BLUE IRIS SECURITY

VERSION 5

PERSPECTIVE SOFTWARE

143 Cadycentre #86 • Northville Michigan 48167 • USA

Copyright ©2024 Ken Pletzer, All Rights Reserved

Last revision: February 23, 2024

Introduction **6**

System Requirements 6
Activation 6
Quick Start 6
What's New 8
Update notes 12
User Interface 43

Cameras **53**

Adding a new camera 53
Video Settings 54
More Video Settings 58
Audio Settings 61
Audio analysis 63
PTZ/Control 66
Advanced Video Topics 70
General settings 74
The Camera Context Menu 77
Camera Window UI 78
Screen layout and frames 79
Camera Groups 80
Triggering and Motion Detection 85
The Motion Sensor 90
Alerts 96
Artificial Intelligence 99
Global AI settings 107
AI Status Window 111
Schedule and Events 112
Webcasting 116
Image Posting 118
Watchdog 119
Configuration synchronization 121
Global Camera Settings 122
Camera Status Window 124

Recording and Clips 127

Recording options 127
Encoder options 133
Manual recording 135
Clip folders 136
The Database and Clips list 140
Database Status Window 145
Clip Playback and The viewer window 146
The speed slider 150
Timeline playback 151
Trigger Search In Clips 153
Trim, Convert, Export 155
FTP Clip Backup 159
Global viewer options 160

Alerts and Actions 161

Conditions 161
Sound 163
Push notification 164
Run a program or write to a file 165
Web request or MQTT 166
Send email 167
Send SMS 169
Make a phone call 171
Set DIO bits 172
Popup toast 173
FTP upload 173
Change shield 174
Change schedule/profile 174
Do command 175
Wait 176
Timecode and other Macros 177
Testing the Action Set 180

Shield, Profiles and Schedules 181

The Shield 181
Camera Pause 181
Profiles 182
Schedules 184
Run, Hold and Temporary Profiles 186
Camera Profile and Schedule Override 186

Remote access 187

The Web Server 187
Networking and Router Configuration 189
Remote Access Wizard 190
NGROK 197
Users and connections 201
Browser interface 206
Mobile device access 207
Remote management 210
SSL and HTTPS 212
More on Security 214
Other Advanced Web Server Topics 215

Email and FTP Servers 219

Email 219
FTP 221

More Options 223

Startup 223
Digital I/O and IoT 224
audio and microphone 229
Joystick 230
Keyboard Shortcuts 231
Macros 232
Other 233

Administration 235

Running as a Service 235
Security Software Exemptions 237

Windows Administrator Access 240
CPU management 241
Status messages, logs and Alerts.....247
Backups 249
Registration and Software Maintenance 250
HTTP Interface 253
JSON interface 261
DDE Interface 276
iOS App DeepLinking.....277
Troubleshooting and FAQ 278

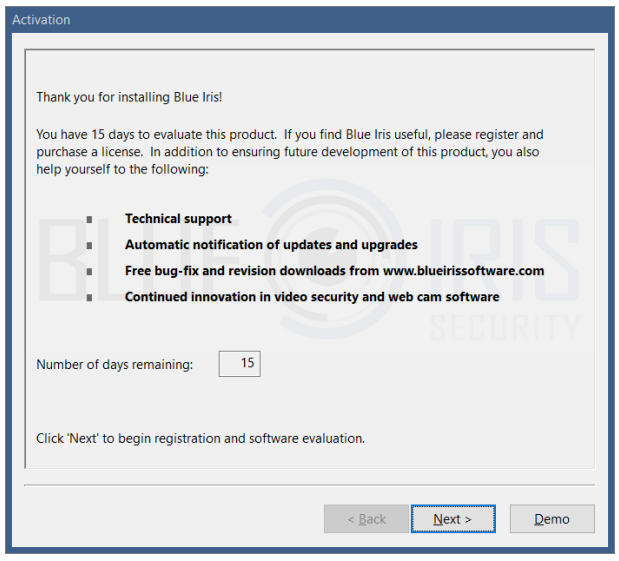
INTRODUCTION

Welcome to Blue Iris version 5. The release of this version marks *20 years* of continuous improvement on what began as a simple piece of software to offer inexpensive power and flexibility in a DIY home video-security solution.

SYSTEM REQUIREMENTS

This software is designed to run optimally on a newer PC running a recent 64-bit version of Windows (7 or newer). For a server OS (2012 or newer), enable the *Desktop Experience* feature. Intel CPUs and Nvidia graphics cards and Windows 10 are recommended. 8GB of RAM is generally adequate along with ample space on a fast hard drive or SSD.

ACTIVATION



Please make the most of the 15 day evaluation period before purchasing. If you need more time please contact support for assistance.

Please write to support@blueirissoftware.com if there is something unclear in this help document.

Click **Next** on this page if you have a license to activate.

QUICK START

First, please start by familiarizing yourself with the basic layout and functionality of the main window as described in the *User Interface* topic below.

In general, you should have a network IP camera working in the browser *prior* to adding it to Blue Iris. The address that you see in the browser's address bar may be required to add that camera as well. See the *Adding a new camera* topic at the top of the Cameras chapter for details.

Refer to the chapter on Administration for tips on overall software operation:

- The importance of making all **Security Software Exemptions** topic cannot be overstated.

- Dual-streaming is the best way to keep CPU usage under control if you are using high-MP cameras (more than 2MP).

Remote access via browser or client app is generally the next priority, and you will find an entire chapter here devoted to that topic.

Please make use of these valuable resources as well:

Our user forum contains an onboarding checklist:

https://blueirissoftware.com/forum/viewtopic.php?f=11&t=2426

Our YouTube channel also contains excellent quick-start guidance:

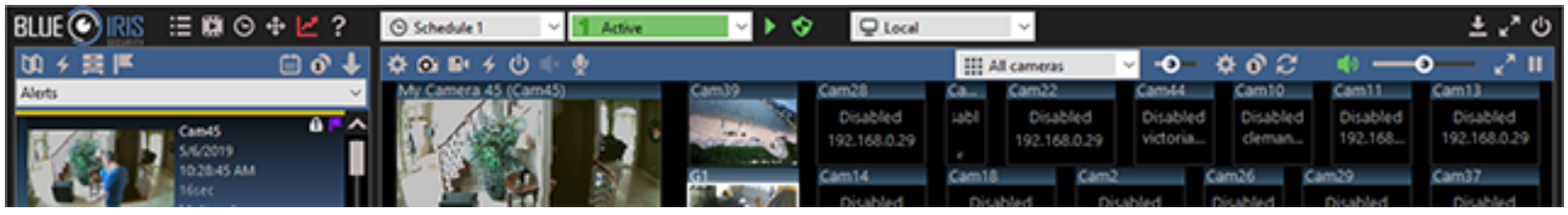
https://www.youtube.com/c/BlueIrisSupport

WHAT'S NEW

With hundreds of updates, so much has changed since version 4 was first released in December 2014. But 4.5 years later, it's time to take Blue Iris to the next level with this major upgrade to version 5. Here's what you can expect to find:

UI refresh

Every element was redesigned and re-rendered for a consistent, high-contrast, high-resolution and modern aesthetic. Buttons and other tools have been more intuitively grouped and sized. A new font has been selected for improved antialiasing and readability.



Help documentation refresh

It's been awhile! The Help may now be read in book format as well as in-context via Adobe Acrobat bookmarks throughout the UI. Major topics previously neglected have been re-written to reflect all that has been added to this software over the years.



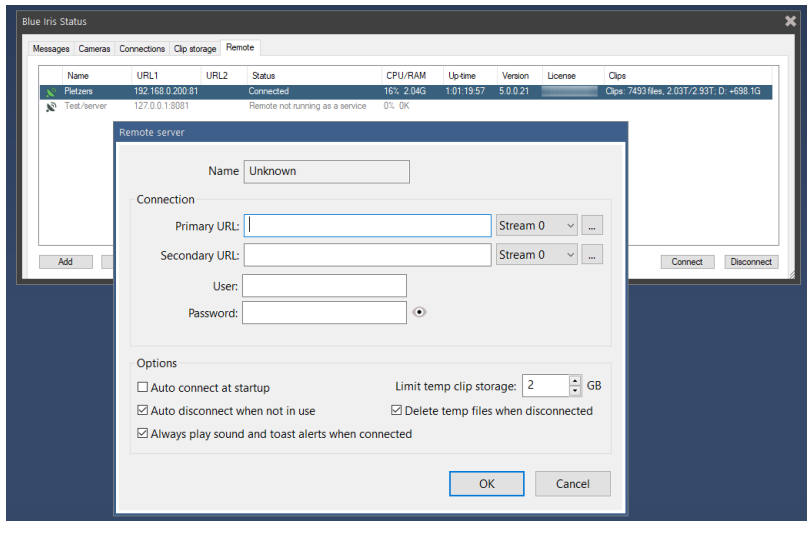
High DPI display awareness

Windows and UI elements will be scaled automatically to match your Windows Display control panel selections. UI elements were designed to look sharp at up to 300 DPI. No more tiny icons on 4K monitors and beyond.

Remote management

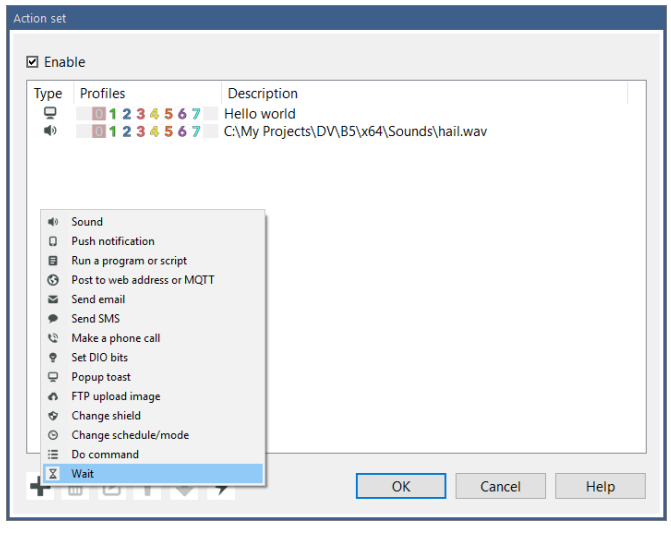
This is perhaps the most significant upgrade in terms of software power and flexibility—you may now use one Blue Iris installation to manage many others simultaneously.

When connected to one or more remote systems via the new remote management control panel, you get a concise view of each system's status. You may then make any remote Blue Iris server 'active' in the UI, giving you complete virtual control of that remote Blue Iris installation without the hassle or many shortcomings of an otherwise "remote desktop" solution. BVR clips are opened using progressive download management so that only the portions of the file of interest are transferred. Status pages, the timeline and clips lists are refreshed as they are updated on the server. Sounds are played and popups may be displayed locally from all remote connected systems. Configuration changes are made seamlessly by uploading any edits.



Alert action set lists

Every possible action that's supported by Blue Iris may now be applied to camera alerts as well as many other conditions such as user account login, status messages, digital input signals, and more. You may create a list of these actions to be executed in any order or combination. Each action has an associated profile selector to allow you to manage actions for all profiles together on one page.



New alert action types

There are also new action types. These include toaster pop-up messages in the lower-right corner of the Windows display, FTP transfers, and simply the ability to wait an arbitrary time between consecutive actions. You now may specify the devices and text for push notifications. Support for legacy Android GCM push notifications was added.

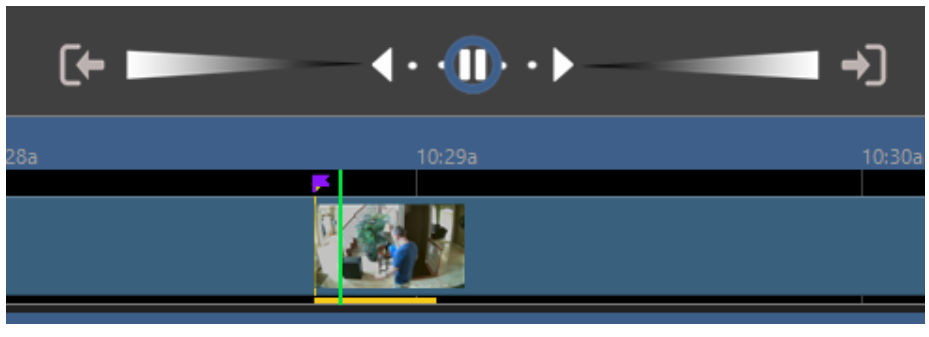
Clip management updates

In addition to its own UI refresh, the timeline view receives a couple of other interesting updates—the ability to zoom in further and have alert images displayed directly on the clip tracks.

The clip view list may be “unfolded” to fill the display with clip images. Days are delimited by a solid color bar.

Viewer playback controls

In place of generic play/pause/stop buttons, a more interactive speed control has been designed and implemented. For BVR content, you may now slide the speed control left to slow down or reverse, or right to speed up and go forward. Click the horizontal control anywhere to set the speed directly, or slide and release to return to the previous setting.



Camera configuration synchronization

On several camera settings pages you will find the option to synchronize that page with another camera’s settings. This allows you to make changes to one camera’s settings and have that affect one or more other cameras’ behavior. This will come in handy if you find yourself setting (and then having to later adjust) the same alerts or other settings across multiple cameras.

Global volume control

You may now use the mute and volume controls to adjust the live volume on all cameras simultaneously. For mixing levels, use the gain control found on each camera's audio settings page. The same mute and volume control is used by the clip viewer window as well.

Technology

The time is right with a major software upgrade to also update development and runtime environments. The latest Microsoft technologies, video processing and runtime libraries are now used and redistributed. While we lose support for the oldest operating systems (dating back to 2001!) we gain support for many emergent technologies which will be further leveraged in the 5.x series.



As we are all interested in getting the most out of our CPU clock cycles, these newer development tools combined with new code optimizations will combine to contribute to a more efficiently running system. Work will continue with Intel and Nvidia to further leverage graphics hardware assistance.

And that's not all!

Unlike other software which is released just once, or which sees an update only every one or two years, this is just the beginning for Blue Iris 5. As with versions past, improvement and innovation will continue over the coming years. The client apps for iOS and Android, as well as the UI3 browser interface all will receive major updates as well.

Artificial intelligence is quickly becoming the major focus for all video security software, and this includes Blue Iris 5. In conjunction with Sentry Smart Alerts, a solution is already in place to reduce false triggers when human recognition is ideal. These options will be expanded to also include free services as well as LPR and facial recognition technologies.

Please keep the suggestions coming, and we thank you for your continued support of Blue Iris.

UPDATE NOTES

As major changes are made to version 5, they will be documented in this section.

5.8.7 - February 14 - 23, 2024

In addition to a number of post-trigger images to send to the AI, and in place of the "motion leading image" option, you may now also specify a number of pre-trigger images as well. These images are synthesized from direct-to-disk frames stored in the pre-trigger buffer.

Improvements have been made to the heuristics used when deciding which image among all analyzed to use for final alert confirmation or cancellation. It is no longer necessary to place a "dummy" object into the the "to cancel" box for processing to continue regardless of a single confirmed object.

5.8.6 - February 2 - 3, 2024

When one trigger ends and a new one begins *within the pre-trigger buffer duration*, there is no longer a loss of video recording. Previously, recording would not restart until the next keyframe was received, which could have resulted in the loss of several seconds of video.

A new setting on status/log defines the age at which a log .txt should be deleted.

5.8.5 - January 22 - 31, 2024

With the Alert tab option for New sources/zones only you may now select whether these new sources are handled exclusively.

The Motion detector option to blackout or obscure the video based on the zone map is now extended to the main stream, BVR playback, as well as BVR export.

The AOI (area of interest) function has been expanded to support dual-streaming and BVR direct-to-disk recording and snapshots (new clips).

The Anamorphic (force size) function has been expanded to support arbitrary sizes with dual-streaming.

5.8.4 - January 10, 2024

Improved watchdog effectiveness when a main stream or audio stream is lost. If the camera does not support audio, please disable it on the Audio tab to prevent watchdog resets.

Motion detection zone crossing has been expanded to offer negated zones for more complex object travel rules.

PTZ UI and controls are automatically hidden when a single camera window is displayed which does not have PTZ UI enabled.

5.8.3 - December 27, 2023

You may now filter alert actions by specifying required global DIO bits.

All dialog windows now draw more efficiently, removing redrawing flashing effects.

For increased resilience, the two largest and most important DB views (new and alerts) are automatically recreated upon startup and all compact/repair operations, just as index.dat has been for some time.

Unmanaged drives or folders no longer complain about the disk/s being offline.

5.8.2 - December 12, 2023

Audio analysis may be configured from the Audio tab in camera settings. This includes power, spectral analysis and spectrograms. Sophisticated patterns may be applied when evaluating the audio signal for triggers.

Audio visualization now occurs in the clip viewer, regardless of playback speed.

5.8.1 - November 22, 2023

Recording folders and drives may now be designated as *shared, exclusive-use,* or *unmanaged*. Used and free space are not considered on unmanaged drives. New clips/images are not added to the database or automatically moved/deleted in unmanaged folders.

The Options/Storage page has been reworked to include an interactive graphical display of the disk usage to facilitate easier distribution of disk space to folders. Also now you will be prompted to repair the DB following any folder path changes.

An option on the right-click menu over the timeline view allows you to set an idle timeout for returning to the live camera view and ‘now’ position.

It’s possible to reroute “talk” audio to an alternate camera.

A 64-bit version of the UScreenCapture driver is now included in the installation. Unfortunately it still seems no longer possible to use this when running as a service.

5.8.0 - September 27, 2023

The flow of the Motion sensor, Trigger and Alert pages has been made more logical. The Alert page timer for *X triggers within Y seconds* has been moved to the more appropriate Trigger/Motion page. The timer for *minimum/max time since last trigger* has been moved to the trigger tab and is now used to prevent the generation of new alert images. The remaining alert timers now prevent *actions* from firing rather than preventing the alert image itself.

The Watchdog tab in camera settings may now have profile-specific settings and may be synced with another camera as was the case with the Trigger, Record and Alerts tabs.

Previously *monostable* ONVIF triggers (without corresponding trigger reset events) were handled as *external*. These are now more appropriately labeled as ONVIF as well.

5.7.9 - August 8, 2023

The FTP component has been brought up to date. It now supports TLS 1.3 as well as SFTP servers.

A new Reolink camera make/model option for RTSP main stream + FLV sub stream. As we battle with Reolink firmware reliability, this combination attempts to emulate the way in which their apps and web services work. These models are notorious for stability problems when multiple RTSP streams are requested.

5.7.8 - July 7, 2023

This version exposes the inner workings of the **static object analysis** as used by the AI via a new **Configure** button on the Trigger/AI page in camera settings.

New functionality includes abandoned and missing object detection, as well as specification of objects that should never be considered static.

5.7.7 - May 24, 2023

In order to reduce the chance for inadvertent configuration errors, this version enforces the use of required settings when dual-streaming is employed. Specifically, direct-to-disk recording, a pre-trigger buffer of at least 5 seconds, and no “limit decoding.”

Whenever the pre-trigger buffer is configured yet it contains no key frame, the yellow caution icon will be shown in the camera's window. In this case, increase the key frame rate to at least 0.25 via direct camera browser configuration.

Pulling the camera's current image for the camera settings/general page, among other functions, has been made more efficient for a more responsive UI.

Duplicate AI labels will be suppressed in the database memo field, showing only the highest confidence, allowing more labels to be visible in this 35-character limited field.

AI static object analysis is under revision to allow more functionality, such as "missing object" and "abandoned object" detection. In this version, you may view the current static object status via the Trigger/AI/Static Object window.

5.7.6 - May 3, 2023

This version revises and hardens database access code in order to increase efficiency and reliability. Specifically, the console will no longer append/update into the database, but rather send these requests to the service.

5.7.5 - April 20, 2023

This version exposes the inner workings of the ONVIF GetEvents code, providing better status feedback as well as providing opportunities to customize actionable events coming from a camera. The option on the Trigger tab to *use ONVIF/camera events* now has a configuration page. The GetEvents thread status/error code is now visible on the General tab as well and will cause a yellow caution on the camera window if in an error state.

5.7.4 - April 4, 2023

Time-lapse may now be applied to timeline video export.

The *use sub stream if available* setting may now also be applied to timeline video export.

For timeline video export, in addition to the previous time-lapse speed multiplier setting, you may instead specify an exact number of seconds, minutes, or hours between frames.

5.7.3 - March 30, 2023

A new option on the right-click menu over the Viewer window allows you to modify the now-default setting to use a BVR's sub stream (if recorded) for scrubbing and high-speed playback.

A small change has been made to the 5.6.8 feature which caused alerts as to be considered locked/protected while their associated clips remain—this now applies only to the *age limit* of the alerts folder. It will no longer apply to the *size limit* on the folder if alerts are being saved as JPG (and .DAT) files.

You may now select to save AI-unknown faces on a per-camera basis. You may also select a specific folder for local faces management instead of using a folder in the Program Files folder, or you may choose to not use local management at all.

5.7.2 - March 22, 2023

This update is all about identifying and resolving storage errors and pitfalls. In addition to overallocation, additional storage issues are now identified and reported.

If a drive is offline, over allocated, or another issue is present, this information is prominently displayed at the bottom of the clips list in a new DB status window. You may display this window manually with a right-click menu option. However, the window may not be dismissed until any issues are resolved.

The software tracks the aggregate MB/s being recorded to each drive. When files are MOVED from one drive to another, this rate is also calculated. When doing continuous recording and archiving files to a NAS, you will want to make sure the recording rate does not exceed the rate at which may be moved.

5.7.1 - March 6, 2023

Motion zones now have associated colors. A new custom GUI control was also developed for zone selection. Double-clicking in this control as well as the profile selection control may now be used to quickly set a single value or to set all values.

It's now possible to add motion zone letter specifications to individual alert action "required AI objects" or "skip with" settings.

Updated Apple push notification service which will expire April 2, 2023; use version 5.7.1 or newer for uninterrupted push notifications from the iOS app. The new expiration is April 2, 2024.

5.7.0 - February 8, 2023

A search box has been added to the top of the clips/alerts list to allow for the quick searching of license plates and AI results. A keyboard shortcut may be added to set focus to this box, and Esc or Return may be used to restore focus to the clips list.

5.6.9 - January 24, 2023

CodeProject.AI integration updates to support version 2.06:

Rather than using a “custom models folder” setting, the software now pulls the list from the AI directly.

If you install the Automatic License Plate Recognition module via the CodeProject.AI dashboard, then enable ALPR on Settings/AI, the software will attempt to locate and match license plates to vehicle objects. Plate numbers may also be used as objects for alert cancelation and confirmation.

Admin access is now required to see the Status window and status icons.

[5.6.9.3] Improved multithreading when analyzing multiple main stream images using AI which may require significant time to decode.

[5.6.9.5] Zones may be specified for *to cancel* and *to confirm* AI objects. For example, person:AB for zones A or B and person:80AB for an 80% confidence as well.

5.6.8 - January 8, 2023

On the Alerts tab in camera settings, the option for *re-triggers* has been expanded to allow for re-triggers only when a new zone or source is added to the trigger.

On AI configuration from the Trigger tab in camera settings, an option for *New alert/analysis on re-trigger after cancellation* has been added. You may have been using some combination of a large quantity of images (using significant system resources) and the “re-triggers” option on the Alerts tab (creating many alert images even after confirmation) in an attempt to achieve similar results, but this new option may now better address the issue of inadvertently missing critical events.

On this same page, the option to replace Email/SMS subjects and bodies has been removed. Instead, use the &MEMO macro in your action sets for this purpose.

You may now limit the age of clips to which users have access with a new setting on Settings/Users. 0 may be used for unlimited access.

Clip maintenance behavior has been modified. AI *confirmed* alerts that belong to existent clips are essentially treated as *protected*—that is, they will not be deleted or moved out of the Alerts folder so long as their parent clip exists. Users may have felt the need to mark these items as protected in the database (which means they are *never* automatically deleted), thereby inadvertently accumulating an inordinate number of these. *Canceled* and *unconfirmed* (no AI involved) alerts will still be maintained on schedule.

5.6.7 - December 20, 2022

When editing Settings/Keyboard shortcuts, you may now define up to 8 custom actions sets to be assigned to keyboard commands [5.6.7.3].

Introducing multiple-camera selection. In the main window, hold the Shift key while selecting cameras. Release the Shift key to temporarily view the subset of selected cameras. The group name is adorned with an "*" in the group selection combo box to signify this state. Revert to the normal group view by Shift-clicking in any space between cameras, using the Esc key enough times, or by entering/exiting layout edit mode. This feature is especially handy for searching for clips or video in the timeline. It may be expanded to allow other commands to be applied to all cameras in the subset.

5.6.6 - December 12, 2022

A right-click context menu has been added to the Timeline window.

The concept of "time selection" is introduced. You may either right-click to use the "set start frame" and "set end frame" commands, or you may double click in the timeline's date/time header to select a unit of time (depending on the zoom level) and then Shift+double click at another location. Double-clicking anywhere below the date/time header will invalidate the selection.

Once time has been selected, it's now possible to Convert/Export from the viewer's Timeline playback mode. The output size and camera layout will mirror what's currently shown in the viewer window. An audio track may be included for the selected camera. The "skip dead air" functionality is available.

Holding control + left or right arrow keys may be used to move forward or backward in the timeline view to the next or previous time division (depending on the zoom level).

5.6.5 - November 20, 2022

The Clip Backup (FTP) and Convert/Export process queues are now multithreaded. The number of simultaneous FTP connections are determined by the FTP server's settings page. The number of convert/export threads is determined by a setting on the Other page in Settings.

GPU usage is now presented wherever CPU usage is also available. The number comes from the Windows "performance counters" for "GPU Engine." This may not be identical to what's shown on Task Manager or Process Explorer.

The software may have become unstable when the mainstream of a dual-streaming camera dropped out while being accessed by remote viewing. A fix has been made.

5.6.4 - November 16, 2022

The database now tracks the number and type of alerts for each clip. Icons for AI-confirmed people and vehicles will also be shown on the clips list along with a count of the number of alerts.

The clips list has also received other visual updates including a graphical representation of the beginning and duration of each item.

5.6.3 - October 26, 2022

Audio has been enabled for the selected camera during timeline playback on either UI3 or locally when a camera is selected and playback speed is normal (1x).

A bug fixed where when canceled/occupied alerts with files are moved out of the alerts view, "errors" shown in the log when database maintenance is ran.

The code-signing certificate used to verify secure binary deliverables has been renewed for another three years and all executables have been re-signed.

5.6.2 - September 23, 2022

The Camera Discovery window now finds MAC addresses along with IP addresses. You also have the option of using the previous ONVIF discovery, or the new full LAN IP and port

scan. With this, it should no longer be necessary to use the external website service Advanced Port Scanner to search your network.

LAN cameras now automatically pull MAC addresses and they are displayed on the Status/Cameras page.

If a camera's MAC was previously determined and the camera experiences connectivity issues, the software with automatically scan the LAN in order to detect an IP address change. If a new address is found, it will be adopted and posted to Status/Log. This provides protection against IP address changes when DHCP is left active on a camera.

5.6.1 - September 16, 2022

A search-in-clips feature has been added to the clip Viewer window with a new magnifying glass icon at the top of the window. You may use this to discover motion and alerts "after the fact" and add them to either the Clipboard or directly to the Alerts list.

5.6.0 - August 16, 2022

Subnet notation may now be used in the Limit IP box on settings/web server/advanced [5.6.0.9]

Algorithms for AI "static object detection" have been rewritten to prevent fewer false static inferences when a new object is actually in motion. Static objects are now saved to the .DAT files for comparative analysis. Additionally, images which were captured but not completely analyzed by the AI are now marked with the "canceled" symbol in the .DAT file.

Many database manipulation functions have been rewritten to allow for records to be inserted rather than strictly appended as was previously required. This allows for new clipboard items to be shown on the All Clips list and to appear on the timeline and arranged by content date rather than by clipboard creation date. It's also possible to move a clipboard item into the alerts list, providing a way to create an ad-hoc alert after the fact.

Alert JPEG and DAT files are no longer renamed when the alert is finalized. Instead, the metadata that was previously added to the filename is now saved as EXIF data within the JPEG file. The changing filename was always challenging for scripting and actions that relied on &ALERT_PATH.

A new camera status “bell” icon replaces the trigger icon once an alert is confirmed. This helps to emphasize the difference between the “triggered” and “alerted” states—not all triggers become alerts based on filters and AI analysis.

5.5.9 - June 28, 2022

A new option for stream encoding, “direct-to-wire,” may be found on Settings/Web Server/Advanced/Streaming configuration. Video may now be passed directly from a camera’s direct-to-disk frame buffer to the browser UI3 and other clients.

A new option for the upload alert action to send an MP4 file. If an email alert action is also configured, this file is shared between these actions.

If you’ve previously installed SenseAI, please update that now to version 1.5, which is now called CodeProject.AI Server.

5.5.8 - June 13, 2022

More formal support for Code Project’s AI Server, now our preferred no-extra-cost AI provider over DeepStack. The CodeProject.AI Server is better supported by its developers and has been found to be more stable overall.

5.5.7 - May 21, 2022

Support for Gmail’s OAuth2 authentication. Gmail will be discontinuing the support for “app passwords” and “less secure apps” at the end of this month. Visit the Settings/Email page to complete OAuth2 authentication if you are using Gmail for alerts.

A new screen capture option to include a mouse cursor with highlighted clicks. This gives you the ability to use the software for general screen recording production, as was done for our Gmail OAuth YouTube demonstration videos.

You may add PTZ preset positions as arguments for firing or skipping individual action set items. Use the format P*n*, where *n* is the preset number 1 or greater.

A new option from the right-click menu in the Clips list allows you to edit the memo field. The option to only display items with memos was previously available.

MQTT code updated to use the Mosquitto version 2.0.14 library.

&ALERT_DB and &ALERT_FILE action set macros now return values which will survive a database compact or rebuild.

Support for 2-way audio on CantonK compatible cameras (those that use port 34567).

JPEG timed “slideshow” playback when the option is used to automatically advance to the next item in the clips list at the end of a video.

5.5.6 - March 12, 2022

Part of a major UI3 browser client release, timeline playback is now available!

It’s now possible to cancel alerts when the camera is focused on specific PTZ presets.

Updated Apple push notification service which will expire March 25, 2022; use 5.5.5.13 or newer for uninterrupted push notifications from the iOS app. The new expiration is April 2, 2023.

5.5.5 - February 2, 2022

Remote Management has received some long-awaited updates. Use of Remote Management is no longer mutually exclusive with use of the local console. It’s also no longer necessary to run as a service, and multiple remote consoles may be connected simultaneously.

The new /time/ interface for timeline playback via Remote Management will be expanded for use in UI3 and the phone client apps.

5.5.4 - December 8, 2021

Updates to support new features in iOS app 2.2.

For each camera in a group you may choose whether or not it will participate in the group audio stream—now on the right-click group layout menu.

.DAT files created by DeepStack analysis are now formally managed in the Alerts folder. They are now represented in the Alert folder size calculations. If you use these files, you may want to run a Database/Regenerate so that their sizes are loaded into the database and any orphan files are adopted, even if there are no associated .JPG files.

If you use the option to burn DeepStack analysis onto alert images, the memo (person:85% for example) and license plate data are added as metadata to the .JPG files so that this information is no longer lost with a full Database/Delete & Regenerate.

Trigger zones are now added to the alert .JPG filename alongside flags so that this information is no longer lost with a full Database/Delete & Regenerate.

5.5.3 - November 16, 2021

A Copy button has been added to the camera settings page to facilitate the quick replication of settings between profiles and cameras.

Right-click menu shortcuts added to several of the command buttons at the top-left of the main window.

5.5.2 - November 3, 2021

Export camera status in CSV format.

Status Alerts now offer the ability to fire on both a timed basis and more quickly for important status updates.

TLS/SSL is now supported for MQTT connections, with the requirement that valid certificates are provided in PEM format.

When DeepStack is auto-started it is added to a Windows “job” object so that if Blue Iris exits unexpectedly, DeepStack is closed as well, preventing a system resource leak.

5.5.1 - September 23, 2021

The DeepStack AI feature to detect/ignore static objects has been improved by implementing some hysteresis—it now takes time (up to 2 minutes) to consider an object either static or “gone” from the scene. This prevents false alerts caused by static objects that only *temporarily* disappear from detection. Also these algorithms are now applied to *all* objects, not just those enumerated in the *to confirm* box.

Utilizing the new dynamic group layout functionality, the group setting to *Only cycle when at least one camera* is detecting motion, triggered or alerted behaves on the browser or client app as it does on the console—showing all cameras at once that meet this requirement.

The camera layout option to *Open in desktop frame* is now memorized *per group* as well as per camera. When selecting a group on the console, cameras are automatically moved to the desktop or back to the console. Cameras that are *not* in the selected group are left as they were. Camera desktop window *position* is currently not group dependent at this time.

Zoom in the clip viewer will now fill all available space.

5.5.0 - September 13, 2021

Groups are now created and deleted explicitly. Previously, the only way to delete a group was to remove each camera individually. In addition, the role of a group has also been expanded to include *layout*. A group's layout now consists of a set of cameras in a particular order. Each camera may have a default zoom position, relative size, and aspect ratio. The group itself may specify a height and aspect ratio, or these may be determined automatically. In addition to the existing left-right ordering, a group's layout may also be broken into *columns* and *subgroups*.

When a camera is zoomed, all layout space available is utilized (previously the zoomed portion was cropped to fit the original aspect). Using this new camera zoom functionality together with layout options to "scale to fill," it's now possible to create layouts which force cameras into grid patterns without spacing via scaling and cropping.

Groups, when displayed via clients, now appear as the group does on the console with headers, borders and icons. You can also force a group's height/aspect on the console to make adjustments easier.

Dynamic layout for phone and other clients. If a group is configured for an automatic aspect ratio and the client sends both a width and height request (&w=xxx&h=yyy) then a temporary layout is created to custom-fit the requested aspect ratio (and resolution if the group is also configured for an automatic height). The next release of the phone apps will support this feature, making group streaming look great in both landscape and portrait on any device.

5.4.9 - June 25, 2021

Specify a maximum trigger time [5.4.9.12].

Playback offsets for new alerts [5.4.9.11] will begin at the motion-leading position rather than the beginning of the entire pre-trigger buffer.

Hold Control as you double-click to open an alert in order to position directly and then pause at the AI-confirmed frame [5.4.9.11].

Specify zones used for DeepStack [5.4.9.9]

Specify known plates for Plate Recognizer for alert rules; “myplates” and “notmyplates” objects may be applied to individual alert actions [5.4.9.9]

Enhanced synchronization between alert images and alert processing. Alert images are not created until timer conditions are met on the Alert tab in camera settings. Processing of “re-triggers” is improved following a canceled alert.

Improved handing of DeepStack static objects and objects outside of detected motion areas.

On the DeepStack status page you may now choose to show/hide Blue Iris detected motion rectangles, helpful for diagnosing objects which do not overlap these areas. Also you may now drag & drop saved alert analysis “.dat” files into this window.

The “run a program or script” action is now “run a program or write to a file.” This will be handy for external logging.

5.4.8 - June 16, 2021

RTMPS is now supported for Flash live video streams to Facebook, etc.

A DeepStack status page has been added. This allows you to inspect DeepStack results and performance following an alert confirmation or when using the testing & tuning options in the clip viewer.

You may now specify 2 objects together with “and” logic on the “to confirm” and “to cancel” fields for DeepStack alert confirmation by combining them with a +. For example, car+licenseplate.

An option to add motion overlays when re-encoding has been added to the Convert/Export clip function.

5.4.7 - May 25, 2021

Support for DeepStack custom model files; specify the path on Settings/AI. Use a custom folder name, not *sharedfiles* as this will conflict with DeepStack’s own models.

[5.4.7.7] select custom models per camera, per profile.

Support for Plate Recognizer's Make/Model/Color analysis for cars.

A new option to only use Plate Recognizer for alerts where either DeepStack or Sentry has confirmed a vehicle alert.

5.4.6 - May 17, 2021

As requested by several customers, a *continuous + triggered* recording mode is now offered separately from the *continuous + alerts* mode. This mode ensures that the main stream is also recorded for *canceled* alerts as well as confirmed alerts.

Replacing the **Analyze image with DeepStack** option on the viewer's right-click menu is a **Testing & tuning menu** with an **Analyze with DeepStack** option. This option pushes BVR video frames through DeepStack as quickly as possible (may not always update in real-time unless you pause and step).

With dual-streaming and direct-to-disk enabled, main stream frames that are sent through DeepStack when the camera is triggered are flagged in the BVR file. As these are played in the viewer with the **Analyze with DeepStack** option enabled, the image border will be shown in blue, allowing you to identify precisely which frames were used for the alert confirmation. A catch-22 arises however if you are using the *continuous + alerts* recording mode, as these frames are never actually recorded—use *continuous* or *continuous + triggered* if you want to take advantage of this tuning feature.

When analyzing multiple frames with DeepStack against both "to confirm" and "to cancel" object lists, an effort is made to choose the "best" confirmed image according to higher confidences and the presence of (more) faces. By default, the alert will continue with a single found "to confirm" object, but you can force continued analysis by placing any object label in the "to cancel" box (even one that will never be found).

The "to confirm" and "to cancel" boxes may now contain labels ending with the * wildcard. This is handy if you have multiple faces for a single person—you might use chris* for example to match defined faces for chris_1, chris_2, chris_side, etc.

A new right-click option in the Alerts list allows you to manually cancel and confirm alerts.

5.4.5 - May 10, 2021

(5.4.5.3) The *pre-trigger image* is now used as the first image sent to AI for alert confirmation. This is an image captured at first motion rather than at the moment of trigger, so it may be earlier in time by as much as the motion sensor's *make time*.

When recording continuously (including the new *continuous + alerts* mode), physical recording is delayed by the duration of the pre-trigger buffer. This allows the opportunity to record the main stream frames in the pre-trigger buffer as required. In addition, this means that if you manually record or start/stop using the traffic signal icon, the pre-trigger buffer will now also be recorded.

By default, the main stream is decoded when a camera is in full-screen or "solo" in the window. A new option on the camera right-click menu allows you to disable this and force the continued use of the sub-stream in these cases.

5.4.4 - April 27, 2021

(5.4.4.3) face recognition must now substantially overlap a "person" object detection. Too many false-positive "unknown" faces result otherwise. A new macro &JSON may be used for access to raw DeepStack object detection data during an alert.

When the *continuous+alerts* record mode is used with a dual-streaming camera along with direct-to-disk, the result is a BVR file which will contain the sub-stream continuously recorded, but the main-stream only recorded when the camera is in a triggered state. During main-stream playback, the sub-stream will be upsampled whenever the main-stream is not available.

The DeepStack *detect/ignore static objects* option will now force a re-analysis of the image each 10 minutes when not triggered in order to refresh the static objects collection.

5.4.3 - April 9, 2021

(5.4.3.5) Minimum confidence may be overridden by appending a : and the number to any label placed in the "to confirm" or "to cancel" boxes on Trigger/AI as well as on each alert action by, for example *person:80,car:70*.

DeepStack objects recognized only when substantially overlapping areas where Blue Iris is also tracking objects in order to reduce the detection of static objects.

Require AI objects or use them to skip individual alert actions.

Motion detection updates to produce fewer/larger object rectangles with more effective edge-vector tracking.

DeepStack “mode” setting. Processing time added to object detection log entries.

5.4.2 - April 6, 2021

A new action set “immediate actions” has been added to the Trigger tab in camera settings. This action set runs before alert AI confirmation.

You may now specify up to 999 images to be sent through DeepStack for alert confirmation (or until the trigger ends).

By popular demand, you may now delay recording or snapshots until *alerted* rather than starting immediately upon a trigger. This allows the AI time to analyze the trigger before recording begins.

With a new option on Settings/AI you may now select to save *unknown* faces to a specific folder for later review or import.

At startup and after PTZ movement, DeepStack will now analyze the scene for initial objects in order to prevent alerts on static objects.

The marked-up alert image is now re-saved to the database so that it will appear on the alerts list.

With a right-click option in the Viewer, you may run a snapshot through DeepStack for analysis. This will eventually be expanded to include BVR content.

5.4.1 - April 3, 2021

Support for DeepStack facial recognition. Maintain the face list from the AI page in Settings.

Alerts may now be canceled with specific DeepStack labels. It’s now possible to Alert only when “unknown” faces appear or only when there is NOT a dog present, etc.

5.4.0 - March 31, 2021

Support for DeepStack integration (without the separate AI Tools package) via new Settings AI page. DeepStack may be used for object classification to confirm alerts containing persons, vehicles, pets, and more.

Plate Recognizer ALPR configuration has been moved to the new Settings AI page. You will need to reconfigure this integration, now done globally.

Support for legacy SeaIO devices from SeaLevel.

Test button added and UI updates to the camera Schedule/Events page.

You may now select to use a specific global schedule on the camera Schedule page.

“Use defaults” button added to the video encoding configuration pages.

Updated Apple push notification service which will expire February 28, 2021; use 5.3.9.10 or newer for uninterrupted push notifications from the iOS app. The new expiration is March 25, 2022.

5.3.9 - January 29, 2021

A new option on Settings/Other allows you to perform an encryption on all passwords stored by Blue Iris (they are otherwise Base-64 encoded). Changing this setting does not affect stored passwords until they are next loaded and re-saved. While this does provide strong security for your passwords in the event someone will have access to your PC registry, the major disadvantage of password encryption is that if you must transfer your .REG settings to another PC, you will need to re-enter all of your passwords, as they may only be decrypted on the PC on which they were encrypted—not ideal for a backup/restore unless they are done on the same PC.

A new button in the Timeline view for “instant reply.” This will automatically begin timeline playback 30 seconds back. You may click it multiple times to transport back 30 seconds at a time.

A new interface to the Sentry Smart Alerts system allows you to select person and/or vehicle detection. Make this change by using the Artificial Intelligence button found on the Alerts tab in camera settings. This may not be fully functional until 5.3.9.1.

When switching from main stream decoding back to sub stream decoding, the main stream frame buffer is now deallocated, returning RAM to the system. Previously once the buffer was allocated, it remained until the camera was reset.

5.3.8 - January 12, 2021

By default, alerts are simply database entries which reference actual video files (clips). You may now right-click on the alerts list to export individual alert segments as video files. If you choose to "replace" the alert, the MP4 file reside in the Alerts folder. When you open the alert while it's still associated with a clip, the clip will be opened for playback, not the exported file.

You may also choose to automatically export alerts as MP4 videos with a new option on the Alerts tab in camera settings. This may be useful for immediate backup or AI analysis of alert video.

When you delete a clip, its alerts which have their own associated files (JPEG or MP4), now will remain in the alerts list and the alerts folder.

Alert list items are now updated with any additional trigger sources and zones when the trigger ends.

Clip list preview images are prepared and drawn asynchronously in order to display the clip list more efficiently and to retain UI responsiveness on systems with very large displays and/or large databases.

5.3.7 - December 20, 2020

There are now a total of 16 possible drive folders configured on the Settings/Clips page.

Added "On red shield" and "On green shield" actions sets editable from the Schedule page in Settings.

Smoother transitions will now occur with auto-cycle both locally and remotely when using dual-streaming. The software attempts to start main-stream decoding on the "next" camera in the cycle at 2.5 seconds prior to the switch.

Settings/Users may be configured with *Profile/schedule changes* access separate from *Administrator* access.

The */admin?trigger* and JSON *trigger* commands, when supplied with either a memo or JPEG image, will always force a new alert list image to be created. Normally, when a camera is re-triggered (triggered again while already triggered), no additional alert list image is created.

Alert counters are maintained for each camera for each user. Previously, these counters were incremented when an alert image was created—now they are incremented only when alerts are actually fired (a push, email, etc). This allows time to *cancel* the alert via AI extensions without the counters increasing.

The "main menu" button has been replaced with a Settings button and an "add camera" button was added. The pop-up menu is still available by right-clicking.

Video overlays are now *always* written to the BVR file. Each overlay object has a new flag *Require live display of overlay at the time of recording* which determines whether or not the overlay is displayed during playback. This allows you to decide whether or not the overlays should also be toggled during playback when you toggle the overlays on and off while actively recording.

Toast popup alert actions will now display a large "hero image" of the camera's current image.

5.3.6 - December 2, 2020

The JSON *alertlist* command with optional parameter *v=2* now reads only the index.dat file which greatly improves the performance for pulling the alerts list from the client phone apps when there are hundreds or thousands of alerts. Individual alert item detail is now appended to the /alerts/ image request with optional parameter *v=2*.

On the Settings window, *Check for Updates* is now *Check for News and Updates*. Notices posted here ultimately will replace Mailchimp email blasts which are now used to advertise our Friday Quick-start Webinar series. When there is news, a clickable blue circle icon will appear in the Blue Iris status bar.

5.3.5 - November 27, 2020

The ONVIF device inspection now pulls all available video profiles as well as profile details necessary to distinguish multiple cameras on the same device.

The network camera configuration page has been revised to allow the selection of an ONVIF profile for each of the main and sub streams. Also, the "params" box was removed. If you

had previously specified anything here, it will be added automatically to the end of the video path.

The ONVIF GetEvents function has been revised to select only events relevant to the camera's selected video source configuration (important for devices with multiple cameras).

5.3.4 - November 22, 2020

A new "clipboard" database view is used to manage arbitrary video selections and associated exports from BVR file content. Use the snapshot icon or the new "crop" icon at the top of viewer window to create a clipboard item. The viewer will immediately open the clipboard item "zoomed in" on just the selected segment. Unless and until the segment is exported, it references the source BVR file and does not have its own file. If the BVR file is deleted, the associated clipboard items (and alerts) are deleted, unless one of these is protected, which then prevents the BVR from being deleted. The UI3 browser convert/export function will now create items which live on the clipboard view rather than solely on the "export queue" view.

You'll find a link to the new clipboard view via the "folder" icon at the top of the clips list. In addition, many new views have been added for motion zones and trigger sources.

When opening a clip from an Alerts list image, the "crop" start/stop icons are atomically adjusted to the beginning and ending of the alert. This allows you to "see" the alert's position in the clip as well as to conveniently export just the alert segment of the clip.

Support for new Doorbird models doorbell and motion sensor.

The MQTT "publish" function was moved into the MQTT thread to maintain UI responsiveness when the MQTT server is offline or misconfigured.

A new option on the Settings/Users pages "camera admin" allows a user to administer specific cameras without having full system administrator privileges. For proper remote UI, this does require an update to the phone app as well.

Motion rectangles are now added to main stream JPEG captures as configured.

5.3.3 - October 1, 2020

When using dual-streaming, JPEG images will be created from the main-stream instead of the sub-stream where possible. Rather than fully spooling up main-stream decoding, the software uses the direct-to-disk pre-trigger frames buffer to synthesize these images. This

means you should specify at least enough pre-trigger time on the Record tab to span the key-frame interval for your main-stream.

An optional parameter *&jpeg=path* has been added to both the *&trigger* and *&flagalert* web server admin requests. This allows you to replace the alert image with one potentially "marked up" by external analysis.

An optional parameter *&decode=x* has been add to the */image/camx* server request. Use x=0 for automatic sub/main stream selection based on resolution; the sub stream will also be upsampled until the main stream is available. Use x=1 to wait for the main stream or x=-1 to always select the sub-stream.

The RTSP server was updated to accommodate requirements of the Monocle portal for viewing cameras on Echo Show.

5.3.2 - August 24, 2020

Changes and preparations are underway for the new major iOS app release.

Status/Storage has been revised to more closely align with what you will see in UI3 and in the new client phone apps.

A QR code has been added to the final page of the Remote Access Wizard which may be read by the client phone apps to quickly enter all server details.

More efficient database rebuild/repair for larger databases.

With a new option on the Record tab in camera settings, you may now choose to re-size JPEGs captured on the clips list or as hi-res alert images.

5.3.1 - July 16, 2020

Your Blue Iris web server now is also an RTSP server. This opens up even more interconnectivity options between Blue Iris and other systems (home automation, video players, etc.) Use the URI */{cam-short-name}* or */{group-name}*. Authentication is completed via *Digest* encryption only. As with */image* and other web service calls, you may add stream, quality, and image size parameters.

5.3.0 - July 9, 2020

When recording direct-to-disk with a dual-streaming camera, now BOTH streams are saved to the BVR file. Files created in this way will no longer be playable on older releases of this software.

The sub stream will be used automatically for timeline playback as well as low-resolution web requests.

A new right-click menu option has been added to the viewer window to select the sub stream for single-camera playback. You will also find this option on the Convert/Export window.

An action set may be run periodically based on the active schedule; configured on the Schedule page in settings. This may be useful as a “keep alive” or a “health” function when interfacing with other systems.

5.2.9 - May 26, 2020

Support for IPv6 addresses in a “dual stack” mode. If your router provides an LAN IPv6 address for your PC, you will now see this on the LAN IP list on Settings/Web server. If your router and ISP support IPv6, you may now connect to your Blue Iris service this way remotely as well. Unless you select to bind to a single address, the software will accept connections from both IP4 and IPv6 addresses.

