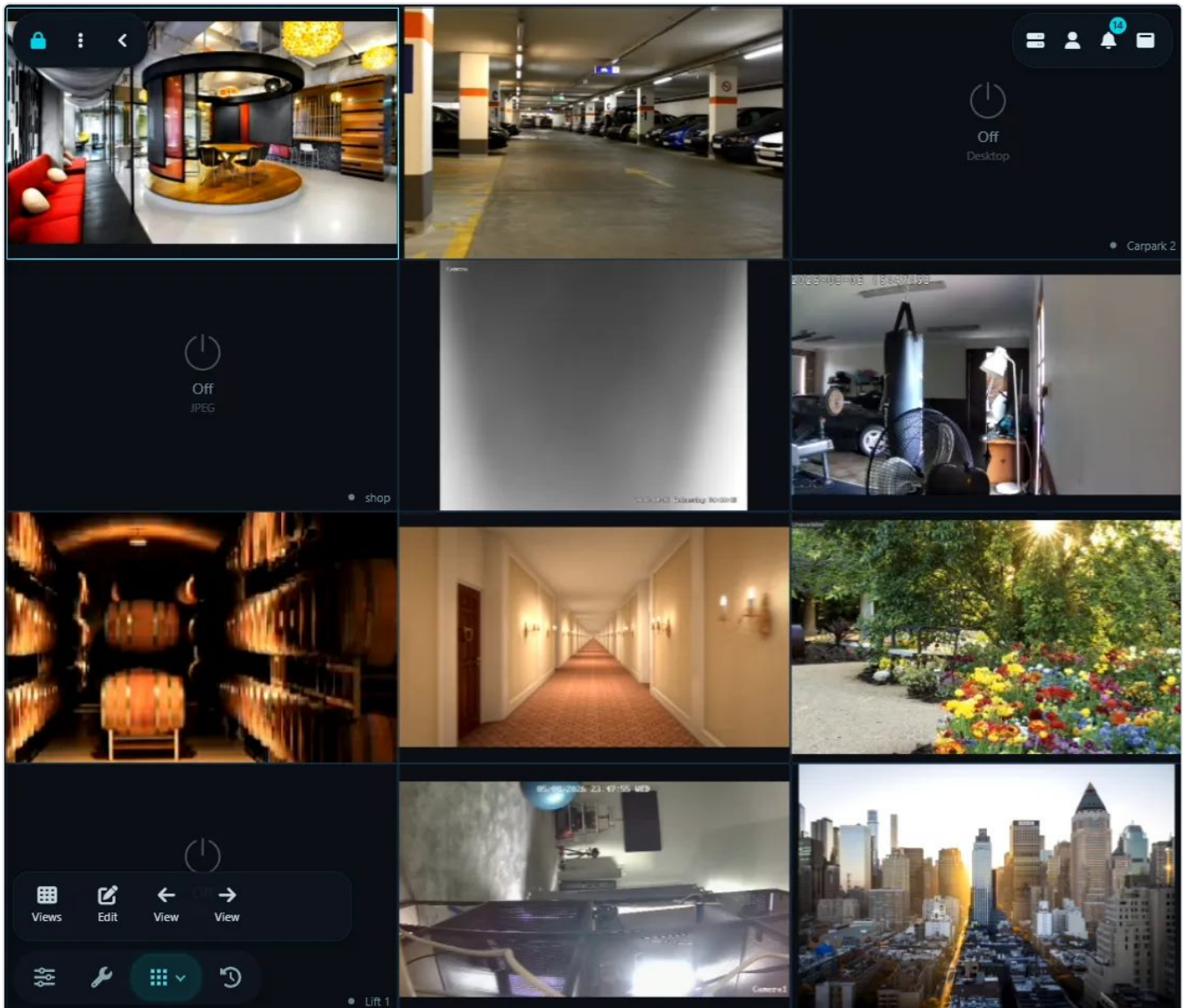
User Interface

Live Viewing Devices

Using the Live View

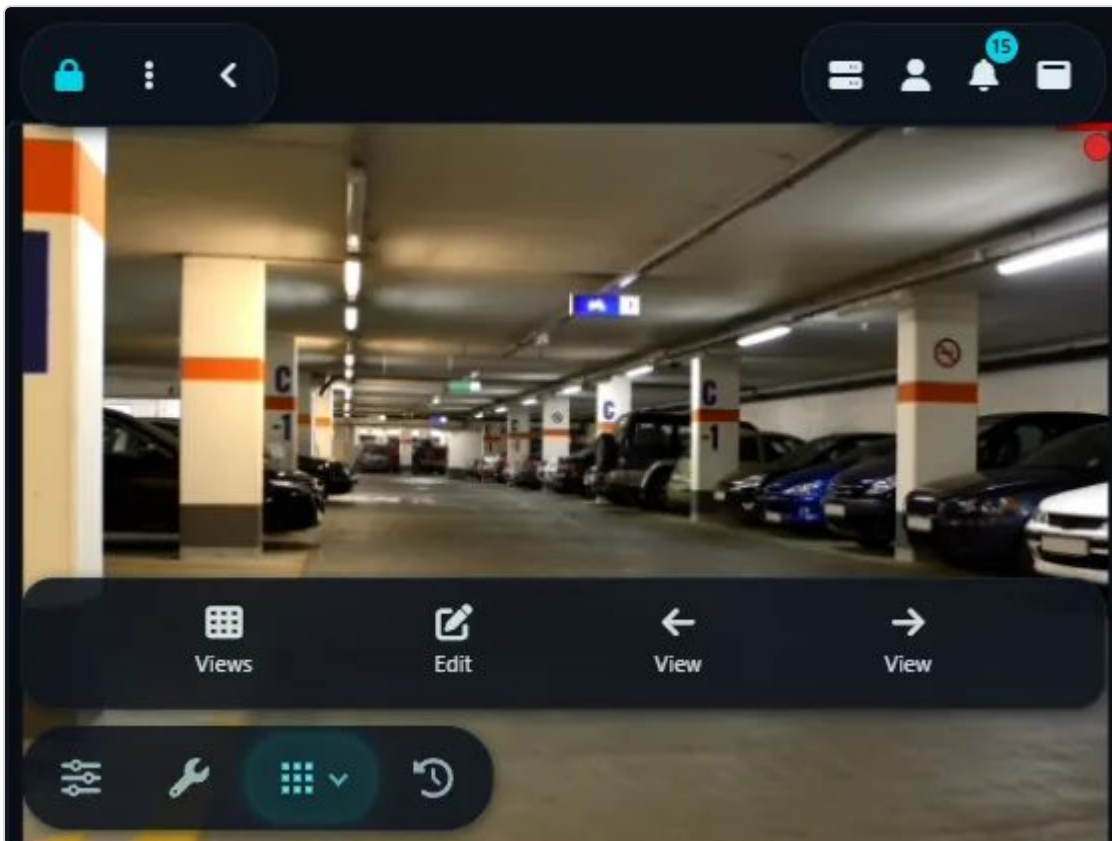
To access Live View, click on the view menu in the top bar and select the Live View  icon.

The live view is your window to real-time streams from your security cameras and microphones. Set up multiple live views in Agent DVR and add any devices you like. Agent DVR intelligently arranges your devices for optimal viewing on any screen.



Panel Markers

The live view has markers to show device state and recording status:



Blue border on left and bottom - Indicates the selected device. Controls on the bottom left apply to this device.

Red "REC" symbol at top right - The device is recording.

Red flashing border at top and right - The device is in an alert state.

Orange flashing border at top and right - Motion has been detected by the device.

You can turn Icons on in the Account Menu - UI Settings. Icons will then be displayed at the bottom left of each device showing their state (recording, alerts enabled, motion detection enabled, schedule enabled)

Buttons/ Icons

The live view includes icons at the bottom for controlling the selected device and the view. Left buttons control the active device, right buttons control the view. Tool-tips explain each button's function and shortcuts.

Device control buttons include:

 Power on/off the device.

 Edit the device.

 Start/Stop manual recording.

 Take a photo.

 Trigger a manual alert.

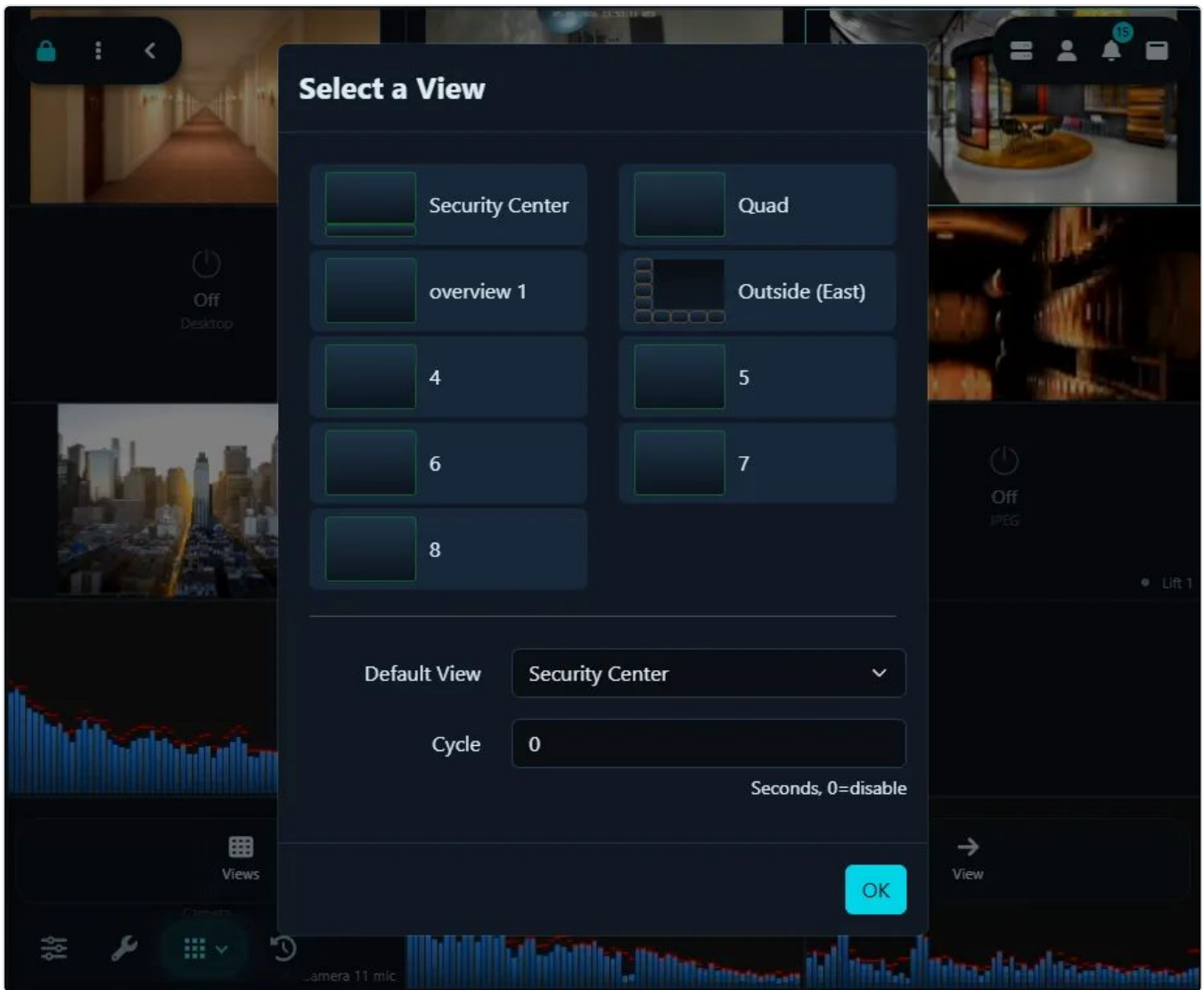
	Open tasks for the device.
	Go to device recordings.
	Go to device photos.
	Playback last 20 seconds from recording.

View control buttons include:

	Toggle the motion highlighter. The motion highlighter feature changes the video to black and white, helping detected motion stand out clearly. When this feature is enabled, everything in the video appears in shades of gray, while any detected movement is highlighted in red. This makes it easier to spot movement, as it contrasts sharply with the grayscale background.
	Open volume control.
	Edit the view.
	Start/Stop playback of live view.
	Open views menu.
	Start/Stop talk.
	Show/Hide PTZ controller.
	Show PTZ presets.
	Previous view.
	Next view.

Using Views

Click the views icon  at the bottom right to open the views menu. Each view shows a preview of the associated [layout](#). To switch to a specific view, simply click on its button. Setting **Cycle** to a number like 3 lets Agent DVR automatically rotate through views with devices every 3 seconds. **Default View** determines the first view shown when you open the browser.



To edit a view (add devices, rename, change layout, etc.), click the edit icon  at the **bottom right**.

Manually cycle through your views in the live screen using the left  and right  arrows. Note: these controls only show views with added devices.

For detailed information on using and customizing layouts, check out our [layouts guide](#).

Using the PTZ Controller

Click on the  icon to show/hide the PTZ (Pan-Tilt-Zoom) controller. Select a device in the live view, and then use the PTZ controller to operate it. Ensure PTZ is configured on your device - edit the device and [see PTZ](#) for setup instructions.

Agent DVR offers 2 different PTZ (Pan-Tilt-Zoom) controller options. To choose your preferred style, head over to the Account Menu and select UI Settings.

Click and drag on the control's background to move it around the live viewer.

Use the round joystick controls by clicking and dragging with the mouse or using touch gestures to control your camera's PTZ.

With the PTZ controller displayed, use numpad arrow keys and numpad +/- for zoom adjustments.

Click or tap the blue arrows or + / - on the zoom control for incremental movements.

Middle-click to show/hide the PTZ control.

For digital PTZ, use the mouse wheel or pinch and swipe gestures on touch devices to zoom. When zoomed in, click and drag to navigate the zoomed area.

Gamepad and Joystick Support

Starting from version 3.9.7.0, Agent DVR supports PTZ control via gamepad. Note that for local usage using a gamepad you may need to set up SSL:



Tips:

To maximize a device, click on it to select it and then click again. If your camera has high and low-res stream URLs, you can set Agent DVR to use the high-res stream when maximized. Edit the device, open the video source settings and set "Use HD stream" to "Maximised Only".

Click on a device to select it. Use the bottom left device controls to switch it on/off, start/stop recording, take photos, trigger manual alerts, or edit and run custom [tasks](#).

Add microphones as well as cameras to the live view. Configure the microphone's display style in the General tab when editing the Microphone settings.

Use the ⋮ menu at the bottom right for more features like RTMP broadcast, starting talk, pausing live video, and locking/unlocking layout positions.

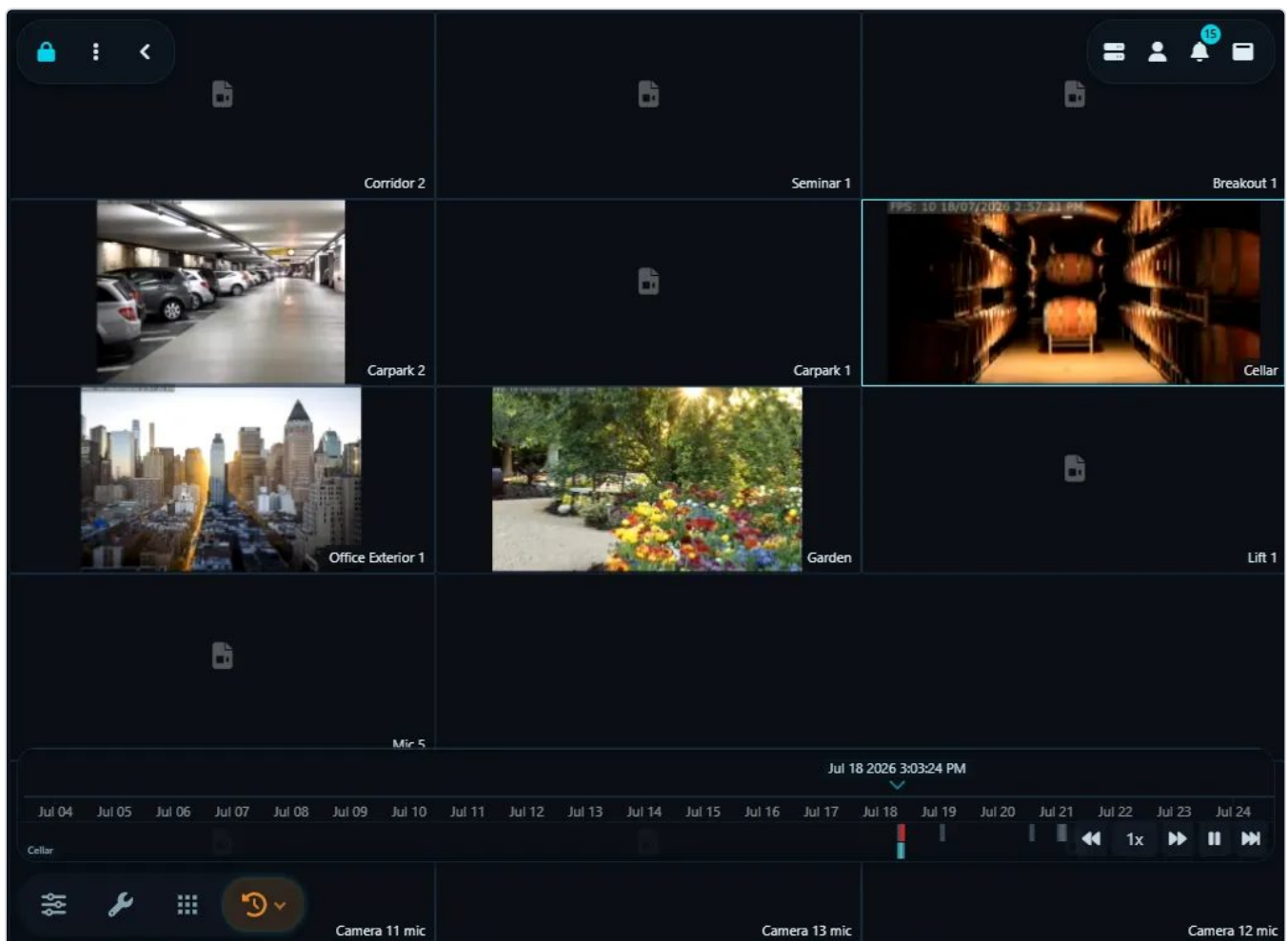
Agent DVR shows which device is selected with a highlight around the left and bottom. Alerting devices will have red flashing lines around the top and right.

Assign a location to your camera to display it next to the camera name, and set the background and border color to match the location color.

Using the Time Machine Tab

The Live View includes a built-in Time Machine tab. Click the ⌚ clock tab at the bottom of the live view to switch from live streaming to Time Machine playback mode. Use it to scrub back through recorded footage and review an event that just happened without leaving the live view.

In Time Machine mode the live view plays back synchronized recordings from your devices instead of live streams. A timeline graph appears at the bottom - click and drag it to select a playback time, then click the Play icon. The Time Machine will automatically align to the nearest available recording. Zoom in and out of the timeline using the mouse wheel, zoom controls, or a pinch gesture on touch devices.



The colored bars on the timeline represent where recordings are available.

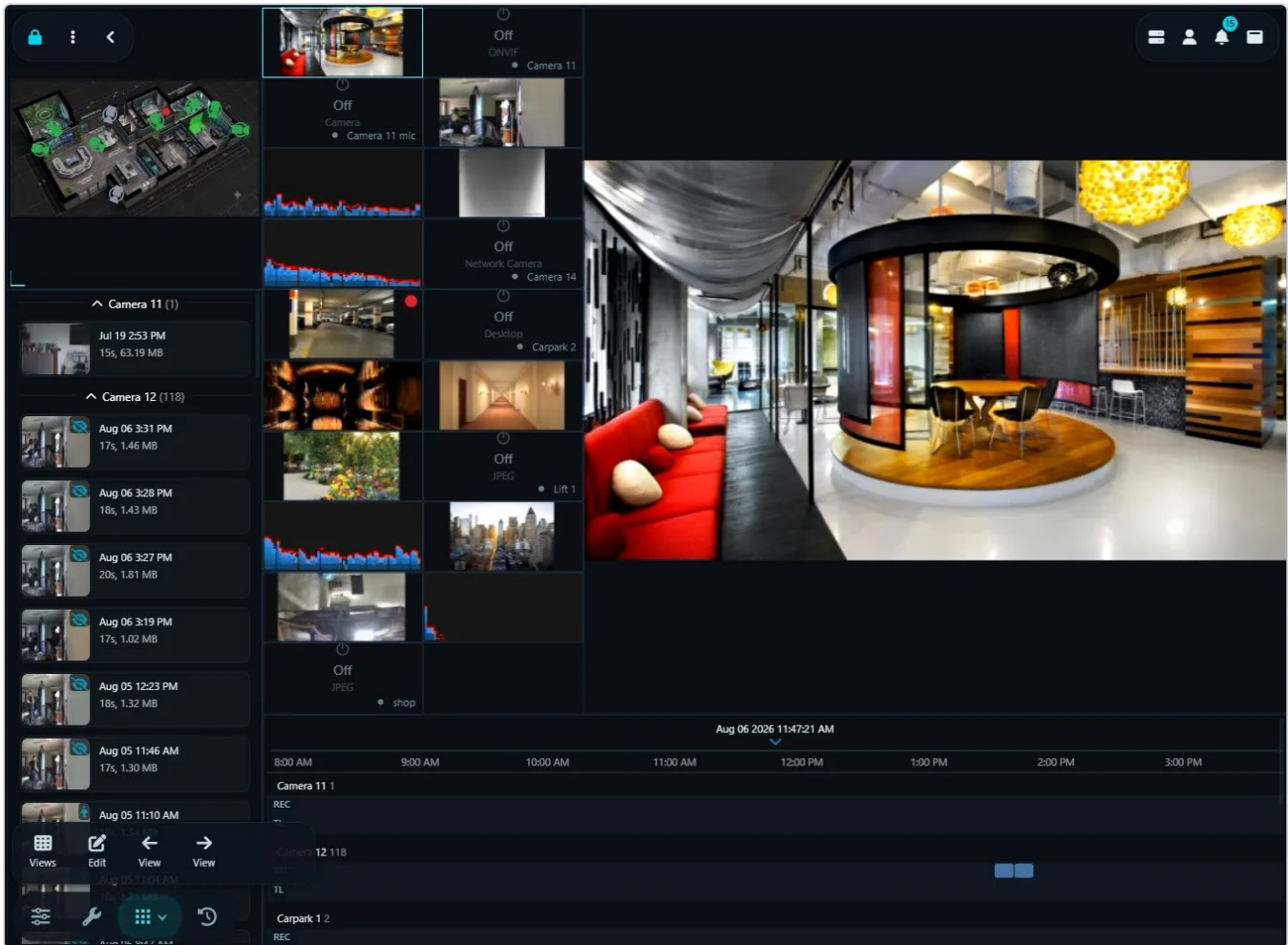
To return to live view drag the time machine so the play head is back in the live green area.

In Time Machine mode the controls menu for the cameras changes to work with the files instead of the live devices.

Layouts

Configuring Layouts

Layouts dictate how devices are displayed in the [live view](#). Use them to arrange multiple cameras exactly how you want - for example a wall display for a monitoring station, or a dedicated view for your outdoor cameras. Agent DVR offers 9 configurable views (editable under Server Settings - User Interface), and each view can have its own layout. To select a view, click the  icon at the bottom right.



Once a view is selected, click the  icon at the bottom right of the live viewer to configure it.

Configure View



Name

Outside (East)

Layout

Desktop



Add or edit layouts in server settings

Selected Device

None



The device that is first selected when displaying this view

☐ Auto Filter

Filter recordings and photos on selected device

Slots



Floorplans
All Plans



Grid Slot
19 Devices

Main Display

Recordings
All Devices



Timeline
All Devices

↑ Click a slot to add a device ↑

OK

Name: Assign a friendly **Name** to your view, like "Outside Cameras".

Layout: Select a layout from the dropdown. A variety of layouts are provided, or you can [create your own](#).

Selected Device: Choose a Device to highlight when this view is loaded.

Auto Filter: If checked, Recordings, Photos, and Timeline controls will only show content from the selected device, ignoring other applied filters. If unchecked, regular device filters are applied.

Once you've chosen a layout, you can start adding devices to the layout slots. The slots are color-coded with a border to signify their type:

Red border - Alert Slot: Displays devices in an Alert state, cycling through multiple ones if available.

Blue border - Motion Slot: Shows devices that have detected motion, cycling through them if there are multiple.

Green border - Grid Slot: Displays devices in a grid layout, automatically adjusting to maximize camera space.

Orange border - Interval Slot: Can contain multiple devices, cycling through them if more than one is present.

Purple border - Control Slot: Displays controls like the recordings browser, floorplans, or timeline. Adding devices filters the content; no devices show all content. Only one control slot of each type can be added to a layout.

Main Display: Shows the currently selected device. **Devices cannot be added to this slot.**

To add devices to a slot, click on the **+** icon in the slot. This will open up the slot configuration control.

Configuring Layout Slots

To configure a slot, drag and drop the devices you want to include from the left column to the right. You can reorder devices in the right-hand column to change how they appear in the live viewer.

Grid Slot

Displays devices arranged in a grid

Drag, drop and reorder devices



Excluded

Camera 11 mic

Camera 12 mic

Camera 13 mic

Mic 5

Seminar 1 mic

Included

Breakout 1

Camera 11

Camera 12

Camera 13

Camera 14

Carpark 1

Carpark 2

Cellar

Corridor 2

Garden

Lift 1

Office Exterior 1

Seminar 1

shop

New Device

OK

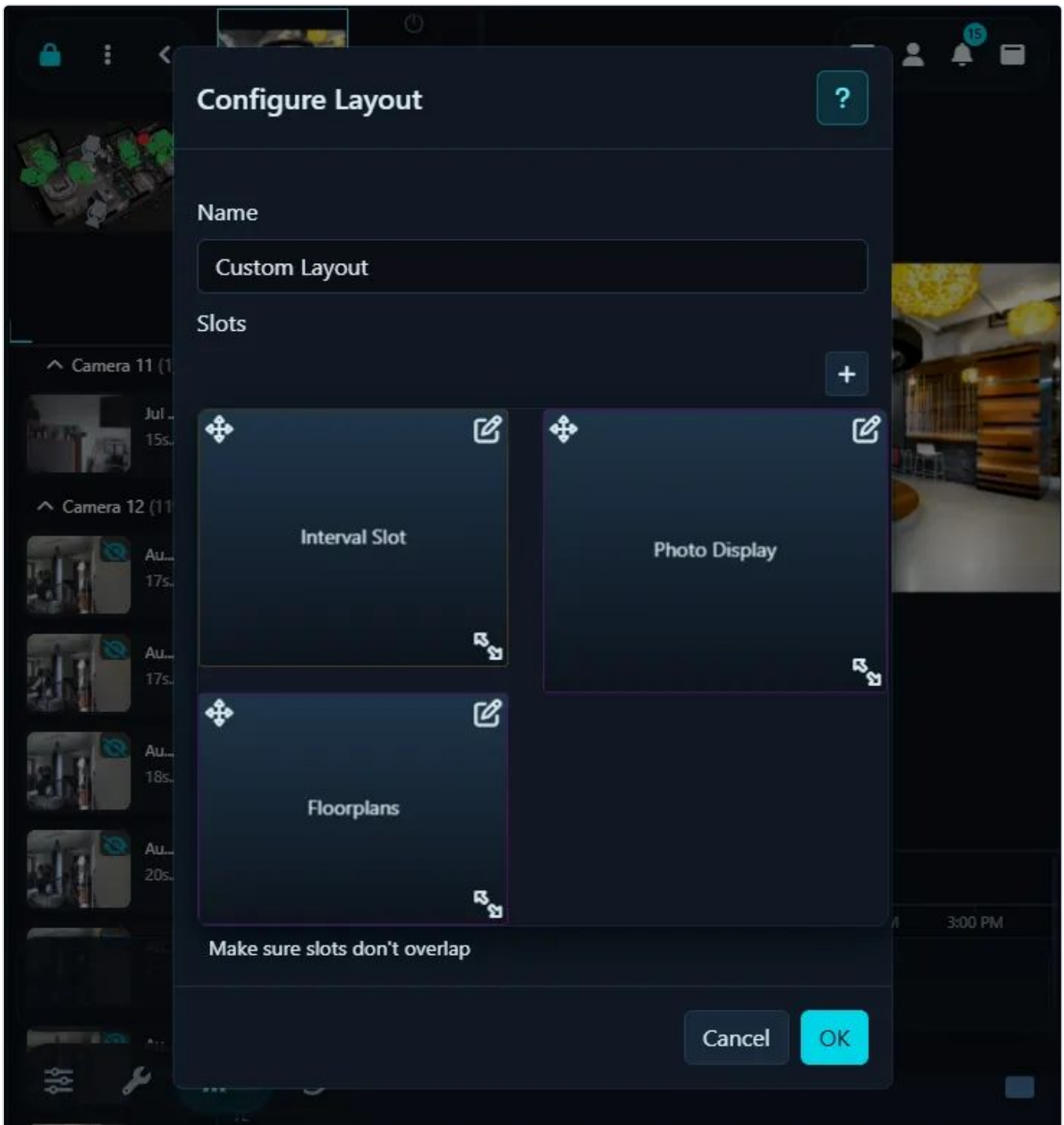
Additionally, you can add a new device directly from this panel, and it will automatically be included in this slot.

Use the bottom controls to move all devices into or out of a slot at once.

Customising Layouts

Create your own layouts in Agent. To start, navigate to the Server menu  - **Settings** - **Layouts**. Here, you can add, edit, or delete layouts.

Click to add a new layout.

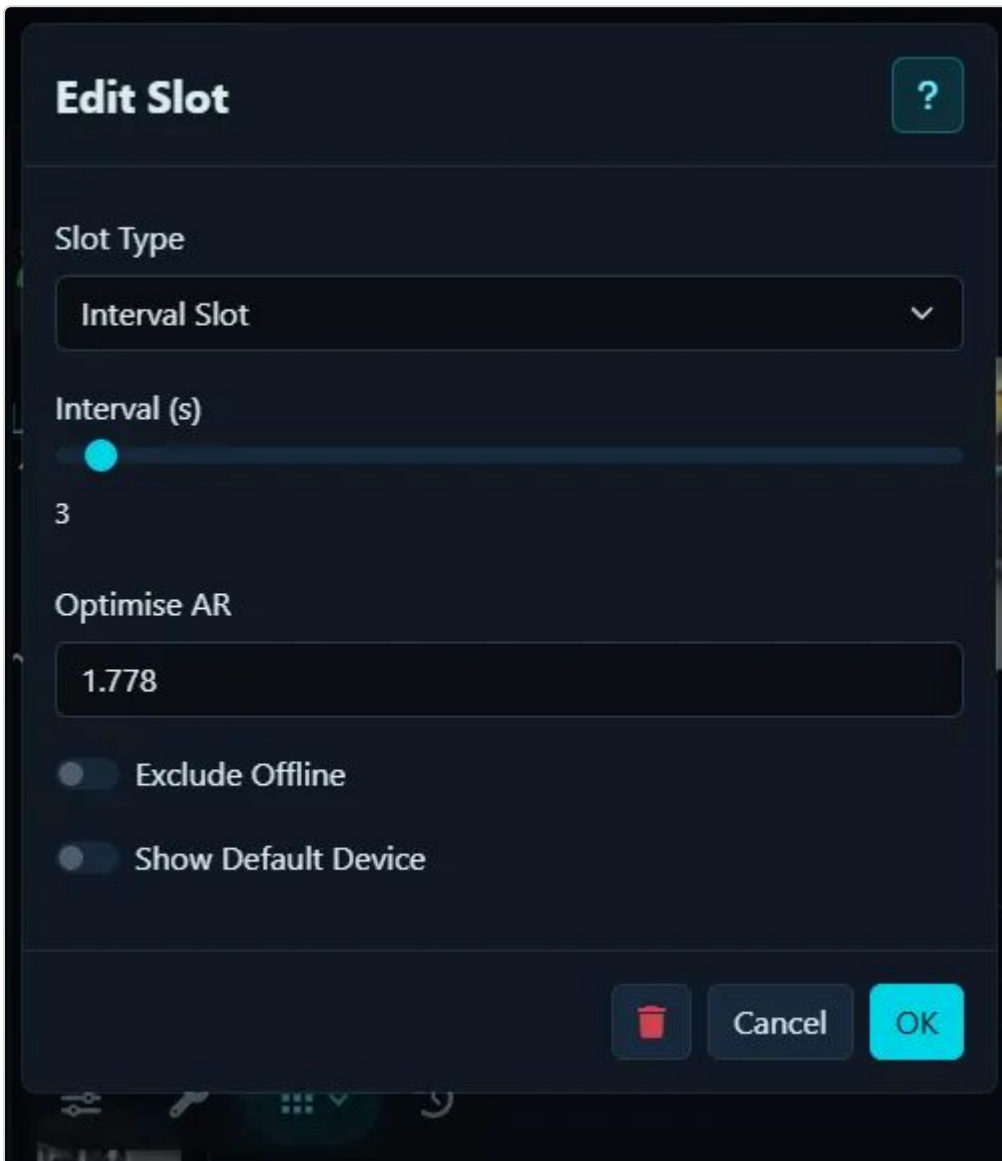


Use the **+** icon to add slots to your layout. (Devices are added to these slots later via the live viewer).

Click and drag slots using the  control, resize them with  and edit them with .

Important: Ensure slots don't overlap. The layout designer snaps to a grid for easy device placement.

Clicking to add or edit a slot opens the slot configuration control:



Slot Type: Choose the type of slot - options are detailed [above](#).

Interval: For slots with multiple devices, this sets the delay (in seconds) for cycling between devices (not applicable to Grid slots).

Optimise AR: Adjust this to optimize the grid layout for different aspect ratios. Use 1.778 for 16:9 cameras and 1.333 for 4:3 cameras.

Skip Offline: Excludes offline controls from the slot (not applicable to Grid view).

Show Default Device: Displays the first enabled device (in motion or alert slot) when there's nothing else to display.

Configure your slot and click OK. To remove a slot, select **Delete**.

Click OK to save your layout. To apply your new layout in the [live viewer](#), click the  icon at the **bottom right** and select your new layout from the dropdown.

Saving and Loading Layouts

Use the Server menu  - **Backup/Restore** option to export and import your layouts.

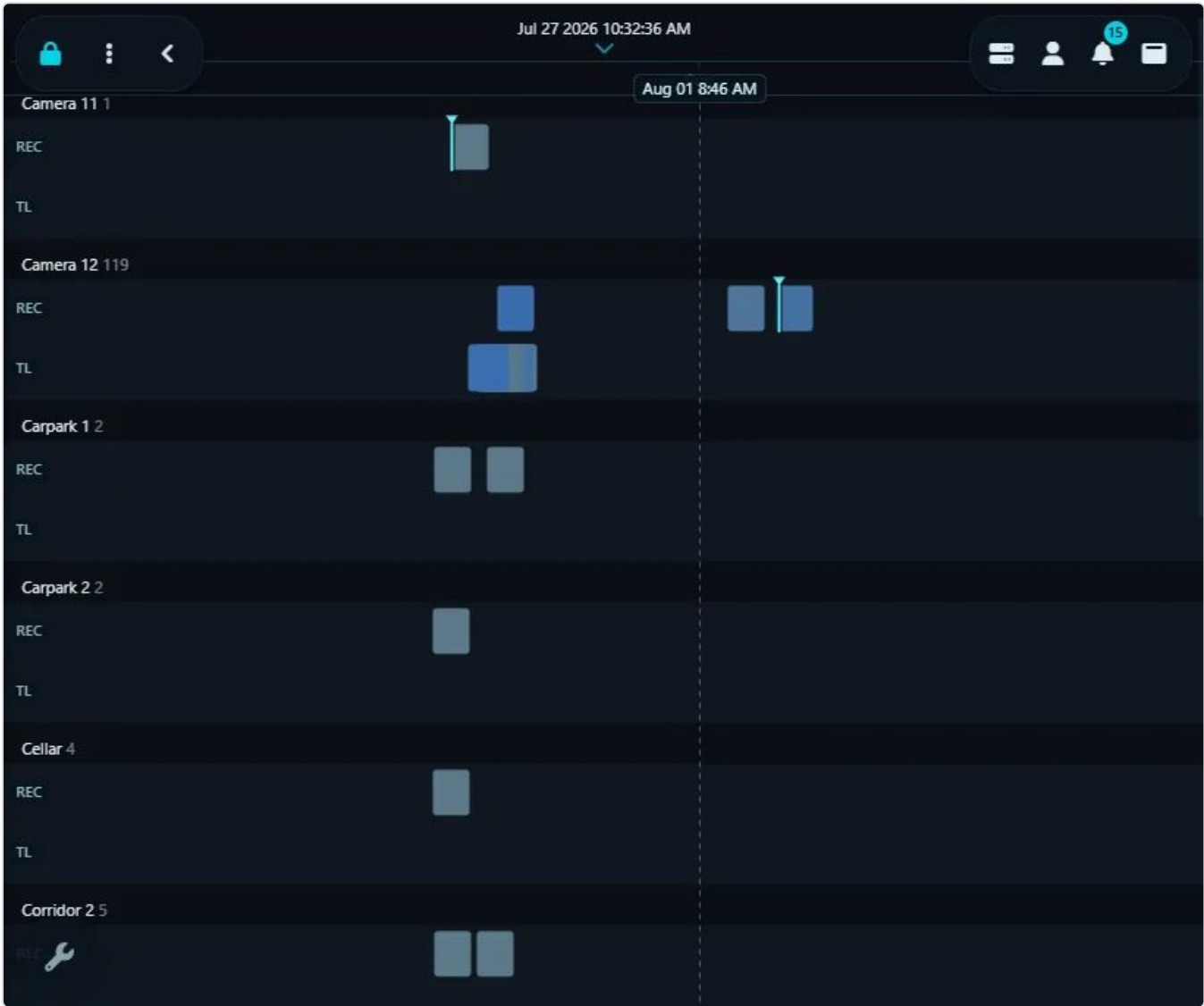
Time Line

Using the Time Line

To access the Time Line, click on the view menu in the top bar and select the Time Line 📅 icon.

The Timeline provides a straightforward way to visualize events in chronological order. Recordings from all devices are arranged sequentially. Swipe or click and drag with the mouse to navigate. To zoom, use ctrl + mouse wheel or just the mouse wheel on the header or on touch use pinch gestures. Click on an activity bar on the timeline to start playback, or on a camera thumbnail to initiate a mini live feed.

Note: The timeline only displays cameras with recordings; cameras without any recordings will not be shown.



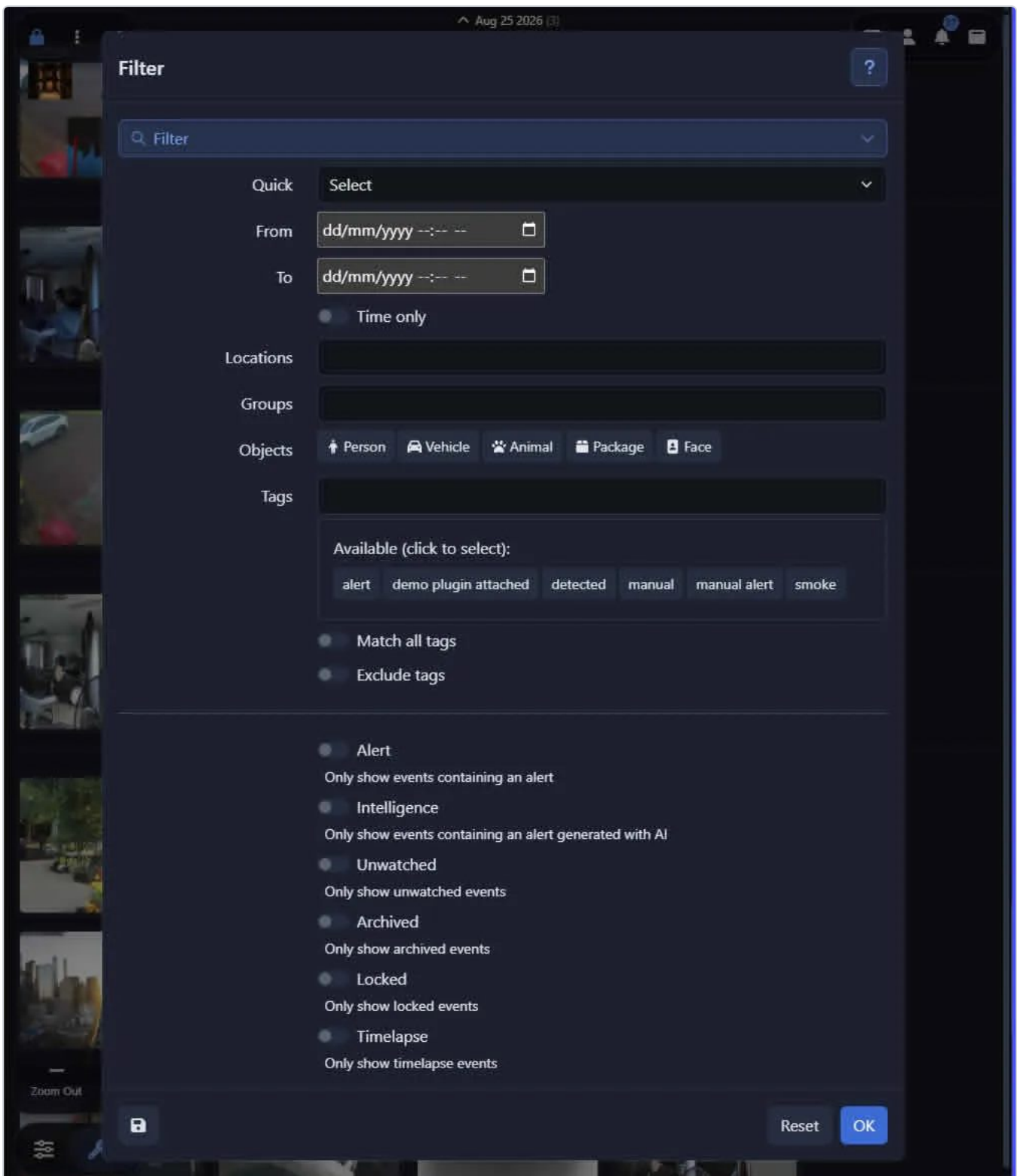
The controls on the toolbar let you:

🕒	Switch to the Time Machine at the currently selected time
—	Zoom out
+	Zoom in

 Zoom reset
 Page left
 Page right
 Go to Now
 Quick Filter
 Filter
 Toggle display mode (by name or by location)

Filtering

To manually filter recordings, click on the filter icon (magnifying glass) at the bottom right.



From/ To: Select a date range for your search.

Locations: Filter by locations. Add locations in the camera settings under the General tab.

Objects: Click the Person, Vehicle, Animal, Package or Face buttons to show only events where [Object Recognition](#) detected that type of object. Selecting several shows events matching any of them. Matching events display a small icon for each detected object type. Recordings made before this feature was added may not be matched.

Tags: Enter tags for filtering, especially useful if you've tagged recordings manually or with [AI](#). 'Timelapse' is an auto tag for timelapse recordings.

Alert: Check this to display only recordings containing an alert event.

Intelligence: Filter to show only recordings with alert events generated by [AI](#).

Unwatched: Check this to display only recordings you haven't viewed yet.

Archived: Check this to display only recordings that have been archived.

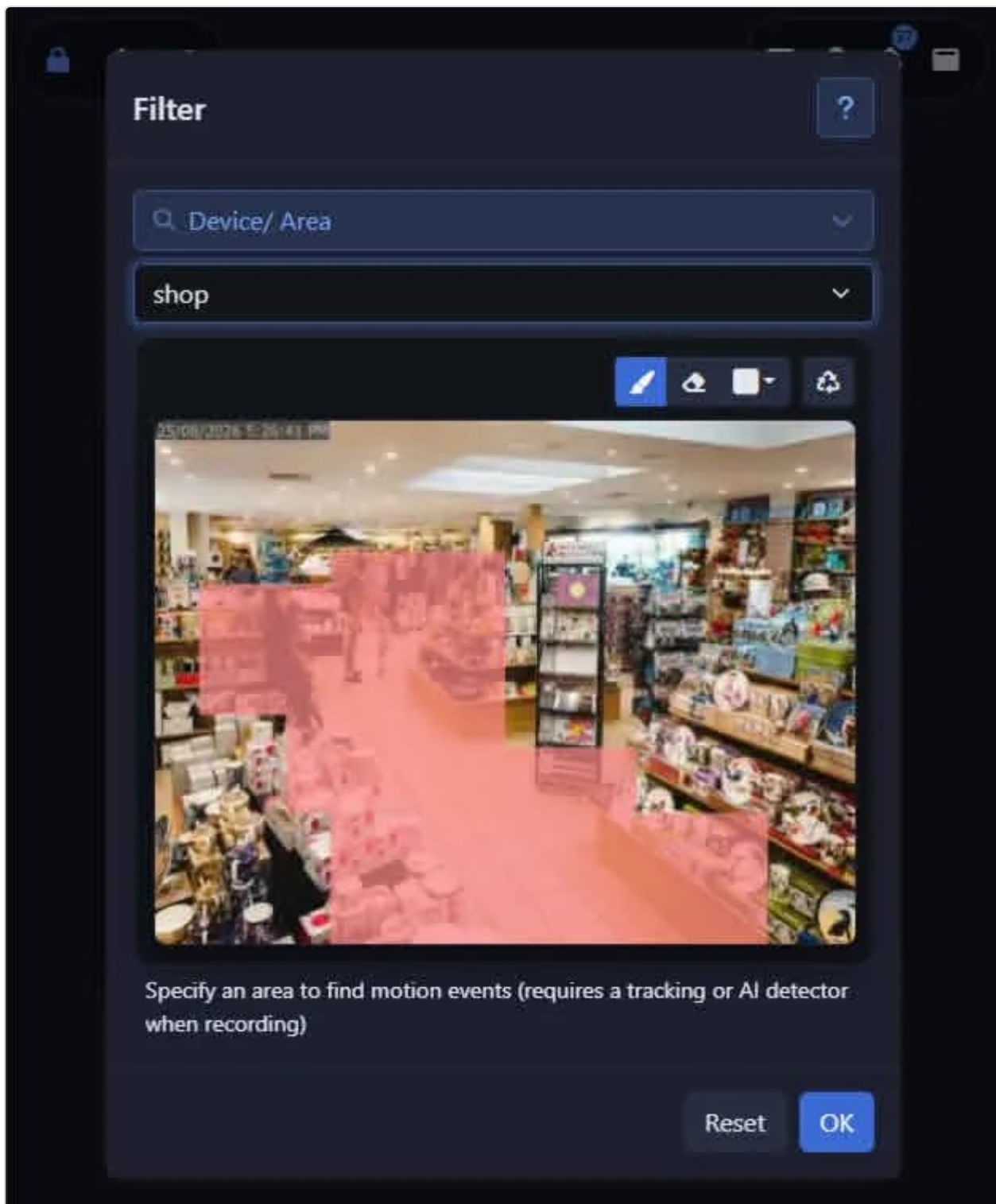
Locked: Check this to display only recordings that are locked.

Click the Remove Filter button to clear filters and display all files.

Click the Save Filter button  to save your filter settings. Access these quickly from the toolbar filter icon .

Motion Searching

To search for motion in specific areas in your recordings, click on the filter icon (magnifying glass) at the bottom right and select "Device/ Area" in the menu.



Device: Select a camera to search

Area: Using the draw tools select an area to search for motion. The selected area is highlighted.

Click OK to search through recordings for motion detected within the highlighted area.

Note: Motion searching is only available for recordings using a tracking motion detector, like object tracking, tripwires or speed - or an AI detector that returns area data (like CodeProject AI). Only applies to recordings created with v5.2.9.0+.

Tips and Tricks

To start playback at a specific time, align the timeline's left-most timestamp with the desired time. Click on a recording underneath, and playback will start and seek to that point.

Timelapse recordings are displayed alongside regular ones but occupy only half the height within the slot.

Recordings are color-coded based on peak motion levels. Bright red bars indicate high movement.

Zoom in enough, and Agent DVR will display thumbnails for recordings when space allows.

Click on a recording to enter [playback mode](#).

A marker line appears on the timeline during playback, helping you track the last viewed recording for each device.

If your screen is wide enough, Agent DVR shows live thumbnails of your devices on the left. Icons may also be displayed - see [recordings](#) for icon details.

Click on a live device thumbnail (if shown) for a mini live feed. Drag this feed around the screen as needed. Click the thumbnail again to exit the mini-player.