IPv6 may also be used for camera addresses on your LAN or elsewhere.

5.2.8 - May 20, 2020

Direct-to-disk BVR recording will now include metadata for video overlays (bitmaps and text), motion detection rectangles, as well as camera state flags (such as DIO input bits, motion sensing and triggered state).

When a BVR file containing these new metadata is opened in the viewer, you may right-click and select from menu options to toggle their display.

5.2.7 - May 1, 2020

You may now specify a second “sub” stream for an RTSP camera. The software will pull video from both streams, using the main stream only for audio and direct-to-disk recording

(and playback) and the sub-stream for everything else. This really has become a necessity with the popularity of 4K (8MP) cameras (and beyond).

5.2.6 - April 22, 2020

This version introduces a split in the automatic update function. You may now choose to continue with (sometimes daily) updates encompassing both major changes and/or minor fixes. Or, you may elect the new option, which will skip updates until changes have been validated as stable by those on the more-frequent update track. In addition, previous stable updates may be made available through this same mechanism, and options exist to backup the main exe and update packages.

5.2.5 - April 9, 2020

Many users take advantage of the camera "clone" functionality in order to record video and images in various ways. You may now select to include all cloned camera clips with the master's clips when the clips list is filtered by camera—there's a new checkbox on the camera settings General page.

This version removes the dependency on the second executable BlueIrisService.exe—now there are fewer moving parts for more stability. This should help with recent security software issues encountered with Sophos and Bit Defender which did not allow the service to launch a second process (BlueIris.exe). You must remove and then re-add the service from the Settings/Startup page before this will take effect. When enabling the service, the software will now also prompt for logon information, check the password, and provide the account with the necessary privileges.

If the service were to ever crash, the console window now more reliably reconnects to the service to prevent interruption in the display.

5.2.4 - March 31, 2020

PTZ preset images may now be viewed on the PTZ/presets page in camera settings. These images are now also manageable via remote management. The images now may also be used for motion zone editor "backgrounds" which may be useful if you are editing at night or when the camera is otherwise offline.

Hardware decoding has been advanced further and the DirectX and D3D11 decoding options are now fully operational on systems which support this. This provides a way for those with AMD and those who may have otherwise been unable to use the existing Intel

and Nvidia options to now take advantage of hardware decoding acceleration. You may select this as a default on settings/cameras, and/or individually on camera settings Video tabs. Use task manager to monitor GPU utilization alongside CPU and check status/log for any initialization issues.

Hardware encoding is out of beta and has been fine-tuned for Intel chipsets. Hardware encoding may be selected on any encoder configuration page throughout the software, as from camera settings/record/format.

You may select to "retain" messages sent to your MQTT broker if you are using these for camera alerts.

5.2.3 - March 26, 2020

The email alert MP4 as well as the push alert GIF will now begin with 5 seconds of "pre-trigger" time, making them immensely more useful. Previously, these began recording only at the time of trigger. The requirement for this feature is that your camera is set to record in "direct-to-disk" mode. Please also check your key frame rate to insure that it's at least 0.50; 1.00 is recommended—this is displayed on the Status/Cameras page alongside the FPS. Also, the video encoding parameters for the email alert MP4 must not specify to resize the video (re-encoding will be required). The email alert MP4 will also be created "direct-to-disk" which will ease use of the CPU, however it may result in a larger file, as this is now the camera's full resolution. Your system must also be able to open and play MP4 files in Blue Iris—you can get the K-Lite codec pack for this if not already installed: https://codecguide.com/download_kl.htm.

5.2.2 - March 20, 2020

Video components were updated and the Intel hardware decoding interface was redesigned and recoded in an attempt to bring some missing features online such as H.265 decoding and H.264 encoding. The 64-bit version is required for all hardware acceleration, and you may need to now update your Nvidia drivers if you were using this. New hardware decoding options include DXVA2 and D3D11VA, but these may still be in "beta."

The BlueIrisService.exe was compiled for 64-bit and now uses updated methods to stop the running BlueIris.exe without resorting to a force-close.

5.2.1 - March 11, 2020

For each action in an action set, you may now assign trigger sources and zones. In addition to the profile, these conditions must be satisfied in order for the action to be executed.

For the action set test function, you may select a profile, a trigger source and zones to be "emulated" during the test.

The "wait" action has been expanded to offer actual synchronization with previous actions or with camera re-triggers. Options are also now provided to cancel previously queued and subsequent actions when the wait is over based on camera state.

The "live pause" icon at the top/right of the cameras window now also pauses camera auto-cycle as well as live video. Also the "live pause" command is available now to add as a keyboard shortcut. Note that you must HOLD DOWN this icon to activate the pause.

5.2.0 - March 4, 2020

Although largely "under the hood,"significant changes made for this release justify a bump in the minor version number.

Camera streaming code has been revised for performance and efficiency. By moving one step "closer to the metal," the goal here was to better support multiple high-bandwidth cameras and to prepare for IPV6 connections. With a larger system, you should see modest reductions in CPU demand as well. It's still possible for the network receive buffer to become overwhelmed if the CPU/GPU cannot keep up with decoding all frames in real-time (when not using the limit decoding feature)—to better handle this we will be adding support for dual-streaming main and sub-streams.

Web server code has been revised for performance and efficiency. By removing layers of abstraction, the web server should be faster and more reliable overall.

The software will prompt for a user login when the **Always run as Windows Admin** has been unchecked on the Settings/Startup page, now even when BlueIris.exe is run with Windows administrator rights.

Updates for Sentry Smart Alerts API 2 preparing for facial recognition

5.1.0 - February 16, 2020

A clip “export” command has been added to the JSON web services. This allows the UI3 to offer a more powerful experience managing video exports and downloads.

Once the evaluation period is over, the software will continue to run as a “viewer only.” This allows BVR files to be opened and exported without a software license.

Copy and Paste buttons have been added to the motion detector mask editing window. Masks may only be pasted when the target image size matches the copied image size.

Using the Shield icon or camera “pause” commands you may now cancel a camera alert in-progress.

5.0.9 - January 31, 2020

Video encoder options now include an audio bitrate selection. This and the audio codec setting are now honored for convert/export.

The /admin?sendkeys interface may now be used to emulate keyboard input. This addition supports integration with HA software requirements.

The Plate Recognizer option from the camera AI settings page now has a minimum confidence setting before a plate number is written to the database.

When using HTTPS for both WAN and LAN, the *secure* flag is added to the HTTP *Set-Cookie* response header. This is required for PCI compliance in some organizations.

When using the option to log all web server connections, failed authentication attempts also now are logged.

5.0.8 - January 10, 2020

The auto-cycle option to *Only cycle when at least one camera is triggered* will now display all triggered cameras together at once

It is now possible to change the selected camera group during timeline playback. This makes is easier to follow motion events without having to exit playback.

The camera settings window now loads tabs as they are visited, allowing this window to open and close more quickly.

Many updates to make Remote Management more reliable when live updates are made to camera and other configuration

UTC timestamps for Alert images now reflect any pre-trigger time that's recorded; previously this was the video frame at the time of trigger. This change helps with alert-to-alert navigation in the timeline view.

The Sound alert may be specified to continue through the duration of a camera trigger.

The daily automatic database compact & repair may be ran on specific days of the week.

The camera red border when recording is now optional.

5.0.7 - December 15, 2019

The web server will now send an "image not found" JPEG in reply to an /alerts/ request for a non-existent database record. Previously there was either no response or a file not found error returned and these both confused the iOS app.

The use of HTTP keep-alive semantics is now optional on the Advanced page from Settings/Web server.

The Plate Recognizer AI integration now pulls a status on the Trigger/AI page. This serves to both validate the token entry as well as to provide usage statistics for the current period.

Camera source triggers (via ONVIF) were previously handled as "external" triggers but are now labeled more appropriately as ONVIF triggers. A new check box on the Alerts tab in camera settings determines whether alerts will fire for ONVIF triggers. The trigger state in Blue Iris now is also maintained until a trigger reset event is received from the camera (previously this was ignored and the trigger ended after the break time only).

One headache from the use of Intel hardware decoding has been the ambiguity between 1088 and 1080 line resolution. The Intel decoder will take a 1080 line source and force an output of 1088 lines. This is because 1080 is not a multiple of 16, yet 1088 is, and that's required by the decoder. This has caused confusion as a new resolution forces a new zone map in the motion detector. Beginning with this version, the output size is cropped at 1080 lines. This will eliminate "garbage" lines from appearing at the bottom of the decoded frames. However, this may result in the need to redesign your zone maps, sorry for that inconvenience.

5.0.6 - November 11, 2019

Camera frame windows now operate more independently. Each frame window now may have its own settings for Temporary full screen (double click), Auto-cycle, Show camera names, and Solo selected camera. This provides much more flexibility for systems with multiple monitors.

Improved audio/video synchronization from timed sources (RTSP, HLS, analog devices)—timing information will be stored to the BVR file and although efforts have been made to improve live and BVR playback synchronization, this timing information is most valuable when exporting to MP4 format.

Improved responsiveness to motion with managed decoding (limit decoding unless required on camera settings Video tab).

5.0.5 - October 23, 2019

You may now select to use the Time-Lapse feature during automatic export configured on the Settings/Clips page or for bulk/background export configured by right-clicking clips. Previously this was only available when exporting from the clip viewer window.

The web server now makes more extensive use of the HTTP connection “keep alive” header to reduce the number of connections to the server. This will help with overall efficiency, but especially when using NGROK and some AT&T routers which have recently introduced a “TCP flooding” prevention mechanism, potentially breaking web services.

The code-signing certificate used to verify secure binary deliverables has been renewed for another three years and all executables have been re-signed.

The architecture used to create group images for streaming has been redesigned and coded to allow for higher frame rate throughput. While it’s now possible to get 30 fps from a group stream, this may still not be practical for most users with dozens of cameras due to the CPU resources required. Flickering of borders and timecode under high system demand should be mitigated as well.

Inter-process communication between service and console has been revised to allow the service to better control the console when required.

The email alert configuration now isolates the “alert image” from the other image types which may be attached.

The full log may now be downloaded from the Status/Log page during remote administration.

The push notification “rich push” and GIF options have been moved from the Settings/Web server/Advanced page to the push notification alert configuration page. And for even more flexibility you may now choose to use the camera’s current image instead of the alert image.

5.0.4 - September 16, 2019

A new “folder” icon at the top of the Clips window allows you to select special database views. Notably, Sentry Smart Alert views may be found here, for either confirmed or canceled alerts. Only newly added alerts will appear in these views unless you repair the database.

A new option on the AI page from Trigger in camera settings allows you to automatically “flag” confirmed Sentry alerts. Until dedicated views can be added to the client phone apps, this may be useful.

5.0.3 - September 15, 2019

With a continued focus on AI for version 5, it was time to upgrade one of the most critical of algorithms in the software—the motion detector. You will find a third choice has been added to the algorithm selection box found on the Motion configuration page from the Trigger tab in camera settings—*Edge vector*. This will eventually replace *simple* as the default. The algorithm discerns between leading edge and trailing edge motion and uses this information to compute a motion vector (magnitude and angle). The goal for this new algorithm is to reduce false positives (a consistent vector is required over the make time in order to trigger) and to feed more advanced AI with more relevant frames. Please provide feedback on effectiveness (in the form of BVR video clips for analysis).

5.0.2 - August 12, 2019

Blue Iris now honors the Windows preference to move the cursor to the default button (usually OK) on pop-up message dialogs.

The code to create and alert images has been moved to its own thread—this makes the video capture thread more efficient and allows for alert image post-processing. Also, the trigger/alerts thread has been re-written to work most effectively with Sentry Smart Alerts.

Sentry Smart Alert configuration has been moved to a new page “Artificial Intelligence” from the Alerts tab in camera settings. ALPR support using Plate Recognizer has been added to this page as well. Sentry works to filter false-alarms via person-detection. ALPR works by analyzing the alert image—if a license tag is found, the number is added to the database and visible on the alerts list.

5.0.1 - August 1, 2019

After a couple of months spent focusing solely on bug fixes and minor usability enhancements, we have reached a point of stability that now allows us to continue with more significant development.

The console now recognizes when the service has crashed and has been restarted. An automatic reconnection is attempted for seamless use of the console window.

The latest version of the Intel MFX library (2019R1) is now being used. This update was made in an attempt to bring stability to systems experiencing memory leaks with some versions of the Intel drivers, and to possibly offer H.265 decoding and (eventually) hardware encoding using Intel QuickSync.

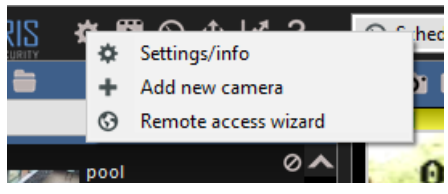
USER INTERFACE

The main window

Settings

Use this button to access the main software settings. It's also possible to right-click to bring up a menu with the Settings command along with other important functions placed here for your convenience.





UI layout

These buttons allow you to toggle the visibility of several important views:

Toggle the Clips list along with the clip layout and filter options. The clips list provides a table representation of either files, alerts, or flagged items.

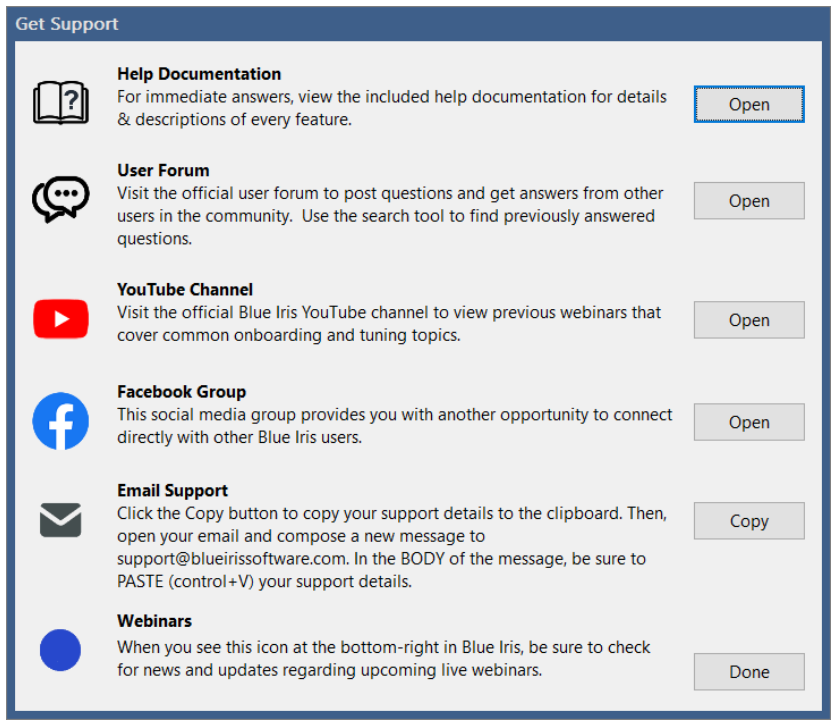


Toggle the Timeline view and associated timeline controls. The timeline view provides a chronological, track-based representation of your video and alerts.

Toggle the PTZ bar for camera movement and control. Along with basic Pan, Tilt and Zoom, this is where you will find controls for brightness, contrast, IR lights and more.

Help

There are several ways to get help with something about which you'd like to learn more:



Before writing an email support request, you may wish to take advantage of our other support offerings for more immediate assistance. These include the documentation you are currently reading, a YouTube channel, a Facebook Group and a robust user forum.

When emailing for support, please first use the **Copy** button. Open your email and paste the support details into the BODY of the message (not the subject line). The support details contain the support email address that you need, which you may copy and paste into the **To** box. Please compose a relevant subject line and provide as much detail as you can about the issue you are experiencing.

Hold **Control** before clicking the **?** icon to open the Help file directly.

Hold **Shift** before clicking the **?** icon to copy the support data to the clipboard, bypassing the Get Support window.

Status window



The status window is a separate “floating” desktop window which provides views of the message log, web server connections, camera statistics, clip storage statistics, as well as remote management status.

Shield, profile, and schedule



Shows and allows you to set the active schedule



Shows and allows you to set the active profile



Shows normal profile/schedule operation. A red stop icon or yellow pause icon may also be displayed.



When green, the shield icon shows protected status. The shield may also be red or yellow in transition states.

Please see the Shield, Profiles and Schedules chapter for more discussion on these icons and their functions.

Remote management



Shown when the local cameras are active in the main window UI. If remote servers have been added on the Remote Management page in Status, you may select one to become the active server.



Shown when a remote Blue Iris server is active in the main window UI.

Main window controls



Standard Windows minimize function—software is shown in the taskbar only. An option to minimize to the “system tray” instead is available on the Startup page in Settings.



Standard Windows maximize function—the software will occupy the entire screen.



When maximized, this icon will “restore” the main window to its previous size and position.



Close the main window UI. If you are running as a service, the software continues to operate in the background.

Live camera window and controls



Play or mute live camera audio. Mute status and volume level should persist as the software is closed and restarted.

Add a new camera.



Full-screen video for the live cameras window. Main window UI elements are hidden, unlike the Windows maximize button. It's possible to start up each time with full screen video with an option on the Startup page in Settings.



Pause live video. This may come in handy when using remote desktop where the constant drawing of video consumes all available bandwidth. You must LONG PRESS this button to activate it, as it easily may be enabled inadvertently.

Selected camera controls

Select a camera by clicking on its window. Currently, there is ever only one selected camera, whether it is located in the main window or in a desktop frame. The selected camera will have a thicker, brighter border than the others.

It's always possible to de-select all cameras by clicking anywhere in the live camera window not occupied by a camera window.



Open Camera Settings. Please see the Cameras chapter for detailed discussion on the many pages and settings available here.



Snapshot saved to the database/clips list. Hold Shift while clicking to save a JPEG image to an arbitrary file location. Hold Control before clicking to immediately mark the snapshot as flagged, which may also include protected (read-only) status.



Manual video record start/stop.



Manual trigger. The alert image is marked as an External trigger in the alerts list.



Enable/disable the camera. Hold Shift while clicking in order to enable/disable all cameras in the selected group at once.



Start/stop live audio. If this option is unavailable, you may have enabled the automatic management of live audio from the selected camera on the Cameras page in Settings.



Hold down to send audio from the PC microphone to the camera. This feature must be developed on a per-camera basis as there is far from an industry standard for how this is implemented. If the "talk" feature is not available for your particular make/model camera selection, the audio will be played from the PC speakers. This does provide you with a way to communicate with cameras/users in close proximity to the Blue Iris PC.

Selected group and controls



Shows and allows you to change the displayed camera group. The clips and timeline views are always filtered to only show items relevant to the selected camera group. Cameras are added to groups on their General pages in Camera Settings.



Groups and group layout may be edited by entering *layout edit mode* with this button. Right-click in a camera window to adjust the layout. You can also drag and drop cameras in this mode. Turn it off when finished to return to normal operation.



Open group settings. Please see the Groups topic in the Cameras chapter for more detail on this window.



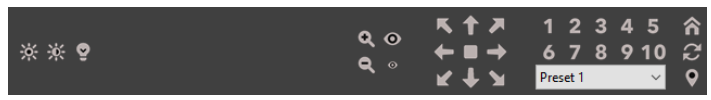
Single-camera or "solo" the selected camera. When in this mode, use the arrow keys on the keyboard to rotate between other cameras in the selected group.



Auto-cycle cameras in the selected group. There are settings on the Cameras page in Settings to **Always solo the selected camera** (which is typically the desired behavior). There's also an option on that page to **Only cycle when in full-screen** video. The remainder of the settings which affect auto-cycle may be found on the Group Settings page for the displayed group—most importantly the "dwell" time.

PTZ controls

Here you find the many controls for camera position—PTZ (Pan, Tilt, Zoom) and Preset position chief among them.



When selecting a camera make/model from the Video page in camera settings, the PTZ protocol is normally selected automatically on the PTZ page as well.

The majority of network cameras support diagonal PTZ movement, but this is not universal.

The center square button serves as “stop” in case the camera misses the mouse-up event for some reason and is stuck moving in one direction continuously. It may also be used to immediately resume the camera event schedule and PTZ preset patrol functions following the manual use of PTZ controls.

Quick access is provided for preset numbers 1-10. For other preset positions, first select it from the list and then use the location/bubble icon. Hold down this icon or one of the numbered buttons to “set” the preset. The “set” functionality is supported for many, but not all cameras—in many cases you will need to set presets via the camera’s own browser interface.

Preset cycle on/off. The software will automatically move between PTZ preset positions which have been selected to participate in this function on the Presets page from the PTZ page in camera settings.

Not all cameras support the following functions:

Move to the preset “home” position.

Zoom in. There is a corresponding zoom out button.

Focus in (near). There is a corresponding focus out (far) button.

Select the brightness level from a pop-up menu.

Select the contrast level from a pop-up menu.

Enable/disable the camera’s IR LEDs and/or “night mode.” Hold down this icon in order to enable the automatic IR LED function (if supported by the camera).

Clip list, layout and filters

The “clips list” may show either actual files, or it may show the “alerts list,” also called triggered “alert images.”



Fold/unfold the clips list. When unfolded, the live video is hidden and the clips list occupies the entire main window UI above the timeline view.



Show triggered alert images. An alert image is captured by default when a camera is triggered and lives only as a postage stamp in the database. It is a “bookmark” into an actual clip video file. When you open an alert image, the corresponding video file is opened at the appropriate time of the triggered alert. Alert images may have corresponding JPEG files, but only when an option is set on the Record page in camera settings.



Show clips, which are actual video files and JPEG snapshots. By default, “all” clips are shown. You can select from a folder list to display only files in a particular folder (that is, New, Stored, etc., as configured on the Clips page in Settings). Also, if one of these folders has subfolders, you may continue to “drill down” into the file structure.



Show flagged items. Flagged items may include a combination of clips (files) and triggered alert images. Flagged items are marked with purple flags in both the clips list and the timeline view.



Show the Clipboard view. The clipboard function in the clip viewer window allows you to tag images and sections of video for later review or export.



Use the **Calendar** icon to filter the clips list to display only items from one particular day. Click it again and use the Cancel button to return to the display of all items.



Use the **Solo** icon to filter the clips list to display only items from one particular camera—the selected camera. If you are using the live view’s camera solo function, the clips list will already be filtered, and it is unnecessary to use this option as well.



Toggle the sort order—either newest first, or oldest first.

If you would prefer the clips list to be docked to the right-hand side of the window rather than the left, double-click in its toolbar area to the left of the calendar icon. The clips list is discussed further in the Recording and Clips chapter.

Timeline view and controls

The timeline view shows a horizontal time-based view of both clips and alerts together. "Tracks" are created based on camera colors. As a clip may contain many video start/positions, a timeline rectangle represents the entire time covered by one clip, but this does not indicate continuous recording over the period represented. However, triggered alerts are represented by a lightning bolt icon above the tracks and an orange band beneath the tracks to represent the time during which the camera was triggered. If you are recording only when triggered, these orange bands therefore will represent times during which video was actually captured.



Adjust the zoom level. You may display a scale in minutes or several days. When zoomed in at the highest levels, alert images are displayed overlaid on the tracks.



Use the time icon to force the timeline view to always display the current time at the right-hand edge.



Instant replay—go back 30 seconds and begin timeline playback. Repeated clicks each will transport back 30 seconds from the current playback time.

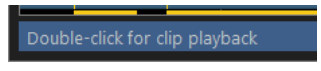


Use the calendar icon to jump immediately to a date of interest.

The timeline view is discussed further in the Timeline playback section of the Recording and Clips chapter.

Tool tip help

As you hover over the various icons in the software, a basic description of the function is displayed here in the lower-left of the main window UI.



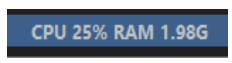
Storage status

The software will display basic storage details here, such as the number and size of clips under management. If there's a problem with the storage configuration or if you are in danger of running out of disk space (due to over allocation, not necessarily low space), you will see a warning in yellow with !! double exclamation points. This warning should not be ignored to prevent an issue with missed recordings.



System status

Your system's vital signs.



The CPU utilization percentage represents the entire system's consumption, not just that of Blue Iris. See the help topic on CPU Management if this value remains at or near 100% for extended periods of time.

The RAM value is that memory used by Blue Iris alone. On a 32-bit operating system, the software may become unstable if the RAM value reads more than 1GB.

Status icons

There are many icons which may you may see displayed in the lower-right corner of the main window UI. Here are their descriptions:



DB maintenance is running—deleting or moving files between folders as configured on the Clips page in Settings. By default, clip maintenance runs each 5 minutes as necessary.



The Log page in Status contains one or more error condition messages. Double click this icon to open the Status window.



The Log page in Status contains one or more warning messages *or* one or more cameras has an error condition or warning, such as low frame rate (less than 15% of the observed actual *max frame rate*), low key frame rate (less than 0.20 if using *direct-to-disk recording*, or less than 0.40 if using *limit decoding*) or there's a push webcasting error. Find the camera/s with this symbol displayed in their window header and then visit the General page in camera settings to further investigate the cause for the warning.



One or more connections has been made on the Connections page in Status.



One or more cameras is in the triggered state.



One or more cameras is detecting motion.



One or more cameras is actively recording video.



One or more alert actions is sending an email message.



One or more alert actions is playing a sound alert.



One or more alert actions is sending an SMS, sending a push notification, or making a TAPI phone call.



One or more alert actions is uploading a file, or FTP is occurring for another reason, such as clip backup configured on the Clips page in Settings.



One or more alert actions is executing a program or script.



The software is being updated, or an update is available. Double-click this icon to directly open the *Check for News and Updates* window.



One or more alert actions is setting DIO output bits.



A remote system is connected and active in the main window UI.

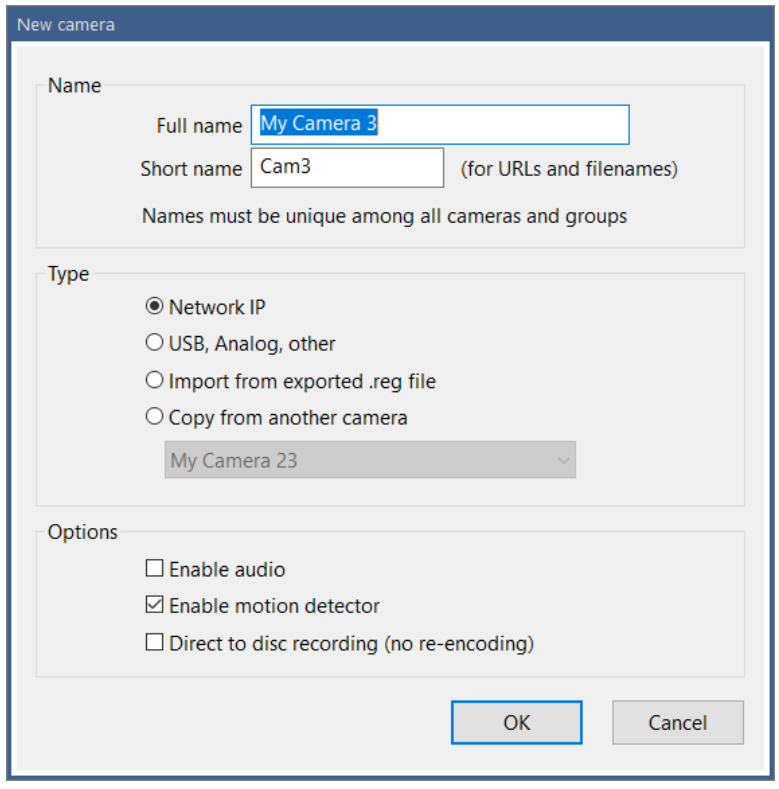


New news items may be found on the Settings page via the **Check for News and Updates** button. Or, double-click this icon.

CAMERAS

ADDING A NEW CAMERA

Use the Main menu button, or right-click in the live camera window to add a new camera.



Before you are taken to the full camera settings window, you are first asked for some basic information, such as the camera name and type, as well as come common options.

A camera has two names—a full or "long" name and a "short" name. The full name may be more descriptive and allows a wider range of characters to be used. The short name is used for URLs (web addresses) and filenames, so the characters you may use are more restrictive. It may be more of an "abbreviation" for the full name.

Both the full name and the short name **must be unique among all cameras and camera group names**. The short name may not both begin and end with a number—it must begin or end with a letter. This allows the software to parse the camera short name from a filename.

The most common type of camera used with Blue Iris is a Network IP camera, one connected with either Ethernet or WiFi. You can use cameras connected in other ways provided you have Windows DirectShow drivers (not proprietary, requiring special software for use).

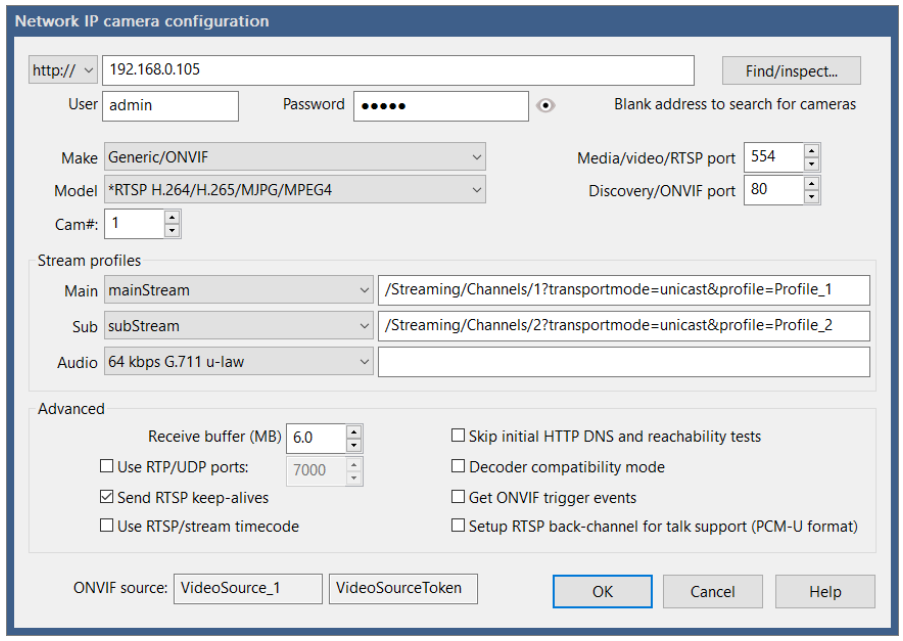
For quick addition of cameras with similar configurations, you may choose to copy the new camera's settings from another camera.

When you click **Ok**, you are taken to the full camera settings window's Video page. In the case of a Network IP camera, the Network IP **Configure** page is also opened automatically.

VIDEO SETTINGS

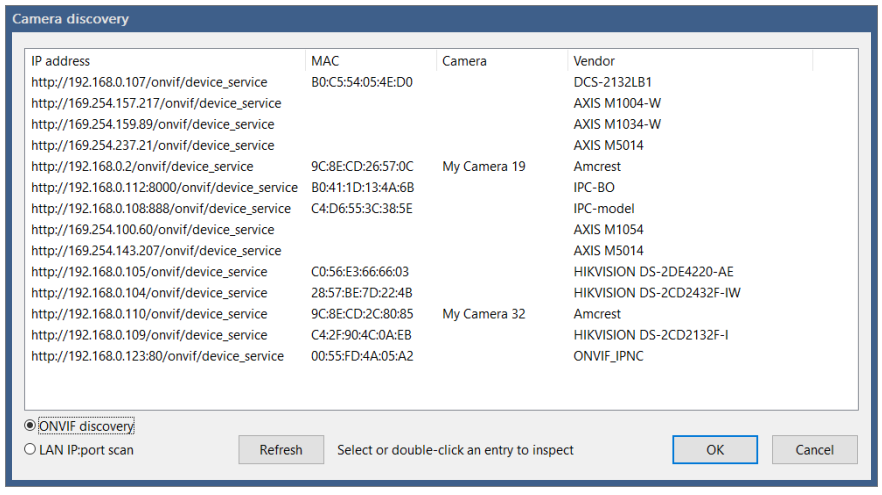
IP cameras

From the Video page, the Network IP **Configure** button opens this window:



Address

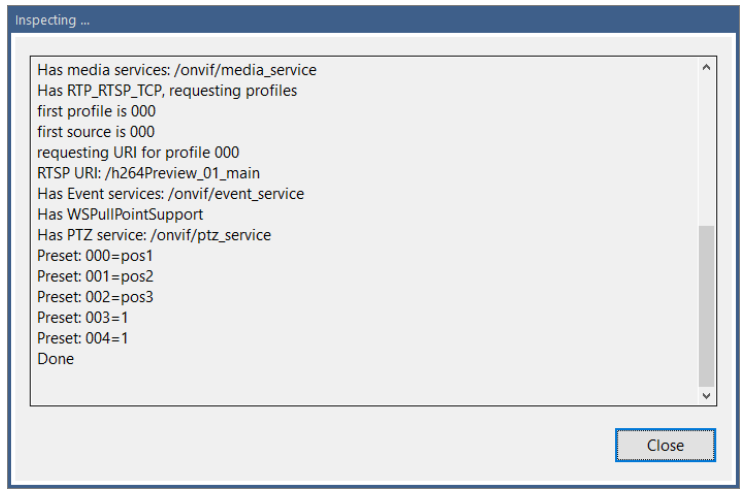
If known, enter a valid camera IP address or network host name in the Address box, as well as the camera's user name and password. If you leave the address box blank, you can try the **Find/Inspect** button to use ONVIF and UPnP to discover cameras connected to the same LAN segment as your PC. Here's an example of what it might find:



You may instead select **LAN IP:port** scan to examine all IP addresses and then detect common camera ports.

For convenience, MAC addresses are displayed, and if a discovered MAC address matches an existing camera, the camera name will also appear.

You may then double-click an item on this list to then immediately inspect the camera using the ONVIF protocol:



If the camera discovery does not find your camera, you may still configure an ONVIF camera by entering its address and then using the **Find/Inspect** button.

There are reasons for and against configuring a camera as ONVIF in Blue Iris. If supported, configuring the camera in this way can be simpler, and in general features such as audio and PTZ will work as well as video. It's also necessary to use ONVIF if you want to use camera-based triggering in most cases. The downside is that there is some functionality which is camera-specific and/or camera-manufacturer-specific, such as the ability to "talk" or send audio to the camera. Some PTZ/control and DIO features may also not be fully implemented via a generic ONVIF configuration. To maintain the best of both, you can always configure using ONVIF and *then* select the specific make/model for your camera or a compatible model if listed.

If you don't know the IP address and the camera does not respond to ONVIF discovery, you can find the address using your router's client table, manufacturer software, or potentially a network port scanner such as:

https://www.advanced-port-scanner.com

Protocol

For most IP cameras, you should retain HTTP as the protocol. For some cameras, HTTPS may be used for JPEG image retrieval only, but this is not common.

Other protocols are listed and these are used to configure the camera using a generic URL such as RTSP:// or MMSH:// etc. This is not recommended unless the camera has no HTTP interface. You may enter the full URL into the address box, press Tab, and it will be automatically parsed for you into protocol, address, and video path.

Make/Model

There are hundreds of compatible cameras here, grouped by “make” or manufacturer. If a compatible camera entry is found here, it is generally preferable to use this rather than the generic category. The audio and PTZ functions will be automatically configured as well based on this selection.

If a compatible camera cannot be identified, and the camera is not responding to ONVIF inspection, you may contact Blue Iris support to have it evaluated for compatibility. You will be asked to supply a WAN address with all applicable ports forwarded to the device for testing.

Ports

The camera’s HTTP port (if not the default 80) should be added to the address, such as 192.168.0.1:8000.

If the camera uses RTSP, RTMP, or another video protocol over a port separate from the HTTP (many DVRs use proprietary video ports), that port number must be specified in the media/video/RTSP port box. The default port for RTSP is 554, which is the most commonly used type of video streaming for Network IP cameras. Some models use RTMP, which has a default of 1935.

The discovery/ONVIF port may be set automatically during the Find/Inspect operation, but setting it manually may be required in some cases. This port number is later used for PTZ operations for cameras configured to use the ONVIF protocol for PTZ. It is also used for the ONVIF *GetEvents* function which is required for camera-based triggering.

Stream profiles

These typically will be populated automatically, either by Find/Inspect or a Make/Model selection.

If you are using a high-megapixel camera (4MP or higher) with an RTSP stream along with direct-to-disk recording, you may specify a *second* video stream path. When used, this is called a “sub-stream” and the primary stream is also known as the “main-stream”. Decoding a high-MP video stream may use large amounts or CPU/GPU time and adding a quantity of these cameras may be impossible on most systems. The software will use the main-stream for audio and recording (and playback), but the sub-stream for everything else, including motion detection and web services.

When using a sub-stream (also called *dual-streaming*), you should also enable *direct-to-disk* recording to BVR format files via the **Video file format and compression** button on the Record tab, otherwise only the sub-stream will be recorded. Also by default, both streams are recorded to the BVR file for flexible playback and more efficient timeline playback. You may choose to only record the main-stream using a setting on the Record tab.

Typically, audio is included with the video in a single stream and the audio path should be **blank**; however there are exceptions.

The camera number selection will replace the macro {CAMNO} in a video path. It's also used internally for some DVR implementations to select the camera number. If the video path has the camera number "hard coded" such as &camera=0, you may need to directly modify this as necessary.

Advanced options

The **receive buffer** is generally set large enough and you should not need to alter this. However for very high bitrate cameras (8192 kbps and above perhaps) on very busy systems (high CPU utilization) it may be required to increase this to up to 20MB to avoid a buffer overrun or dropped packets.

The **RTP/UDP** option is for certain RTSP streaming connections. If your camera is not producing a stream in Blue Iris, yet works with the VLC software using the same RTSP video path, there's a chance that VLC is using RTP/UDP. Blue Iris does not use this by default as it's less reliable and requires the use of multiple ports for streaming. With this option you will need to specify a port number, however *4* ports are actually used, so this number must be evenly divisible by 4.

RTSP "**keep alives**" are reply packets sent occasionally to the camera. Most cameras either require them or tolerate them. In rare cases, these "break" the stream and will cause continuous re-connects each 20-30 seconds.

The RTSP and other video protocols include **time code**—which is a way to keep video frames in proper playback order and timing. However, this time code is not always accurate, so it's possible to disable it here. The software will otherwise use a combination of realtime and frame rates to synthesize the time code.

The software by default first verifies the camera is online by "pinging" its HTTP port before continuing on to video streaming. This allows a check for address redirection, and possibly a session key or cookie as well that may be required for other functionality on some models.

You may elect to bypass this functionality here by selecting **Skip initial HTTP DNS and reachability tests**.

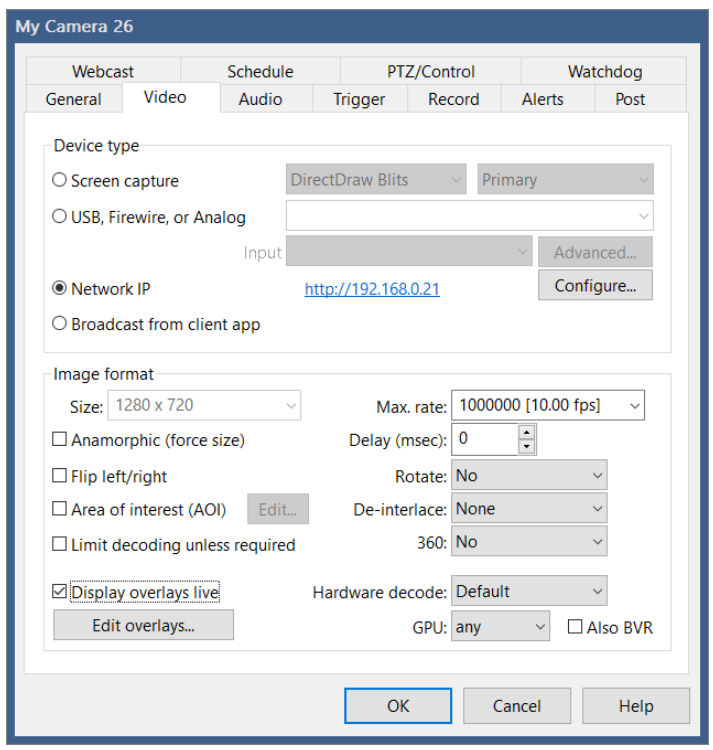
The **Decoder compatibility mode** exists primarily to offer an alternative JPEG decoder which may be more compatible with some cameras, at the expense of CPU time. For RTSP streaming, it also causes the software to ignore dropped packets and to proceed with decoding regardless. This may result in more frames processed, but there may be incomplete frames as a result, showing video glitching.

Use **Get ONVIF trigger events** only with a camera that's been setup with ONVIF, has a valid ONVIF port number, and for which you would like to use camera-based triggering. The software will query the device for trigger and alert information during operation.

The **Setup RTSP back channel for talk** option is used in rare cases. In most cases, the ability to talk or to send audio to the camera is implemented on a per-camera basis and that requires that this box be *un*-checked. One device known to actually implement this feature is the older models of the *Doorbird* doorbell camera.

MORE VIDEO SETTINGS

When not adding a network IP camera, this is the first page you will see instead. Many settings are valid for all camera types as well.

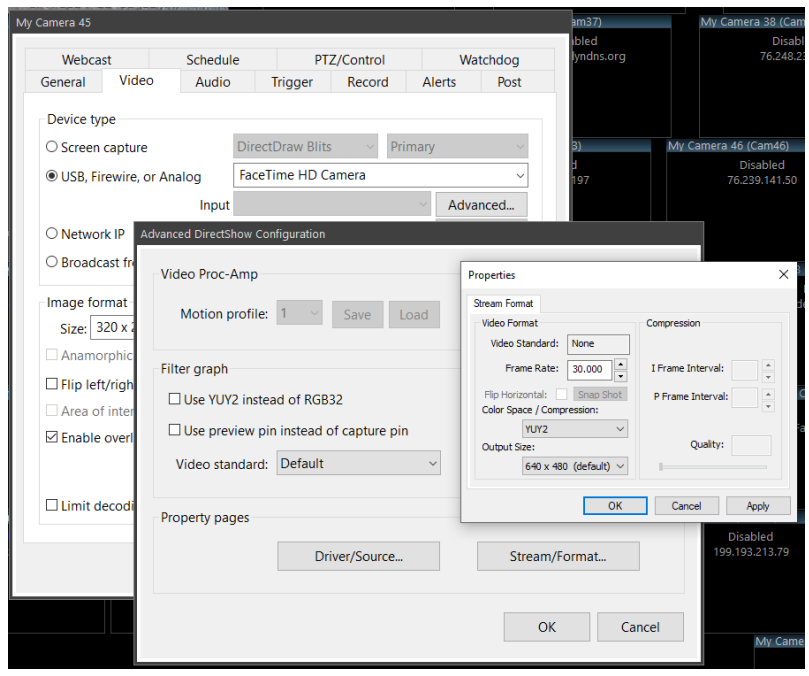


The **Screen capture** device offers a method to use the PC screen as a camera source. You may choose the capture technology, one of:

UScreenCapture	an efficient DirectShow driver
DirectDraw Blits	uses display drivers to copy directly from the screen
Blackness	display only a black image
DirectDraw + Cursor	add a drawn cursor icon

As the service process generally cannot interact with the desktop UI, it may not be possible to use this option (apart from *Blackness*) when running as a service.

USB, Firewire (IEEE-1394) and Analog cameras (via digitizing device) may be added. In all cases, compatible Windows DirectShow drivers must be available. That is, the camera should be working outside of Blue Iris using general Windows software such as Movie Maker or AmCap. If the device requires proprietary software from the manufacturer for operation, it may not be compatible with Blue Iris. When a compatible device is selected, you may edit its **Advanced** properties:



If you are unable to get video from your camera initially, it's worth trying an opposite setting for both the **YUY2** and **Preview pin** options.

It's possible to open two **property pages** that are implemented by the camera's driver here. In some cases this may be required to configure a camera to use MJPG compression, which may be the only way it's able to supply 30fps video at HD resolution for example.

The **Video Proc-Amp** section is used to have Blue Iris memorize the driver's proc-amp settings on a per-profile basis. When the camera's effective active profile changes, these settings will be sent to the camera driver. These settings typically include things like brightness, contrast, color mode, etc. This can be used to force the camera into high-contrast black and white mode at night for example.

The **Broadcast from client app** device type may be used in conjunction with the iOS phone app. From the app you may begin a stream from the phone to your Blue Iris in order to use the phone as a video source.

Image format

In the case of a Network IP camera, the image size and max frame rate are determined for you based on what the camera is sending to Blue Iris. If these are not as you expect, they need to be set in the camera's browser interface directly. In some cases, there may be parameters as part of the video URL which control these settings however.

The **max frame rate** will be adjusted higher automatically, but never lower. This value is used internally by Blue Iris only to allocate buffers, and *is not a setting* per se for network IP cameras. The proper way to adjust the FPS for a network camera is via its own browser interface, typically on a settings page like Video Encoding. However this setting *is* used to adjust the FPS (frames per second) on USB and other camera types. If the *actual* frame rate dips below 15% of the max frame rate, the yellow caution symbol will be displayed in the camera's window header.

The **Anamorphic** option will unlock the image size field for network IP cameras. The actual resolution from the camera will not change, but you can scale or stretch the image as required to obtain the proper aspect ratio or appearance that is required. When using dual-streaming, this option *must always be used* if the sub stream aspect ratio differs from the main stream aspect ratio. In such case, it initially will be automatically enabled and properly set for you.

Flip and **Rotate** settings are offered to account for cameras mounted upside down, at mirrors, etc.

The **AOI (area of interest)** setting may be used with network IP cameras to select a sub-set of the camera's video frame as the video source.

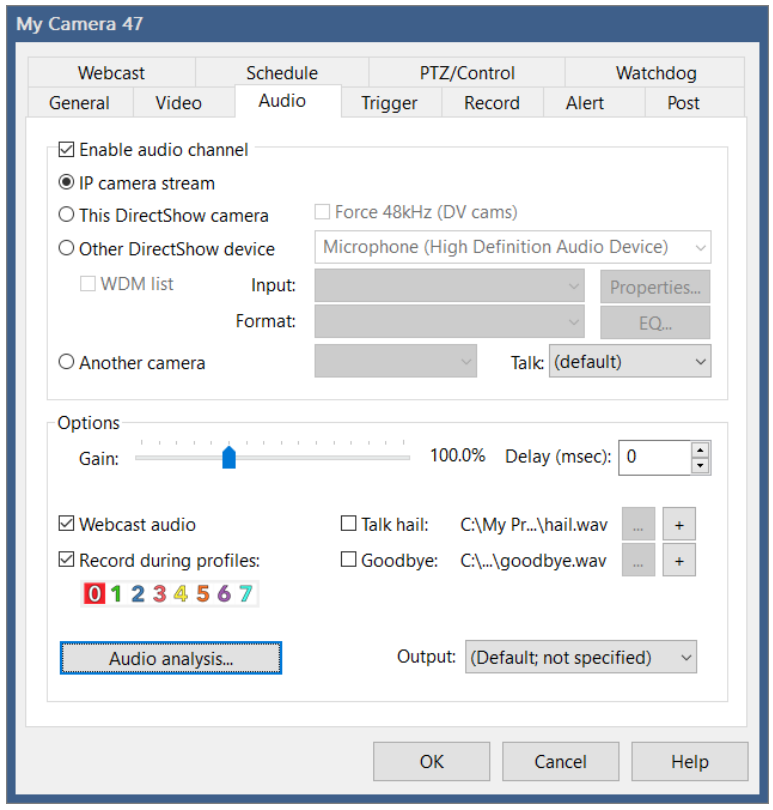
A video **Delay** setting may be used if video arrives much earlier than audio in an attempt to force audio-video synchronization. This is specified in milliseconds (ms).

The option to **De-interlace** video exists only for older analog video sources which merged two video images (fields) into a single frame. This is now rare and deprecated.

Settings for **360, Hardware decoding, Limit decoding,** and **Overlays** are discussed in a section to follow, **Advanced Video Topics**.

AUDIO SETTINGS

You may need to visit this page to enable audio streaming from your camera if it was not enabled initially at the New camera window.



Source

IP camera stream is the proper selection for most network IP cameras. Firewire cameras once offered a multiplexed audio-video stream, and for this you would select DirectShow camera. Otherwise, most USB cameras actually use *separate* devices for audio and video and you must select the audio device here with **Other DirectShow device**.

Instead of using the camera's own audio, it's also possible to mirror the audio from another camera to this one by selecting that camera here.

Options

The Gain slider is used to adjust the camera's relative volume when it's not possible or convenient to adjust the camera volume in another way (as through the direct browser interface or property pages in the case of a DirectShow source). This function applies a multiplication factor to all samples received, so it may result in "clipping" at higher values.

An audio **Delay** setting may be used if audio arrives much earlier than video in an attempt to force audio-video synchronization. This is specified in milliseconds (ms).

By default audio is always recorded and always streamed to web and phone clients. For privacy, legal, or other concerns, you may select to disable this during specific active profiles.