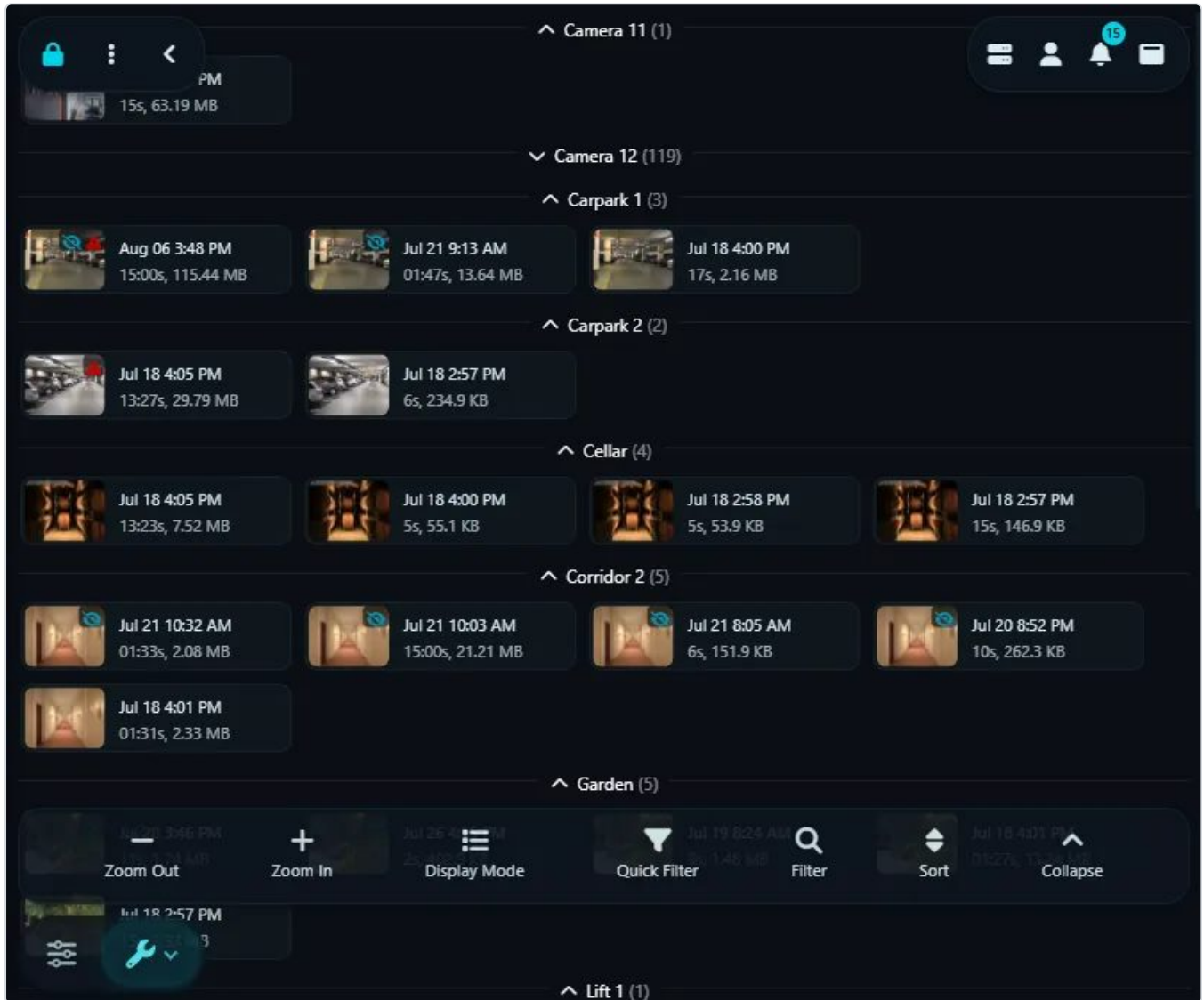
Recordings

Using Recordings

To access Recordings, click on the view menu in the top bar and select the Recordings  icon.

The Recordings view lists everything your cameras and microphones have captured, with thumbnail previews and details for each file. Camera recording can be triggered by motion detection, alerts, schedules or started manually.

Files are saved locally on your computer. To locate your recordings, refer to [Server Settings - Storage](#).



Filtering

See [Filtering](#)

Motion Searching

See [Motion Searching](#)

Tips and Tricks

Minimize and maximize each device using the icon  next to the device name.

Icons displayed next to recordings indicate:

: Unwatched recording.

: Timelapse recording.

: Recording contains an AI-generated alert event.

: Recording contains an alert event.

: File is locked and will not be deleted.

: File has been archived.

Tip: From v3.7.2.0+, edit these flags in edit mode.

For raw mode recordings, playback is possible during recording. "Recording Started" notifications can be clicked for instant playback. For encoded recordings, switch to the **VP8 codec** in server settings for similar functionality. **H264** does not support playback during recording.

Zoom in and out with   for larger thumbnails or a simplified list view.

Use the collapse/expand icon  at the bottom right to toggle all devices.

Click the search icon  to filter recordings, similar to the [Timeline filter](#).

Use the sort icon  to change the display mode (by device or date).

Click the edit icon  to enter edit mode. Select recordings individually or in bulk for various actions.

With selected recordings, use bottom left icons to delete, archive, upload, lock, download, or queue for [playback](#). Locked recordings will not be archived by storage management.

File Merge Tags

Merge tags let you build custom filename patterns - Agent DVR replaces each tag with device details or the date and time when the file is created.

Available tags for filename merging:

{ID}: The ID of the device.

{TYPE}: The type ID of the device (1 = microphone, 2 = camera).

{NAME}: The name of the device.

{0:yyyy-MM-dd_HH-mm-ss_fff}, {0:MM-dd}: Any valid date-time formatter.

Examples of date-time formatters:

{0:yyyy-MM-dd_HH-mm-ss_fff}: e.g.

2026-01-07_14-32-05_123

{0:MM-dd}: e.g.

01-07

Example filename:

{NAME}_{0:yyyy-MM-dd_HH-mm-ss}.mp4

→

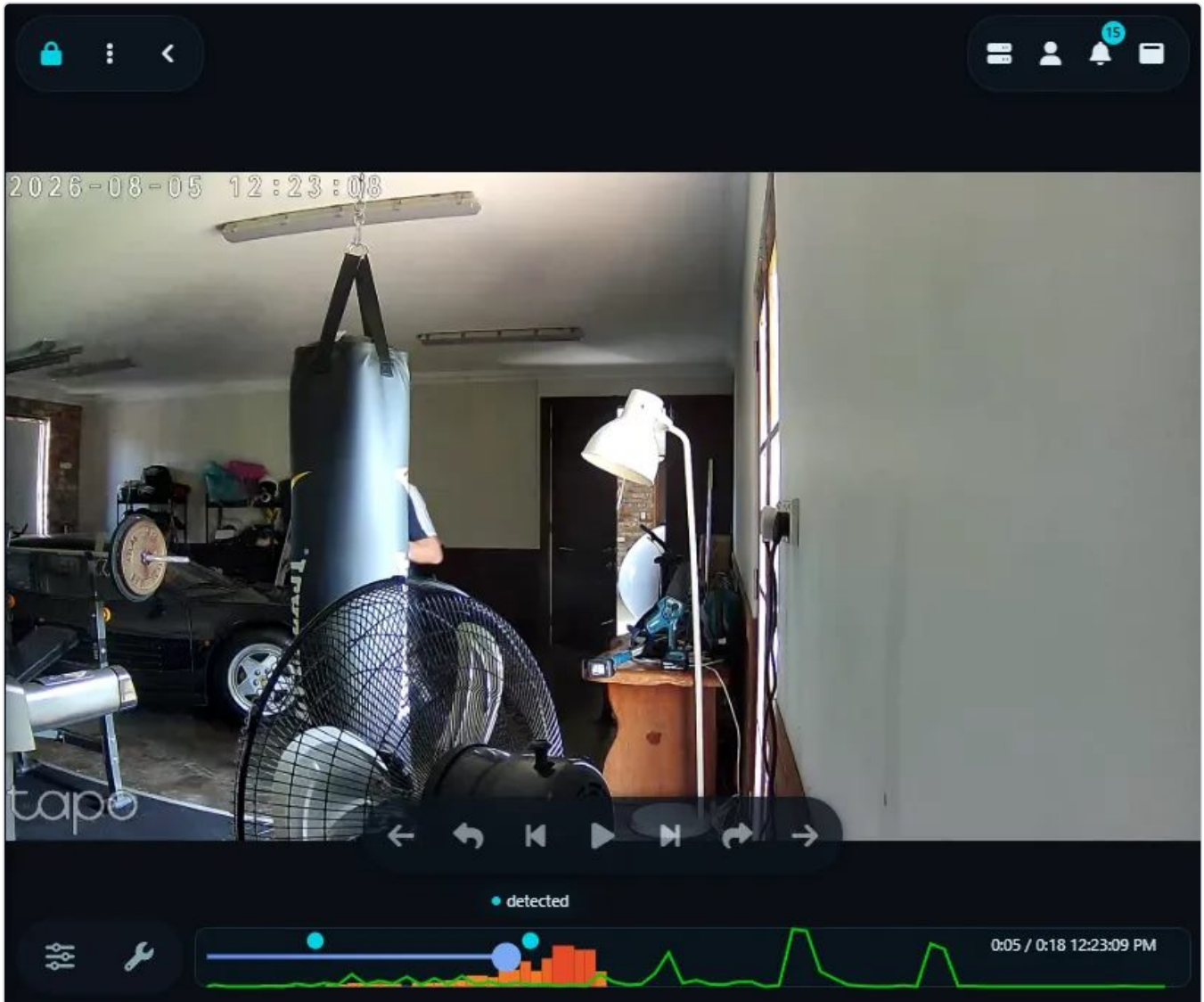
FrontDoor_2026-01-07_14-32-05.mp4

Playback

Controlling Playback

To access Playback, click on a recording in the Time Line, the Time Machine tab in the Live View, or the Recordings view, or click any notification that pops up about new recordings.

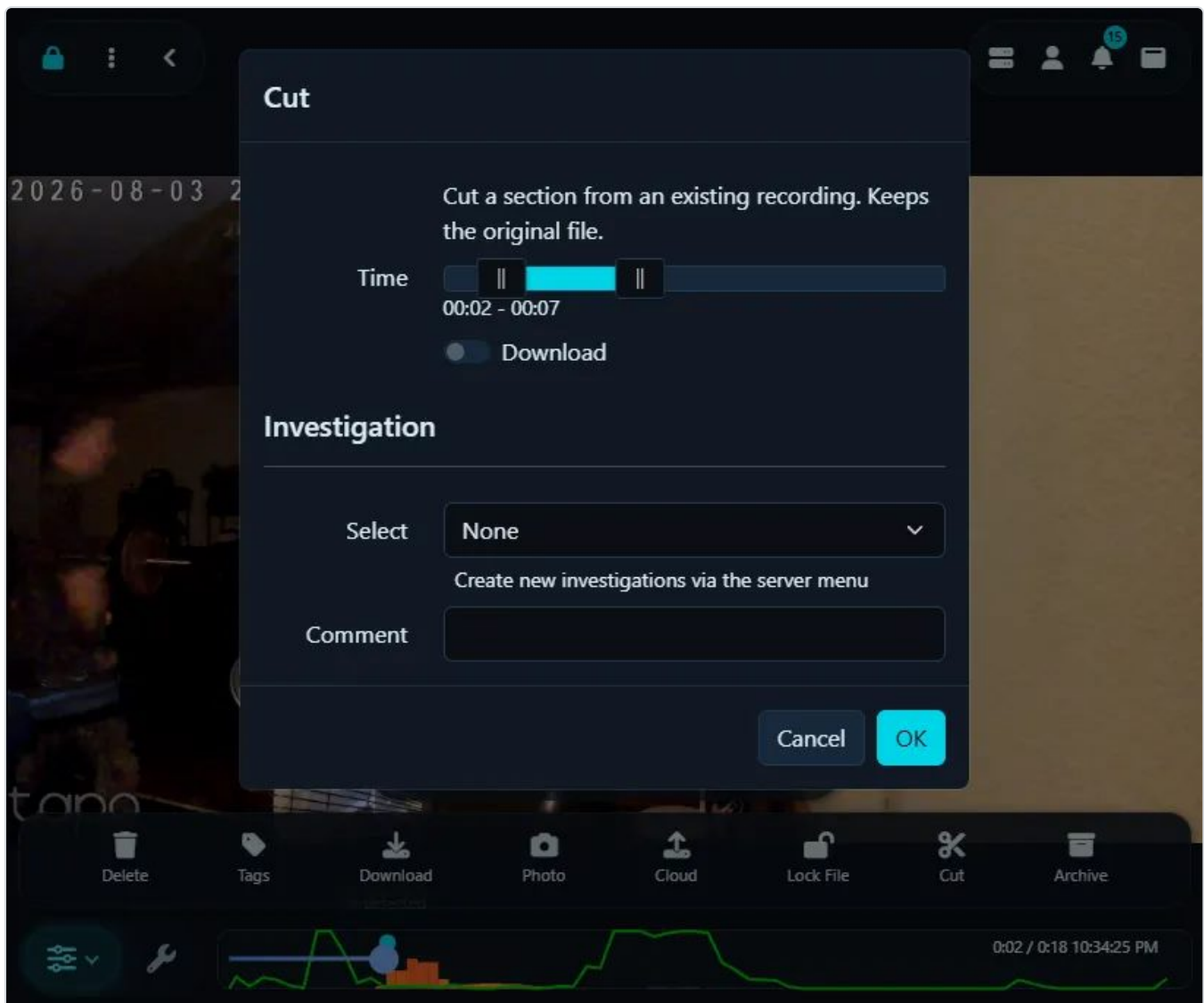
Playback in Agent DVR provides easy ways to manage your recorded content.



Start playback of recorded content from either the [timeline](#) or [recordings](#) view. You can also click on any new recording alert to begin playback immediately.

Cutting Recordings

To extract interesting parts from recordings, click on the menu icon during playback and select Cut ✂. Choose the time range you wish to keep in the current recording and click OK. Agent DVR will create the clip and replace the original file. A notification will appear in the UI when the edit is complete.



Tips and Tricks

The bottom bar displays the detected motion level throughout the recording. The bar's height indicates motion intensity, with red bars showing triggered motion detection. Dots on this bar are tags - notes added manually or by AI/events during recording. Tags display their text when the playback cursor reaches a dot. From v5.3.1.0+ there may also be a green line overlay showing the volume of audio in the recording.

Click anywhere on the bar to jump to that point in the recording. The UI shows the current position, duration, and recording time over the navigation control.

Use the mouse wheel or pinch gesture to zoom in and out of playback. When zoomed in, click and drag to navigate the zoomed area.

Click the photo icon  to snapshot that moment in the recording.

On mobile devices, swipe left or right to cycle through recordings.

Access additional features via the bottom right menu. Adjust playback speed, download the recording, navigate between files, manually tag the recording for easy filtering, or play all selected recordings automatically.

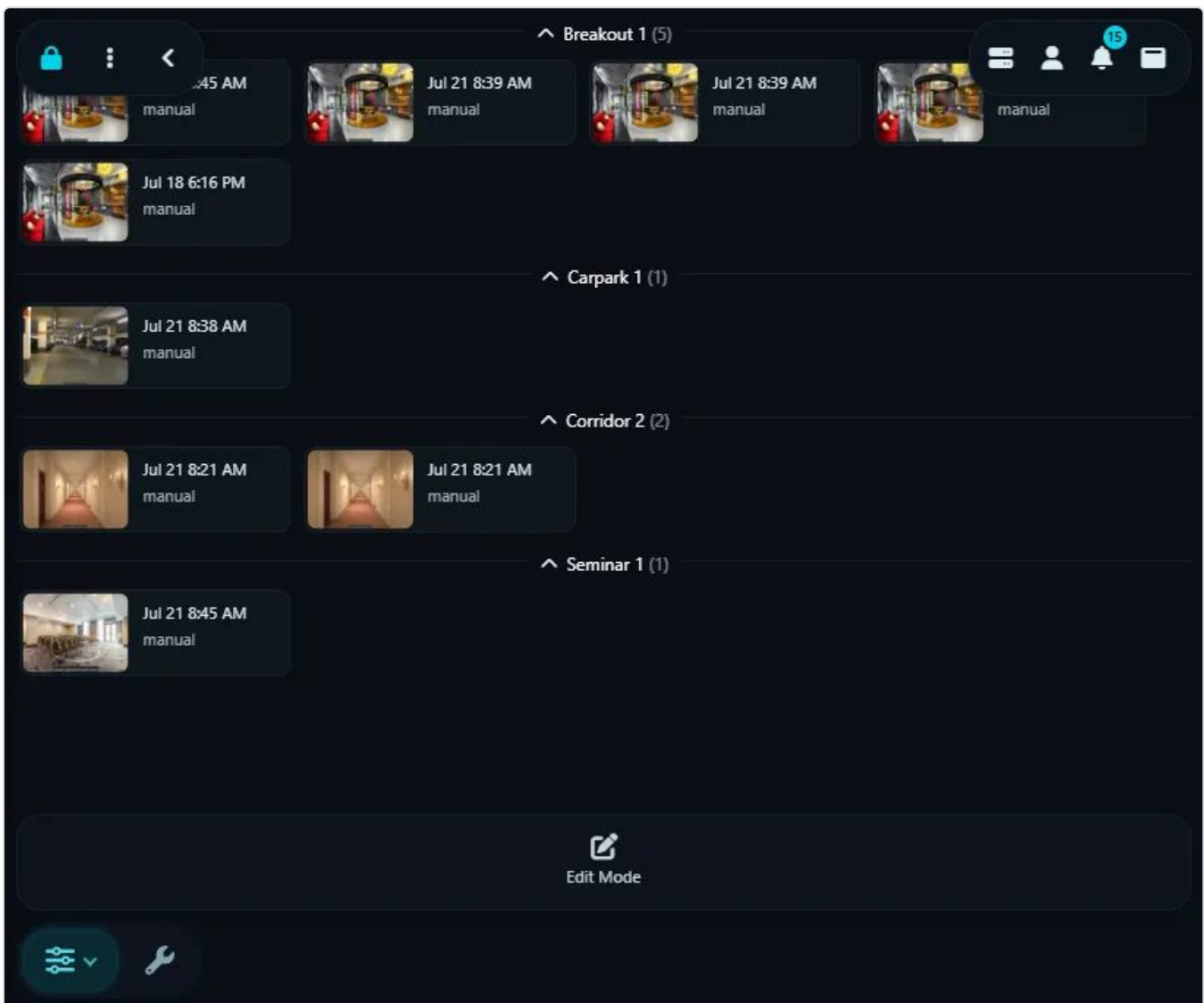
Photos

Accessing Photos

To access Photos, click on the view menu in the top bar and select the Photos  icon.

Photos provides details and thumbnail previews of all photos recorded by Agent.

Files are saved locally on your computer. To locate your photos, see [Server Settings - Storage](#). Photos are typically stored in the "grabs" subdirectory within the recordings folder. They can be saved manually, automatically (via interval, motion, or alert triggers), or as a result of AI processing (such as object recognition, alert filters, LPR, facial recognition, etc.).



Filtering

To manually filter photos, click on the filter icon (magnifying glass) at the bottom right.

From/ To: Select a date range for your search.

Locations: Filter by locations. Add locations in the camera settings under the General tab.

Groups: Filter by device group.

Objects: Click the Person, Vehicle, Animal, Package or Face buttons to show only photos where [Object Recognition](#) detected that type of object.

Tags: Enter tags for filtering.

Click the Remove Filter button  to clear filters and display all files.

Click the Save Filter button  to save your filter settings. Access these quickly from the toolbar filter icon .

Tips and Tricks

Minimize and maximize each device using the icon  next to the device name.

Zoom in and out with   for larger thumbnails or a simplified list view of photos.

Click the collapse/expand icon  at the bottom right to toggle all devices.

Click the search icon  to filter photos, similar to the [Timeline filter](#).

Use the sort icon  to change the display mode (by device or date).

Click the edit icon  to enter edit mode. Select photos individually or in bulk for various actions.

With selected photos, use bottom icons to delete, archive, upload, download, or browse through them.

Click on a photo for a full-size display. Use the bottom right controls to download or tag the photo for easy searching.

New in 3.9.7.0+ Zoom in and pan around the image using mouse or touch gestures.

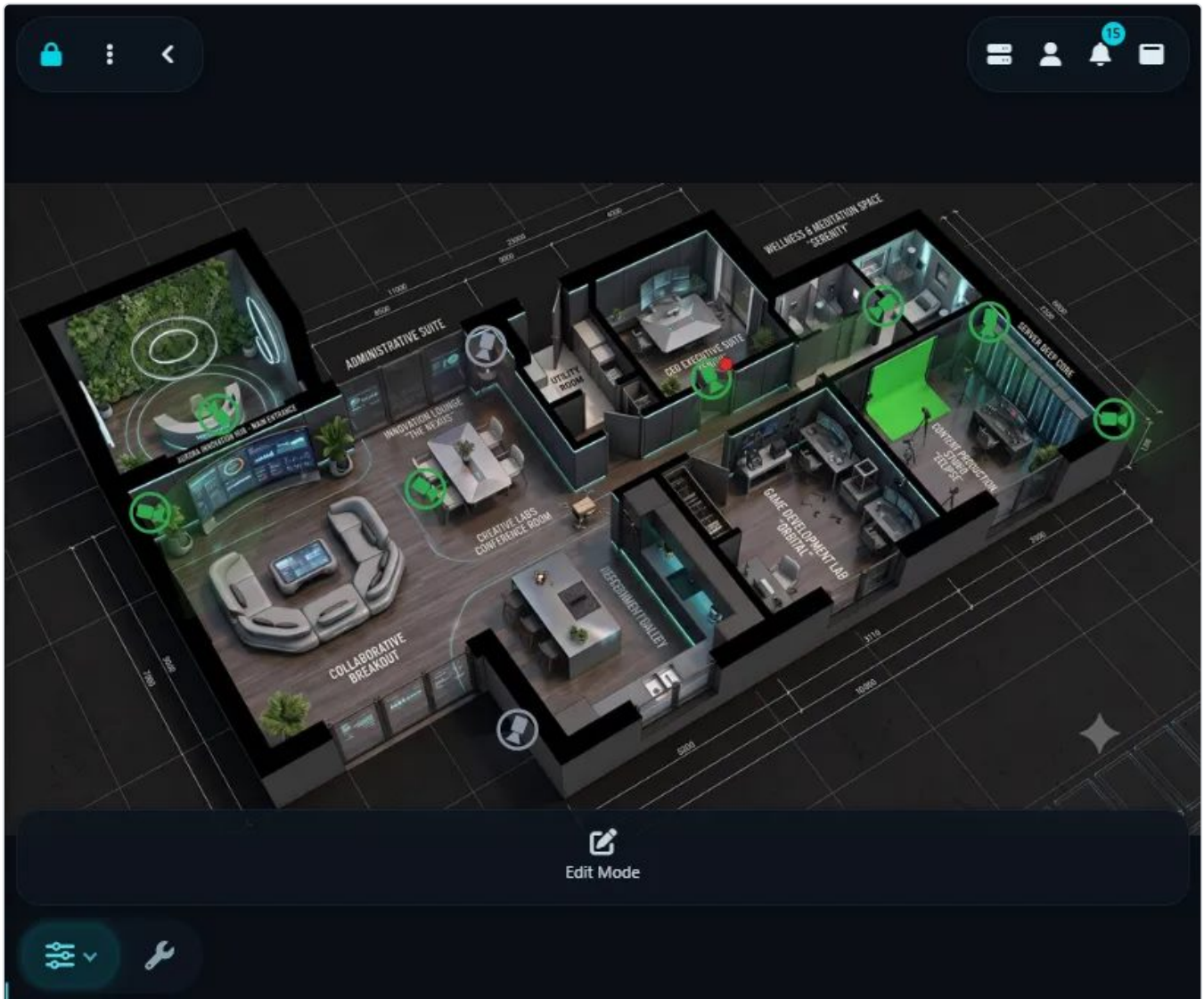
On mobile, with a photo displayed, swipe left or right to cycle through photos.

Floor Plans

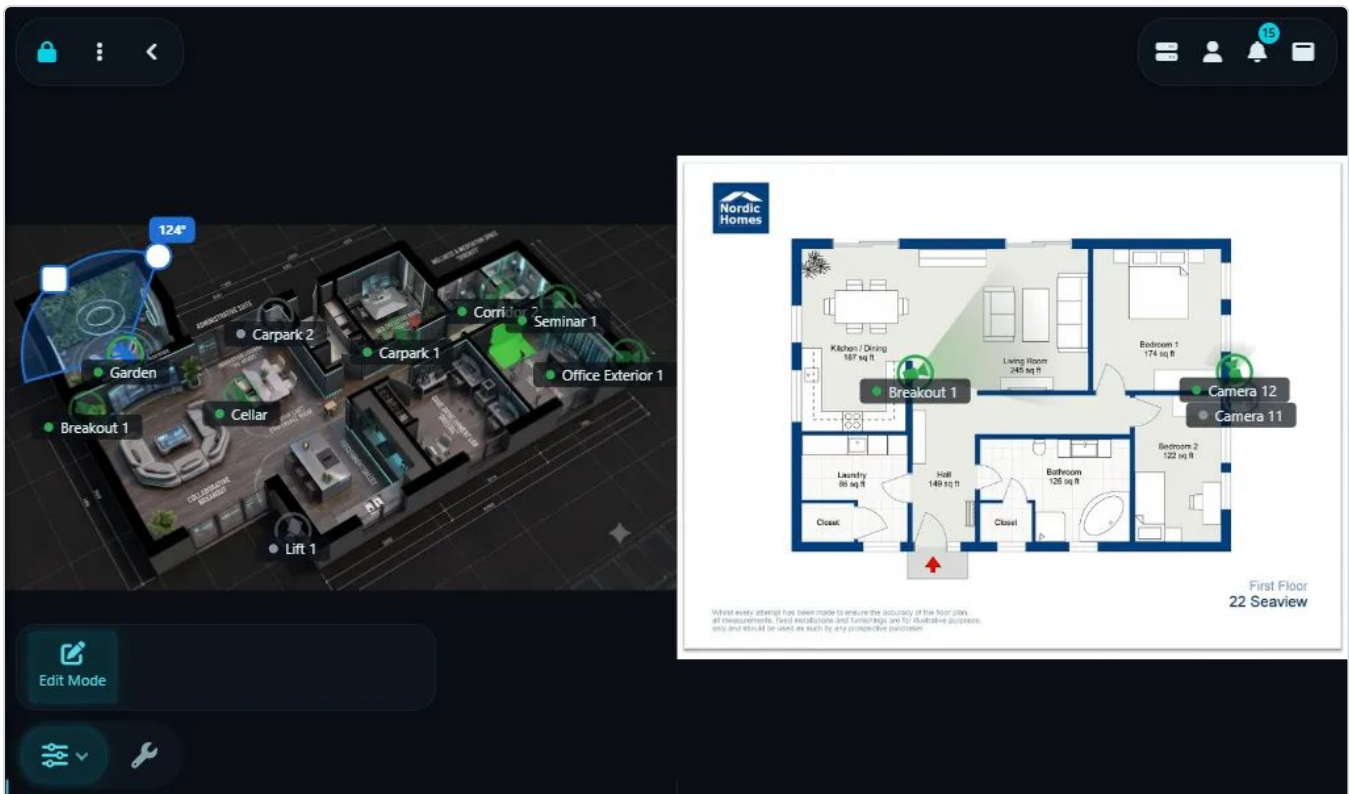
Setting up Floor Plans

To access Floor Plans, click on the view menu in the top bar and select the Floor Plans  icon.

Floorplans allow you to visualize the placement of your devices around your property, enabling quick switching to live views from those devices and real-time monitoring of alert states. Access floorplans via the view selector at the top left of the screen.



To start with floorplans, click the edit icon at the bottom right. Name your plan and upload an image of your floorplan. Agent DVR will resize it to fit the area. Then select the devices you want to include on the floorplan and click OK. Agent DVR will place the devices at random locations. You can enter or exit edit mode by clicking the edit icon at the bottom left:



To position devices on the floorplan, first make sure a camera isn't selected by clicking on the background, then toggle the edit icon at bottom left to display the edit controls. You can then click and drag their icons (camera or microphone) to the desired location. Use the square grip to rotate a device and the circular grip to adjust its field of view. Once you're done editing, click the edit button again to exit edit mode. You can customize the device icons in Agent DVR by editing the device and setting the Icon field on the General tab.

Using Floor Plans

Agent DVR provides 9 available slots for floorplans (editable in Server Settings under User Interface, Plans field). Agent DVR arranges all floorplans with associated devices in a grid layout. Click on a floorplan to select it, and click again to maximize or minimize it. To edit a floorplan, click the Views icon  at the bottom right and choose a plan from the list.

Tips and Tricks

To remove a floorplan, edit it and deselect all devices.

When a device alerts, its detection area will flash red.

If a device is recording, a recording marker will appear next to it.

An offline device's detection area will be dark gray; online, it will be green.

Click a device (outside edit mode) to open a mini live feed (video and audio). Drag the feed to reposition it. Click the device again to close the mini player. The selected device will animate to indicate active viewing.

With a device selected, the bottom left controls change to allow various operations like powering on/off, editing, starting recording, etc.

Use the expand icon in the mini live player for full-size video. Click again to exit full-screen mode.

Agent DVR automatically saves your changes.

You can upload any size image for floorplans. Agent DVR rescales the UI to accommodate it on different devices.

Virtual Reality

About VR Mode

To access Virtual Reality, click on the view menu in the top bar and select the Virtual Reality  icon.



VR mode in Agent DVR uses the cameras from your configured views in live mode to arrange cameras in a Virtual Reality or 3D environment. To see cameras in VR, you need to configure at least one view in the live viewer. The VR viewer uses the same views as the live viewer.

Using Virtual Reality

If you have a compatible VR device, the UI offers an immersive VR mode.

To select a camera, point at it with your controller and press the trigger. Press again on the same camera to toggle between maximised and normal view.

To teleport, point at the floor and press the trigger to move to that position.

If you have a game pad you can use the **left stick** to move around the room and the **right stick** to look around. Use the **D-Pad** to pan and tilt a PTZ camera and the triggers to zoom in and out.

To exit VR, walk through the doorway on the left wall or press Escape.

Using Mouse and Keyboard

Click the VR canvas to capture the mouse - you can then look around by moving it. Press **Escape** to release the mouse without exiting VR.

Use the **Arrow Keys** to move around the room. Diagonal movement is supported by holding two arrow keys together. A blue dot appears when your cursor is over something interactive. **Left click** or press **Space** to interact. Mouse wheel will zoom in and out the selected camera.

To exit VR, walk through the doorway on the left wall, or press **Escape** while the mouse is not captured.

Additional keyboard shortcuts (you can configure these via the key manager in account menu):

Key	Action
Space	Select / interact (same as left click)
Enter	Show / hide the control panel
Escape	Release mouse lock / exit VR
O	Toggle power on selected device
R	Toggle recording on selected device
G	Take a photo on selected device
T	Trigger a manual alert on selected device

Using the Control Panel

Once you have a camera selected (by clicking on it) you will see a glowing border around it and you can interact with it via the control panel.

Use the main control desk to interact with the selected device. There are buttons on the desk to switch power, take photos, start and stop recording or trigger manual alerts.

Use the two main left and right arrow controls to cycle through configured views. Views appear only if they have devices set.

Use the two toggle buttons on the right to pop up configured floor plans as separate monitors and an overlay PTZ controller.

A red marker in the top right corner signifies recording, and a red border indicates an alert.

Press **Enter** to show or hide the control panel at any time.

Notes

VR mode requires an SSL connection if you are not running on localhost or via the web portal.

Immersive VR requires a browser with WebXR support. Current versions of Chrome and Firefox support WebXR without any additional configuration. Ensure SteamVR is running before launching if you are using a PC-tethered headset.

Mobile support requires Android O+ and varies on iOS depending on specific OS/hardware versions.

VR mode has been tested on the Vive and Google Cardboard. If you've successfully used it on other devices, please [let us know](#).

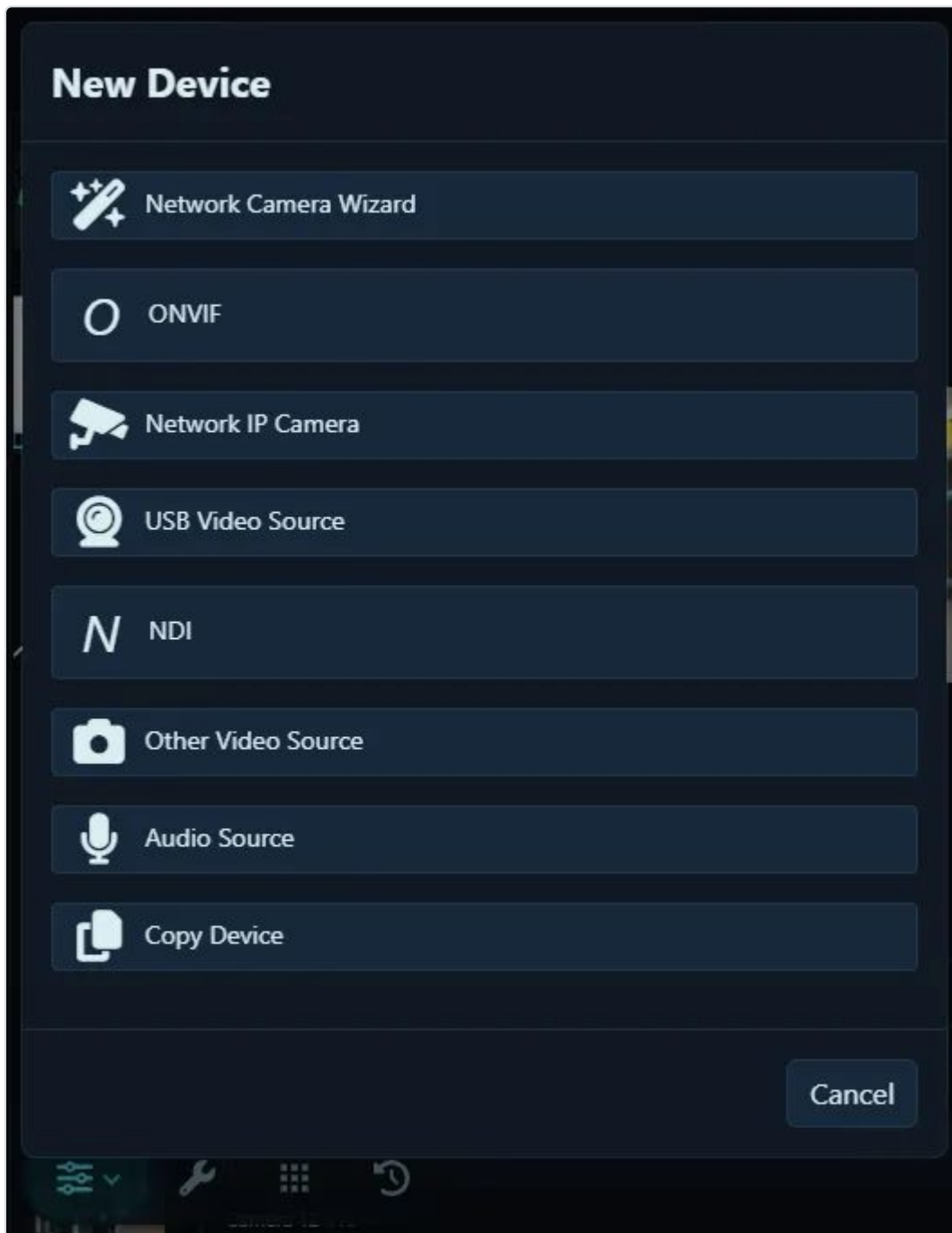
Configuration

Adding Cameras

About

Agent DVR works with a wide range of video sources, from ONVIF and RTSP IP cameras to USB webcams and multi-channel DVR systems.

Click on the Server icon  at the top right of the Agent DVR UI and select "New Device" under **Devices**. Alternatively, in the [Live View](#), click on the Edit icon  at the bottom right and choose "New Device".

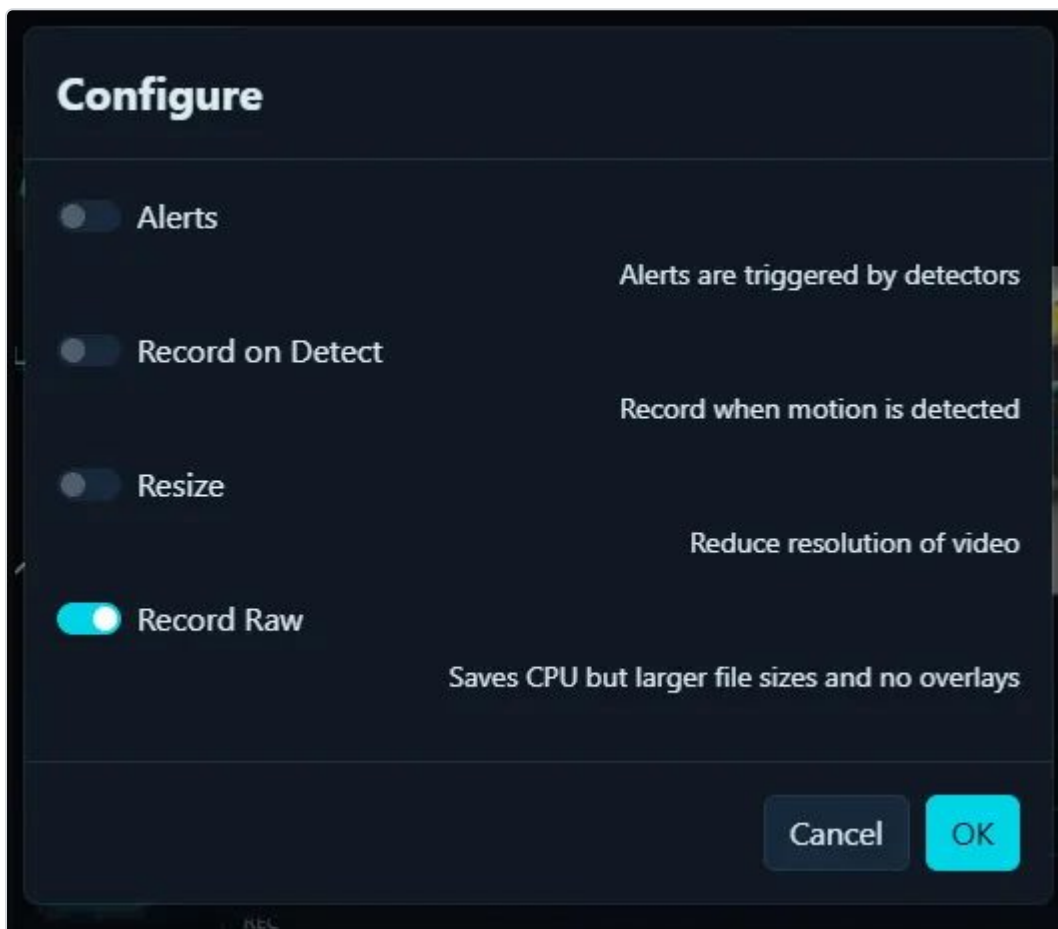


Choose from the available options. To use the wizard, which helps you discover devices on the local network and connects to your camera using the Agent DVR camera database, click on "Network Camera Wizard". For ONVIF compatible cameras, select "ONVIF". If you already have an RTSP, MJPEG, or another URL for your

camera, choose "Network IP Camera" (or "Other Video Source" for other source types). For adding an audio source like a local USB microphone or other network audio sources, click on "Audio Source".

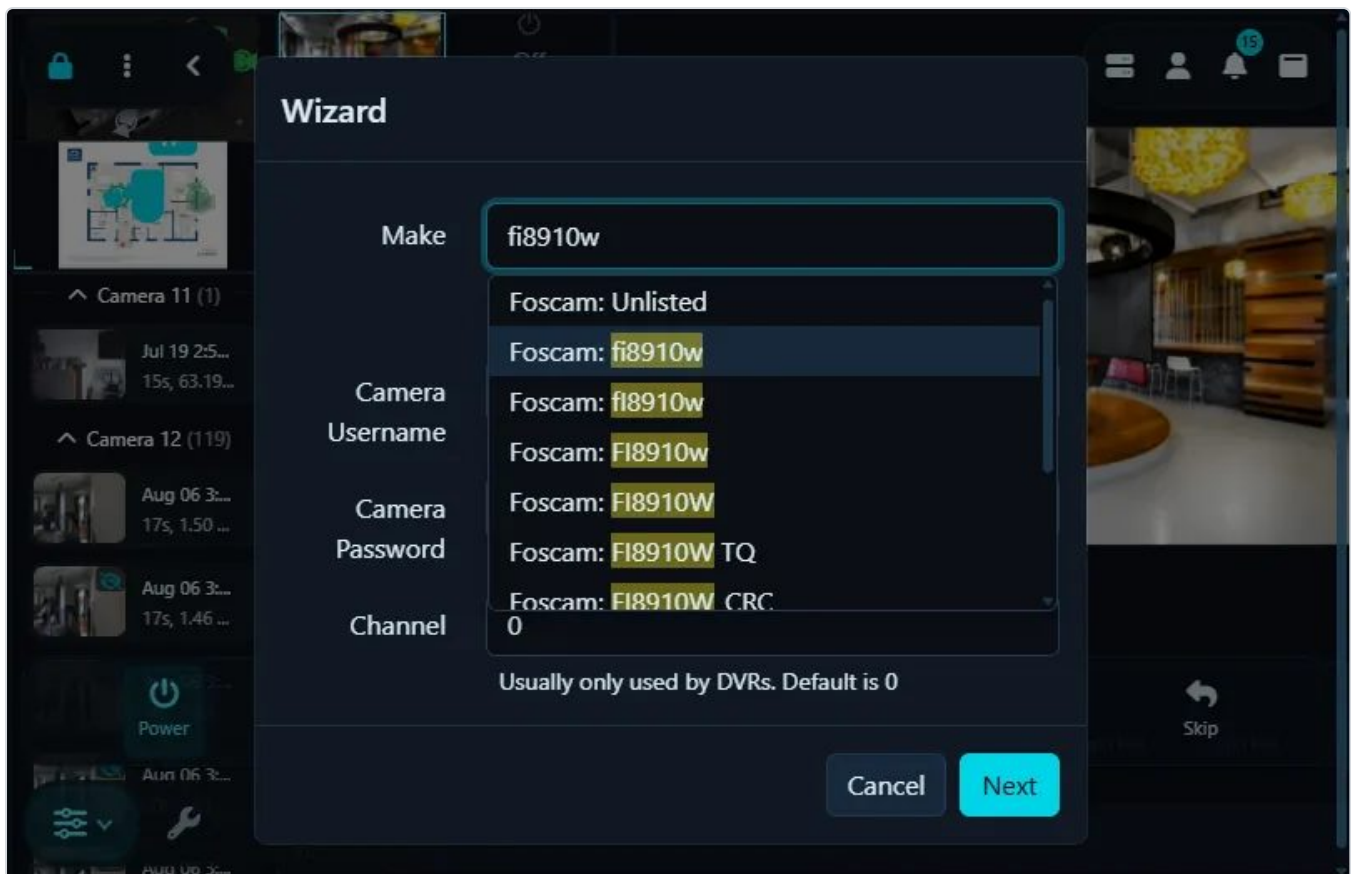
Configuration

The second step in adding a new device involves setting up some basic features. If you enable "Alerts," Agent DVR will configure your camera with a simple motion detector to raise alert events. To record upon motion detection, select the "Record on Detect" option. For high-resolution cameras, the "Resize" option can reduce the resolution, saving CPU usage. "Record Raw" means Agent DVR will record the stream directly from the camera to disk without encoding, significantly reducing resource usage. Note that Raw Record is only available for network video sources (not USB cameras or local devices like desktop streams). You can edit all these options later.



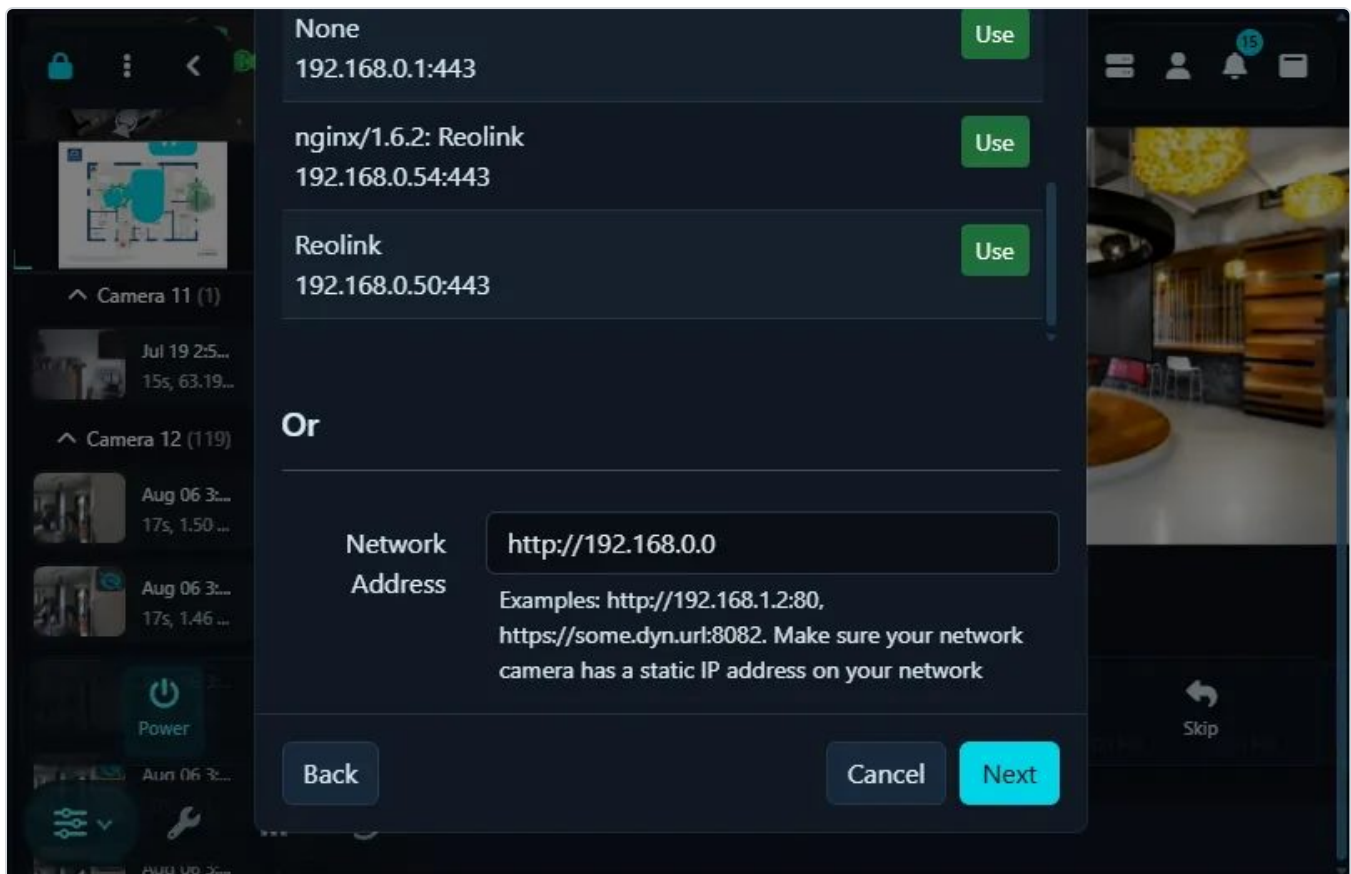
Using the Wizard

Start by typing the name of your camera manufacturer in Agent DVR. The system will suggest options. **Click on a suggestion to select it.** If your manufacturer isn't listed, choose "Unlisted," or select "<Manufacturer>: Unlisted" for unknown models. This information helps Agent DVR narrow down potential video connection addresses.



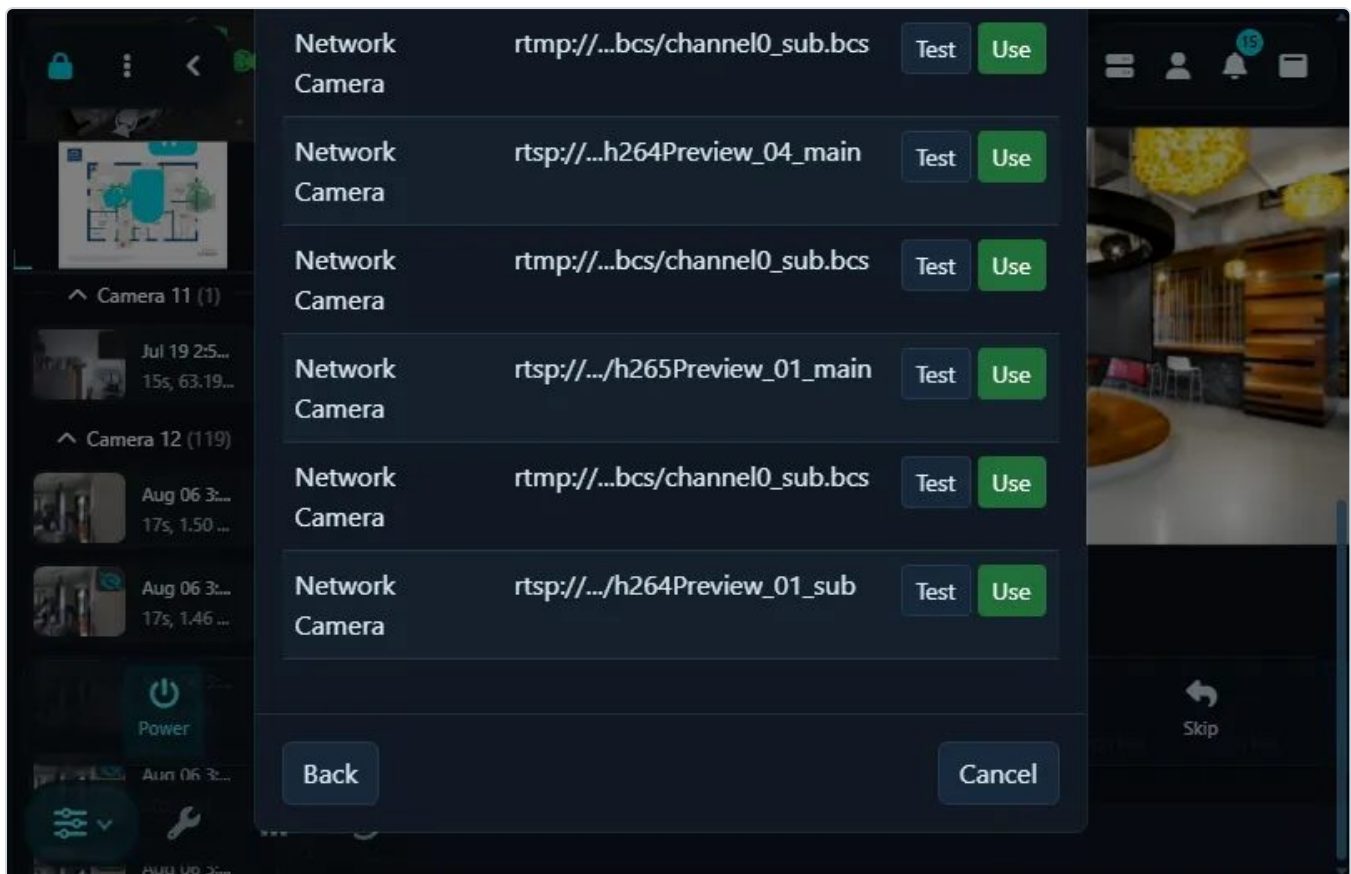
Enter your camera's username and password (these are the credentials used to access your camera's web or app interface, **not** your iSpyConnect.com login).

Enter the Channel number (usually '0' for IP cameras, but may differ for DVR systems with multiple cameras).



Next, identify or enter your camera's Network Address. Agent DVR can automatically discover local devices. After the network scan, click on a device name to try accessing it in a web browser, and if it's your IP camera, click "Use" next to it. You can also manually enter the network address in the format of `http://IP-ADDRESS:PORT` or `https://WEB-ADDRESS:PORT`. Use the  icon to rescan your network.

Tip: Set your IP cameras with static IP addresses on your network to maintain consistent connectivity. Here's a helpful guide: [Setting Static IP Addresses](#).



After selecting an address, Agent DVR will scan for video endpoints. Choose one from the list by clicking "Use."

Tip: Prefer IP Camera options over MJPEG or JPEG for better audio and frame rates.

If no endpoints are found, verify your details or contact the manufacturer for direct camera stream access. Alternatively, add the device using "Video Source" for manual configuration or as an ONVIF device.

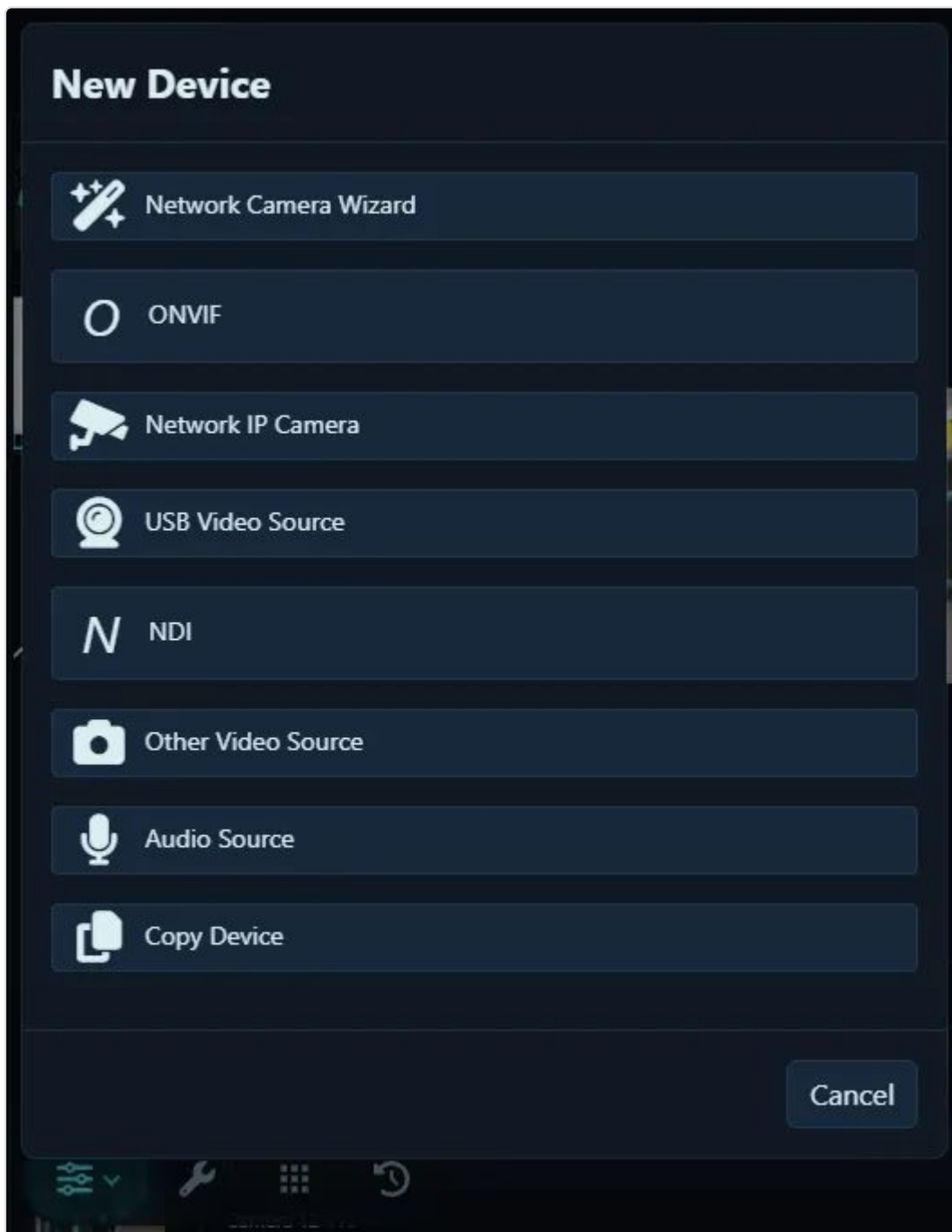
Adding Microphones

About

Click on the Server icon  at the top right of the Agent DVR UI and select "New Device" under **Devices**. Alternatively, in the [Live View](#), click the Edit icon  at the bottom right and choose "New Device".

You can add Microphones as standalone devices that record audio to files, or pair them with cameras to include sound in camera recordings. For pairing a microphone with a camera, see [Editing Cameras](#).

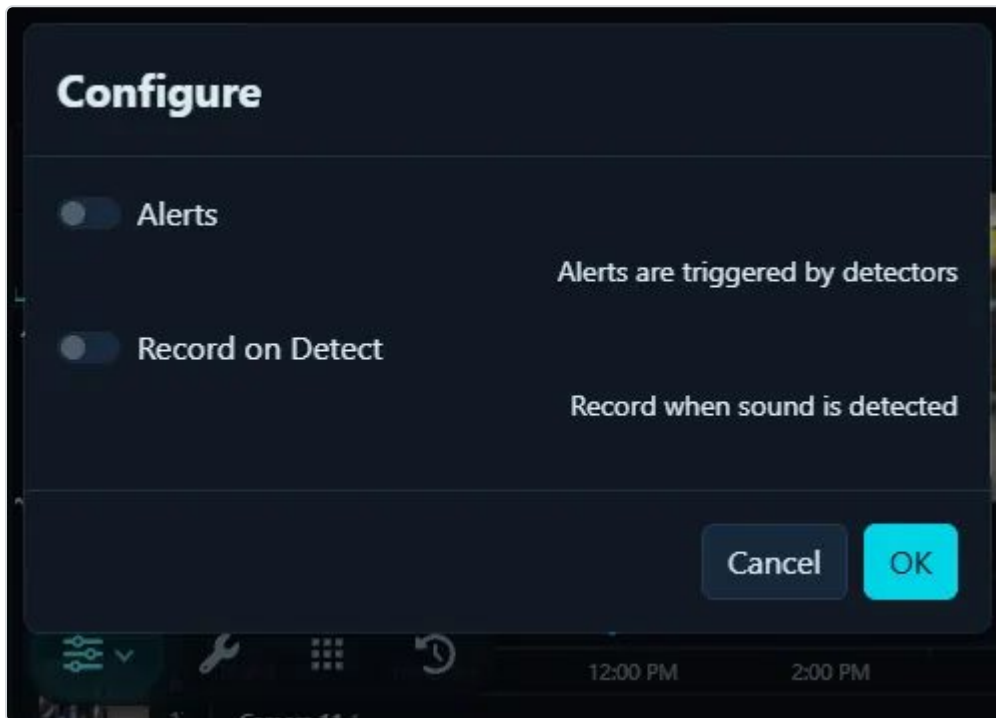
Tip: If you add an IP camera with an audio track in its stream, Agent DVR will automatically add and configure a paired Microphone control.



Click on "Audio Source" to add a new microphone.

Configuration

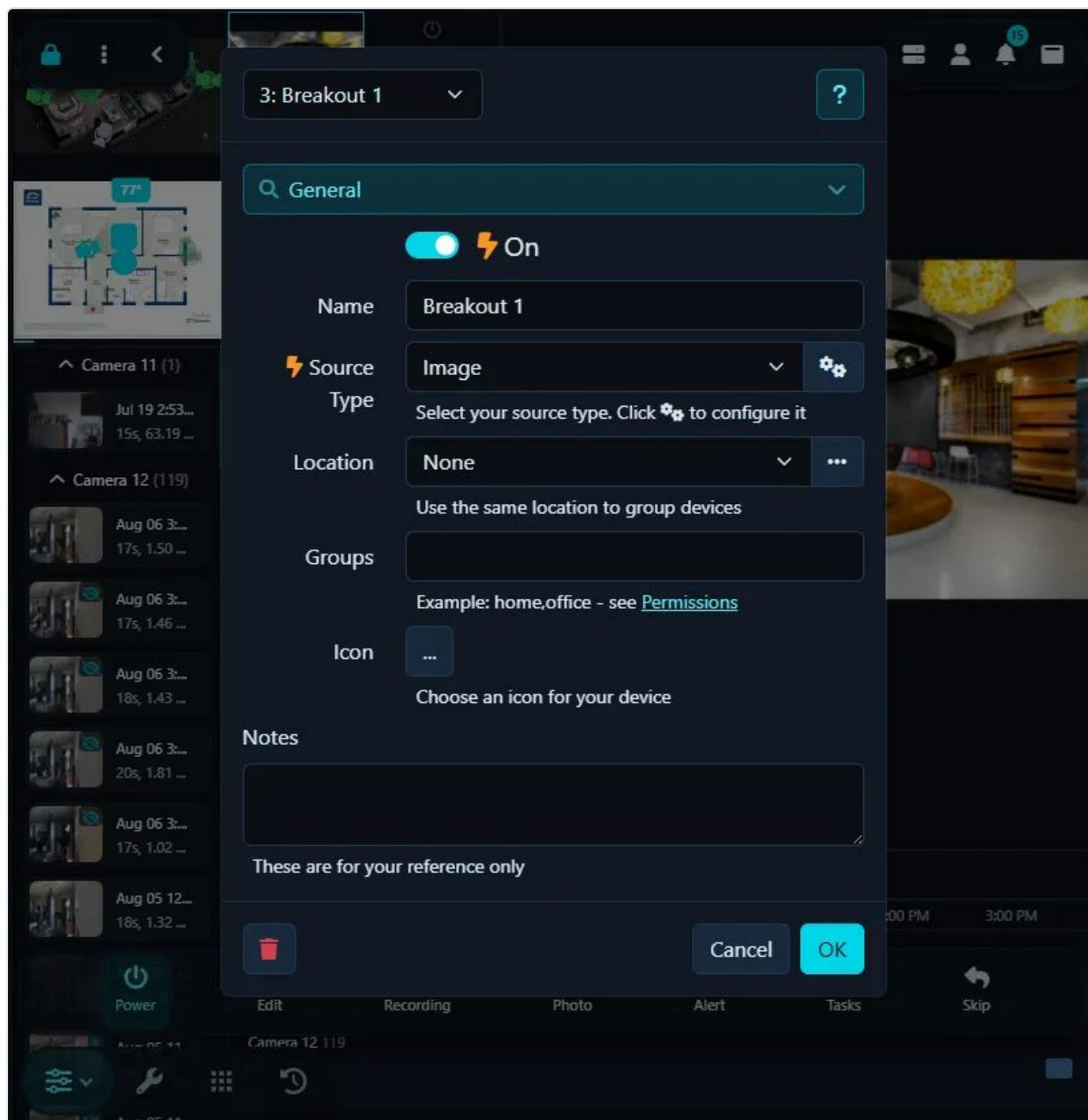
The second step in adding a new audio device is to set up some basic features. By enabling "Alerts," Agent DVR will configure your microphone with a sound detector, preparing it to raise Alert events. To record audio when Agent DVR detects sound, select the "Record on Detect" option. You can modify these options later as needed.



Editing Cameras

About

Click on the Server icon  at the top right of the Agent DVR UI and select "Edit Devices" under **Devices**. Choose the device you wish to edit and click the Edit icon . Alternatively, in the [Live View](#), click a camera to select it and then click the edit icon on the bottom toolbar (or press the shortcut key "E"). On Desktop, you can right-click the camera in the Live View or anywhere in Agent DVR where there is a live thumbnail, like the timeline.



This is the main interface for configuring your devices. Displayed at the top are your object ID (in this case, 7), the device name (Back Yard), and on the right, the main device menu which grants access to all

configurable areas, referred to as tabs. The lightning bolt icon ⚡ next to a setting indicates that changes apply immediately, without needing to click OK.

General

This tab provides access to general and frequently used settings.

Name: Give your camera a descriptive name, like "Office" or "Back Yard".

Enabled: Controls whether the camera is active in Agent. Note: This does not power down your device unless it's a USB camera.

Decoder: Moved to [Advanced Video Source Settings](#).

Source Type: Choose how Agent DVR connects to your devices. [See Video Source Types](#). Click the button to the right of the drop-down to configure it.

Location: Manage locations with a button click. Add locations like "Main House" and assign a color and GPS location to them. When devices are assigned to locations, they will be color-coded in the live view.

Groups: Used in [Remote Permissions](#) and [Local Users](#).

Icon: Choose an icon for your device (used on the floorplans).

Notes: Add your own notes about this device. These are for your reference only.

Adjustments

This tab provides access to various adjustments for the live feed.

Max Framerate: Use this to make Agent DVR ignore frames, reducing CPU usage.

Resize: Check this to have Agent DVR resize frames. Set the size with Resize Width and Resize Height in the Advanced section below.

Image Correction: Click the button to set the mode, focal length, limit, and scale for converting fisheye and 360 cameras into regular rectangular views. Use the virtual cameras option to create multiple virtual cameras from fisheye video feeds. Virtual cameras support independent digital PTZ.

Flip: Vertically or horizontally mirror the live video, useful if your camera is mounted upside down.

Rotate: Rotates the video through 90 or 270 degrees, useful for sideways-mounted cameras.

Overlay Image: Provide a transparent .png file via  - **Upload**, and Agent DVR will overlay it on your camera stream.

Resize Width and Resize Height: Set the resize dimensions (enter 0 for automatic). To apply, disable and re-enable the camera.

Fill Mode: Controls how the camera renders in live view - **Use Default:** use the setting in Server Settings - Playback - Fill mode (Center Images on older versions). **Center:** maintain aspect ratio. **Fill:** fill the available space.

Event Buffer: Specify time to buffer the live stream for events like push and email video. Agent DVR will buffer only if these features are in use.

Actions

Tell Agent DVR what to do when various events occur, such as Alerts, devices being turned off, recordings finishing, etc. [See Actions](#) for more details.

Alerts

Alerts are generated by AI, motion detection and plugins. For more information, [see Alerts](#).

Audio

Configure an audio device to pair with your camera (this is automatically configured if your camera has an audio stream). You can also configure an overlay audio display here.

Tip: Click to configure the microphone and you can change the colors of the audio display.

Microphone: Click the button to associate a microphone with the camera. Once associated, the mic will provide audio for recordings and be enabled/disabled with the camera. Agent DVR will automatically add and pair a microphone control if your Camera has audio in its stream; otherwise, you will need to [add a microphone](#) to Agent DVR first via  - **Add Device**.

Ignore Audio: If your camera has its own audio stream (common in many IP cameras) and you don't want Agent DVR to use it, check this option. Enable and disable the camera to apply this change.

Configure: Click to configure the associated microphone.

Location: Select a location in the frame to draw the audio overlay.

Display Style: Select a display style for the visual representation of the audio on the camera live stream.

Show Background: Show a background color behind the audio.

Width: Specify the width of the audio control.

Height: Specify the height of the audio control.

Cloud

Automatically upload this camera's recordings and photos to cloud storage such as Google Drive, Dropbox, OneDrive or S3 for off-site backup.

Provider: Choose which cloud provider to upload to - see  - **Settings - Cloud** to configure cloud providers.

Upload Recordings: Check this to automatically upload recordings.

Upload Photos: Check this to automatically upload photos.

Folder: The remote folder to upload into.

Path: This is the path that Agent DVR will upload to. You can use {MEDIATYPE}, {DATE}, {NAME} and {DIR} here. For example, {MEDIATYPE}/{NAME}/ will upload video to Video/somefilename.mp4.

Filename: Optional filename templates for uploaded recordings and photos. Use a date template like {0:yyyy-MM-dd_HH-mm-ss_fff} or {C} for a counter value.

Counter Max: The maximum value for {C} - once this is reached, it resets to 0.

If you have issues with cloud uploads, please check the logs on the local UI at /logs.html.

Detector

For detailed information on motion detection, [see Motion Detection](#).

FTP

FTP recordings or photos to your FTP servers. You can also set up basic live streaming using FTP and a bit of JavaScript. See [Server FTP Settings](#).

Photos

Enabled: Switch on or off Photo upload.

Server: You will need to add your FTP server into  - **Settings - FTP** and then select it in this list.

Mode: Choose between Detected, Alert, Interval, or None. Detected and Alert only send images when something is happening. Interval will constantly send images to your server. Use None if you want to only trigger FTP images via the [API](#).

Interval: The minimum time between frames when mode is set to Interval.

Delay: The minimum time between frames when mode is set to Detected or Alert.

Use Photo URL: Upload the image from the JPEG URL (see the [Photos](#) tab) instead of the decoded live stream.

Quality: This sets the quality of the jpeg image. Lower quality has a smaller file size.

Overlay Text: Optionally add some text to the image.

Filename: The filename that gets saved to the server, for example, {C}.webp or myfiles/{C}/frame.webp. You can use a template date format here or the special {C} which substitutes in a counter value. For example, if Counter Max is 20, you will get 0.webp, 1.webp, 2.webp ... 20.webp, and then 0.webp uploaded. You can also use {NAME} to merge in the device name (v4.4.7.0+).

Counter Max: The maximum value for {C} - once this is reached, it resets to 0.

Invert Counter: {C} stays at 0 (so the newest image is always 0) - existing files get progressively renamed up to Counter Max. Note that if your filename includes a date-time formatter, this may not work

correctly.

Video

Enabled: Switch on or off Video upload.

Server: You will need to add your FTP server into  - **Settings - FTP** and then select it in this list.

Filename: The filename that gets uploaded to the server **excluding the file type extension (e.g., .mp4)**, for example, {C}. You can use a fixed filename like "myvideo", a template date format, or the special {C} which substitutes in a counter value. For example, if Counter Max is 20, you will get 0.mp4, 1.mp4, 2.mp4 ... 20.mp4, and then 0.mp4 uploaded. Agent DVR will append the file extension as it can vary depending on what format it is recording to.

Counter Max: The maximum value for {C} - once this is reached, it resets to 0.

FTP Image Streaming

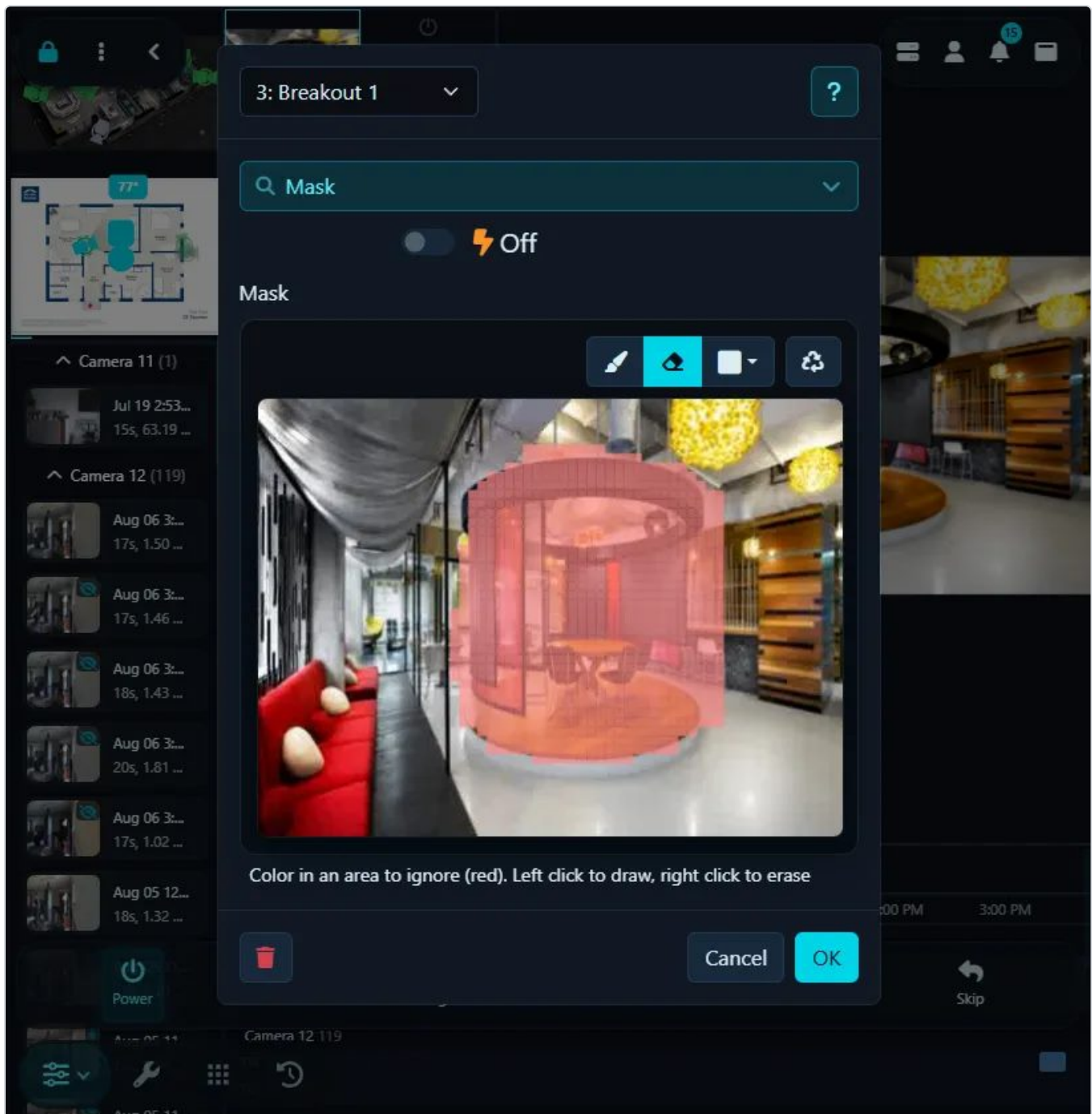
If you want to display the images you are uploading on a website, you can use this script (you'll need to modify the _targetimage variable to point to the image you are uploading). This will only work if you have specified a fixed filename to your uploaded image, like "myimage.webp" (i.e., it continually overwrites the same file).

```
<img src="" id="agentfeed" style="width:320px;height:240px" alt=" Agent DVR Feed" title=" Agent
DVR feed"/>
<a href="https://www.ispyconnect.com/download" target="_blank">Agent DVR - free surveillance
software</a>
<script type="text/javascript">
var oImage;
var _targetimage = "myimage.webp";
function getcamerafeed() {
oImage = new Image;
oImage.onload = getnextframe;
var _src = _targetimage + "?r=" + Math.random();
oImage.src = _src;
}
function getnextframe() {
document.getElementById("agentfeed").src = oImage.src;
oImage = new Image;
oImage.onload = getnextframe;

var delay = 2000;
window.setTimeout("loadframe()", delay);

}
function loadframe() {
var _src = _targetimage + "?r=" + Math.random();
oImage.src = _src;
}
window.onload = getcamerafeed();
</script>
```

Mask



A privacy mask is a straightforward way to conceal areas in your video that you prefer to keep private, such as a neighbor's window or garden. Activate the 'Enabled' switch and use the provided tools above the preview video to create blackout areas. Keep in mind, you'll need to encode your recordings (see our [Recording section](#)) to ensure the mask is applied to your recorded videos.

MQTT

Use actions to send messages via MQTT, or enable the option in this tab to automatically forward all events to your MQTT server.

MQTT Events: Toggle this on to have Agent DVR automatically send event packets for this device to your MQTT server. You will need an [MQTT server configured](#). With [Home Assistant Discovery](#) enabled this also publishes the device to Home Assistant.

Photos

The Photos feature stores captured images locally, making them accessible through the Agent DVR User Interface. For more details on how to utilize this feature, please refer to our [Photos guide](#).

Enabled: Toggle to turn Photo saving on or off.

JPEG URL: (Optional) Set a URL to have Agent DVR download a snapshot from your camera, instead of using the decoded video stream.

Mode: Choose from Detected, Alert, Interval, or None. 'Detected' and 'Alert' save images based on activity, while 'Interval' saves images continuously. Use 'None' if you prefer saving photos only through the [API](#).

Interval: The minimum time between frames in 'Interval' mode.

Delay: Set the minimum time between frames for 'Detected' or 'Alert' modes.

Quality: Adjust the jpeg image quality. Lower quality means smaller file sizes.

Overlay Text: Add optional text to your image.

Apply Zoom: Apply the current digital pan and zoom to saved photos.

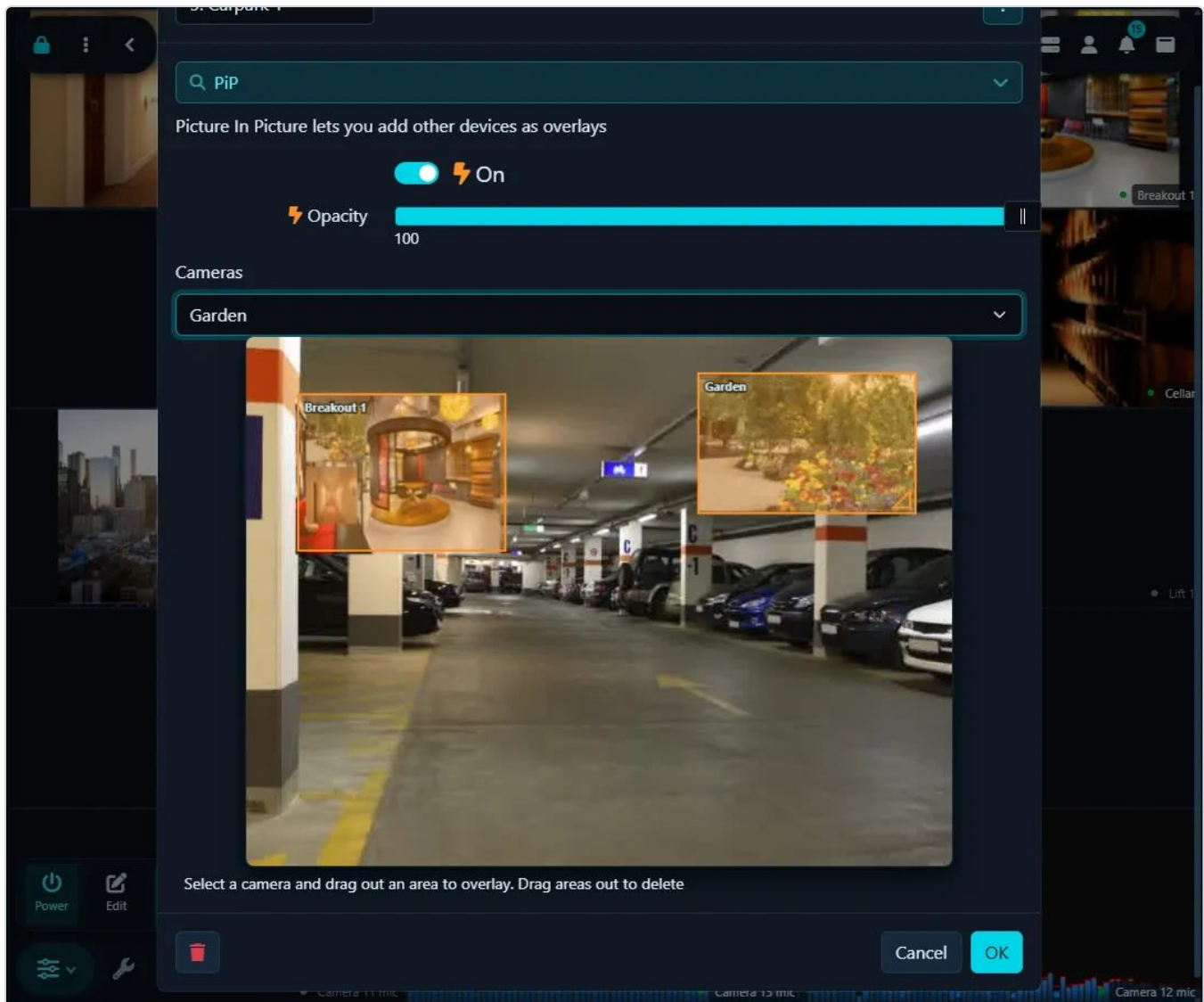
Filename: Specify the filename format for saved images. Use a date template or {C} for a counter value. For instance, with Counter Max at 20, files will be named 0.webp, 1.webp, ... 20.webp, and then start over at 0.webp.

FTP: Upload images to your FTP server as per the settings in the FTP tab (v4.0.0.1+).

FTP Filename: The filename template to use when uploading photos to your FTP server.

Counter Max: Set the maximum value for {C}. Once reached, it resets to 0.

PiP (Picture in Picture)



This tool allows you to overlay multiple camera feeds onto a single display. To activate, select 'Enabled', choose a camera from the dropdown menu, and draw a rectangle on the preview video. You can resize and reposition this rectangle by dragging the bottom right corner or the entire frame. To remove an overlay, simply drag it out of the preview area. This intuitive feature offers a streamlined approach to managing multiple camera views.

Opacity: Set the opacity of the embedded video (may have a small performance hit).

Plugins

Agent DVR is equipped to handle both video and audio plugins, enabling external applications to process media in real time and generate alerts and detection events. Plugins can be installed through the remote website portal at ispyconnect.com. Navigate to  - **Plugins** for installation. If you're interested in developing custom plugins, please refer to our [plugins guide](#).

PTZ (Pan, Tilt and Zoom)

Agent DVR provides robust support for multiple PTZ (Pan, Tilt, and Zoom) devices. The user interface for controlling PTZ can be found on the [Live View](#) page.

Controller: Select the method used to control PTZ (usually your camera model). Choose 'Digital' for digital-only cameras. If selecting 'ONVIF', ensure your source type on the General tab is set to ONVIF and properly configured.

Pelco: Access Pelco Settings for communication configuration with your Pelco device.

ONVIF: Adjust the speed for ONVIF PTZ commands. Toggle angular PTZ control support if your device doesn't support dual-axis movement.

Note: If your camera moves continuously or behaves unusually with ONVIF, disabling angular controls might resolve the issue. Some ONVIF devices operate with simple up/down/left/right commands.

PTZ URL: Usually left blank so Agent DVR uses your IP camera URL to send commands, but it can be overridden here if necessary.

Calibration Delay: To prevent false alerts, Agent DVR ignores motion events for a brief period when PTZ is used, as camera movement might trigger the motion detector.

Digital PTZ: Enable digital pan, tilt and zoom via touch or the mouse wheel.

Port: Set this to the port your camera uses for its web interface (commonly port 80).

Channel: Optionally set the channel number to match your camera's channel.

Username: Override the camera username (leave blank to use the default username).

Password: Override the camera password (leave blank to use the default password).

Flip: Mirror the controls horizontally, vertically, or both.

Rotate: Rotate the control orientation by 0, 90, or 270 degrees, useful if your camera is mounted sideways.

Zoom Out Delay: Automatically zooms the camera back out after a period of time to ensure it doesn't remain zoomed in. Set to 0 to disable this feature.

Zoom Out Delay (digital): The same as Zoom Out Delay, but for digital zoom. Set to 0 to disable.

Adding PTZ Support for Unlisted Cameras

Agent DVR uses a JSON file to control PTZ cameras (called "PTZ.json"). You can find this file in the folder:

Agent/

You can have a go at adding support for your camera (if you're technically minded) by editing this file. Some key points to consider:

If you modify this file you'll need to restart Agent DVR to load in the changes

Use [Fiddler](#) to find the commands your camera takes to control PTZ (by using the existing web interface at the same time fiddler is running).

Check the existing entries for matches against what you see in Fiddler. Chances are another model will be compatible.

Make sure you specify a new, sequential ID in the Camera entry

The CommandURL entry is relative to the network address of your camera, so shouldn't start with http://... it should start with /

The entries for the PTZ directions (Left,LeftUp etc) get appended to the querystring in CommandURL. Agent DVR automatically builds the URL.

To test your changes make sure you remember to edit the camera and change the PTZ mode to your new entry.

If you get it working please [send it to us](#) so we can include it in future versions of Agent DVR (and make it available to download as an update).

PTZ Scheduler

The PTZ Schedule feature in Agent DVR allows you to create a daily list of scheduled commands for your PTZ camera. This functionality is designed to facilitate complex patrol movements. For instance, you can configure a schedule to move the camera to position 1 every 300 seconds (5 minutes), starting at 12:00:00, and repeat this 12 times for a total duration of one hour. You can then create similar entries for positions 2, 3, and so on, starting at 12:01:00, 12:02:00, etc., to establish an hour-long, dynamic patrol schedule for your camera.

PTZ Scheduler

PTZ Schedule: Enable or disable the PTZ schedule feature.

Suspend on Move: Pause the PTZ schedule for a specified number of seconds if the camera's PTZ controls are used manually.

Suspend on Motion: Temporarily halt the PTZ schedule if motion is detected.

Configure: Opens the schedule editor. Each entry has a time (or sunrise/sunset with an offset), the days to run, a repeat interval and count, and the PTZ command to execute.

PTZ Patrol

The PTZ Patrol feature offers a streamlined approach to setting up camera patrols. Simply add a series of patrol points along with their respective durations (the time in seconds the camera should remain at each point). Activating the patrol function enables the camera to automatically cycle through these points.

This feature can be easily enabled or disabled using the device scheduler.

PTZ Patrol

PTZ Patrol: Toggle the PTZ Patrol function on or off (available from v4.4.2.0+).

Configure: Access the [PTZ Patrol settings](#) guide.

PTZ Patrol Settings

The PTZ Patrol system lets you add a sequence of PTZ commands with a delay between each position. When enabled Agent DVR will cycle through these positions in order.

Note that the camera may need to be enabled to display a list of available commands

The Patrol system uses the settings under PTZ Schedule settings to pause the patrol if motion is detected or if the camera is moved manually.

Note that the camera moving can trigger motion detection. Check the motion timeout setting on the detector tab.

This feature can be easily enabled or disabled using the device scheduler.

PTZ Tracking

Tracking functionality in Agent DVR employs an object tracker to identify moving objects within the camera's view and then uses the PTZ controller to follow them within the scene.

Enabled: Activate or deactivate the PTZ tracker.

Configure: Configure the PTZ tracker settings:

Tracking

Tracking Mode: Select from Any Direction, Horizontal Only, or Vertical Only.

Reverse: Inverse tracking direction. For example, if movement is detected to the right, the camera will move left, which can be helpful for capturing fast-moving events like traffic.

Track Stop Delay: The maximum time to track an object before stopping, in milliseconds.

Auto Home: Configure the camera to return to a preset 'Home' position after movement is no longer detected, if your camera supports a home command.

Home Command: Select the specific Home Command for your camera to use for the Auto Home feature.

Auto Home Delay: Determine the wait time after movement ceases before initiating the Home command.

Recording

Agent DVR offers a variety of recording modes, including motion detection, alert, group detection, group alert, manual command, or schedule. IP cameras often provide two streams: a low-resolution live stream ideal for motion detection and live viewing, and a high-resolution main stream suitable for raw recording. For optimal performance, configure your IP camera sources (under General - **Source Type**) in Agent DVR with these two streams. Agent DVR utilizes the high-resolution stream for direct recording, bypassing the need for CPU-intensive decoding and encoding.

To record based on Group Detection and Group Alert, specify the group in the [Alerts](#) tab.

If only one stream is available, Agent DVR can record it raw as well, reducing CPU usage by avoiding encoding. Set the Encoder to Raw Live Stream for this. If playback issues arise, switch the Encoder to Encode and remove the main record URL from the **Source Type** configuration.

In raw recording mode, overlays (such as masks, overlay images, timestamps, etc.) will not be visible on recordings, as Agent DVR saves the raw video from the camera directly. To include these elements, set the Encoder to Encode and remove the main stream setting from the **Source Type**.

Mode: Options include Alert, Detect, Group Alert, Group Detect, Manual, Constant or Disabled. **Alert** records during Alert events (see [Alerts](#)). **Detect** records when movement is detected. **Group Alert and Group Detect** record when any devices in the camera's group alert or detect. **Manual** records on command or via schedule, and can record continuously. **Disabled** prevents all recordings. Manual recording is available in all modes except Disabled. **Constant** Record will always record, giving you 24/7 continuous recording (you won't be able to stop recording via the live UI).

Encoder:

Important: We don't encode the raw recording stream because to encode we first need to decode the stream. If we are decoding the raw record stream then it's more efficient to just use it as the live stream.

Choose a recording method:

Raw Live Stream: Saves the raw data from the camera's live stream. Minimal CPU usage. Doesn't include overlays or masks. Only works with FFmpeg sources (like IP Camera or Onvif). Other sources will use Encode.

Raw Record Stream: Saves the raw data from the camera's record stream. Minimal CPU usage. Doesn't include overlays or masks. Only works with FFmpeg sources (like IP Camera or Onvif). Other sources will use Encode.

Encode: Encodes the Live stream to a video file. Includes overlays and masks. If you want high resolution recordings then set the Live stream to a high resolution endpoint on your camera.

Motion Adaptive Encode: This will encode at a low framerate unless motion is detected.

Action Adaptive Encode: This will encode at a low framerate unless triggered by the "Trigger Activity Detected" action, so AI or external events can control when full framerate is recorded.

See Advanced Settings for encoding options. Note that Raw recording supports instant playback (watch whilst you record). Encoded files need to finish saving before they are playable.

Max Record Time: Maximum recording duration before starting a new file.

Min Record Time: Minimum recording duration.

Inactivity Timeout: Duration to continue recording after motion or alert triggers cease.

Buffer: Pre-record buffer time in seconds, dumped to disk when recording starts.

Max Framerate: Maximum framerate for encoding, affecting CPU/disk usage and quality.

Advanced Settings

Note that some of these settings only apply to videos that are being encoded and not saved raw from the camera.

Use System Clock: Use system clock for frame timestamps to address out-of-sequence timestamps from some cameras, which might cause packet loss. This may result in choppy playback.

Codec: See [Encoding](#).

H264 Profile: Select the H264 encoding profile (Auto, Baseline, Main or High).

Encode Device: Leave blank for the default, or specify a device index or path (for example /dev/dri/renderD128) if multiple GPUs are available.

Adaptive Framerate: Adaptive Encode modes record at a low framerate without audio when there's no activity and at a higher rate with audio when activity is detected, conserving disk space while maintaining a continuous record. This sets the time between frames when idle.

Apply Transforms: Apply flip and rotate transformations to raw recordings. This can increase CPU usage, especially for high-resolution cameras.

Apply Digital Zoom: Apply the current digital zoom and pan while recording (encode only).

Filename: Enter a template filename, excluding the file type extension. Agent DVR adds the extension based on the encoder used. The default is {id}_{0:yyyy-MM-dd_HH-mm-ss_fff}. See [merge tags](#).

Save Thumbnails: By default Agent DVR saves a small and a large thumbnail for each recording (taken at the point of maximum movement if you have a motion detector running). This is used to display images

for recordings in the UI.

Trigger Timeout: Duration to keep recording from a "Trigger Recording" action. This resets with every action call. (v4.3.7.0+)

Reduce: Reduce the size of the encoded video file (v5.3.1.0+)

Quality: Recording quality setting, applicable only to encoded video.

Encoding

By default Agent DVR will save the raw stream from your camera when possible - this minimizes the CPU usage of the application but has some drawbacks (no overlays or masks are written to the file). To encode instead set the Encoder in recording settings to **Encode** and then expand the Advanced section at the bottom to configure the encoder.

Agent DVR supports encoding to H264, H265 (see [terms, section 26](#)), VP8, VP9 and AV1. H264 is the default but you may get less disk space usage with other codecs potentially at the cost of higher CPU usage. If you have GPU enabled and hardware available Agent DVR will attempt to use it for generating files. Check the logs at /logs.html to check if Agent DVR has managed to use the hardware device and make sure via task manager that it's not using too much CPU. If it is you might need to adjust the encoder or resolution of the source video.

When no hardware encoder is available, Agent DVR encodes in software. The default (LGPL) FFmpeg build uses the OpenH264 encoder for this. For better software encoding quality you can enable **Software Encoders (FFmpeg GPL)** in [Server Settings - General](#), which downloads an optional GPL-licensed FFmpeg build that includes the x264 and x265 encoders. Agent DVR shows a notice on the camera's Recording tab when a camera is recording with software encoding and this option would help. Note that H265 software encoding requires the GPL build - without it, H265 recordings automatically fall back to H264.

RTMP

Use RTMP to stream this camera live to platforms like YouTube and Twitch, or to your own streaming server. Configure the specific RTMP server you wish to use for streaming this device.

RTMP Server: Choose an RTMP server from your server settings for live streaming this device to external platforms. 'Default' will select the first available server.

Schedule

Manage your camera's recording times with scheduled entries that can enable or disable the camera, start or stop recording, and modify various settings on a weekly calendar or specific dates (version 4.4.4.0+).

Tip: By enabling "Apply Schedule at Start" in  - **Settings - General**, Agent DVR will automatically configure your devices according to the set schedule upon startup. Without this setting enabled, Agent DVR will start with the devices in their last known state.

To add a new schedule entry, edit your camera, navigate to the 'Schedule' tab, click 'Configure', then 'Add':

Enabled: Activate this schedule entry by checking this option. Active entries are indicated with a green tick in the Schedule summary, while inactive ones have an X.

Type: Choose between a specific time, sunrise, or sunset. For sunrise or sunset options, assign a location with GPS coordinates on the General tab for accurate time calculations.

Sunrise Offset: When using sunrise or sunset, set an offset time in minutes from the calculated time.

Time: Specify a local time for the schedule entry (not applicable if sunrise or sunset is selected).

Command: Select a command to execute. Options include Alert Action Run, which schedules alert actions at specific times (see [Actions](#)). From version 4.0.9.0+, there's also an option to adjust the sensitivity of the motion or sound detector on a schedule under Detector: Set Sensitivity.

Date: Set a specific date for the action or choose which days of the week the schedule should run. Switch between modes by clearing any set date.

Days: Choose which days of the week the schedule should be active. Selected days will be highlighted.

Storage

See [Storage Settings](#)

Talk

The Talk feature lets you speak through your camera's speaker for two-way audio, for example to greet a visitor or warn off an intruder. Agent DVR includes support for talk functions on various devices. To enable talk capabilities through the user interface, select the appropriate talk model. Access to the talk function is available in the [Live View](#) section.

Model: Select the talk model for your device. Click the button next to the drop-down to configure it.

Gain: Controls your outgoing voice volume.

To select the microphone to use in the UI click on the Account menu - UI Settings (v5.8.1.0+)

To select where talk is played back when using local playback (playback from the computer running Agent DVR) click on the  - **Settings** - **General** and set the Talk Device option.

Timelapse

Agent DVR offers the capability to create timelapse recordings from your cameras or a sequence of images. This is ideal for condensing hours or days into a short video, such as a construction project, a garden growing or a sunset. These timelapse recordings are identifiable on the [timeline](#) as half-height bars and can be viewed in the [recordings](#) section, marked with a "TL" overlay. The generation of timelapses can be managed using the scheduler feature.

To solely save photos, set a Photo Frame interval. For generating timelapse videos, configure a Video Frame interval. For instance, setting a frame rate of 5 and a video frame interval of 60 seconds will produce a video playing at 5 frames per second, with each frame representing 1 minute of real time.

Enabled: Enable or disable timelapse generation.

Frame Rate: Set the frame rate for the generated video file, in frames per second (fps).

Video Frame Interval: Specify the frequency for adding a frame to the video file (set to 0 to disable).

Use Photo URL: Capture frames from the camera's JPEG URL (see the [Photos](#) tab) instead of the live stream.

Photo Frame Interval: Determine how often to capture a photo and save it to the grabs directory (set to 0 to disable).

Save Every: Configure the interval, in minutes, to complete and start a new timelapse video file.

Filename: Enter a template filename for generated timelapse files, for example {0:yyyy-MM-dd_HH-mm-ss_fff}.

Timestamp

The timestamp options in Agent DVR allow you to overlay a timestamp (and optionally additional data) onto your live video streams. It's important to note that these timestamps will only be visible in your recordings if you are encoding them (using CPU or GPU, not raw recording from the device). For more information on encoding, refer to the [Recording](#) section.

Use Global Settings: Style the timestamp with the shared defaults from **Server Settings - UI**. Turn this off to customize the timestamp for this camera.

Formatter: Customize the content of your timestamp. This supports multiline formatting and updates via the [API](#). Available tags include:

{FPS} - Displays frames per second.

{0:G} - Shows date and time.

{0:T} - Shows time only.

{NAME} - Displays the camera name.

{LEVEL} - Displays the motion detector level.

{REC} - Indicates "REC" if the camera is recording.

{RES} - Video resolution

{SPACE}, {MEMORY}, {CPU} - Current system stats.

{0:ddMMMyy} - Displays a [custom date format](#).

Position: Decide where in the frame to place the timestamp.

Text Color: Set the color of the timestamp text.