Please note that if you want to further remove audio from a *group* audio stream this may be done through the *group layout edit* function.

Talk

Using a microphone to talk or send audio to the camera is supported for many models. This is completely dependent on the make/model selection on the network IP camera configuration page from the Video page described above in this chapter. If talk is not supported by Blue Iris on the chosen model, the sound will be played from the PC's speakers instead.

You may select on this page a WAV sound file to be played when talk begins (a "hail" sound clip) and when talk ends (a "goodbye" sound clip). Think Star Trek communicator sounds here for example.

AUDIO ANALYSIS

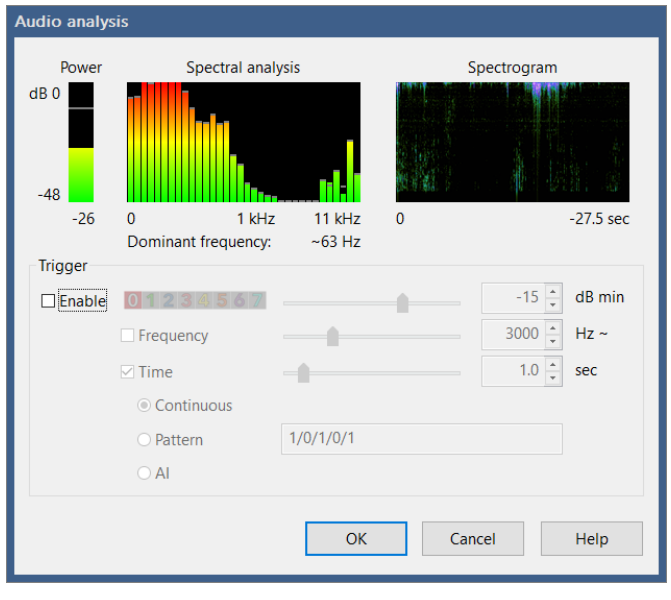
Most cameras supply an audio signal. In the past this was simply stored away for playback purposes only. However, a great deal of valuable information may be contained in the audio track to either enhance the utility of the video or to offer new functionality entirely. A camera's audio signal may be visualized in several ways:

Power is the energy content of the signal. Because of the way that humans perceive volume, the relationship between digital signal values and volume is not linear. The decibel (dB) scale was invented to represent this quantitatively. In order for a perceived doubling of volume, the dB value must increase by 3. Also, as volume and signal strength are not absolute, 0 dB represents maximum volume in a particular context. dB numbers then *go down* from there. That is, -3 dB is 1/2 the volume of 0 dB, -6 dB is half again and so on. After -48 dB, and certainly at -96 dB, you have (near) silence.

Spectral analysis is used to discover the frequency content of a digital audio signal. The theoretical maximum frequency that can be represented in a digital audio signal is 1/2 of the sampling rate, and this is called the Nyquist frequency. So if you are sampling at 16000Hz, the maximum detectable frequency is 8000Hz.

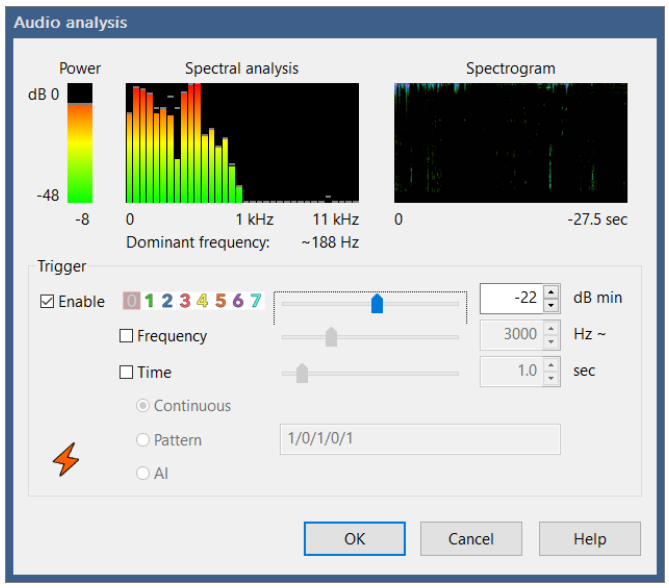
Spectrograms are used to visualize spectral analyses *over time*. Each frequency "bin" becomes a pixel on the Y axis, with each 512 sample set processed over time on the X axis. It is the spectrogram which may be fed into an AI system in order to identify (or more importantly, classify) audio sources. This may become an open area of research for Blue Iris.

Here's what wind noise looks like:

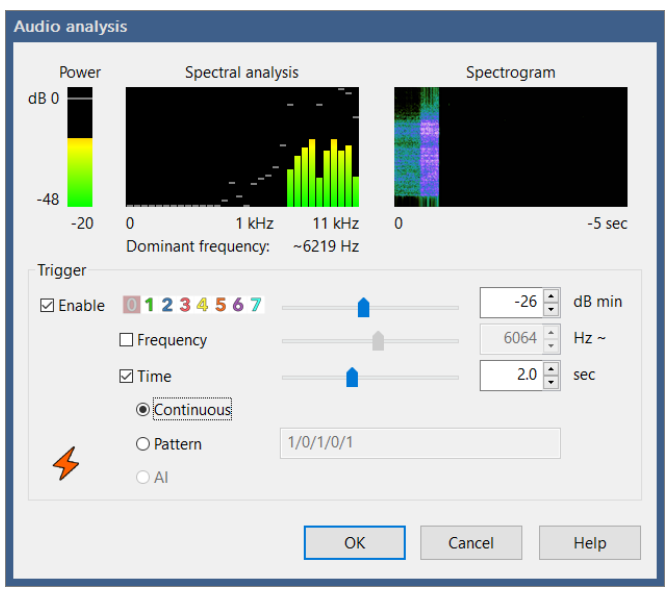


Audio triggering

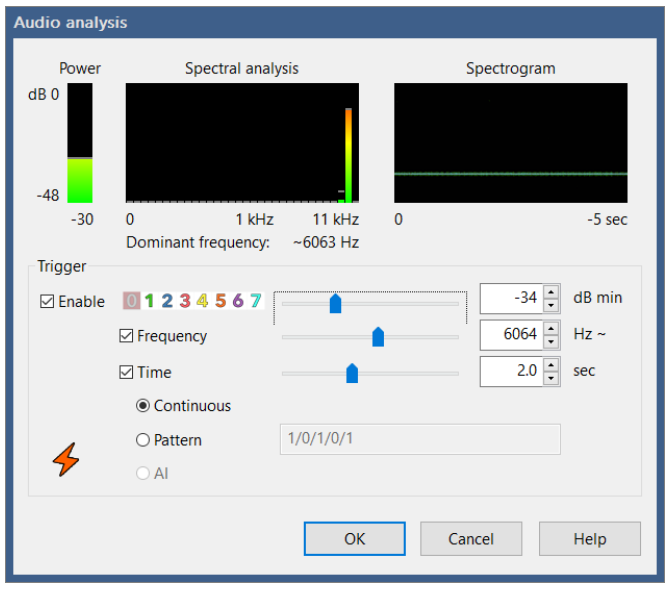
Today, the power content, dominant frequency, and the use of these values with some basic pattern matching may be used for trigger analysis. The lighting bolt icon appears for testing when conditions are right for triggering.



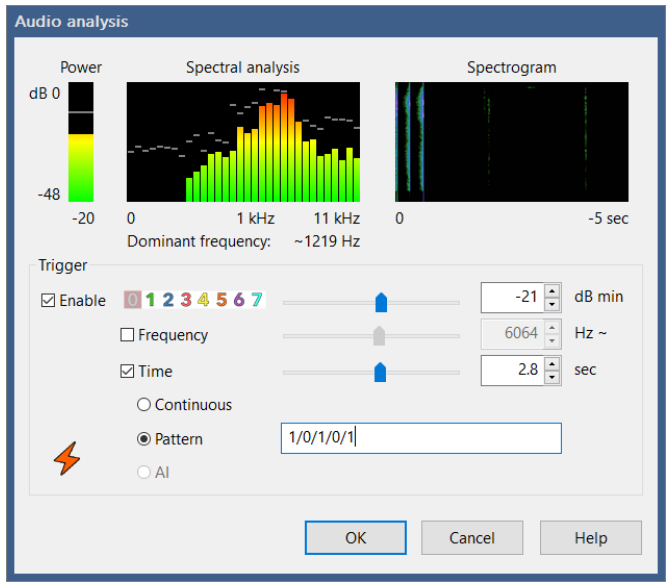
The most basic model involves triggering with a single significant sample set over a specified minimum dB level.



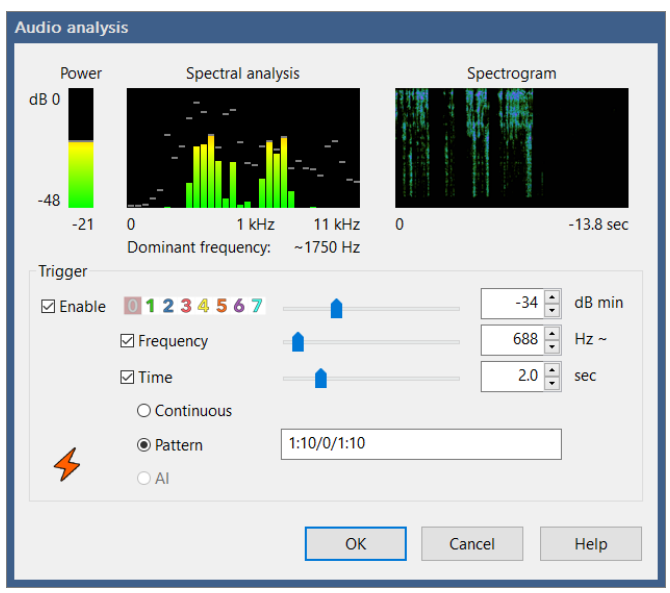
You may specify that the signal must maintain a dB level for a set duration. The signal represented in this example is high frequency white noise.



Here a signal generator was used to provide a proper frequency over the required 2.0 seconds in order to trigger. You may use this to recognize your doorbell, phone ringer, fire or other home alarms.

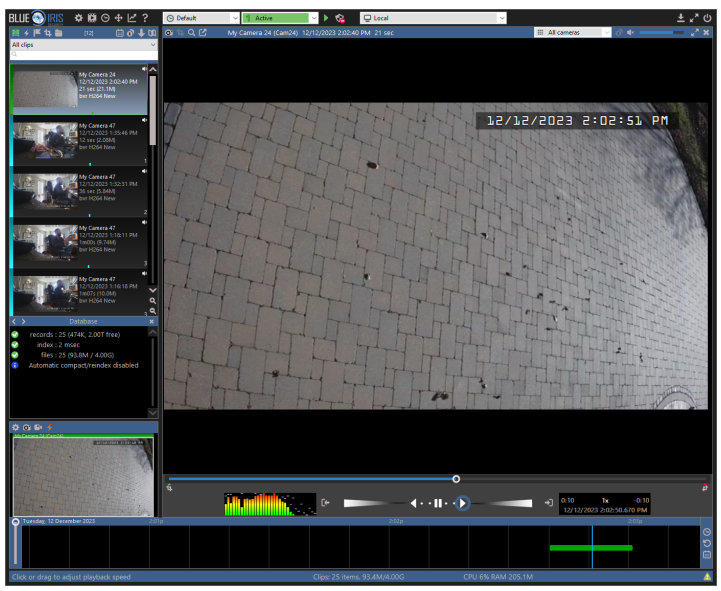


Pattern matching provides methods to specify more complex signal matching. 1's and 0's are used to denote dB power spikes over time. This example shows 3 hand claps within 2.8 seconds and a corresponding trigger.



Here, triggering was achieved with a typical human voice speaking range (100-1000 Hz). The pattern shown here requires two instances of approximately 688 Hz over 2.0 seconds with a break between these. Also shown here, the minimum time for the pattern make/break may be overridden for each pattern component (in milliseconds) by placing it after a colon. The future addition of frequency ranges may further the utility of this type of detection.

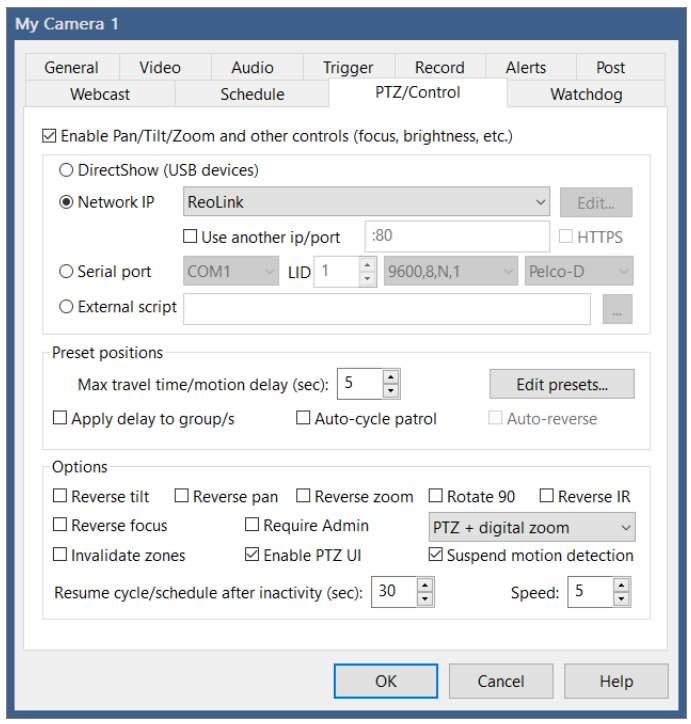
It's possible to replace the 1's in a pattern with specific frequencies (and minimum durations). In this case, the 0's are not required. If you are able to whistle a tune, you may be able to use this ability to trigger a camera, disarm, open a gate—the possibilities are many.



The clip viewer now features audio visualization in the form of spectral analysis. This display is updated as the video moves at any speed, with or without audio played on the speakers. As AI may be applied to spectrograms in the future, this may become an exciting way in which to *search clip audio* for specific types of sounds.

PTZ/CONTROL

Although the PTZ page primarily deals with a camera's ability to Pan, Tilt, Zoom, there are a number of other functions enabled via this page for camera control. Examples include image exposure, DIO (digital I/O) and camera reset.



When using a network IP camera, the type of camera has likely already been pre-populated here for you. Rarely for USB cameras, a PTZ interface is exposed through the DirectShow driver and that may be selected here.

Many analog camera systems have separate serial port-based PTZ motors/drivers. These generally operate using one of several common formats such as Pelco-P or D. You must know the LID (logical ID) and serial port format (baud rate, stop bits, etc.) in order for this to be properly configured. If your network IP camera uses Pelco over the Ethernet connection, you would still use the Network IP option, not serial port.

An **External script** or program may be called for each PTZ command, allowing you to handle this yourself, external to Blue Iris. The parameter sent to the script is a simple command such as UP, DOWN, LEFT, RIGHT, etc.

Options

You may use a combination of settings to adjust for cameras mounted in different ways, or whose drivers expect mirrored commands. These include **Reverse tilt, Reverse pan, Reverse zoom, Reverse focus, Reverse IR lights,** and **Rotate 90**.

Select **Require admin** to prevent non-administrators from manipulating your camera positions. Individual users on the Users page in Settings may be granted PTZ control as well.

By default, **PTZ + digital zoom** is selected and allows you to adjust the PTZ camera position by clicking directly on the camera window when the camera is either "solo" or in a full-screen mode. This is combined with *digital* zoom, which allows you to use the mouse wheel to zoom-in by making the image larger directly beneath the cursor. In order to use a "hand" icon to drag the image while digitally zoomed-in, you may instead select the option for **PTZ unless zoomed**, or **No PTZ cursor** at all.

In addition to the PTZ cursor and digital zoom capabilities, some cameras offer methods for **Direct PTZ positioning** which is invoked here by holding the **Ctrl** key and clicking on the area of the image where you would like to center (and zoom if supported). **Shift+Ctrl** may be used to zoom out instead (where supported).

You may also deselect the option to **Enable PTZ UI**. If disabled, it will not be possible to use the PTZ controls in the main window UI when this camera is selected.

By default, motion detection is suspending during PTZ operation and for 1.5 seconds afterward (move button is released). You may disable this behavior here.

By default, preset-cycle and scheduled PTZ events are disabled for a period of 30 seconds following any manual PTZ activity and this may be adjusted here. This prevents the user from "fighting" with these other functions.

When using motion zones (described in Triggering and Motion detection below) you may choose to "**invalidate**" these when there is manual user PTZ input. Typically your zones are configured against a particular background, and if the camera position changes, these may not longer be valid. However, if you stick to using preset positions instead of arbitrary directional movements, there is a feature to create a custom motion zone map for each preset.

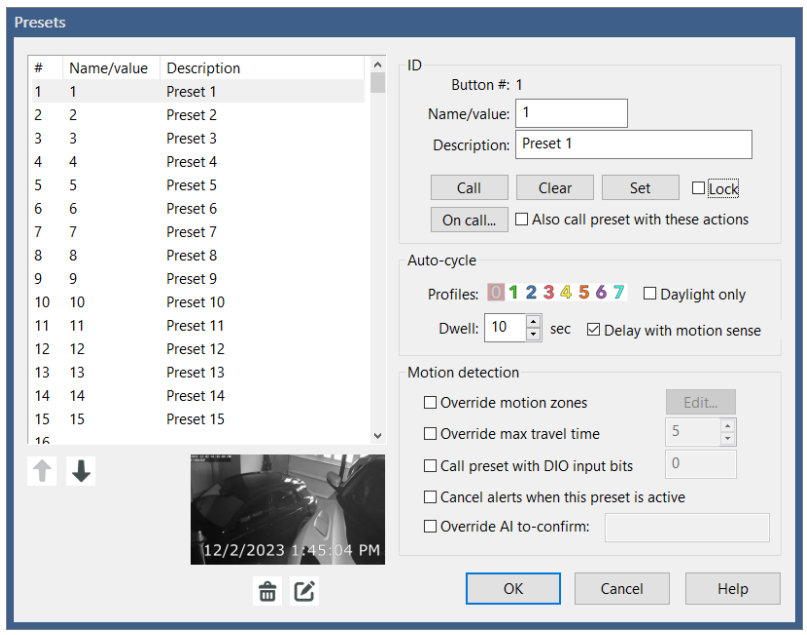
For cameras which support PTZ speed, you may select an initial value here. You may then adjust this using the right-click menu over a camera window.

Preset positions

As motion detection may be suspended during manual movements, it may also be suspended for a preset number of seconds following a preset position change. This is called the "**max travel time**." It's possible to apply this motion suspension to all cameras which are members of any of this camera's groups with the **Apply to group/s** setting.

Auto-cycle patrol may be enabled here, but it also has an icon in the PTZ pane in the main window UI. If you select to **auto-reverse** the cycle, it will "bounce" from end to end such as 1-2-3-4-3-2-1 rather than 1-2-3-4-1-2-3-4.

Click **Edit presets** to adjust individual preset settings.



You may specify up to 40 presets per camera. Although it is most straightforward to configure these 1:1 against what you have configured in the camera, it's possible to set these arbitrarily as well.

The # column refers to the button number in the main window UI. The **name/value** is what is used or sometimes "sent" to the camera for each button. The **description** is typically just FYI, but rarely may be significant to the camera as well.

Use the **Call** button to send the command to the camera immediately for testing. Use **Clear** to remove the name/value and description. Only presets with these values set may be used in the UI or remotely via client app or browser. Use the **Set** button to send a command to the camera to assign the current PTZ position to this preset number. The **Lock** option exists to prevent the accidental re-setting of specific presets via the UI or phone apps.

Use the **On call…** button to define an *action set* to be executed in response to use of the preset button. By default, this occurs *in addition* to what's sent to the camera. Un-check the **Also call preset with these actions** option to skip the camera's normal preset command.

You may choose whether each preset participates in the auto-cycle patrol function, and during which active profiles. Select **Daylight only** to skip this preset before sunrise or after sunset. You may also select how long to wait after calling this preset before calling the next. If you select to **Delay with motion sense**, the next preset will not be called until the camera is un-triggered and is no longer detecting motion.

Motion Detection

Each preset may have its own motion zone map to *override* the one defined for the camera and current profile on the Motion Sensor dialog from the Trigger page. Keep in mind that these maps are resolution-dependent—if the camera image size changes, a new "Zone-A only" map will be created specific to that resolution. If a preset's map is in use and another preset is called *without* an override map, the software will reload the map defined on the Motion Sensor page for the current profile (if one is defined). The *profile-specific* map will also be loaded in the event of a camera restart or profile change—for this reason, when using *preset override* zone maps, you may want to disable the *profile-specific* zone maps altogether and be sure to call a preset each time the camera is restarted (by adding a preset to the Schedule page Events list). For testing and verification, you will find the currently-loaded map's name shown at the bottom of the Motion Sensor dialog. See the topic later in this chapter for instructions on defining motion zone maps.

If certain presets require more or less time to move into position than others, you may select to override the value set on the PTZ page here.

You may specify one or more global DIO bits to be monitored in order to automatically send the selected preset position to the camera. All specified DIO bits must be active in order to trigger.

Select **Cancel alerts when this preset is active** if you want to bypass alerts for this preset position. Recording will still occur when the camera is triggered, if configured. If you are using AI alert confirmation, you may also alter the "to confirm" objects list based on preset position.

Position images

Each preset position may have an associated camera image saved to disk. This image is used to identify the preset position via the UI3 browser interface currently, but may be used for other clients in the future.

360

Use this setting to inform the software that this camera has a fish-eye lens. If this camera is mounted on a ceiling, this can capture a 360-degree view. Mounted on a wall or door, this creates a 180-degree panorama. Your setting here determines how the camera is **de-warped** when viewed via either the clip Viewer window or a remote client.

As it may be extremely CPU-intensive to render the video in this way, it is not currently offered for live video display.

Many cameras with this feature also offer multiple video streams that can be used to break up the warped view into several de-warped views. In this case, you may consider adding multiple camera windows to the software, each requesting a separate view from the camera.

Hardware decoding

With appropriate hardware, it's possible to "off-load" some of the processing that's required to view or otherwise process live video from the CPU to the GPU (graphics card). The software has integrated support for both Intel QuickSync as well as Nvidia hardware decoding (NVDEC). Please see ark.intel.com to learn which chips have this capability and to compare their relative performance. Please see the following link to learn which Nvidia hardware offers this capability:

https://developer.nvidia.com/video-encode-and-decode-gpu-support-matrix-new

This may be enabled globally on the Cameras page in Settings, or here on the Video page per-camera. You may use a mix of these as well for specific cameras.

In testing, there are limits to the number of cameras that may be assigned to decode video via hardware and this will depend on the hardware as well as the overall MP/s (megapixels/second, based on FPS and frame size) being processed by the camera. When limits are reached, actual FPS from the camera will be seen to *decline*, indicating that the processing thread is saturated as it waits for the hardware to complete decoding.

Not all cameras or camera stream formats will be compatible with this technology. The software will attempt to disable this feature and return to software decoding if necessary, and this condition should be logged to the Log page in Status. For the best chance at compatibility, you should ensure that the stream is encoded as "simply" as possible via

direct camera settings. H.264 “main” profile without manufacturer-specific add-ons such as + or “smart” modes is most likely to be compatible. However as hardware decoding and its associated drivers improve, newer encoding methods such as H.265 and “high” profiles may also be supported soon if not today.

With Intel decoding, you have the option to add **VideoPostProc** (VPP). This uses hardware as well for colorspace conversion. The H.264/265 codecs use a YUV variant, whereas Blue Iris must use RGB for motion detection and display. The chipset may provide some assistance with this conversion. VPP is not compatible with the anamorphic or AOI features at this time (anamorphic video is often used when dual-streaming) so it will be automatically bypassed.

The options to use DirectX VA2 and D3D11 VA make use of your video card drivers more directly and may be able to leverage additional features of your hardware, such as AMD decoding acceleration. These may also work with Intel and Nvidia hardware for benchmarking or comparison.

If the software believes that it is using hardware-accelerated decoding, you will see a value in the HA column on Status/Cameras (I=Intel, N=Nvidia). Monitor actual use of your GPU alongside CPU with the Windows Task Manager.

The **Also BVR** checkbox will cause the software to also attempt hardware decoding for BVR clips that were recorded by this camera. As hardware decoding may add a delay (one or several frames) as it creates a “pipeline” for decoding, this may cause an initial “black screen” and then interfere with the smooth use of video scrubbing both in the viewer window and when remote viewing.

Limit decoding

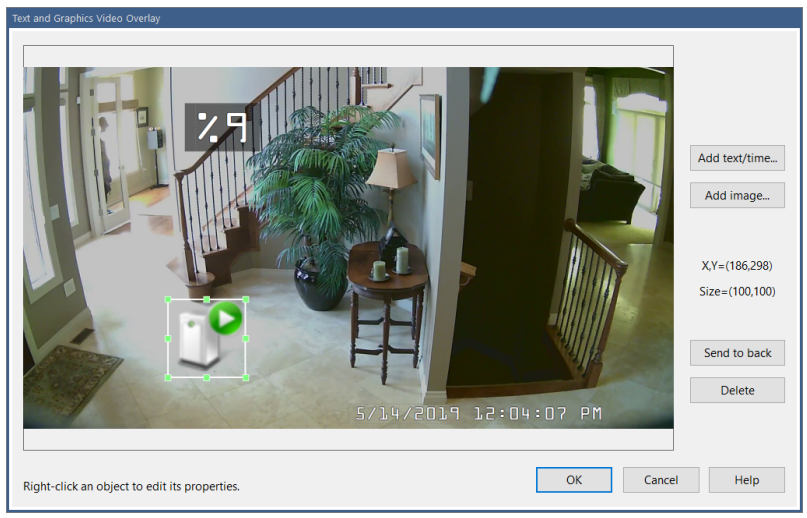
The option to **Limit decoding unless required** is another way to manage CPU resources. When enabled, only *key frames* are normally decoded and displayed. A key frame is a “complete” frame—all other frames rely on key frames in order to be rendered, as they contain only the “changes” from frame to frame. When you select the camera in the main window UI, or if someone is viewing the camera (or one of its groups) via a client app, then *all* frames will once again be decoded for display.

This CPU-saving scheme works great as long as your camera is actually sending an adequate number of key frames. It is recommended to have about 1 key frame/second coming from the camera. This is a setting in the camera’s browser-based settings, usually under a “video encoding” section. It may be labeled as “key frame rate” or “i-frame interval” for example.

You can view the actual rate on either the General page in camera settings, or on the Cameras page in Status. It is shown after the overall frame rate—for example 15.0/1.0 indicates 15 fps with 1 key frame/second. A value of 0.5 or less is considered insufficient to use this feature.

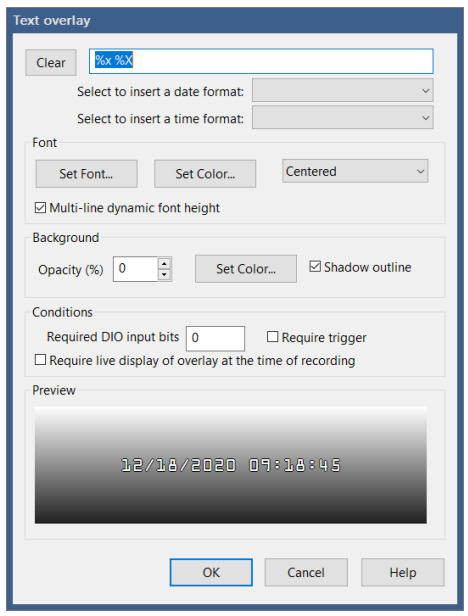
Overlays

By default, a current time stamp overlay is drawn on each video frame. Use the **Edit** button to customize this.



Use the mouse to select, position, and size existing elements. Buttons exist here to also **Delete** and "**Send to back**" in order to manage objects which may be layered in some way.

Use the **Add text/time** button to add a new text overlay:

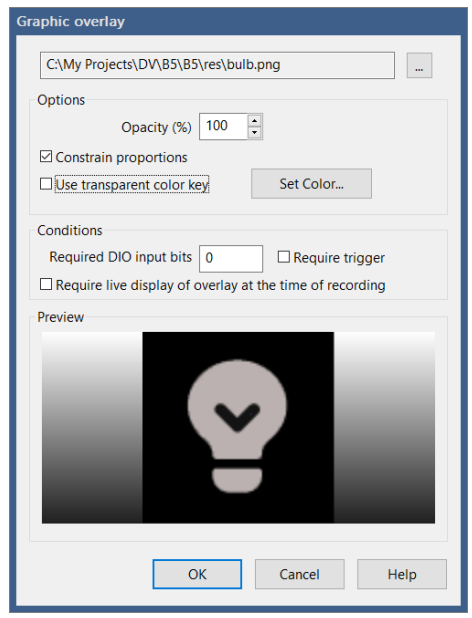


You may choose a preset time or date macro or enter your own. Please see the topic at the end of the Alerts and Actions chapter for a complete list of possible macros. Use the two character sequence \n to force a "new line" in the text for a multiline overlay.

Opacity and shadowing may increase the CPU time required to render the text.

You may select to only draw the overlay when specific global DIO bits are set, the camera is triggered, or only when overlay display is enabled for live viewing. Even if overlays are disabled for live viewing, they are still written to the BVR file and may be displayed upon playback unless *Require live display of overlay at the time of recording* is selected here.

Use the **Add image** button to add a graphic overlay:



A PNG file has a built-in transparency channel. Other formats such as JPG and BMP are supported, but transparency for these involves color substitution—you select the color which should be rendered as transparent.

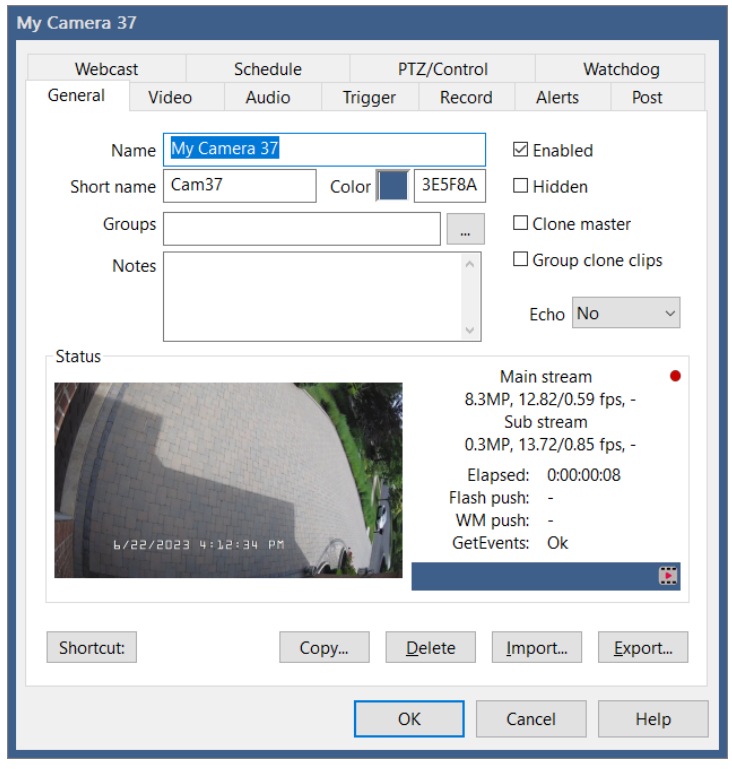
As with text overlays, the use of opacity and transparency here will result in higher CPU demand.

Select to **constrain proportions** to maintain the object's "natural" aspect ratio. Un-select this option to be able to size the object as you please.

You may select to only draw the overlay when specific global DIO bits are set, the camera is triggered, or only when overlay display is enabled for live viewing. Even if overlays are disabled for live viewing, they are still written to the BVR file and may be displayed upon playback unless *Require live display of overlay at the time of recording* is selected here.

GENERAL SETTINGS

Camera name considerations were discussed at the beginning of this chapter. Groups will be discussed in a topic below. However, several other important settings may be found on the General page:



You may assign an **Event color** to the camera. This will be used in the clips list to highlight clips recorded from this camera. It's also used in the timeline view to create tracks, where cameras with the same color are grouped together onto a single track. Click the color box to open a color-picker window, or edit/paste the hex RGB value directly.

Notes exists here for your benefit only, and are not used otherwise by the software.

You may un-check the **Enabled** option to disable the camera, or check the **Hidden** box to hide it. Whether or not disabled and hidden cameras are actually *displayed* locally or remotely is controlled by right-click options while in *group layout*—access that using the *pencil* icon next to the group selection box.

If you have added multiple cameras with the same IP address, video path and camera number, the software *clones* the video stream internally—only a single stream request is actually made to the camera. Which camera window actually connects to the camera may be otherwise random unless you mark one as the designated **Clone master**. By using this option on each camera that would otherwise be cloned, you may defeat the cloning feature altogether and force the software to make multiple streaming requests from a single camera. In order to identify cloned cameras, and asterisk (*) is shown after its name in its window title bar.

If you select to **Group clone clips,** all cloned camera clips will be included with the master's clips when the clips list is filtered by camera.

Until a proper dedicated Amazon Echo app can be developed, beta functionality exists to determine what Echo is able to set concerning this camera. Options include Enable, Select, etc.

Status

This page displays several vital statistics regarding the camera's streaming. These values are also visible on the Cameras page in Status.

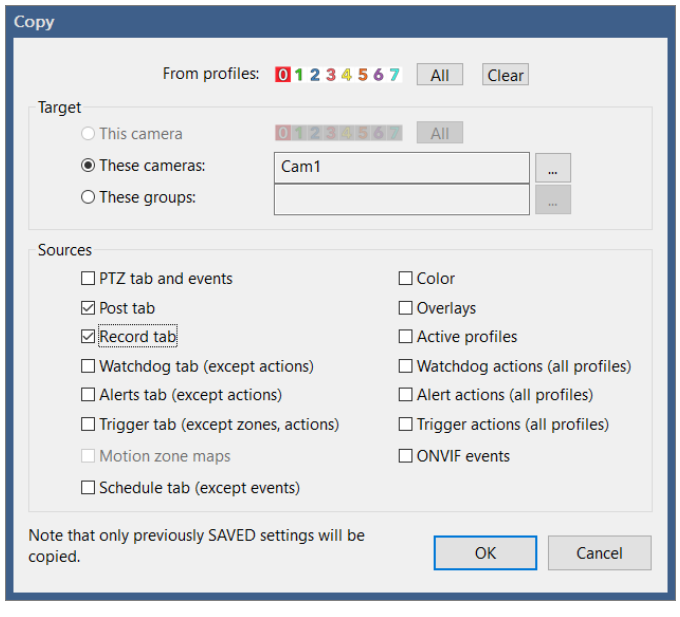
If the camera is actively pushing to a Windows Media or Flash server, that connection status is visible here. These features are discussed on the Webcast page.

If a network IP camera is configured with the **Get ONVIF trigger events** option, the status of that thread is also visible here.

The blue bar on this page will have icons displayed which contribute to the global status window at the bottom of the main window UI.

Copy

The Copy button allows you to quickly share settings among profiles or cameras or groups of cameras:



Copying settings among profiles of the *same camera* applies only to the Trigger, Alerts, Record and Watchdog tabs. This operation will automatically disable the "sync with" option on these tabs. See the **Configuration Synchronization** topic below, as you may be able to use that feature instead if settings change often.

Copying settings to other cameras retains the “sync with” settings from the source camera. Affected cameras will be automatically reset in order to load new settings.

Note that this function copies settings found in the registry (that is, *saved* settings). If you have made changes to the camera configuration that currently exist only in memory, you may want to first click OK to save them and then return to this window to complete the copy operation.

Export and Import

You may save the camera’s settings to a .REG file, and then later import that same file to restore its settings. This is one way to “copy” settings from one camera to another as well. The default registry export format is compressed and this format is required when using the Import button. However if you hold the Shift key while clicking Export, the file will be saved in a human-readable text format. To re-import this type of registry file, you must double-click it from Windows.

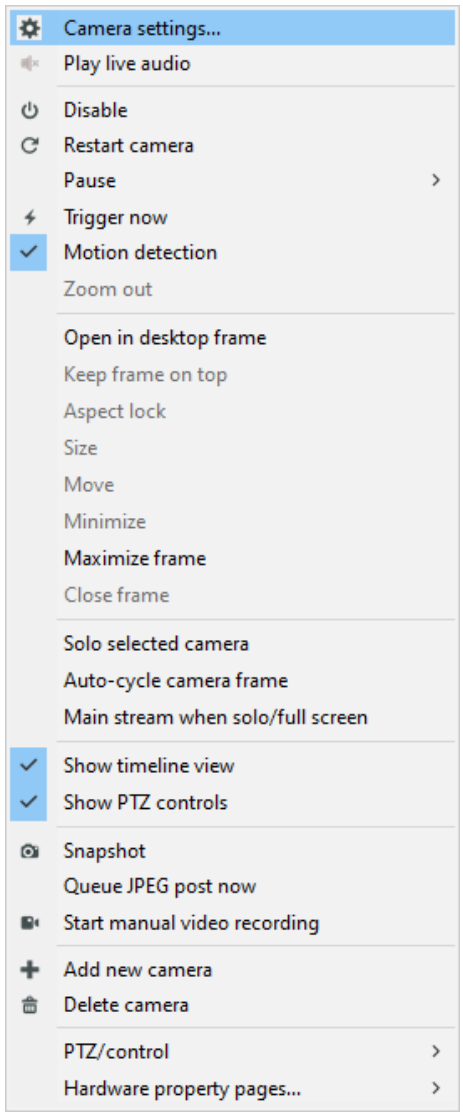
There are buttons to export and import all software settings (including all cameras) at once on the About page in Settings.

Keyboard shortcut

Use the button to **Set KB shortcut** in order to assign a keyboard key combination to this camera. When these keys are used, the camera will be selected. The selected camera may be “soloed” where it is visible alone (an icon at the top of the main window UI controls this feature), or it may be used to determine the source of live audio (see Cameras page in Settings). The camera’s group may be configured for “auto-mixing mode” where the selected camera is used for the group stream, potentially useful in a demonstration or video production application.

THE CAMERA CONTEXT MENU

Right-click in a camera window to bring up this menu:



Many of these commands are available via UI buttons as well and are described elsewhere. However some are available from here alone.

The option to **Restart camera** is a *soft reset*, done in software only. If you want to physically reset the camera, you may find the option on the PTZ/control menu if it's supported by your camera (or just power cycle it).

Camera **Pause** is equivalent to setting the Shield icon to red, but for this camera only. Hold Shift while selecting this option in order to affect all cameras in the selected group at once.

Motion detection is enabled on the Trigger tab in camera settings, however the option exists here as well for convenience.

The section with **Size**, **Move**, **Minimize**, **Maximize**, **Keep frame on top**, and **Aspect lock** are applicable only when the camera is open in a desktop *frame* window (alone or with other cameras).

Use **Queue JPEG post now** to immediately upload an image using the destination set on the Post page in camera settings.

For USB and analog cameras, addition **Hardware property pages** may be available.

Commands to set the camera's DIO outputs and to send a reset command to the camera may be found on the **PTZ/control** menu.

CAMERA WINDOW UI

All available space in the live video window is divided into one or more *camera windows*. By default, a camera window has a border rectangle, a title bar (or header), and video that is displayed in an appropriate *aspect ratio* based on the camera stream resolution. You may customize this display by entering *group layout edit mode* with the pencil icon that's found to the right of the group selection box at the top. Right-click on a camera window to turn off borders and/or titles. You may also override the normal aspect ratios so that cameras are sized more similarly or to fill the empty space. When you perform digital zooming using the mouse wheel, the empty space is utilized and *memorized* when done in layout edit mode.

In addition to the camera's name (or short name if full name will not fit), the title bar may also display a number of status icons:



A number to the left of the name tells you that the camera is operating under a custom profile rather than the global profile. This may be due to a setting on the **schedule** tab in camera settings. Four of the most common status icons are shown in this example. Here are descriptions for each of them:

 Motion is detected

 The camera is currently a triggered state

 The camera is currently in an alerted state

 The camera was alerted; cleared when you click on the window or view the alert

 The camera is currently triggered via an audio source

 Video is now being recorded

 Video was being recorded; the file is still open to receive more video

 Live audio is being played to the computer speakers

 Audio from the computer or app microphone is being sent to the camera

 The camera is paused (right-click option or via phone app)

 The FPS or keyframe rate is too low, or there is a a publishing error

 An image is currently being posted via FTP (see **Post** tab settings)

SCREEN LAYOUT AND FRAMES

Screen layout is determined by the active *group* selection. In order to adjust the layout, you must activate *layout edit mode* (see the Groups topic below).

A camera window open on the desktop is called a *frame* window. Additional cameras may be added to one frame window by dragging them into the frame. The entire frame may then be sized or positioned, possibly onto a secondary monitor. Individual cameras may be removed from the frame by right-clicking and un-checking the option to **Open in desktop frame**. Several options also exist on that menu to maximize, minimize, or close the entire frame (returning all cameras to the main window UI).

Blue Iris remembers the position of all frame windows when it is closed and restarted.

Rearranging camera windows

While *layout edit mode* is active, use drag and drop within the main window UI or within a frame window to rearrange cameras. Many popular remote desktop solutions do not support drag and drop, so it may only be possible to do the this at the console directly.

Digital zoom

Use the mouse wheel over a camera window to zoom-in digitally (the camera lens does not actually move). When zoomed-in, the mouse cursor will become a "hand" icon and may be used to pan around, unless it's a single-camera view and **PTZ w/mouse cursor** is enabled on the PTZ tab.

Use the mouse wheel again to zoom out, or you will find a **Zoom out** command on the right-click menu.

The sense of the mouse wheel may be reversed using a setting on the Other page in Settings.

CAMERA GROUPS

A camera group is used for viewing a subset of cameras a specified layout. They are also used to provide users access to only a subset of all cameras via the Users page in Settings.

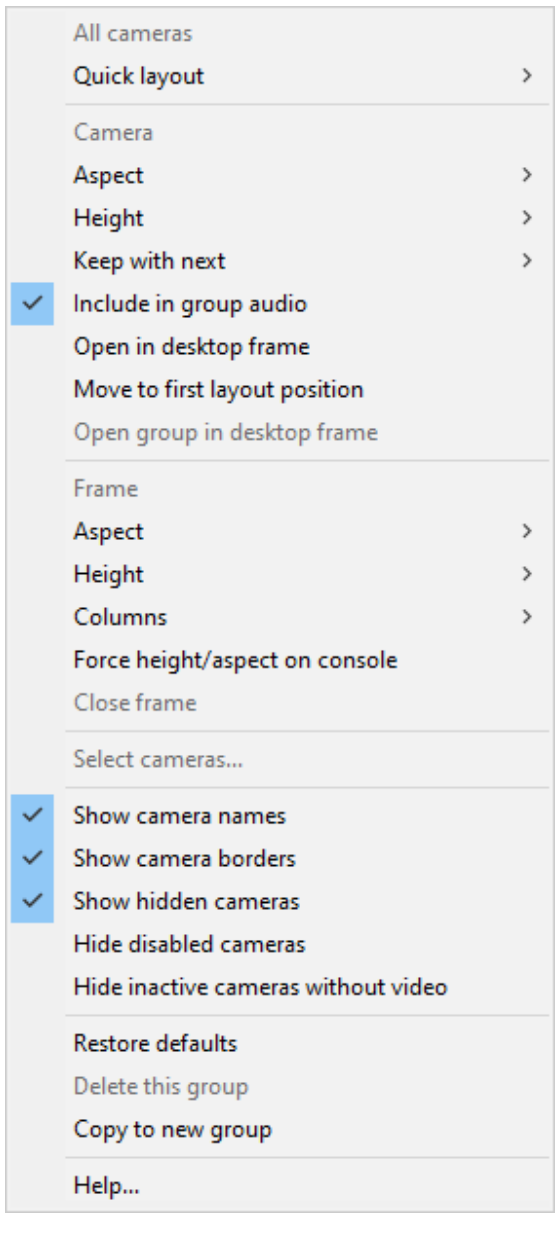
A group is selected for viewing in the main window UI by using the selector box at the top of the window. The clips and timeline views are always filtered to only show items relevant to the selected camera group.

Editing, adding and removing groups

Groups and group layout may be edited by entering *layout edit mode* with this button which is found to the right of the group selector box. Turn it off when finished to return to normal operation.

When in layout edit mode, it's possible to rearrange cameras via drag & drop or to move them into or out of desktop windows, called *frames*. Changing camera zoom position is also memorized as the default for this group layout.

The right-click menu is used to make other layout changes:



The group name is shown at the top of this menu. Following are two sections, one for the camera that was right-clicked and one for the entire frame.

By default, layout resolution and aspect ratio are automatic and a camera's source resolution is used to define its aspect ratio. However you may override a camera's aspect in order to get it to "fit" better into the layout with other cameras. You also may use a combination of zoom (crop) and "scale to fill" options to completely remove space between cameras if so desired.

If you select a height and/or aspect ratio for the entire frame, this will be used for remote viewing via browser or phone app. However, by default, the resolution and aspect are handled automatically on the console. You may use the option to **Force height/aspect on console** in order to see exactly what the remote viewer will see. You may do so temporarily just for editing, or keep this option enabled permanently to guarantee a specific layout on the console as well.

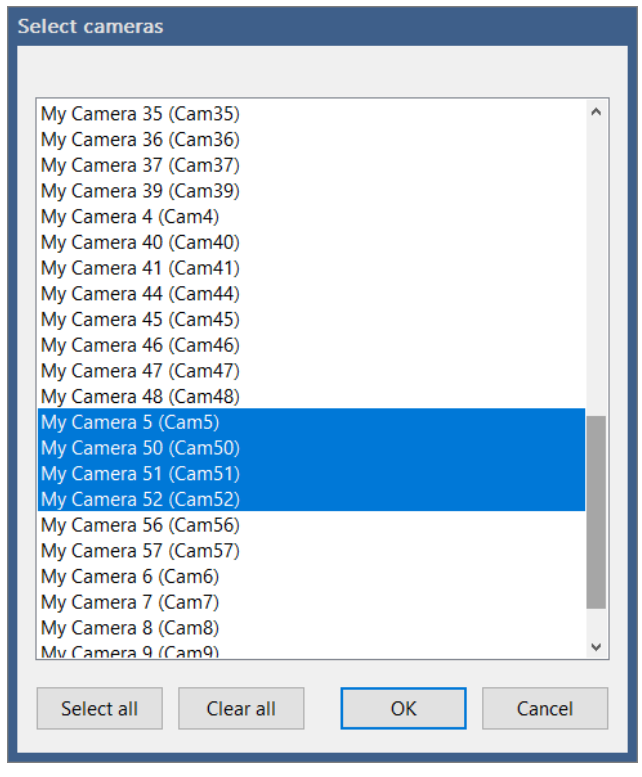
Camera layout proceeds “in reading order” from left to right in rows going from top to bottom. You may optionally select to divide the frame into columns as well. If you select one or more cameras to have a larger height relative to the others, other cameras will fill the space around these cameras, again going from left to right.

Use the **Keep with next** option to further define *subgroups* so that they always stick together. Up to 8 cameras may be combined in this way and it’s possible to have multiple sub groups. All cameras in a sub group will have the same relative height. To change the subgroup relative height, edit the first camera’s height setting. To change the subgroup aspect ratio, hold *Control* while accessing the height menu.

The background spaces are shown in green when in layout edit mode. If you see red however, this indicates that you have selected a layout that cannot be accommodated, most likely due to having too many cameras with relative height differences.

Note that the options to show/hide names (headers), borders, hidden cameras, disabled cameras and inactive cameras affect both the console and remote views. For this reason, you may want to create separate groups specifically designed for remote access.

Use the **Select cameras** option to select the members of the group:

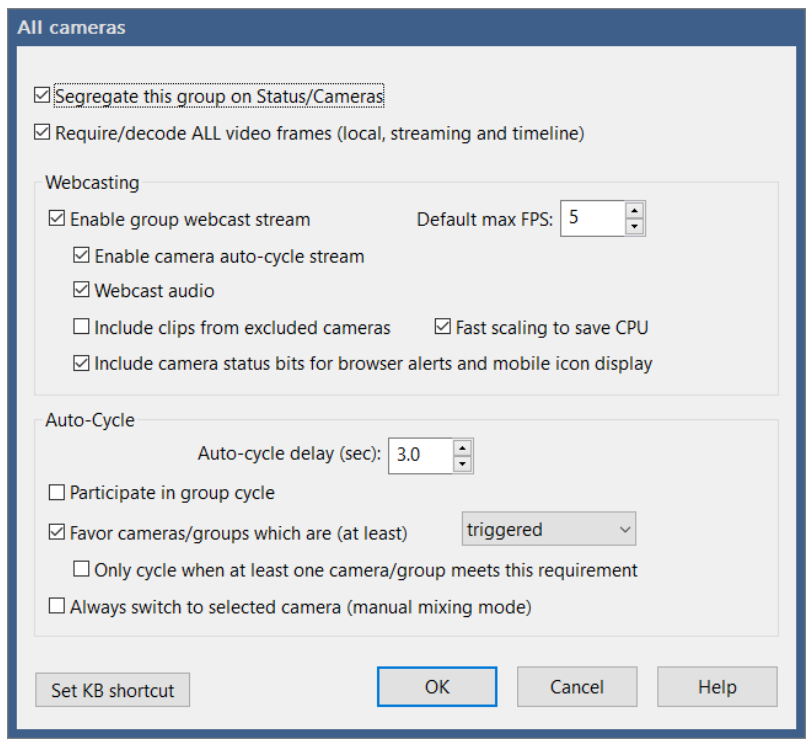


You will find options to **Delete this group** and **Copy to new group** as well. A group should have a name *unique* from all camera short names in order to prevent conflict when requesting cameras and group streams remotely.