Auto Font Size: Automatically pick an appropriate font size for the video width.
Font Size: Adjust the font size of the timestamp (may require tuning for high resolution cameras).
Outline Color: Choose the color for the outline of the timestamp text.
Outline Size: Specify the size of the text outline.
Back Color: Select the background color for the timestamp.
Show Background: Toggle the background color of the timestamp on or off.
Opacity: Set the opacity of the timestamp overlay.
Font Family: Select from available fonts on your system.
Align: Choose the alignment of the text within its bounding rectangle.
Bold: Option to make the timestamp text bold.
Italic: Option to make the timestamp text italic.
Time Offset: Apply an offset in hours to the time displayed in the timestamp.

AI Facial Recognition

See [Facial Recognition](#)

AI LPR

See [LPR](#)

AI Object Recognition

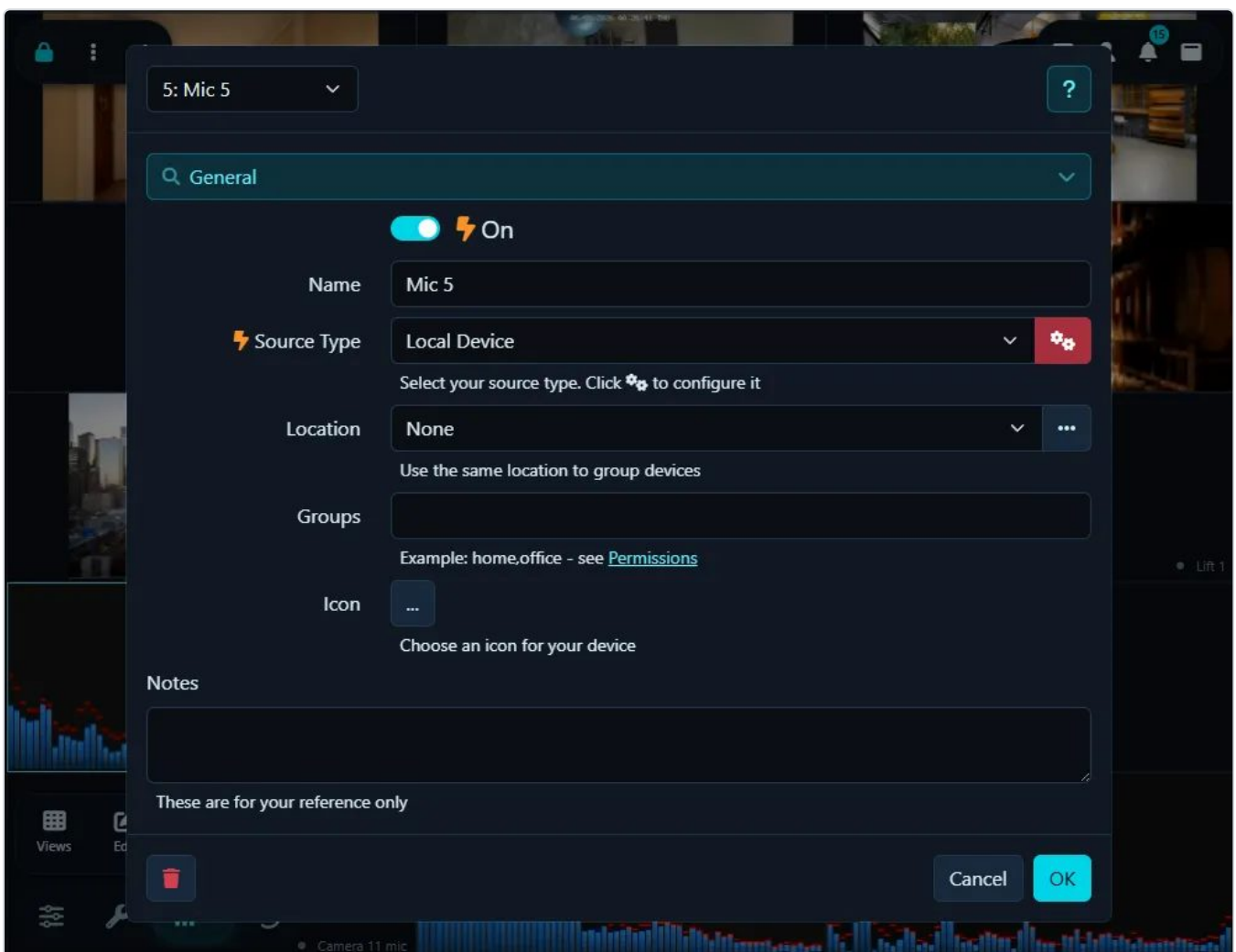
See [Object Recognition](#)

Editing Microphones

About

Editing a microphone lets you set up sound detection, audio recording, alerts, cloud uploads and schedules for that device.

Accessing the device settings in Agent DVR is straightforward. Begin by clicking on the Server icon  at the top right of the Agent DVR User Interface. From there, select "Edit Devices" under **Devices**. You can then choose the device you wish to modify and click the Edit icon . Alternatively, in the [Live View](#), you can select a microphone and click the edit icon on the bottom toolbar, or simply use the shortcut key "E". On Desktop, right-click the Microphone in the Live View or in any area within Agent DVR where a live thumbnail is displayed, like the timeline.



This interface is the central hub for configuring your devices. At the top, it displays essential details like the object ID (for example, "15"), and the device name (like "Office"). On the right side, you'll find the main device menu, which provides access to various configurable areas, referred to as tabs. Notably, a * next to certain settings indicates that changes to these settings are applied immediately, without the need to click 'OK'.

General

This tab provides access to general settings that are commonly used in configuration.

Name: Assign a descriptive name to your microphone, like "Office" or "Back Yard."
Location: Manage locations by clicking the button. You can add locations such as "Main House" and assign a color to them. Devices assigned to locations will be color-coded in the live view.
Groups: Utilized in permissions .
Source Type: Select the method by which Agent DVR connects to your devices. See Audio Source Types .
Enabled: Toggle to turn the microphone on or off in Agent.
Icon: Choose an icon for your device.
Notes: Add your own notes about this device. These are for your reference only.
Schedule: Activate or deactivate the scheduler. If disabled, no scheduled events will be triggered.
MQTT Events: Enable or disable automatic MQTT event packets that Agent DVR sends to your MQTT server - requires a configured MQTT server . With Home Assistant Discovery enabled this also publishes the microphone to Home Assistant.
Display Style: Choose the display style for the microphone in the live view: 'Analyzer' (spectrum analyzer), 'Analyzer Mirrored', 'Radial Spectrum', 'Audio Level' (overall volume level), 'Historical' (volume level graph over time) or 'None'.
Color: Select a color for the audio bars.
Trigger Color: Choose a color for the trigger points (the volume level that activates audio detection).
Back Color: Select a background color for the audio overlay.

Actions

Instruct Agent DVR on the desired actions to take in response to various events, such as Alerts, devices being turned off, or when recordings are completed. For more information on configuring these responses, refer to the [Actions guide](#).

Alerts

Alerts in Agent DVR are triggered by AI, motion detection and various plugins. For a detailed understanding of how these alerts function and can be configured, please refer to the [Alerts guide](#).

Cloud

Automatically upload completed audio recordings to your cloud storage account, giving you an off-site backup of important sound events.

Provider: Select your cloud provider for uploads. Configure your cloud providers in  - **Settings - Cloud**. For additional details, see [More info](#).

Upload Recordings: Enable this to automatically upload your recordings.

Folder: The remote folder to upload into.

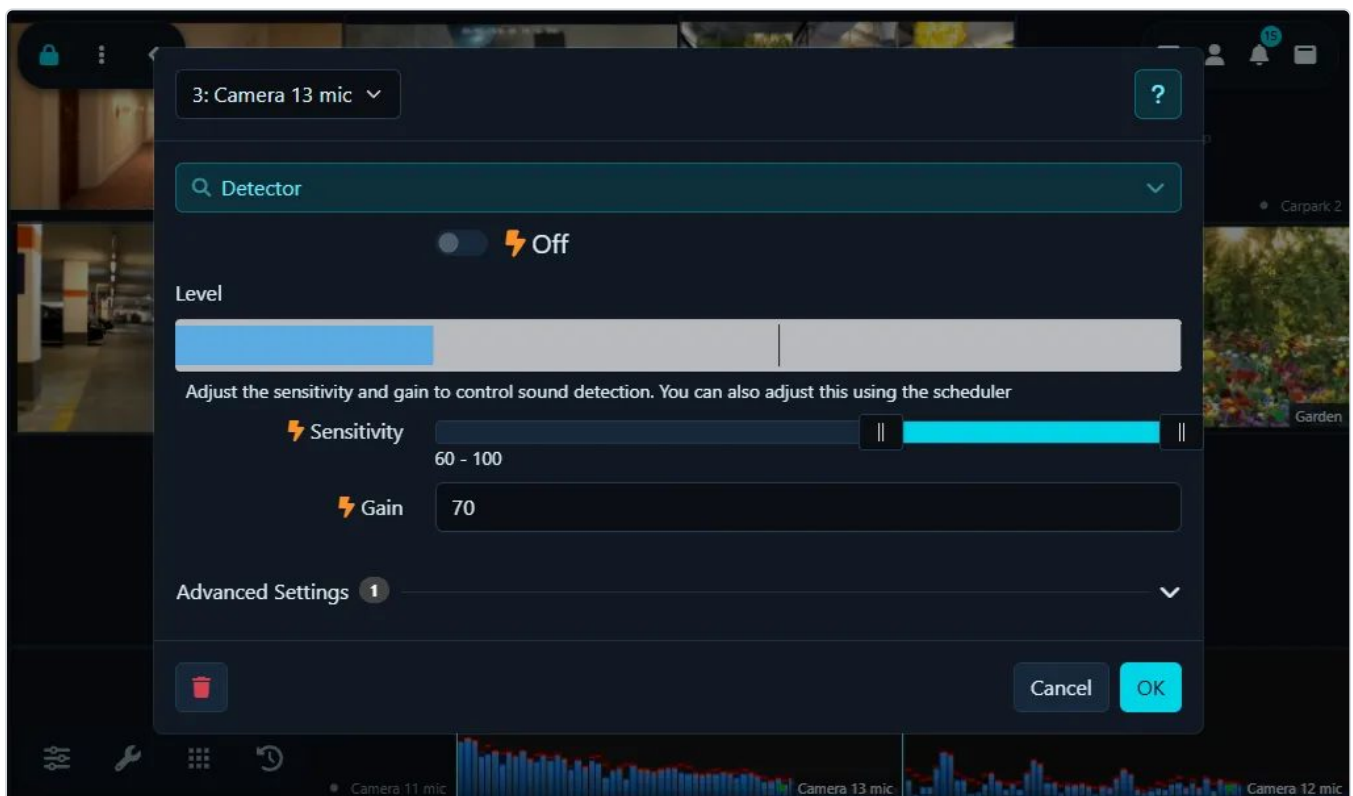
Path: Define the upload path for Agent DVR. For example, using [MEDIATYPE]/[NAME] will upload a video file to Video/somefilename.mp4. The actual filename is determined in the recording tab.

Filename: A template for uploaded filenames, for example {0:yyyy-MM-dd_HH-mm-ss_fff} or {C} (exclude the file extension).

Counter Max: The maximum value of the {C} counter before it resets.

Detector

The sound detector feature listens for increases in volume. Use sound detection to catch events a camera might miss, such as breaking glass, a barking dog, a crying baby or an alarm siren. Any sound exceeding the lower limit is highlighted in **red**, making it easier to identify the sources causing alerts.



Enabled: Activate or deactivate the sound detector.

Sensitivity: Adjust the level of sound required to trigger sound detection. Minimum and maximum values can be set, with the numbers below the slider indicating the percentage of the maximum volume range.

Gain: Apply a multiplier to the detected volume to enhance or reduce the sensitivity of sound detection.

Timeout: Set the duration (in seconds, between 1 and 60, default is 3) for which the microphone remains in a detected state after sound detection ceases. This helps reduce fast repeating events.

Plugin

Agent DVR is equipped to handle both video and audio plugins, enabling external applications to process media in real time and generate alerts and detection events. Plugins can be installed through the remote website portal at ispyconnect.com. Navigate to  - **Plugins** for installation. If you're interested in developing custom plugins, please refer to our [plugins guide](#).

Recording

Agent DVR has the capability to record audio based on sound detection, alerts, manual commands, or according to a predefined schedule.

Mode: 'Alert' triggers recording only when sound detection causes an Alert event (see [Alerts](#)). 'Detect' records whenever sound is detected by Agent. 'Group Alert' and 'Group Detect' record when any device in the same alert group alerts or detects. 'Manual' means recording only occurs when manually initiated or scheduled. 'Constant' records continuously. 'Disabled' turns recording off.

Encoder: Choose the audio format for recordings: MP3, OGG or WAV.

Filename: Enter a template for the filename, excluding the file type extension (e.g., .mp3). Agent DVR will append the appropriate extension based on the encoder in use. The default filename format is {id}_{0:yyyy-MM-dd_HH-mm-ss_fff}. See [merge tags](#).

Max Record Time: Set the maximum duration for each recording. Upon reaching this limit, Agent DVR will complete the current recording and start a new one.

Min Record Time: Define the minimum duration for a recording.

Inactivity Timeout: For recordings triggered by motion or alerts, this determines how long recording continues after the triggering motion or sound ceases.

Trigger Timeout: In the case of recording initiated by a "Trigger Recording" [action](#), this sets how long the recording should continue. This timer resets with each new trigger recording action call.

Buffer: Specify the amount of time in seconds to buffer audio from the microphone before the start of a recording. This essentially acts as pre-recording, with the buffered content being saved to disk once recording begins.

FTP

Upload completed audio recordings to an FTP server. Add your FTP servers in  - **Settings - FTP**. See [Server FTP Settings](#).

Enabled: Switch recording uploads on or off.

Server: Select one of your configured FTP servers.

Filename: A template for uploaded filenames, for example {0:yyyy-MM-dd_HH-mm-ss_fff} or {C} (exclude the file extension).

Counter Max: The maximum value of the {C} counter before it resets.

Schedule

Add schedule entries to manage when the microphone is enabled or disabled, when recording starts or stops, and to adjust other settings on a weekly calendar basis.

Tip: Enabling "Apply Schedule at Start" in  - **Settings - General** allows Agent DVR to determine and apply the appropriate settings to your devices based on the established schedule at startup. Without this option enabled, Agent DVR will start with the devices in their last known state.

To add a new schedule entry, simply click on 'Add':

Enabled: Activate this schedule entry. Active entries are indicated with a green tick in the Schedule summary, while inactive ones are marked with an X.

Time: Set a specific local time for the schedule entry to run.

Days: Choose which days of the week the schedule should operate. Selected days will be highlighted.

Command: Select a command for execution. Options include Alert Action Run, which allows you to schedule alert actions at specific times. For more details, refer to [Actions](#).

Storage

See [Storage Settings](#)

AI Audio Recognition

See [Audio Recognition](#)

Motion Detection

About

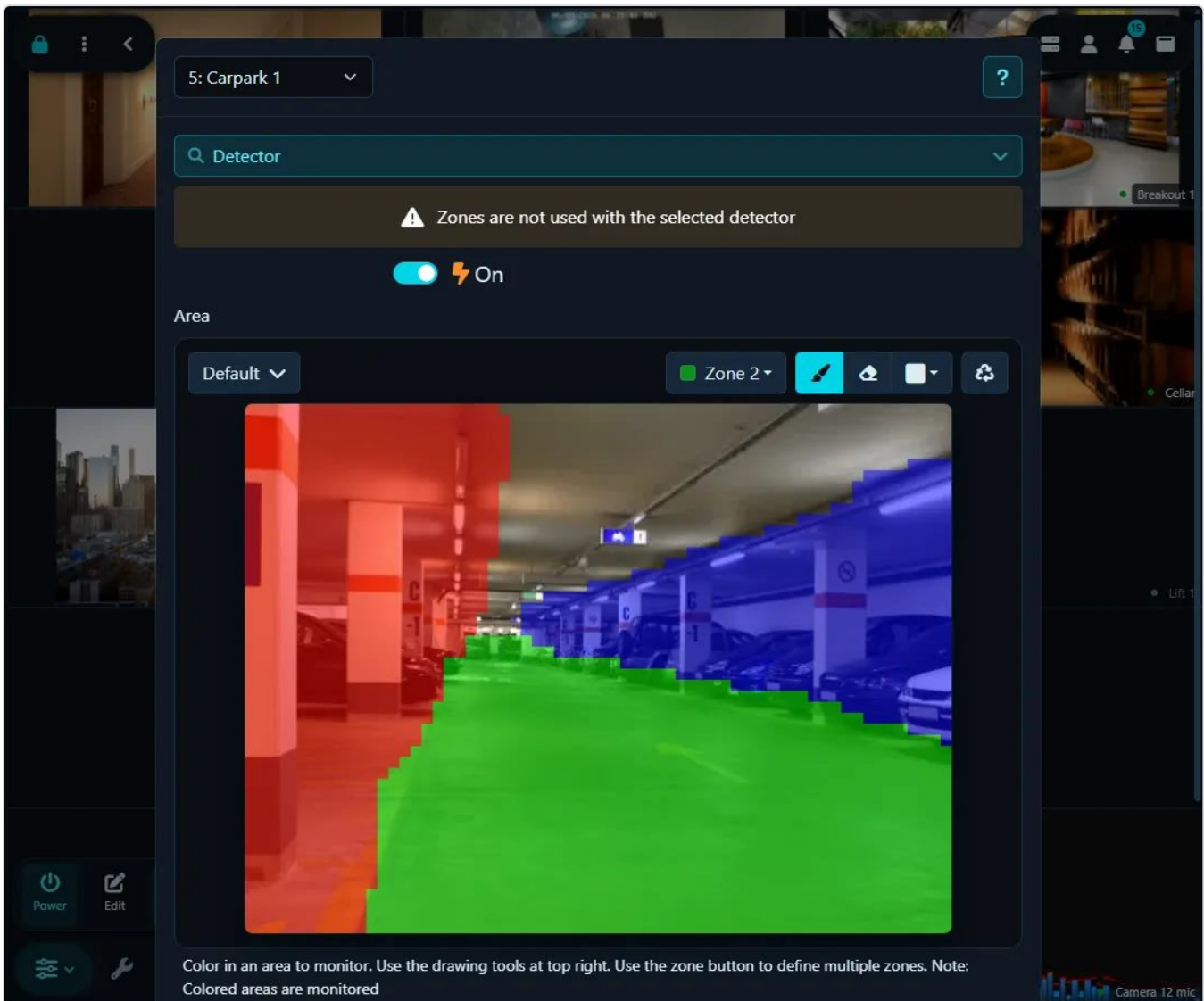
Motion detection watches your camera feeds for movement so Agent DVR can record and alert only when something actually happens. This saves disk space, makes footage much quicker to review, and can notify you the moment someone enters your driveway or a vehicle pulls up outside.

Motion detection in Agent DVR plays a crucial role in initiating [Alerts](#) and facilitating [AI processing](#). You can configure Agent DVR to record upon motion detection or when an alert is triggered. For setting up these options, navigate to the **Recording** menu and refer to the **Mode** setting. Additionally, motion detection can be used to activate various [Actions](#).

It's important to note that motion detection can sometimes lead to false alerts due to its inability to distinguish between actual object movement and environmental factors like wind, rain, or changes in brightness. To reduce such false alerts, you can enhance motion detection's accuracy by [integrating Agent DVR with CodeProject.AI](#) for more sophisticated alert filtering.

Setting up Motion Detection

Motion zones let you focus detection on the areas that matter, like a doorway, driveway or garden path, while ignoring busy areas such as roads or waving trees that cause false alerts.



The motion detector area control in Agent DVR is accessible by editing a camera and selecting **Detector** from the top-right menu. To set up a detector, you start by defining zones to monitor. Agent DVR supports up to 9 zones, each represented by a different color, selectable via the Zone dropdown. To create a zone, click on the pen tool  and draw over the video preview. Use the left mouse button or touch for drawing, and on desktop, the right mouse button to erase. The nib tool  adjusts the size of the drawing nib, while the eraser tool  removes drawn areas. The reset tool  can be used to fill the entire area with the selected zone. Agent DVR then monitors these colored areas for motion.

Enabled: Toggle the use of the detector.

Detector: Choose a motion detector type and configure it using the  button. The various motion detectors are explained in their respective sections.

Overlay: Show or hide the motion detection overlay on the live video.

Color: Adjust the color of the motion detection overlay (not applicable for all detectors).

Blur: Pixelate detected objects in the live video, useful for privacy.

Timeout: Set the duration (in seconds, between 1 and 60, default is 3) for which the camera remains in a motion state after detecting motion stops. This helps reduce fast repeating events.

Using Zones

Zones are crucial for AI detectors (Face/ LPR/ Object Recognition) and object tracking detectors (like trip wire, speed, object tracking). You can select which zones will trigger an alert in the detector configuration, or specify [Actions](#) for alerts in specific zones.

The simple detector activates an alert if sufficient motion is detected across all zones.

Some detector types do not utilize the zone settings, such as MQTT, ONVIF, or motion triggered via API calls.

Using Motion Areas

Motion areas are configurable groups of zones that you can name and save for future use. To save your current motion zone configuration as a new area, click on the edit icon next to **Area**. These tools allow you to add, edit, and delete areas.

To apply a motion area when moving your PTZ camera to a PTZ Preset position (using the Agent DVR UI):

Create and save a new motion zone configuration with a specific name, like "carpark".

Add a new [Action](#):

If: "PTZ Preset Applied"

Select the PTZ Preset Command (e.g., "Go Preset 1"). Note: Your camera must support PTZ presets for this to work.

Click to Add a Task:

Task: "Set Motion Detection Area"

Select your new area ("carpark").

Click OK twice. Now, whenever you select the preset, or if Agent DVR sets the preset through scheduling or another event, this motion area will be applied automatically.

You can also modify the motion detector area using the [Scheduler](#). This feature allows for different motion zone configurations depending on the time of day, week, or specific dates.

Simple Detector

Simple

The simple detector identifies any kind of movement within the camera's field of view. It uses very little CPU (only the ONVIF detector, which relies on the camera itself, uses less). Movements detected are highlighted in **red**, allowing you to easily discern the source of movement in the scene. It is a good default choice for most cameras, and pairs well with an [AI server](#) to filter out false alerts.

Advanced: For additional settings and options, refer to the [advanced section](#) below.

Sensitivity: Adjust the level of motion required to trigger the detection. Setting both minimum and maximum values can refine the detection; for example, a maximum value of 80 could help ignore large-

scale brightness changes. The numbers under the slider represent the percentage of pixels changed.

Gain: Apply a multiplier to the changed pixels to increase or decrease the sensitivity of the motion detection.

HAAR Object Detector

This method employs files known as HAAR cascades to recognize objects in the video feed. However, you might achieve better results using the simple detector together with an [AI Server](#).

Tracking Detector

Detected objects are outlined. Adjust the size limits to filter results

Advanced

- Width Limits** 8 - 30
Upper and lower limits for detected objects
- Height Limits** 12 - 30
Upper and lower limits for detected objects
- Minimum Travel** 10
Distance object must move (percentage of width)
- Minimum Time** 1
Minimum time object must be observed for (x 0.1s)
- ☐ **Display Total**
- ☐ **Heat Map**
Displays an overlay of traffic to visualize movement patterns
- Alert Zones**
Available (click to select):

1 2 3 4 5 6 7 8 9

Zones that generate alerts. Selected zones are BIG
- Check Corners (Alerts)** 0
Checks around the center point of the object bounding box to find detector zones for alerts. 0 = center only, 100 = whole area.

Cancel **OK**

Frame Size: Select the size of the frame for processing. Smaller frames reduce CPU usage but may be less accurate.

Detect Interval: Set the frequency of frame processing, in milliseconds. For example, 200 equals 5 times per second, and 1000 equals once per second.

Width Limits and Height Limits: Define the size range of objects for Agent DVR to detect, expressed as a percentage of the frame's width or height. Adjusting these sliders will display an overlay on the video, indicating the size range of objects being targeted.

Use GPU: Option to use GPU for processing, available only if your GPU supports Cuda and the necessary drivers are installed.

File: Choose the HAAR Cascade file to configure the object detector. Default files are provided for detecting faces and cat faces.

Alert Condition and Alert Number: Configure Agent DVR to generate alerts based on object detection depending on the number of objects detected. For instance, to trigger an alert upon recognizing a face, set the condition to "More Than" and the Alert Number to 0.

Alert Zones: Specify the motion zones to be included in the monitoring area.

Check Corners: For further details, see [Checking Corners](#).

Corner Checking

Agent DVR uses a sophisticated method to determine if detected objects should trigger alerts or actions based on your zone configuration. It does this by checking the center point of the detected object and, optionally, a grid expanding out to the corners of the object's bounding box. You can adjust this feature by setting a percentage that represents the distance from the center point to the corner of the bounding box for zone checks. Essentially, a setting of 0 means only the center point is checked, 100 checks out to all corners, and 50 checks to the midpoints between the center and each corner of the bounding rectangle. If you are receiving numerous event notifications where the object doesn't appear to be within the designated zone, then setting Check Corners to 0 could be beneficial.

MQTT

You have the ability to initiate motion detection from your MQTT server. First, ensure that you have set up [MQTT](#) appropriately. Then, to trigger object detection, simply pass the command indicated in the detector configuration screen to the **SERVER/commands** channel where SERVER is your server name (displayed in the server menu which you can edit in Settings). This integration allows for a more versatile and responsive motion detection system, leveraging the capabilities of your MQTT server.

ONVIF

Many ONVIF-compatible devices come equipped with their own motion detection capabilities. When you select this mode and pair it with an ONVIF-capable camera (using the ONVIF connection type in Agent), Agent DVR will rely on the device itself to provide motion detection events and trigger actions based on

those. Because the analysis happens on the camera, this is the lightest option on server CPU. If you encounter any issues with this functionality, it's advisable to check the logs (accessible at /logs.html on the local server) as it's possible that your camera may not support ONVIF detection. For more information on configuring these settings, please refer to [Server ONVIF settings](#).

Event Timeout: Time in seconds to wait before resetting the motion state. Set this higher than the event notification interval of your camera.

Person Detector

This method employs a specialized algorithm specifically designed to detect pedestrians. However, you might find that using the simple detector and integrating [AI for alert filtering](#) provides better results.

Use GPU: Decide whether to use GPU for processing, available only if your GPU supports Cuda and the necessary drivers are installed.

Frame Size: Select the frame size for processing. Note that smaller frames are less CPU-intensive but may yield less accurate results.

Detect Interval: Set the frequency for frame processing, in milliseconds. For instance, 200 equals 5 times per second, while 1000 equals once per second.

Alert Condition and Alert Number: Configure the criteria for generating alerts based on the number of detected people. For example, to trigger an alert when a person is detected, set the condition to "More Than" and enter 0 in the Alert Number field.

Alert Zones: Choose the specific motion zones that should be monitored within the detection area.

Check Corners: For more detailed settings, refer to [Checking Corners](#).

Confidence: The minimum confidence level required for a detection to count.

Reolink

Some Reolink cameras offer an API endpoint that Agent DVR can poll to receive motion or AI alert states. If your camera supports this feature, you can utilize this detector. To check if your camera has this capability, try accessing the URL: `http://[IP ADDRESS]/api.cgi?cmd=GetMdState&channel=0&rs=Get&user=[USERNAME]&password=[PASSWORD]` (replace [IP ADDRESS], [USERNAME], and [PASSWORD] with your camera's IP address and login credentials). A successful connection will return JSON-formatted text rather than an error page.

Interval: Determine the frequency at which Agent DVR polls your camera for alerts or motion data.

Channel: The channel to poll. Use 0 for standalone cameras; channels may differ on an NVR.

Mode: Select between 'Motion' and 'AI'. Both modes trigger motion detector events in Agent DVR, which can be used for recording (set the record mode to Detect). The 'AI' option triggers motion detection if the camera identifies specific object classes (such as dog_cat, face, people, vehicle).

Use SSL: Connect to the camera over HTTPS.

You can configure actions to perform tasks when objects tagged as dog_cat, face, people, or vehicle are detected.

Note: To enable the AI feature, you might need to activate tracking in the camera's web UI and set the minimum and maximum object size parameters. Agent DVR will then tag your recordings with the objects identified by Reolink.

Hikvision

Hikvision cameras offer an ISAPI endpoint that Agent DVR can monitor to receive motion or AI alert states. If your camera supports this feature, you can utilize this detector. Check the docs for your camera to see if this is supported.

Use SSL: Whether or not to use SSL for the connection.

Port: Agent will use port 80 or 443 depending on Use SSL but you can override that here.

Channel: The channel your camera is using - for cameras this would be 1 but if you have a Hikvision NVR it might be different

Sensitivity: Value between 0 (least sensitive) to 100 (most sensitive) for the motion detector.

Note: when this detector starts, Agent DVR enables motion detection on the camera and applies the Sensitivity value above to it. It doesn't change anything else on the camera - detection zones, schedules and smart event configuration are left as they are. If you don't want the sensitivity changed, set the slider to match the value already configured on your camera. If you don't want Agent DVR to write to the camera at all, use the [ONVIF detector](#) instead, which only listens for events.

These cameras can also detect other events (like line crossing, intrusion, loitering or region entrance). Agent DVR maps each event to a named category and raises an "AI Object Found" event tagged with that category name, for example: Line Crossing Detection, Intrusion Detection, Region Entrance, Region Exit, Loitering, Parking, Unattended Baggage. Add an [action](#) under "AI Object Found" and use these tags to filter it. To see which events your camera generates, set Logging to Debug in Server Settings and check the logs in the server menu.

To get alerts only when a person is detected: in the camera's own web UI, enable a smart event (like Intrusion Detection or Line Crossing) with the target type set to Human (on AcuSense models), then add an [action](#) on "AI Object Found" filtered by that event's tag. Alternatively, use Agent DVR's own [Object Recognition](#) with a person filter - that works with any detector and any camera.

Compared to the ONVIF detector: ONVIF reports generic motion on/off and never modifies the camera's configuration, while the Hikvision detector surfaces the camera's individual smart event types so you can act on them separately. On a Hikvision camera, use this detector if you want the camera's AI events; use ONVIF if you just want basic motion detection.

Speed Detection

This method employs scene information provided by you to track moving objects, estimate their speed, and generate alerts if the objects are moving too fast or too slowly.

Advanced: For more detailed settings, refer to the [advanced section](#) below.

Width Limits and Height Limits: Define the size range for object detection in the scene, with values expressed as a percentage of the scene's width or height. Adjusting these sliders will display an overlay on the video, indicating the target size range of objects.

Minimum Travel: Set the minimum distance an object must move to be considered in motion, based on a percentage of the scene's width.

Minimum Time: Specify the time duration an object must be in motion to be tracked, in tenths of a second (e.g., 1 = 0.1 seconds, 10 = 1 second).

Speed Measurement: Select the preferred unit of speed measurement for the overlay.

Speed Limits: Determine the lower and upper limits of speed detection. Movements outside this range will trigger motion detection events.

Horizontal and Vertical Distance: Enter the total distance across the scene in meters. Agent DVR uses this measurement to calculate the speed of moving objects.

Alert Zones: Choose which motion zones are included in the monitoring area.

Check Corners: For additional settings, see [Checking Corners](#).

Object Tracking

This detector identifies and tracks moving objects, triggering motion detection events based on the duration of their presence in the scene and the distance they travel.

Advanced: For more detailed settings and options, refer to the [advanced section](#) below.

Width Limits and Height Limits: Specify the size range for object detection, with values given as a percentage of the scene's width or height. Adjusting these sliders will overlay a visual representation of the targeted object size range on the video.

Minimum Travel: Define the minimum distance an object must move to be recognized as a moving object, relative to the width of the scene.

Minimum Time: Set the minimum time duration an object must be in motion to be considered for tracking, in tenths of a second (e.g., 1 = 0.1 seconds, 10 = 1 second).

Display Total: Add a counter to the live video feed to keep track of moving objects.

Heat Map: Visualize movement patterns over time by adding lines to tracked objects.

Alert Zones: Choose which motion zones should be included in the monitoring area.

Check Corners: For additional information, see [Checking Corners](#).

As Agent DVR monitors and tracks movement in the scene, it displays colored rectangles around detected objects. The colors have the following meanings:

White: Object just detected and is under consideration.

Yellow: Object detected for multiple frames.

Orange: Object has moved for at least the minimum time specified in the tracking settings.

Red: Object has met all tracking requirements to trigger a motion detection event.

Trip Wires

This detector recognizes and tracks moving objects, triggering motion detection events when they cross predefined trip wires in the scene. Use it for line crossing detection, for example to get an alert when someone crosses a fence line or enters through a gate. To add trip wires, simply click and drag on the live video. You can create up to 10 trip wires. To remove a trip wire, click and drag one of its points out of the scene.

Advanced: For more detailed settings and options, refer to the [advanced section](#) below.

Width Limits and Height Limits: Set the size range of objects to be detected, with values expressed as a percentage of the scene's width or height. Adjusting these sliders will overlay a visual representation of the target size range on the video.

Minimum Travel: Specify the minimum distance an object must move to be recognized as a moving object, relative to the width of the scene.

Minimum Time: Define the minimum time duration an object must be in motion to be tracked, in tenths of a second (e.g., 1 = 0.1 seconds, 10 = 1 second).

Repeat Trigger: Enable this to allow an object to trigger the same trip wire multiple times. By default, an object can only trigger a trip wire once.

Count: Show a count of the number of times objects have crossed the trip wire, along with the direction of crossing. Options include counting left, right, both, or total crossings.

Alert: Configure the system to generate an alert if the trip wire is crossed in a specified direction or any direction.

Alert Zones: Choose which motion zones are included in the monitoring area.

Check Corners: For additional information, see [Checking Corners](#).

Via API

To start motion detection for a camera using an [API call](#), you must define the object type (ot) and object ID (oid). For example, for a camera (ot=2) with an ID of 1 (oid=1; this ID is displayed at the top of the edit

control when editing a device), the API call should be structured as follows:

```
http://localhost:8090/command/detect?ot=2&oid=1
```

Advanced Settings

The default settings for detectors are generally suitable for most scenes, but you can fine-tune them for enhanced performance if necessary.

Analyzer: The current available analyzer is the CNT background subtractor, known for its high accuracy and low CPU usage.

Frame Size: Select the frame size for processing. Smaller frames reduce CPU usage and may actually improve tracking due to noise reduction.

Tracker: Choose the OpenCV tracker for object tracking. Options include:

MOSSE: This tracker offers the lowest CPU usage but is the least accurate.

CSRT: The most accurate option, but it also uses more CPU (default).

Max Objects: Set a limit on the number of objects to track simultaneously. More objects mean higher CPU usage.

Detect Interval: Define the frequency of frame processing for motion detection, in milliseconds (e.g., 200 for 5 times per second, 1000 for once per second).

Track Interval: Set the tracker processing frequency. A higher interval may lose fast-moving objects (e.g., 200 for 5 times per second, 1000 for once per second).

Pixel Stability: Determine the number of samples for a pixel to be considered stable and the maximum 'credit' a pixel can earn for remaining the same color. These settings are crucial for effective background subtraction and movement detection. [More info](#)

Use History: Enable this to learn about consistently moving objects in the scene. It's generally recommended to keep this disabled unless necessary.

Parallel Process: Activate parallel processing in the motion detection algorithm. It's advisable to keep this enabled.

Tracking Timeout: Specify the time to wait (in seconds) for an object to reappear before ceasing to track it.

Movement Timeout: Set the duration (in seconds) to wait for a stationary object to move again before stopping its tracking.

Tip! Noise in the image can affect tracking results. Set the frame size to small to blur out noise and improve tracking results.

Video Sources

About

Source Types for your cameras are configured on the General tab, accessible when [editing cameras](#). This section is where you establish and configure the connection settings for each of your cameras. It's an essential step in ensuring that Agent DVR can successfully communicate and interact with your camera devices.

Clone

The Clone source type offers a straightforward way to replicate a camera, including its video and audio streams, into a new device. This functionality enables you to apply different motion processing, recording rules, and alerts on the newly created device without impacting the original camera's settings. Because the clone reuses the original camera feed, it does not open a second connection to the camera. It's important to note that if the original camera is disabled, the cloned device will lose its video connection.

Camera: Select the device you wish to clone.

Desktop

The Desktop source type records your computer screen as a video source, which is useful for monitoring a kiosk or keeping evidence of remote sessions. Desktop video sources can be utilized on all platforms except when running Agent DVR as a Windows Service. If desktop capture is needed on Windows, it is necessary to run Agent DVR as a local console application rather than as a service. For guidance on how to switch to a local console application, please refer to [Troubleshooting](#).

Screen: Choose which screen to record from.

Capture Mouse: Enable this option to include the mouse pointer in the video capture (Windows only).

Area: Define a specific area of the screen to capture by clicking and dragging (this feature is only available on Windows).

Dummy

Dummy devices provide an option to use either a solid color or an image as a background. This can be useful for testing purposes, combining video from other devices using the Picture in Picture feature or RTMP streaming multiple cameras.

Width: Set the pixel width of the dummy camera, for example, 640.

Height: Specify the pixel height of the dummy camera, for example, 480.

Frame Rate: Define the framerate of the camera, such as 10 fps.

Back Color: Choose the color for the video background.

Image: Provide a path to an image on your local drive. This image will override the background color.

DVR

The DVR option in Agent DVR provides a means to connect to commonly used DVR devices that lack standard RTSP or HTTP video endpoints. Use it to pull individual camera channels from an existing standalone recorder into Agent DVR alongside your other devices.

Model: Select from a list of supported DVR models.

Host: Input the IP address of your DVR within your network. Also, include the port it's operating on, or leave the port field empty to default to the standard port for the selected model.

Username: Enter the username used for logging into your DVR.

Password: Provide the password associated with your DVR login credentials.

Channel: Specify the channel number of the camera on your DVR. For instance, if a DVR operates 4 cameras, you would add each camera using channels 1-4 (or possibly 0-3, depending on the DVR's channel configuration).

File

The File source type in Agent DVR allows you to use a pre-recorded video clip and play it back as if it were a live camera feed. This is handy for trying out motion detection and alert settings without a live camera.

File Path: Provide the local path to the video file you wish to use.

Loop: Enable this option to automatically replay the file once it reaches the end.

IP Camera or Network Camera

The Network Camera source type is designed for connecting to network (IP) cameras, utilizing FFmpeg for the connection. It is the usual choice for any camera on your network that provides an RTSP stream or HTTP video URL. If FFmpeg cannot establish a connection, you can alternatively use VLC by installing it and selecting it as the [decoder](#).

Username: Your login username for the camera (this is different from your iSpyConnect username).

Password: The password for accessing your camera (not your iSpyConnect password).

Live URL: The URL for the live video stream from your camera. If your camera provides a low-resolution stream, use that URL here. Use the "..." button to launch a wizard that helps discover available connections.

Record URL: The URL for the main (record) video stream from your camera. If your camera offers a high-resolution stream, use that URL here. The "..." button initiates a wizard to find available connections.

Use HD Stream: Show the record (HD) stream in live view instead of the live stream, either only when maximised or in both the main and maximised views. Requires the recording mode to be set to Raw

Record.

HD On Demand: Only connect to the high definition record stream when it's needed, for example when the camera is maximised in live view or recording. This saves bandwidth and data quotas on metered or mobile connections. Recordings made this way start without buffered footage and can be delayed a few seconds while the stream connects. If the record stream fails to connect, Agent DVR records the live stream instead.

If Experimental Features is enabled in [Server Settings](#), an additional RTSP (Alternate) source type is available. This is a simplified RTSP connection (username, password and live URL only) offered as an alternative way to connect RTSP cameras.

For assistance with playback issues, refer to [Glitchy / Stuttering Video](#).

JPEG or Image

The JPEG/Image source type is designed to connect to JPEG or other image-based sources. Use it for cameras or devices that publish snapshots or an image URL over HTTP.

Username: Enter the username for the camera (not your iSpyConnect username).

Password: Enter the password for the camera (not your iSpyConnect password).

URL/ Path: Specify the connection URL for the live image feed from your camera. The "..." button launches a wizard to help find available connections.

Reload Interval: For static images (such as weather GIFs that only change occasionally), set a reload interval to periodically check for new images. For JPEG and video feeds, this interval should be set to 0.

Local Device

Connect USB webcams, capture cards and other local hardware video sources using this option.

Device: Select from the list of detected local video devices.

Video Resolution: Choose the desired video resolution.

On Linux, the device options might be empty, often due to permissions issues. To resolve this, add your user to the video permissions group with the following commands:

```
sudo adduser YOUR_USERNAME video

sudo usermod -a -G video YOUR_USERNAME
```

...Then restart your computer.

If your device is detected but no video resolution options are available, you can manually add the resolution setting in the [ffmpeg settings](#) under Options, e.g:

```
video_size=720x576
```

MJPEG

Connect to MJPEG sources. While the IP Camera option is typically preferred, the MJPEG option serves as a backup for cases where certain cameras are incompatible with the standard IP Camera setup.

Username: Enter your login username for the camera (note: this is different from your iSpyConnect username).

Password: Provide the password for your camera (not your iSpyConnect password).

Live URL: Specify the URL for the live video stream from your camera. Use the "..." button to access a wizard that helps find available connections.

Record URL: Enter the URL for the record stream from your camera. Again, the "..." button can help you discover available connections.

Use Internal Decoder: The FFmpeg decoder used by Agent DVR may encounter difficulties with some streams that have non-standard boundary markers. Enable this option to switch to Agent DVR's internal decoder. Note: Using the internal decoder means the Record URL will not be utilized.

Use HD Stream: Show the record (HD) stream in live view instead of the live stream, either only when maximised or in both the main and maximised views. Requires the recording mode to be set to Raw Record.

HD On Demand: Only connect to the high definition record stream when it's needed, for example when the camera is maximised in live view or recording. This saves bandwidth and data quotas on metered or mobile connections. Recordings made this way start without buffered footage and can be delayed a few seconds while the stream connects. If the record stream fails to connect, Agent DVR records the live stream instead.

NDI

Access Network Device Interface (NDI) sources for video streaming over a network. For NDI discovery settings, see [NDI server settings](#).

Source: Select from the list of detected NDI sources. It's important to choose a source from the detected list rather than manually typing it in. Refer to the NDI settings to include endpoints for detecting remote sources.

Audio Level: Adjust the audio level coming from the selected NDI source.

Nest

This option provides integration support for legacy Nest and Dropcam cameras that can share a public video feed. Google has discontinued Dropcam and no longer offers public sharing on newer Google Nest cameras, so this source type only works with older devices. See [Nest and Dropcam Cameras](#) for details.

Public URL: Enter the URL where your camera can be accessed publicly.

Get Video URLs: Click this button, and Agent DVR will find the direct link to your camera's video stream.

Video URL: This field will be automatically filled in after you click the 'Get Video URLs' button.

Web Browser

The Web Browser source type renders a web browser as a video source within Agent DVR, so you can display a status dashboard or any web page as a camera feed. If not already available, it will automatically download and install a headless version of Chromium to facilitate this feature.

Username: Enter the username to log in to the web page if required.

Password: Enter the password to log in to the web page if required.

Width: The width of the browser window.

Height: The height of the browser window.

URL: Enter the URL to load (e.g., <https://www.example.com>).

Reload Interval: Determine how frequently the page should be reloaded.

To force a page reload, you can enable the **Prevent JPEG cache** option found under the Advanced settings.

To set cookies for the browser, use the **Cookies** option in Advanced settings. For example, to set a cookie named 'mycookie' with the value 'myvalue', enter 'mycookie=myvalue' in the Cookies field.

ONVIF

Agent DVR offers built-in support for almost all ONVIF-compatible cameras. ONVIF is an open standard used by most modern IP cameras, and connecting with it lets Agent DVR discover the available video streams automatically. If you encounter connection issues with your ONVIF devices, check the logs at </logs.html> for potential errors.

Username: Enter the username for your camera (not your iSpyConnect username).

Password: Provide the password for your camera (not your iSpyConnect password).

Service URL: This is the URL for your camera's service definition. Agent DVR can usually detect these automatically: click a detected device to populate the Service URL. If your device isn't found automatically, you can enter it manually. It should look like 'http://IPADDRESS:PORT/onvif/device_service'.

RTSP Port Override: Override your camera's RTSP port if necessary, such as when port forwarding on a different network with a different RTSP port. Generally, leave this as 0. This port is used for live video and

audio streaming from your camera.

HTTP Port Override: Override the HTTP port of your camera if port forwarding on another network with a different HTTP port. Usually, this should be left as 0. This port is for obtaining JPEG images from your camera.

Timeout: Set the duration Agent DVR will try connecting to your camera before timing out.

Discover: Click this button to allow Agent DVR to connect to your camera using the provided credentials and retrieve video connection options, populating the URLs below.

Live URL: After discovery, select a low-resolution video stream for live viewing and motion detection.

Override URL: Optionally, add an override URL for the Live URL if you prefer that over the discovered options.

Record URL: After discovery, choose a high-resolution video stream for raw recording.

Override URL: Optionally, add an override URL for the Record URL if you prefer that over the discovered options.

Use Snapshot URI for Photos: Opt to download photos directly from the camera instead of generating images from the live video stream.

Use HD Stream: Show the record (HD) stream in live view instead of the live stream, either only when maximised or in both the main and maximised views. Requires the recording mode to be set to Raw Record.

HD On Demand: Only connect to the high definition record stream when it's needed, for example when the camera is maximised in live view or recording. This saves bandwidth and data quotas on metered or mobile connections. Recordings made this way start without buffered footage and can be delayed a few seconds while the stream connects. If the record stream fails to connect, Agent DVR records the live stream instead.

Force Reload: If your camera appends a unique token to video stream URLs valid for only one session, enable this option to get a new video URL for each connection attempt, which can help with reconnection issues.

For assistance with playback issues, refer to [Corrupted / Stuttering Video](#).

Advanced Settings

Advanced options in Agent DVR offer extra tools for enhanced connectivity with your devices. To access these options, go to Edit Camera, select the General tab, click to configure the video source, and then select the Advanced tab.

Decoder: Options include CPU, GPU, VLC (if installed) and None. VLC can decode streams that FFmpeg (used by Agent) might not. Switching the decoder requires disabling and re-enabling the camera. **None**

is available only for network camera source types: it bypasses video decoding entirely, so it requires raw recording mode, and motion detection and AI alert filtering won't function.

If FFmpeg fails to decode some RTSP streams from certain camera models, resulting in errors like "Invalid data found when processing input," try switching the decoder to **VLC** (Install VLC from [here](#) and restart Agent DVR for detection).

GPU Decoder: Select the specific hardware GPU decoder to use. Choose default to use the [default setting](#).

Decode Device: If you have multiple GPUs, specify which device to use for decoding. Leave blank for the default, or enter a device index or path (for example /dev/dri/renderD128).

Cookies: Add any necessary cookies for accessing your camera's video stream.

Basic Authentication: Toggle Basic Authentication for camera login on or off.

Use HTTP 1.0: Force usage of HTTP 1.0 for compatibility with older cameras.

Validate Certificate: Validate SSL certificates when connecting. Leave this off for cameras that use self-signed certificates.

Prevent JPEG cache: Append a unique parameter to JPEG requests to prevent caching. Can cause issues with some cameras.

Headers: Include any additional headers required for accessing your camera's video stream.

User Agent: Set the user agent for the connection if specified by your camera.

Connection Timeout: Set the maximum wait time for a response from the camera before timing out.

Reconnect Interval: Configure a periodic interval to close and reopen the connection to the camera.

Reconnect Strategy: Choose the schedule for reconnection attempts if the camera connection is lost. Options include an elastic schedule (2, 5, 10, 30 seconds) or immediate reconnection.

VLC Options: Specify any additional options to pass into VLC when connecting to your camera.

FFmpeg Settings

These are general FFmpeg settings that allow you to fine-tune how Agent DVR connects to your cameras. To access these settings, go to Edit Camera, select the General tab, click to configure the video source, and select the FFMPEG tab.

Prefer TCP: Enabling this option makes FFmpeg prefer TCP connections to your camera, which provides error correction at the cost of increased CPU usage and network traffic.

Auto Switch: Automatically switch between TCP and UDP transports if the connection fails.

HTTP Tunneling: Tunnel RTSP over HTTP. This can help when connecting through firewalls or proxies.

Low Delay: Reduce latency in the stream. Disabling this can improve stream quality.

Scale Mode: Select a scale mode for FFmpeg. The default mode is Fast Bilinear.

Find Best Stream: Enable this option to let FFmpeg automatically choose the best video and audio streams from the connection.

Video Stream Index: If 'Find Best Stream' is unchecked, you can manually select the video stream index. 0 = automatic.