Group settings



Use the gears icon to the right of the group selection box to open group settings. A number of options here control how the group may be viewed remotely and how it and its cameras participate in auto-cycling.



By default, a separate section will be shown on the Status/Cameras window for this group. To prevent this, deselect the option to **Segregate this group on Status/Cameras**.

By default, all video frames will be decoded for each camera, either live, streaming, or in timeline playback. As this may be too CPU intensive for some configurations, the option is given to decode and display only the *key frames* found in the video, which may result in a playback rate of 1 FPS or less. Deselect the **Require/decode ALL video frames** option to decode and display only the key frames.

Webcasting

By default, the group will be viewable via remote browser or app and its cameras will be arranged to fit into a rectangle roughly sizing each camera in half. You may instead force a specific size using the **layout edit mode**. The default FPS (frames/second) for a group view is 10, however you may find that using a lower value such as 5 is sufficient, as this will save considerable CPU resources. Use the **Fast scaling to save CPU** option to override the global scaling setting on the Settings/Other pages just for this stream.

By default, all frames are decoded for a fluid display when viewing a group stream. If this becomes too CPU-intensive, you may unselect the option to R**equire/decode all video**

frames (streaming or timeline) which will result in the decoding of *keyframes* only, typically providing a display update each 1-4 seconds.

If you select to **Enable camera auto-cycle stream**, a second stream will be made available remotely, specifically for cycling through the cameras in the group. The group name used for this in URLs (/image, /mjpg and RTSP) and internally is the '@' symbol followed by the group name.

If **Webcast audio** is selected, audio from all visible cameras is mixed into a single audio stream. You may remove a specific camera from the group audio stream by using an option on the layout edit mode right-click menu.

By default, the remote clients exclude clips for which there is no corresponding visible camera. However, you may override this behavior by selecting **Include clips from excluded cameras**.

By default, status bits are sent to browser and phone clients to allow them to display status icons and play alert sounds. You may disable this on a per-group basis.

Auto-Cycle

There are two types of auto-cycle, either individual cameras within a group, or a cycle through the groups themselves. Do not confuse this with *PTZ preset cycle* where a camera cycles through its PTZ preset positions.

Group cycle is initiated when you start from the **All cameras** group and you enable auto-cycle in the main window, and at least one other group exists and has enabled the option to P**articipate in group cycle**. The **All cameras** group itself may or not participate. The software will cycle through each group in turn, pausing for the **Auto-Cycle delay** time.

Camera auto-cycle is initiated when you start from any group *other* than **All cameras**, *OR*, there are no groups that have enabled the option to **Participate in group cycle,** *OR*, you "long press" the auto-cycle icon with the All cameras group selected.

The option to **Favor cameras or groups which are (at least) sensing motion, triggered or alerted** will cause some cameras or groups to be skipped in the cycle if there are others where there is activity. Furthermore, there is an option to **Only cycle if there is at least one camera/group** that meets this requirement. In this case the software will display the camera group (in the case of camera auto-cycle) or the **All cameras** group (in the case of group auto-cycle) until a camera is sensing motion, triggered, or alerted as required.

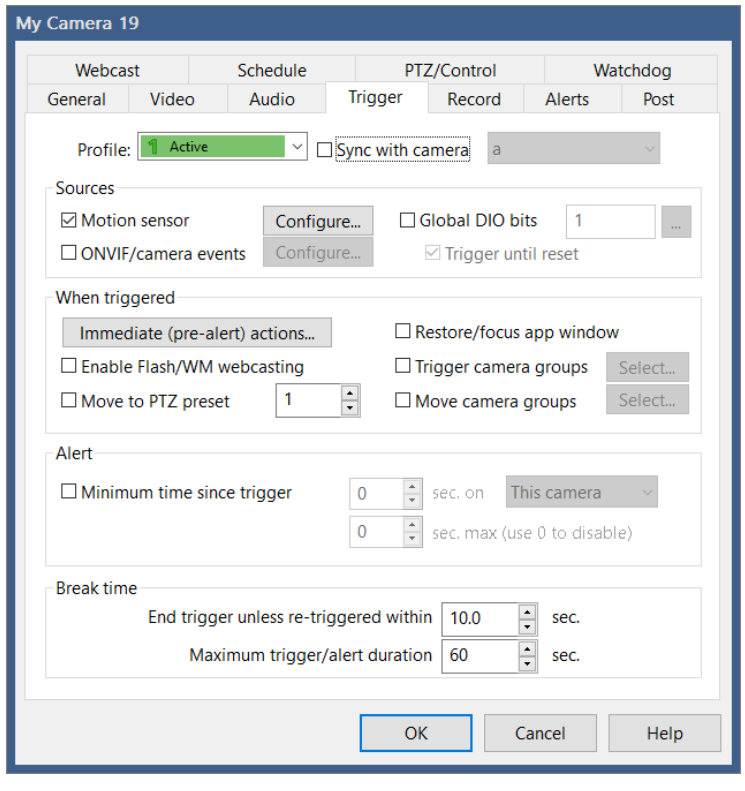
Note that in the case of camera auto-cycle, you must also select one *enabled* camera in the group to begin the cycle *unless* **Only cycle if there is at least one camera triggered** is also used.

The option to **Always switch to selected camera (manual mixing mode)** is a specialized mode which may be used to manually switch between cameras in the group rather than in a timed cycle. Think of a video studio where the producer selects the camera to be "live" based on what's happening in the scene or interview.

If auto-cycle does not begin, check to see if you may have the option to **Only cycle when Cameras window is in full-screen mode** selected on the Cameras page in Settings.

TRIGGERING AND MOTION DETECTION

When a camera is *triggered*, you will see its border painted orange and a lighting bolt icon appear in its header as well as in the main window status bar. By default, video is recorded *when triggered* and an *alert* is generated, which creates an image on the *alerts list* and fires actions such as a siren, push notifications, etc.

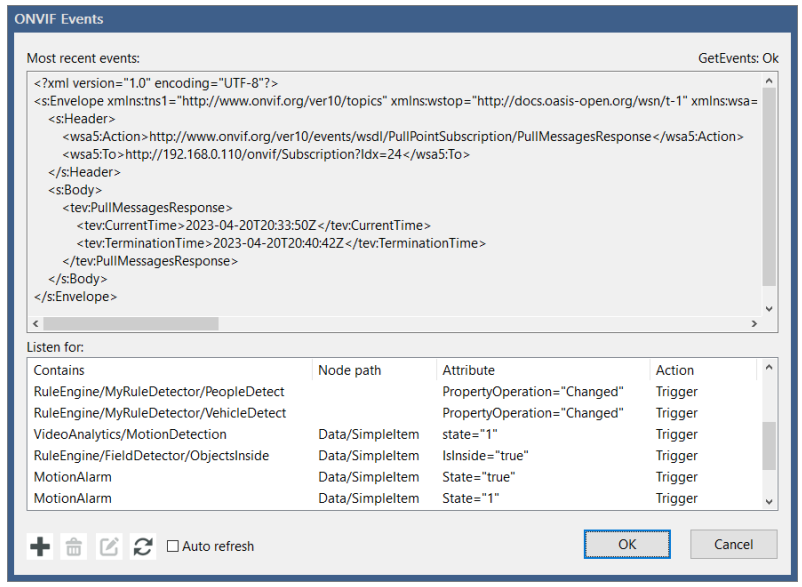


Settings on this page as well as on the Record, Alerts and Watchdog pages may change with the active profile. They may also be synchronized with another camera—please see that topic below.

Sources

The **Motion sensor** is the software's original and most commonly used trigger source. It is discussed in a topic to follow.

Some cameras (Axis is one brand) have proprietary metadata included in their RTSP or other streams which may be used as a trigger source by enabling the **ONVIF/camera events** source option (without need to use the Configure button). However the primary purpose of this option to use an ONVIF *GetEvents PullPointSubscription* to pull trigger events from the camera. For this to work, the **Find/Inspect** button must be used and **GetEvents** must be enabled on the Video/Network camera page. Use the Configure button to manage the ONVIF events that will be monitored:



The most recent XML data received from the camera will be displayed here for analysis. Here's some XML from the camera that shows two actionable messages:

```
<tev:PullMessagesResponse>
       <tev:CurrentTime>2023-04-19T19:11:01Z</tev:CurrentTime>
       <tev:TerminationTime>2023-04-19T19:19:35Z</tev:TerminationTime>
       <wsnt:NotificationMessage>
              <wsnt:Topic Dialect="http://www.onvif.org/ver10/tev/topicExpression/ConcreteSet">tns1:RuleEngine/
CellMotionDetector/Motion</wsnt:Topic>
              <wsnt:Message>
                     <tt:Message PropertyOperation="Changed" UtcTime="2023-04-19T19:11:00Z">
                            <tt:Source>
                                   <tt:SimpleItem Value="000" Name="VideoSourceConfigurationToken"/>
                                   <tt:SimpleItem Value="000" Name="VideoAnalyticsConfigurationToken"/>
                                   <tt:SimpleItem Value="000" Name="Rule"/>
                            </tt:Source>
                            <tt:Data>
                                   <tt:SimpleItem Value="true" Name="IsMotion"/>
                            </tt:Data>
                     </tt:Message>
              </wsnt:Message>
       </wsnt:NotificationMessage>
       <wsnt:NotificationMessage>
              <wsnt:Topic Dialect="http://www.onvif.org/ver10/tev/topicExpression/ConcreteSet">tns1:VideoSource/
MotionAlarm</wsnt:Topic>
              <wsnt:Message>
                     <tt:Message PropertyOperation="Changed" UtcTime="2023-04-19T19:11:00Z">
                            <tt:Source>
                                   <tt:SimpleItem Value="000" Name="Source"/>
                            </tt:Source>
                            <tt:Data>
                                   <tt:SimpleItem Value="true" Name="State"/>
                            </tt:Data>
                     </tt:Message>
              </wsnt:Message>
       </wsnt:NotificationMessage>
</tev:PullMessagesResponse>
```

The first example notification message above shows a topic of RuleEngineCellMotionDetector/Motion and the second a topic of VideoSource/MotionAlarm. Many default "**Listen for**" conditions are preloaded for you. However you may modify this list as required by your device. Each NotificationMessage that's received is checked against:

Contains text that must appear anywhere in the message

Node path a node path consisting of multiple node names separated by splashes that must exist in the message

Attribute an attribute name or a name="value" pair that must exist in the node path (or anywhere if a node path is not specified). Note: for our search purposes, the special case node "SimpleItem" which always has *separate* Name= and Value= attributes will be considered to have a *single* attribute where Name="Value" instead.

Action determines what should happen if a matching message is received. The default is simply to normally trigger the camera. However you may also specify individual actions for *setting* the trigger and *resetting* the trigger, possibly with corresponding *value="true"* and *value="false"* attributed events. Ignoring a message is also an available action, which may be useful for first excluding a class of messages before a more general class is considered.

Memo/label (optional) this will added to the alert memo in the database, and may then be used as a "required AI object" for alert actions. If left blank, a combination of the *contains* and *attribute* fields for the event are used as the alert memo.

Events with corresponding set/reset actions are considered *bistable* ONVIF triggers and these triggers only reset when the reset event occurs via ONVIF (ignoring the normal trigger break time).

While monitoring the status of what's being received from the camera in realtime, you have the option of either refreshing the most recent events either manually or automatically.

Global DIO (Digital Input/Output) input bits refers to electrical signals received either by a DIO device such as a SeaLevel box or Arduino serial port, as configure on the DIO and IoT page in Settings. The decimal number entered here actually represents the DIO input numbers in a binary format, any of which should trigger this camera:

The 1st input has a bit value of 1
The 2nd input has a bit value of 2
The 3rd input has a bit value of 4
The 4th input has a bit value of 8
The 5th input has a bit value of 16
The 6th input has a bit value of 32

…and so on in powers of 2. So if you want the 1st and 4th inputs to trigger this camera, enter a value of 9 into this box. For any of the 1st 8 inputs, enter 255. Use the "**…**" button to have this value calculated automatically.

The camera itself may have DIO terminals which may be used as a trigger source. These events may come over ONVIF *GetEvents* or via proprietary RTSP metadata etc.

Configured on the Watchdog page, the camera may be triggered when there is a loss of signal.

Configured on the Audio page, the camera may be triggered when there is sound of sufficient amplitude and duration.

It's possible that this camera is triggered in response to the trigger on another camera, and this is called a *Group* trigger. Group triggers do not propagate when cameras in the group also are configured to trigger their own groups.

The camera may be triggered by other *External* means, possibly via a menu command or an action set executed for another purpose.

When triggered

When a camera is triggered, most commonly recording may begin, an "alert image" may be captured and alert actions may be executed. These are configured on the Record and Alerts pages. However, there are other possible trigger responses:

You may choose to run **Immediate (pre-alert) actions** prior to creating or confirming the alert with artificial intelligence (AI, discussed in the Alerts section).

All cameras in one or more **camera groups** may be triggered simultaneously.

You may want to **restore/focus** the main window UI if it has been minimized. There's a related setting on the Cameras page in Settings to also move the window to the foreground if it has been moved behind other windows.

Tip: to apply the restore/focus functionality *when alerted* instead of *when triggered*, you can add a **do command** action to the "On alert" action set with /admin args of **console=restore**.

You may want to move the camera to a particular **PTZ preset position**, along with all other cameras in selected groups.

You can link **Flash or Windows Media webcasting** with a camera's triggered state. The software will push video to one of these services only when the camera is triggered. Note that this means no video will be pushed when the camera is *not* triggered.

Alert

Before generating an alert for a trigger, you may consider the **Minimum time since the last trigger** on this or a group of cameras. If multiple cameras cover a specific area for example, you may not want them all to generate alerts at the same time. The maximum setting works in the opposite way—the alert will be generated *only if* another camera or group has been recently alerted within the time you specify. It's possible to use the minimum setting without the maximum setting by setting maximum to 0.

See the section on Alerts to determine what happens next.

Break time

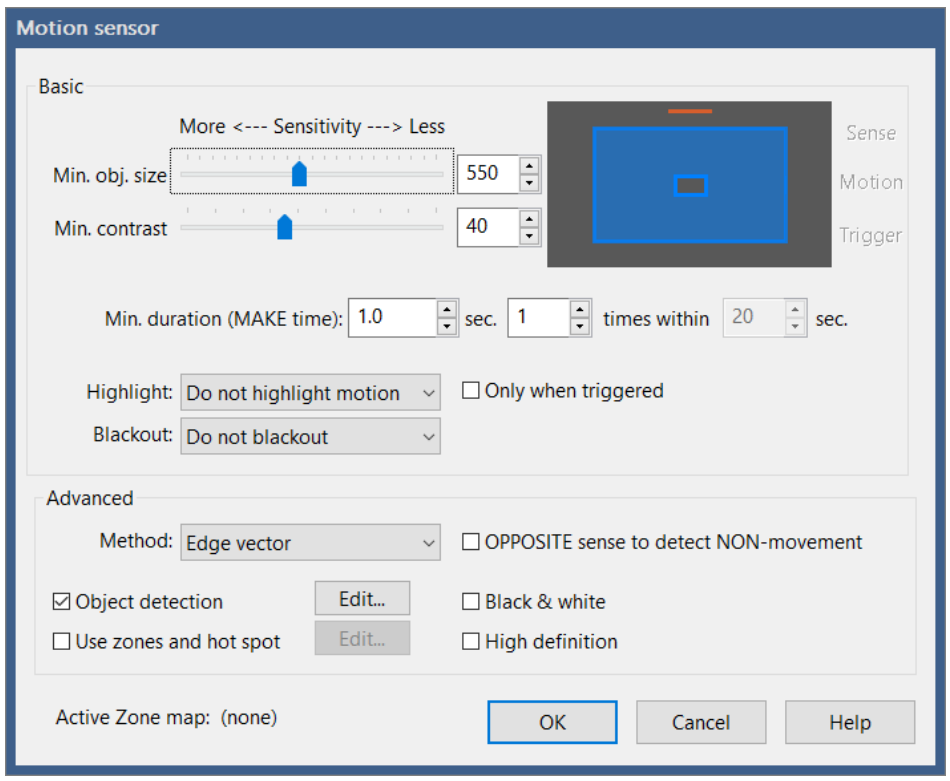
The *Break time* is simply the duration of the triggered state. If there is no additional triggering during the break time, the trigger state will expire and recording will stop (unless otherwise configured on the Record page).

If an additional trigger occurs while the camera is already triggered, this is called a *re-trigger*, and the break timer is reset. The triggered state (and associated recording etc.) always continue for this period of time beyond the most recent trigger event.

An overall maximum trigger time is configurable. You may defeat this with a value of '0'. Like the Alert page setting for *new and re-triggers*, this option provides another method to "re-alert" for continuing motion or other triggers. However it also forces the trigger to end, which may affect recording file cuts and other "on trigger" events.

THE MOTION SENSOR

The motion sensor is the most commonly used method for triggering the camera to record and to fire alerts. The software may consider overall "change" in the image from frame to frame, or it may attempt to isolate "objects" and track them for movement.



Basic

There is some persistence or hysteresis involved to reduce noise, but at its core, the motion sensor simply counts the number of changed pixels from frame to frame.

The **object size** and **contrast** may be considered *thresholds*. This is the *amount* of change that must occur to be considered motion—"contrast" for individual pixels, and "object size" for the number of overall pixels that must be changing.

By moving either slider to the left, you will make the motion detection more sensitive, as there will be lower thresholds to overcome. The software attempts to show this visually with a small box in the center of a camera preview window to represent the *minimum* object size. There may also be a larger rectangle surrounding this—this is the *maximum* object size as set under Object detection below. This image is updated in realtime—if someone were to walk through the scene, an additional rectangle is drawn to represent the amount of actual motion. If this realtime rectangle is larger than the minimum and smaller than the maximum, the camera is considered to be *sensing motion*.

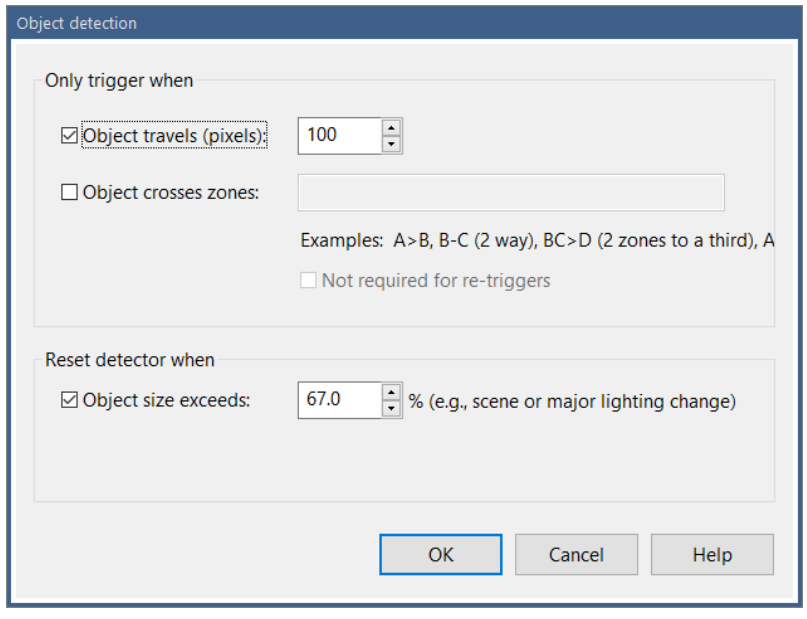
It's not until the motion sensing persists for a time specified by the **minimum duration** or "make time" that the camera is actually triggered. A make time setting of 0 seconds is possible—in this case a single frame of motion is all that it takes to trigger.

You may reduce the possibility of a false alert by requiring a number of movements of the make time duration within a specified time window. This feature allows you to ignore short-lived motion events which may be of no consequence. Generally if there's a break-in or anything else of concern, multiple triggers would occur over a short period of time.

You may select to have motion pixels and/or object rectangles drawn onto each frame of video by using the **Highlight** option. Highlighting may be limited to frames where the camera is triggered. You may also **Blackout** areas of the image which are specifically excluded from any motion zone (those are discussed below).

Object detection

The software can use an algorithm to attempt to identify rectangular groups of changing pixels and then to classify them as *objects*. When highlighting is enabled, objects are drawn with yellow boxes, orange when they reach triggering threshold.



To force a trigger, in addition to existing for a specific amount of time (the motion sensor's *make time*), an identified object also must **travel** a specific number of pixels, set here. The *center point* of the object is used for this purpose.

Zone crossing

You may require that an object also **cross specific zones** (as determined by the movement of its *center point*) in order to trigger. Zones are discussed below. They have letters A-H, where H is the special "hotspot" zone. There is a special syntax to use when specifying zone crossing:

A	Object must enter zone A
AB	Object must have entered both zones A *and* B, overlapping or not
A>B	Object must travel from zone A to zone B
A-B	Object must travel between zones A and B in either direction
AB>C	Object must have entered both zones A *and* B before traveling to zone C
ABC>D	Object must have entered zones A *and* B *and* C before traveling to zone D
A!B>*C*	Object must travel from zone A to zone C without first having been in zone B
A>*BC*	Object must travel from zone A to zone B and C *simultaneously*—which would only be possible with overlapping zones

When two zone letters are used together, this is an *and* condition. The object must have existed in both zones (not necessary simultaneously) *before* possibly moving to a third.

When any zone letter is preceded by an exclamation point (!), that zone must *not* have been entered.

Or conditions may be specified by adding multiple zone crossing rules separated by commas.

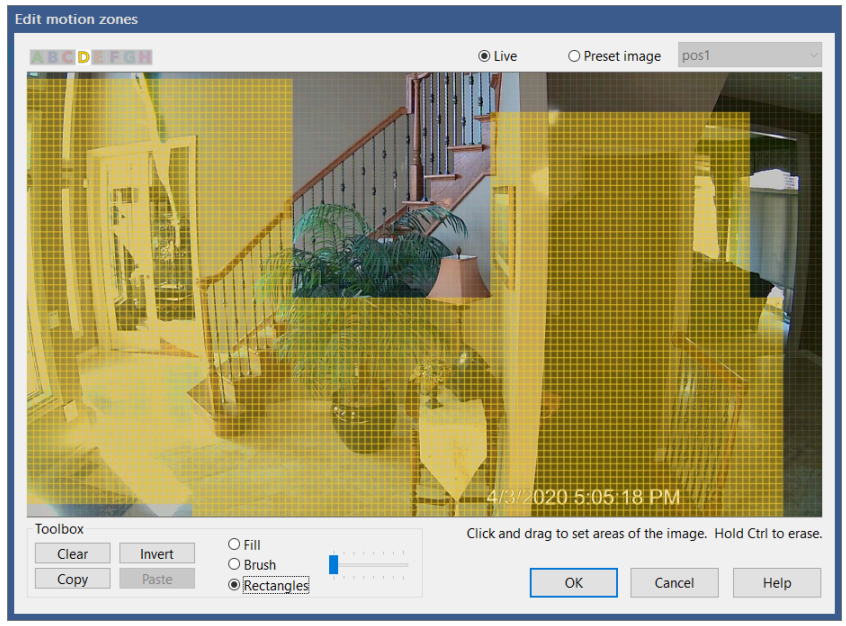
Select **Not required for re-triggers** to bypass this filter for re-triggers (triggering while the camera is already in a triggered state). This will make it easier to maintain a triggered state once this condition is initially met.

A maximum object size may be specified to **reset** the motion sensor. This object size is represented as the larger blue rectangle on the image preview back on the motion sensor page. This is useful to filter out very large changes possibly due to lighting or camera movement (a *scene change*).

Zones and hotspot

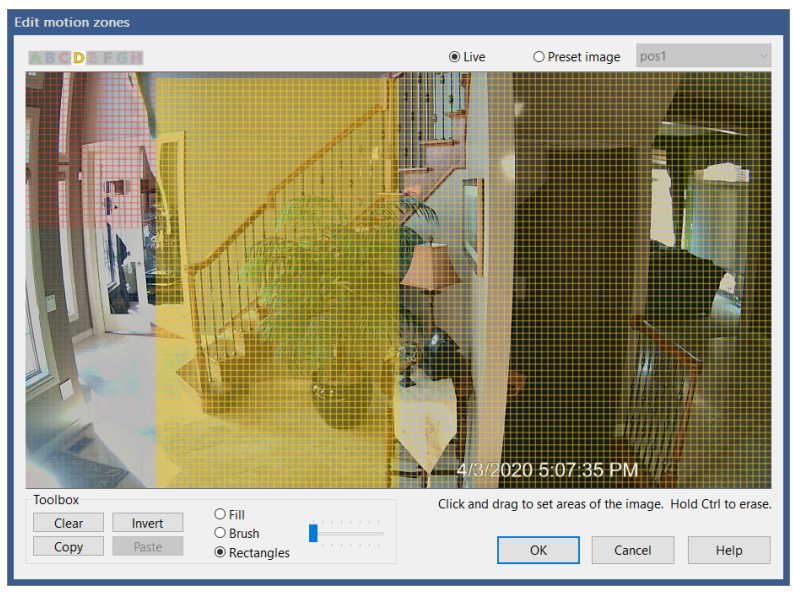
Zones allow you to identify parts of the image for consideration by object detection. They are also noted with an alert image in the clips list so that you may know more specifically the source of motion.

In an opposite sense, any part of the image not covered by a zone is essentially *masked*—that is, not considered for motion at all.



By default, the entire image is Zone A. If your intention is to simply mask out parts of the image, you may remove elements of the image from Zone A by holding the Control key and drawing rectangles. You may instead **Invert** or **Clear** the image and then re-draw areas to be monitored.

Each zone is displayed and manipulated in turn as it is selected at the top of the window. Areas which are part of other zones are shown with hatch marks for your convenience. Here's an example where Zone B is being drawn. Zone D is shown with hatch marking in yellow. Zone H (the Hotspot zone) is sown with magenta hatch marking:



Zones may or may not overlap. This does not affect use for masking, but it may affect the way that object detection functions. An object is considered to have been in or traveled to a zone if the *center point* of that object touches the zone.

Of important note, a motion detection *object* as used by object detection and tracking *must always exist in one or more zones*. This means there must be continuous zone coverage through areas where an object is being tracked. Instead of worrying about zones overlapping or abutting, it is much easier to just setup one zone to be used as an overall "mask" and then draw additional zones to be used with object detection and tracking. For example, if zone A is left as representing the entire image, you may then draw smaller zones B and C anywhere on the image, and then apply an object tracking rule $B>C$ without consideration of how those zones are aligned or spaced.

As it is possible to define multiple zone maps, perhaps for different active profiles or for recently used PTZ presets, and it's possible to invalidate the zone map using PTZ movements, the currently active zone map is identified for your information on the bottom of the motion sensor page.

The **Copy** and **Paste** buttons exist to give you the ability to take the zone map for one camera or one profile and apply it to another. The target camera and profile must have the same resolution and setting for the "high definition" box on the motion sensor page.

The Hotspot zone

This is a zone for special applications only and should not be generally used. Objects or motion in this zone will *override* the make time and other rules and force an immediate trigger. This can result in a huge number of false triggers, so it should be used with caution.

Opposite sense

A very interesting feature, this reverses the function of the motion detector, so that it may be used to identify *the absence* of motion. You may be interested in the (lack of) movement of a child or an elder for example.

When using this feature, you will want to set the minimum duration or *make time* of the motion sensor to a much higher value than the default of 1 second. If you specify 60 seconds for example, the camera will be triggered for recording and alerts if there is *no* motion in any 60 second period of time.

More advanced motion sensor options

A number of additional settings may be used to fine-tune or further enhance motion sensor accuracy.

The **Black and white** and **Cancel shadows** options alter contrast calculations. **Black and white** attempts to simply remove the effect of color differences. In order to cancel shadows, higher contrast may be required between neighboring pixels.

By default, to save CPU and smooth-out noise, the image is *reduced* by considering it in *blocks*. The **High definition** option actually increases the number of motion detection blocks that are used by typically 4x.

You may select to use either a *Simple, Gaussian,* or *Edge Vector* **Algorithm**. The Gaussian algorithm uses slightly more complex heuristics for tracking pixel changes over time, possibly helping to reduce false positives, but at a slight increase in CPU demand.

The *simple* algorithm emulates Blue Iris version 4, but the newer and somewhat more sophisticated *edge vector* algorithm is now the default for version 5. This new algorithm distinguishes between the leading and trailing edges of motion and you will see this if you enable a highlighting option either in camera settings or in the viewer for testing. The leading edge is painted a bright shade of blue, while the trailing edge appears in orange. The remainder of the movement is a darker blue as was used in the *simple* algorithm.

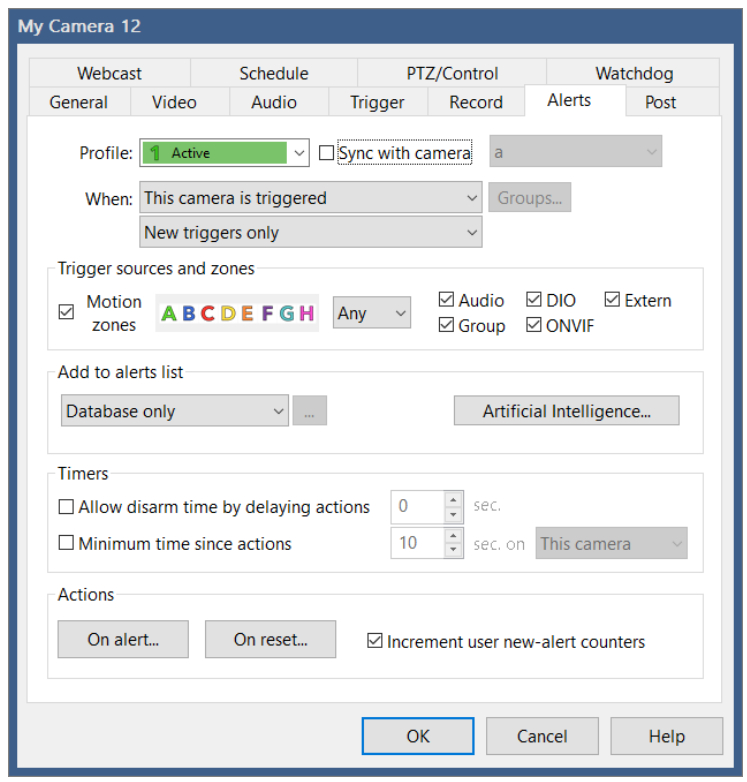
The algorithm uses the leading and trailing edges to compute a *vector*, which consists of a magnitude and angle for the motion of the object. A trigger will only occur if this vector is consistent for the duration of the *make time*.

The goal here is to reduce false positives and to provide more meaningful input to more advanced AI.

The **Active Zone Map** display exists primarily for troubleshooting (for example, “why did the camera trigger when that part of the image is not covered by any motion zone?”). It’s possible that the zone map will change based on profile, PTZ movement, or PTZ preset calls. Each profile and each PTZ preset position may have its own zone map, and it’s possible to “cancel” use of the zone map when PTZ commands are used. “\Motion” indicates profile 1, “\Motion\1” is actually profile 2, “\Motion\2” is profile 3 and so on. “\PTZ\Presets\1”, 2 etc., do correspond to the actual preset numbers.

ALERTS

OK, the camera has been triggered, but what happens next? In addition to recording, you may generate an alert image, use AI to confirm the alert and then fire any number of actions.



Settings on this page as well as on the Record, Trigger and Watchdog pages may change with the active profile. They may also be synchronized with another camera—please see that topic below.

When to alert

By default, the actions defined for this alert are only fired when this camera is triggered. However, you may want one camera to represent all cameras in specific groups, or all cameras on the system in this regard.

By default, an alert may occur only at the *leading-edge* of the camera's trigger state (a *new* trigger). If the camera is *triggered again* while it is *already in a triggered state,* this is called a *re-trigger*. If you enable the option to alert for re-triggers as well, this will result in more alerts overall.

The option is given to only re-trigger if motion moves into new zones or additional trigger sources are added. In this case you may choose to handle the new zones/sources *additively* (taking into account previous sources) or *exclusively* (considering only the new sources).

Trigger sources and zones

The alert may be filtered to only occur with *specific types of triggers*. And furthermore for a motion sensor trigger, you may require that *specific zones* where entered (as determined by the *center point* of an object) in conjunction with the object detection and tracking feature. When not using object detection tracking, *any* individual pixel change within the specified zones (still dependent upon the Any/All/= selection) will qualify to fire the alert.

The Any/All/= selection determines how the zone filter is interpreted. Here are some examples of this if you check only the boxes for zones B and C, and whether alerts will fire or not:

Alert zones	Triggered zone/s	Any	All	=
BC	A	No	No	No
BC	B (or AB)	Yes	No	No
BC	ABC	Yes	Yes	No
BC	BC	Yes	Yes	Yes

Add to alerts list

An alert image is a special kind of database entry. It is taken at the leading edge of a trigger and acts as "bookmark" into a video file to mark the position of an event. The clips list has a filter to show just the alert images, and these are managed as dependents of the actual video file to which they refer—that is when the video is deleted, so too are its alert images (unless they have their own files, discussed below). As there may be many more alert images than video files, they have their own schedule for automatic deletion on the Clips page in Settings.

It's possible to ask the software to create either **full-resolution** JPEG files or exported MP4 video files for alerts along with the "postage stamp" images in the database. When this option is used, these new files will live in the *Alerts* folder by default—they *do not replace the actual clips* recorded to other folders. Furthermore, they will not be automatically deleted when the associated clip is deleted—instead, these files become subject to the age and folder size settings for the Alerts folder specified on the Settings/Storage page. With a further option **Export when flagged** a JPEG is always created initially, but the creation of the exported MP4 file only occurs after the alert is *flagged*—this option is on the right-click menu (or long-press with a finger in the phone app). IMPORTANT NOTE: you must be recording to the default BVR file format in order to export to MP4.

Timers

Timers exist to both reduce the number of false-positive alerts as well as to reduce the overall alert frequency.

The **Allow disarm time by delaying actions** setting basically gives you time to manually cancel the alert, perhaps as you enter the home or building where the camera would normally be triggered. This occurs *after* the camera is triggered, starts to record, an alert image is generated and AI confirms the alert.

The **Minimum time between actions** is used simply to reduce the number of consecutive actions. Following a confirmed alert, you may not be interested in receiving emails or push notifications in quick succession as motion and triggering continue.



When a camera moves from the Triggered state to the Alerted state, the lightning bolt icon is replaced with a bell icon. This icon remains (in a semitransparent state) until either you click on the camera window or review one of its recordings.

Actions

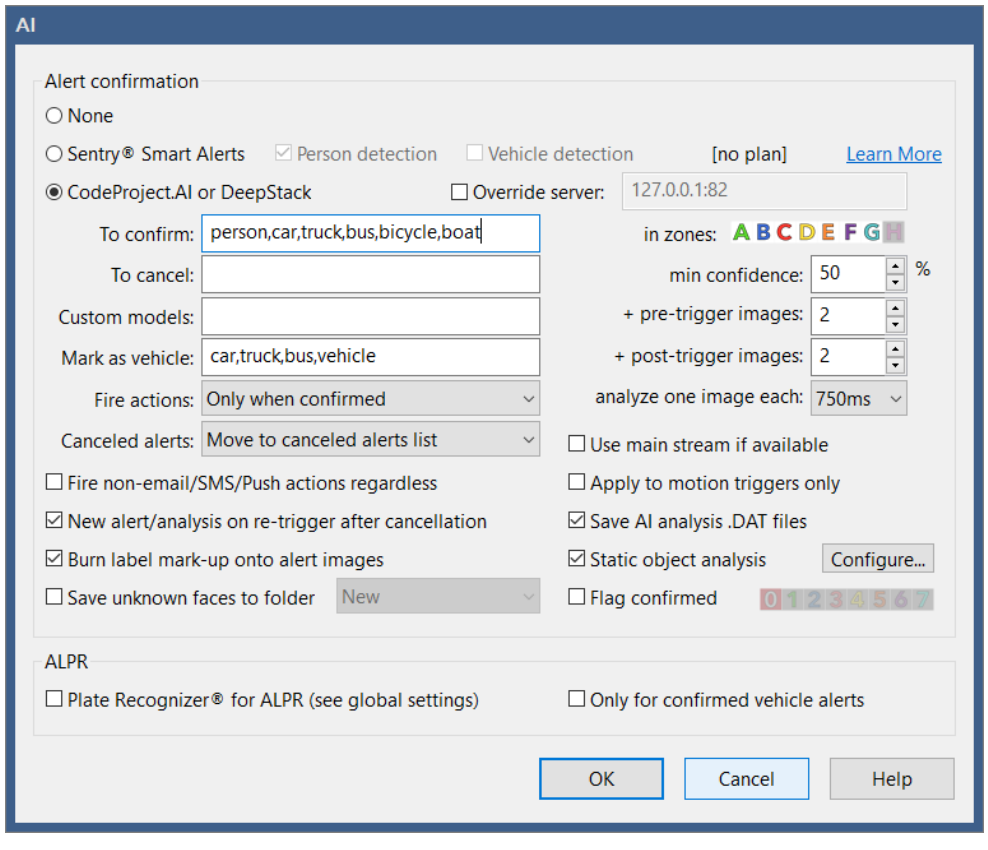
An action set may be defined for both *"On alert*" and *"On reset." On alert* actions only fire when the camera is triggered and all conditions defined on this page are satisfied. *On reset* actions only fire when the camera returns to a non-triggered and all *on alert* actions have finished.

Please see the Alerts and Actions chapter for details on possible alert actions.

The software typically maintains a counter of new alerts on a per-user, per-camera basis. This is used primarily by the phone apps to display "badge" numbers on the app icon and cameras list. If you deselect *Increment user new-alert counters*, this will not occur for this camera.

ARTIFICIAL INTELLIGENCE

Artificial intelligence may be used to make the motion detector “smarter” in order to reduce the incidence of false alerts.



Alert confirmation

It’s possible to have an alert image first analyzed by an external service prior to executing any alert actions. Blue Iris partnered with *Sentry Smart Alerts* for “person detection” as an initial AI provider. With this technology, the alert image is sent to their server for analysis. Only if it is determined to contain a person and/or vehicle, alerts are fired; if not, the trigger and its alert actions are considered *canceled* and alert images are marked accordingly in the clips and timeline views. Click the *learn more* link for more information.

AI using either the **CodeProject.AI Server (now preferred)** or DeepStack is another exciting (and no charge) option for object classification. You must first install and configure AI—see the AI page in global Settings. For advanced users, you may split the AI processing among multiple AI servers by specifying another server here.

You may select AI *labels* that correspond to objects which you would like **to confirm** an alert. The field is pre-populated with the most common; see AI documentation for additional possibilities. AI ranks its detection confidence as a percentage, and you may select here the **min. confidence %** from 1-100 in order to confirm an alert.

Labels may also be used to specifically *cancel* alerts. For an alert to proceed, labels (corresponding to detected objects and faces) must appear in the **to confirm** box (or that

box may be empty), but must *not* appear in the **to cancel** box. For example, although you may specify *person* in the **to confirm** box, a specific *face name* in the **to cancel** box will cancel the alert.

You may override the default confidence % for any label by appending a : and a number to the label, for example *person:80*. Require that an object first appear in a specific zone or zones by adding those following the optional confidence number, for example *person:AB* for zones A or B, or *person:80AB* for zones A or B with a confidence of at least 80%.

A wildcard character * may be added to the end of any label—this is especially handy if you have taught the AI multiple faces for a single person (for example chris* to match defined faces for chris_1, chris_2, chris_side, etc.).

You may combine two labels with "and" logic by using a +, for example, car+licenseplate. In this case, the confidence may only be overridden for the combination, such as car+licenseplate:80.

By default, one pre-trigger image, the **alert image** (trigger-leading) and 2 additional images following the trigger are considered for object detection. However, you may instruct the software to check additional pre-trigger and real-time images at a 50, 100, 200, 250, 500, or 750 millisecond, or a 1-5 second interval by specifying more **Additional pre-trigger or post-trigger images to analyze** (up to 999, or until the camera trigger ends).

An attempt is made to choose the image with the best confidence and highest number of confirmed or canceled objects when deciding whether to confirm or cancel the alert. Additional preference is given to images with more faces and/or more license plate characters. If you have selected a large number of post-trigger images, processing may be terminated early if object confidence declines.

By default, analysis will **Use the main stream if available**. If you are using dual-streams from the camera, this provides more information for the AI with which to work. However, you might consider using the *sub stream* for analysis instead by unchecking this box if you need to lower CPU demand or if the two streams are significantly out of synchronization.

You may select to not **Begin analysis with motion-leading image** by un-checking this option. This may be required in an LPR (license plate recognition) environment where the motion-leading image may be always only a small part of the vehicle as it enters the frame.

By default, all **Custom model** files are considered, although you may select a subset here by specifying one or more (comma delimited; omit the file extensions). Custom models are

enabled on the global Settings AI page. This list can be either an *inclusion* list or an *exclusion* list That is, if *any* model is given the :0 designation, then all models are used *except* those marked :0; however if there are no :0 entries, then *only* the models listed will be used. You may also add *faces:0* or *objects:0* or *alpr:0* here to specifically skip face, default object, or license plate detections respectively, but note that this then makes the list an *exclusion* list for the purpose of custom models. Tip: specify a single non-existent model name ("none") and **no** custom models will be used.

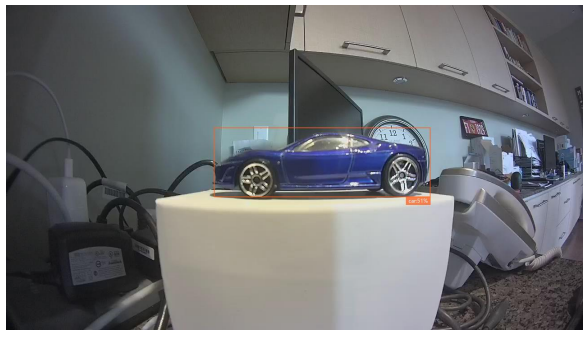
By default, alert confirmation is used to cancel alerts. Normally alerts are also canceled if there's a problem communicating with the AI. Use the **Fire actions** selection to change this behavior. You may also select to only **Fire non-Email/SMS/Push actions regardless** in the event of alert cancellation.

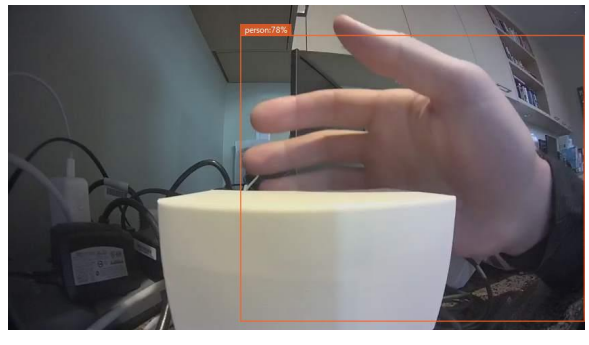
By default, the option for **New alert/analysis on re-trigger after cancellation** is enabled. If an alert is canceled, yet the trigger and motion continue, you may want to automatically create additional alerts to analysis continuing motion. Otherwise, a new alert can not be analyzed until the current trigger ends.

Select to **Save AI analysis details** if you would like to later review AI performance for testing and tuning. Please see below for discussion on the AI status page. AI analysis detail are saved as .DAT files in the Alerts folder. By default, Alerts are only database entries and occupy no space in the Alerts folder, however please be aware that these .DAT files will contribute to the Alerts folder size calculation and may cause Alerts to be deleted once this folder reaches its defined capacity (default is only 1GB).

If you select to **Auto-flag confirmed alerts**, these alerts will also be added to the Flagged database view. You will be able to use the flag icon at the top of the clips list or in the iOS or Android app to quickly get a list of only AI confirmed alerts.

Select **Burn label mark-up onto alert images** to replace the alert image with one where the detected objects have been outlined and labeled. The new marked-up JPEG is also saved to the Alerts folder if you have selected to store alerts as **High-res JPEG files**.



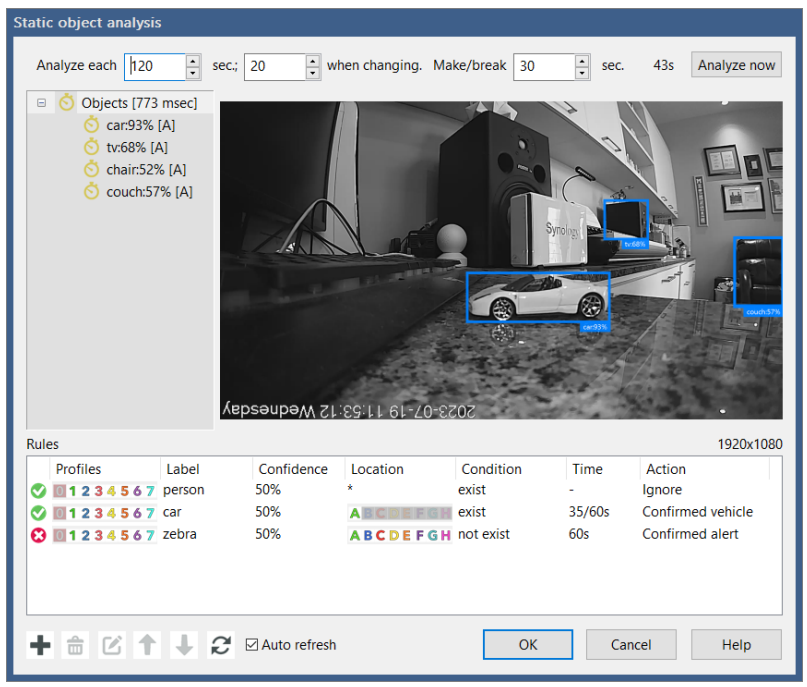


Hide canceled alerts

By default, when AI cancels an alert, its image is also removed from the default Alerts list and from the timeline both locally and on the phone apps. You may still view these alert images by selecting the *canceled alerts* view in the clips list. For a trim database, bypass the canceled alerts list altogether by using the option to immediately **delete** canceled alerts.

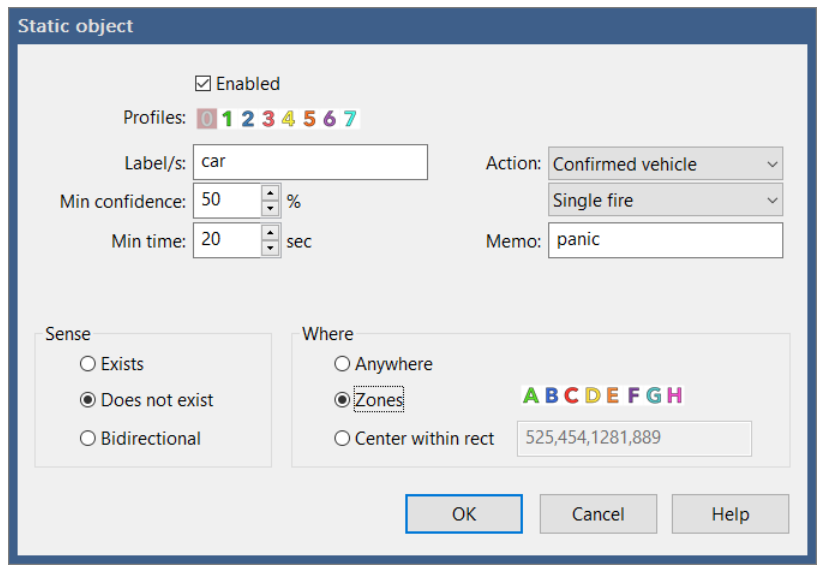
Static object analysis

The software may also be configured to attempt to cancel alerts if detected objects are determined to be in an *occupied* state. That is, they have not moved for a predetermined amount of time.



By default, the scene is analyzed each 120 seconds, but more frequently (each 20 seconds) if the scene has changed (objects have appeared, moved, or disappeared). An object must be present or missing for a number of seconds (the **make/break** time) before being considered either static or removed from the static object array.

You may define **rules** to be applied to the static object array.



Specify one or more object **labels** (comma delimited) and a minimum object **confidence**.

Choose the **Regard as NOT static** action to prevent specified objects from ever being considered static.