Audio Stream Index: Similar to the video stream index, this allows manual selection of the audio stream when 'Find Best Stream' is disabled. 0 = automatic.

Thread Count: Sets the number of threads for stream decoding. 0 = automatic. Fewer threads can reduce lag.

Options: Place to input any additional FFmpeg options you wish to apply.

Filter: See below.

FFmpeg Troubleshooting

For assistance with playback issues, refer to [Corrupted / Stuttering Video](#).

FFmpeg Filters

Using ffmpeg filters you can apply realtime effects and overlays to your video. Note that for these to persist to recordings you will need to set the recording mode to Encode.

To use these edit the camera and on the General tab click on video source settings - ffmpeg settings. These effects will only apply if you are using an ffmpeg decoder.

Examples:

Crop and blur an area:

```
[in]split[main][crop];[crop]crop=w=200:h=100:x=50:y=50,boxblur=10[blurred];[main][blurred]overlay=x=50:y=50[out]
```

Add text overlay:

```
[in]drawtext=text='Hello, World!':x=10:y=10:fontsize=24:fontcolor=white[out]
```

Combine:

```
[in]drawtext=text='Hello, World!':x=10:y=10:fontsize=24:fontcolor=white,split[main][crop];[crop]crop=w=200:h=100:x=50:y=50,boxblur=10[blurred];[main][blurred]overlay=x=50:y=50[out]
```

[FFmpeg Documentation](#) ↗

Audio Sources

About

Source Types for microphones are configured in the General tab when [editing microphones](#). This section is where you control the connection settings for your microphone, ensuring correct communication between the microphone and Agent DVR.

Camera

The Camera source type is utilized when the camera's media stream (typically RTSP) includes an audio track, and Agent DVR has automatically created a corresponding microphone control for it. This source type is not editable, as it is configured based on the audio component of the camera's media stream.

Clone

The Clone source type enables you to duplicate the audio from an existing device into a new one. This allows for separate sound processing, recording rules, and alerts to be applied to the new device without impacting the original. It's important to note that if the original device is disabled, the clone will lose its audio connection.

Microphone: Select the device you wish to clone.

iSpy Server

This option allows you to stream audio from [iSpyServer](#), a feature of the iSpy software that facilitates local and remote streaming.

URL: Enter the URL for the audio stream from iSpyServer. For example: `http://192.168.1.20:9000/`

Local Device

Connect to USB microphones or other local hardware audio sources using this option.

Device: Select from the list of detected local audio devices.

Option: On Windows, choose the audio format (sample rate and channels) for the selected device.

MP3

Stream audio from an MP3 network source using this option.

URL: Enter the URL to the MP3 audio stream. For example: `http://192.168.1.20/livestream.mp3`

NDI

Connect to the audio stream from a Network Device Interface (NDI) source on your network. For NDI discovery settings, see [NDI server settings](#).

Source: Select from the list of detected NDI sources.

Audio Level: Adjust the audio level coming from the selected NDI source.

File or URL

The Network Microphone source type streams audio from a network audio source or a local file.

File/URL: Enter the file path or URL from which to stream audio. Examples include `http://192.168.1.20/livestream.mp3` or `D:\test.mp3`

Analyse Duration: Specify the duration for FFmpeg to analyze the streams to determine the best codecs and streams. A value of 0 means the decision is made automatically.

Loop: When playing a file, automatically replay it once it reaches the end.

Decoder: Choose between FFmpeg or VLC (if VLC is installed).

Options: Input any additional FFmpeg options as required.

The File source type is a simpler option for playing back a local audio file:

File Path: The path to the audio file to play.

Loop: Automatically replay the file once it reaches the end.

Wasapi

For Windows users, this option allows for the integration of WASAPI audio devices, including capturing the sound your computer is playing.

Device: Select the desired WASAPI device from the available options. Choose Loopback to capture the computer's audio output.

Wave

This option allows you to connect to a Wave (.wav) network audio source.

URL: Enter the URL to the audio stream.

Sample Rate: Specify the sample rate of the audio.

Channels: Define the number of audio channels in the stream.

Advanced

Advanced options provide additional tools to help you connect to your devices.

Prefer TCP: Prefer TCP connections for network audio, which provides error correction at the cost of increased overhead.

Auto Switch: Automatically switch between TCP and UDP transports if the connection fails.

HTTP Tunneling: Tunnel RTSP over HTTP. This can help when connecting through firewalls or proxies.

Validate Certificate: Validate SSL certificates when connecting. Leave this off for devices that use self-signed certificates.

Low Delay: Reduce latency in the stream. Disabling this can improve stream quality.

Connection Timeout: Specify how long to wait (in milliseconds) for the microphone to respond before giving up.

Reconnect Interval: Set this to periodically close and reconnect the connection to the microphone (in seconds, 0 = never).

Server Settings

About

To tailor your settings, click on the **Server icon**  located at the top right of the Agent DVR UI, and select **"Settings"** from the **Configuration** menu. Please note, if the server icon is highlighted with a colored background, this indicates you are operating on another user's Agent DVR server through [permissions](#), which may limit access to some features.

General

General options for your Agent DVR server, covering its name, default language, update track and how it manages CPU load.

Name: Assign a unique name to your Agent DVR instance. This is especially useful if you manage multiple servers on your account. Note: changing the server name may affect permissions you have assigned to other people.

Beta Track: Check for updates from the beta track instead of the release track.

Default Language: Set the default language for your server

Default Voice: The default voice used for text to speech.

Max CPU: Specify the maximum CPU usage for your server. Alerts will be sent if this limit is reached, and Agent DVR will adjust camera framerates to manage the load.

Tuning: Optimize Agent DVR for your hardware: Performance (high FPS, fewer cameras), Balance, or Capacity (more cameras or less powerful hardware).

Check for Updates: Enable checking for new versions of Agent DVR.

Talk Device: The audio output device used for talk playback.

ONVIF Discovery: Enable or disable periodic ONVIF device discovery on your network.

Experimental Features: Activate this to test new features in Agent. These features are typically under development and should generally be used only for testing purposes.

Software Encoders (FFmpeg GPL): Agent DVR uses an LGPL build of FFmpeg by default. Enable this to download the optional GPL-licensed FFmpeg build, which adds the x264 and x265 software encoders for higher quality H.264/H.265 encoding on systems without GPU acceleration. When you change this, Agent DVR downloads the selected build in the background and then restarts automatically to apply it. Systems with a supported GPU don't need this option. Both FFmpeg builds are open source - build scripts and source code are available at github.com/ispysoftware/agentdvr-ffmpeg-build, and each download includes its license texts in the licenses folder.

Default Camera Login: A pre-filled username and password used when adding new camera devices (useful if your cameras share one login).

Min Framerate: The minimum framerate cameras will be reduced to when Agent DVR is lowering CPU load.

CPU Priority: Set the priority of the Agent DVR process on your system. Recommend Above Normal.

Apply Schedule at Start: Enable this to apply your scheduling settings on startup, ensuring your devices are in the correct state according to your schedule. If unchecked, Agent DVR will start with devices in their last known state.

Notify on Disconnect: Activate this to receive notifications if your server disconnects from web services unexpectedly.

VLC Directory: Specify the installation directory of VLC (v3+). This is usually auto-detected by the system.

Push to Talk: Enable push to talk mode, where communication is only possible when the talk button is pressed.

SignalR Method: Select the SignalR method (used by Agent DVR for setting up remote connections). This is mainly for troubleshooting remote access issues.

Wait for SignalR: Enable this to wait for a SignalR response at startup, which can help resolve connection issues on macOS.

AI Servers

Connect Agent DVR to AI servers to add intelligent features like object recognition to your cameras.

[See AI Settings](#)

Cloud

Connect Agent DVR to your cloud storage accounts here so your cameras can upload recordings and photos offsite automatically.

Supported Cloud Providers

Box
Drive
DropBox
NextCloud / WebDav
OneDrive
OneDrive Business
OpenDrive
S3

Click the appropriate button to authorize Agent DVR to connect with your cloud host. If you encounter any issues, consider temporarily disabling 2-factor authentication on your cloud host account. Once Agent DVR has access, you can manage cloud uploads by adjusting your [camera cloud settings](#).

S3 Cloud Storage

For S3 Storage options, oauth is not used. Instead, you'll need to provide a client ID and a secret key for uploads. Agent DVR is compatible with Amazon S3 and other S3 Providers like Google Cloud.

Amazon S3 Settings

Set up your storage account on AWS and enter the required S3 parameters. The URL field should be left blank for Amazon S3, as it's automatically configured.

Google Cloud S3 Settings

For Google Cloud S3 storage, begin by creating a new bucket in the Google Cloud interface. Then, generate an [Access Key](#), which will provide a key and a secret for Agent DVR configuration. Set the URL to **https://storage.googleapis.com**. Note: The region name is not required for this setup.

FTP Servers

Configure and manage your FTP servers conveniently here. Once a server is added, you can easily select it for any camera through the editing options. For more details on camera FTP settings, please refer to [camera FTP](#).

Name: Assign a local name to your server for easy identification within Agent.

Username: Enter your FTP server username.

Password: Enter your FTP server password.

Server: Specify your FTP server URL, starting with ftp:// or sftp:// (e.g., ftp://192.168.12.1).

Port: The port number your FTP server uses, typically 21 for ftp:// and 22 for sftp://.

Use SFTP: Enable this option if your server utilizes SFTP.

Use Passive: Opt for Passive FTP mode by checking this.

Rename: Activating this will have Agent DVR upload files under a temporary name and then rename them post-upload. This is particularly useful to minimize flicker when streaming video via FTP and javascript. [Learn more](#).

Max Queue: Set a limit for the upload queue size. If this limit is reached, Agent DVR will stop accepting new files for upload. Note that the queue size is managed on a per-camera basis.

Layouts

Layouts control how your cameras are arranged on the live view. Using this tab you can add, edit and delete [layouts](#)

LDAP

Use your LDAP server (openLDAP, Active Directory etc) to handle logins. This uses the local logins feature so requires a license. You can find these settings on the LDAP tab of the Users dialog in Server Settings.

Using LDAP your users can sign into the local web client using their LDAP logins. This will authenticate them against your LDAP server and create a local account for them automatically.

Enabled: Turn logins with LDAP on or off.

Server Address: Enter your LDAP server address, eg ldap.example.com

Port: LDAP server port. Usually 389 or 636 for LDAP over SSL. If you are using Active Directory and encounter Referral errors, try port 3268 (Global Catalog).

Is Active Directory: Check this if you are using AD (it modifies some of the fields passed to LDAP).

Use SSL: Check if you are using a secure connection

Validate Certificate: Validate the server's SSL certificate. Leave this off for self-signed certificates.

Use Basic Authentication: Use basic authentication when binding to the LDAP server.

LDAP Search Base: Domain Search bases. eg DC=myorg,DC=com

Protocol Version: Default is 3

Common Name: The attribute used to match usernames, eg sAMAccountName for Active Directory or uid for openLDAP.

Service Login: Optional username and password for a service account used to look up user details and group membership. Required if your server does not allow anonymous binding.

Group Permissions

Using Group Permissions you can add LDAP user group names and permissions to apply to those groups. You must add at least one LDAP group to configure LDAP logins. When a user logs in the system will match their LDAP usergroup membership against these groups and apply the permissions it finds. If a user is a member of multiple groups the permissions will be combined (via an OR operation).

LDAP Configuration Examples

Active Directory (Windows Server)

Basic Configuration

Server Address	dc1.company.local
Port	389 (LDAP) or 636 (LDAPS)
Is Active Directory	✓ Enabled
Use SSL	✓ Enabled (recommended)
Use Basic Authentication	✓ Enabled
LDAP Search Base	DC=company,DC=local
Protocol Version	3
Common Name	sAMAccountName

Service Login (Optional)

Username	ldap-service@company.local
Password	[service account password]

Login Formats:

Users can login with:

- john.doe
- COMPANY\john.doe
- john.doe@company.local

OpenLDAP Server

Basic Configuration

Server Address	ldap.company.com
Port	389 (LDAP) or 636 (LDAPS)
Is Active Directory	✗ Disabled
Use SSL	✓ Enabled (recommended)
Use Basic Authentication	✓ Enabled
LDAP Search Base	dc=company,dc=com
Protocol Version	3
Common Name	uid

Service Login (Required)

Username	cn=ldap-reader,ou=system,dc=company,dc=com
Password	[service account password]

Important:

Service account is required for user searches since anonymous binding is typically disabled.

User Login:

Users login with their uid:

ForumSys Public Test Server

Basic Configuration

Server Address	ldap.forumsys.com
Port	389
Is Active Directory	✗ Disabled
Use SSL	✗ Disabled (test only)
Use Basic Authentication	✓ Enabled
LDAP Search Base	dc=example,dc=com
Protocol Version	3
Common Name	uid

Service Login (Not Required)

Username	(leave blank)
Password	(leave blank)

Test Users Available:

einstein / password

newton / password

galileo / password

tesla / password

Google Secure LDAP

Basic Configuration

Server Address	ldap.google.com
Port	636
Is Active Directory	✗ Disabled
Use SSL	✓ Enabled
Use Basic Authentication	✓ Enabled
LDAP Search Base	dc=company,dc=com
Protocol Version	3
Common Name	uid

Service Login (Required)

Username	[service account email]
Password	[service account password]

Required:

Service account must be configured in Google Admin Console with proper LDAP permissions.

⚙️ Configuration Notes & Troubleshooting

SSL/TLS Recommendations

- **Production:** Always use SSL (port 636) or StartTLS (port 389 with SSL enabled)
- **Testing:** Non-SSL connections acceptable for testing environments only

Active Directory vs OpenLDAP

- **Active Directory:** Use `sAMAccountName` for Common Name
- **OpenLDAP/Others:** Typically use `uid` for Common Name

Port Selection

- **389:** Standard LDAP (can use StartTLS)
- **636:** LDAP over SSL (LDAPS)
- **3268:** AD Global Catalog (unencrypted)
- **3269:** AD Global Catalog over SSL

Service Accounts

- **Active Directory:** Can use UPN format (`service@domain.com`)
- **OpenLDAP:** Requires full DN format (`cn=service,ou=users,dc=domain,dc=com`)
- **Optional:** If not specified, user credentials will be used for group lookups

Common Issues

Certificate Errors

Ensure SSL certificates are valid or configure certificate validation properly.

Connection Timeouts

Ensure LDAP ports are accessible from your server and firewall rules allow traffic.

Permission Denied

Service account must have read permissions on user and group objects.

Users Not Found

Search base must be broad enough to include all users and groups in your directory.

OAUTH

Use a third-party Identity Provider (like Okta, Microsoft Entra ID, Google, etc.) to handle logins via the OAuth 2.0 and OpenID Connect standards. This uses the local logins feature so requires a license.

Using OAuth2, your users can sign into the local web client using their existing company credentials. This will authenticate them against your provider, and if successful, will create or update a local account for them automatically.

Enabled: Turn logins with OAuth2 on or off.

Provider Name: A friendly name for the provider that appears on the login button, for example "Sign in with Google".

Client ID: The unique public identifier for your application, provided by your Identity Provider.

Client Secret: The Client Secret for your application. Keep this confidential.

Issuer: The root URL of your provider's authorization server. This is the base URL from which all other endpoints are discovered.

Authorization Endpoint: The URL where the user is sent to log in.

Token Endpoint: The URL your application uses to exchange the authorization code for an ID token.

Redirect URI: The exact URL the provider will send the user back to after a successful login. This must be whitelisted with your provider. For LAN apps, this is typically a localhost address (e.g., `http://localhost:8090/`).

Scope: A space-separated list of permissions your app is requesting. At a minimum, this must include `openid profile email` and a scope for groups e.g., `groups`

Username Claim: The name of the claim in the ID token to use as the user's unique username. Standard practice is to use `preferred_username` or `email`

Group Claim: The name of the claim in the ID token that contains the user's group memberships. This is often `groups`

Group Permissions

Using Group Permissions you can map group names from your Identity Provider to a set of permissions in this application. You must add at least one group mapping to configure OAuth2 logins. When a user logs in, the system will check the group claims in their token, match them against these rules, and apply the permissions it finds. If a user is a member of multiple mapped groups, the permissions will be combined (via an OR operation), giving them the most permissive access.

OAuth2 Configuration Examples

Okta

Provider Configuration

Issuer	<code>https://your-tenant.okta.com</code>
Authorization Endpoint	<code>https://your-tenant.okta.com/oauth2/v1/authorize</code>
Token Endpoint	<code>https://your-tenant.okta.com/oauth2/v1/token</code>
Client ID	Found in Okta Application settings
Redirect URI	<code>http://localhost:8090/</code>
Scope	<code>openid profile email groups</code>
Username Claim	<code>preferred_username</code>
Group Claim	<code>groups</code>

Okta Setup Notes

⚠ Important Configuration:

In your Okta Application's **General Settings**, you must whitelist your URLs:

- **Sign-in redirect URIs:** Add your full Redirect URI (e.g., `http://localhost:8090/`).
- **Sign-out redirect URIs:** Add the URL you want users sent to after logout (e.g., `http://localhost:8090/`).

Getting Group Claims:

To include groups in the token, go to your Okta Application's **Sign On** tab, edit the "OpenID Connect ID Token" section, and configure a **Groups claim filter**.

Firewall / 403 Errors:

If you get connection errors, you may need to add your Redirect URI to the trusted list under **Security > API > Trusted Origins**.

⚙ Troubleshooting

400 Bad Request on Login or Logout

This almost always means the **Sign-in redirect URI** or **Sign-out redirect URI** is not correctly configured and whitelisted in your provider's application settings. The URL must match exactly what the application is sending.

Connection Error / 403 Forbidden / IDX20803

Your Identity Provider is blocking the request from your server. This is usually a firewall or security policy. In Okta, you must add your application's base URL (e.g., `http://localhost:8090`) to the trusted list under **Security > API > Trusted Origins**. Other providers may have similar "CORS" or "Web Origins" settings.

No Groups Returned

This can have several causes:

- The **Scope** in your configuration is missing the required scope for groups e.g., `groups`
- The user you are testing with is not a member of any groups in the Identity Provider.
- The provider is not configured to send the groups claim. In Okta, you must explicitly configure a **Groups claim filter** in the Application's "Sign On" settings to add the groups to the ID Token.
- The **Group Claim** name in your configuration does not match the claim name in the token e.g., your config says `groups` but the token contains `roles`

Licensing

Use this tab to [license Agent DVR for business use/ enable port forward remote access](#).

Do you have a license for Agent DVR and want to move it to a new computer? See [License Transfer](#). You can just delete the old license and it will let you add a new license for the new computer.

You can also purchase licenses in volume via Invoice. See [Volume Licensing](#).

Licensing via commandline

If you don't have access to Agent via the local network (for example you are using ProxMox or some other virtual environment) then you can license Agent DVR using the following commands. Access the computer using the terminal and go to the folder containing the Agent executable. Make sure Agent isn't running:

These commands should work on v5.9.3.0+

```
sudo systemctl stop AgentDVR.service
```

```
Agent show-id
```

This will display the Unique ID you need to license agent or transfer your license.

```
Agent license "LICENSE-GOES-HERE"
```

Call this with your license and restart Agent to apply.

```
sudo systemctl start AgentDVR.service
```

to restart the Agent DVR service.

For older versions:

```
sudo systemctl stop AgentDVR.service
```

Get your Unique ID by editing Agent/Media/XML/config.xml and look for UniqueID. Agent will need to have been run at least once to generate this file.

License Agent and then copy the license text into a new (or existing) field in the same file:

```
<License>LICENSE-GOES-HERE</License>.
```

```
sudo systemctl start AgentDVR.service
```

to restart the Agent DVR service.

White Labelling

Once Agent DVR is [Licensed](#) you can white label it for your business or your clients using the options on the Whitelabel Options tab (requires a white-label license):

White labelling options apply to your own server UI not to our remote web platform

Product Name Set an alternate product name to appear at the top of the UI (max 6 characters)

Show Logo Upload a **logo** using the Server Menu - File Upload option and this will be displayed by clients whilst the web app loads.

Show Help Links Switch on or off help links in the app that take the user to our website.

Show Remote Show or hide links to our remote services and integrations.

Show Licensing Show or hide this licensing tab. Note that if this tab is hidden the only way to display it again is to stop the Agent DVR service, edit Media/XML/config.xml in the Agent DVR directory and set

ShowLicensing to "true" and then restart it.

About Text Set the text that is displayed when you click on the Information icon in the UI.

Local Server

These settings control the built-in web server that hosts the Agent DVR user interface. Change them to move the web server port, enable HTTPS or restrict who can connect.

Port: The local port used by Agent. Default is 8090.

WAN Port: If you have port forwarded Agent DVR then specify the External port here (used for mobile application connections).

SSL Port: The port for SSL connections to your server. Set to 0 to disable. Before setting this, please [read the guidelines](#).

SSL Only: Accept only SSL requests. Test that SSL is working first!

SSL Certificate: The certificate file for SSL connections.

SSL Password: The password for your SSL certificate.

Trusted Proxies: IP addresses of reverse proxies allowed to report the real client IP. Leave blank unless you run a proxy (e.g. nginx, Caddy, Cloudflare Tunnel) in front of Agent.

Bind to Interface: By default, Agent DVR monitors all interfaces. You can specify a particular network interface for monitoring here. If this setting disrupts access, you can revert to the default by setting BindInterface to '*' in Agent/Media/XML/config.xml.

Protect API: Enable basic authentication for API endpoints. Note that this may affect some integrations.

Access Timeout: Set a time limit for server access via permissions (in minutes). 0 for unlimited access.

Max Sessions: Limit the number of simultaneous web browser connections. Exceeding connections will be disconnected. Set to 0 for unlimited.

Enable ZeroConf: Enable the automatic network discovery service, which allows Agent DVR to be discovered by other applications including the mobile apps and the Windows tray app.

Block External Access: Check this option to completely block access from the remote web portal.

Turn Server

The TURN server is key to enabling remote access to your Agent DVR server and devices. It helps facilitate connections when direct peer-to-peer connections are not possible, such as when devices are behind NATs or firewalls.

Agent DVR comes with a built in TURN server and configures it and keeps it running automatically. You can also use your own TURN server if you have a [license for remote access](#).

STUN Servers: List of publicly available STUN servers to use when setting up connections.

TURN Server: Specify whether to use the inbuilt TURN server or a custom TURN server. Disabling the TURN server may break access.

TURN Address: The IP address to use for the TURN server. Leave blank for automatic.

TURN Port: The STUN/ TURN server port (default 3478).

TURN Server min port: Lower bound of the port range for TURN relay allocations. Default is 50000. Forwarding this range is recommended but usually not required, as relay traffic normally travels through the TURN port.

TURN Server max port: Upper bound of the port range for TURN relay allocations. Default is 50100. Forwarding this range is recommended but usually not required.

Use the **Custom TURN server** settings if you want to use an externally hosted TURN server for direct remote connections to Agent DVR. If you configure these options you'll need to set the TURN server mode above to **Custom**. You'll need to get these details from your provider. A license is required for remote access to Agent DVR.

User Interface

These options customize the Agent DVR interface, from default timestamps on video and date and time formats to which sections of the UI are available.

Limits

Max Alerts: The maximum number of alerts to store. When this limit is reached Agent will delete old alerts.

Views: The number of available views on the live screen.

Plans: The number of available plans on the floor plans screen.

Timestamp Defaults

The default timestamp style for cameras that use the global timestamp settings.

Formatter: The timestamp text. Example: {FPS},{RES},{0:G},{0:T},{NAME},{REC},{0:dd MMM yy}

Position: Where the timestamp appears on the video, or None to hide it.

Text Color / Back Color: The text and background colors of the timestamp.

Show Background: Draw a background behind the timestamp text.

Opacity: The opacity of the timestamp background.

Auto Font Size: Size the timestamp font automatically based on the video resolution, or uncheck to set a fixed **Font Size**.

Outline Color / Outline Size: Add an outline to the timestamp text.

Time Formats

Culture Code: Set the culture code for date formatting on timestamps (e.g., en-US for American English, fr-CA for Canadian French). See [this list](#) for more options.

Time Format: Choose the format for date and time display in the Agent DVR UI. Default is 12-hour format ("MMM DD YYYY h:mm:ss A"). For 24-hour format, use "YYYY-MM-DD H:mm:ss".

Time Format (small): Choose the format for small date display in the Agent DVR UI. Default is 12-hour format ("MMM DD h:mm A").

Date Format: Choose the date format

YYYY: 4-digit year '2019'

YY: 2-digit year '19'

MMMM: Full-length month 'June'

MMM: 3 character month 'Jun'

MM: Month of the year, zero-padded '06'

M: Month of the year '6'

DD: Day of the month, zero-padded '01'

D: Day of the month '1'

Do: Day of the month with numeric ordinal contraction '1st'

HH: hour of day from 0-24, zero-padded, '14'

H: hour of day from 0-24, '14'

hh: hour of day on 12-hour clock, zero-padded, '02'

h: hour of the day on 12 hour clock, '2'

mm: minute, zero-padded, '04'

m: minute, '4'

ss: second, zero-padded

s: second

A: 'AM' or 'PM'

a: 'am' or 'pm'

Player Defaults

Skip to Motion: When playing back recordings skip to the first instance of movement.

Tags

File Tags: The set of available tags for tagging recordings. This is automatically populated as you tag recordings or you can edit it here.

Image Tags: The set of available tags for tagging images. This is automatically populated as you tag images or you can edit it here.

Sections

Check the available viewers to display in the UI. Uncheck any sections you wish to hide. Check the "Admin has all" button to enable all sections for administrators.

Logging

Control how much detail Agent DVR writes to its logs. Turn up the log level or the component options below when troubleshooting an issue, then turn them back down to keep log files manageable.

Max Log Size: Determines the maximum number of entries that can be held in the log queue.

Log Level: Choose how much detail to log, from None up to Debug.

WebRTC: Enables logging of WebRTC connections, useful for debugging live view issues.

ONVIF: Enables debug logging for ONVIF devices.

FFMPEG Log Level: Adjust the debug output level for ffmpeg. Caution: The Trace setting can rapidly fill your logs and should be used only briefly for specific debugging purposes.

SignalR Logging: Enables logging of communications with the SignalR server, useful for detailed debugging.

Syslog Logging

Agent DVR can stream its logs to a syslog server (v6.2.6.0+). This can be useful for monitoring and debugging. You can configure the server to send logs to in [Logging](#).

Enabled: Toggle to turn Syslog Logging on or off.

Server: Specify the server address eg: logs1.papertrailapp.com

Port: The port to use

Category: Select the Syslog Category (or Facility).

MQTT

MQTT, a key IoT messaging protocol, facilitates seamless integration of devices and services across your network. Configure MQTT settings here to enable [MQTT Events](#) on your devices, or use [Actions](#) for sending custom messages to the MQTT server. Also, Agent DVR can be configured to react to MQTT commands. For more details, see [MQTT](#).

Enabled: Toggle to activate or deactivate MQTT.

Server: Input the IP address of your MQTT Server.

Port: Specify the port used by your MQTT Server (default is 1883).

Home Assistant Discovery: Advertise devices that have MQTT Events enabled to Home Assistant, so they appear there automatically with sensors and switches. See [Home Assistant](#) for details.

Check Interval: Set the interval in seconds for Agent DVR to send keep-alive messages, ensuring a stable connection.

Protocol: Choose the connection protocol, either None or TLS.

LWT delay: Sends an offline message to the status topic after a delay (in seconds, 0 to disable).

Validate Certificate: Validate the server's TLS certificate. Leave this off for self-signed certificates.

Protocol Version: The MQTT protocol version to use. Leave on Default unless your server requires a specific version.

QoS: Quality of Service level. Refer to your MQTT server documentation for details.

Client ID: Your MQTT client ID. Leave blank to generate automatically.

Username: Your MQTT server username.

Password: Your MQTT server password.

Discovery Prefix: The topic prefix used for Home Assistant discovery messages (default is homeassistant). Only change this if you have changed the discovery prefix in Home Assistant's MQTT integration.

Send Stats: Enable this to allow Agent DVR to send statistics to MQTT, such as CPU usage, memory usage, and drive usage.

NDI

NDI (Network Device Interface) simplifies the process of accessing IP video sources, offering built-in discovery features. Many cameras and video surveillance systems are already NDI-ready, making integration with Agent DVR effortless. For more information about NDI technology and compatible devices, visit [ndi.tv](#)[↗]. Agent DVR supports NDI sources with video and audio capabilities, as well as PTZ control via NDI.

Groups: Here, you can add NDI groups if applicable. Enter each group on a new line.

Extra IPs: Add specific NDI IP addresses for device scanning. Each IP should be on a new line.

Show local devices: Toggle this option to decide whether NDI devices on the local computer (which is running Agent DVR) should be displayed in the list.

ONVIF

Agent DVR utilizes keywords in ONVIF event XML packets to identify motion events. Since these packets can vary across different camera models, we provide an option for you to add custom event XML from your camera to trigger ONVIF events. This feature is particularly useful if you encounter issues with standard ONVIF event detection.

Detect XML: Insert the specific ONVIF XML event packet from your camera here.

Event Logging: Enable this to log all incoming XML from the camera, which is helpful for debugging purposes. Access these logs at /logs.html on your local server.

For instance, if you notice entries in the logs at /logs.html like:

```
Ignored ONVIF event: <tt:Source xmlns:tt="http://www.onvif.org/ver10/schema"><tt:SimpleItem
Name="VideoSource" Value="V_SRC_000" /><tt:SimpleItem Name="Rule" Value="MyMotionDetectorRule"
/></tt:Source><tt:Data xmlns:tt="http://www.onvif.org/ver10/schema"><tt:SimpleItem Name="State"
Value="true" /></tt:Data>
```

And Agent DVR is not recognizing it as a motion event, you can add the following to the Detect XML field:

```
<tt:SimpleItem Name="Rule" Value="MyMotionDetectorRule" /></tt:Source><tt:Data
xmlns:tt="http://www.onvif.org/ver10/schema"><tt:SimpleItem Name="State" Value="true" />
</tt:Data>
```

Agent DVR will then interpret events containing this specific text as motion events.

Playback

These settings govern how Agent DVR renders and delivers video to the web browser and through the API.

Max Stream Size: Sets the highest resolution for streaming to the web client. Higher resolutions can significantly increase CPU usage.

High DPI: Streams video at the full resolution of high-density displays (4K monitors, Macs, phones) for a sharper picture, at the cost of more encoding load. Stream size limits still apply.

Disabled: Standard resolution (default).

GPU: Full resolution only for viewers using GPU encoding, where the extra load is negligible.

Enabled: Full resolution for all viewers. Increases CPU usage with software encoding.

Default Font: The default font used for rendering text like timestamps onto video.
Video FPS: The maximum frames per second (framerate) for video sent to the web browser.
Fill Mode: Choose whether the camera image fills the available space (Fill) or keeps its original aspect ratio (Center).
Use GPU: Enable GPU usage for decoding saved video files.
Use GPU for web client: Use the GPU to encode video streamed to web clients. Requires Force H264.
JPEG Quality: The default quality setting for encoding jpeg images. Higher values can use more CPU and storage.

Max MJPEG Size: The maximum MJPEG stream size Agent DVR will generate via the API.
Default MJPEG Size: The default MJPEG stream size Agent DVR will generate via the API, used when no size parameter is specified.
Force H264: Use H264 for streaming video to clients. Uncheck this if the live view stops working.
Default GPU Device: Choose the default GPU device to use when you have more than one.
Default GPU Decoder *: Choose the preferred hardware decoder. Agent DVR will try other options if the preferred one fails.
Default Record Codec *: Choose the preferred hardware encoder. Agent DVR will use alternative options if necessary.
AI Shard Size: The maximum number of devices per inference session in the internal AI system. Lower values improve stability under high concurrency at the cost of additional GPU memory. Changes apply after restart.
High Performance Resizing: Use a basic resizing algorithm to reduce CPU usage. This is fast but can result in jagged lines in images.
Resize files for playback: Resize recorded files when playing them back to reduce load. Uncheck this for full resolution photo support during playback.

* Note that GPU encoding and decoding depend on your computer's hardware compatibility, drivers, and FFmpeg library support. To check if Agent DVR is utilizing your hardware devices, start a recording and view the logs at /logs.html in the local client. Agent DVR should revert to CPU-based encoding if GPU encoding is unsuccessful.

RTMP Servers

Agent DVR offers the capability to stream video to RTMP endpoints like Twitch and YouTube, enabling you to broadcast or embed the stream on your website. For more information on how to embed these streams, please refer to [RTMP Settings](#).

RTMP streaming can be activated from the Server  menu or scheduled to start and stop automatically using a [device scheduler](#).

URL: The RTMP endpoint to publish video to, typically in the format of <code>rtmp://a.rtmp.youtube.com/live2</code> .
Stream Key: Refer to the embedding guide linked above for instructions on obtaining your stream key.
Size: Select a resolution for your broadcast. Remember, higher resolutions consume more bandwidth and CPU resources.
Quality: Adjust the basic quality setting. The default is 8. Lower values mean reduced quality but also lower bandwidth usage.
Frame Rate: Set your desired frame rate for the video. The default is 15 frames per second.
Codec: Choose the encoder used for the stream. GPU encoders reduce CPU usage.
Include Audio: Include audio in your stream. If disabled, Agent DVR will create a dummy silent audio track.
Max Duration: Set the maximum streaming duration in seconds. Agent DVR will stop streaming after this period. Enter 0 for continuous streaming.
Stream at startup: Start streaming to this server when Agent DVR starts, using the last device streamed to it.

Security

These settings are designed to manage how Agent DVR handles the arming and disarming of the system, either through the UI lock icon or via integrations/API.

Arm Delay: The time delay in seconds from when you click the Arm icon (the lock icon at the top left in Agent) to when Agent DVR actually activates alerts.
Disarm Code: This code is used to disarm Agent DVR, applicable in tools like Alexa . The default code is 1234 .
Arm Profile: Choose a profile to automatically apply when the system is armed (using the lock icon in the top left corner of the UI).
Disarm Profile: Choose a profile to automatically apply when the system is disarmed (using the unlock icon in the top left corner of the UI).

SMTP

Use these settings to send email alerts from Agent DVR through your own mail server. You have the option to use an [ispyconnect.com](#) subscription for email alerts or configure your own SMTP server. **Remember, to send emails, you need to [set up an action for email sending](#).** For help with any issues, refer to [SMTP Troubleshooting](#).

Use SMTP: Enable this to use your own SMTP server for messaging.

Username: Your SMTP server username.

Password: Your SMTP server password.

From Address: The email address to send from, for example, you@yourdomain.com.

Server: The IP or web address of your SMTP server.

Port: The port your SMTP server uses. The default is 25.

Use SSL: Enable this option for SMTP communication over SSL.

Alert Template: Set the default Subject and Message for alert emails.

Validate Certificate: Validate the server's SSL certificate. Leave this off for self-signed certificates.

Send full size images: Check this to send images in full resolution instead of sending resized, smaller versions.

Embed Images: Show images in the mail body. This can cause duplicate images in some email clients.

Storage

These options help with disk management for your recordings: get an email warning before a storage location fills up and protect important footage from automatic deletion.

Configure: See [Storage Settings](#)

Storage Email Address: Provide an email address to receive alerts when storage limits are reached. This requires SMTP settings or a subscription.

Notify Trigger: Set the percentage of used space in the storage location to trigger an email notification. Note that this refers to the allocated max space, not the free space on the drive.

Email Interval: Determine the frequency of storage warning emails, measured in hours.

Storage Interval: Adjust the frequency of [Storage Management](#) operations by Agent DVR.

Auto Lock Tags Automatically lock recordings with specified tags to prevent accidental deletion or removal by storage management. To delete these recordings, you will need to unlock them in the UI.

Users

For information on remote user permissions, please refer to [Remote Permissions](#).

Note: The free version of Agent DVR allows for one admin user to be added.

With an appropriate [license](#), you can add multiple users with different permissions to your local Agent DVR server, for example to give family members or a security team their own logins with limited access.

To add users, go to Server Settings and access the Users tab.

Username: This is the username for local server login (it is different from your ispyconnect.com username).

Password: Create a password for the local account.

Groups: Assign or create groups for the user. Groups function similarly to remote user permissions, but there's no need to include the server name. To restrict access:

Assign a group name in the device settings under the General tab (e.g., "outside").

In the user's permissions, add the group "outside" to restrict their access to devices labeled as such.

Assign a group name to all other devices - if a device is not assigned to a group it will be visible to everybody.

Is Admin: Grants full access to all features and settings. If the user is an admin, the 'Read Only' setting below is disregarded.

PTZ: Allows PTZ (Pan-Tilt-Zoom) control access.

Own Settings: The user can save their own views, filters, floorplans and key mappings. If this is unchecked they will use the admin accounts configuration.

Read Only: Restricts the user from modifying device settings.

Downloads: Permits the user to download recordings.

Audio: Allows the user to listen to live and recorded audio.

Talk: Enables the user to use talk-back features.

Controls: Allows the user to use device controls like record and photo. Only applies if Read Only is checked.

Content: Allows access to recordings and photos.

Forgot the Admin Login?

If you forget the admin login and are locked out of Agent DVR, you can reset it by following these steps:

Stop the Agent DVR service, if it's running.

Open a console window: Click Start, type "cmd", right-click on "Command Prompt" and select "Run as administrator".

Navigate to the Agent DVR directory, typically "cd C:\Program Files\Agent".

Reset the local password by typing "Agent.exe reset-local-login" on Windows or "dotnet Agent.dll reset-local-login" on macOS and Linux.

Restart the Agent DVR service using the same method as for stopping it.

You can automate the adding of new users using [LDAP](#) or [OAuth2](#).

Session Management

From the Server menu, click on Session Management to access these controls. This is only visible to administrators.

This displays the usernames and IP addresses of recent logins to the server. You can force disconnect specific sessions from here.

The Session Log

From version 6.2.8.0, Agent DVR also keeps a plain text audit log of session activity in **sessionlog.txt**, located in the Media folder (on Windows this is typically C:\Program Files\Agent\Media). This covers both local user accounts and remote users connecting through the website - each entry records whether the session was local or remote.

The session log records:

User connections and disconnections, with the username, IP address and session ID.
Playback of recordings, including timeline playback.
Downloads and streaming of recorded files.

When the log file reaches 10MB it is renamed with a timestamp and a new log file is started, so recent history is always available without the file growing indefinitely.

Actions

About

Actions in Agent DVR are responses to specific events, like camera/AI alerts or device disconnections. Use them to respond automatically, for example sounding an alarm, switching on lights via a smart plug URL, or triggering recording on another camera. To access and configure Actions, edit a device and navigate to the **Actions** section in the menu.

Click 'Add' to create a new action. You will be presented with a configuration screen similar to the images below:

Action Configuration



☒ On

Name person recognized

Enter a name (optional)

If Alert

With tag person

Used

alert bicycle bus car detected manual manual alert person truck

Tags to filter on eg: dog,cat or person (optional). AI tags use the language in server settings

Rule Or

To apply to tag filtering, example: person AND vehicle, or person OR vehicle

In Zones

Available (click to select):

1 2 3 4 5 6 7 8 9

Select zones to filter by (AI or tracking events only). Selected zones are BIG

Repeat Timeout

0

Time in seconds before this can repeat

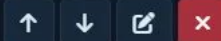
Tasks

Tasks to perform when this action is triggered

Sound: doorbell.wav



Send Push Notification: {TIME} {TAGS} {NAME} (Alert)

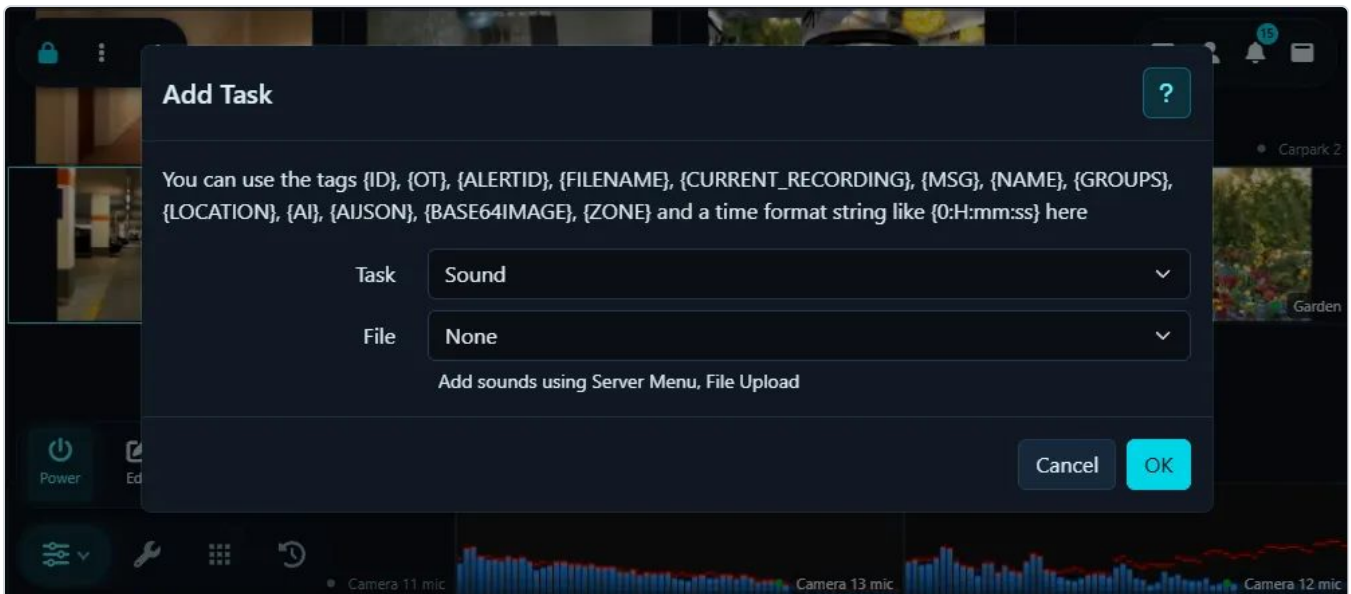


Add Task



Cancel

OK



There is a wide range of events that can trigger actions. Multiple actions can be associated with each event, and you can incorporate various tags within these actions to create dynamic responses.

Configuring an Action

Active: Toggle this to activate or deactivate the action. Alternatively, you can use the [Schedule](#) and the [API](#) with commands like `actionOn`, `actionOff`, and `actionRun`, using the ID shown above.

Name: An optional name for the action.

If: Select an [available event](#) (see below).

With tag: (AI Events). This is mainly used with [AI events](#). For instance, if you select **AI: Object Found** and enter **cat** here, the action will trigger only when a cat is detected. Note that the tag matches based on the language selected in Server Settings - General.

Rule: Choose whether multiple tags must all match (AND) or any can match (OR).

In Zones: (AI Events). Specify motion zones (from the motion detection tab) to filter the detected objects. For example, selecting zone **1** and **cat** as the tag, the action will only trigger when a cat is detected in zone 1. Leave blank to include all zones.

Repeat Timeout: This suppresses the event if it has been raised within this interval and also resets the timer. For example, with 'Vehicle detected' as the trigger and a 30-second timeout, an alert will be sent once, with subsequent alerts paused until there's a 30-second gap in the detected traffic.

Add Task: Click to add a task. You can assign multiple tasks to an action (v4.5.5.0+).

Available Actions

Actions can respond to a wide range of system, device and AI events. The events you can set up actions for are:

AI Server Down (AI Server has returned an error - event will fire after requests have failed 3 times and not recur until the server is back online)
AI Server Up (AI Server has exited the error state)
AI: Ask AI Positive Result (It found an object you were looking for)
AI: Ask AI Result (fires on any Ask AI response, positive or not)
AI: Describe Response Received (An image was described by AI - the description is in {MESSAGE} and {AIJSON} tags)
AI: Face Recognized
AI: Face Not Recognized
AI: License Plate Recognized
AI: License Plate Not Recognized
AI: Loiter Detected
AI: Object Found
AI: Object Not Found
AI: Sound Recognized (mics only)
Alert
Alert Finished
Call URL Response Received - This is triggered by the response you get when a "Call URL" task runs, letting you respond to it with other tasks.
Manual Alert
Motion Detected
Motion Finished
None - use this if you want to trigger the action yourself with the "Action: Run" command on the schedule
ONVIF Event ON - use this to for example start and stop recording based on ONVIF logical state updates (requires the motion detector type to be set to ONVIF)
ONVIF Event OFF
ONVIF Event Received (fires on any ONVIF event from the camera)
Photo Taken
PTZ Preset Applied

Reconnect Failed
Recording Failed
Recording Finished
Recording Started
Source Disconnected
Source Reconnected
Source Covered/ Tampered
Switch Device Off
Switch Device On
System: Armed
System: Disarmed
System: No UI Connected - when the last UI session closes
System: Profile Applied
System: UI Connected - when someone opens a browser to view your system
System: UI Disconnected - when the session is closed (happens roughly a minute after the browser disconnects)
Timelapse Started
Timelapse Stopped

Any plugin events and [custom tasks](#) you have added also appear at the end of this list.

Detecting Loitering

To detect loitering (people or objects staying in one place for a certain time period) you'll need to configure the following:

Set up an AI server in server settings
Add an Action for AI: Loiter Detected
Set the tag you are looking for - this would usually be person but you could use car to detect cars parked in an area for too long or suitcase for left luggage or a cat sitting on your sofa. You can use multiple tags here for example car,bus,truck . For a list of available objects to find see the classes list in object recognition when you edit the camera.
Specify the zones you want to look for the object in. Use the detector tab to draw out motion zones.
Specify the number of seconds you will tolerate the detected object being in the zone for.

Add Tasks to perform when the conditions are met.

Note: The loiter detector uses the settings from the object recognition settings like check corners and overlay

Adding Custom Events

Beyond the pre-set events, you can create custom events by adding [Tasks](#). Once a task is created, it will appear in the **Events** list. You can then set up an **Action** to respond to this task. Tasks can be triggered from the Live page in the UI (by selecting a camera and then clicking the task icon at the bottom left) or through the **Action: Run** command found in the [Schedule](#).

Custom Tasks

Tasks are commands you can attach to devices to manually trigger [Actions](#). Actions can call third party APIs to perform tasks like open doors, turn lights on, play sounds etc. To add, delete and execute tasks select a device on the Live page and click on the task icon .

Setting up a task:

Enter some text to describe the task, for example "Turn Lights On" and click the + button. Click OK

Click to edit the device using the edit icon . Select the Actions panel in the editor using the menu at top right.

Add an action. Select the "If" condition to be the task you just created (tasks are shown at the bottom of the list of available actions) and then configure what you want the task to do.

Click OK

You can now manually trigger this action from the live view by clicking on the tasks button and clicking the Go arrow button next to the task.

You can also trigger tasks via the [Agent DVR API](#).

Available Tasks

Tasks are what an action does when its event fires, from sending an email alert or push notification to controlling recording on other devices. The list of available tasks you can perform (under **Then**) is:

Alert - triggers an alert on the device

Beep - plays a beep through the Agent DVR computer's speaker

Call URL - call any URL with an optional Auth token. You can call the [Agent DVR API](#) here, or send alerts to Discord, Slack, ntfy and similar services (see [Webhooks](#)). If you have [Protect API](#) checked in server settings you will need to provide an authorization header. To do this you will need to add a [User Account](#) via Server Settings and enter a Basic Auth Header value:

Generate

BASIC YWRtaW46YWRtaW4=

Execute Command

Also see [commands](#)

To add your own commands/ scripts you can add .bat or .sh files into the Commands directory. You can then pass parameters into the batch file. For example, to copy all photos to the root of the D drive:

Create a plain text file containing:

```
copy %1 D:\
```

Save it as copyPhoto.bat (on linux use .sh - you will need to make this file executable using chmod +x) to Agent/Commands

Then add an action:

if: "Photo Taken"

then: "Execute Command"

File: copyPhoto

Parameters: "{FILENAME}"

Cloud upload current recording - upload the current recording to the device's [cloud provider](#)

Delay - pause before running the next task

Enable / Disable Ask AI

Enable / Disable Facial Recognition

Enable / Disable LPR

Enable / Disable Object Recognition

Enable / Disable Patrol On (PTZ patrol on a device)

Enable / Disable Sound Recognition

FTP upload current recording - upload the current recording to the device's [FTP server](#)

Log - write a message to the Agent DVR log

MQTT - send an MQTT message

MQTT Image - send a raw live image in jpeg bytes to a topic

Network Message

PTZ Command - move the camera to a preset or run a PTZ command

Send Email (with optional image attachments)
Send Email with Video (specify duration - this includes a buffer of the event). v4.9.8.0+
Send Push Notification
Send SMS
Set Motion Detector Area (select the Area you defined on the Detector)
Show Message - displays message on viewing web browsers
Sound (on Agent DVR computer)
Sound (through camera)
Sound (through web browser)

Due to browser security this requires interaction with the web page first (e.g. clicking on something). To work around this in chrome go to <chrome://settings/content/sound> and add the address of your server (or our website if you are using the remote portal) to the Allowed List.

Start Recording On (some device) - will record until stopped.
Start RTMP Streaming
Start Timelapse On (some device)
Stop Recording On (some device)
Stop RTMP Streaming
Stop Timelapse On (some device)
Switch Device On
Switch Device Off
System: Apply Profile - switch Profile
System: Arm
System: Disarm
Tag Recording - add a tag to the current recording
Take Photo On (some device)
Text to Speech (on Agent DVR computer - requires an iSpyConnect.com account as text is rendered via webservice calls)
Text to Speech (through web browser)

Due to browser security this requires interaction with the web page first (e.g. clicking on something)

Text to Speech (through camera)

Trigger Adaptive Encode On (another device)

Trigger Alert On (another device)

Trigger Ask AI (another device)

Trigger Audio Recognition (another device)

Trigger Detect On (another device)

Trigger Face Recognition (another device)

Trigger LPR (another device)

Trigger Object Recognition (another device)

Trigger Recording (with timeout) (another device). This will record up to the trigger recording timeout setting on the Recording tab. This timeout resets with every trigger recording action call.

UI: Change View - switch connected UIs to a different view

Using Tags

Tags in the **Then** fields of Agent DVR actions allow you to create dynamic responses. It's important to note that some tags are context-specific. For instance, {FILENAME} isn't available for Alert Events, and {AI} isn't available if the event wasn't generated by an AI server.

{ID}: The object ID, visible at the top left of the editor when editing a camera or microphone in Agent.

{OT}: The object type ID. 1 for Microphone, 2 for Camera.

{FILENAME}: The filename. Applicable to events like Recording Started, Recording Finished, and Snapshot Taken. It's the full local path to the file.

{CURRENT_RECORDING}: The filename of the current recording. Full local path to the file. (v5.0.6.0+)

{MESSAGE}: The name of the event that triggered the action, e.g., "Manual Alert".

{EVENT}: The event type.

{NAME}: The name of the device (found on the General tab).

{GROUPS}: The groups to which the device belongs (found on the General tab).

{SERVER}: The server name (from Server Settings).

{ALERTID}: The ID of the alert (-1 if there is no associated alert).

{ALERTCOUNT}: The device's alert count.

{TIME} and {DATE}: The current time and date on the server.

{RECORDED}: "REC" if the device is recording, otherwise empty.

{TAGS}: The tags associated with the event.

{PLUGIN}: The message from a plugin event.

{LOCATION}: The location of the camera (found on the General tab).

{LEVEL} and {DB}: The motion or audio level. {DB} is the decibel level for audio devices. Measured when the action runs. (v4.3.7.0+)

{AI}: A comma-separated list of detected objects from [AI](#), plates from [LPR](#), or detected faces from [Facial Recognition](#).

{AIJSON}: JSON data returned from AI or LPR.

{ZONE}: The zone that triggered the action (empty if not using AI or a CSV list for multiple zones like 1,2,3).

{BASE64IMAGE}: Live image data URL. It's the raw base64 encoded bytes, so format as needed e.g.,

```
p=data:image/jpeg;base64,{BASE64IMAGE}
```

(Available v4.5.9.0+). Live image resized to 640px width.

{BASE64IMAGE-LG}: Live image data URL. It's the raw base64 encoded bytes, so format as needed e.g.,

```
p=data:image/jpeg;base64,{BASE64IMAGE-LG}
```

(Available v6.0.8.0+). Live image resized to 1280px width.

{BASE64IMAGE-NATIVE}: Live image data URL. It's the raw base64 encoded bytes, so format as needed e.g.,

```
p=data:image/jpeg;base64,{BASE64IMAGE-NATIVE}
```

(Available v6.0.8.0+). Native live image.

For example, with an event **AI: Face Recognized**, a **Then** task **Text to Speech** with the text

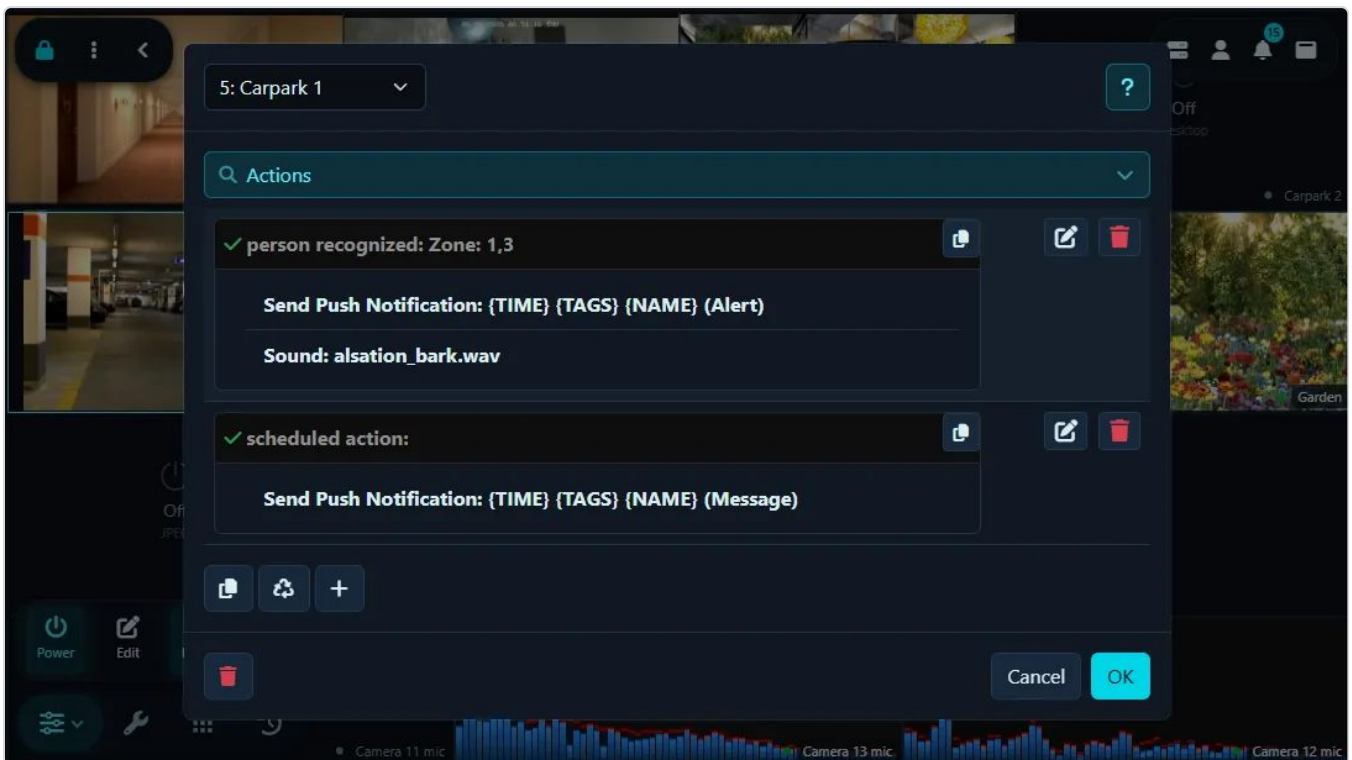
```
Hello {AI}
```

will greet each recognized person by name.

Note: If you use {BASE64IMAGE} tags with a file related event like "Photo Taken" it will use the full size image from the file. Otherwise it will resize the current live view image.

Be cautious with trigger alerts on actions to avoid cyclical routes, for instance an alert on Camera 1 triggers an alert on Camera 2, which in turn triggers an alert on Camera 1.

Once an action is added, the table control displays a summary of your actions. A green tick indicates an active action.



You can use the [scheduler](#) to enable/disable actions or trigger an action. For example, you might schedule an action to send an email with two images at a specific time.

Schedule Entry?

On

TypeTime

For sunrise/ sunset, set a location on the General tab

Offset0

Time offset if using sunrise or sunset (minutes)

Time08:00 AM

local time at Agent DVR Server is 16:51:56

Schedule Mode

Set a specific date or select days for a weekly schedule. Clear the date to use days instead

Date

dd/mm/yyyy

Or

Days

Sun

Mon

Tue

Wed

Thu

Fri

Sat

Command

CommandAction: RUN

Actionscheduled action (1 Task)

Applies to Action On, Off and Run commands

Cancel

OK

In this example, an action was added to send an email with 2 images, set to None event. Then a schedule entry was created to execute that action at 8AM on Sunday and Saturday.

Investigations

About

Investigations (v6.0.5.0+) let you collect and manage related video, audio and image files in one place, for example to gather all the evidence relating to an incident.

Accessing the Investigations Interface

The Investigations user interface (UI) can be accessed through the server menu. This centralized interface allows you to efficiently gather and organize video, audio, and image files in one location.

Key Features of Investigations

- **Data Collection:** Seamlessly collect video, audio, and image files.
- **Commenting:** Add comments to provide context and insights.
- **Detail Tracking:** Monitor and track essential details related to each investigation.
- **Data Export:** Download all collected data as a comprehensive ZIP file.

Creating a New Investigation

To initiate a new investigation:

1. Click the **plus (+)** button.
2. Enter a name for the investigation.
3. Add an initial comment to provide context.
4. Click **OK** to create the investigation.

Return to this view later to review the media you have added, download individual files, or remove content as needed.

Adding Media to an Investigation

Enhance your investigation by adding relevant media files:

- Navigate to the **Files** or **Photos** view.
- Enter edit mode by clicking the edit icon.
- Select the desired content to add.
- Click the **plus (+)** button in the toolbar to include the selected media. Add a comment and click **OK**.

Additionally, you can add files to an investigation while they are playing back or extract a specific section from a file using the **Cut** tool and add it directly to the investigation via the new UI.

Downloading Investigations

Once you have gathered all necessary media and details, you can download the entire investigation as a ZIP file for easy sharing and archival purposes. Alternatively, you can edit the investigation to download specific files.

Upon completion of an investigation, you have the option to either delete it (note that deleting an investigation will **not** remove the captured media) or disable it by toggling the On/Off switch in the editor to remove it from the UI options.

Alerts

About

Agent DVR uses [motion detection](#) or [AI](#) to generate alerts. To access and configure Alerts settings, edit a device and select **Alerts** in the menu.

Alerts initiate an "Alert" [Action](#), allowing you to execute tasks like sending an email, sounding an alarm, calling a URL, etc., when Agent DVR raises Alerts.

Agent DVR can record video based on Alert or Motion Detection. To minimize unnecessary recordings, set the **Recording Mode** on the Recording tab to "Alert" and then configure how Agent DVR raises alerts using the settings below.

Agent DVR features a master switch for arming and disarming the system.

The top left icon displays a  symbol when Agent DVR is armed and a  symbol when Agent DVR is disarmed. Click the symbol to toggle between these states.

If Agent DVR is disarmed, no alerts will be triggered. Additionally, a warning about Agent DVR being disarmed will be displayed upon login.

Tip: If you are using trip wires to trigger alerts and they are not being activated, ensure that the [Alert](#) setting is not configured to "None".

Alert Settings

These settings control when a device raises an alert and how often alerts can repeat.

Enabled: Toggle to enable or disable Alerts for a device.

Mode: Choose from **Detected**, **Not Detected**, or **Actions Only** (v4.5.0.0+). Trigger an alert when motion is detected, or conversely, when no movement is detected (useful for monitoring machinery). Use **Actions Only** to trigger alerts exclusively via actions. See [Alert Filtering](#) for more details.

Detection Delay: The time in seconds before an alert is triggered after detection.

Not detected alert delay: The time in seconds before an alert is triggered if no motion is detected.

Reset Mode: Choose how to manage alert resets (based on an interval or an idle timeout).

Interval: The minimum time in seconds to use for the alert reset mode:

Interval: If set to 60, alerts will be suppressed for 1 minute.

Idle Timeout: If set to 60, alerts will be suppressed until 1 minute of inactivity has elapsed.

Alert Group: Specify a group for raising alerts. Alerts in a group can trigger recording on all devices within that group. The group's interval setting overrides the device's minimum interval. Group Alert and Group Detect modes are available under the [Recording](#) tab.

Messaging: Enable or disable messaging actions like Email or SMS (configured on the [Actions](#) tab). [See our wizard for formatting your number](#)

Describe Alerts: Use AI to describe alert images - see [Describe Alerts](#).

Prompt: The prompt sent to the AI along with the alert images - see [Describe Alerts](#).

Video Previews: Generate a looping video preview of the recording when an alert is viewed - see [Alert Display](#). Switch this off if you review large numbers of alerts quickly and just want the alert image on its own.

Describe Alerts

Describe Alerts uses AI to write a short description of what triggered an alert. Agent sends a few frames from the moment of the event to your AI provider and stores the reply with the alert. The description also appears in [push notifications](#) via the {AI} template tag, so instead of "Motion detected" your phone shows something like "A person is carrying a package to the front door".

Carpark 2 Manual Alert (manual, person)

Aug 09 11:53 AM



Did we get this right? 

1. person 92%



Ahoy, ye hearties! A jolly fellow from the Domino's crew be holdin' a grand stack o' fresh grub, lookin' proud as a captain with his treasure! He's got a mighty thumbs-up and a grin that says, 'Here be the finest scan for hungry bellies!' Aye, a true bounty for the taking!

OK

Describe Alerts: Check this to describe alert images. It uses the AI provider configured in Server Settings - AI; [Ask AI](#) does not need to be enabled on the camera. If no provider is configured Agent shows a warning with a button that opens the Gemini setup dialog - Gemini has a free usage tier that covers typical use and the dialog links to where you can get a free API key.

Prompt: The prompt sent to the AI with the images. The default asks for a KEYWORDS line (used to tag the alert - see Reply keywords below) followed by a one sentence description of the activity, focused on people, vehicles and animals, with a brief note when it looks like a false trigger (insects, rain, shadows). You can have some fun with this though, for example "Describe what is happening in pirate speak".

AI Frames (Advanced): How many frames to send with each request (1 to 8, default 3). Agent samples frames a second apart ending at the moment of the alert, so more frames show the AI more of the event. Fewer frames are cheaper on paid API keys and faster on local AI servers. Note that on free tiers the daily request limit counts requests, not frames - lowering this does not make the daily cap go further. If the provider rate limits your API key, Agent logs a warning and shows a notice in the camera editor.

Reply keywords

You can tell the AI to reply with a keyword and Agent will act on it. Keywords are matched at the start of the reply, case insensitive. The description is always stored with the alert in the UI so you can see what the AI decided.

KEYWORDS: - a first line like "KEYWORDS: person, package" is stripped from the description and added to the alert's tags. Recognized words: person, vehicle, animal, package, fire, smoke, nothing (anything else is ignored). Tagged alerts work with tag filtering and search just like object detection tags. The default prompt asks for this.

unimportant - the description is left out of the push notification text. The alert and notification still fire.

Describe never suppresses alerts or notifications - it only annotates them. To have AI decide whether an alert fires at all (for example, only alert when a person is present), set the alert **Mode** to [AI Trigger](#) and use the **Look for** field on the AI tab. Combined with recording on detect, that gives you "record all motion but only alert on real activity".

Example prompts

Security (default):

On the first line reply with KEYWORDS: followed by any of these that apply: person, vehicle, animal, package, fire, smoke, nothing. On the next line, in one short sentence, describe the activity for a security notification, focusing on any people, vehicles or animals. If it looks like a false trigger (an insect, rain, headlights or shadows) just say so briefly.

Quiet notifications:

In one short sentence describe any people, vehicles or animals. If nothing important is happening reply with just the word unimportant.

Deliveries:

In one short sentence describe any deliveries or people approaching the door. If nothing is being delivered and no one is approaching reply with just the word unimportant.

Pets:

In one short sentence describe what any animals in view are doing.

Fun:

Describe what is happening in pirate speak.

Once alerts are being described you can integrate the results with the [Actions](#) system using the **AI: Describe Response Received** event. You can use {MESSAGE} and {AIJSON} in tasks from this action for other integrations.

Push Alerts

Push alerts can push real-time notifications to your mobile devices (iOS/ Android) via our mobile applications. See [mobile push alerts](#)

On: Switch on or off Push Alerts.

Alert Template: The text of the notification. You can use [tags](#) like {NAME} and {TAGS} here. {AI} adds the [Describe Alerts](#) description, so notifications read like "Person carrying a package at the front door".

Push Video: Generate and push a short video notification (iOS/ Telegram only).

Include Audio: Include audio in the generated clip (iOS/ Telegram only).

Note: Push alerts use our web services so are subscription only.

Alert Filtering

See [Alert Filtering](#)

Manual Alerts

You have the option to trigger alerts manually for individual devices. To initiate a manual alert, go to the [Live](#) view, select the desired device, and then click on the  icon located at the bottom left of the screen.

These manual alerts will activate recordings if the device's recording mode is set to Alert. To associate [actions](#) with a manual alert, you should use the "Manual Alert" event rather than the standard "Alert" event.

Alerts Summary

As Agent DVR generates alerts, or as you trigger manual alerts, you'll see a counter increase at the top right of the Agent DVR UI. This is the system alert counter. Clicking on it displays a summary of alert events:

14

Off
JPEG

Off
Camera

KRYTON

Carpark 1

Aug 06 3:48 PM manual

Carpark 2

Aug 05 2:40 PM

Office Exterior 1

Aug 05 9:02 AM manual

Carpark 2

Aug 04 8:52 AM

Carpark 2

Aug 03 8:25 AM

Carpark 2

Aug 03 8:04 AM

Carpark 2

Jul 30 9:49 AM

Carpark 2

Jul 30 9:47 AM

Carpark 2

Jul 29 11:40 AM

Carpark 2

Jul 29 11:01 AM

Carpark 2

Jul 29 10:57 AM

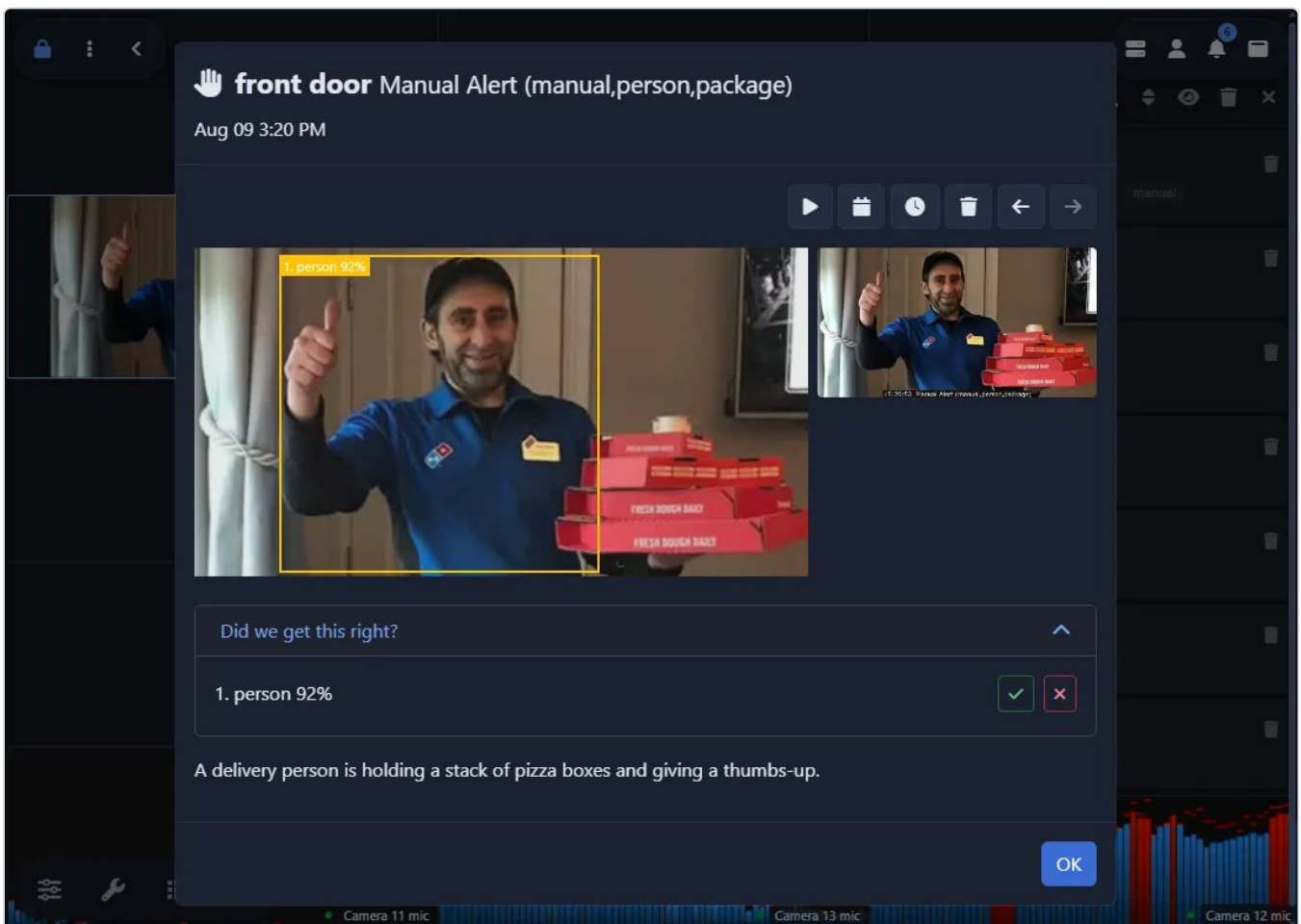
Agent DVR generates thumbnails for each event when possible. Clicking a thumbnail opens the [alert display](#) with the image and video from the event. To acknowledge an alert, click on its text. This action switches the view to the [timeline](#), providing context for the event with any other system recordings. The timeline will automatically navigate to just before the event occurred. If a recording is available, you can click on it in the Agent DVR UI, and playback will start from the point the alert was generated.

To delete alerts, use the bin icon to clear all alerts or remove them individually. Close the alerts panel by clicking the icon button in the top bar.

Alert panel icons indicate the alert type: manual alerts are marked with 🚫, alerts generated by Agent DVR with ⚠️, AI-generated alerts with 💡, and alerts suppressed by feedback with 🚫.

Alert Display

Clicking an alert thumbnail opens the alert display, which brings together everything Agent knows about the event: the alert image, an animated video preview of the recording, the detection feedback panel and the AI description.



Video preview

For camera alerts Agent generates a short looping video preview from the recording that covers the alert, so you can see what happened without leaving the panel. Previews are created on demand when you open the alert - nothing is generated in the background. The alert opens with the image shown full width; when the

preview is ready an inset tile appears and the preview swaps into the large position (the alert image keeps the large spot if the feedback panel is open, since the numbered detection boxes are drawn on it).

Click the smaller tile to swap which media is shown large.

Click the preview while it's large to open the recording for full playback.

A **REC** badge means the camera is still recording the event - the preview covers the recording so far, and reopening the alert later fetches the complete version.

If no recording covers the alert time (for example, recording is off), or the camera's **Video Previews** setting is off (see [Alert Settings](#)), the preview never appears and the alert image is simply shown on its own.

Detections and feedback

Alerts raised by [Object Recognition](#) store their detections with the alert. On cameras with **Learn From Feedback** enabled, expanding the collapsible "**Did we get this right?**" panel draws each detection as a numbered box on the alert image with its label and confidence, and lists it with  and  buttons - confirming or rejecting detections teaches Agent to suppress similar false alerts on that camera, and everything is learned locally. See [Learning From Feedback](#) for how the learning and suppressed alerts work.

To show detection boxes on alert images without the learning feature, enable the **Overlay** in the camera's [Object Recognition](#) settings - the boxes are then drawn into the alert image (and live video) itself.

AI description

If [Describe Alerts](#) is enabled, the AI's description of the event is shown below the feedback panel - the same text that appears in [push notifications](#) via the {AI} tag.

The toolbar buttons above the image play the recording, jump to the event on the [Timeline](#) or [Time Machine](#), delete the alert and step to the previous or next alert.

Using MQTT

About

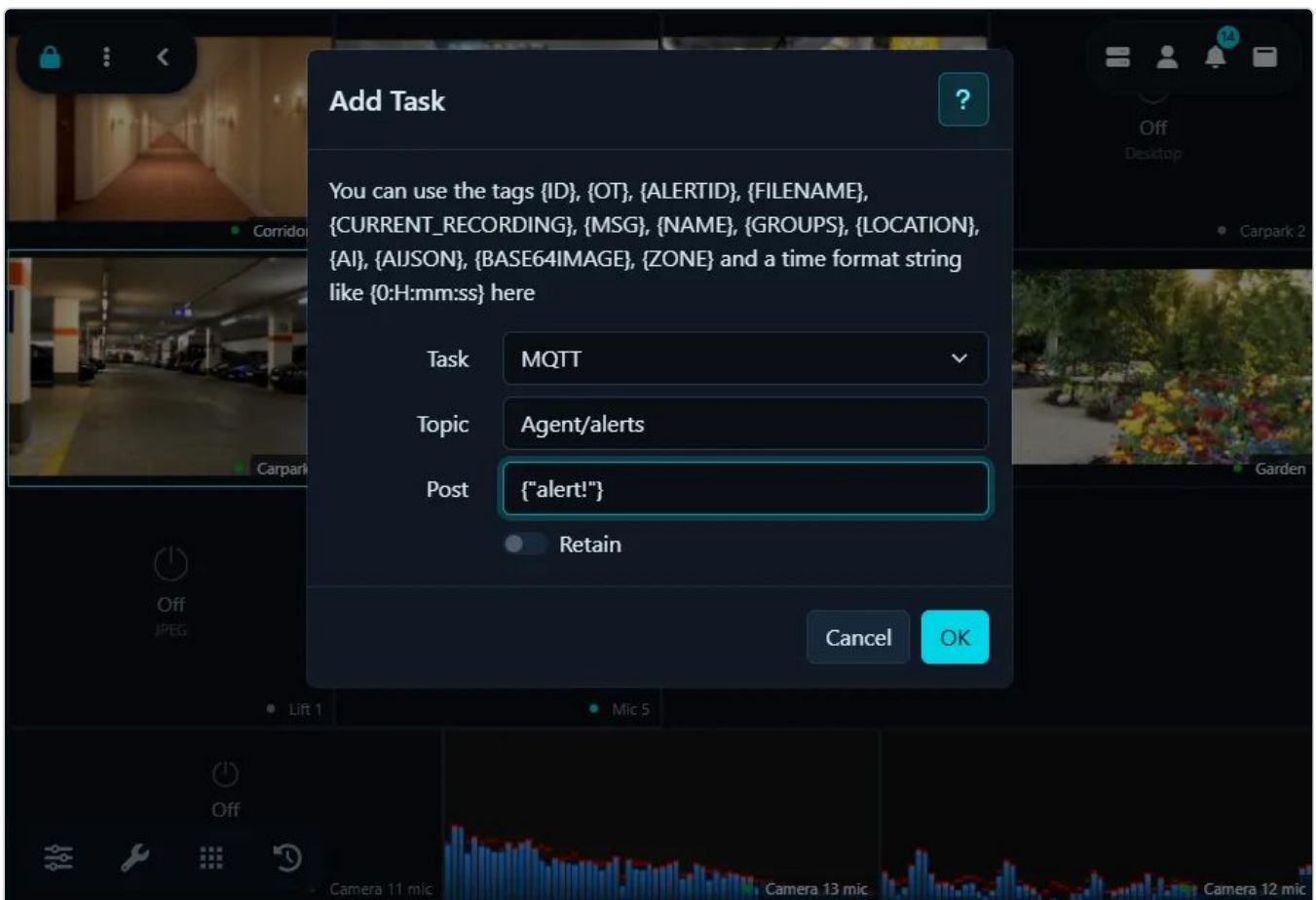
MQTT, which stands for Message Queuing Telemetry Transport, is a lightweight and efficient messaging protocol widely used in the Internet of Things (IoT) for device-to-device communication. It's designed to work under limited network bandwidth and with low-power devices, making it ideal for connecting remote sensors, mobile devices, and various small-scale gadgets to the internet.

Agent DVR can both publish events to MQTT and receive commands over it, making it a flexible bridge between your cameras and your smart home or home automation system.

Connecting

Connect Agent DVR to your MQTT server using the Settings menu. Once connected, you can set alert actions to publish messages to your MQTT server. [See MQTT Server Settings](#) for details.

To configure this, edit your device and select **Actions** in the menu. Add an action for an alert (or other event) and choose MQTT as the task type. Here, you can specify the topic and message to post.



Specify the topic to post to (e.g., Agent/alerts) and craft your message accordingly.

Sending Commands

Agent DVR can also receive and process MQTT messages on the **SERVER/commands** topic, where SERVER is your server name (displayed in the server menu, editable in Settings). Any slashes, underscores and hyphens are removed from the server name for MQTT topics. These commands are formatted similarly to the [HTTP API](#). Just replace /command with cmd=:

To turn all devices on: **cmd=allon**.

To take a photo on a specific device: **cmd=snapshot&ot=2&oid=1**.

Using mosquitto, you can send a command like (replace SERVER with your server name):

```
mosquitto_pub -t 'SERVER/commands' -m 'cmd=record&ot=2&oid=1'
```

Agent DVR will execute the command and send a JSON response to the **SERVER/responses** topic.

Auto MQTT

Agent DVR features an automatic MQTT configuration that sends default events, statuses, and usage statistics. To activate this feature, enable the "MQTT Events" option on the [MQTT tab](#) while editing a device.

This configuration includes flags for topics such as motion, connected, alert, recording, timelapse, alerts (armed state) and detector (motion detection on or off).

If you use Home Assistant you don't need to work with these topics directly: see [Home Assistant](#) for automatic setup.

Troubleshooting

If you encounter frequent disconnects and reconnects in MQTT, it typically indicates that the Client ID specified in Server Settings under MQTT is being used by multiple clients. It's important to ensure that each client connected to MQTT has a unique Client ID.

Home Assistant

Agent DVR can announce its devices to [Home Assistant](#) automatically using MQTT discovery. Your cameras and microphones then appear in Home Assistant as devices with sensors and switches, ready to use in dashboards and automations with no YAML configuration.

What you get

Motion sensor: on while the detector sees activity.
Alert sensor: on while the device is alerting.
Connected sensor: whether the device is online.
Recording sensor: on while the device is recording.
Enabled switch: turn the device on or off from Home Assistant.

Alerts switch: arm or disarm alerts from Home Assistant.

Detector switch: turn motion detection on or off from Home Assistant.

With **Send Stats** enabled the server also appears as a device with CPU, memory and disk usage sensors. All entities show as unavailable in Home Assistant when Agent DVR goes offline.

Setting it up

You need an MQTT broker (typically the Mosquitto add-on on your Home Assistant machine) and Home Assistant's MQTT integration connected to it. No extra ports need to be opened for Agent DVR: it connects out to the broker just like Home Assistant does.

On a new install, just enter your broker's address and login under **Home Assistant** on the welcome screen. That's it: MQTT and discovery are switched on for you, and every camera and microphone you add afterwards will appear in Home Assistant automatically.

To set it up later (or on an existing install), go to [Server Settings - MQTT](#), configure your broker and enable both **Enabled** and **Home Assistant Discovery**. Then enable **MQTT Events** on each device you want published (MQTT tab when editing the device). Devices added while discovery is on have MQTT Events enabled automatically; devices that existed before keep their current setting.

Notes

Devices appear in Home Assistant within a few seconds of Agent DVR connecting to the broker. Renaming a device or toggling MQTT Events updates Home Assistant automatically.

The **Discovery Prefix** in advanced MQTT settings must match the discovery prefix in Home Assistant's MQTT integration. Leave both at the default (homeassistant) unless you know you've changed it.

Turning Home Assistant Discovery off removes the entities from Home Assistant.

The switches use Agent DVR's [MQTT commands](#) under the hood, so anything else on your MQTT network can send the same commands.

Using Profiles

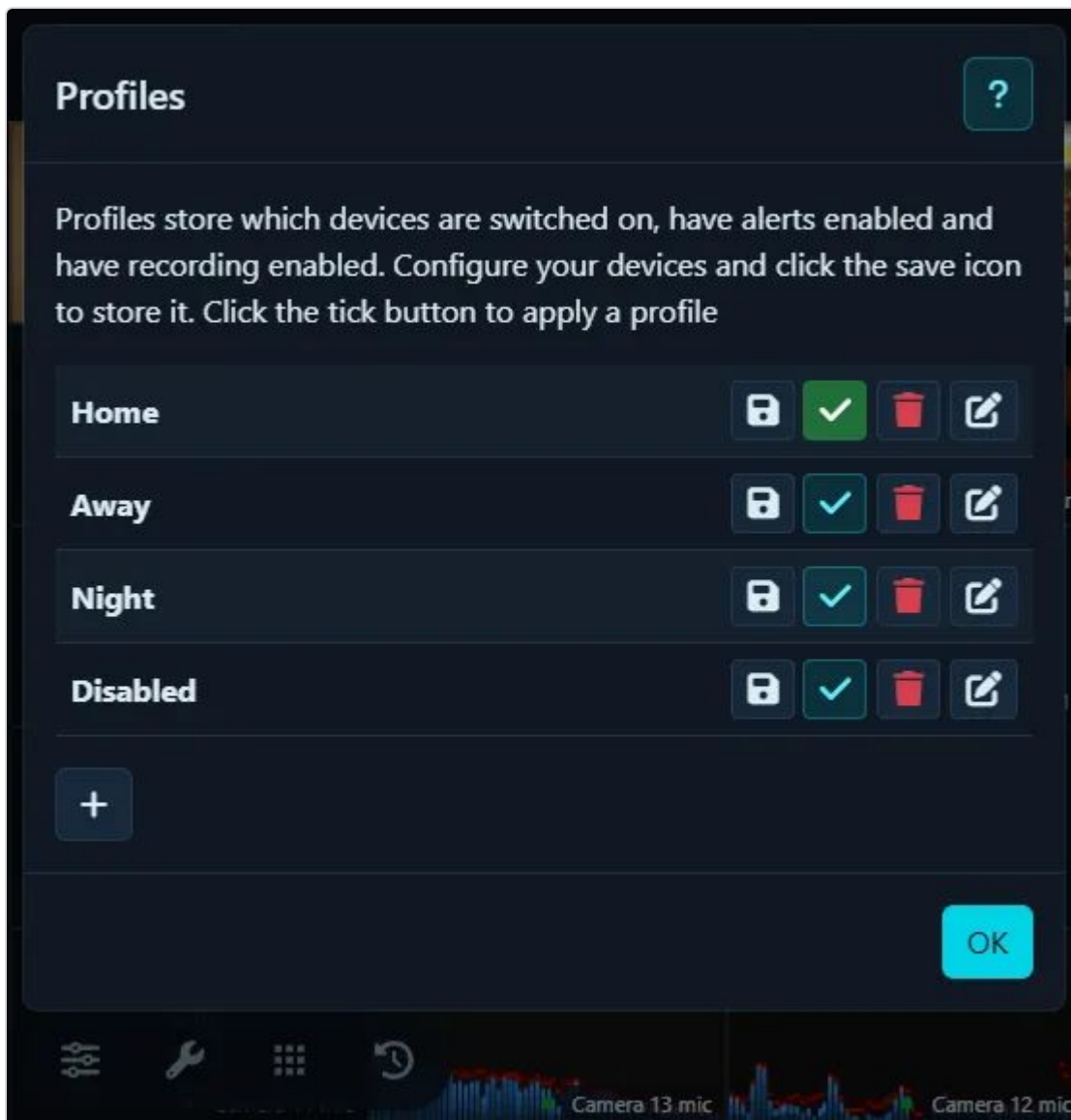
About

Profiles let you switch your whole system between different configurations, such as Home, Away and Night, with a single click. Each profile in Agent DVR stores key settings about your devices:

Enabled Status
Alerts Enabled
Record Mode (Alert/ Detect/ Manual)
Recording Status (manual recording on/ off)
Photos Enabled
FTP Enabled
Timelapse Enabled
Facial Recognition Enabled
Object Recognition Enabled
LPR Enabled
Motion Detector Enabled
Cloud Upload Recordings Enabled
Cloud Upload Photos Enabled
Plugin Enabled
Which Actions are enabled/ disabled (v4.1.0.0+)
Motion/ sound detector type, gain, and sensitivity settings

There are four profiles: Home, Away, Night, and Disabled. You can rename these profiles, but remember, some integrations need the original names to function properly.

To set up a profile, configure your device settings the way you want them, then go to  - **Profiles** and click the Save icon next to the profile you want to update. Do the same for other profiles as needed.



Click the ✓ button to apply a profile. It'll highlight to show the most recently used profile.

Click the 💾 button to save the current device settings to the profile.

Click the ✎ button to rename the profile.

Tip: You can also apply these profiles via the [API](#) (using `setProfile`) or through [integrations](#). Plus, you can set a default profile in Settings - Security for when you arm or disarm Agent.

Notifications

About

Agent DVR can let you know the moment something happens. It supports email alerts via SMTP, Push Notifications (via web browser, iOS and Android apps), Telegram, IFTTT and third party push (like Pushsafer). You can also send alerts to Discord, Slack, Mattermost, Google Chat, Microsoft Teams, ntfy and similar services using [Webhooks](#).

Email with SMTP

We offer our own mail servers for sending out notifications as part of an Agent DVR subscription. However, you also have the option to use your own SMTP server without needing a subscription. For more information, see [SMTP Settings](#).

Server Settings

Q SMTP

☐ Use SMTP
Required for email notifications if you don't have a remote access subscription

Username

Password

From Address

Server
example: mail.yourserver.com

Port

☒ Use SSL

Alert Template

You can use the tags {TAGSLIST}

Subject

Message

Advanced Settings 3

Cancel OK

To configure SMTP in Agent DVR, click on the server icon and navigate to Settings. Then, select the SMTP tab. Input your SMTP server details. After clicking OK, Agent DVR (v3.2.1.0+) will send a test email to your "From Address" using these settings. Make sure to enable 'Use SMTP' at the top of the settings page.

SMTP Troubleshooting

SMTP (email) notifications in Agent DVR are tied to specific device actions. To set up email notifications, edit your device and go to Actions. Select an event, like an Alert, and choose the "Send Email" action. Input your email address and confirm by clicking OK.

If you're not receiving email alerts, ensure the following:

Agent DVR is armed (indicated by a closed padlock icon in the top left).

Alerts are active (check the top checkbox on the Alerts tab in device settings).

Messaging is enabled (Messaging checkbox on the Alerts tab).

You have an active iSpyconnect.com subscription or SMTP configured in Server Settings.

Your setup triggers alerts (e.g., Detector is configured and active).

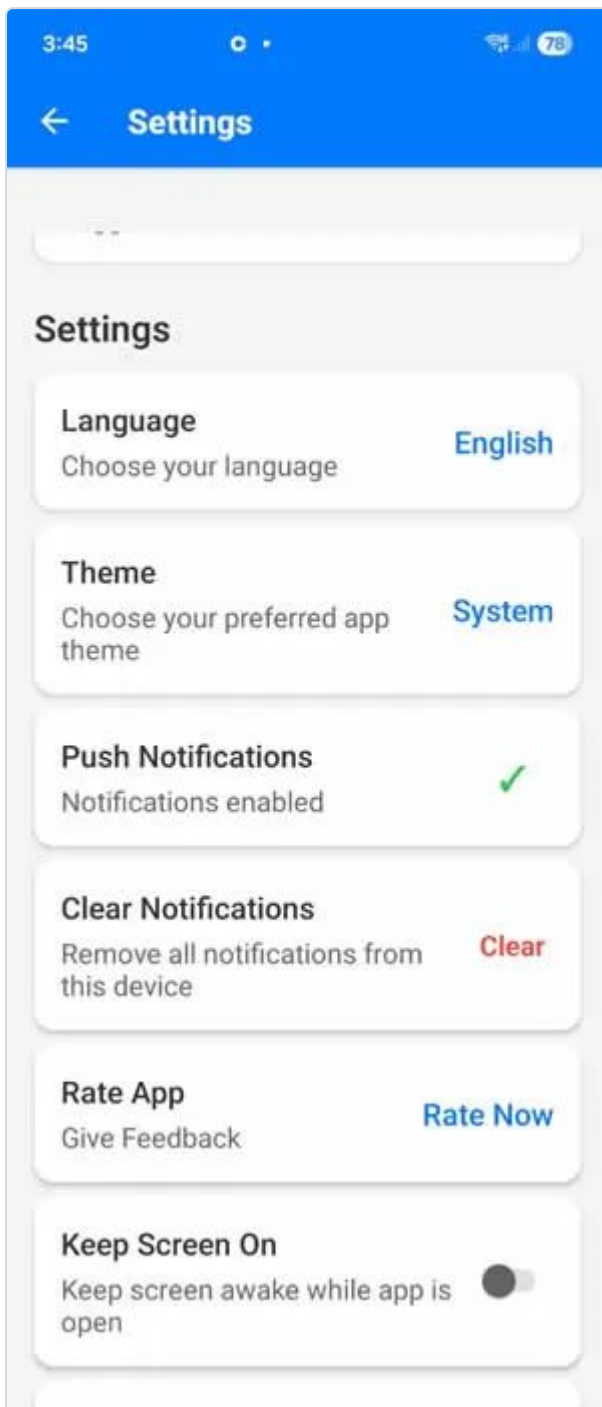
If emails aren't arriving, verify your server settings and check the local logs at /logs.html for any failure messages. Also, check your junk mail in case the emails are flagged as spam.

For Gmail users, Google no longer supports signing in with your normal account password from external applications. Enable 2-Step Verification on your Google account and create an [App Password](#), then use that as the SMTP password. Other providers may block application access, requiring you to use our services for email notifications.

Push Notifications

Receive push notifications through the Agent DVR mobile apps available for iOS, Android, and Desktop (subscribers only).

Push notifications are delivered to the account owner only (the account Agent DVR is connected to). To send push notifications to other people, use a third-party provider like [Pushsafer](#).



Getting Started

Install the **Agent DVR Remote** app from your device's app store. Open the app, tap the settings button (gear icon) on the server list page, and confirm that Push Notifications is enabled.

Agent DVR sends push notifications when an alert fires. For this to work:

- Alerts must be enabled on the device.
- The system must be armed (green padlock in the top-left corner of the Agent DVR UI).

You can also trigger push notifications from custom scenarios using [Actions](#).

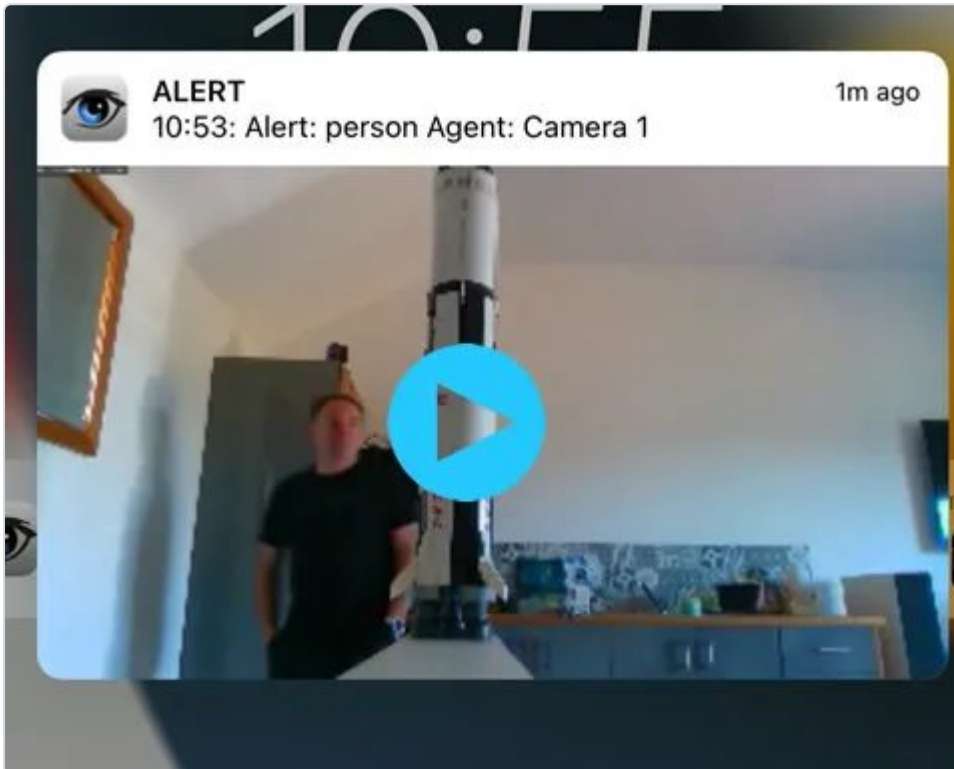
Desktop users can enable push notifications through Chrome.

What's Included

Push notifications cover all Alert and Manual Alert events from your devices, with an image grab when available. To opt out for a specific device, uncheck **Push Alerts** on the [Alerts tab](#) in that device's settings.

Rich Notifications

Android and iOS notifications can include a camera snapshot. iOS also supports short video clips of the triggering event: enable this by checking **Push Video** on the [Alerts tab](#).



Browser Notifications

Agent DVR can notify you with browser alerts when an alert or recording is triggered. Under Account  - Notification Settings see the options to enable or disable browser notifications for New Recordings or Alerts. An alarm will then sound for any alert generated.

Push Safer

You can use [pushsafer](#) to send push notifications with images via actions instead - edit a device, select actions and add an action like:

If: Alert
Then: Call URL
URL: https://www.pushsafer.com/api
Upload Image: 0 (image will be sent in the {BASE64IMAGE} tag below)
Method: POST

Body: t=Agent&m=Alert&s=11&d=a&is=1&v=3&k=PRIVATE KEY&p=data:image/jpeg;base64,
{BASE64IMAGE}

(Replace PRIVATE KEY with your private key from pushsafer)

Network Drives

Setting Up

Network Drives

Agent DVR can store recordings, photos and other content on a network share or NAS instead of the local disk, which is handy for keeping large amounts of footage or protecting recordings if the local machine is stolen or damaged.

Here's how to get it set up:

1: First, select your server in the Agent DVR portal.

2: Go to the Settings tab and click on the Settings button.

3: Select the Storage tab.

4: Click to add a new storage location.

5: Type in the UNC path to your desired save location (remember, use the UNC path, not a mapped drive like z:\). It should start with the network machine name, like \\wdmycloud\public\AgentDVR or \\davesPC\c\$\Agent.

6: Under Network Storage, fill in the network machine name (e.g., wdmycloud or davesPC) and (on Windows) the username and password used to access the device. On Linux and macOS you will need to grant the user Agent DVR is running as permissions to access the location.

Tip #1: If Agent DVR struggles to connect to the drive, consider setting the folder to public read/write access.

Tip #2: If Agent DVR is running as a service and you're facing issues connecting to your NAS then it might be due to the set of permissions Windows is granting your service. Try these steps:

Identify the Service Account:

Open the "Services" management console (services.msc).

Locate **Agent** in the list, right-click it, and select "Properties".

Go to the "Log On" tab to see which account the service is running under.

If the service runs under the "Local System account", change it to a user account with access to the NAS drive:

Select "This account".

Enter the username and password of a user account with access to the NAS drive.

Click "OK" and restart the service.