You may also choose to **trigger** the camera or immediately **alert** in a number of different ways when the rule is satisfied. Use the options for "trigger set" and "trigger reset" carefully, as they override the normal trigger *break time,* so they must be matched.

For trigger and alert actions, you may choose the minimum time for the object/s to either **exist (become abandoned) or not exist (become missing)** before the action is fired. The **bidirectional** sense may be used to detect objects as they both appear *and* disappear.

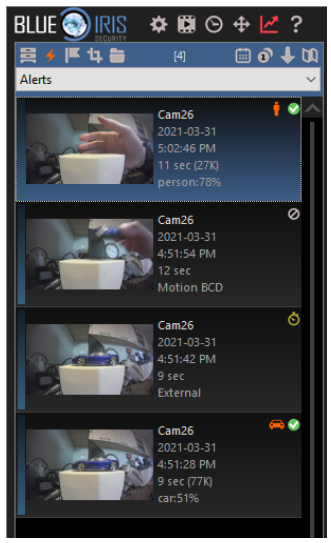
Bidirectional rules are **single fire** as an object appears or disappears. For the exist/not exist senses, you may instead choose **repetitive** firing of the trigger or alert.

An option **memo** may be specified to use for the trigger or alert. If left blank, the memo will be comprised of the object with its detected confidence (eg., car:82%), or the label with "no" prepended (eg., no car) for missing objects.

You may choose to apply the rule anywhere in the image, in specific zones, or within a specific rectangle. If you add a new rule while an object is selected, it's label name and rectangle will be automatically set for you. You may also first *draw* a rectangle on the image and this will be used for the rule.

AI shown in the Alerts list

Shown here from bottom-up are a *confirmed vehicle* alert, an *occupied* alert, a *canceled* alert, and a *confirmed person* alert.



Motion sensor notes

The image used for analysis may be *masked* to remove areas of the image from consideration. Areas of the frame (*zones*) are defined via the **Use zones and hotspot** feature on the Trigger/Motion sensor page. Any part of the image not covered by *at least one zone* is considered *masked*. Zones may also be excluded using the checkboxes on the Trigger/AI page.

By default, triggers due to motion in the hotspot zone (H) will bypass AI confirmation and alerts will proceed immediately. However, if zone H is selected here, AI confirmation *will* be applied to these triggers as well.

You may also benefit form configuring the motion sensor to use more sensitive settings so that more events will be evaluated by the AI. This is done by lowering the object size and contrast, as well as possibly reverting to the “simple” detection algorithm.

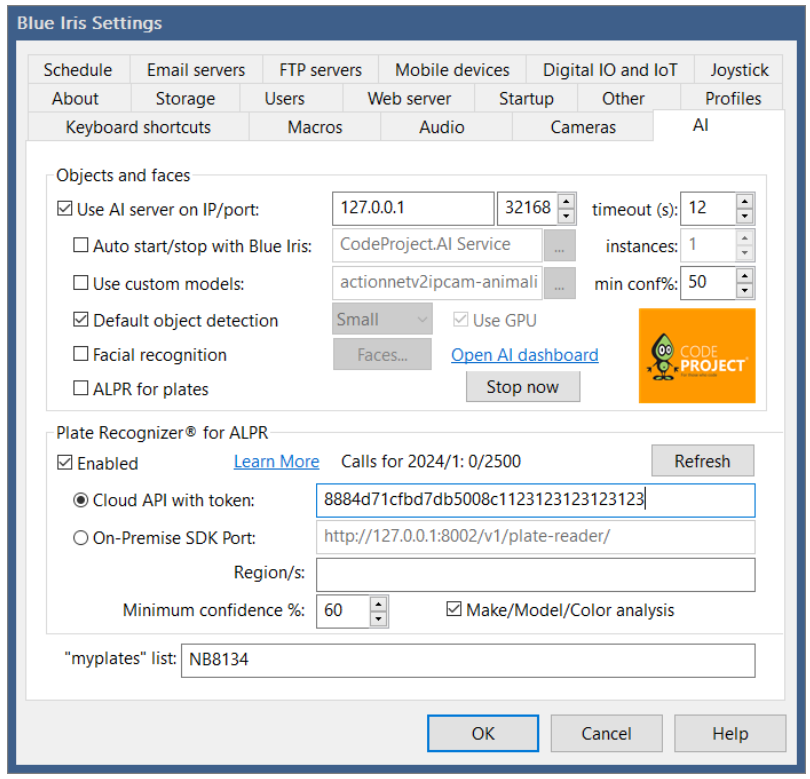
ALPR

ALPR (automatic license plate recognition) is a built-in feature with newer CodeProject.AI builds. See the AI tab in global Settings for the configuration of either CodeProject.AI or Plate Recognizer for ALPR.

When using dual-streaming, insure that your pre-trigger buffer is at least as large as the time between key frames in the main stream in order to send hi-resolution images to Plate Recognizer. If your key frame rate is 0.5, this means at least 2.0 seconds of pre-trigger time so that the buffer will contain at least one key frame.

A successful plate number reading will appear on the alert image entry in the database as well as in the Status Log. The software will attempt to *apply* the license plate tag to a vehicle object if one was identified by the AI and there is sufficient overlap between the two.

GLOBAL AI SETTINGS



Objects and Faces

CodeProject.AI Server and DeepStack are exciting open-source technologies for recognizing objects, scenes and faces. To make use of this integration with Blue Iris, you must first install CodeProject.AI Server from:

https://www.codeproject.com/AI/index.aspx

Although now deprecated, you may still find the old DeepStack at:

https://docs.deepstack.cc/windows/

With DeepStack, you may choose between the standard CPU version, or you may experiment with versions designed for your specific GPU. It's recommended that you stick with the default installation folder. You don't need to bother with additional instructions on these websites, as Blue Iris will handle running the AI for you automatically and will do model and mode selection for you automatically as well. The port number specified must not be the same as your Blue Iris port and must not be in-use by any other system software.

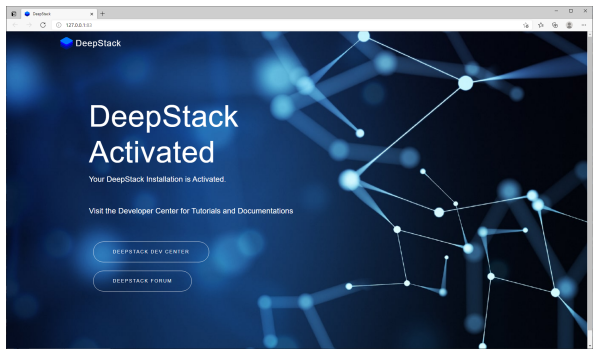
Unless you are hosting another PC running AI, you should allow Blue Iris to start and stop the AI automatically for you. With DeepStack, you may select the number of sequential-port instances to create—if you select port 5000 and 3 instances, 3 DeepStack servers will be created on ports 5000, 5001 and 5002. Use the **override server** option on the Trigger/AI page in order to specify a server port per camera.

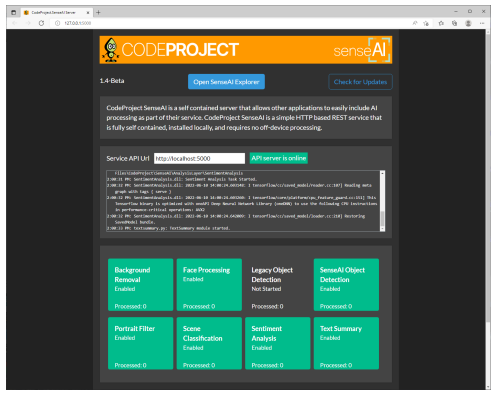
The **timeout** (seconds) setting determines how long the software will wait for a response from the AI once a request for analysis has been sent.

The **min. conf %** (1-100%) setting will be sent to the AI as part of the analysis request. It may use this value to determine which objects to omit from its response. The Alert/AI page for each camera has its own minimum confidence setting which is used to determine which detected objects will be considered for alert confirmation or cancelation.

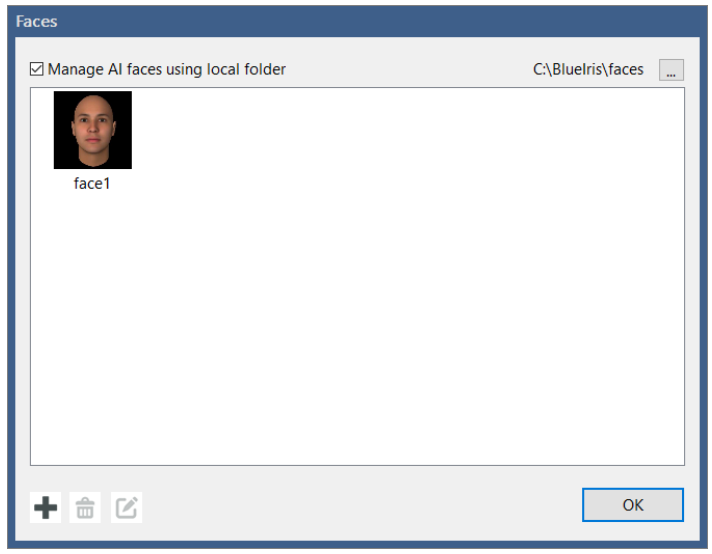
The **mode** setting (Tiny, Small, Medium, or Large) refers to the computational complexity that will be applied—this equates to more CPU utilization and time, with possibly better accuracy. For example, it might take the AI 500ms when set to **Medium** to analyze an image for both faces and objects, but could be 2000ms or more when set to **Large**.

If the AI is running properly, the Open dashboard button will show a page similar to one of these in your browser:





Enable Facial recognition to analyze alert images for faces and match them to names that you specify.



By default, JPEG files for faces are stored in a folder *Faces* in your Blue Iris program files folder. By default they are named face1, face2, etc., but you may assign your own names by clicking on a label or using the **Edit** button. With CodeProject.AI, you may instead choose to manage faces directly through their supplied interface.

Names should not conflict with the standard object names used by the AI (person, car, dog, etc.). The label *unknown* may be used to refer to a face without a match.

You may select to automatically crop out unknown faces and save them to a specific folder for later analysis or import into the AI for recognition.

You may download additional custom object model *.pt* files, or you may train the AI yourself to create these files. Please consult the specific AI documentation for instructions. You must tell Blue Iris where to find these *.pt* files. Please do not place your custom files into the existing AI *sharedfiles* folder.

If you install the Automatic License Plate Recognition (**ALPR**) module via the CodeProject.AI dashboard, then enable ALPR for plates here, the software will attempt to locate and match license plates to vehicle objects. Plate numbers may also be used as objects for alert cancelation and confirmation

Plate Recognizer© for ALPR

You may send alert images to Plate Recognizer© in order to read license plate information and to have this added to the database alerts list. This is currently offered as an add-on **Cloud API** service although an **On-premises SDK** may be offered in the future. Use the **Learn More** link to connect with Plate Recognizer and obtain your token.

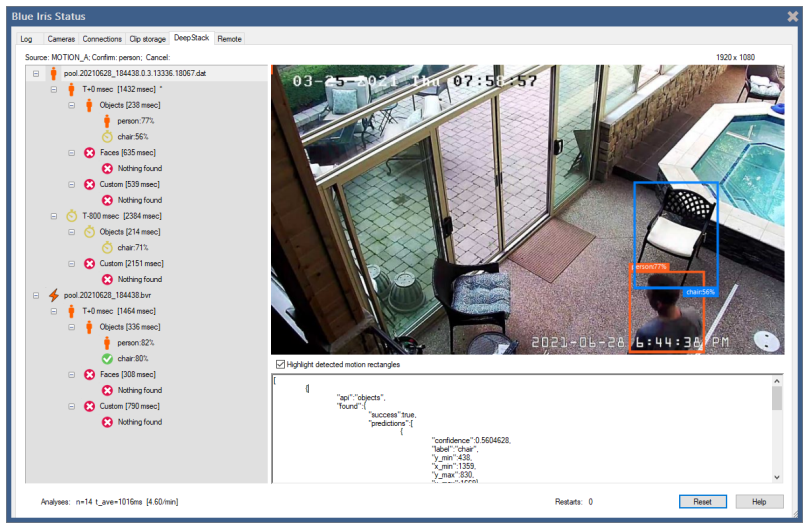
https://platerecognizer.com/blueiris?utm_source=blueiris&utm_medium=appv5

Use the **Regions** box to specify one or more (comma separated) country codes for optimal plate recognition. Users in the USA and Australia may further specify a state or province. Examples: gb, it, us, us-ny, etc.

Specify **myplates** (comma delimited) in order to use the **myplates** and **notmyplates** values in the **skipped** and **required** boxes for individual alert actions.

AI STATUS WINDOW

Open this status window to inspect AI performance and results for testing and tuning.



While this window is open, then an alert is opened where **Save AI analysis details** was enabled, the alert confirmation details will be loaded. In this example you will see that there were three images ran through AI at T-800, and T+0 milliseconds relative to the trigger time. AI processing time appears as [1432 msec]. An asterisk (*) marks the image that was ultimately used to confirm or cancel the alert.

Objects are grouped according to the AI model that was used for their detection—one of Objects, Faces, or Custom.

A red X shows an object that was either insignificant or below the confidence threshold.

A stopwatch icon is used to show objects that have been determined to not have moved or are “static” in the scene.

The raw JSON returned from AI is also displayed for expert users.

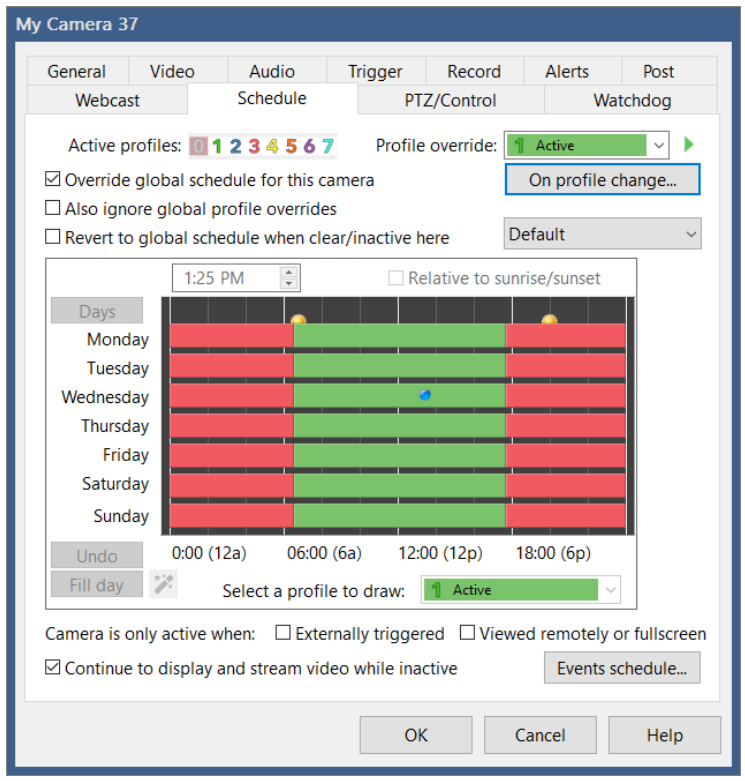
Select to **Highlight detected motion rectangles** in order to see the areas in which Blue Iris is attempting to match AI objects. The motion icon is used to show objects that were rejected because they did not overlap areas where motion was detected.

When this window is open while **Testing & Tuning AI** is enabled in the clip viewer window, results here will be updated as you play or seek through the video.

To reset the content displayed here, either close the status window completely or use the **Reset** button. The **Reset** button also resets tracked AI statistics such as the number of analyses performed, the average time required per analysis, as well as the per-minute analysis rate.

You may select during which active global profiles the camera is itself **Active**. Whether or not the camera is active will further be determined by the Schedule page here in camera settings. *Inactive* cameras do nothing but display live video, unless that too is disabled on this page.

The global schedule has already been covered in the Shield, Profiles and Schedules chapter. However, although not generally recommended as it makes keeping straight the active profile more difficult, it's possible to override the global schedule on a per-camera basis:



By default, an override of the global profile (whenever the green "play" icon at the top of the main window UI is replaced with a stop or pause icon) will also override this camera's scheduled profile. You may override this behavior with the setting A**lso ignore manual global profiles overrides**.

By default, when this camera's schedule shows inactive (profile 0, clear), the camera is inactive. However, you may select to **Revert to global schedule when clear/inactive here** so that the effective camera profile becomes the active *global* profile whenever it would otherwise be Inactive based on this camera-specific schedule.

To really complicate things, it's also possible to override the global *and* camera schedules temporarily or indefinitely by selecting a **profile override** on this page or via the phone apps.

Regardless of how the camera's active profile changes, it will be logged if it does not match the global profile, and an action set may be configured with the **On profile change** button.

Whenever the camera's active profile differs from the globally active profile, that number is shown at the top-left of the camera's header in the live video window.

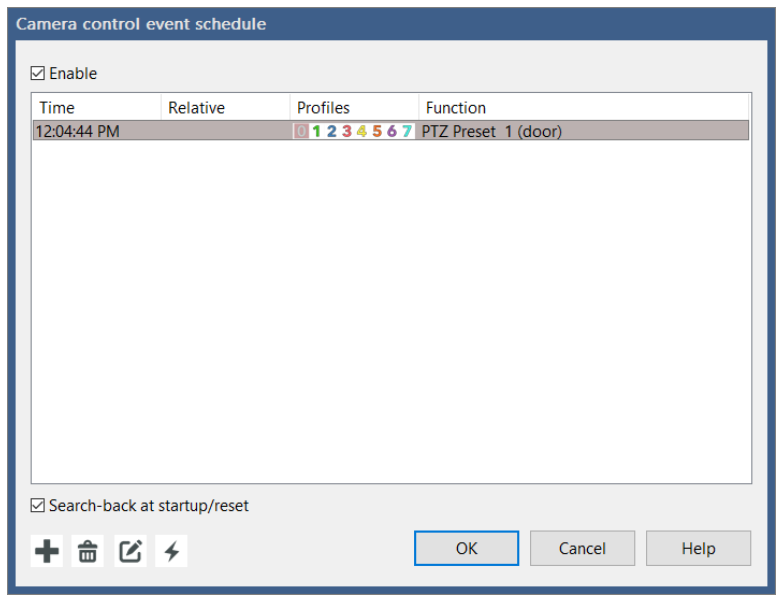
There are options here to force the camera into the inactive state (profile 0) unless the camera is currently **externally triggered,** being **viewed remotely,** or is in **full-screen** display.

By default, the camera continues to **display and stream live video when inactive**. However if you'd rather break the stream and see a gray window with an *Inactive* message, this is an option by unchecking this box.

If you place a file *inactive.jpg* in the Blue Iris program folder under subfolders *cameras* and the then the camera short name, this will be displayed when the camera is inactive and not displaying video.

Events

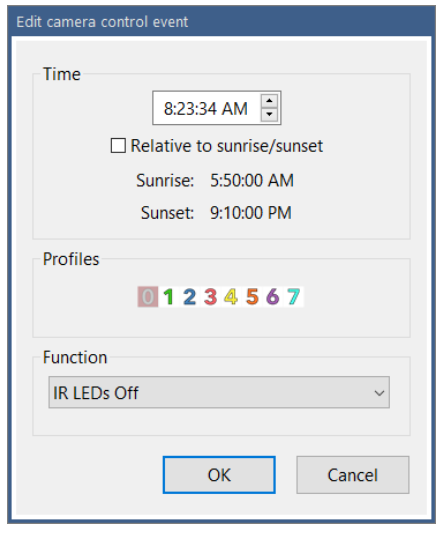
Somewhat hidden on the Schedule page is the option to set a timed events list for the camera.



Events are executed at the specified times throughout the day. By selecting the **Search-back at startup/reset** option, the software will send the most recent event of each type when the software is first started or the camera is reset. That is, if you have a PTZ preset position 0 at 12 noon, and a PTZ preset position 1 at 12 midnight, and the software is started at 3pm, the PTZ preset position 0 command will be sent to the camera.

Event search-back also applies when using the option on the PTZ page to **resume cycle/ schedule** after a period of time. This allows you to use manual PTZ control, yet return to a normally scheduled PTZ preset position after a period of time without manual PTZ control.

When adding or editing an event you have these options:

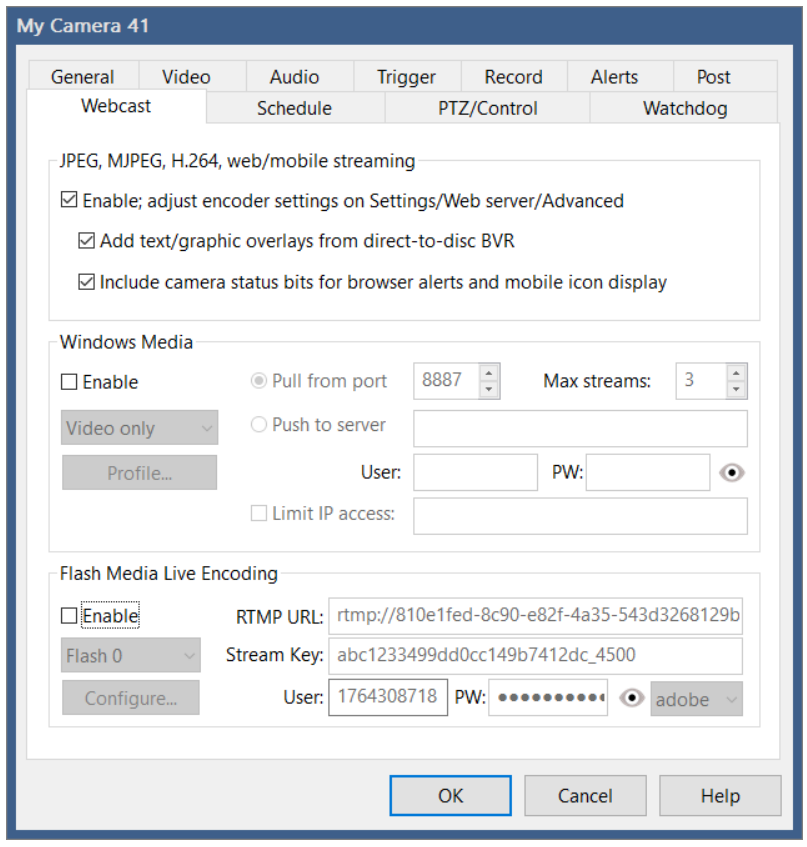


If the time is set with proximity to either sunrise or sunset, you may instruct the software to maintain this offset and move the event accordingly as the seasons change. Sunrise and sunset are only accurate if you have set your latitude and longitude on the Schedule page in global Settings.

Each event may be set to fire only when specific profiles are active.

Use the lighting bolt icon to **Test** (execute) the selected action.

If you want this camera to be visible for remote clients, browsers and apps, leave this **Enabled**.



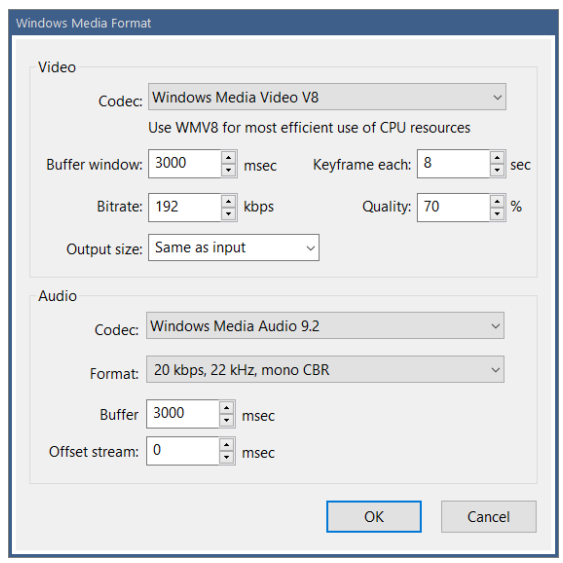
Note that if disabled here for camera-specific webcasting, the camera *may still appear remotely* if it's included in one or more groups for which webcasting is enabled.

Direct-to-disk recording (by definition) does not include video overlays from Blue Iris such as the date and time. However, you may select here to automatically draw these items to captured video frames as they are served to remote clients.

By default, status bits are sent to browser and phone clients to allow them to display status icons and play alert sounds. You may disable this on a per-group basis.

Windows Media

Although largely deprecated at this point(even by Microsoft), it is still possible for the software to push a video stream to a Windows Media Server or to serve a Windows Media stream on a specific port (users "pull" from this port). Options exist here to select the maximum number of viewers for *pull* or to specify the username and password for a *push* server. Windows Media encoding options are possible:



Flash Media Live Encoding

The RTMP protocol may be used to *push* video to a Flash Media server. There are many popular services for this such as *YouTube* and *Ustream* (a paid service), or you may have your own server located on premises or elsewhere.

If you are hosting a video stream with a number of viewers, it will be more efficient (and maybe only possible) to serve the video in this way, rather than having a large number of clients attempting to connect to your Blue Iris server directly.

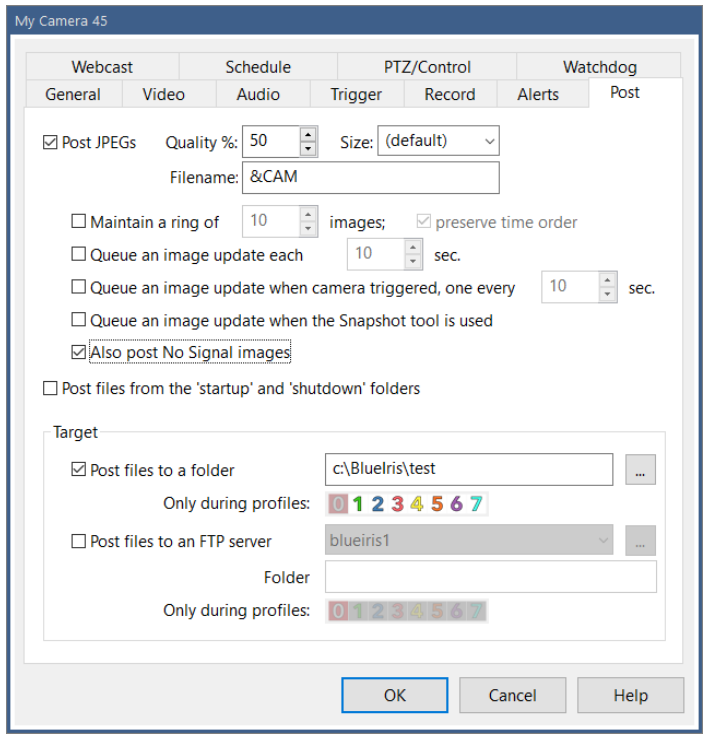
Users have reported that the streaming is more stable to these servers if audio is included, regardless of whether it is just silence or not.

Use the **Configure** button to define the required bit rate and frame size and other encoding parameters as required by your server.

Most servers require *adobe* authentication, but the option exists here for *llnw* as well.

IMAGE POSTING

This feature may be used to periodically upload images to a web space or to a local folder.



You may select the **Quality** and **Size** for the images generated. You may use &CAM for the **Filename** as well as other standard time formatting codes as documented in the Alerts and Actions chapter. The *.jpg* suffix is automatically appended and should not be included here.

When you request a **Ring** of images, a number is appended to the filename in sequence beginning with 0 and the software replaces previous images in a round-robin fashion. If you also select the **preserve time order** feature, the newest image is always number 0, then 1, etc. Use this with some caution however, as it involves a *rename* operation on the server for *each file after each upload*, and this can take significant time to complete.

Images may be uploaded on a **timed** basis, and/or only in response to a camera **trigger** or use of the **snapshot** command. It's also possible to queue an upload manually via a command on the camera's right-click menu.

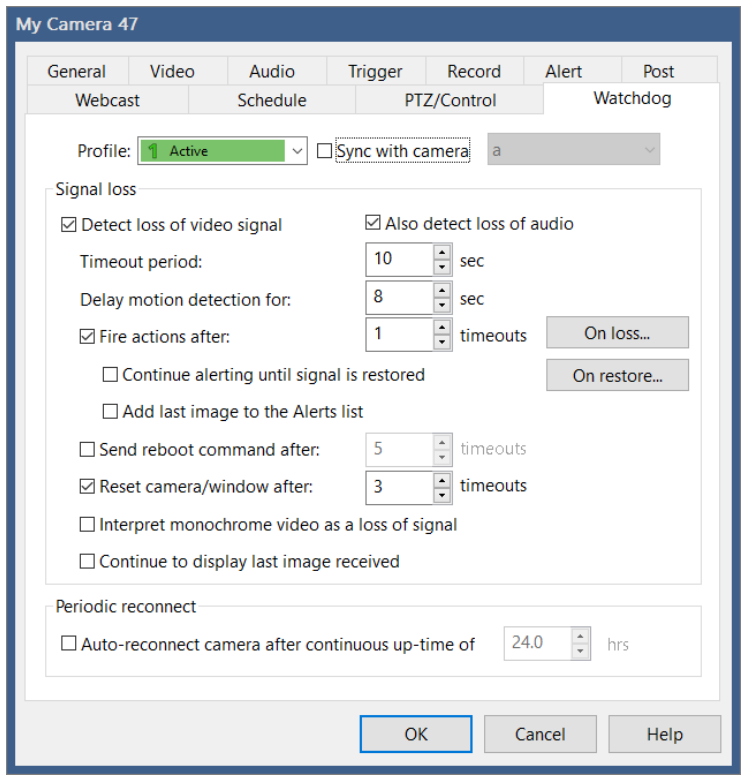
By default, images are only uploaded when the camera has a signal. If you would like to continue posting images through no-signal periods, an option is given for this.

You may have the software upload files for you automatically upon software (or camera) startup and shutdown. All files found in the *startup* and *shutdown* folders in the Blue Iris program file folder under a subfolder *cameras* and the camera's short name will be uploaded. Please be aware that this may delay a software (or camera) shutdown as these files are being uploaded.

If an FTP destination folder is not specified, the FTP server's default folder is used. If the folder specified here begins with a / (forward slash), this is considered a root or **absolute** folder from the root. Otherwise, the folder is **appended** to the server's default folder.

WATCHDOG

The Watchdog function waits for the camera to go offline and then replaces the image with a *no signal* message, possibly with the last known image from the camera as well.



Settings on this page as well as on the Trigger, Record and Alerts pages may change with the active profile. They may also be synchronized with another camera—please see that topic below.

The **timeout period** defines the duration of time before the watchdog kicks in. The software will then automatically attempt to restart the camera stream by reconnecting to the network IP camera. If a number of timeouts occur in succession, you may choose to completely **restart the camera window** and/or **send a reboot command to the camera** as well. Of course, depending on how or why the camera is offline, it may not receive that command.

The option exists to **Delay motion detection** for a period of time following the timeout period. This prevents potentially unwanted triggering that may result when the camera image suddenly jumps forward in time.

More-so for analog cameras which may display a green or blue frame when there's no signal, the option exists to interpret that as a signal loss.

It's possible to **trigger the camera** following a specified number of watchdog timeouts, and the **continue triggering until the signal is restored**. This may be useful if you want recording or image posting to kick-in, or to fire camera trigger alerts.

However if you want to fire specific alert actions in response to signal loss or reacquisition, you may define a separate action set for each condition here instead.

No-signal images

You may choose to serve a custom JPEG image in place of the default "no signal" on grey. To do this, create a JPEG *nosignal.jpg* and place it inside of the camera's folder that is found by default at:

C:\Program Files\Blue Iris 5\Cameras\(camera's short name)

You may need to create this folder if it does not already exist.

If you un-check the option to **Continue to display and stream video while inactive** on the Schedule tab, another grey screen with an "inactive" message is displayed. You may create a JPEG file *inactive.jpg* and place it in this same folder to serve in place of this default message.

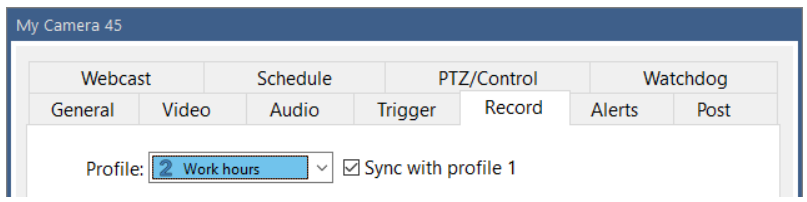
CONFIGURATION SYNCHRONIZATION

With a number of cameras, and the ability to define settings for multiple profiles each, managing all of these pages of options can become overwhelming. It's possible to synchronize settings between profiles and among cameras to make this task easier.

You will find at the top of the Trigger, Alerts, Record and Watchdog pages the option to synchronize the page. This replaces the functionality found in older versions where copy and paste buttons were tediously required.

Profile synchronization

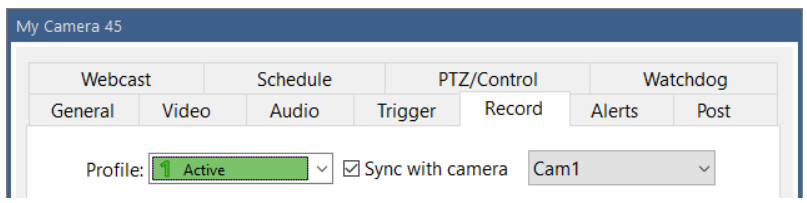
When a profile other than 1 is selected, you have the option to synchronize that profile with Profile 1 and *this is the default setting*.



This allows you to immediately use multiple global profiles without the need to go into each camera and re-define everything you've already defined for profile 1. You need only to visit those cameras where alternate behavior is required for the newly-used profiles.

Camera synchronization

When Profile 1 is selected, you have the option to synchronize the camera with another camera's settings entirely.

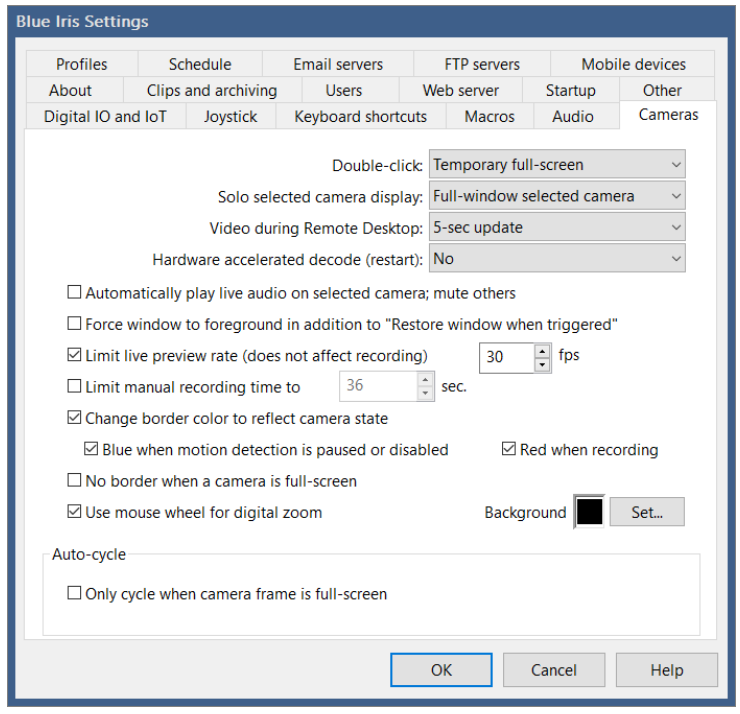


This will apply to *all profiles* on the camera unless you have selected to not synchronize specific individual profiles (by unchecking their **sync with profile 1** boxes). That is, if profile 2 is active and camera A's profile 2 syncs with profile 1, and camera A's profile 1 syncs with camera B, camera A will use camera B's profile 2 settings.

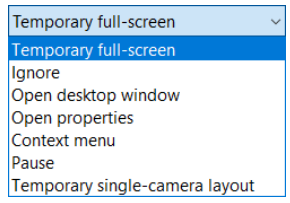
Yes it is possible to synchronize cameras in a "chain" sequence, each referencing another camera, but this is not recommended for efficiency or sanity. A settings loop will be detected and discontinued after 10 "hops."

GLOBAL CAMERA SETTINGS

There is a Cameras page in Settings, which is found on the main menu. Several of these items are discussed elsewhere in context.

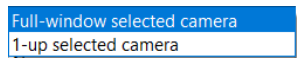


You may define what happens when you **double-click** a camera window.



By default a double-click will open the camera individually temporarily **full-screen**. While in temporary full-screen mode, use the arrow keys to select another camera. Use Esc or the right-click menu options to exit full-screen. Use **Pause** to toggle between paused indefinitely and to cancel pause—this is equivalent to setting the Shield icon red, but for this camera only. The **Temporary single-camera layout** option temporarily enables the "solo" feature where only the selected camera is displayed—use *Esc* to return to normal.

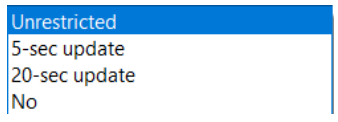
The definition of camera **Solo** may be changed here.



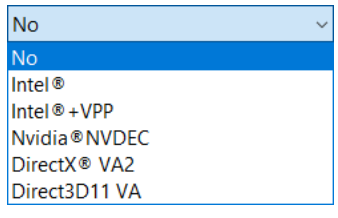
By default, a "soloed" camera is shown alone in the live video window. It's also possible to select it to be at the "1-up" position. This means it is displayed larger than the other cameras. If the current group layout was configured with varying camera heights, these are temporarily ignored.

If you connect to the Blue Iris PC using a remote desktop solution, it may be desirable to limit live video drawing during that session. It takes considerable remote desktop resources

to continuously draw the live camera display, making it difficult to navigate the UI. It has been found that Windows is unable to properly identify this condition in most cases, so you may need to instead use the **pause** icon at the top-right of the live video window once you are connected.



It's possible to leverage graphics hardware for video decoding, easing the burden on the CPU. Here you may select a technology to use globally:



This setting may be overridden on a per-camera basis on the Video page in camera settings. Additional discussion on this topic is found in the Advanced Video Topics section of the Cameras chapter.

The option to **Automatically play audio on selected camera; mute others** is a handy way to manage live video audio without having to explicitly use the speaker icon each time you are interested in hearing camera audio.

Select to **Limit live preview rate** to save CPU cycles by not attempting to draw each and every video frame to the display.

If you uncheck the option to **Change the camera border** with its state, it will remain white regardless of whether there's motion, it's triggered, etc. If you would like to know when the motion detector is disabled, it is possible to have the border painted blue in this case. You may choose to have **No border when a camera is full-screen**.

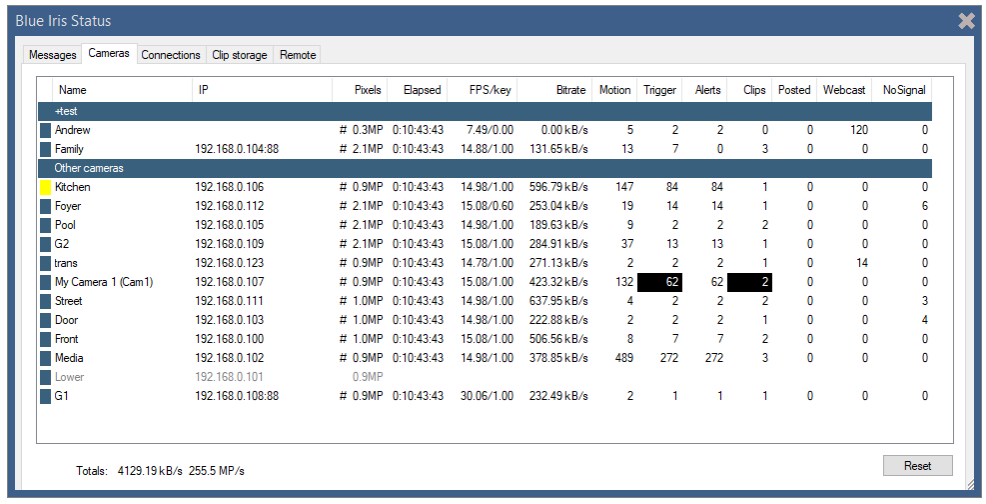
The color of the live video window behind all cameras windows may be set here.

The mouse wheel is by default used for **Digital zoom**. You may disable this behavior here.

Auto-cycle and its global settings that are found here are discussed in the Camera Groups topic above.

CAMERA STATUS WINDOW

Here you will find an overview of your cameras and their current operation. There are also a number of metrics important for optimizing performance.



Pixels

This is the number of picture elements in each image—the width multiplied by the height. The value is given in MP (megapixels or millions of pixels). You may click the **Pixels** column header to switch between MP and XxY resolution formats.

HA

Hardware acceleration. When a value is shown, the camera is currently using *hardware decoding* (I=Intel, I+=Intel+VPP, N=Nvidia, DX=DirectX, I2=Intel Beta).

Elapsed

The time since the last camera window restart.

FPS/Key

The FPS is the number of Frames per Second on average currently being received from the camera. The value that follows is the number of *key* frames per second. A key frame is a complete frame—one that may be displayed without reference or dependence upon another frame. These are sometimes called I-frames and define a *GOP* (group of pictures).

The key frame rate is an important consideration for multiple software functions. A key frame rate of approximately 0.50-1.00 is desirable for optimal use of the *direct-to-disk recording* option as well as the *limit-decoding unless required* functionality. Adjust this rate within the camera's web browser interface.

Direct-to-disk recording can only begin on a key frame boundary—if the rate is too low, this means that video frames between a trigger event and the next key frame rate may be lost. One way to compensate for this is to use *pre-trigger time* on the Record page.

When limit-decoding is being used, only key frames are decoded unless all video is required for display or analysis. This means that only key frames are fed to the motion detector when the camera is not triggered or selected for streaming or viewing. If the key frame rate is much lower than 1.00, the motion detector may not operate effectively and events may be missed.

Bitrate

The bitrate is the average amount of data received from the camera per unit time, expressed as kB/s or kilobytes per second. A kilobyte here is 1024 bytes. You may see other representations of bitrate as either kbps or Mbps, which are kilo-*bits* per second and *mega*-bits per second. In networking, unlike in general computing, a byte consists of 10 bits. So the relationship between this is kbps = kB/s multiplied by 10 and Mbps = kbps / 1024.

Status counters

The *Motion*, *Trigger*, *Alerts*, *Clips*, *Posted*, *Webcast*, and *NoSignal* columns are resettable counters.

Motion represents the number of motion events, not necessarily leading to a Trigger or Alert.

Trigger represents the number of trigger events, when there was sufficient motion to trigger, or the camera was triggering in another way. If this cell is black, the camera is currently in the triggered state.

Alerts represents the number of times that a trigger resulted in one or more alerts fired—emails, push notifications, alarms etc.

Clips represents the number of files created. If this cell is black, the camera is actively recording.

Posted represents the number of frames sent via FTP or saved to disk according to settings on the Post page in camera settings.

Webcast represents the number of frames viewed by web server or app users.

NoSignal represents the number of times the camera signal was lost. The signal may have been immediately restored causing no loss of video, or it may have been out for longer. These events are logged to the Log page in status.

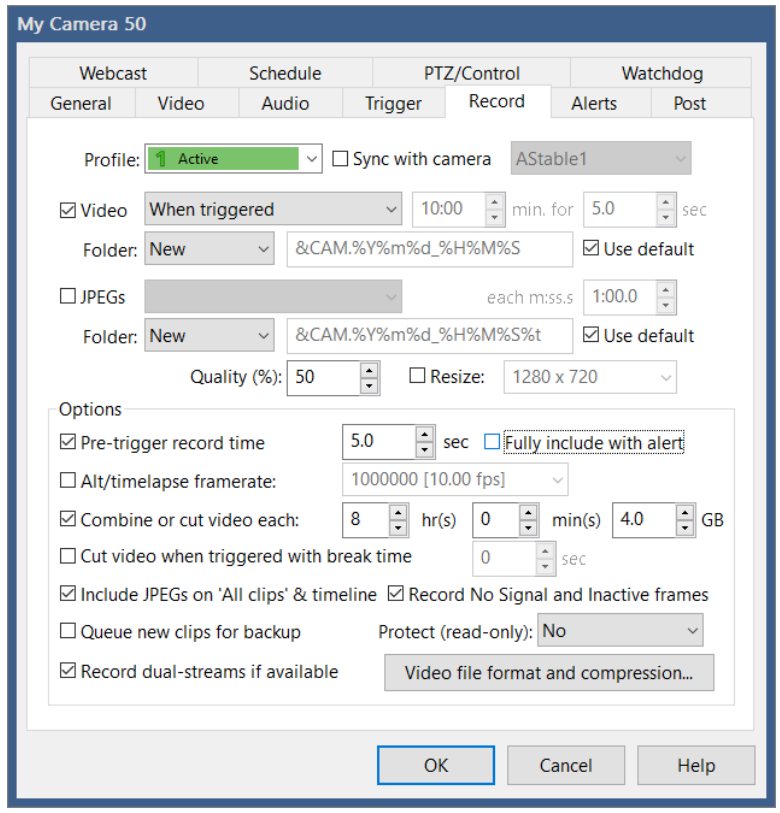
RECORDING AND CLIPS

Here you will find descriptions for settings that control what's recorded from your cameras, when it's recorded, where it's stored, how to access it, and how long it's kept.

When a camera is actively recording, you will see this "LED" icon in its window title bar. When this icon appears gray, this indicates that the camera is not actively recording, but the recording file remains open and is waiting for additional trigger events to record. If you prefer to have "one file per trigger event" you may disable the **Combine or cut** feature that's described below.

RECORDING OPTIONS

Recording is configured on the Record page in camera settings.



Settings on this page as well as on the Trigger and Alerts pages may change with the active profile. They may also be synchronized with another camera—please see that topic at the end of the Cameras chapter.

Video

When triggered. Video is only recorded when the camera is in a triggered state. This can greatly save on storage space over continuous recording. The **pre-trigger video buffer** applies only to this type of video recording. By default, multiple trigger events are stored into one file—see **Combine or cut** below.

When alerted. Much like *When triggered,* but video is only recorded when the camera is in a triggered state *and* the alert has been confirmed by AI or otherwise.

Continuous. Record video all of the time the camera is online and active.

Periodic. Record video in defined intervals in a *discontinuous* or *time-lapse* manner—meaning that playback gaps are removed.

Triggered + periodic. Combines *when triggered* with *periodic*. All frames are recorded when the camera is in the triggered state.

C*ontinuous sub + alerts*. When used with a dual-streaming camera along with direct-to-disk, the result is a BVR file which will contain the sub-stream continuously recorded, but the main-stream only recorded when the camera is in an alerted state. During main-stream playback, the sub-stream will be upsampled whenever the main-stream is not available. This dual-stream hybrid may be exported only when re-encoding is selected, although you may still export the main-stream in segments when not re-encoding. When not using dual-streams or direct-to-disk, recording of the sub (or only) stream is continuous.

Continuous sub + triggered. Similar to *Continuous sub + alerts,* but main stream recording occurs upon *trigger,* not just alerts, ensuring that the main stream is recorded even for *canceled* alerts.

By default new video goes to the *New* clips folder as defined on the Clips page in Settings.

It's recommended that you retain the default filename format. It is possible to override this however to add a subfolder for the camera and/or month and year for example:

&CAM\&CAM.%Y%m%d_%H%M%S

%Y%m\&CAM.%Y%m%d_%H%M%S

The actual filename portion of the path should always either begin or end with the camera name, either &CAM.xxxx or xxxx.&CAM. This is the way in which many software features are able to identify files as belonging to particular cameras—the short name must *not* begin with a number, while the segment at the opposite end of the filename *must* begin with a number (typically part of the date or time).

Also, the filename should retain the time specification to avoid duplicating filenames between successive recordings. A table of time formatting codes may be found at the end of the Alerts and Actions chapter.

Video Options

The **pre-trigger record time** is really an *encoded video buffer* when used in conjunction with *direct-to-disk recording*. For the proper operation of recording and many other functions, this buffer must always contain at least one key frame (full image) from each stream. Given that most cameras send a key frame each 1-4 seconds, a minimum of 5.0 seconds of buffering is enforced. You will need to increase this buffer size if your camera has a key frame rate of less than 0.25 fps. Without a network camera or without direct-to-disk recording, this buffer will contain raw RGB bitmaps, so will be limited to 1.0 seconds to conserve system resources.

This is a useful feature for capturing the moments leading up to a trigger event, as recording will begin at the first key frame in this buffer. If your camera is sending a key frame each 4 seconds, with a 5 second buffer, it's possible only 1 second of pre-trigger video will actually be recorded. This would be another potential reason to increase the buffer beyond its 5 second enforced minimum. FPS and key frame rates are displayed on the About tab.

When an alert is replayed or exported, by default up-to 2 seconds of the pre-trigger record time is included as part of the playback. This allows you to see movement immediately leading up to the trigger while still recording the full pre-trigger time. If you'd prefer that alert playback begin earlier, at the beginning of the pre-trigger time, select the option to **Fully include with alert**.

The **Alt/time-lapse frame rate** purposely "drops" frames as necessary to lower the fps that is recorded. If you select a rate that's less than 2fps, the time scale of the recording will be adjusted to playback at 2fps regardless. This creates a "time-lapse" effect where motion and activity will be played back at greater than realtime speeds. For time-accurate output, this may not be used with direct-to-disk, as only key frames would be recorded, and these may not align with your desired alternate frame rate.

The **Combine or cut video** option exists to *combine* events into fewer files when recording *when triggered,* but it also *cuts* video into segments for the other recording modes. For w*hen triggered,* un-check this option in order to have one file recorded for each event. Although you may *choose* whether or not to create new files on a timed basis, you must *always* specify a maximum size for a file before a new one is created.

If the cut time specified is 5 minutes or more and equally divides a day, such as 10, 20, or 30 minutes, or 1, 2, 3, 4, 6, 8, or 12 hours, recording will be aligned to the realtime clock. That is, if you have a cut time of 12 hours, yet start recording at 11am, a new file will be created at 12pm to cover 12pm-12am. The Blue Iris BVR file format allows for appending and continuation across camera or software restarts, however, so this effect will be mitigated when possible.

The **Cut video when triggered with break time** option can be used with continuous recording such that each new file created always begins with a trigger event. The cut will occur only if there's been at least a specified amount of time where the camera remained in a non-triggered state (a break time).

By default the software does not record video when there's a "no signal" or "inactive" condition displayed. Of course, there's an option to override this.

If your camera is configured to supply both a main stream and a sub stream and you are also configured to record direct-to-disk in the default BVR file format, by default the **Record dual-streams if available** option will cause both of these streams to be saved to the file. Uncheck this option to save only the main stream. As the sub stream is used for motion detection and it requires minimal bandwidth, it's advised that you retain this option selected for tuning and flexible playback.

Snapshots

Periodic JPEG images may be saved to a specific folder that's been defined on the Clips page in Settings—by default the New folder.

As with video files, it's possible to override the file format for snapshots as well, but the same naming restrictions apply here as well.

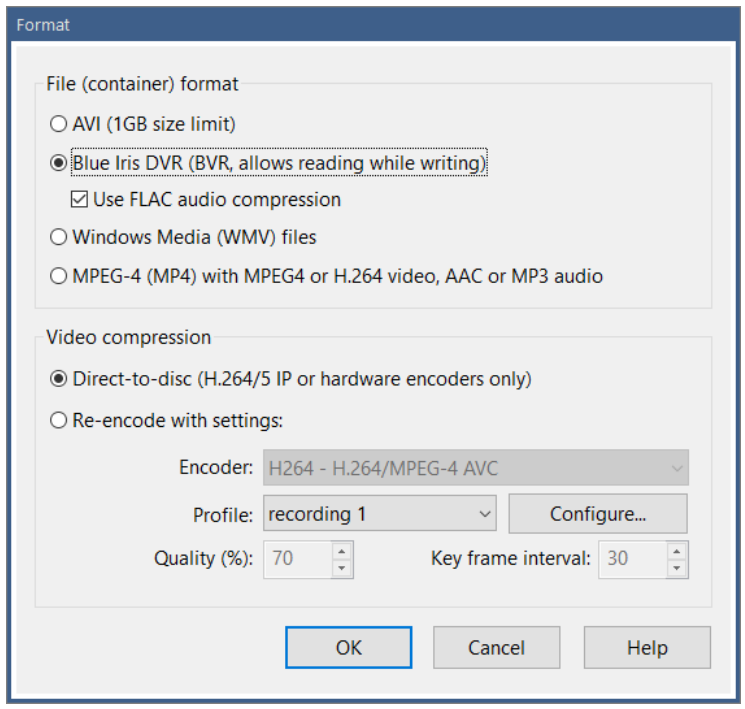
There's an option to save an image only when triggered. Depending on your timing for trigger break time and snapshot interval, one or more images may be saved.

You may select the quality in percentage to use for the JPEG compression.

By default, snapshots are included on the Clips list "all" view and in the timeline view. You may wish to remove these with an option here. Snapshots will still always show in camera-specific lists and folder-specific lists (New, Stored, etc).

Video file format and compression

This page controls the video file-type that's used, and whether it is modified prior to storage.



It's recommended that you retain the default, yet proprietary, BVR file format. There are a great many software features which rely on this simple flat-file format. It's the only one offered that may be played at the same time that it's also open for active writing for example. It's the only one that may be used for multiple-camera timeline playback. It also offers the best overall experience with remote viewing. Select another format only if absolutely required by a particular use-case. You can always use the Trim/Convert/Export tool from the clip viewer to save it into another "export format" later on if you need to share the video.

Direct-to-Disk

This option may be used to save considerable CPU time. Video taken from a network IP camera stream is directly saved to disk without re-encoding it. There are some disadvantages to this however:

- Recording may only begin on a key frame boundary. Check that your camera is sending sufficient key frames on the Cameras page in Status (at least 0.50 per second).
- Video overlays are not saved as meta-data, not directly burned into the video. This may be an advantage however as you may toggle from on/off during playback.
- Cannot be used with time-lapse options. All video frames must be saved, as each frame relies on the previous one in order to be decoded for display.

- You may want to alter the quality, size, or other video characteristics.
- May only be used by network IP cameras with H.264 or H.265 streams.
- May not be used by analog or USB cameras, unless it's an uncommon source that supplies H.264 or H.265 video.

Re-encoding

If this is your only option or you have CPU cycles to spare, you may choose to re-encode the video prior to saving to the disk. Only H.264 is offered at this time, but a number of encoding parameters are configurable. Recording parameters may be saved as "profiles" and you may select which profile to use for each camera. See the Encoder Options section below for more detail.

More options



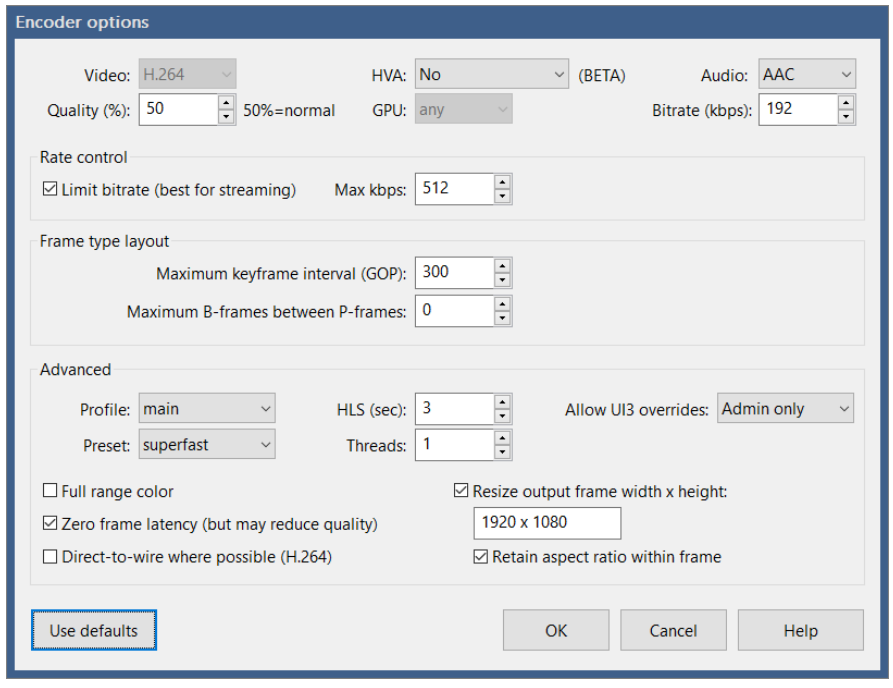
The **Queue new clips for backup** setting works in conjunction with the clip backup function configured on the Clips page in Settings, described later in this chapter. A clip (either a video or a snapshot) will show a cloud icon in the clips list when it's queued.



You may choose to have new clips automatically marked as read-only (protected). These clips will show a padlock icon in the clips list. Use caution with this setting, as these clips will not be automatically moved or deleted by rules established on the Clips page in Settings, possibly resulting in a disk-full condition.

ENCODER OPTIONS

Video and audio encoding options may be configured for a number of purposes, including recording, exporting, and publishing video.



Video encoding settings are only applicable when *re-encoding* video. When video is taken from a camera and saved *direct-to-disk*, served *direct-to-wire*, or when video is exported from BVR format to MP4 without alteration, these video encoding settings are not used.

In all cases however, the audio is re-encoded to either AAC or MP3 format. AAC is more typically found in MP4 files, but MP3 is offered as well for compatibility with external systems which may more easily ingest this format. The audio bitrate is typically in the range of 10-256 kbps (kilobits per second). Note that the actual output audio bitrate may also be limited by the input sampling rate—specifying a value of 512 for example may be overkill given a typical camera's 8kHz/16-bit/mono input signal.

If your Nvidia or Intel hardware supports encoding you may choose to enable this here. Many cards, if they support this at all, only support a maximum of 2 sessions. If an error occurs using hardware encoding, this is always noted to the Log page in Status, and the software "falls back" to software-based encoding. This is still considered a BETA option (for experimentation by experts only).

Rate control

When recording, this is typically best done "quality based" or VBR (Variable Bit Rate). Only consider use of the rate control feature when encoding for streaming, not recording. A network connection has a maximum bitrate that it may support, and by using the rate control feature you can insure the stream stays within the network's capability.

Frame type layout

H.264/265 video is divided into groups of pictures (GOP), which is the **keyframe interval**, or number of frames from one keyframe to the next. A *keyframe* is a complete frame—one that may be displayed without reference or dependence upon another frame. These are sometimes called *I-frames*. The frames in-between keyframes are *P-frames* and *B-frames*. These frames contain only the *differences* from one frame to the next and may be *predictive*.

The keyframe interval is also best in the 15-30 range for recording, but can be much higher (300 or so) for remote streaming applications. B-frames are not used for "main" profile encoding, only for extended or "high" profile encoding.

Advanced

The **profile** defaults to *main*. It is recommend that you retain this setting unless you are encoding for a specific external system which requires otherwise.

The **preset** defaults to *superfast*. When combined with the **zero frame rate latency** option, this provides the least amount of latency for video encoding. Changing this may have the possibility to increase overall image quality during re-encoding, but always at the expense of more CPU resource. Also, latency translates to "blackness" at the beginning of the video for one or more frames as the encoder must setup a "pipeline" and does immediately produce output.

The **HLS (sec)** setting is only relevant when hosting an HTTP Live Stream session via the Blue Iris web server, and this is not commonly done.

Allow UI3 overrides must be enabled in order for users to make changes to the bitrate, quality, etc., from the UI3 (web browser interface) stream profile editing pages. By default, only admin users have this ability.

The option is provided to **Resize the output frame.** If not used, the video output resolution will equal the input resolution. You may be necessary for instance to take your 5MP camera video and resize it for consumption online where videos are typically only 640x480, 1280x720, 1920x1088 etc.

When **Direct to Wire** is in effect, video is passed directly from a camera's direct-to-disk frame buffer to the browser UI3 and other clients. This has the huge benefit of using NO CPU for the decoding and re-encoding of the video. However, this also means the video will not have Blue Iris overlays and is limited to either the sub or main stream WITHOUT

MODIFICATION—that is, it becomes imperative to manage the stream encoding properties on the camera side. You should have a reasonable key frame rate (0.40 or higher) and use H.264 (as UI3 and the phone apps cannot decode H.265 at this time).

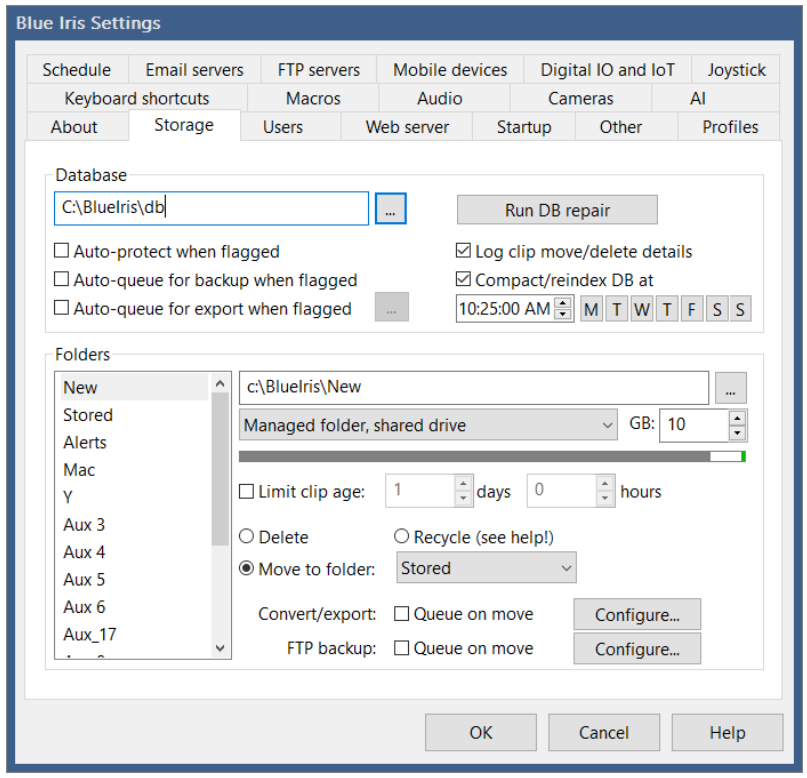
MANUAL RECORDING



Use the video camera icon at the top of the main window to manually start and stop recording on the selected camera. By default, this provides only 30 seconds of recording—this may be adjusted on the Cameras page in Settings.

CLIP FOLDERS

By default, there are four folders configured to store and manage recordings—*Database*, *New*, *Stored*, and *Alerts*. More precisely, only *New* and *Stored* are used to store video files; the *Database* folder hosts a series of *.dat* files which are used by the software to keep track of the other managed folders, and the *Alerts* folder will remain empty unless you have asked for **Hi-res JPEG files** on the Alert tab in camera settings. *The Alerts folder may not be used otherwise for direct recording, even if you rename it.*



There are several other folders which may be configured as well. By default, new recording is made to the *New* folder, but you may select another folder on the camera's Record page in settings.

Click on a folder name in the folder list to edit its location and other parameters. You can also rename a folder directly on the list by *slowly* double-clicking—sometimes called a "click and a half."

Each folder may be configured to reference a different volume or drive entirely—excluding the *Alerts* folder, that is a total of **15** possible drives. Although *New* and *Database* should remain on your fastest storage possible because of frequent access, the only other requirement is that these folders not be "nested" in any way—*db* should not be inside of the *New* folder, or vice-versa for example. If accidentally configured this way, it will not be possible to leave the page or click **Ok**.

A folder may be one of four *types*:

Managed folder, shared drive. The default for normal usage. Recordings are indexed in the database and accessible through the software. Files will be moved/deleted according to the size and age limits configured for the folder. The drive may be shared with other applications and the operating system.

Managed folder, unmanaged drive. Use judiciously when the software has trouble reading used/free space on the drive. Recordings are indexed in the database and accessible through the software. Files will be moved/deleted according to the size and age limits configured for the folder, *but the software will not regard the used or free space on the drive when making these decisions*.

Managed folder, exclusive-use drive. This setting informs the software to expect *only* Blue Iris related files on the drive and to throw appropriate errors or to run appropriate repair operations if other files are detected. A feature soon may be added to automatically maximize the use of a drive, but caution should still be taken not to over-allocate the drive.

Unmanaged folder. Recordings will **not** be indexed in the database or accessible through the software directly (you may still drag/drop them into the window). Files will **not** be automatically moved or deleted. You will be responsible for the prevention of the drive running out of space. This option exists primarily to provide an "output folder" for functions such as AI faces, JPEG snapshots, exports, and similar. Files in this folder are considered "other files" on a shared drive. An unmanaged folder should **not** be configured onto an exclusive-use drive!

Each folder is given a **size** (in gigabytes or GB) and an optional **age** (in days and hours). Once a folder reaches either occupancy limit, always the *oldest* clips in that folder are moved or deleted in sequence until order is restored.

By default, even though configured on the same drive, the *New* and *Stored* folders are configured to "cascade." Recordings begin in the New folder, and are then later moved to Stored after a period of time, and are then finally deleted after another period of time.

Camera—>*New*—>*Stored*—>Trash
0 days 7 days 14 days

Often the *Stored* folder is configured as a NAS (Network Attached Storage, usually Ethernet) or other external storage (USB etc) and the concept of cascading is appropriate. It is

common and reasonable to use a single storage folder scheme instead by configuring the *New* folder to delete rather than move to *Stored*.

Important note: when creating cascading folders, be sure they cascade **DOWN** the folder list, **not up**. Move from Aux 2—>Aux 3 for example, not the other way around.

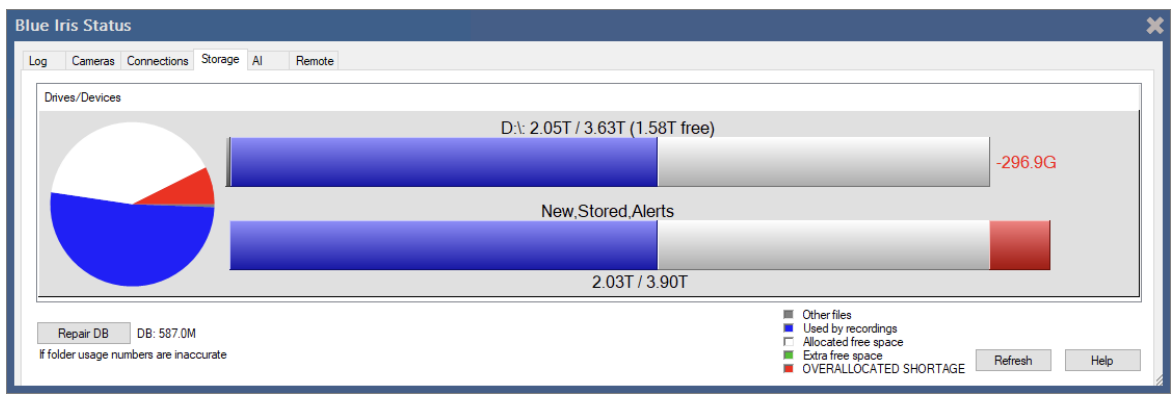
Important note: set the **size** accurately and to ensure it will actually "fit" onto the drive. If you ask the software to use too much space, this is called an *overallocation* and the software will complain about it in a number of ways, notably with a message at the bottom of the main window that looks like ***!! C: -26.3GB*** meaning you asked for 26.3GB more on the C: drive than you actually have. This does *not* mean the drive is *currently* out of space, but if not addressed, the drive *will* run out of space, and that will lead to other complications and instability.



Important note: folder age limits are absolute, not relative or cumulative. This means that if *New* is set to move to *Stored* at 7 days, and then *Stored* is set to delete at 14 days, the file will be deleted 14 days after it was created, not 21.

Use the option to **Recycle** instead of **Delete** judiciously. This requires more system resources, and can be Windows user-specific. If you are running as a service, you should be running with a named user account, not *Local Service* if you are considering use of the *Recycle* bin.

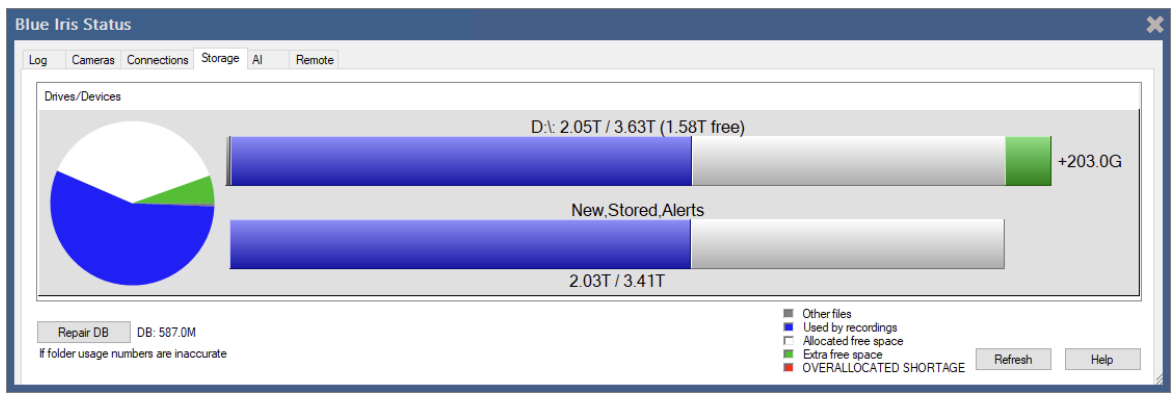
The Storage page in Status offers a visual overview of your storage settings:



Here we see an overallocation as we've selected 3.90TB for New, Stored, and Alerts. This will not fit on the drive by over 296GB. The first segmented bar graph shows the drive's size, used space (in blue) and free space (in white). The next bar graph shows your Blue Iris folders which are configured to use this drive—used space is blue, unused space is white, but the *red* indicates requested space which will not fit onto the drive. This must be

corrected in order to prevent the drive from eventually running out of space as new clips are created.

By lowering the total requested space to 3.4TB, here is the new chart:



The green space on the C: drive bar graph now represents *extra* space or "headroom." A drive should always be configured with enough headroom for a *complete clip from each camera* that's recording to that drive, along with space for Windows temp files etc.

Do NOT attempt to allocate or use every last (giga) byte on the drive!

Other files on a shared drive are normally drawn in grey. If these other files are actually Blue Iris video files in managed folders, use the **Repair DB** button to re-adopt them. If you see yellow instead, this is an indication the drive was designated as *exclusive-use*, and this discrepancy should be corrected.

THE DATABASE AND CLIPS LIST

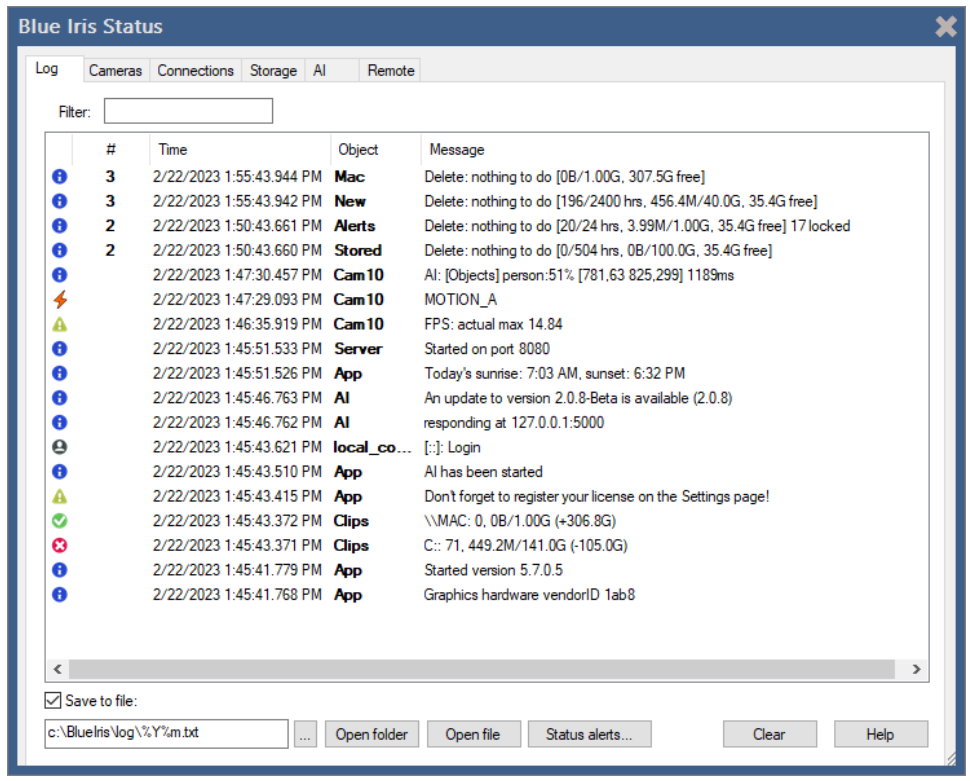
As discussed, because of constant access, the *database* folder should remain on your fastest local storage. It is the database that determines how much of each folder is currently occupied, as well as what is shown on the clips and alerts lists. There are a number of ways to filter this, but if a discrepancy is found, you can **Repair** the database either with a button on the Storage page in Status, or via a right-click menu in the Clips list, *Database—>Repair/Regenerate*.

Database maintenance is ran each 5 minutes. This is the function that actually deletes and moves files between folders according to the rules defined. You may start it manually at any time with right-click menu option in Clips, *Database—>Run maintenance*. If maintenance runs continuously, this may indicate that you are adding to folders faster than items may be moved out of the folders—adjustments are required to prevent one or more drives from running out of space.

Database compact/reindex is normally performed each night at 2am. The primary purpose of this function is to remove "holes" in the database produced by deleted records. It is typically a short process, but recording is suspended during this time. If 2am is not a good time to pause recording, you may wish to change this time, select specific days of the week for it to occur, or disable it altogether and perform it manually on occasion by using the right-click menu option in Clips, *Database—>Compact/Reindex*. If you disable this option yet neglect to perform it manually, the database will grow unbounded and performance will suffer.

The option for **Database Delete & Regenerate** also exists. This one *really* creates a new database from scratch and re-adopts everything. Please note that video and JPEGs are retained, but alert images and other flags that exist only in the database will be lost. You do have the option to save each alert image as a file instead with an option on the Alerts tab in each camera's settings pages.

To better audit "what happened" to clips and why they were deleted, you may wish to enable the option to **Log clip move/delete details**.



Each folder's statistics appear in the format *240/336 hrs, 69.6M/30.0G, 20.4G free*. This indicates:

240	the oldest file in the folder (hours)
336	the maximum age set for the folder (hours)
69.6M	the occupancy, or what's in the folder
30.0G	the maximum size set for the folder
20.4G	the actual free space on the drive

An error condition here indicates the C: drive will run out of space due to overallocation:

C:	the drive
9	the number of clips
1.89G	the storage space on the drive used by Blue Iris
45.0G	the amount of space you allocated to use on the drive
-22.6G	the amount of the overallocation, calculated as:

actual free space - (allocated space - used space)

Clips list filters

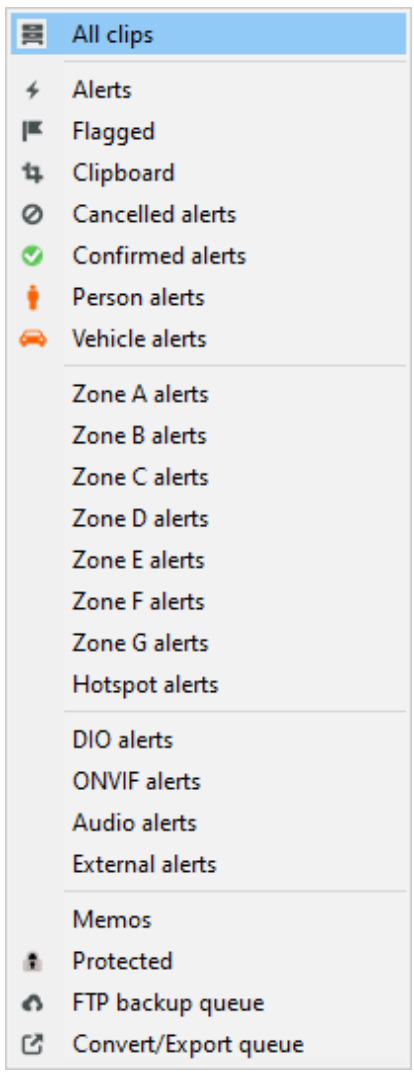


Fold/unfold the clips list. When unfolded, the live video is hidden and the clips list occupies the entire main window UI above the timeline view.

Show triggered alert images. An alert image is captured by default when a camera is triggered and lives only as a postage stamp in the database. It is a "bookmark" into an actual clip video file. When you open an alert image, the corresponding video file is opened at the appropriate time of the triggered alert. Alert images may have corresponding JPEG files, but only when an option is set on the Record page in camera settings.

Show clips, which are actual video files and JPEG snapshots. By default, *All* clips are shown. You can select from a folder list to display only files in a particular folder (that is, *New*, *Stored*, etc.). Also, if one of these folders has subfolders, you may continue to "drill down" into the file structure.

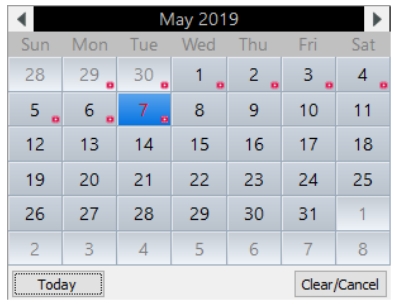
Show flagged items. Flagged items may include a combination of clips (files) and triggered alert images. Flagged items are marked with purple flags in both the clips list and the timeline view.



Select another view of the database. You may choose to view only alerts that have been either confirmed or canceled by AI, alerts that have motion in a particular zone, alerts that have a particular trigger source other than motion, or only items with an associated text memo.

You may monitor FTP transfer and Convert/Export progress here as well. The "clipboard" view is used to save images and video selections from the viewer as well as exports from the UI3 browser interface.

Use the **Calendar** icon to filter the clips list to display only items from one particular day. Click it again and use the **Clear/Cancel** button to return to the display of all items.



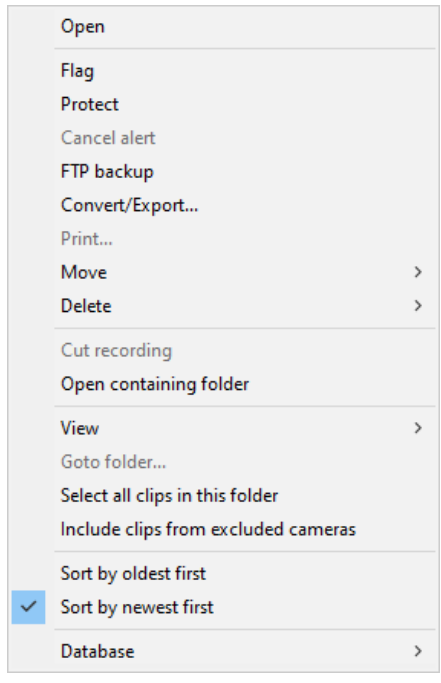
A red dot on a day indicates clips or alert images on that day.

Use the **Solo** icon to filter the clips list to display only items from one particular camera—the selected camera. If you are using the live view's camera solo function, the clips list will already be filtered, and it is unnecessary to use this option as well.

Toggle the sort order—either newest first, or oldest first.

Clips list context menu

Several options are repeated on this menu, however many are available here solely.



You may just double-click an item on the clips list, or click once and then use the *Enter* key to **Open** it in the viewer window.

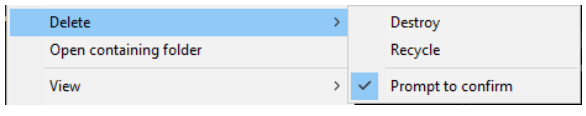
You may "hold down" an item on the clips list to toggle its **Flagged** status. With an option on Clips in Settings, flagged items may be automatically marked as **Protected** as well. A protected item (also called *read-only*) is not automatically moved or deleted by database

maintenance. Use this with caution, as this can lead to a disk-full condition if too many items are protected.

Items may be selected for **FTP backup** and/or batch **Convert/Export**. These topics are discussed in sections below.

You may **Print** a JPEG snapshot directly from this menu. It's also possible to manually **Move** or **Delete** a file.





The Cut recording option may be used on a clip that is currently open for recording. It will force the camera to close the file and then create a new clip as required. This is a great way to create a short BVR file to share with support if necessary.

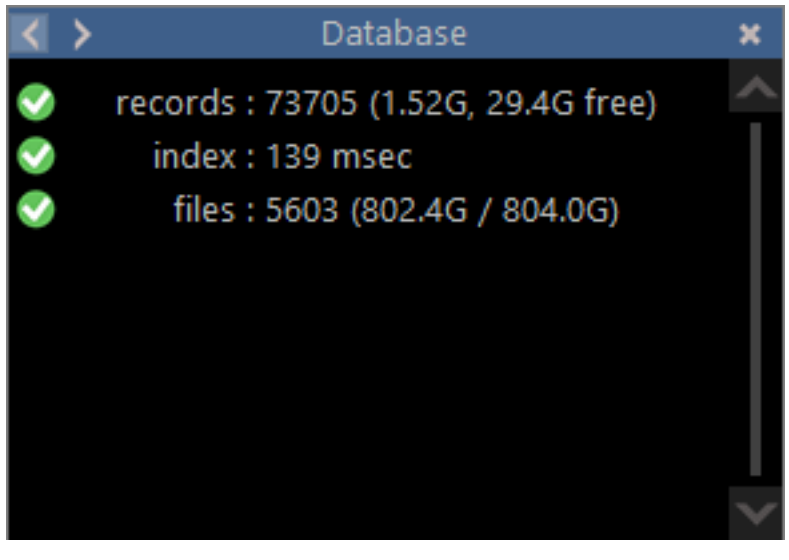
The clip may be moved to another managed folder, or you may create a sub-folder in the clip's current folder. You may also **copy** the file or **export** it. When you export here, the clip is deleted from Blue Iris.

Note that an *alert image* cannot be moved, copied, or exported here unless it has an associated JPEG file created using the **hi-res** option on the Alerts tab in camera settings. Recall that an alert image is normally just a database entry referencing an actual clip. Furthermore, deleting an alert image does *not* delete its associated video clip.

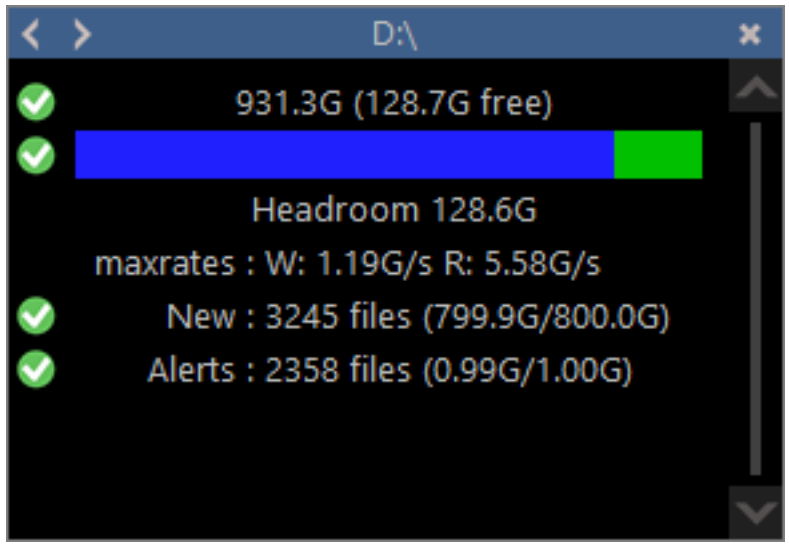
Normally, only clips from visible cameras are shown. If you'd prefer to see all clips regardless, use the **Include clips from excluded cameras** option.

DATABASE STATUS WINDOW

Issues regarding storage configuration and availability are so critical to continuous security that a special status window was developed to be displayed at the bottom of the clips/alerts list to provide an overview of the database status. This window will appear automatically as necessary to immediately alert you in the case of any trouble, but you may open it manually with a right-click option.



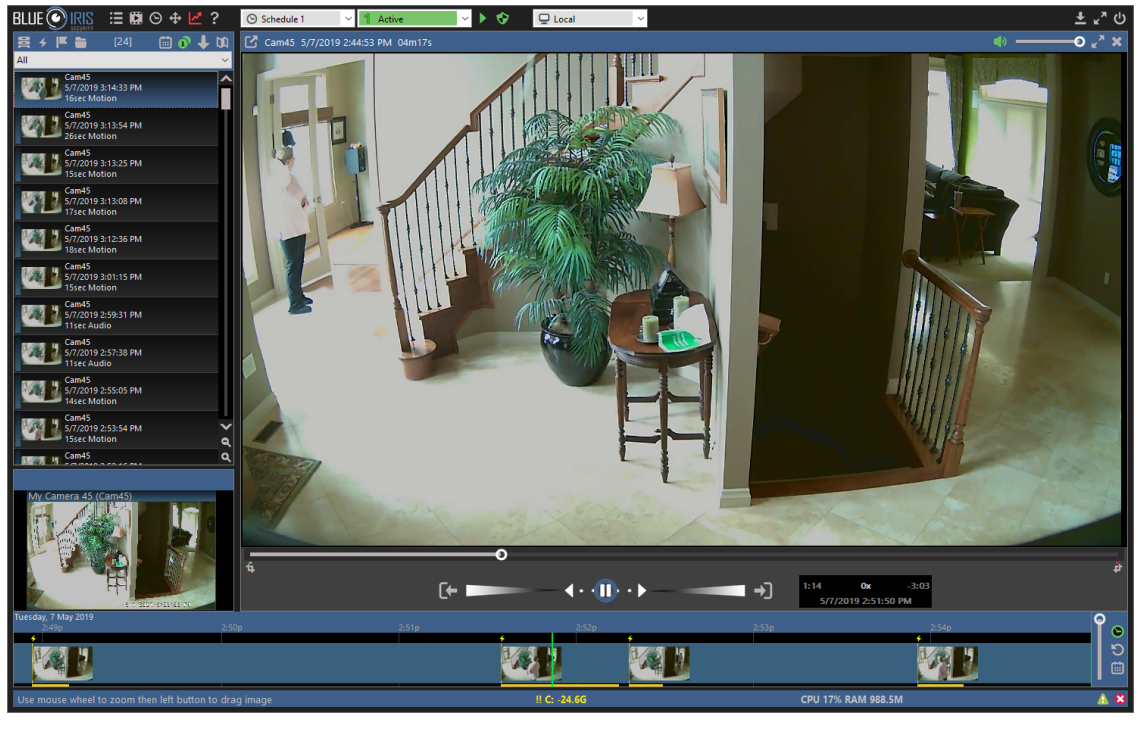
Use the < and > buttons at the top left of the status window to navigate between drive-specific pages:



CLIP PLAYBACK AND THE VIEWER WINDOW

Double-click a clip or alert image on the clips list to open the video for playback. It's also possible to drag and drop a file from Windows into the main window UI to open it for playback.

Note that only BVR clips may be opened for viewing while they are still open for recording.



Use the video position slider or the timeline view to "scrub" through the video. A video file that was recorded using the *When triggered* setting on the Record page in camera settings will only contain video at the times indicated by orange in the timeline.

A full-screen option for the viewer is available as well as a mute and volume control separate from the live clips window. Live camera audio will be automatically muted while the viewer window is open.

Save the current frame as a JPEG. Save to a managed clip folder and it will be added to the clips database. Hold SHIFT to skip the folder prompt and just use the previous folder. Hold CTRL to mark the new database entry as flagged.

Create a time "cropped" version of the clip on the "clipboard view." Until exported, the cropped version depends on the source video file. As used with trim/export, first position the crop icons at the bottom of the video position slider.

Use of the Search button is described in a section below.

Use of the Trim button is described in a section below.

Close the viewer by using the Esc key or the X button.

Digital zoom

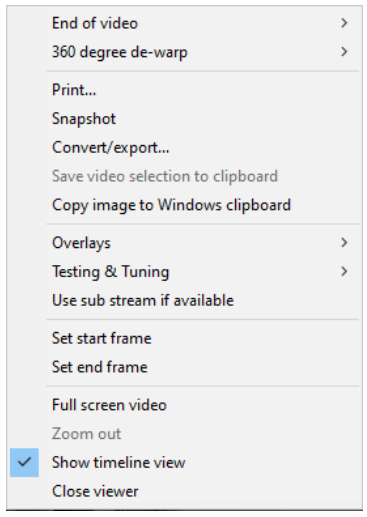
Use the mouse wheel over a camera window to zoom in digitally (the camera lens does not actually move). When zoomed in, the mouse cursor will become a "hand" icon and may be used to pan around.

Use the mouse wheel again to zoom out, or you will find a **Zoom out** command on the right-click menu.

The sense of the mouse wheel may be reversed using a setting on the Other page in Settings.

Viewer context menu

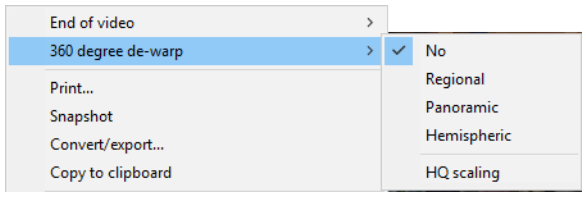
Several options are repeated on this menu, however many are available here solely.



At the **End of the video** you may select to *Stop*, *Loop*, or go to the *Next video*. When playing back a video opened via an alert image, there may be several events played. Note that moving to the *Next video* in this case would open the next alert image on the list, possibly re-playing some of the events already viewed.



For video recorded from a camera with a fish-eye lens, you may choose the way in which it is displayed with the 360 degree de-warp menu.



Regional creates a panoramic scene where you may use the mouse to drag the image left and right to view a section of the video at a time.

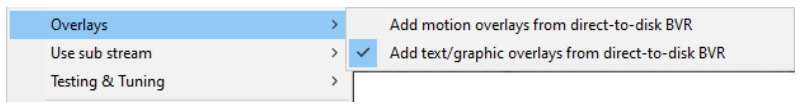
Panoramic creates a 2-row version of the panoramic scene, not requiring you to scroll through the image.

Hemispheric may be used to correct the fish-eye effect for cameras mounted on a wall or doorway.

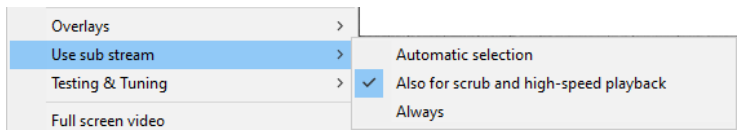
Use the **HQ scaling** option for a higher-quality image (at the expense of more CPU of course).

You may copy the current viewer image **to the Windows clipboard** at the maximum resolution of the source regardless of how it's scaled for display. The **Save video selection to clipboar**d option is equivalent to using the **crop** icon at the top of the window.

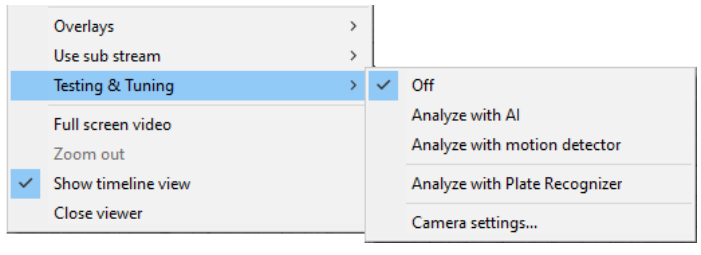
The **Overlays** sub menu contains options for adding motion rectangles and/or other text and graphic overlays to the display. These are saved as metadata only in direct-to-disk BVR files. For other formats, the overlays are "burned into the video" and cannot be turned off.



The **Use sub stream** menu is used in conjunction with a dual-stream BVR file to tell the software which stream to display. As the sub stream requires much less system resources to decode and display, it will be used by default for scrubbing and high-speed playback.



The **Testing & Tuning** menu may be used to fine-tune your camera's motion sensor settings found on the Motion sensor page from the Trigger page in camera settings.



- This is available for BVR files only
- Works best with clips captured using "direct-to-disk" recording or ones without added motion highlighting
- For your convenience, you may edit the camera's current settings to make immediate adjustment to motion settings.

You may select to **Analyze with motion detector** to *see what Blue Iris sees* as motion.

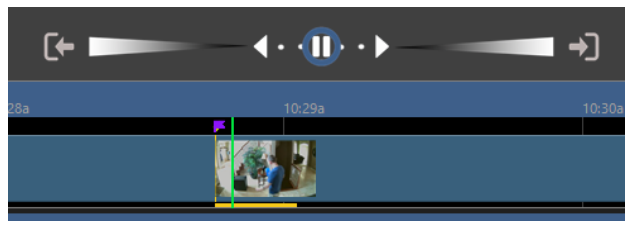
- Position the video about 3 seconds before an event—this will give the motion sensor time to "learn" the video before it can begin to actually discriminate motion
- Begin playback at 1x up to 8x normal speed.
- Masked areas (no zone coverage) will be drawn in black
- Motion will be highlighted and rectangles drawn around objects
- When there's significant motion, a trigger state will cause object rectangles and the viewer window border to be drawn in orange.

In addition, if the **AI** is installed and running, you may push BVR video frames through the AI *to see what the AI sees*. Frames are processed as quickly as possible (but may not always update in real-time unless you pause and step). If using dual-streams from a camera, bear in mind that the sub stream is used for initial motion detection, but main stream frames are sent to AI.

- Don't forget to turn off this mode when you are finished with it!

If you ask Blue Iris support for assistance with fine-tuning your motion detection, you may be asked to supply a BVR file to be used for this purpose. It should have several seconds of time *before* the event of interest—either something that is triggering that should not, or something that should not trigger, but does anyway. Supplying a clip which begins immediately at the time of trigger is generally insufficient to adequately train the motion detector.

THE SPEED SLIDER



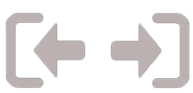
This single control, reminiscent of an analog “jog shuttle” control, allows control of both playback speed and direction, and can be used in several ways.

You can click on the play and pause icons for basic playback control.

The dots immediately to the left and right of the pause icon are used for frame stepping and slow motion.

Click anywhere on the control further to the left or right for high-speed playback in either direction, up to 256x.

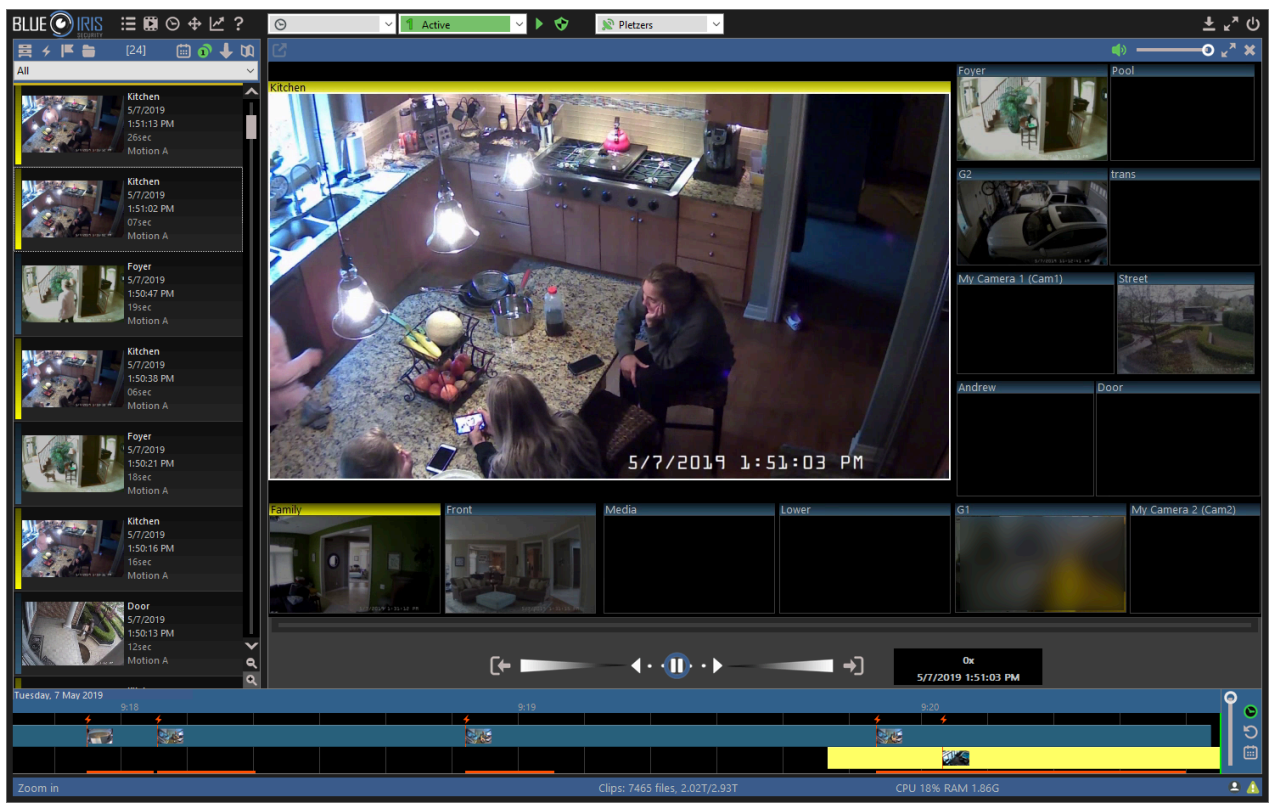
You can click and drag the blue ring for interactive speed control. Release the ring to return to the previously selected speed position.



These icons are used to move to the next or previous item on the current clips or alerts list. Hold the Control key when clicking to move by +/- 30 seconds or by entire pages in timeline playback.

TIMELINE PLAYBACK

Double-click anywhere in the timeline view or use the **Replay** button to enter *timeline playback*. Use the Esc key, **Now** button, or the **X** icon to close timeline playback.