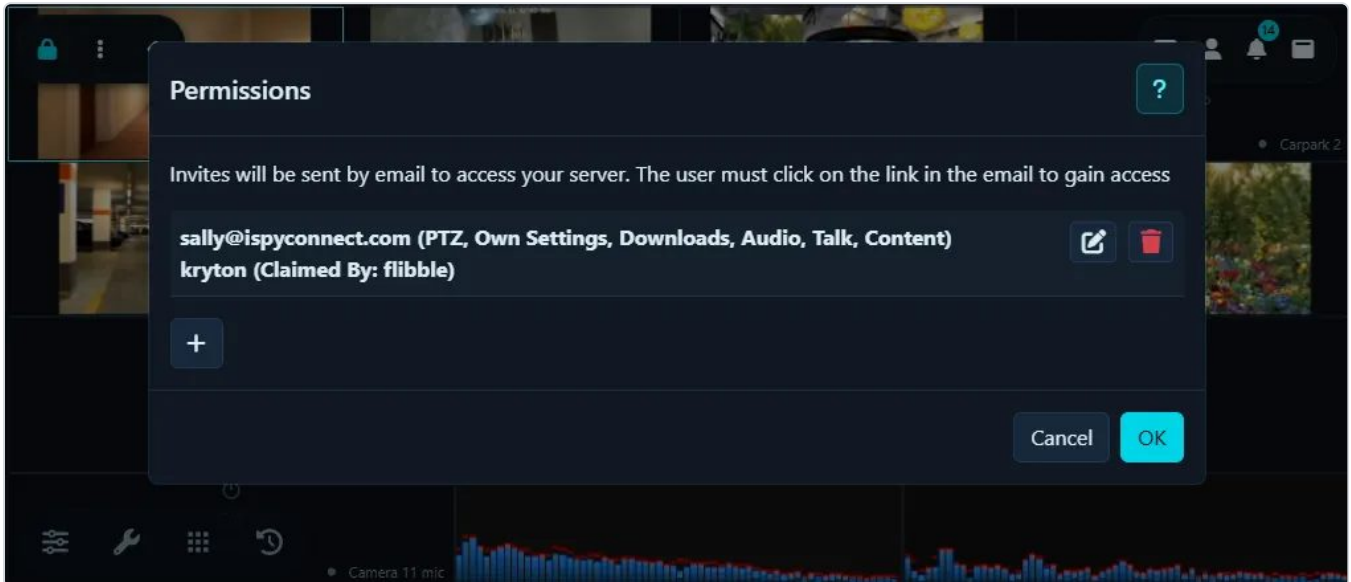
Attempt to add the NAS again.

That's it! You're all set to use your network drives with Agent DVR.

Permissions

Granting Access

Check out [Local Users](#) for local user permissions.



Sharing access to your cameras and microphones with friends, family, customers, or co-workers is easy with iSpyConnect. While you need a subscription to share access, the people you share with **don't need a subscription**.

To grant access:

- 1: Go to the "Permissions" link under the Account menu  on the web portal.
- 2: We'll send an email link to the person you're sharing with. They'll need to click this link and create an account to access your server.
- 3: You can give them full access (switching on/off, recording, deleting, etc.) or read-only access, and you can revoke access anytime.

Tip: If they don't receive the link, or it hasn't applied to their account, use the edit button next to the permission for an **Access Code**. They can use this code at ispyconnect.com/app after logging in.

Note: Invited people don't need their own subscription to access your server. They only need one if they want to add their own servers.

Troubleshooting: If your server isn't showing up for them, ensure it's connected and online, then check your configuration in [Permission Groups](#).

Configuring Permissions

Use these settings to control exactly what each invited user can see and do:

?

sally@ispyconnect.com

☒ Own Settings

User can download recordings (recordings could contain audio)

Record/ Photo etc. Only applies if Read-Only.

Allow access to recordings and photos.

krypton

kryton seans-macbook-air

This is the link we sent them to gain access. If they didn't receive it please send this manually.

OK

PTZ: User can control PTZ.

Read Only: User can view video but can't edit settings.

Own Settings: The user can save their own views, filters, floorplans and key mappings. If this is unchecked they will use the admin accounts configuration.

Downloads: User can download recordings.

Audio: User can listen to live and recorded audio.

Talk: User can use talk functionality.

Groups: See Groups section below.

Access Code: Share this with the user if needed.

Permission Groups

Permission groups let you limit an invited user to specific cameras and microphones, for example sharing only your outdoor devices.

Specify the server name and optionally groups here to restrict access to certain devices. The default server name is "Agent", but you can change it under Server settings. Group names are **not** case sensitive.

To restrict access to certain devices:

Assign a group name in the device settings under the General tab (e.g., "outside").

In the user's Groups field, add the group "outside" to restrict their access to devices labeled as such.

Assign a group name to all other devices - if a device is not assigned to a group it will be visible to everybody.

If the user can't see your server, make sure the server name matches the one in their permissions.

Important: If you change the server name, update the permissions to match. For instance, change "Agent,neighbours,police" to "MyPC,neighbours,police".

Tip: Use the special device group name **"exclude"** to keep a camera or microphone from appearing in someone else's access.

Note: The device's Groups field is also used by the HTTP and command line interface to control device groups.

RTMP Streaming

About

Stream live to YouTube, Twitch, or any RTMP provider. Optionally embed the video in your website. Note: RTMP push requires a subscription or a license.

Adding RTMP Servers

Agent DVR supports simultaneous streaming to multiple RTMP endpoints. To add an RTMP server click on Server Menu, Settings (under Configuration) - select "RTMP Streaming" in the menu and Add a new server. You can control the resolution using the Size dropdown and the bitrate using the Quality slider. If your stream is buffering frequently then try reducing the size or the quality or both to get smooth playback.

Streaming to YouTube

- 1: Log into YouTube and visit [YouTube Live Dashboard](#) ↗.
- 2: Create a new Live Stream and note the **Server URL** and **Stream name/key**.
- 3: In Agent DVR, open Server Settings and select "RTMP Streaming". Add a server and enter the URL and Stream Key from YouTube.
- 4: Adjust streaming duration if needed (default is 900 seconds).
- 5: To embed this in your website, right-click on the YouTube live player and select "Copy embed code" to get the HTML for your webpage.

After these steps, start streaming live to your site.

Manual Streaming

Click the Server menu and RTMP Streaming in the System menu. Click the "..." button next to your RTMP server entry to configure the device or view to live stream. The stream to your RTMP platform should start. Give it a few seconds to buffer.

Scheduled Device Streaming

Use this to live stream a camera automatically at set times of day. Edit a device and set the RTMP server to use under the RTMP tab. Select the Schedule tab and click to configure the Schedule. Add a schedule command "RTMP Streaming Start" and set the times and days. Then add an "RTMP Streaming Stop" command.

Scheduled View Streaming

Setting up scheduled view streaming is a bit more involved. You will need to add an Action to a device and then schedule a call to that action:

1: After adding the RTMP server, go to <http://localhost:8090/q.json?cmd=getstreamingstatus> and copy the **ident** of the RTMP server you want to use (excluding the quotes)

2: Add an action to the device with If: None, then: Call URL, URL: <http://localhost:8090/q.json?cmd=start-rtmp-view&ident=ident&ind=0> where ind is the index of the view you want to stream (from 0-8)

3: Add a schedule entry in the device scheduler for "Action: Run" and select the action you just created.

You can add another action/ schedule entry to stop using the URL <http://localhost:8090/q.json?cmd=stop-rtmp&ident=ident>. Make sure the schedule is enabled on the General tab.

You could also use curl to make these API calls.

Setting up SSL

About

The free version of Agent DVR is great for local connections using HTTP. For remote connections, though, security is essential, and that's where SSL comes in. For a secure remote connection to your Agent DVR with no setup, use our [remote web portal](#).

Important: Setting up SSL, DNS, and port forwarding can get a bit tricky, and we can't guarantee it'll work reliably on all networks. We recommend sticking with using our remote web portal for remote access. You'll still need a computer running Agent that's connected to your cameras but you won't need to mess around with anything else.

Pro Tip: Once you've got SSL and DNS up and running, you can access your Agent DVR from your mobile device and add it as an app through your browser's tool menu.

SSL on Windows

Agent DVR now terminates SSL itself, so all you need is a **PKCS#12** certificate file (a `.p12` or `.pfx`) that contains the private key. You no longer need to install the certificate into Windows or bind it with `netsh`.

Option 1 - quick self-signed certificate (for testing): run this in PowerShell to create a certificate for localhost and export it to a `.p12` (change the password to suit):

```
$cert = New-SelfSignedCertificate -DnsName "localhost" -CertStoreLocation "Cert:\CurrentUser\My"
-NotAfter (Get-Date).AddYears(5)
$pwd = ConvertTo-SecureString -String "yourpassword" -Force -AsPlainText
Export-PfxCertificate -Cert $cert -FilePath "C:\Agent\certificate.p12" -Password $pwd
```

For a public hostname use `-DnsName "youragentserver.ddns.net"` instead of localhost.

Option 2 - real certificate (Let's Encrypt): follow the [letsencrypt instructions](#), then convert the generated `.pem` files to a `.p12` with `openssl`:

```
openssl pkcs12 -export -out C:\Certbot\live\youragentserver.ddns.net\certificate.p12 -inkey
C:\Certbot\live\youragentserver.ddns.net\privkey.pem -in
C:\Certbot\live\youragentserver.ddns.net\fullchain.pem
```

Open Agent DVR, click the Server icon - Settings - Local Server tab and set:

SSL Port: the port to serve HTTPS on, e.g. 8443 (or 443 for the standard HTTPS port).

SSL Certificate: the full path to your `.p12` file, e.g. `C:\Agent\certificate.p12`

SSL Password: the password you set when creating the certificate.

Click OK. Agent restarts the local server automatically. Watch the log for `Accepting SSL connections at https://...`. You can now load the UI at **`https://your.server.address:8443`**. Be sure to use **`https://`** as browsing with `http://` to the SSL port returns an empty response.

A self-signed certificate (Option 1) is not trusted by browsers, so the first time you visit you will see a privacy warning. Click **Advanced** then **Continue to localhost (unsafe)** to proceed. This is expected for self-signed certificates. A real certificate (Option 2) will not show the warning.

SSL on Linux / macOS

Agent DVR terminates SSL itself from a **PKCS#12** certificate file (a `.p12` or `.pfx`) that contains the private key.

Quick self-signed certificate (for testing):

```
openssl req -x509 -newkey rsa:2048 -keyout key.pem -out cert.pem -days 1825 -nodes -subj  
"/CN=localhost"  
openssl pkcs12 -export -out certificate.p12 -inkey key.pem -in cert.pem -passout  
pass:yourpassword
```

Real certificate (Let's Encrypt): follow the [letsencrypt instructions](#) ↗, then convert the generated `.pem` files to a `.p12` (run from the folder your certificate was saved to):

```
openssl pkcs12 -export -out certificate.p12 -inkey privkey.pem -in fullchain.pem
```

In Agent DVR's local UI click the Server icon, Server Settings, Local Server tab, then set **SSL Port**, **SSL Certificate** (the full path to your `.p12` file) and **SSL Password**, and click OK. Agent restarts the local server automatically and you can load the UI at **`https://your.server.address:8443`** (use **`https://`**).

On Linux, ports below 1024 (including the standard HTTPS port 443) require root. Agent DVR installed as a service runs as root, so 443 works; if you run it manually as a normal user choose a high port such as 8443.

Make sure the certificate file is readable by the Agent process. If needed run `chmod 644 certificate.p12`. A self-signed certificate triggers a browser privacy warning the first time (click **Advanced** then proceed); a real certificate will not.

Storage Management

About

Agent DVR combines Media directories and individual device folders to manage your storage space efficiently. Set size and age limits so old recordings are cleared automatically and your drives never fill up, or use archive options and file locking to copy old content to cold storage and keep important content in the database.

Media Directory Settings

Multiple storage locations can be added in Agent DVR using the settings in [Server Settings](#). Open Server Settings and select the Storage tab. Click **Configure** then click to add or edit a storage location. Each location acts as a base for device storage and has its own rules for size and file age.

To manage a storage location:

Location: Path or UNC path to your storage location.

Default: Set as the default location for new devices.

Management: Enable storage management to automatically clear old content.

Max Size: Set a limit for this location's size in MB (0 = unlimited).

Max Age: Set a maximum file age in hours (0 = unlimited).

Delete to Recycle Bin: Opt to delete files to the recycle bin instead of permanent deletion (Windows only).

Network Storage: For Windows users, input details if authentication is required for your storage path.

Media Archive

Each storage location can be associated with an archive. Archives are usually large drives that hold recordings for a long period of time. Agent DVR can move recordings to the archive instead of deleting them.

To manage an archive location see [Server Settings](#). Open Server Settings and select the Storage tab. Click **Configure**

Archive Location: Set a location for archiving recordings. See [merge tags](#). You can also use {DIR} for the device's directory name and {GRABS} which resolves to "grabs/" if it's a photo or nothing if it's a recording.

Photos Location: Set a location for archiving photos. If blank, Agent DVR uses the main Archive Location.

Index Archived Files: Check this option to keep the file in the database with the new path to the archived location (recordings only).

Archive Expires: Option to delete archive content older than the set number of days. Set to 0 to disable. The process to check and delete archived content runs once a day (at midnight GMT).

Device Settings

Agent DVR also offers detailed storage settings for each device. Find these under the Storage tab when [editing a device](#).

Location: Select one of the media locations defined in server settings.

Folder: Name of the folder within the location for this device's files.

Archive: Enable to move files to the archive location instead of deleting. Keep an eye on archive space. Locked files will not be archived.

Enabled: (under Storage Management) Toggle storage management for this device.

Max Size: Maximum size for this device's media folder (MB).

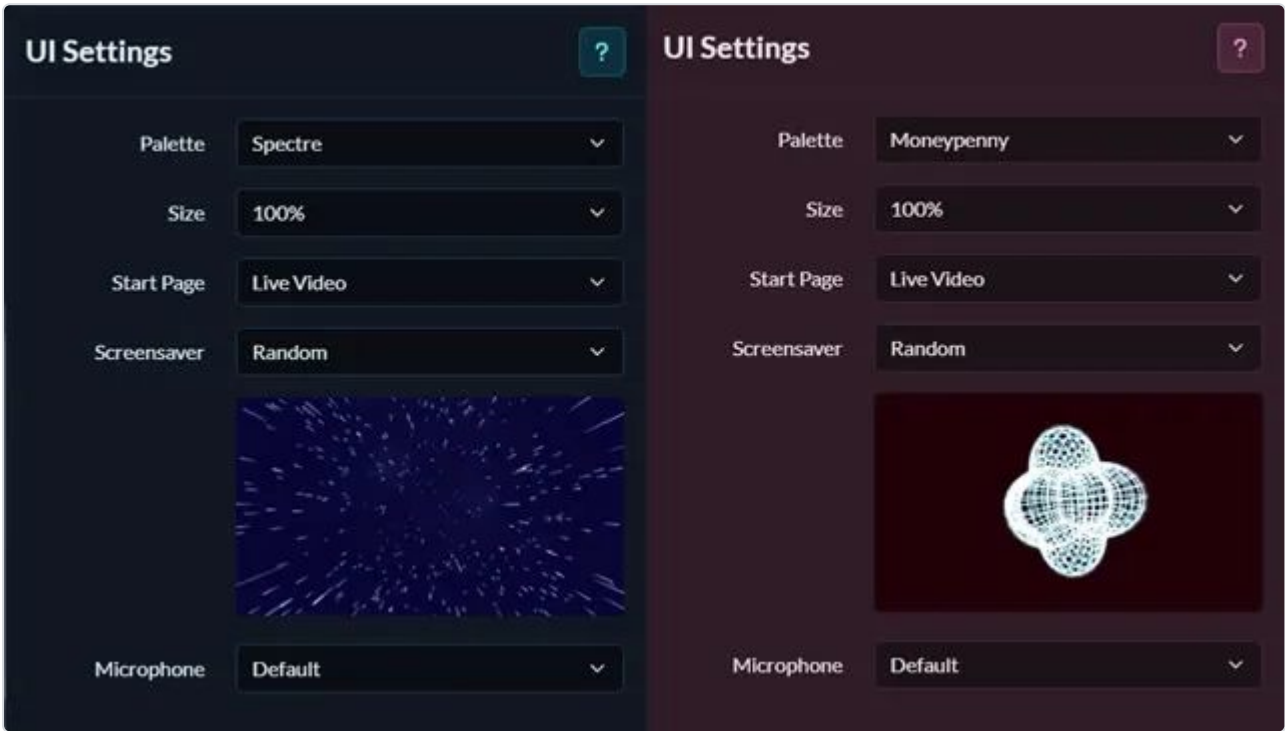
Max Age: Maximum age for files in this device's media folder (hours).

Themes

About

Themes in Agent DVR let you customize the look and feel of the entire user interface.

To change the theme, click on **Account Menu** (👤) - **UI Settings**.



Palette: Pick a color scheme

Size: Choose a size. Use this to make things more readable on high resolution devices.

Start Page: Choose a view to start on: Live, Timeline, Recordings, Photos, Floor plans or Virtual Reality.

Screensaver: Choose a screensaver. This is displayed when connecting or logging in.

Microphone: Choose a default microphone to use for talk.

Display Options

Labels: Toggle object names display on or off in the live view.

Icons: Toggle icons at the bottom left of each device showing their state (recording, alerts enabled, motion detection enabled, schedule enabled)

Recording Icon: Toggles the red recording indicator

FPS Limiter: Limit frames per second in some views to save CPU. Or turn it off for smoother visuals at the cost of some CPU.

Hide Playback Controls: Auto hide playback controls when viewing recordings.

Show Clip Info: Pop up information about the clip when playback starts.

Motion Indicator: Flash border on devices that detect movement or sound.

Alert Indicator: Flash border on devices that alert.

Grid: Toggles the display of grid lines in the UI.

Auto mobile layout: Always use grid layout on mobile devices (only visible on mobile devices).

Audio/ Video Options

Autoplay Audio: Start playing audio automatically when the interface loads.

Auto Mute: Stop and start audio playback based on browser tab visibility

Connection Settings

Use server time: Show event timestamps in the server timezone, or stick with local time

Local Data: Cache data in the local browser when possible (speeds up the UI)

Auto reconnect: Automatically reconnect to Agent DVR if the connection is lost

Input Controls

Shortcut Keys: Toggle shortcut key support

Joystick: Toggle joystick support

Invert Controller: Invert the Y-Axis of the Joystick

User Interface

Confirm: Display Confirm dialog box when performing certain actions (like Delete)

Shortcut Keys

Editing Shortcut Keys

You can easily create and manage shortcut keys in Agent DVR (v5.6.7.0+) by following these steps:

Click on the  Account Menu icon at the top-right corner of the screen.

Select **Key Mappings** from the menu.

To set a new shortcut key, click the corresponding button and press the key combination you want. The key presses will be recorded automatically.

To remove a key, click **✕**.

Use the options at the bottom to:

 reset your key mappings to default settings.

 download your current key settings.

 upload saved key settings.

Use the menu at top right to change the key mappings for different sections, like **General**, **Devices**, or **PTZ**.

Your key mappings are saved to your account on the Agent DVR server, so they are always accessible.

Note: The following keys cannot be used as shortcuts because they are reserved by the browser: **F11**, **Ctrl+Q**, **Ctrl+N**, **Ctrl+W**, **Ctrl+T**, and **Ctrl+Tab**.

Customizing Controls

Customizing Menu Buttons

The Controls feature allows you to customize which buttons appear in the application's menus. To access this click on the Account Menu - Controls.

To rearrange controls drag and drop them into the order you want. Click to toggle the display of the control. Click OK to apply.

Your button configuration is saved locally to the web browser so you can have different options on different devices.

FFmpeg Install

FFmpeg Setup

Agent DVR has been updated to use FFmpeg v8.

If you're reading this message then chances are you've upgraded Agent DVR and are having problems updating it (as it normally installs FFmpeg automatically). To get things working again:

macOS: Open a terminal and run :

```
launchctl bootout gui/$(id -u) ~/Library/LaunchAgents/com.ispy.agent.dvr.plist  
brew install ffmpeg  
  
launchctl bootstrap gui/$(id -u) ~/Library/LaunchAgents/com.ispy.agent.dvr.plist
```

On older installs the service is a system daemon instead - if that file doesn't exist, use `sudo launchctl bootout system /Library/LaunchDaemons/com.ispy.agent.dvr.plist` and `sudo launchctl bootstrap system /Library/LaunchDaemons/com.ispy.agent.dvr.plist`.

FFmpeg Troubleshooting

Run Agent DVR from the terminal to see where it is looking for FFmpeg.

If you have built or installed FFmpeg in a location that it isn't checking you can set an override in the Media/XML/config.xml file in the FFMPEG_DIR element for example:

```
<FFMPEG_DIR>/home/ffmpeg_v5</FFMPEG_DIR>
```

Integrations

API

API

Agent DVR has a full HTTP REST API that lets you control cameras, recording and the rest of the system from your own scripts and applications. Interactive API documentation is below. You can also open it [in a new window](#).

https://ispysoftware.github.io/Agent_API/

Integrations

Mobile Applications

Our mobile apps let you connect over your LAN or via our remote services. They're available for both Android and iOS devices.

Download the [Agent DVR Remote Android App](#) ↗.

Download the [Agent DVR Remote IOS App](#) ↗.

Python Wrapper

There's a python wrapper for basic UI functionality here: [agent-py](#) ↗.

URL Parameters

You can open Agent DVR to a specific view by calling the Agent DVR url with (case sensitive):

```
?start=Live&viewIndex=3 (live view on view 3)
```

```
?start=Live&viewIndex=3&ot=2&oid=2&max=true (live view on view 3, cam id 2 maximised). "oid" is the object id of the device (visible at the top of the dialog when you edit the camera), "ot" is the object type - 1 = microphone, 2 = camera.
```

```
?start=TimeMachine (timemachine view)
```

```
?start=Timeline (timeline view)
```

```
?start=Photos (photos view)
```

```
?start=Recordings (recordings view)
```

```
?start=Floorplans&planIndex=2 (floorplans view on plan 2)
```

```
?start=VR (virtual reality)
```

You can open Agent DVR with a specific language (bypassing the language selection). Just pass in the 2 letter language code: **?lang=fr**

You can pass in the name of a saved filter to apply using a filter parameter - eg: ?

start=Recordings&filter=intruder. You can also pass in a from and to time for the filter using javascript ticks. eg ?start=timeline&from=1657841514949&to=1657852514949.

Set default theme options (theme options are available in the account menu - theme settings):

```
?theme=darkly&variant=dark&large=false
```

```
?theme=sketchy&variant=primary&large=true
```

Auto play audio on load (may also require changing browser settings):

```
?playaudio=true
```

Start in minimised mode (top and bottom UI bars hidden):

```
?mini=true
```

Pass in local username and password for auto login (caution - this will expose your credentials to the network):

```
?un=username&pwd=password
```

Open a specific alert by alert id (in the alert json):

```
?alertid=xxx
```

Commands

To access Commands in Agent DVR, click on the Server icon  at the top right of the Agent DVR UI, and select "Commands" under **System**. A quick shortcut is to press "Alt-C".

Agent DVR includes several pre-built commands that can control multiple devices simultaneously. These commands utilize the [API](#) to perform various tasks. You have the flexibility to add your own custom commands for calling the API or running software on your computer.

Calling a Script File

To execute a generic script file, simply add a .bat file (or .sh file on Linux/macOS) to the commands directory. The script's filename (without the extension) will appear in the Commands list and can be clicked to run. Note: You might need to reload the UI for it to appear.

Calling the API

Create a new .bat file in the Commands folder where Agent DVR is installed. The first line should be:

```
REM ispy-internal
```

This line indicates that the file should be processed internally by Agent DVR, not executed as a standalone application.

The subsequent lines are interpreted as commands for the Agent DVR's API. For instance:

```
REM ispy-internal

switchon&group=external

switchoff&group=internal

record&group=external

broadcast 'external cameras are on and recording'
```

These commands are appended to API calls in the format **/command.cgi?cmd=....** Thus, you can use any command available in the [API](#).

The example commands above will activate all devices labeled as "external", deactivate all "internal" devices, start recording on "external" devices, and send a broadcast message to all connected clients.

Refer to the **readme** command button for examples and the API documentation for a list of available commands.

Remember to use **&** instead of **?** to separate parameters in your commands.

After reloading the UI and pressing "Shift-Alt-C", your new command should be visible in the list. Click on it to execute.

From version 3.8.1.0+, you can use location names in commands (e.g., **switchon&location=home**). Just assign a location to your devices first!

Amazon Alexa

From version 2.9.5.0, Agent DVR offers Amazon Alexa integration. This feature allows you to control Agent DVR using voice commands through Alexa-enabled devices. You can arm or disarm the system or display live video feeds on Alexa Show devices.

To set it up, select 'Alexa' under Integrations in the Server menu of Agent DVR. This redirects you to Amazon for linking your accounts.

Once linked, run Alexa's discovery process. It should find two devices: the security panel and the camera control.

Now you can use voice commands like:

"Alexa, arm Agent in home mode"

"Alexa, show Agent camera"

Set your security code in Agent DVR Settings for operations requiring authentication. The default code is 1234.

The Alexa profiles (Home / Away / Night) match those in Agent DVR. Configure them in Server - Profiles.

For multiple servers, set a server name in settings and use it in voice commands.

Home Assistant

Agent DVR fully integrates with Home Assistant, allowing you to add Agent DVR into your Home Assistant setup. Embed the Agent DVR panel in the lovelace UI or select individual cameras. It also includes a control for the main security panel. For more information, see the Home Assistant link under Server - Integrations.

Agent DVR can also publish its devices to Home Assistant as sensors and switches via MQTT: see [Home Assistant MQTT discovery](#).

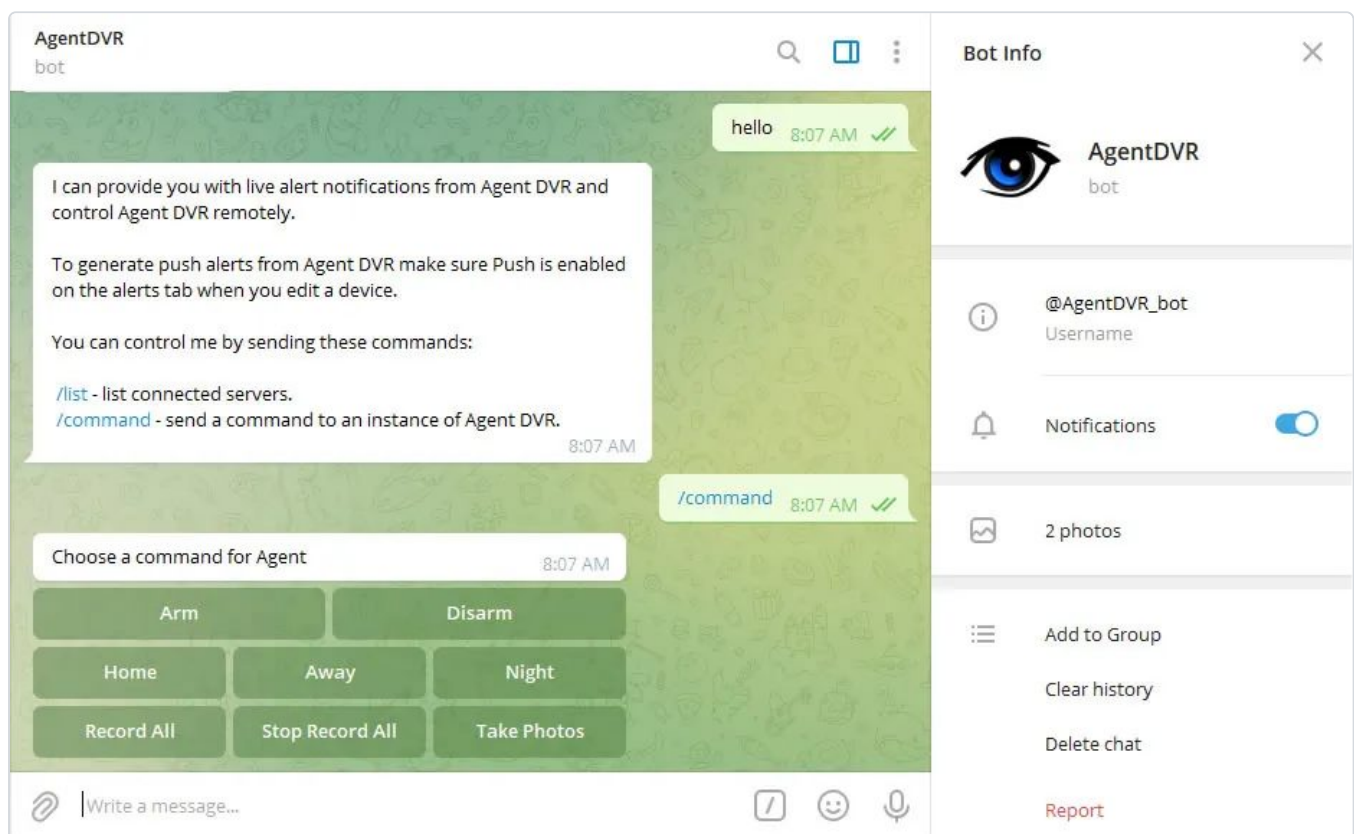
IFTTT (If This Then That)

IFTTT lets you set up actions and triggers with IoT devices. Start by linking your IFTTT account with iSpyConnect.com, accessible under Server - Integrations.

Push Alerts

Setting up mobile push alerts is detailed at [Setting up Push Alerts](#).

Telegram



Connect Agent DVR with the Telegram chatbot for control and live alert notifications. Enable [Push notifications](#) in device settings for live alerts. Begin by selecting the Telegram button under the Server icon in the remote web interface.

To disconnect Telegram you will need to use the remote web portal account menu.

Bot Commands

/list - List connected servers

/command - Send a command to an Agent DVR Server

/groupalerts - (in a group) Send alerts to this group

/privatealerts - (in private chat) Send alerts back to this private chat

Webhooks (Discord, Slack and more)

Agent DVR can send alerts to any service that accepts incoming webhooks, including Discord, Slack, Mattermost, Google Chat, Microsoft Teams and ntfy. No account linking is needed: you create a webhook URL in the target service and Agent DVR posts alerts to it directly, so this also works on servers with no internet-facing remote access.

The general setup is the same for every service. Edit your camera or microphone, open the **Actions** tab and add an action:

If: Alert (or any other event)

Then: Call URL

URL: the webhook URL from the service

Method: POST

Body: the message, formatted as shown for each service below

You can use [tags](#) like {NAME}, {MESSAGE}, {AI} and {ZONE} in the Body field to build the message dynamically.

JSON message bodies require Agent DVR v7.8.7.0 or newer. On older versions add a line to the **Headers** field:

```
Content-Type: application/json
```

Discord

In Discord, open your channel's settings (gear icon) and choose **Integrations - Webhooks - New Webhook**, then **Copy Webhook URL**. In the Agent DVR action use:

URL: the copied webhook URL

Body:

```
{"content": "{MESSAGE}: {NAME} on {SERVER} {AI}"}
```

To attach snapshots to the Discord message, set the **Upload Image** slider to 1 or more (v7.8.7.0+). Each image beyond the first is captured half a second apart.

Slack

Create a Slack app at api.slack.com/apps, enable **Incoming Webhooks**, click **Add New Webhook to Workspace**, pick a channel and copy the URL (it starts with hooks.slack.com). In the Agent DVR action use:

URL: the copied webhook URL

Body:

```
{"text":"{MESSAGE}: {NAME} on {SERVER} {AI}"}
```

Slack incoming webhooks are text only, so leave Upload Image at 0.

Mattermost

In Mattermost, go to **Main Menu - Integrations - Incoming Webhooks - Add Incoming Webhook**, pick a channel and copy the URL. Use the same Body format as Slack:

```
{"text":"{MESSAGE}: {NAME} on {SERVER}"}
```

Google Chat

In a Google Chat space (Workspace accounts), click the space name and choose **Apps & integrations - Webhooks - Add webhook**, then copy the URL. Use the same Body format as Slack:

```
{"text":"{MESSAGE}: {NAME} on {SERVER}"}
```

Microsoft Teams

In Teams, click the three dots next to a channel, choose **Workflows** and add the template **Post to a channel when a webhook request is received**, then copy the URL it gives you. Teams requires the message as an Adaptive Card:

```
{"type":"message","attachments":  
[{"contentType":"application/vnd.microsoft.card.adaptive","content":  
{"type":"AdaptiveCard","version":"1.4","body":[{"type":"TextBlock","text":"{MESSAGE}: {NAME} on {SERVER}","wrap":true}]}]}
```

ntfy

[ntfy](https://ntfy.sh) sends push notifications to your phone with no account required, and can also be self hosted. Pick a topic name that is hard to guess (anyone who knows it can subscribe), then:

URL: <https://ntfy.sh/your-topic-name>

Body: plain text (no JSON), e.g.

```
{MESSAGE}: {NAME} on {SERVER}
```

Headers (optional, one per line):

```
Title: Agent DVR
Tags: rotating_light
Priority: high
```

Install the ntfy app on your phone and subscribe to your topic to receive the alerts.

Other services

Anything that accepts an HTTP POST works the same way, for example Home Assistant webhook triggers (<http://homeassistant.local:8123/api/webhook/your-id> - though the [MQTT integration](#) is richer). Agent DVR sends JSON bodies as application/json and anything else as form encoded. You can add extra headers (for example API keys) in the **Headers** field, one per line as **Name: Value**.

Servers

About

Agent DVR integrates fully with AI servers like DeepStack AI, CodeProject AI, PlateRecognizer.com, Claude, Gemini, OpenAI (ChatGPT) and local LLMs like Ollama, vLLM and LM Studio to add smart alert filtering, object recognition, scene recognition and intelligent event control.

In addition to DeepStack and CodeProject AI, you can also use other AI servers that support the same API:

Object Recognition & Computer Vision

<https://codeproject.github.io/> - Cross Platform GPU/CPU based AI Processing Server

<https://docs.platerecognizer.com/> - License Plate Recognition Server (Web based API)

<https://github.com/runningman84/docker-coral-rest-server> - Tensorflow-lite models on an RPi (or Linux/Mac) with acceleration from Coral USB stick

<https://github.com/robmarkcole/coral-pi-rest-server/> - Tensorflow-lite models on a Coral USB accelerator via a Flask app

<https://xnorpx.github.io/blue-onyx/> - Blue Onyx Object Detection Service

Cloud AI Services

<https://platform.openai.com/> - OpenAI API (ChatGPT, GPT-4 Vision) for image analysis and chat

<https://console.anthropic.com/> - Anthropic Claude API for advanced reasoning and image understanding

<https://ai.google.dev/> - Google Gemini API for multimodal AI capabilities

<https://docs.anthropic.com/> - Claude API Documentation

<https://platform.openai.com/docs/> - OpenAI API Documentation

<https://ai.google.dev/gemini-api/docs> - Gemini API Documentation

Local AI Servers (LLMs)

<https://ollama.com/> - Ollama: Run large language models locally

<https://docs.vllm.ai/> - vLLM: High-throughput LLM inference and serving

<https://lmstudio.ai/> - LM Studio: Easy-to-use desktop app for local LLMs

<https://github.com/ollama/ollama> - Ollama GitHub repository

<https://github.com/vllm-project/vllm> - vLLM GitHub repository

Note: Cloud AI services require API keys and may incur usage costs. Local AI servers run on your own hardware and keep data private but require more system resources.

Adding AI models

Custom AI models let you extend Agent DVR's object detection beyond the built-in options, for example to recognize wildlife, delivery vehicles or anything else a trained model can find. To add your own model files into Agent DVR, go to **Server Settings > AI Settings** and click **Object Recognition** under **AI Models**. Agent comes with two pre-built models that have been performance tuned for Agent DVR.

Before you configure a model, you will need to add it to Agent DVR's Models folder (see [building AI models](#)). This is usually found at **Agent/Media/Models/ONNX** (path may vary by OS). The full path is displayed on the Add Model page if you are unsure. Agent uses **.onnx** models. You can convert other AI model formats to ONNX using Python tools.

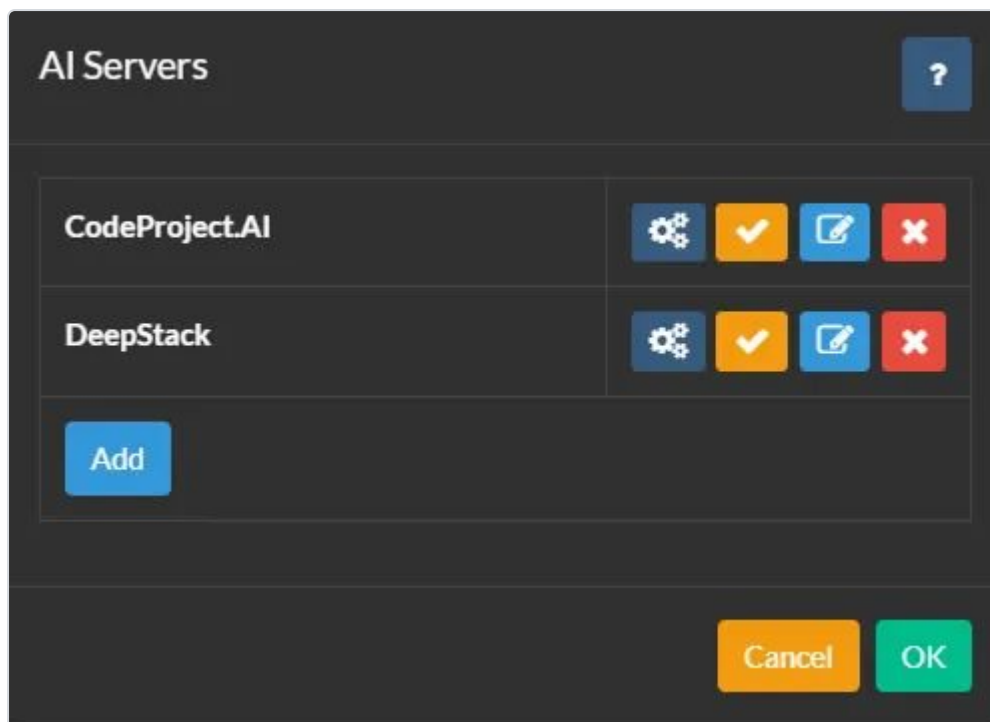
Once you've built and copied the model, adding it to Agent is easy - click to add a model:

Name: Give your model a name - this can be anything you like.
Description: An optional description of what the model does.
Model File: Select the model filename you copied into the folder.
Labels: Enter a list of labels (or "classes") that your model looks for in CSV format without quotes (spaces are automatically trimmed).
Layout: Select whether your model is NCHW or NHWC. Most models are NCHW if you are unsure.
Channel Order: Select if your model wants images in RGB or BGR. Most models use RGB. If your model is single channel (grayscale) this will be ignored.
Normalize: Select how the data should be normalized before it's used in your model. Most models use Rescaling (0-1), which divides pixel values by 255.
Pad Image: This controls whether the image should be stretched to the input dimensions or padded with black bars. Usually it's better to pad images for accuracy.
Has NMS: Check this if your model already performs Non-Maximum Suppression internally. Otherwise Agent will perform NMS itself. NMS controls how result rectangles are filtered.
Default NMS: Set the overlap limiter for NMS (default is 45% overlap).

Once you have added your model, it will be available for use in your device's [Object Recognition](#) tab. If you have problems, you can come back to the model configuration and make changes. Agent also supports reloading the model file, so you can copy over it with a new version while it's running.

Setting up AI Servers

Newer versions of Agent DVR have AI built into them enabling much faster processing and less overhead. Use the [local AI](#) which can respond in real-time instead of slower AI servers.



To set up AI Servers, click on the  icon at the top right of the main Agent DVR UI. Then click on **Settings** under **Configuration**, select **AI Settings** from the dropdown menu, and click **AI Servers**.

Agent DVR integrates with [CodeProject.AI](#) for various AI features including object recognition, face recognition, ALPR (Automatic License Plate Recognition), and super resolution (enhance).

PlateRecognizer.com is also supported as an ALPR provider. CodeProject.AI is open source, free, and compatible with most platforms.

To start, install an AI server for your platform and connect Agent DVR to it by clicking **AI Servers** and then **Add**.

You can add as many AI servers to Agent DVR as needed. Cameras in Agent DVR can be configured to use different AI servers for each function, or you can use one AI server for all tasks.

Warning: AI processing can be resource-intensive. Ensure your computer has adequate power to run it.

Configuring your Server

Name: Name your server, e.g., Cat Catcher.

AI Server URL: Enter the URL of your AI server, e.g., <http://localhost:32168/>

API Key: Enter your key if set up (optional).

Timeout: The timeout in seconds for server requests.

Retry delay: The time in seconds before retrying a failed request to this server.

Click **OK** to save your settings.

Using OpenAI

To set up OpenAI ("ChatGPT") to answer questions about what's happening in your video feed, navigate to Server Settings  - **AI Settings** and select "OpenAI" under Ask AI.

URL: Enter the URL for the service. The default is "https://api.openai.com/v1/responses".

OpenAI API Key: After registering with OpenAI, go to the [API Keys Page](#) and generate a new secret key. Copy and paste this key into the specified field.

Model: Specify the model to be used. The default is **gpt-5.4-mini**. OpenAI may remove or change this at a later time.

Max Tokens: This sets the maximum token usage per request. If you encounter issues, check the logs at /logs.html as it could be related to token usage.

Once OpenAI is configured, refer to [Ask AI](#) for instructions on how to use it for answering general questions about what's happening in your camera feed.

Using Claude

To set up Claude AI to answer questions about what's happening in your video feed, navigate to Server Settings  - **AI Settings** and select "Claude" under Ask AI.

URL: Enter the URL to the service. Default is "https://api.anthropic.com/v1/messages".

Claude API Key: After signing up for Claude, visit the [API Keys Page](#) and create a new secret key. Copy and paste this key into the field.

Version: Specify the API version to use. The default is **2023-06-01**. This may be removed or changed at some point by Anthropic.

Model: Specify the model to use. The default at time of writing is **claude-sonnet-4-6** (Claude Sonnet 4.6).

Max Tokens: This controls the maximum token spend per request. Check the logs at /logs.html if you have issues as it might be related to token spend.

Once Claude is configured see [Ask AI](#) for how to use it to recognise general scenarios in your camera feed.

Using Gemini

To set up Gemini to answer questions about what's happening in your video feed, navigate to Server Settings  - **AI Settings** and select "Gemini" under Ask AI.

URL: Enter the URL to the service. Default is "https://generativelanguage.googleapis.com".

Gemini API Key: After signing up for Gemini, visit the [API Keys Page](#) and create a new secret key. Copy and paste this key into the field.

Version: Specify the API version to use. The default is **v1beta**. This may be removed or changed at some point by Google.

Model: Specify the model to use. The default at time of writing is **gemini-2.5-flash**. Once you have entered an API key, Agent will list the vision models available to your account.

Max Tokens: This controls the maximum token spend per request. Check the logs at /logs.html if you have issues as it might be related to token spend.

Once Gemini is configured see [Ask AI](#) for how to use it to recognise general scenarios in your camera feed.

Using Other LLM servers

You can use your own local LLM servers (like vLLM, Ollama, and LM Studio) to describe the images Agent DVR captures from your cameras in Alert events and answer questions about what's happening in your video streams. See [Describe Alerts](#) and [Ask AI](#).

To configure a local AI server, go to Server Settings  - **AI Settings** and click the Configure button next to the LLM you want to use (Ollama, vLLM, or LM Studio).

URL: Specify the endpoint where your LLM server is running. Default URLs are:

- Ollama:

```
http://localhost:11434/api/chat
```

- vLLM:

```
http://localhost:8000/v1/chat/completions
```

- LM Studio:

```
http://localhost:1234/v1/chat/completions
```

API Key: If your LLM server requires authentication, enter the API key here. Most local servers don't require this unless specifically configured.

Model: Select the vision-capable model to use for image analysis. You must have already downloaded and loaded this model in your LLM server. Agent suggests some popular options, including:

- Qwen VL models (high performance)
- Gemma 4 (good range of sizes)
- Llama 3.2 Vision (Meta)
- Mistral Small 3.1
- moondream (very small, good for low-end hardware, Ollama only)

Temperature: Controls creativity vs. accuracy in responses (0.0-1.0). Lower values (0.3-0.4) produce more factual, consistent descriptions. Higher values (0.6-0.8) generate more varied, creative responses. Recommended: 0.4 for security camera analysis.

Max Tokens: Maximum number of words/tokens in the AI's response. Higher values allow more detailed descriptions but take longer to generate. Recommended: 300-500 for detailed image analysis, 150-250 for brief descriptions.

top_p: Controls response diversity by limiting vocabulary selection (0.0-1.0). Lower values use more common words, higher values allow more varied vocabulary. Recommended: 0.9 for good balance of accuracy and natural language.

top_k: Limits the model to choosing from the top K most likely next words. Lower values (20-40) produce more focused responses, higher values (80-100) allow more variety. Recommended: 50 for reliable image descriptions.

Note: You must install and configure your chosen LLM server separately. Ensure you have downloaded a vision-capable model before configuring Agent DVR. For best results with security cameras, use models with at least 7B parameters and ensure your system has adequate VRAM (5GB+ recommended).

Using PlateRecognizer.com

To configure LPR (ANPR or License Plate Recognition) in Agent DVR, go to Server Settings  - AI Settings and enter the details under **Plate Recognizer**. Sign up for a Free Trial at [Plate Recognizer](#). No credit card required.

URL: Enter the URL to the service. Default is "https://api.platerecognizer.com/v1/plate-reader/", or use your own server if hosting your own instance.

Token: After signing up for Plate Recognizer, visit the [Account Page](#) and copy the **API Token**.

Regions: Leave blank for default or enter a CSV list of [regions](#).

Config: Enter additional configuration values [from the docs](#) if needed.

Using DoubleTake

DoubleTake is an open source platform that provides a unified API for processing facial recognition using:

CompreFace

Amazon Rekognition

DeepStack

CodeProject.AI Server

Facebox

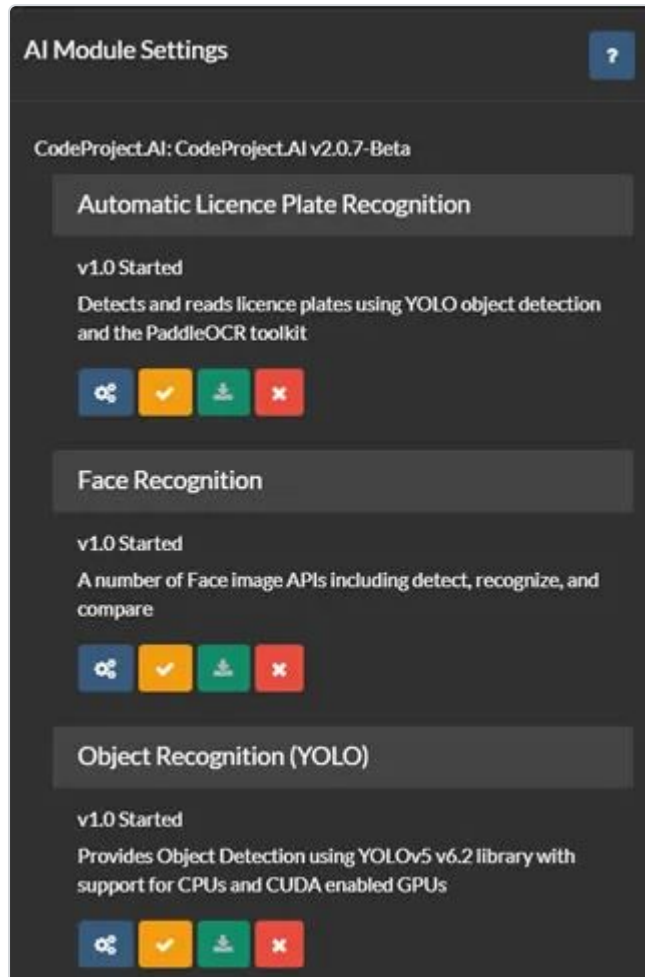
You will need to install and configure [DoubleTake](#) with your preferred facial recognition options.

Once DoubleTake is set up, open Agent DVR and go to Server Settings  - **AI Settings** and click the Configure button next to DoubleTake.

Enter the URL to your doubletake server (e.g. <http://localhost:3000/>) and your password if set up.

Click OK, then edit a camera and go to Facial Recognition. Set the AI Server option to DoubleTake and [configure facial recognition](#) as needed.

Managing AI Modules



In the AI server list (referenced above), you have options to configure, test, edit, and remove AI servers. Click on the configure  button to display the modules available or installed on the selected server.

Agent DVR retrieves the current module list from your server and offers a user interface for installing, uninstalling, configuring, and testing each module. Support is provided for all default CodeProject.AI modules, although Agent DVR only utilizes a subset of these.

It is recommended to install only one of the Object Recognition module options. Review the description of each to determine the best fit for your system.

To utilize ALPR (Automatic License Plate Recognition), Super Resolution, or Face Recognition in Agent DVR, you will need to install the respective module from this page. Typically, default settings suffice for these modules, but you can configure them by clicking on the  icon under each module.

Configuration

Local Object Recognition

Agent DVR supports live **real-time** object recognition using AI model files (.onnx). This local AI object detection runs entirely on your own hardware (no cloud service required), so you can be alerted only when something that matters appears, like a person or a car, instead of every time a tree moves. You will need a [license](#) (or active subscription) to use this feature. See [AI Servers](#) for configuring Agent to use external AI servers.

To get started, edit your camera and go to the **Object Recognition** tab. Choose your AI server at the top. The default is **Internal**, which is Agent DVR's built-in AI. If you want to use an AI server, add it in Server Settings - AI Settings - AI Servers and then select it here.