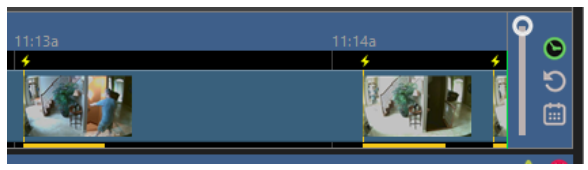


Timeline playback opens a display with a camera layout similar to the live camera display. All clips which were open for recording at the time represented by the green position indicator and timecode will be opened for playback. You can reposition by clicking anywhere in the timeline view, or clicking and dragging to “scrub” the video.

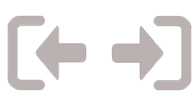
It’s also possible to click and drag the date and time bar at the top of the timeline while playback is paused.



Use the mouse wheel or the vertical layout sider to increase or decrease the zoom level. When substantially zoomed-in, alert images will be displayed.



The speed slider may be used as it was for normal clip playback.



Use these icons to jump to the previous or next alert position respectively. If there are no alerts currently visible on the timeline, these buttons will jump backward or forward by a time equal to 1/2 of the visible timeline (a page jump).

Now—show live video and continue to scroll the timeline as time passes.

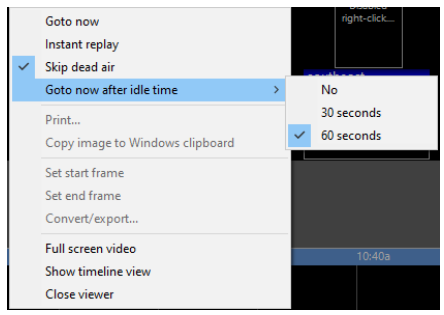
Instant replay—go back 30 seconds and begin timeline playback. Repeated clicks each will transport back 30 seconds from the current playback time.

Use the calendar icon to jump immediately to any date of interest.

If audio is enabled, audio is played from the selected camera's video when the playback speed is 1x forward. **Click** a camera's video window to select that camera.

Double-click a camera's video window while in timeline playback to directly open the source clip for normal clip playback. You may use all clip viewer functionality available such as Convert/Export. Return to timeline playback by using the *Esc* key, or completely close the viewer window by using the X icon.

Goto now after idle time. Use the right-click menu over the timeline view to access a feature to automatically return to a live camera view and current 'now' position after a period of inactivity:



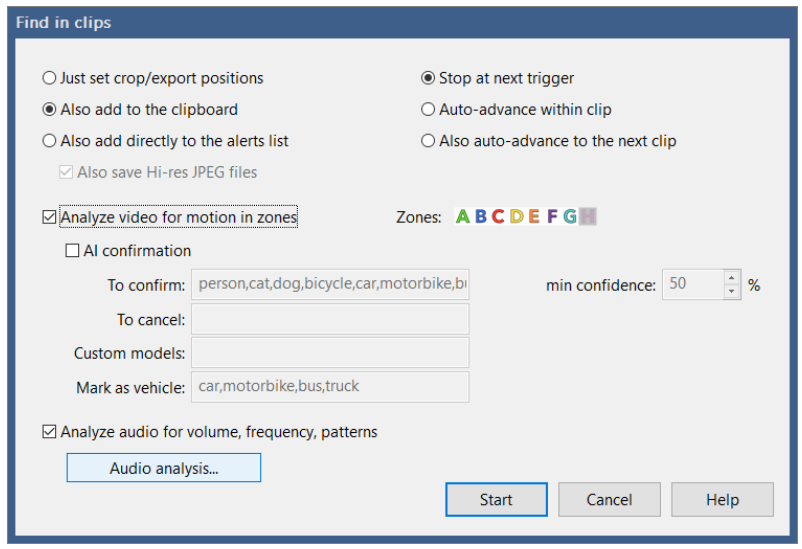
You may **Convert/Export** from the timeline view by first *selecting time*. To do this, either adjust the time position and use the **Set** options on this menu, or double-click and then shift+double-click in the header of the timeline view where the dates and times are displayed. Hint: first adjust the time scale factor to achieve an appropriate granularity of selection.

Note: The timeline view's idle timer does not run while the convert/export dialog is open or a single clip is open for playback in the viewer window.

TRIGGER SEARCH IN CLIPS

When triggered, cameras are typically configured to save alert images to the database which then may undergo AI confirmation. However, the *search-in-clips* feature allows you to run continuously-recorded video through the camera's motion detector and then optionally apply AI confirmation *after-the-fact*.

To begin, open a BVR video clip from the clips list into the Viewer window. Then use the search icon or find the option on the right-click menu.



You may choose to end the search when the next trigger is found. The start and stop crop icons will have been automatically adjusted. From here you may review the video, export the video segment, or create a clipboard entry using the clipboard icon.

For batch functionality, you may select to have the triggers added to the clipboard automatically or to the alerts list directly. If you have a set of clips displayed from a particular camera and date range, you may apply the search to all clips in the list by selecting the **Auto-advance to the next clip** option.

A dual-streaming camera's motion detector *zone* settings apply to its sub stream video. If you have dual-stream clips, you should first right-click in the viewer and select to **Use sub stream -> Always** if you plan to search specific zones. You may search using the main stream, but zone filtering may not be functional.

When selecting AI confirmation, the camera's AI settings will be used by default, but you may override them here. CodeProject.AI or Deepstack must be installed and operational.

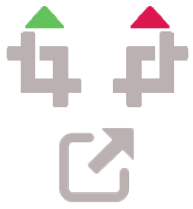
You may also or instead **Analyze audio for volume, frequency and patterns**. This works similarly to the camera's audio triggering functionality and uses the same Audio Analysis configuration window.

As with normal motion detector operation, a frame is analyzed each 512msec. When motion is detected, this becomes 128msec, and frames are also analyzed by the AI. For confirmation, AI objects must overlap areas where motion is also detected and must match the **confidence** and **to confirm/cancel** selections.

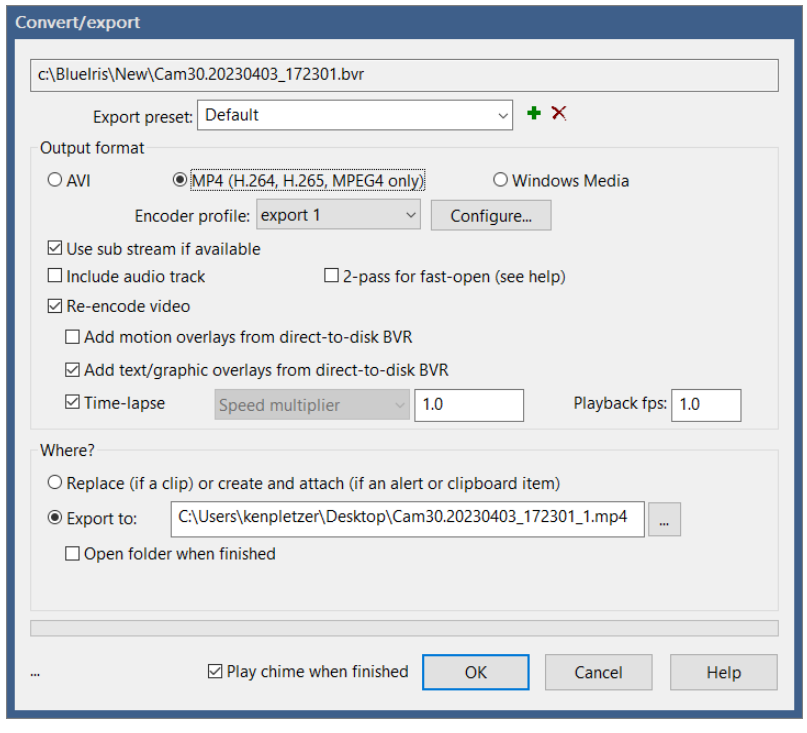
When saving directly to the Alerts list, JPEG files with optional AI markup are saved to the Alerts folder based on the associated camera's current settings for these.

Use the Esc key or manipulate the speed or position sliders in any way to stop the search. This feature is not yet available over Remote Management.

TRIM, CONVERT, EXPORT



With a BVR clip open in the viewer, you may optionally use the green and red crop icons to set the beginning and ending position for trim or export. For a more precise frame selection, you can instead right-click in the viewer window and use the **Set start frame** and **Set end frame** options. Then use the Export button found at the top-left of the viewer window:



Use an **Export preset** to memorize the settings used on this window for quick recall in the future. To create a new preset, enter its name and use the + button.

The **Output format** may be one of **AVI**, **MP4**, or **WMV** (Windows Media). Microsoft has largely deprecated AVI and WMV. In order to share your video with others, you should select **MP4**.

If the BVR file was captured after version 5.3 with a direct-to-disk and a dual-streaming camera, it will actually contain TWO video streams—the *main stream* and the *sub stream*. Decoding the main stream is much more CPU intensive, so the sub stream should be used whenever the full resolution is not required.

Using the **2-pass for fast open** option for MP4 files makes the MP4 easier to use on a web server and may make it easier for an OS to generate a preview image. However, this feature may make the file incompatible with some players.

It is necessary to **re-encode** the video:

• if the source file contains MJPEG instead of MPEG4, H.264 or H.265

- if you will be using the time-lapse feature
- if you wish to add the camera's text and graphic overlays which were not recorded due to use of *direct-to-disk* recording
- if you require a more precise start time and the trim position is not at the beginning of the video, due to the fact that recording (and export) may only begin on a key-frame boundary
- if you desire to change the frame size or the video quality
- when exporting video from the timeline

Re-encoding however will be much slower and CPU intensive than exporting otherwise.

A **time-lapse video** may be created if you select to **re-encode** but do *not* select to include the audio track. You may directly choose the target relative playback speed as well as the maximum frames/second for playback.

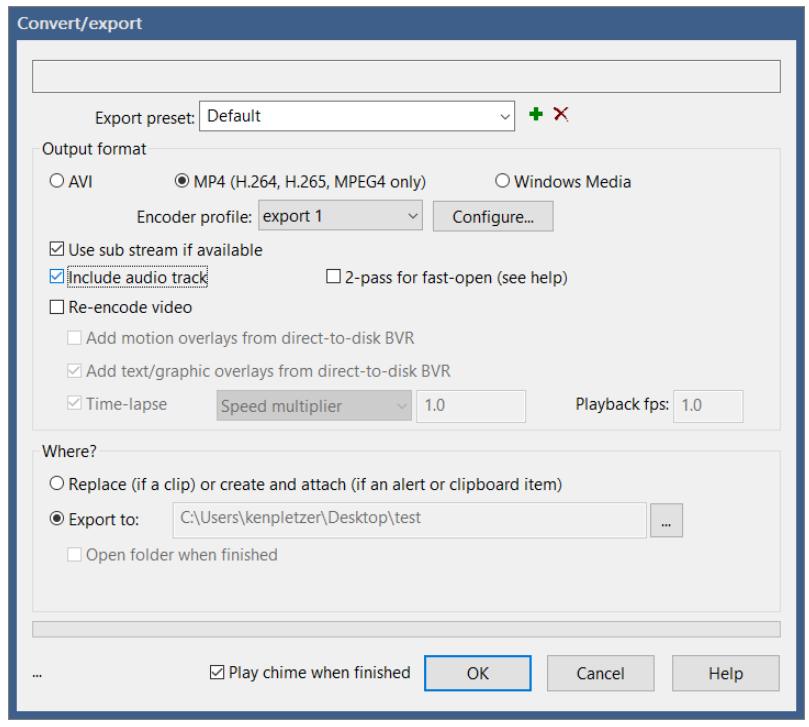
Output file

When exporting from a clip found on the clips list, you may select to either replace the current file or to create a new one. When you replace the file, the original file in the clips list database will be replaced. It's worth noting that any alert images associated with the clip will likely lose their ability to accurately point to positions of interest in the clip.

When you create a new file, this should generally be to a location *outside* of any folder that's managed by Blue Iris. If you do choose a Blue Iris folder, it will be inserted into the database at the time position corresponding to the first exported frame.

Batch export

To batch convert/export one or more BVR clips, first select them on the clips list, and then right-click to select *Convert/Export* from the popup menu:



You can display a list of clips waiting for batch export by right-clicking in the clips window and selecting *View—>Convert/Export queue*. It should be possible to remove items from this queue if necessary by selecting and using the *Del* key.

Please note that the Convert/Export queue currently has a single export folder setting. If you select additional clips for export and change this folder, you will be changing the folder that's used for the remainder of the clips in the queue.

Convert with folder move

With an option on the Clips page in Settings, you may select to automatically add clips to the Convert/Export queue as they are moved between folders as part of clip folder and database maintenance.

The same restrictions apply to this as with manual batch export. Note that if you are not replacing the original files, there is a single export folder for the queue at any one time.

MP4 and AVI playability

Many Windows systems are not properly configured to playback MP4 files. Furthermore, AVI files created here have H.264 video content, which may have the same issue. A popular and recommend package to install that will allow a Windows systems to play these files is available here:

https://www.codecguide.com/download_kl.htm

Only the *basic* install is required, without additional software it may attempt to install.

Timeline export

You may export from the timeline if you first enter timeline playback and *select time*. Time may be selected using options on the right-click context menu, but you may also double-click in the timeline header—once to set the starting time and then again while holding the Shift key to set the ending time.

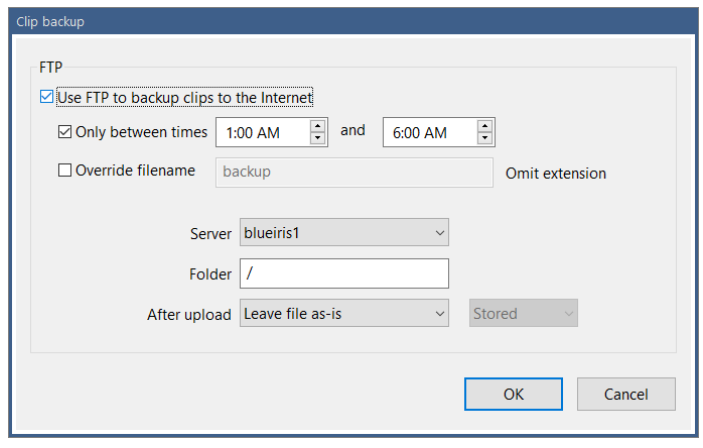
When exporting from the timeline you may use a time multiplier, or you instead may select a specific frame interval in seconds, minutes or hours. This allows you to create a video which spans clips potentially over multiple days.

FTP CLIP BACKUP

The clips list maintains a queue of clips to be uploaded to an FTP server of your choice. Clips in this queue are marked with a cloud icon which will turn green when upload is complete. You may view and edit this queue by right-clicking in the clips window and selecting *View—>FTP backup queue*.

Clips may be automatically added to this queue as soon as they are closed by the camera using an option on the Record page in camera settings. You may also add them to the queue manually using a right-click option in the clips list. Finally, clips may also be added to this queue as they are moved between folders by the clips and database maintenance operation.

To edit the designation server and other parameters for this feature, use the Configure button to the right of the Queue for backup checkbox on the Clips page in Settings. This Configure button is used for all clips in the queue regardless of whether or not you are using the Queue for backup function on the Clips page.



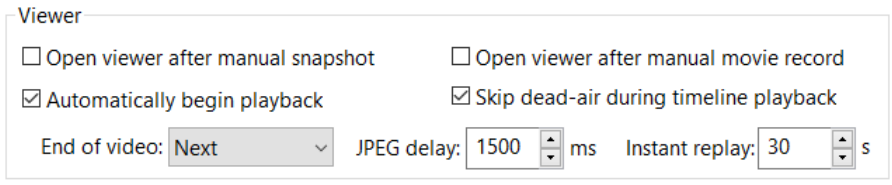
You may enable or temporarily disable the queue here. You may select a time range during which the queue may operate.

By default the filename used will be the clip's same filename from the clips folder. You may instead specify another format. Time formatting codes may be used to prevent filename conflicts—please see the complete list found at the end of the Alerts and Actions chapter.

If a destination folder is not specified, the FTP server's default folder is used. If the folder specified here begins with a / (forward slash), this is considered a root or **absolute** folder from the root. Otherwise, the folder is **appended** to the server's default folder.

GLOBAL VIEWER OPTIONS

These are found on the Other page in Settings.



Upon use of either the Snapshot or Video buttons, the viewer window may be immediately opened.

You may select whether to **begin playback automatically** when a video is opened.

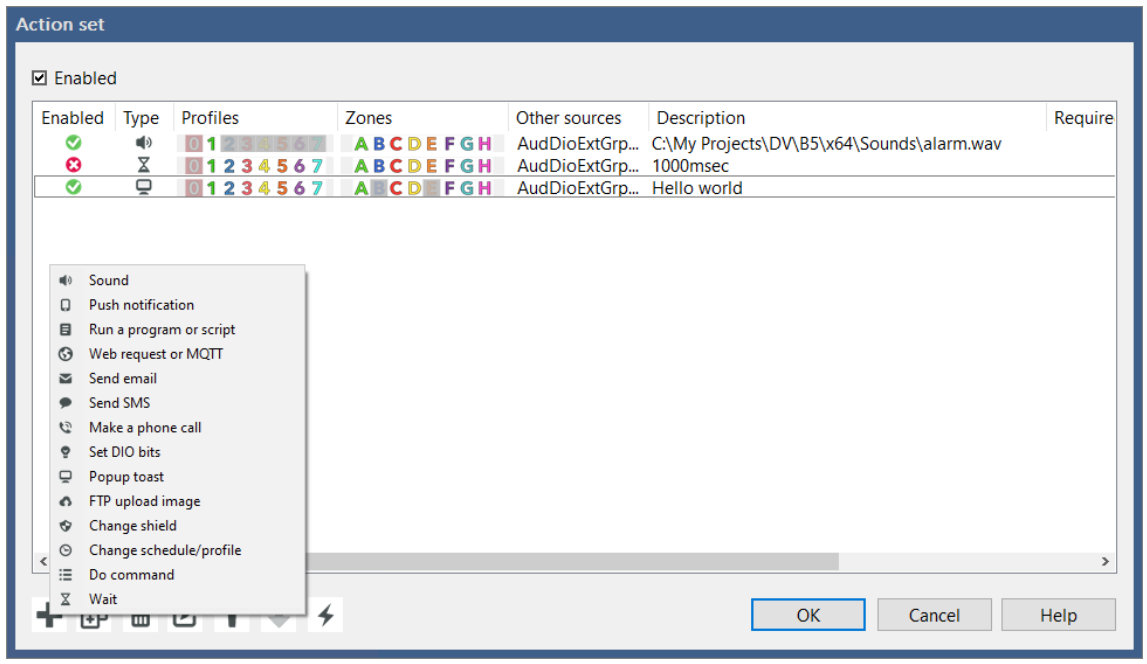
You may select what occurs at the **end of the video** as well, although this is also selectable via a right-click option in the viewer window as described under the *Viewer context menu* topic. If your clips list contains JPEGs, you may define the time to display the JPEG before advancing to the next clip. This happens automatically after advancing from a video, but the Play and Pause buttons also may be used while a JPEG is open in order to start and stop the automatic slideshow.

For timeline playback, it's possible to have the software recognize large portions of time where "nothing is happening" and to automatically move forward to the next event or clip by enabling the **Skip dead-air during timeline playback** option.

The **Instant replay** setting determines how far back in time to begin timeline playback when the instant replay button is used in the timeline view.

ALERTS AND ACTIONS

In response to a camera trigger or other alert, you may define a set of actions to be executed.

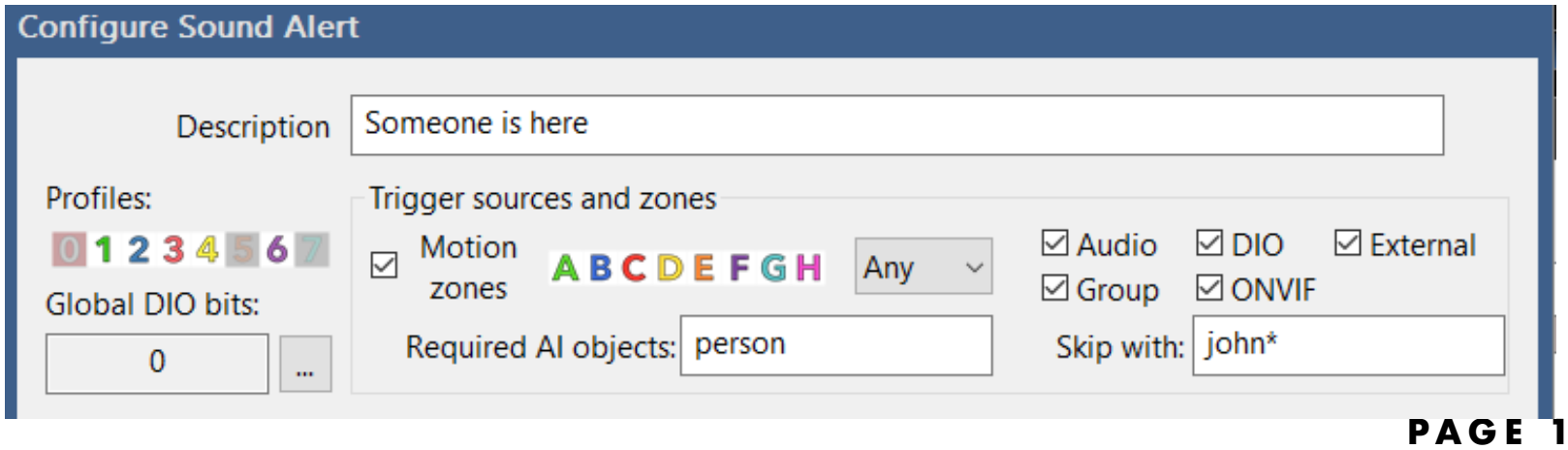


Action items on this list are executed in order from top to bottom. Alerts of different types may execute simultaneously however. That is, push notifications, sounds, and emails execute in order, but these all have separate queues and threads.

The action set will be executed only if the Enable box is checked. Each action item also has associated enable and profile controls, and that action will only be executed if the active profile matches one of the control's selected profiles. See the profile control in the main window UI and the chapter on Schedules and Profiles.

CONDITIONS

You may set required conditions for each action. Select active profiles, required global DIO input bits, trigger sources, motion zones, as well as **Required AI objects** (comma delimited) if you are using AI. You may also specify AI objects which will cause the action to be **skipped**. You may specify the minimum confidence % for any label by appending a : and a number to the label, for example *person:80*.



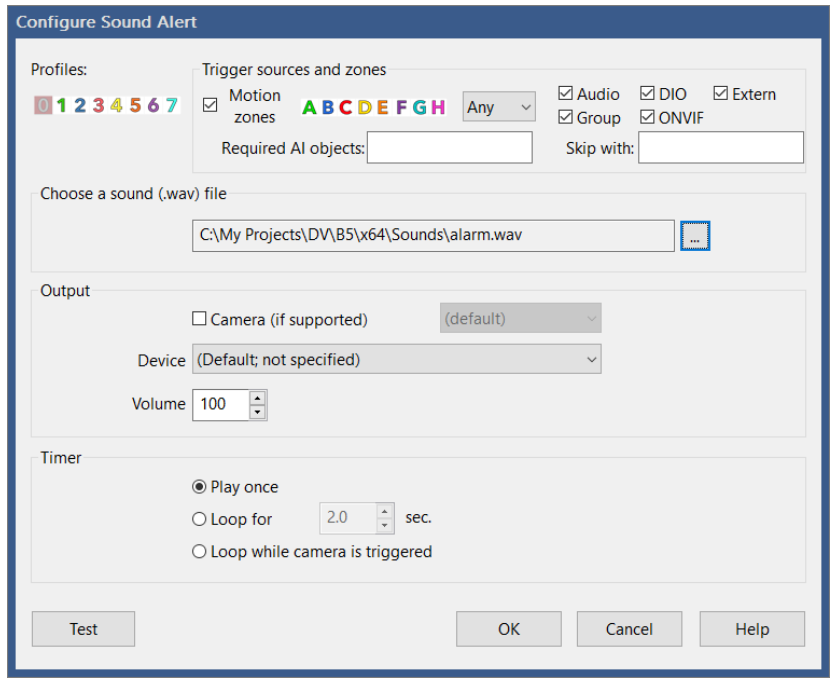
One or more PTZ preset positions may also be specified along with any AI objects in the required and skip boxes. Use the format P*n* where *n* is a PTZ preset number 1 or greater.

You may combine two labels with "and" logic by using a +, for example, car+licenseplate. In this case, the confidence may only be overridden for the combination, such as car+licenseplate:80. You can even specify a combination of PTZ presets and AI objects. For example, P1+person, requiring that a person is detected while the camera is focused on PTZ preset 1.

If you are using license plate recognition, plate numbers may also be added to the AI objects **required** and **skipped** boxes. Use the special labels **myplates** and **notmyplates** to reference all known or unknown plates as specified on the Settings/AI page.

SOUND

Perhaps the most basic action, play a sound file. The file should be in standard Windows WAV format, but the sampling rate and channel layout should not be a concern.



Output

For camera trigger alerts, you may choose to send the sound to the camera speaker instead of the PC speakers. This is only possible if you have “talk” to the camera working beforehand. 2-way camera audio is not a standardized camera function, which means it is only supported for a subset of cameras.

For playback to the PC speakers, the device setting should generally remain “not specified.” You may attempt playback to another audio device connected to the PC by selecting it from the device list.

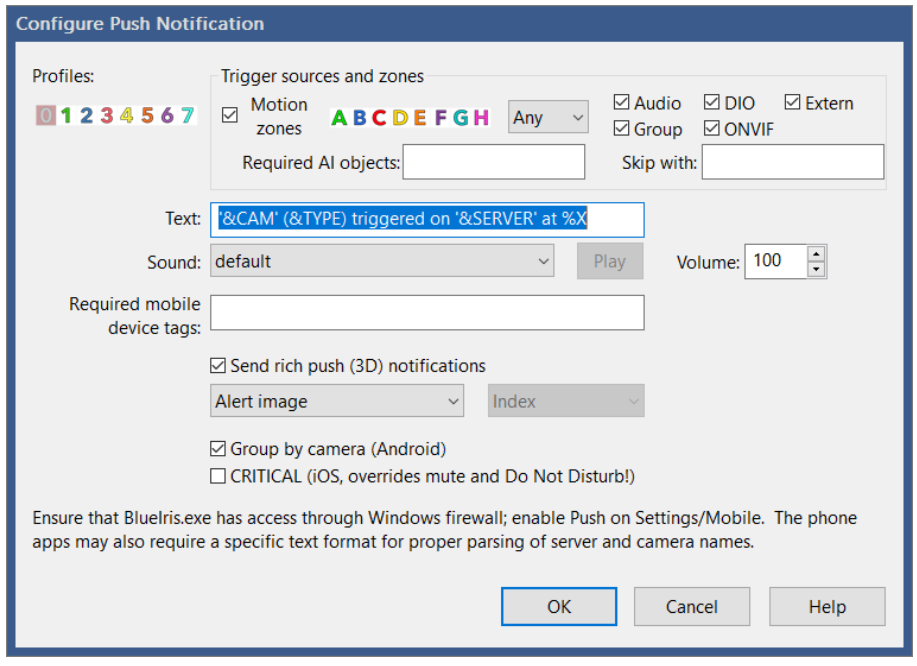
Use the volume setting to change the playback volume by percentage. A value of 100 is full volume.

Timer

You may select to loop the file for a specified duration, or select to loop the file only while the camera is triggered. Otherwise, the sound file will be played just once.

PUSH NOTIFICATION

Push notifications require either an iOS or Android device with the installed and configured Blue Iris app.



As long as you are on a recent version of the app, it is no longer necessary to retain the default text format with its parentheses and apostrophes—you may alter this as you require.

You may specify any of the 50+ sounds that have been pre-installed on both the PC software and the apps.

If you would like to send this notification to only a subset of connected mobile devices, you may specify one or more "tags." Separate multiple tags with semicolons. A mobile device must have any one of the specified tags in order to receive the alert. Please see the Mobile devices tab in Settings. Leave this box blank to send to all mobile devices.

The *last user* of the device is also significant. The push will only be sent to a device whose last user has access to receive push notifications during the active profile and from the alerting camera.

The option to **Send rich push (3D) notifications** allows you to send a camera image along with the text. You may choose to send either the alert image (if this action is in response to a trigger) or the camera's current image. Further with iOS (not Android at the time of this writing), it's possible to send a short 10-image GIF movie instead of the JPEG.

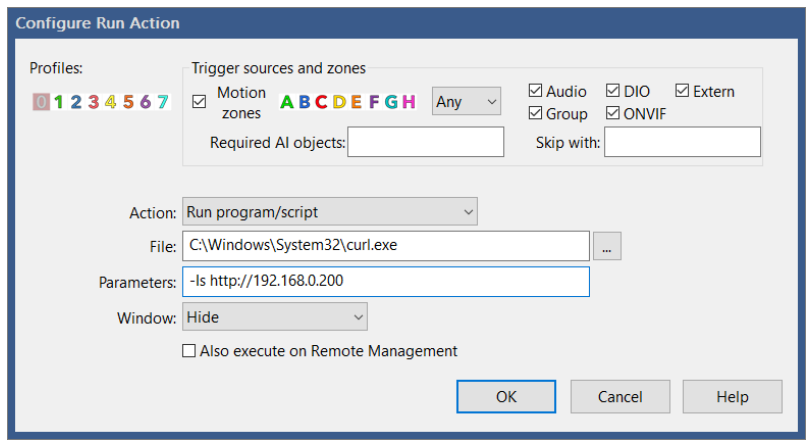
To combine same-camera notifications on Android, select **Group by camera**.

Select **CRITICAL** alerts for iOS with caution. This gives Blue Iris the ability to override the mute and "do not disturb" settings on the device. This must also be enabled/approved in Settings/Blue Iris/Notifications on the device.

As the notification is sent via contact with either an Apple or Google web server, you must ensure that the BlueIris.exe file has access through any firewall or other security software. In addition, as notifications to Apple require a security certificate that's renewed annually, you should always ensure the software is up-to-date to retain this functionality.

RUN A PROGRAM OR WRITE TO A FILE

You may select any executable (generally .EXE) or batch (Windows .BAT script) file to be executed.



Parameters may be used as required by the file that you specify. For example, you may send the camera's short name to a script by specifying &CAM.

Change the **Action** to **Write to file** (either append or replace) if you want to instead write the **Parameters** to a file. You may use \r and/or \n which will be substituted for carriage return or line feed respectively.

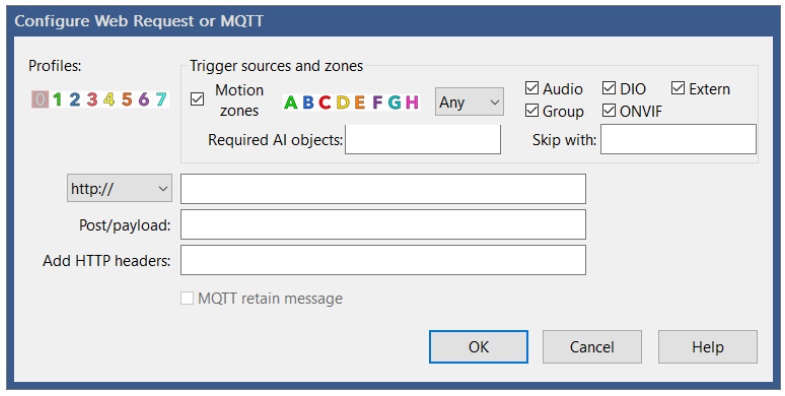
The Windows interface of the program or script may either be hidden or displayed as desired.

When Blue Iris runs as a service, the window will always be invisible as the service runs "in the background" without UI. You should also be mindful that the service may not have access to your file's drive specification or access to run it. To overcome this, you should run the service with your own Windows login rather than Local System.

Select to **Also execute on Remote Management** in order to send this alert to all connected Remote Management clients.

WEB REQUEST OR MQTT

This action is really two-in-one. Select HTTP or HTTPS to request or post to a specified web address. Select MQTT to send a payload of text to an MQTT server.



For HTTP or HTTPS requests, you must omit the http:// or https:// in the address box. HTTP GET semantics will be used if the post/payload box is empty, otherwise POST semantics will be used. You may specify additional HTTP headers—separate multiple headers with \n, for example

Authorization: Bearer ABCDEFGH

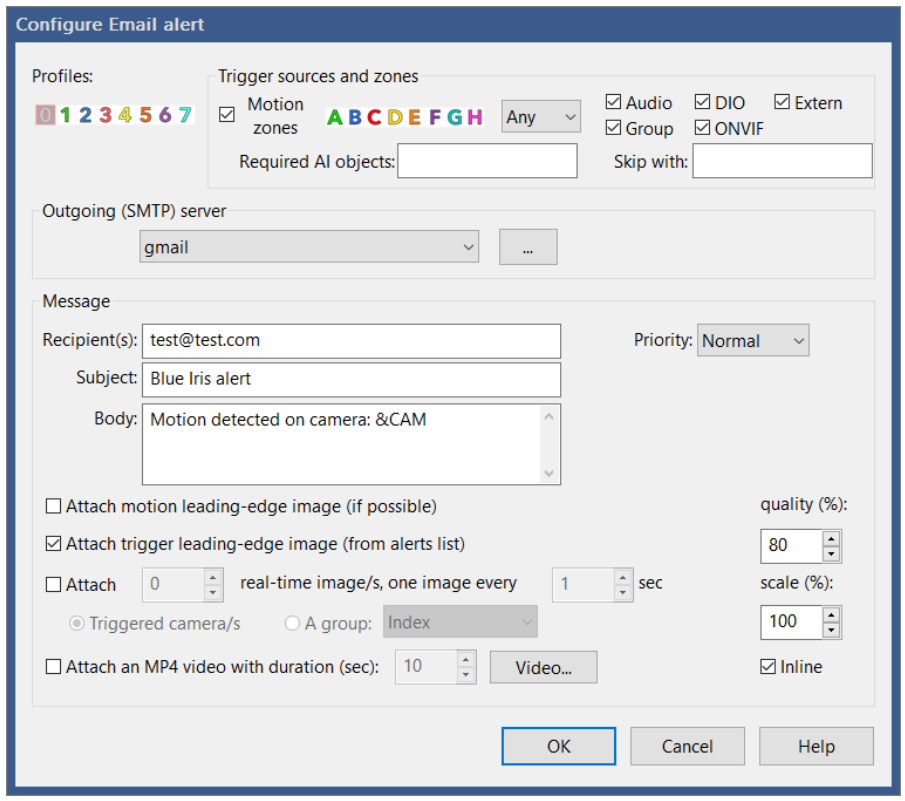
Authorization: Bearer ABCDEFGH\nX-My-Custom-Header: test

For MQTT requests sent to the topic BlueIris/admin, possible payloads are identical to those offered by the web server /admin interface, documented in the Administration chapter. The **retain** option causes the MQTT broker to cache the last message on each topic to be delivered to any client which may connect.

Please see the list of macros at the end of this chapter which may be used in the payload.

SEND EMAIL

Use an SMTP server such as Gmail to send yourself a message.



Outgoing server

You may configure multiple SMTP email servers. Please see the chapter on Email and FTP servers for more information on how to properly use Gmail or another service. There is no need to “enable less secure apps” when using these services if properly configured.

Message

As you may be familiar with other email clients, you may specify Priority, Recipients, a Subject and Body for your message. In order to send a message to multiple people or devices, you may either specify multiple recipients here each separated by a semicolon, and/or add multiple email actions to the action set.

Please see the list of macros at the end of this chapter which may be used in the subject or message body.

Attachments

Including images or a video from a camera is only applicable for camera trigger action sets. Otherwise, you may include group images.

A motion leading-edge image is captured when the camera is transitioning from a non-motion to a motion state. This image occurs at the “make time” amount of time before the

camera is actually triggered, possibly providing additional insight into the cause of the trigger.

A trigger leading-edge image is captured when the camera actually enters the triggered state. This is the “alert image” as it is saved to the database with a reduced resolution unless you have chosen to save alert images as hi-res JPEG files on the camera settings Trigger page.

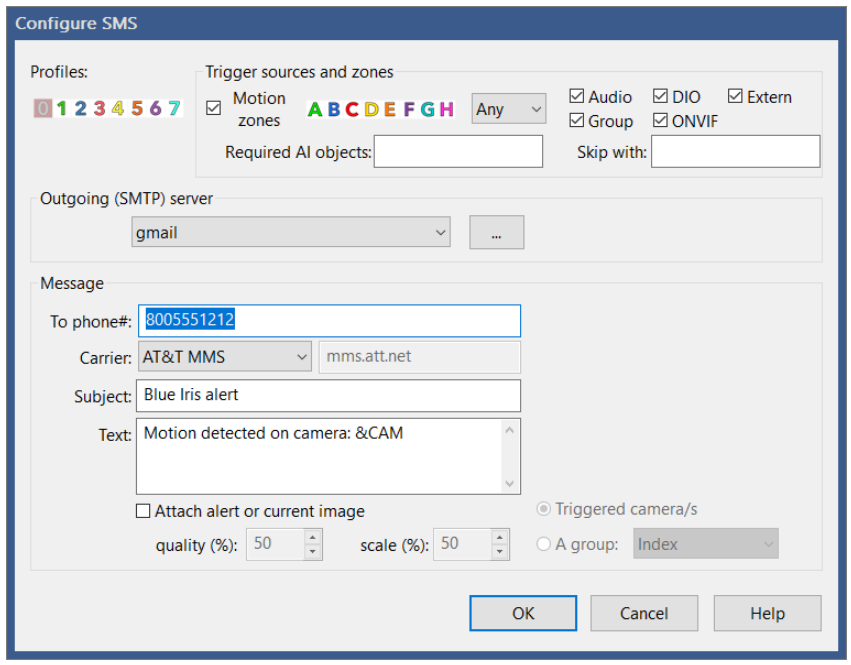
In addition to motion leading-edge and trigger leading-edge (alert) images, you may specify a number of additional real-time images, each spaced by a number of seconds.

You may select image quality and scale (in percentage) as well as advanced video encoding properties such as bit rate and key frames.

“Inline images” are an alternate way to attach images to email messages. They should appear in the body of the message rather than as attachment icons.

SEND SMS

This action is like a hybrid between the Email and Push notification actions. It's not necessary if you are using one of the phone apps available for iOS or Android—use Push notification instead.



To send an SMS, Blue Iris must send an email to your phone carrier's "gateway" address, and not all carriers have such a feature. You must first configure and have working an outgoing email server, please see the chapter on Email and FTP servers.

The email that is sent goes to (your phone number)@(your carrier's gateway). Using any other email client, you may test this outside of Blue Iris to verify function and compatibility. Many popular carriers are are preconfigured for you, however if your carrier is not listed, you may select "other" and manually specify the gateway domain which you have obtained from them.

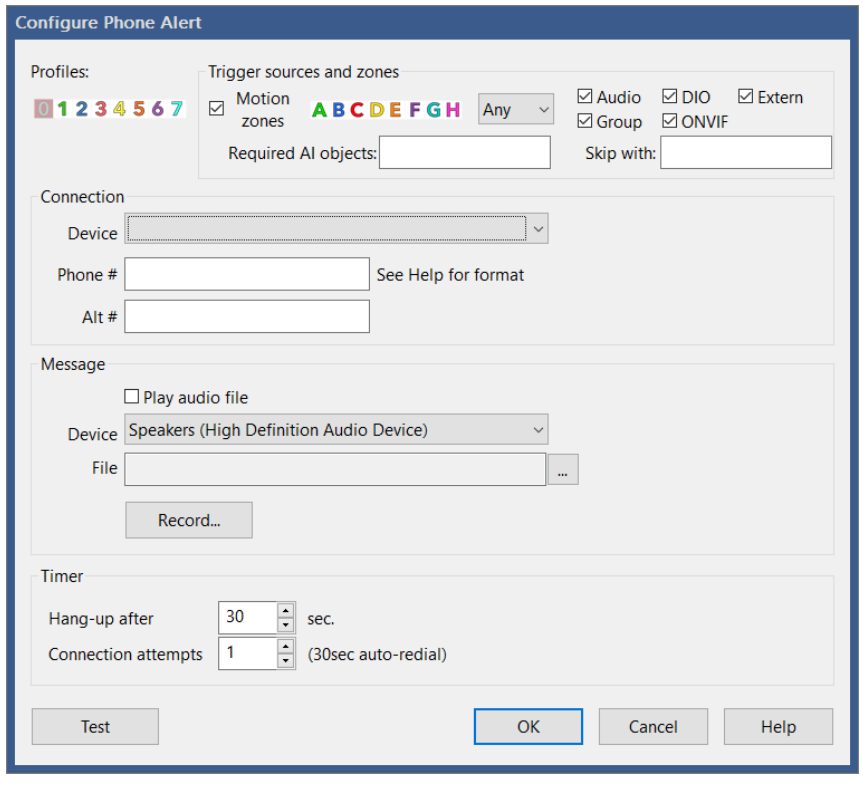
Please see the list of macros at the end of this chapter which may be used in the subject or message body.

Although more limited, you may choose to attach images of specific quality and scale as you may with the Email action.

Please be advised that some carriers (T-Mobile) have been known to block messages and accounts which send messages that include "spam" words such as **Alert, Info, Test, Contact, Us, Sales, Webmaster or Item**. Please avoid these in your SMS subject lines or body text.

MAKE A PHONE CALL

This action is somewhat deprecated, as it requires specialized hardware which may be difficult to source and configure. A PC modem with a connection to your sound card and a TAPI hardware driver are required. Such hardware is used for “answering machine” applications as well as “robo calling.”



Connection

The TAPI device will appear only if properly configured in hardware and OS. The phone number may include special formatting characters as used by your modem to indicate pauses for example. A second alternate phone number may be specified—the software will alternate between the two numbers until a connection is established.

Message

If you would like to hear a message when the call is connected, you may specify a standard Windows WAV sound file. The option is provided here to record a compatible file using your default Windows microphone.

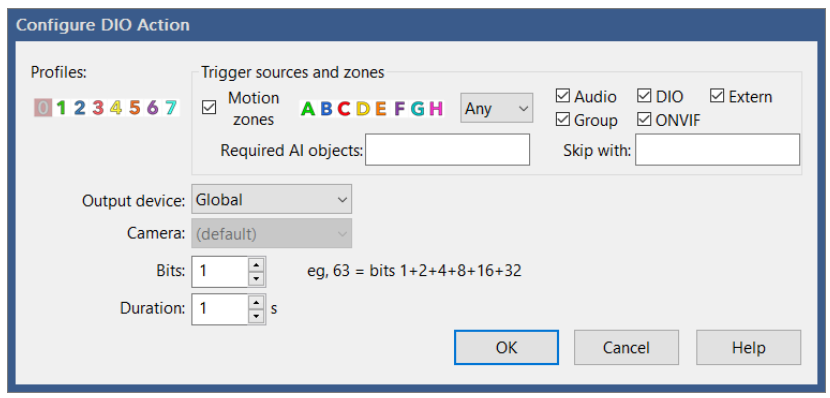
The device specified is for your sound hardware which will have a cable (internal to the PC) running from the sound card to the modem.

Timer

You may specify the duration of the phone call, as well as the number of total attempts made to make a connection. If the line is busy, a pre-set 30 second timeout is used between re-dials.

SET DIO BITS

DIO or Digital Input and Output provides a powerful way to interact with external hardware. The DIO device may be connected by USB, Ethernet, or may be internal to a camera. Please see the Digital I/O and IoT topic in the More Options chapter.



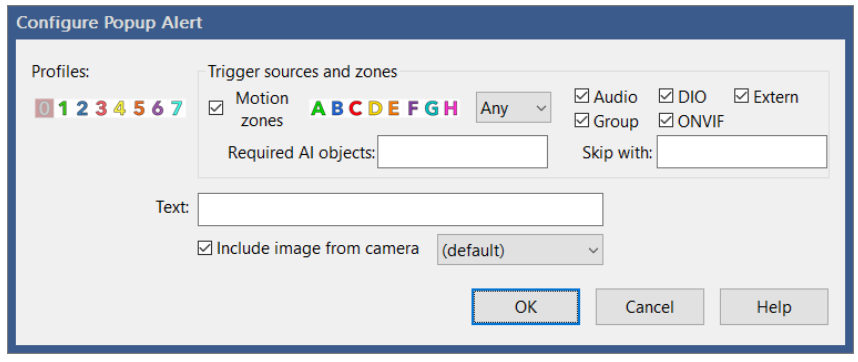
The output device may be set to Global or Camera. The Global DIO device is set on the DIO and IoT page in Settings. Many cameras however also offer DIO input/output terminals which may be used instead. Blue Iris must support the use of camera DIO based on its PTZ/control setting.

When the DIO device offers multiple output terminals, each output is addressed as a “bit.” The first output will have a value of ‘1’. Subsequent outputs follow in powers of 2, that is, 2, 4, 8, 16, and so on. When setting multiple outputs simultaneously, the bit value will be the total of these powers of 2. For example, to set the 1st and 4th outputs, specify a bit value of 9 (1+8).

Specify the duration in seconds to hold the output active. When the timer expires, the output(s) are reset.

POPUP TOAST

Recent versions of Windows include “notification popups” otherwise known as “popup toast” messages.

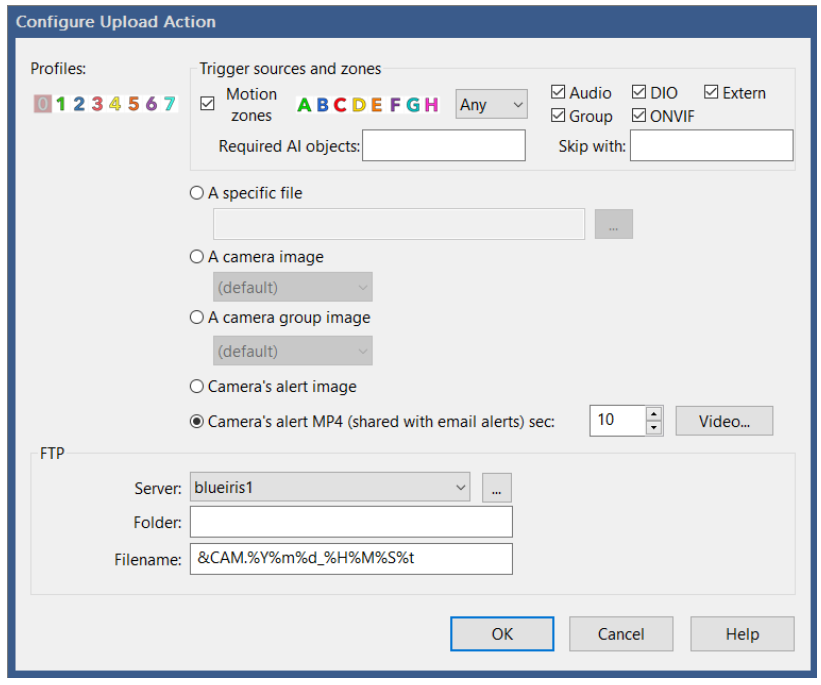


You may specify the text to be displayed along with the inclusion of a current camera image.

It is only possible to display these images if the console is open—when running as a service the software does not otherwise have a UI. However if you are connected to a server using remote management, that server’s popups will be displayed locally.

FTP UPLOAD

You may use a pre-configured FTP server to send a specific file, a camera image or a group image.

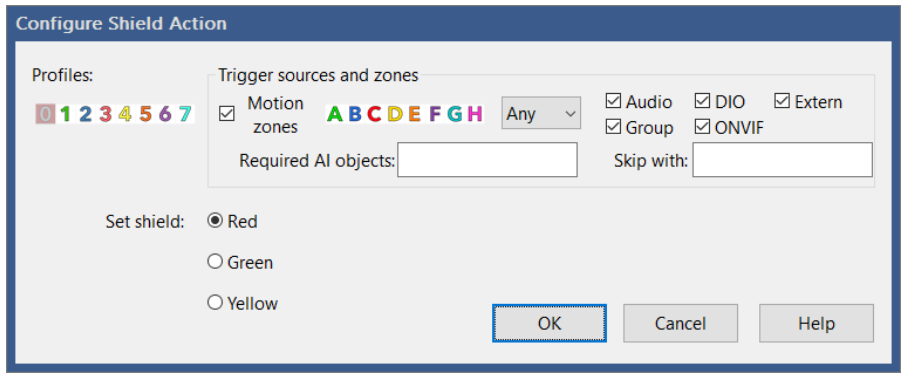


If a destination folder is not specified, the FTP server’s default folder is used. If the folder specified here begins with a / (forward slash), this is considered a root or **absolute** folder from the root. Otherwise, the folder is **appended** to the server’s default folder.

Please see the chapter on Email and FTP servers for more information on configuration of the FTP server.