The following details are for configuring Agent DVR with its fast built-in AI. You can also add any other models you like, for example [Ultralytics YOLO models](#).

Model: Select the AI model you want to use. Agent will automatically download built-in models as needed. The **Small** model is good for low-end hardware or lots of cameras. The **Medium** model is good for better accuracy but uses more processing power.

Mode: Select when you want AI to process frames from your video. If you select **Interval**, Agent will use the **Processing Rate** field below to continuously analyze your video feed.

Configure Overlay: Set up drawing real-time results on live video: enable the overlay, show labels and confidence, set line width and colors, or blur recognized objects (for example, people). The overlay is great for tuning the confidence limit.

Use GPU: Check this to use your GPU instead of CPU.

Device: Select the device to run the model on.

Processing Rate: This is only used when **Mode** is **Interval** - it controls the rate that frames are sent to the model. Enter 1 for 1 frame per second, 20 for 20 frames per second or 0.1 for 1 frame every 10 seconds.

Confidence: This filters the results from the model. Adjust this higher to reduce false positives, but note it may also miss objects.

Check Corners: Refer to [Checking Corners](#) for more details.

Find: Specify objects for the AI to detect. The list of options here comes from the model configuration.

Static Objects: Choose how to filter objects that aren't moving. **Ignore Static Objects** ignores objects detected repeatedly in the same position (like parked cars); they still alert the first time they appear.

Moving Only only reports objects where the motion detector currently sees movement, so still objects never alert (no effect with camera-side detectors like ONVIF, Reolink, Hikvision or MQTT).

Movement Tolerance: Allowed movement between detections when checking for static objects. Low values rarely match; high values suppress more. Recommended: 40-60.

Learn From Feedback: Let Agent learn from you. With this enabled you can confirm or reject detections in the alert viewer and Agent will learn to suppress similar false alerts on this camera. See [Learning From Feedback](#).

Custom Models

To add your own models to AI, copy the model file (.onnx) into Agent's Models folder and see [Adding Models](#).

Actions

Object Recognition generates **AI: Object Found** and **AI: Object Not Found** events for use in [Actions](#).

Photos

For information on photos, see [Photos](#).

Learning From Feedback

Agent DVR can learn from your feedback to reduce false alerts, camera by camera. When a detection gets it wrong - a bush that looks like a person at night, a flag the AI keeps calling a bird - you can tell Agent and it will learn to suppress similar detections on that camera in the future. Everything runs **100% locally**: no images or data ever leave your machine, and the detection model itself is never modified, so this is always safe to use and easy to reset.

Enabling

Edit your camera, go to the **Object Recognition** tab and switch on **Learn From Feedback**. Agent will automatically download a small embedding model the first time it's needed.

Giving Feedback

With feedback enabled, alerts generated by object recognition store the detection results alongside the alert image. Open an alert in the [Alerts panel](#) and you'll see boxes drawn over each detection with a **"Did we get this right?"** prompt:

✓ **Correct:** Confirms the detection. Confirmed examples protect similar detections from ever being suppressed.

✗ **Incorrect:** Rejects the detection. Agent learns the appearance of rejected detections for that camera and object type. After a few rejections of similar-looking detections (at least 3), Agent starts suppressing matching false alerts automatically.

You can change or remove a verdict at any time by clicking the button again.

The **"Did we get this right?"** panel collapses - click its header to hide or show the prompts and detection overlays. Agent remembers your choice (per browser), so once you're happy with how a camera is performing you can collapse the panel and just see clean alert images. Collapsing the panel never stops the learning - suppression keeps working. To stop learning entirely, switch off **Learn From Feedback** on the camera instead (note this also stops suppression).

Suppressed Alerts

Suppression is deliberately conservative - a detection is only suppressed when it clearly matches your rejected examples and doesn't match any confirmed ones. When Agent suppresses what would otherwise have been an alert, it stores a **suppressed alert** instead so nothing ever disappears silently. Click the  icon in the Alerts panel header to show or hide them (the icon only appears when suppressed alerts exist; they're kept separately and don't count against your normal alerts).

If Agent suppressed something it shouldn't have, open the suppressed alert and mark the detection as **Correct** - this lifts the suppression for similar detections immediately.

How It Works

Agent uses a general-purpose vision model to create a compact mathematical "fingerprint" of each detection. Your verdicts file these fingerprints as confirmed or rejected examples per camera and object type. Future detections are compared against your examples by similarity - the same approach used by [Facial Recognition](#). Your chosen detection model and its classes are untouched.

Resetting

To remove everything a camera has learned, click **Clear Learning** on the camera's **Object Recognition** tab and confirm - suppressed alerts will start alerting again. Learned feedback is stored in **FeedbackDB.json** in Agent's XML folder; the **clearfeedback** API command is also available (optionally with **cameravid** and **label** parameters). Learned feedback (and learned faces) are included in the server configuration export/import, so your training moves with your settings to a new computer.

Copying Learning Between Cameras

You can copy a camera's learned feedback to other cameras with **Copy Settings** - tick **Learning** (under **Object Recognition**) in the section list. This replaces the target cameras' learning with a copy of the source's. It's most useful for cameras covering the same or a similar scene - learned examples are appearance-based, so feedback about a bush on one camera only helps another camera that can see something like that bush.

Converting Ultralytics YOLO Models to ONNX

Agent DVR supports ONNX model files for object recognition. You can download pretrained models and convert them to ONNX format in a few steps.

The example below uses the YOLO26s model via Ultralytics. YOLO26s is a smaller, general-purpose model with a good speed/accuracy trade-off.

Prerequisites

Python 3.10 or newer
pip available in PATH
Internet connection
~1-2 GB free disk space

Step 1 - Install Ultralytics

```
pip install ultralytics
```

Step 2 - Download the YOLO26s Model

Ultralytics automatically downloads the pretrained weights when first used:

```
yolo detect predict model=yolo26s.pt source=https://ultralytics.com/images/bus.jpg
```

Step 3 - Convert to ONNX

Once downloaded, export the model to ONNX format:

```
yolo export model=yolo26s.pt format=onnx opset=12 simplify=True
```

Python Alternative

```
from ultralytics import YOLO

model = YOLO("yolo26s.pt")
model.export(format="onnx", opset=12, simplify=True)
```

Step 4 - Locate the ONNX File

The exported `yolo26s.onnx` file will be created in your working directory or in the

```
runs/export
```

folder.

Step 5 - Copy to Agent DVR

Move the ONNX file into your Agent DVR ONNX models folder (on the Agent server), for example:

```
Agent\Media\Models\ONNX\
```

Step 6 - Add the Model in Agent DVR

Go to **Server Settings** > **AI Settings** > **AI Models**.

Click **Object Recognition** and add a new model.

Enter a name e.g. `yolo26s` and select the `.onnx` file in the dropdown.

Leave the remaining options at their defaults and click **OK**.

Edit your camera, open the **Object Recognition** tab, set **Server** to **Internal**, and choose your new model.

Local Face Recognition

Agent DVR supports live **real-time** facial recognition using AI, running locally on your own hardware. Use it to know who is at the door and trigger different actions for recognized and unknown faces. You will need a [license](#) (or active subscription) to use this feature. See [AI Servers](#) for configuring Agent to use external AI servers.

To get started, edit your camera and go to the **Facial Recognition** tab. Choose your AI server at the top. The default is **Internal**, which is Agent DVR's built-in AI. If you want to use an AI server, add it in Server Settings - AI Settings - AI Servers and then select it here.

The following details are for configuring Agent DVR with its fast built-in AI.

Mode: Select when you want AI to process frames from your video. If you select **Interval**, Agent will use the **Processing Rate** field below to continuously analyze your video feed.

Configure Overlay: Set up drawing real-time results on live video: enable the overlay, show labels and confidence, set line width and colors, or blur faces. The overlay is great for tuning the confidence limit.

Use GPU: Check this to use your GPU instead of CPU.

Device: Select the device to run the model on.

Processing Rate: This is only used when **Mode** is **Interval** - it controls the rate that frames are sent to the model. Enter 1 for 1 frame per second, 20 for 20 frames per second or 0.1 for 1 frame every 10 seconds.

Confidence: This filters the results from the model. Adjust this higher to reduce false positives, but note it may also miss people.

Check Corners: Refer to [Checking Corners](#) for more details.

You can choose which face recognition model Agent uses in Server Settings - AI Settings - AI Models - Face Recognition.

Faces to Recognize

Click Edit Faces to upload photos of people you want to recognize. You can upload multiple photos of the same person to improve results. You can upload images from your file system or use a built in webcam to capture photos (requires SSL or localhost).

Actions

Facial Recognition generates **AI: Face Recognized** and **AI: Face Not Recognized** events for use in [Actions](#).

Photos

For information on photos, see [Photos](#).

Local License Plate Recognition

Agent DVR supports live **real-time** license plate recognition, running locally on your own hardware. Use it to log every vehicle entering a driveway or car park and trigger actions, like opening a gate, when a known

plate is recognized. You will need a [license](#) (or active subscription) to use this feature. See [AI Servers](#) for configuring Agent to use external AI servers.

To get started, edit your camera and go to the **LPR** tab. Choose your AI server at the top. The default is **Internal**, which is Agent DVR's built-in AI. If you want to use an AI server, add it in Server Settings - AI Settings - AI Servers and then select it here.

The following details are for configuring Agent DVR with its fast built-in AI.

Mode: Select when you want AI to process frames from your video. If you select **Interval**, Agent will use the **Processing Rate** field below to continuously analyze your video feed.

Configure Overlay: Set up drawing real-time results on live video: enable the overlay, show labels and confidence, set line width and colors, or blur detected license plates. The overlay is great for tuning the confidence limit.

Use GPU: Check this to use your GPU instead of CPU. Note that this currently only works on Windows or macOS due to GPU driver and runtime support. Linux currently falls back to CPU.

Device: Select the device to run the model on.

Processing Rate: This is only used when **Mode** is **Interval** - it controls the rate that frames are sent to the model. Enter 1 for 1 frame per second, 20 for 20 frames per second or 0.1 for 1 frame every 10 seconds.

Confidence: This filters the results from the model. Adjust this higher to reduce false positives, but note it may also miss objects.

Check Corners: Refer to [Checking Corners](#) for more details.

License Plates to Look For

License Plates: Enter a comma-separated list of plates or a URL to a CSV file containing plates. Agent DVR will generate **License Plate Recognized** and **License Plate Not Recognized** events for these plates, which can trigger actions.

Reload Interval: Set the frequency for reloading the plate list from the URL.

Normalize: Adjust commonly misidentified plates to improve matching.

Actions

LPR generates **AI: License Plate Recognized** and **AI: License Plate Not Recognized** events for use in [Actions](#).

Photos

For information on photos, see [Photos](#).

AI Alert Filtering

Alert filtering combines motion detection with AI so you only get alerted when something that matters is detected, like a person on the porch, rather than moving branches or passing headlights. It's the most effective way to reduce false alarms. To set up Alert filtering in Agent DVR, follow these steps:

Configure and enable a [Motion Detector](#). For minimal CPU usage, use the Simple detector. Ensure at least one zone is defined to cover the area you want to monitor.

On the [Alerts tab](#), set the Mode to **Actions Only** and enable Alerts.

On the recording tab, set the Mode to **Alerts** (if you want recordings)

Enable Object Recognition on the [Object Recognition](#) tab. Set the mode to **Motion Detected**, select a model, and click **Find** to choose objects for detection, like Person, Dog, Car, etc.

Go to **Actions** in the tab menu and add an Action for the event **AI: Object Found**.

Select zones to specify where to detect objects, like different zones for your driveway and the road. For instance, selecting the driveway zone will only trigger an alert if a car is detected there.

Under **Tasks**, click Add to create an **Alert** task. Click OK twice to confirm.

Agent DVR will process AI object recognition upon motion detection. If it detects a specified object in a chosen zone, it will trigger an action to raise an alert. Absence of zone selection will trigger alerts for any zone.

Set up alert filters similarly for [LPR Recognition](#), [Face Recognition](#), or [Audio Recognition](#).

For constant AI object recognition without a motion detection trigger, set the **Mode** on Object Recognition to **Interval**. Monitor the impact on your hardware resources and adjust as needed.

You can configure multiple actions for different objects in various zones. Use the {AI} tag in actions to reference the detected object.

If your AI server is non-responsive and you're using it to filter **motion detection** Alerts, Agent DVR will treat all events as valid alerts until the server resumes. This behavior can be toggled with the **Motion Pass-through** switch under Object Recognition.

Utilize filters in your [actions](#) to execute different responses based on Agent DVR's detections. For example, you could configure a verbal "intruder detected" alert for a person at a doorway, or play a barking sound if a cat is detected on your couch.

AI Filter Troubleshooting

If AI isn't effectively filtering your recordings, consider the following:

Ensure the **Find** setting matches one of the Available options.

Verify that the master alert switch at the top left of Agent DVR shows a closed padlock, indicating active alerts.

Confirm that the recording mode is set to **Alert** and not Detect.

Ensure the alert mode is set to **Actions Only**.

Try lowering the Confidence level under Object Recognition.

Check /logs.html for error messages, possibly indicating server issues or network blocks.

Monitor AI server performance and ensure it's not causing system overload or timeouts.

If AI detects all object classes, it may indicate GPU issues. Check GPU drivers or switch to a CPU-based AI module.

AI Object Recognition

Object Recognition

Off

AI Server

local

Add or edit AI servers in Server Settings - AI Settings

Mode

Alert

When to run this AI process

Configure Overlay

AI Photos

Save photos when objects are recognized using AI

Minimum Interval

1

Minimum time between requests (seconds)

Confidence

60

Minimum Confidence

Model

AI uses models to look for specific things

Discover

Get Models

Click to find available AI models

Model

/v1/vision/custom/license-plate,/v1/vision/detection

Available (click to select):

default

ipcam-animal

ipcam-combined

ipcam-dark

ipcam-general

license-plate

Click Get Models to find models

Object Classes

dayplate,nightplate,person,bicycle,car,motorcycle,airplane,bus,train,truck,boat

Only modify this if you are using [customised object classes](#)

Objects to look for

Specify objects to look for. [Use actions](#) in the menu to act on found or missing objects

Find

Select the objects to look for

Advanced Settings

6

Cancel

OK

Object Recognition in Agent DVR uses either our [local AI](#) or an AI server (CodeProject.AI recommended) to recognize specific objects in video feeds and can generate events, raise alerts, or act as a [filter on motion alerts](#).

Enabled: Toggle to enable or disable the AI process.

AI Server: Select from your configured [servers](#), or use the default option.

Mode: Choose the trigger for the AI process. Trigger via API only by setting this to None and calling [triggerObject](#).

Motion Pass-through: If the AI server is down and filtering alerts, this allows alerts to pass through without filtering.

Use Snapshot URI: Use a high-resolution frame from your camera instead of the current live stream frame.

Resize Mode: Resize images before sending them to the AI server to reduce load and improve response times.

Configure Overlay: Set up drawing AI results on the live video stream, including labels, confidence, line width, colors and blurring.

Request Interval: Set the minimum time between server requests.

Confidence: Set the minimum confidence level to recognize an object.

Check Corners: Refer to [Checking Corners](#) for more details.

Models

Discover: Retrieve installed models from your server (specific to CodeProject.AI).

AI Endpoint: Choose from available models or use the default endpoint.

AI Object Classes: Automatically populated with relevant classes or manually entered.

Find: Specify objects for the AI to detect.

Static Objects: Filter objects that aren't moving. **Ignore Static Objects** ignores objects detected repeatedly in the same position; **Moving Only** only reports objects where the motion detector currently sees movement.

Movement Tolerance: Allowed movement between detections when checking for static objects.

Custom Models

To add custom models to CodeProject.AI, copy the model file to the specified directory. Access it via the Discover button, but manually add the object list to **Object Classes**.

Change the directory for model storage by editing the Object Recognition module settings.

Actions

Object Recognition generates **AI: Object Found** and **AI: Object Not Found** events for use in [Actions](#).

Photos

For information on photos, see [photos](#).

Ask AI

Agent DVR uses AI servers (OpenAI/ Claude/ Gemini/ Local LLMs like Ollama, LM Studio, vLLM etc) to answer human readable questions about the images from your cameras. This can then generate events, raise alerts, or act as a [filter on motion alerts](#). You will need to complete the settings in Server Settings - AI Settings - [Ask AI](#).

There may be a third-party cost associated with using the selected AI provider's API so be sure to check that your setup is only sending requests when you need to. **Google offers a free usage tier for Gemini API keys on personal Google Accounts; check Google's current pricing for limits.**

You can check the Logs at /logs.html on the local server to see when requests are sent. Set the Server Settings - Logging - Log Level to Info.

Enabled: Toggle to enable or disable the AI process.
Provider: Choose which AI provider you want to use to process images. The provider will need to be configured in server settings - AI Settings. If you select Default then the first configured provider will be used.
Mode: Choose the trigger for the AI process. Trigger via API only by setting this to None and calling triggerAskAI
Motion Pass-through: If the AI server is down and filtering alerts, this allows alerts to pass through without filtering.
Use Snapshot URI: Use a high-resolution frame from your camera instead of the current live stream frame.
Resize Mode: Resize images before sending them to the AI server to reduce load and improve response times.
Configure Overlay: Set up drawing AI results on the live video stream.
Request Interval: Set the minimum time between server requests.
Detail Mode: Choose Low or High image detail. Low is cheaper to use than High and fine for most scenarios.
Use Video: Send a short video clip instead of an image (Gemini only). Set the Duration in seconds and check Include Audio to send sound along with the video.

AI Messaging

Message: Enter your question for AI here. Some examples:

If you see fire in this image respond with FIRE. If you see a dog sitting on a sofa, respond with DOG. If the door is open respond with DOOR. If multiple conditions are met separate them with a ,

If the light on the machine on the bench is red respond with ALERT

If a police car is parked in the driveway respond with POLICE

If there is any mail or packages on the floor respond with MAIL

If it looks like someone has broken into my house respond with BREAKIN

Find: Enter the tags that you have instructed AI to respond with. For example FIRE, DOG, DOOR

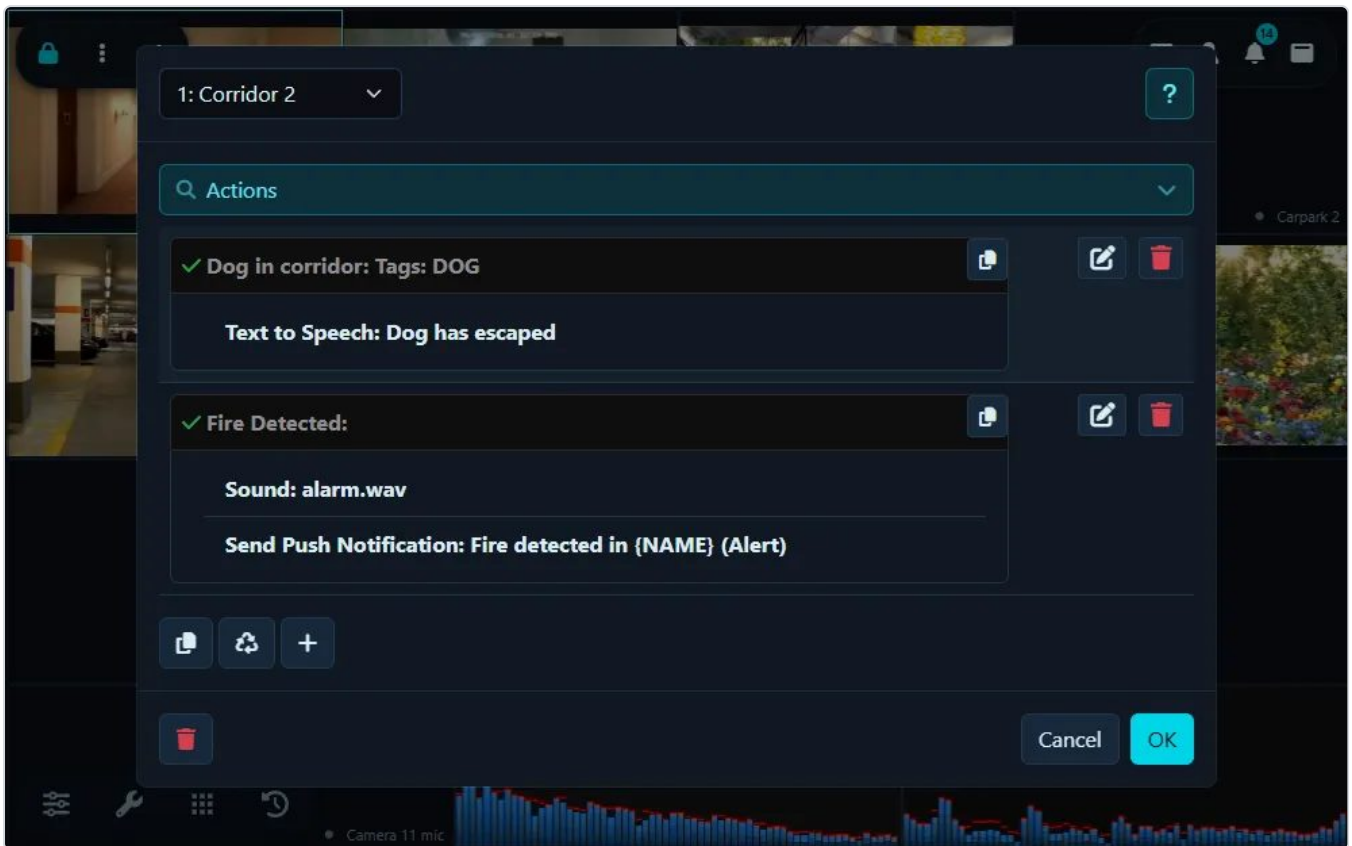
No Repeats: Ignore tags that were returned in the last call to AI

As noted above you can ask for multiple conditions to be met in the message and set up actions to handle each result.

Tip! You can add the special tag [TIME] into your messages to pass the current local time to AI - which lets you perform checks based on time of day. For example, "The current time is [TIME] if that is later than 8pm and the garage door is open respond only with GARAGE"

Actions

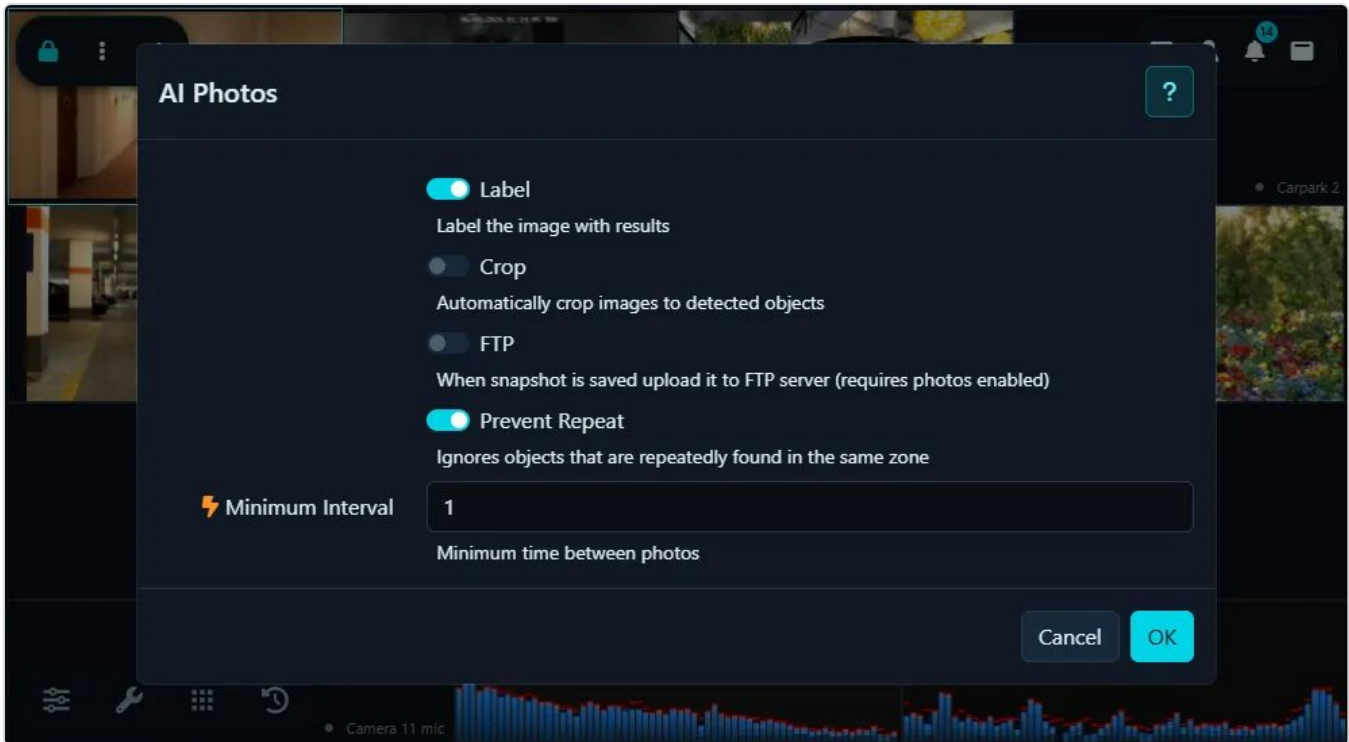
Ask AI generates **AI: Ask AI Positive Result** events for use in [Actions](#).



Photos

For information on photos, see [photos](#). Note that AI doesn't yet return any spatial data about where things are in the image so crop and static detection are currently not working.

AI Photos



AI processes can capture photos when objects are recognized, offering options for saving, cropping, FTP uploading, and more.

To configure this, go to the **Photos** option at the bottom of each AI configuration tab when editing a camera. Enable Photos and click to configure.

Label: Agent DVR overlays boxes on the image and labels the detected objects.

Crop: Agent DVR crops the image to each detected area and saves multiple images, one for each region.

FTP: Uploads the saved images to the camera's configured FTP server.

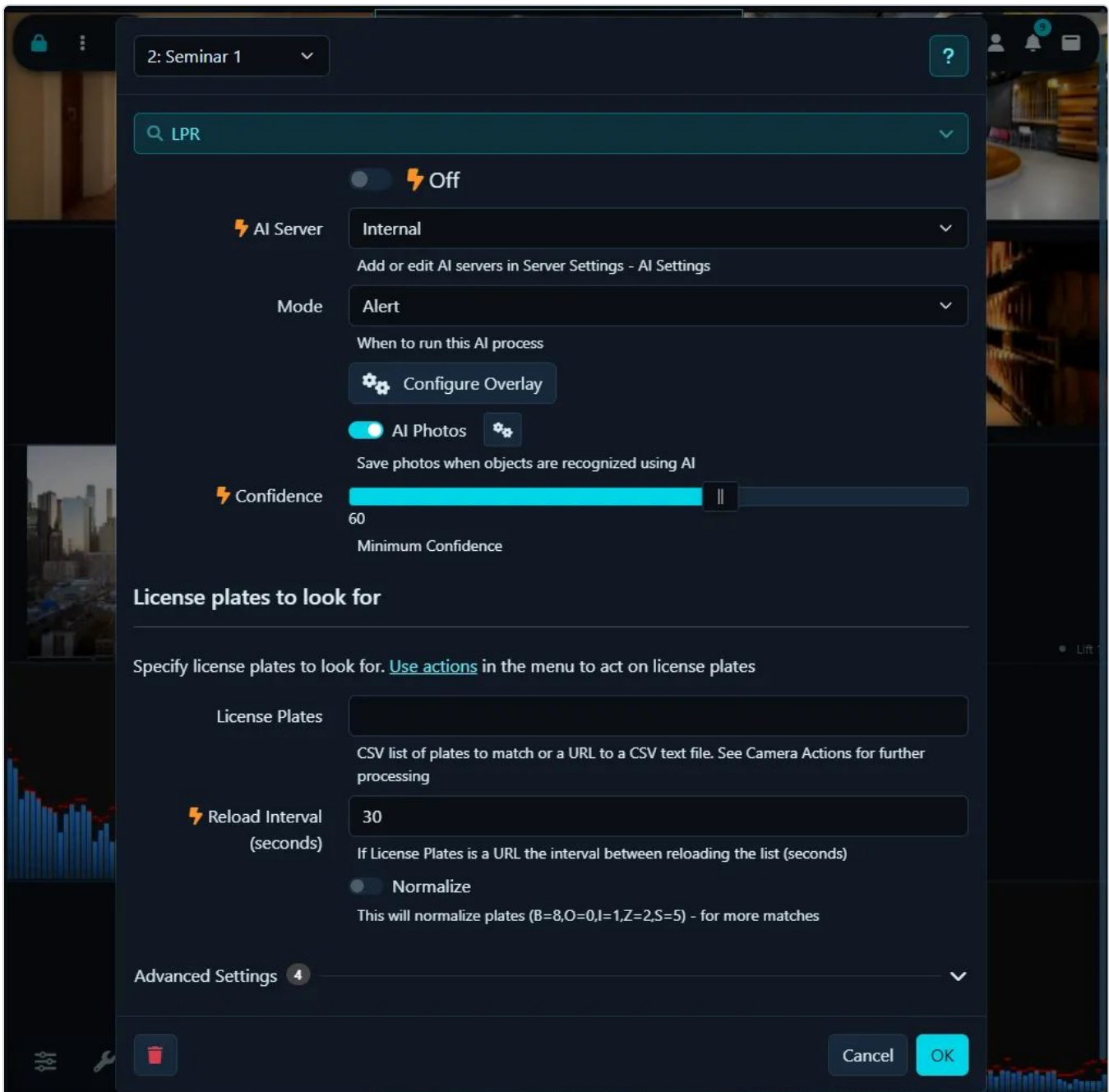
Prevent Repeat: Agent DVR avoids saving multiple copies of the same object until it leaves the motion zone.

Minimum Interval: Set the minimum time between photos, in seconds.

Exercise caution with AI photos settings as incorrect configurations can lead to an excessive number of images being saved. Monitor the frequency of saved images after setup.

LPR or ALPR

Newer versions of Agent DVR have AI built into them enabling much faster processing and less overhead. Use the [local AI](#) which can respond in real-time instead of slower AI servers.



LPR (License Plate Recognition, also known as ALPR/ ANPR) utilizes an AI server to recognize and read license plates from cars in your video feeds. It generates events, raises alerts, or acts as a filter on motion alerts.

Enabled: Toggle to enable or disable the AI process.

AI Server: Choose from your configured [servers](#) or use the default option. Agent DVR supports LPR via CodeProject.AI, PlateRecognizer.com, Gemini or any OpenAI compatible vision LLM (like vLLM, Ollama and LM Studio).

Mode: Choose the trigger for the AI process. Trigger via API only by setting this to None and calling [triggerLPR](#).

Use Snapshot URI: Opt for a high-resolution frame from your camera instead of the current live stream frame.

Resize Mode: Resize images before sending them to the AI server to reduce load and improve response times.

Configure Overlay: Set up drawing AI results on the live video stream.

Request Interval: Set the minimum time between server requests to reduce load.

Confidence: Define the minimum confidence level to recognize a license plate.

Check Corners: Refer to [Checking Corners](#) for more details.

License Plates: Enter a comma-separated list of plates or a URL to a CSV file containing plates. Agent DVR will generate **License Plate Recognized** and **License Plate Not Recognized** events for these plates, which can trigger actions.

Reload Interval: Set the frequency for reloading the plate list from the URL.

Normalize: Adjust commonly misidentified plates to improve matching.

Make, Model, and Color: Enable this **only** if using a paid plan on PlateRecognizer.com that supports these features. It's **not** included in the free plan. Details will be included in {AIJSON} in Agent DVR Actions.

Actions

LPR generates **AI: License Plate Recognized** and **AI: License Plate Not Recognized** events for use in [Actions](#).

Photos

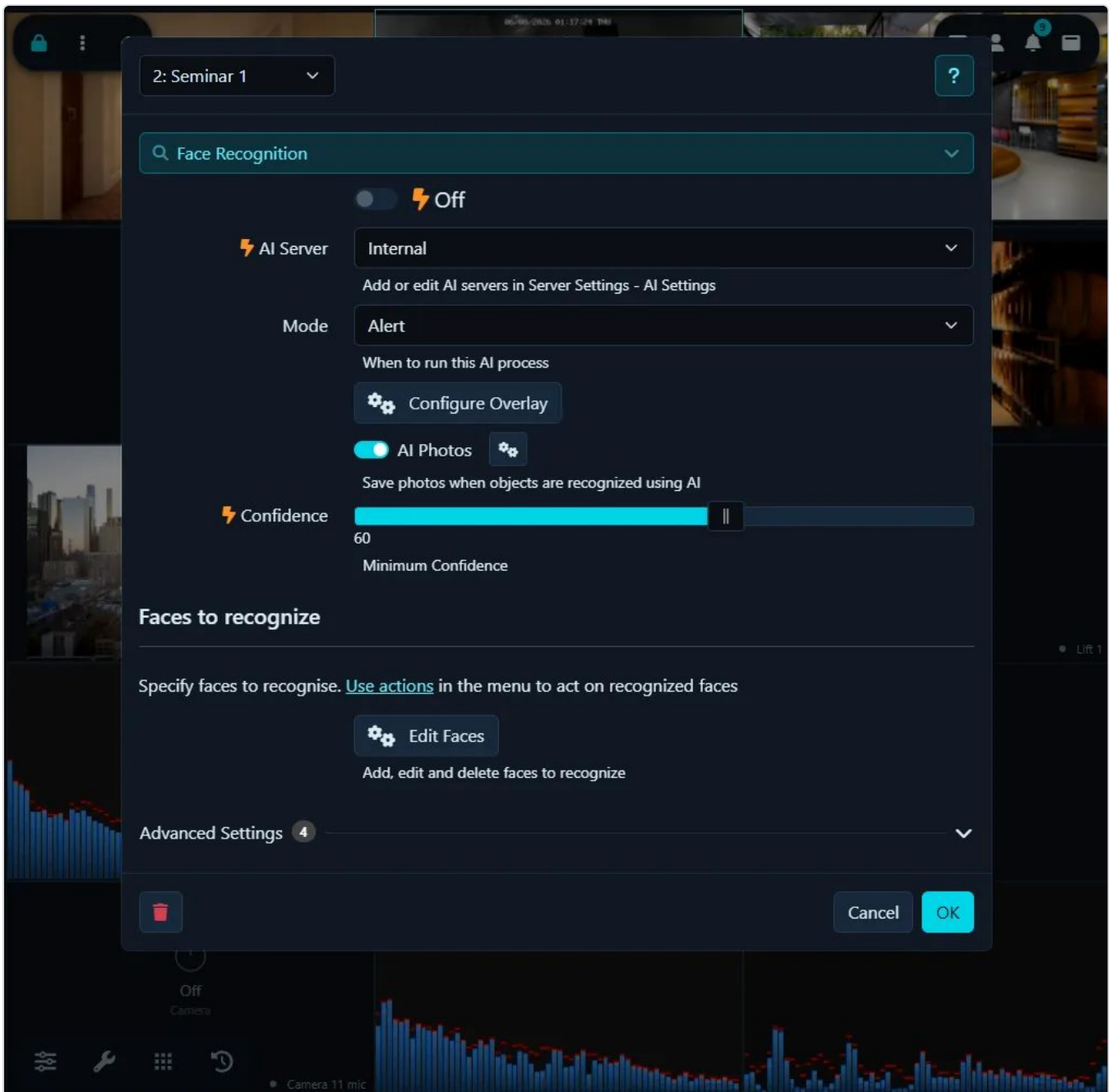
For information on photos, see [photos](#).

Using ALPR-Database

You can set up an integration with ALPR-Database.com to store your license plates. See [Agent DVR with ALPR-Database](#) for instructions.

AI Face Recognition

Newer versions of Agent DVR have AI built into them enabling much faster processing and less overhead. Use the [local AI](#) which can respond in real-time instead of slower AI servers.



Face Recognition utilizes an AI server (recommended: CodeProject.AI) to recognize specific faces in video feeds. It can generate events, raise alerts, or act as a [filter on motion alerts](#). Faces can be added, edited, or deleted using your camera or by uploading images. See **Edit Faces** in this tab for more.

Enabled: Toggle to enable or disable the AI process.

AI Server: Select from your configured [servers](#), or use the default option.

Mode: Choose the trigger for the AI process. Trigger via API only by setting this to None and calling [triggerFace](#)

Use Snapshot URI: Opt for a high-resolution frame from your camera instead of the current live stream frame.

Resize Mode: Resize images before sending them to the AI server to reduce load and improve response times.

Configure Overlay: Set up drawing AI results on the live video stream.

Request Interval: Set the minimum time between server requests to reduce load.

Confidence: Define the minimum confidence level to recognize a face.

Check Corners: Refer to [Checking Corners](#) for more details.

Edit Faces: Upload images to the server database for recognition. Ensure that only one face is visible and clearly defined in each image.

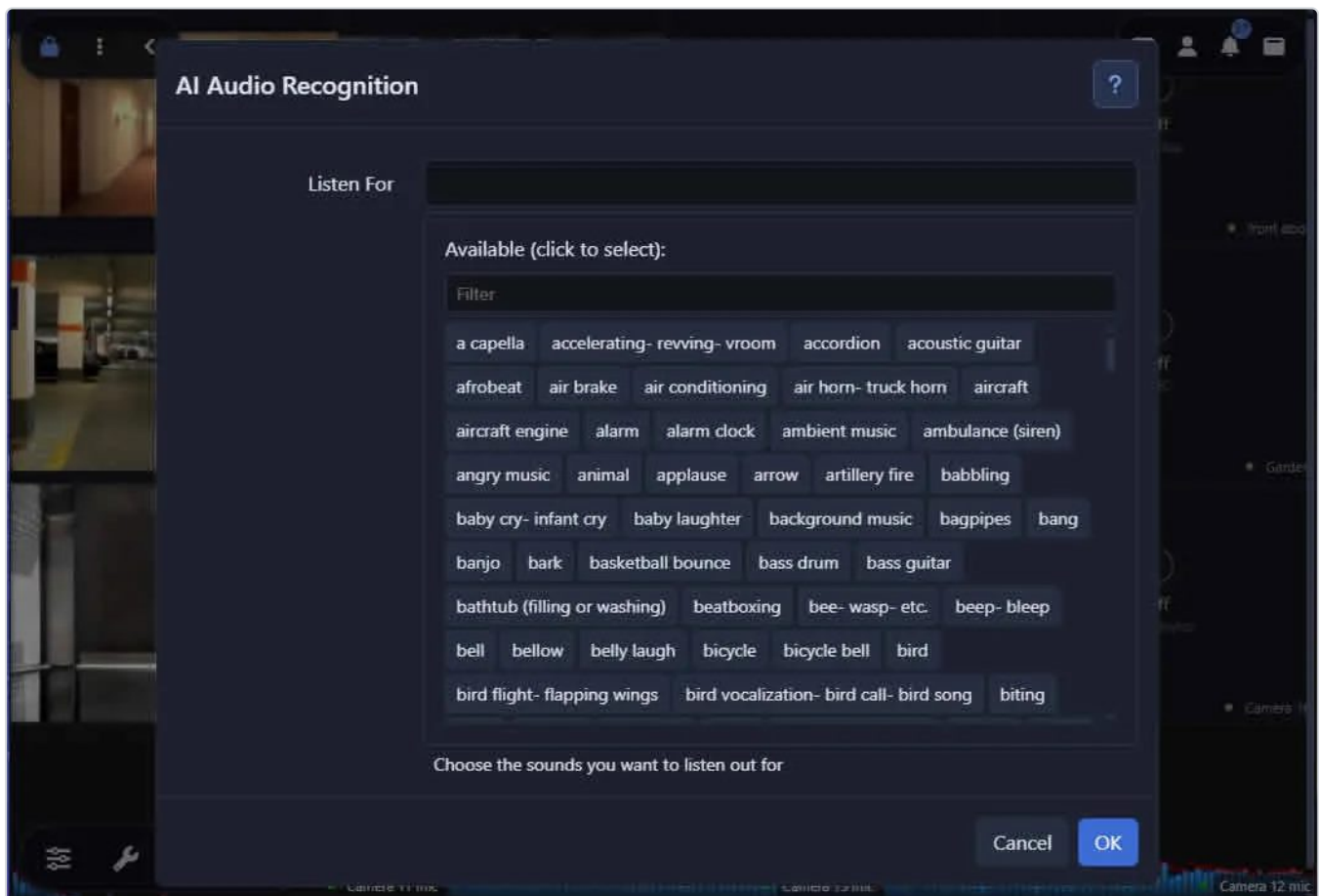
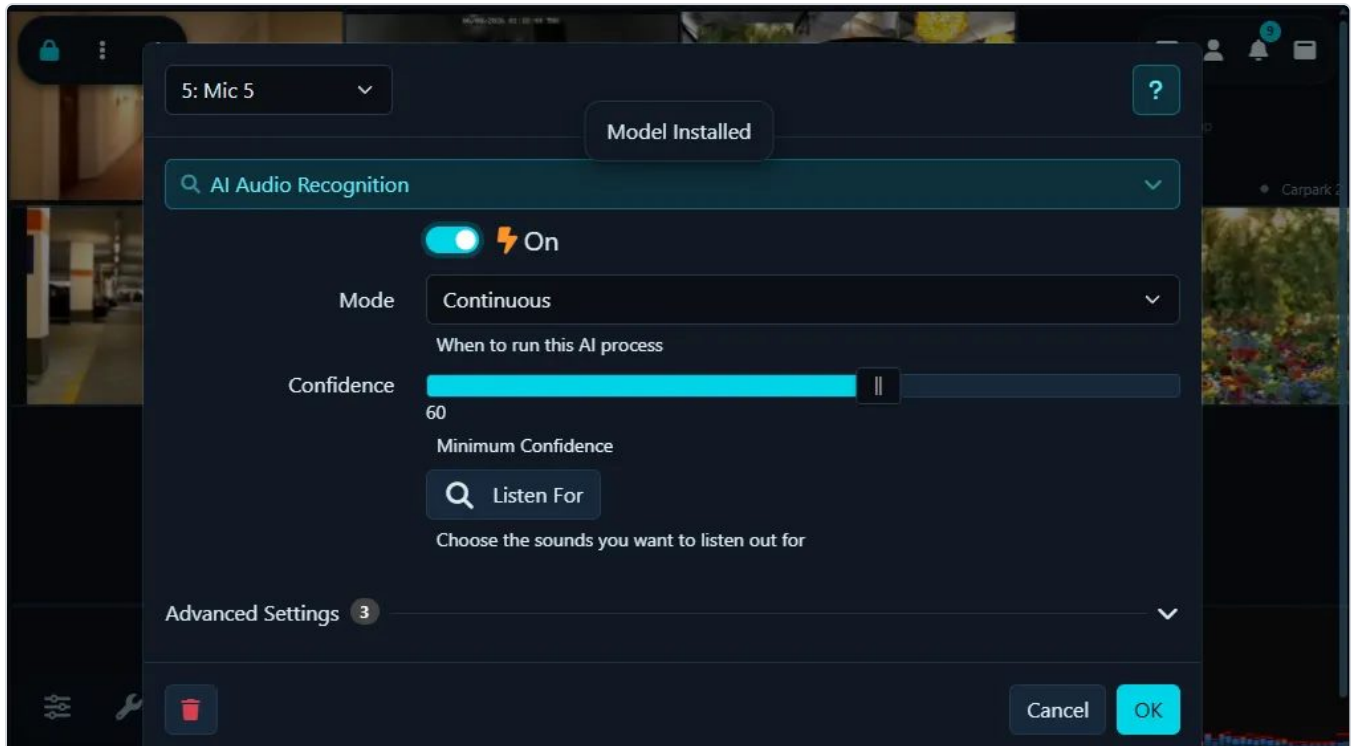
Actions

Face Recognition generates **AI: Face Recognized** and **AI: Face Not Recognized** events for use in [Actions](#).

Photos

For information on photos, see [photos](#).

AI Audio Recognition



AI-based audio recognition in Agent DVR responds to recognized sounds from microphones or audio streams.

You will need to edit the Microphone settings to set up audio recognition. If you have a camera with an audio stream you can access the audio settings by editing the camera, selecting the Audio tab and clicking "Configure".

Enabled: Toggle to enable or disable the AI process.
Mode: Choose the trigger for the AI process.
Confidence: Set the minimum confidence level for sound recognition.
Listen For: Select specific sounds for the AI to detect.
Overlay: Displays recognized sounds on the live audio visualization. Only the sounds you have chosen under Listen For are shown, so what appears on screen matches what raises alerts.
Overlay All Sounds: Also display sounds you are <i>not</i> listening for, so the overlay shows everything the model recognizes. Useful for working out why a sound isn't being picked up.
Use GPU: Check this to use your GPU instead of CPU.
Device: Select the device to run the model on.

Clicking **Listen For** shows available sounds for detection. Select sounds as needed.

If a sound isn't being detected, turn on **Overlay** and **Overlay All Sounds**, then play the sound and watch the audio visualization. The overlay lists each recognized sound with its confidence, so you can see whether the model heard nothing at all, heard the sound but below your **Confidence** setting, or classified it as something else - in which case add that sound to **Listen For**. Turn **Overlay All Sounds** back off when you are done, so the overlay only shows sounds that actually raise alerts.

Use the [Action AI: Sound Recognized](#) to perform tasks when a sound is identified.

Audio recognition can also be used to [filter alerts](#), similar to cameras.

AI Language

To change the language used for labels and tagging in image overlays, go to Server Menu  - Settings - General - Default Language.

Adding Actions to AI Events

Agent DVR generates events through AI processes, which can trigger [Actions](#). For instance, Object Recognition generates "**Object Found**" and "**Object Not Found**" events. Each AI system in Agent DVR produces unique events.

These events can trigger various actions, such as raising alerts, calling URLs with object labels, executing programs, or publishing messages to MQTT servers. Use tags {AI} for labels or {AIJSON} for the full JSON response from the AI server in actions.

Account Management

Account Management

Account Settings

To access Account Settings, log in to the remote web portal and click on the  icon at top right, then **Account Settings**.

This form enables you to set your username and email address information as well as change your password and set your time zone.

Business Information

See the form fields on [Account Settings](#) to configure your business information for receipts and invoices.

2 Factor Authentication

Set up 2FA

To configure 2 factor authentication see [Account Settings](#) and check the option to Enable 2FA. When you click OK you will be prompted to scan a QR code to set up an authenticator app to provide secondary authentication to access the Agent DVR User Interface.

If you lose access to your mobile device please [Contact Us](#) from your registered email address and we can reset it for you.

Subscriptions

Manage Subscription

To manage your subscription, including upgrading and cancellation, log in to the remote web portal and click on the  icon at top right, then **Change Subscription**.

Change Payment Method

Your payment details are held securely by the payment provider (PayPal or Stripe) — we never see or store your card number or PayPal login, which is why there's no option to edit them in your account. If you just want to update your card or the payment method behind your PayPal account, see below — no cancellation needed. To switch between PayPal and card, or to a different PayPal account:

Cancel your current subscription: log in to the [remote web portal](#), click the  icon at top right, then **Change Subscription** and cancel. Don't worry — your subscription stays active until the end of the period you've already paid for.

Before it expires, [re-subscribe](#) using your new payment method.

Paying by card? Card payments are processed by Stripe, and you can update your card without cancelling anything: click **Update Payment Method** on your subscription on the [License Management](#) page, or log in directly to the [Stripe customer portal](#) with the email address you used when you subscribed. Stripe will email you a one-time code to sign in, then you can add your new card and remove the old one.

Paying with PayPal? If you just want to change the card or bank account that funds your existing PayPal subscription, you can do that in PayPal without cancelling anything: click **Update Payment Method** on your subscription on the [License Management](#) page, or log in at [paypal.com](#) and go to **Settings - Payments - Automatic Payments**. Select the iSpyConnect subscription and choose a different payment method. To switch to a *different* PayPal account, cancel and re-subscribe as above.

Card expired or payment failed? If a renewal payment doesn't go through, don't panic — PayPal and Stripe both automatically retry failed payments over the following days, so if you fix the problem in time (update your card in the Stripe customer portal, or the payment method behind your PayPal account — see above) the subscription recovers by itself. If all the retries fail, the subscription is cancelled — just re-subscribe from the [buy page](#) with your new payment details. Any problems, [contact us](#) and we'll get you sorted.

Payment History

Payment History

To view your payment history and download receipts and invoices, log in to the remote web portal and click on the  icon at top right, then **Payment History**.

Account Permissions

Account Permissions

To set up permissions to let other people access your server over the web, see [Permissions](#).