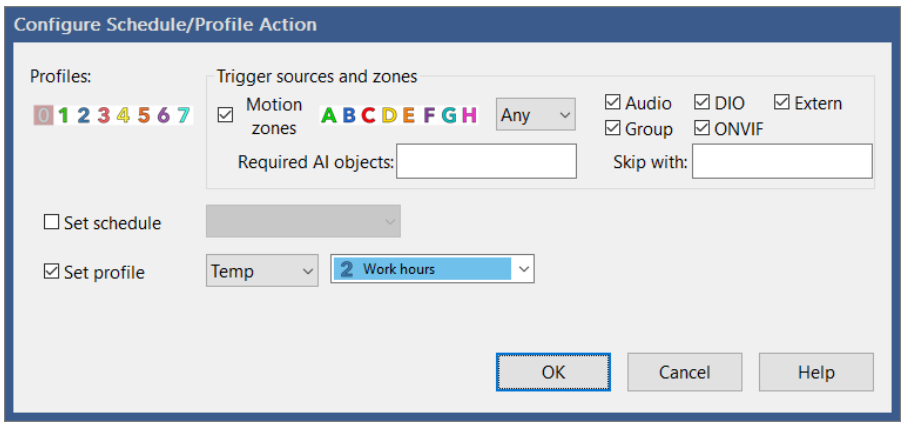
CHANGE SHIELD

The Shield icon at the top of the main window UI may be set here. In general a green shield indicates normal operation, recording and alerts. A red shield indicates an inactive state—no recording or alerts. Yellow is a transition state from red to green. The specific function of the Shield may be configured on the Other page in Settings.



CHANGE SCHEDULE/PROFILE

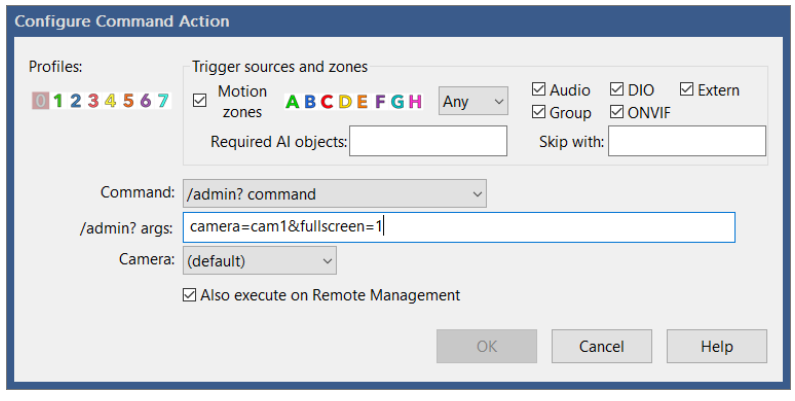
The current schedule and profile are also displayed at the top of the main window UI alongside the shield icon. Please see the chapter on Schedule and Profiles for descriptions of these settings.



The profile may be set to Hold, Temp, or Run. When set to Hold, the profile will not change again until it's done manually or the schedule is changed—a red square icon appears to the right of the profile selector at the top of the UI. When set to Temp, the profile will reset to the scheduled profile after a time specified on the Profiles page in Settings—a yellow pause icon appears to the right of the profile selector. When set to Run, the selected active profile is determined by the active schedule and time, not by the profile selection here.

DO COMMAND

Many commands and functions available as buttons throughout the software are available for selection here. For example, you can take a snapshot on a camera or move its PTZ preset position.

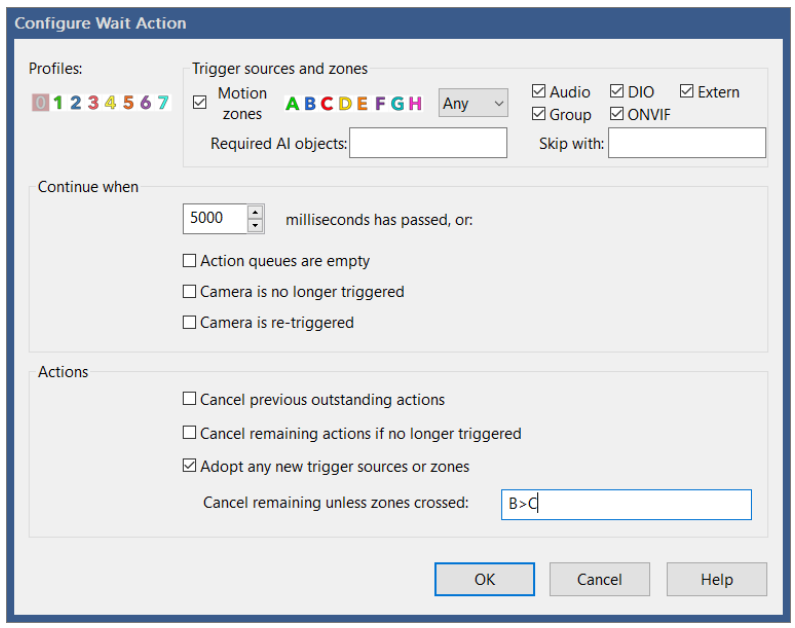


Select the **/admin? command** option to execute any arbitrary command available through the /admin HTTP interface as documented in the Administration chapter.

Select to **Also execute on Remote Management** in order to send this alert to all connected Remote Management clients as well.

WAIT

This action exists to provide some synchronization between other items on the action set list. As execution queues exist separately for each action type, they may execute simultaneously. If you want to send an email message and then wait before a push notification is sent, it will be necessary to add a Wait action in-between the other two.



By default, the action set continues after a specific time duration has elapsed. The time is specified in millisecond (1/1000 second) units—use 2000 for 2 seconds.

For synchronization among the actions, you may choose to wait until any previous actions have fully completed before continuing. You may also wait for the camera to be *re-triggered*, that is, triggered again while still in the triggered state.

When the wait is over, you may choose to cancel anything that's been queued but not yet executed. You may also choose to cancel the remainder of the action set if the camera is no longer triggered.

By default, the action set adopts the camera's trigger sources and motion detection zones at the beginning of the trigger. For the remainder of the action set, you may choose to use any new sources or zones that were added to the trigger during the time of the wait. You may choose to only continue the action set if specific zone crossings have occurred. The syntax used here is identical to that of the zone crossing feature of the motion sensor.

One possible use case would be to send escalating alerts as the camera remains triggered. For example, if a door is opened, maybe play a chime. If the door is held open for 10 seconds, sound an alarm; if open for 30 seconds, call the police, etc.

TIMECODE AND OTHER MACROS

Several actions allow the use of macros—variable text that is substituted based on context or pre-set elsewhere.

Macro	
&AIMSEC	The number of milliseconds required for the AI inference on the current alert.
&ALERT_DB	The DB record locator for the most recent alert image for the camera.
&ALERT_CLIP	The DB record locator for the most recent alert image's clip for the camera.
&ALERT_JPEG	For MQTT/web requests, a base-64 encoded JPEG corresponding to the Alerts list image
&ALERT_PATH	A temporary path to the most recent alert image on the camera
&ALERT_TIME	The alert record's creation time in ISO8601 format
&CAM	Camera's short name
&FILE	The path to the currently recording clip on the camera
&IMAGE_PATH	A temporary path to the most recent image from the camera
&JSON	Raw JSON return from AI object detection that either confirmed or canceled the alert
&LAN	The current system LAN address as shown on the Settings/Web server page
&MEMO	The alert's AI findings, e.g., person:81%
&MOTION_RECT	The coordinates of a rectangle enclosing the motion [left,top,right,bottom]; values are normalized 0-1.
&NAME	Camera's long name
&PLATE	License plate captured with ALPR if configured
&PRESET	The most recently used PTZ preset on the camera
&PROFILE	The active profile number
&SERVER	The system name as set on the Settings/About page
&TYPE	The source of the camera trigger, for example MOTION_A, EXTERNAL, or DIO. The letters following MOTION refer to the motion zones.
&WAN	The current system WAN address as shown on the Settings/Web server page
%x, %X, etc.	Date and time. See the table below for a full list of time formatting macros.

Standard time formatting macros

Macro	
%a	Abbreviated weekday name
%A	Full weekday name
%b	Abbreviated month name
%B	Full month name
%c	Date and time representation appropriate for locale
%d	Day of month as decimal number (01 – 31)
%D	The English ordinal suffix for the day of the month (2 characters st, nd, rd or th. Works well with j)
%H	Hour in 24-hour format (00 – 23)
%I	Hour in 12-hour format (01 – 12)
%j	Day of year as decimal number (001 – 366)
%m	Month as decimal number (01 – 12)
%M	Minute as decimal number (00 – 59)
%p	Current locale's A.M./P.M. indicator for 12-hour clock
%S	Second as decimal number (00 – 59)
%t	Milliseconds as decimal number (000 – 999)
%T	The current time in ISO8601 format
%U	Week of year as decimal number, with Sunday as first day of week (00 – 53)
%w	Weekday as decimal number (0 – 6; Sunday is 0)
%W	Week of year as decimal number, with Monday as first day of week (00 – 53)
%x	Date representation for current locale
%X	Time representation for current locale
%y	Year without century, as decimal number (00 – 99)
%Y	Year with century, as decimal number
%z, %Z	Time-zone name or abbreviation; no characters if time zone is unknown
%%	Percent sign

You may place a # character immediately following the % to eliminate leading zeros in many of the formatting codes. For example, %#H will show 9 at 9am instead of 09.

Time Zone Correction

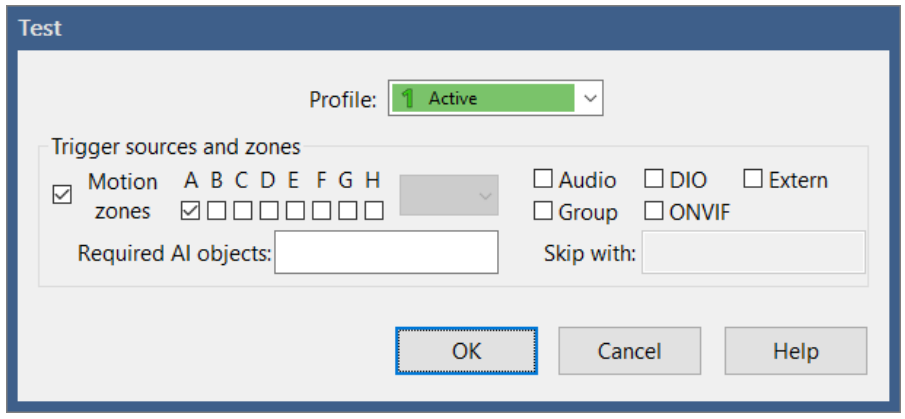
For time zone correction in a text object overlay, add the special sequence {+n} to the beginning of the string, where n is a number 1-23, and the sign is either + or -. For example, a text overlay of **{+3}%c** will display the time 3 hours ahead of local time.

Additional special macros

Macro	
%1-9	A numbered macro defined on the Macros page in Settings
%10-999	Additional macros defined in REGEDIT key: HKEY_LOCAL_MACHINE\SOFTWARE\Perspective Software\Blue Iris\Macros
%000	The system name as set on Settings/General
%001	The camera's current alert 'memo'
%002	The camera's current alert license plate
%003	The camera's currently active profile name
%004	The camera's currently active zone mask name
%005	A string with identifying camera details (login, IP address, ports)
%006	The camera's current FPS on the main stream
%007	The camera's current bit rate in kB/s on the main stream (a kB here is 1024 bytes)
%008	The system's current WAN IP address
%009	The camera's current network address
%010	The system's current CPU usage %
%011	The current formatted amount of RAM used by Blue Iris
%012	Formatted system uptime (days:hours:minutes:seconds)
%013	Formatted system version (5.4.9.15)
%014	The current UN-formatted amount of RAM used by Blue Iris
%015	The camera's full name
%016	The camera's short name
%017	The system's current RAM usage %
%018	The system's current GPU usage %
%019	Sunrise time, local format
%020	Sunset time, local format
%021	Global schedule name
%022	The camera's current peak audio dB
%f	The camera's current FPS (sub stream if dual)
%k	The camera's current bit rate in kB/s (sub stream if dual) (a kB here is 1024 bytes)
%n	The camera's most recent PTZ preset position
%P	The camera's currently active profile number

TESTING THE ACTION SET

Use this icon to test your action set.



You may select test conditions including the current profile, the trigger sources and motion zones, as well as AI detected objects (comma delimited).

Upon completion, status and error conditions are displayed in sequence. You will be notified of the number of actions that were skipped because the profile, trigger sources, or motion zones prevented the actions.

Note that when testing, the action set runs in the *console* UI process. If you are running Blue Iris as a service in the background, "real" action sets run in the *service* process, and this can create discrepancies in what you experience:

- The service has no access to the Windows UI, meaning there are no visible windows.
- The service may have limited access to some hardware, which in some cases will include access to the sound card to play sounds.
- Popup toast actions will only appear when the console is open.
- The service by default runs as a user called "local service" which does not have the same access to the system as your user account. For most action types, it's recommended that you run the service with your own user account instead. This is changed by opening the Windows service manager (search for services) and edit the Blue Iris service entry Login page. See the Administration chapter for instructions.
- The service may not understand your file system designations like "H:" etc. as these are user-specific. You should always use UNC names where possible (\\server\share).

SHIELD, PROFILES AND SCHEDULES

Schedules and profiles allow you to change the behavior of the software based on the time of day, week, in response to an event, or arbitrarily. The shield icon and camera "pause" functionality are closely related, so all of these topics will be covered in this chapter.



THE SHIELD

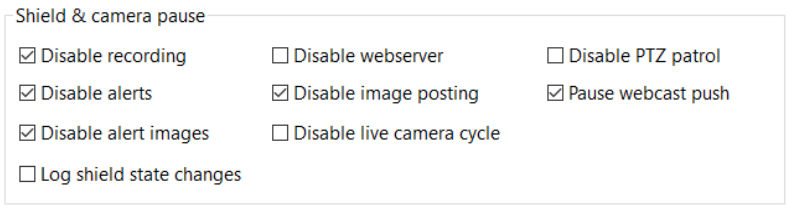


This icon represents the global "armed" or "disarmed" state of the software. When it's green, the software is "armed" and all functionality is enabled (unless otherwise overridden by something described below). When it's red, the software is disarmed.



A yellow state represents an automated transition from red to green, perhaps allowing you time to exit the building. The amount of time spent in the yellow state is determined by a setting on the Startup page in Settings. By default, the software starts up with the shield in the yellow state.

The specific functions which are disarmed may be adjusted on the Other page in Settings:





By default, recording, trigger alerts (actions), alert images (trigger database entries), image posting (camera Post page settings) and webcast "push" (as to YouTube or UStream) are disabled when the shield is shown as disabled.

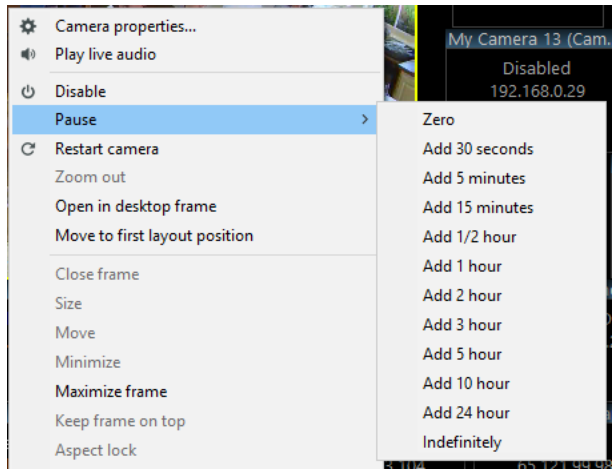
CAMERA PAUSE

When a camera is "paused" it is equivalent to using the shield icon, but on an individual camera rather than globally. When paused, the camera window's border will be drawn in light blue and a pause icon will appear in its header.



Unless the pause is indefinite, a countdown timer in minutes:seconds appears near the camera name in the header.

A camera may be paused or un-paused via a right-click menu:



It is also possible to change the camera's pause state via the client phone apps.

PROFILES

A profile defines a mode of operation or a configuration. Only one global profile is active at any given time (although it may be overridden on a per-camera basis as described below). The simplest use for profiles can be "day" vs "night" or "work hours" vs "after hours."

For example, using camera settings pages for Record, Trigger, and Alerts, you may configure profile 1 for recording and alerting on all motion, and profile 2 for recording only without alerts.

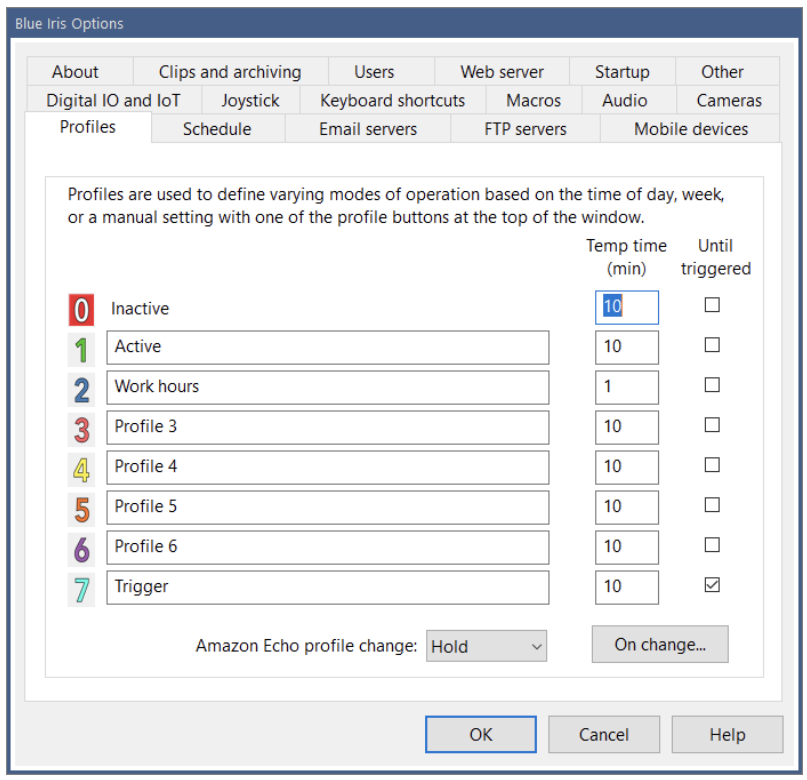
The original use for profiles in Blue Iris version 1 was to allow you to configure the motion detection differently based on the time of day. Generally at night, cameras operate in black and white, and trigger much differently than they do during the day. So in another example, you might use profile 1 for the night and profile 2 for the day.

Profiles may also be used arbitrarily—configure profile 7 perhaps to provide a sensitive trigger and to provide one specific type of alert. For example, you may be acutely or temporarily interested in someone entering through the garage and would like to receive a push notification for this, but then return to normal operation afterward.

There are 8 profiles, 0-7. Profile 1 is the default profile that will be used unless you otherwise change it with a schedule or override.

Profile 0 (the symbol ~ was used previously) has a special function, and is always called the "inactive" profile. When a camera's effective profile is profile 0, it is considered *inactive* and this is very similar to using the camera pause function or the shield icon globally. When inactive however, the camera does nothing but display live video—and even that can be disabled with a setting found on the Schedule page in camera settings.

You may rename the remaining profiles 1-7 on the Profiles page in Settings:



Each profile may be assigned a **Temp time**, a time to remain temporarily active before returning to the normally active profile (as defined by a schedule, see below). You may select that the temporary state is immediately canceled when any camera is triggered. Use a value of 0 in the **Temp time** field to **hold** the profile indefinitely regardless of scheduled profile changes.

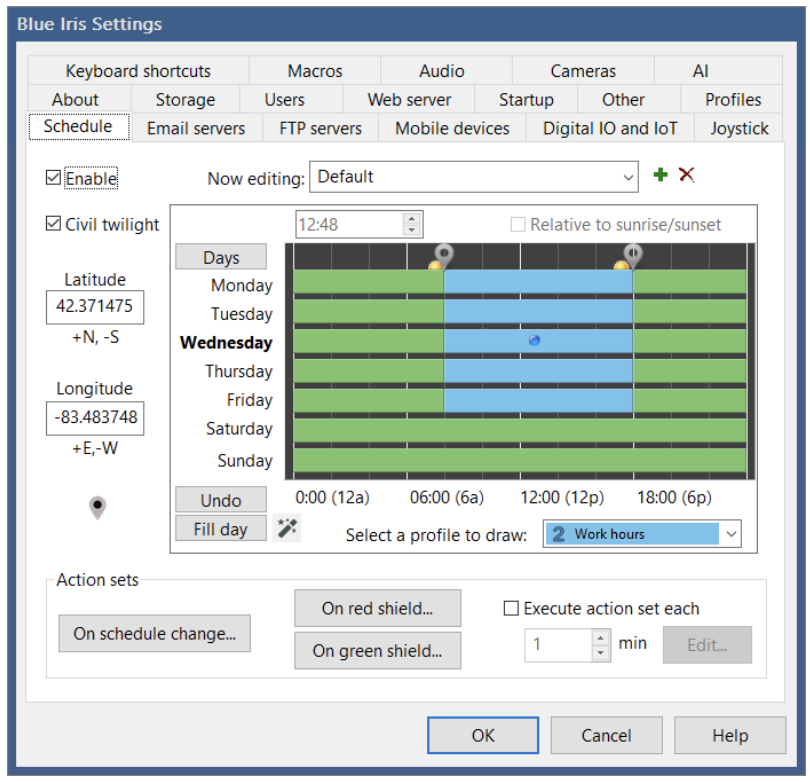
In the main window UI, a yellow pause icon to the right of the profile selection box corresponds to a **temporary** profile change, whereas a red square icon is used for **hold**.

A Beta Amazon Echo integration may be able to change the active profile, and you may be able to select a temporary or indefinite (hold) state.

Use the **On change** button to define an action set for execution whenever the active profile is changed.

SCHEDULES

A schedule is used to automate the active profile based on the time of day and/or week. If there is no active schedule, profile 1 is considered to be the active profile 24/7.



You may define a number of schedules. Common uses for schedules are for differing times of the year, such as vacation, summer, winter, etc.

A schedule is created by drawing it. You may pick any color (profile) to draw, and then click and drag anywhere in the schedule window to draw a filled rectangle in the selected color (profile). You can do this over and over again as required, but it's not necessary to be precise in your drawing, as you can easily adjust the start/stop times in other ways.

It's important to note that the "select a profile to draw" box is *not a setting itself.* It will not remain on your selection when you return to this screen. It is merely used to select the color that you currently drawing.

The blue dot represents the current day and time.

Editing the start/stop times

Use the Days button to toggle between selection of all days, weekdays, or weekend days. Instead, you may click on an individual day label, or hold the control key to select multiple days arbitrarily.

When the schedule contains profile changes, you will see "bubble location" icons appear at the top of the schedule showing times when the active profile changes. You may drag these

icons to align these to 5 minute increments. If you bring two icons close enough together, they will merge together to eliminate one of the profile changes they represented. For even finer tuning, you may "select" an individual bubble icon by clicking on it, and then use the time edit box to enter a time directly.

A single level of "un-do" is possible by using the Undo button.

Setting times relative to sunrise or sunset

By setting your latitude and longitude at least approximately, you may take advantage of a feature to automatically move the preset transition bubbles along with the change in sunrise or sunset each day. First move a time bubble icon within proximity of either sunrise or sunset, and then select the "relative to sunrise/sunset" checkbox.

Positive latitude is above the equator (N), and negative latitude is below the equator (S). Positive longitude is east of the prime meridian (E), while negative longitude is west of the prime meridian (a north-south line that runs through a point in England). For example, the USA has positive latitude and negative longitude.

The "civil twilight" selection provides a larger period between sunset and sunrise (night).

The Magic button



The Magic button exists to quickly generate common schedule layouts. These are inactive during work hours, inactive during work hours but only during weekdays, or multiple profiles for those same times. Click the magic button repeatedly to rotate between these. Once selected, you may customize the schedule as required.

Action sets

You may configure an action set to be executed whenever the schedule changes, or on a periodic basis. This may be used to provide a "keep alive" or "health" message to an external system via MQTT for example.

If you select a number of minutes which equally divides a day (such as 1, 2, 4, 5, 6, 10, 12, 15, 30, 60 minutes) the execution is aligned to these time divisions.

Shield change action sets

You may configure action sets to be executed when the Shield icon transitions to red (disarmed) or green (armed).

RUN, HOLD AND TEMPORARY PROFILES

When a schedule is running normally and the active profile is set automatically, this is called the “run” state and a green play icon is shown.

When the active profile is overridden in some way, this is considered a temporary or transient state and a yellow pause icon is shown. The active profile will automatically revert and the schedule will return to the run state after an amount of time specified on the Profiles page in Settings. A value of ‘0’ for this setting will hold the profile indefinitely in the temporary state. You may click the pause icon to immediately return to the run state.

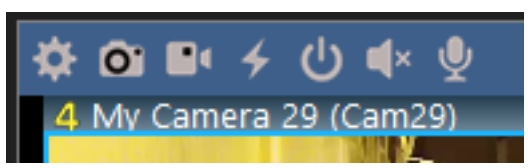
The profile and schedule may also be in a “hold” state where a red stop icon is shown. The active profile will remain until you act, regardless of the timeout setting on the Profiles page. You may hold down either the run or pause icons to force the hold state. Click the stop icon to return to the run state.

CAMERA PROFILE AND SCHEDULE OVERRIDE

It’s possible for any camera to be configured with its own profile schedule. This is done on the Schedule page in camera settings.

By default, a change to the global schedule will override all camera schedules and set all cameras to the same active profile. This however can be overridden on the camera’s Schedule page. You may also choose for a camera to use the global schedule and active profile whenever the camera’s schedule selects the “inactive” profile (clear).

And just like it’s possible to temporarily override the global schedule by selecting it in a number ways, it’s also possible to change an individual camera’s profile temporarily. However, this is only possible via the client apps for iOS and Android at the time of this writing.



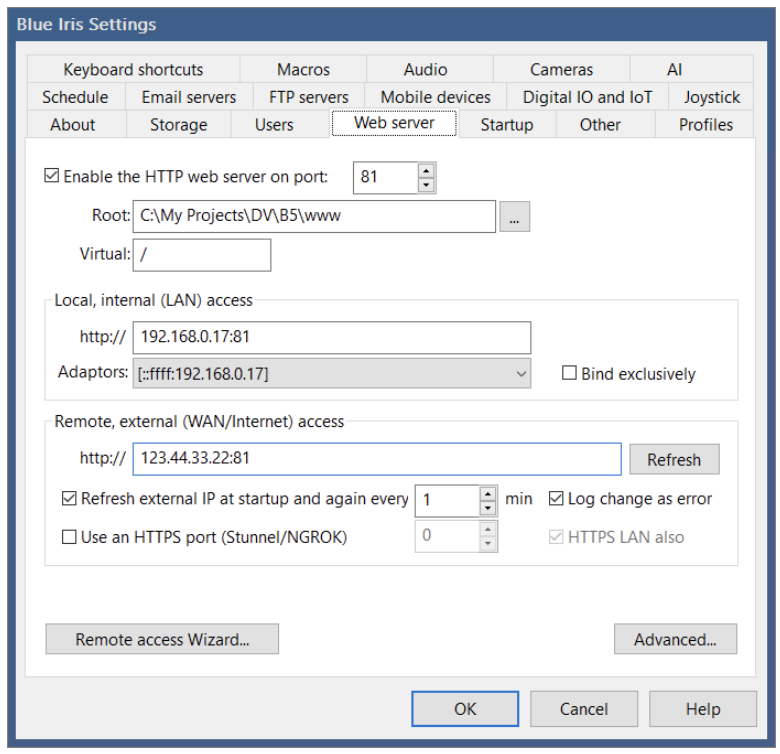
When a camera’s effective active profile differs from the global profile, the active profile number will be shown in the camera’s header.

REMOTE ACCESS

Once you have your cameras added and working with Blue Iris, you may want to access them remotely via PC, browser, smart phone, smart TV, etc. Blue Iris includes a local web server which offers a range of services. No 3rd party web sites or services are otherwise required, although some may be leveraged for various functionality.

THE WEB SERVER

The built-in web server "listens" for incoming connections on a specific *port*. A port is a bit like a "channel" where each network address (IP address) may have several simultaneous "open" or accessible services. Each port may in turn be used for multiple simultaneous conversations.



The default port used by HTTP (normal browser and web server traffic) is 80. In order to avoid conflict with other HTTP servers potentially installed on the PC, Blue Iris uses a default of port 81. Because the default HTTP port is 80, you will not normally see this port number added to addresses in your web browser. When using any other port, you will add the port number following a colon to the address, such as 192.168.0.14:81 instead of 192.168.0.14 (port 80 assumed).

The files served up by the web server are stored in a folder "www" in the Blue Iris installation folder, and from a client (browser or phone app) will appear to be the "root," which is to say the base of the accessible file structure. The files served will be part of the new "UI3" browser interface (described below) rather than the legacy pages. You should not have to change any of these values for normal operation.

It's possible that your system has multiple LAN IP addresses (local numbers such as 192.168.0.14)—one for each interface such as Ethernet, IPv6, WiFi, Bluetooth. By default, Blue Iris listens to the same port number on *all* interfaces. You can force the software to use one interface only by selecting the **Bind exclusively** checkbox. You should use this only if advised or you are an expert, as the LAN IP address and/or available interfaces can change, rendering the web server inoperative. Also, it may not be possible to use this option in conjunction with HTTPS/Stunnel/NGROK, as that requires the software to listen to the loopback address (127.0.0.1), to be discussed.

If your PC is connected to the Internet, it will have a WAN (wide-area network) address as well. This is the address that potentially may be used from *outside* of your home or office to gain access to your Blue Iris web server and cameras. In most cases, this address is subject to change by your ISP (Internet Service Provider, generally the cable or satellite company)—these are called *dynamic* IP addresses and this behavior is generally not a concern for our purposes. A dynamic address may appear to change daily or never at all. It is NOT necessary for Blue Iris to know the WAN address in order to operate the web server, but as this address is used for remote access, the software makes it available for your information and convenient retrieval in a number of ways.

The software can continuously check for a newly assigned WAN address. The new address can be "published" to the Blue Iris server so that it may be retrieved by the client apps using an option on the About page in Settings. The new address may also be published to the Log page in Status, possibly with "error" status so that it can be pushed to you using the Status Alerts.

The use of SSL (secure sockets layer) for HTTPS (secure HTTP) is possible via an added software layer. Software such as the recommended (and free) Stunnel operates a second web server (a second port) on your PC to listen for HTTPS connections. Stunnel decodes these conversations and sends them to the Blue Iris HTTP server. NGROK also offers an HTTPS connection. These will be further discussed in topics below.

As the web server is automatically installed and running, it should in most cases become immediately available if you open a browser on the PC and use the address:

http://127.0.0.1:81

This is a special IP address that always refers to the local PC you are using. The :81 refers to the default Blue Iris port number on the PC. You may also use the PC's LAN IP address, for example (yours will be different):

http://192.168.0.14:81

The IPv6 equivalents to these are:

http://[::1]:81

and (for example)

http://[2604:9108:80e:5223:8877:cc6f:3c6e:be5d]:81

Notice that in order to use an IPv6 IP address, you need to enclose it with brackets []. Also, an IP4 address in IPv6 format will look like this: [::ffff:192.168.0.14].

Due to security software and other default protective measures, just because a web service is running on the Blue Iris PC does not mean it will be immediately visible to anyone else on the LAN (your local-area network, generally equating to your home or office), let alone from the outside (the Internet or WAN, wide-area network).

NETWORKING AND ROUTER CONFIGURATION

There are two ways to configure remote access. The first is most direct, but involves "opening a port" on your router to allow remote traffic to connect through to your PC on a specific port (channel). This may be a simple task, or it may be extremely challenging, depending on your network topology (hardware and connections) and networking experience. If your attempts fail, or if your ISP simply disallows these type of connections on any port (some satellite services notoriously), your recourse is to use a *secure tunnel*.

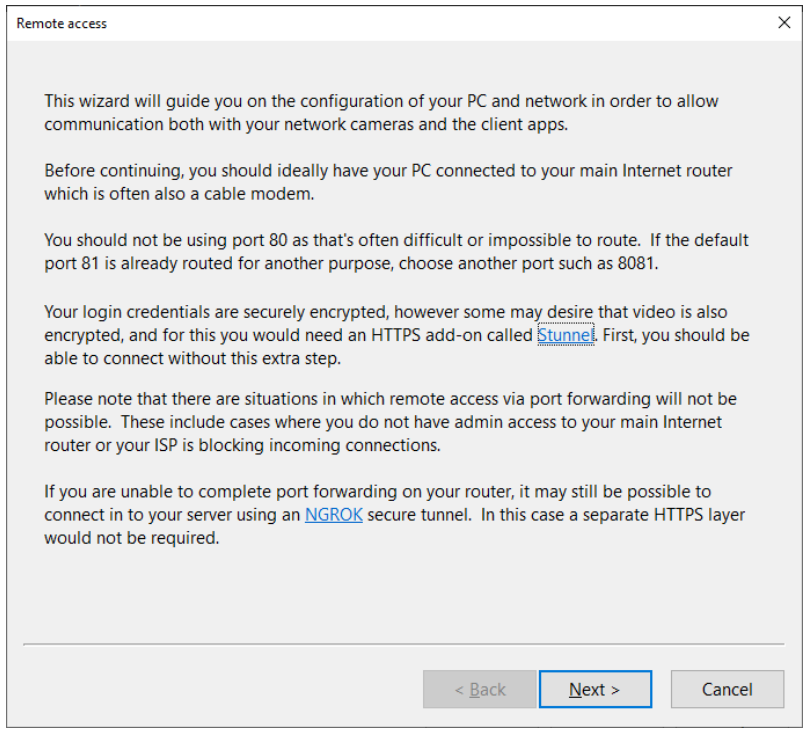
A secure tunnel is what something like a Nest thermostat or Rachio sprinkler system uses to provide you access to your home devices without configuring any of your router or other network hardware—the local devices and your remote clients (phone apps) "meet up" at a designated website (typically operated by the device manufacturer). If it becomes necessary to use a secure tunnel instead of opening a port through your router, the NGROK service is recommended (https://ngrok.com). This is a free service and requires minimal configuration on the local PC.

Please understand that as there are so many variables both hardware and software, router configuration for remote access is strictly *not* a Blue Iris support issue, however we do all that we can to assist, beginning with the Remote Access Wizard.

REMOTE ACCESS WIZARD

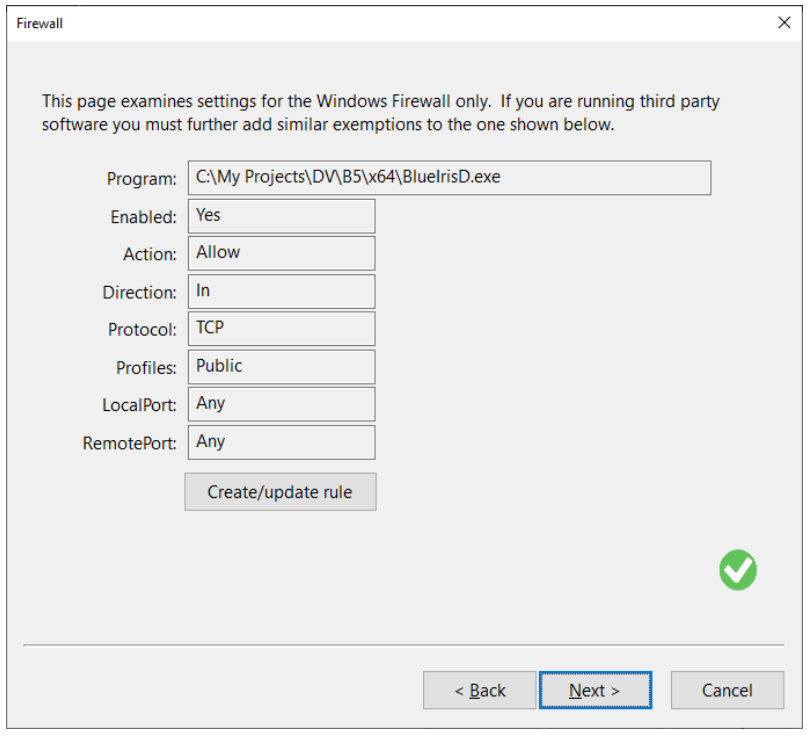
The Remote Access Wizard covers many topics which must be addressed for remote access regardless of the type of connection you will be making. It is accessed either from the main menu or from a button on the Web server page in Settings.

Introduction



Firewall and antivirus

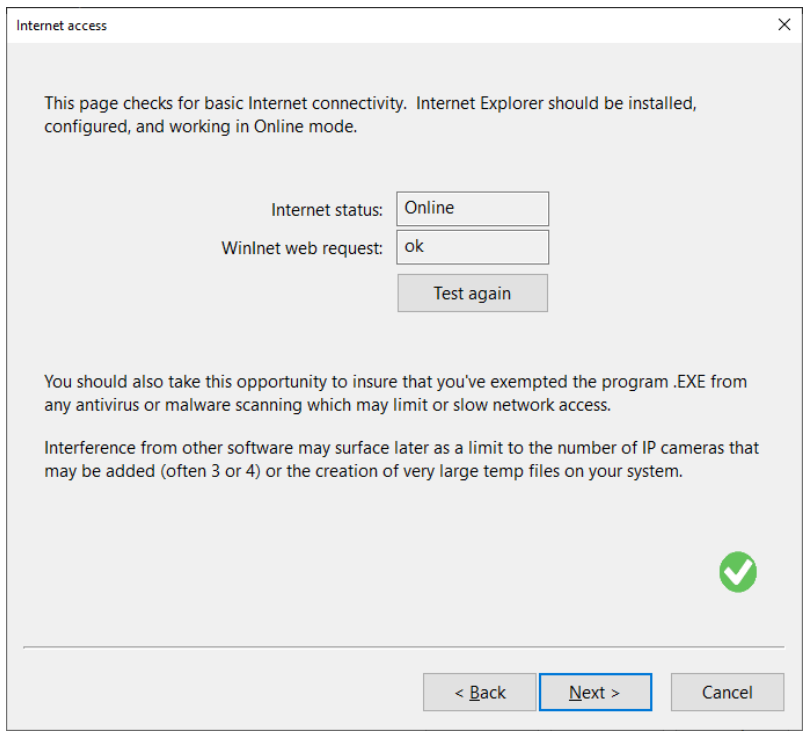
The first step is to ensure there is no local firewall or antivirus software restricting access to the Blue Iris server port. If you do not see a green check mark, use the **Create/update rule** button. When you first launched Blue Iris, you would have been queried by the operating system on whether to allow Blue Iris access through the firewall. If you did not say Yes at that time, you may repair that now.



Note that this addresses the Windows firewall only. You may have additional firewall and security software installed on the PC which may also need to be adjusted to “trust” Blue Iris to use the Internet. It’s also possible to have a *hardware* firewall appliance, a separate device or built-in to the router. These may require configuration through their respective browser interfaces.

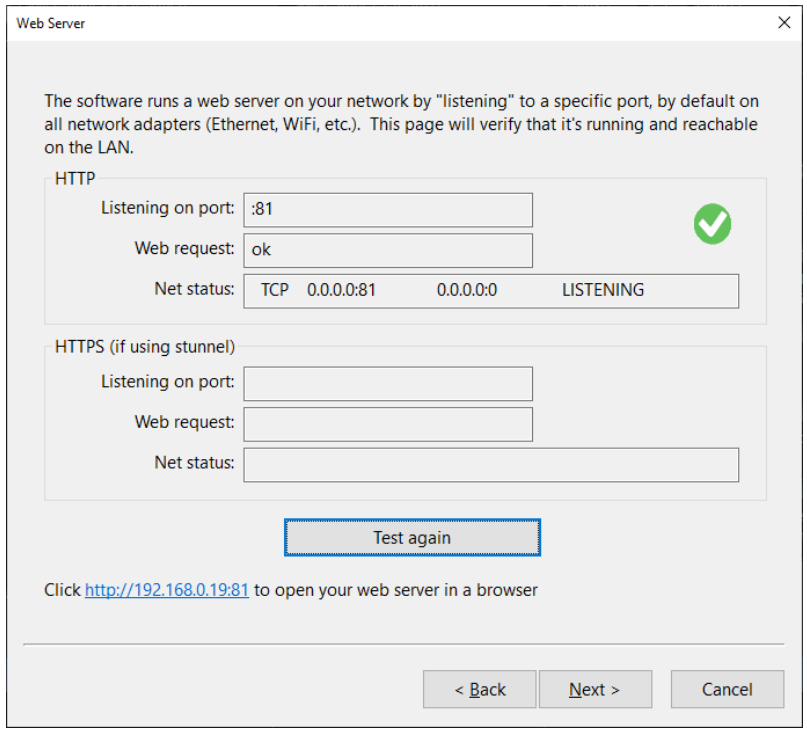
Internet access

This next step basically tests access through the firewall to verify outbound connectivity. If you do not see a green check mark here, you must return to the previous step and address all installed firewall software on the PC to make exemptions for Blue Iris.



Web server

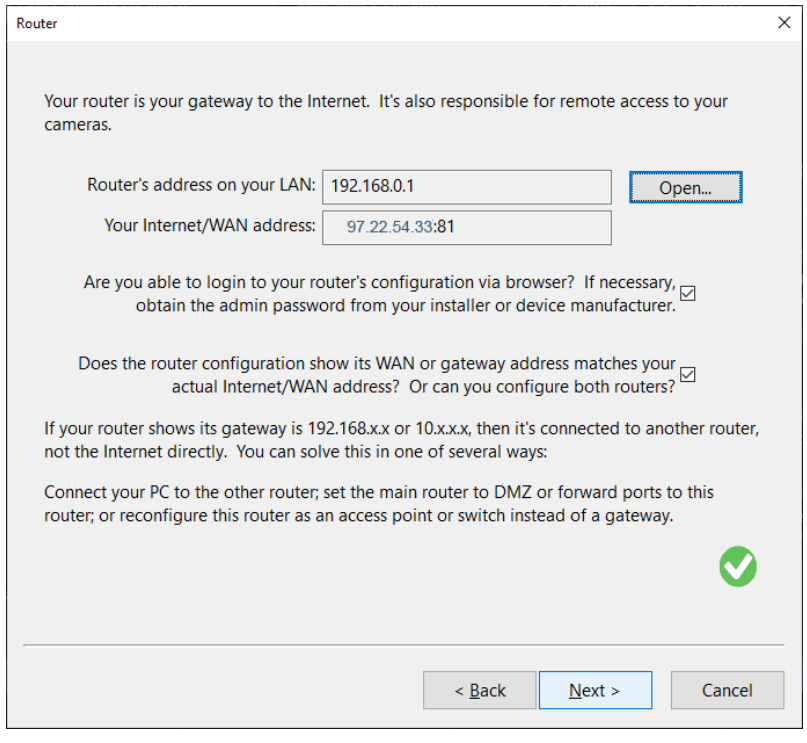
This step verifies that the Blue Iris service is actually running (listening) on the specified port. If all steps are successful to this point, you should have local access to your Blue Iris server from any other PC on the LAN (same home or office network). If you are unable to access the Blue Iris server locally, the PCs or devices may be on separate LAN segments and it may be necessary to move/connect the Blue Iris PC to a more central or root segment (closer to the modem via switch instead of through possibly multiple routers). If you are unfamiliar with these topics, you may need to contact a networking support service.



If you are running Stunnel or NGROK for HTTPS, that uses a second port, and that is tested here as well.

Router

This step ensures that you are able to access the configuration on your router. If you are using a secure tunnel with NGROK or otherwise, this step and the next may not be relevant or required.

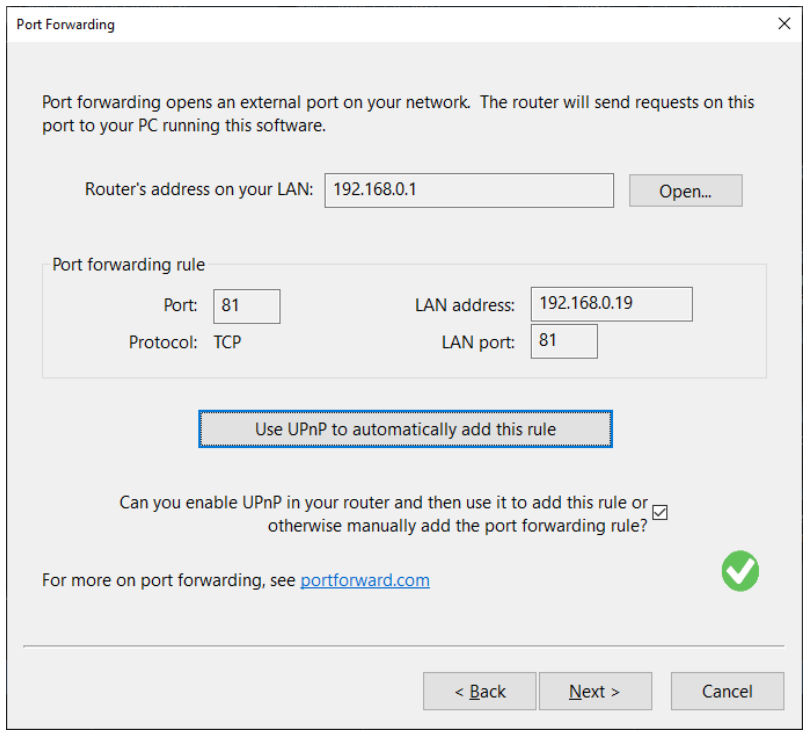


Your router's LAN IP address is identified and displayed, and you may use the **Open** button to bring it up in a browser. If you are unaware of your router's login information or it was

installed on your behalf, you may need to contact the installer or the router's manufacturer for this information.

Port forwarding

The act of opening the port for remote access is called "port forwarding" in most router setup pages, but may only be found on Advanced pages in the interface. Port forwarding works by assigning a public/remote port number to a service (the Blue Iris web server). The router then *forwards* all inbound traffic on this port to your Blue Iris PC. Technically the PC port number may be set differently from the remote port number, but to keep things straight these two are generally set to the same number. The protocol selection should be TCP or "both."



UPnP is a technology which attempts to complete this step for you. It is not always going to be effective, as it may be turned off as a feature in your router for security. Also, although Blue Iris requests the rule to be permanent, this is often not honored and the router resets (removes) the port forwarding rule and it must be completed over and over perhaps daily or weekly.

Multiple routers

If your Blue Iris PC is not connected directly to the modem via a simple switch (hub), there may be multiple routers to configure, and these require configuration in series. That is, the router that "sees" the Internet must be configured to send traffic to the next router in sequence, which finally connects to the Blue Iris PC. For example:

Internet —> Router 1 —> Router 2 —> Blue Iris PC

66.22.11.11 —> 192.168.0.1 —> 192.168.0.2 —> 192.168.1.6

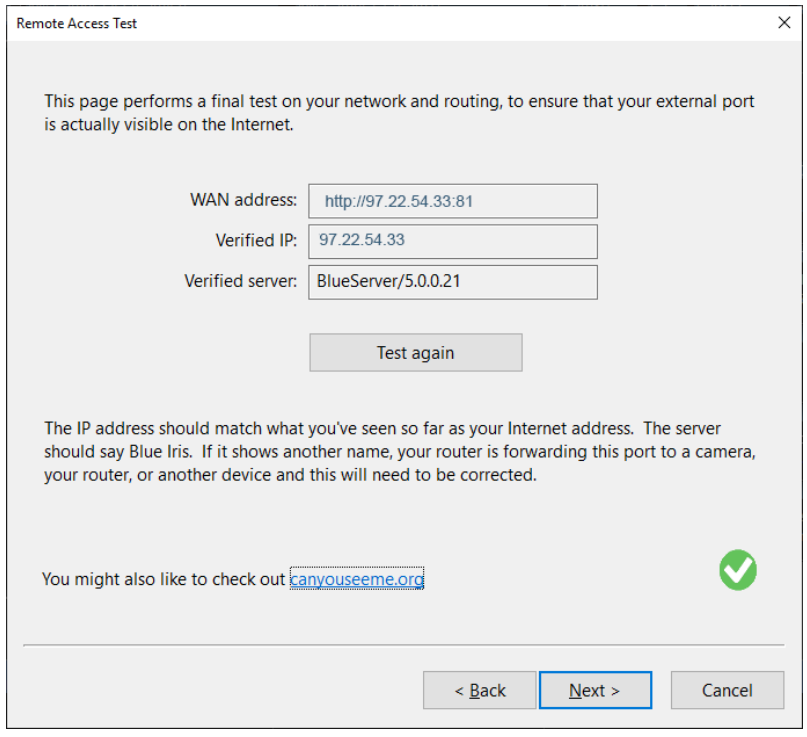
(and 192.168.1.1)

Router 1 may have a LAN address of 192.168.0.1. Router 2 is a “client” of router 1, and may have a LAN address of 192.168.0.2 for example. In this example, port forwarding is completed on router 1 to send port 81 traffic to 192.168.0.2. The Blue Iris PC is a client on router 2 with a LAN address of (for example) 192.168.1.6. Router 2 would be configured to forward traffic on port 81 to 192.168.1.6.

This is sometimes called multiple NAT (network address translation), because each router uses a different address set (notice the .1.x instead of .0.x in the addresses that each router handles).

Remote access test

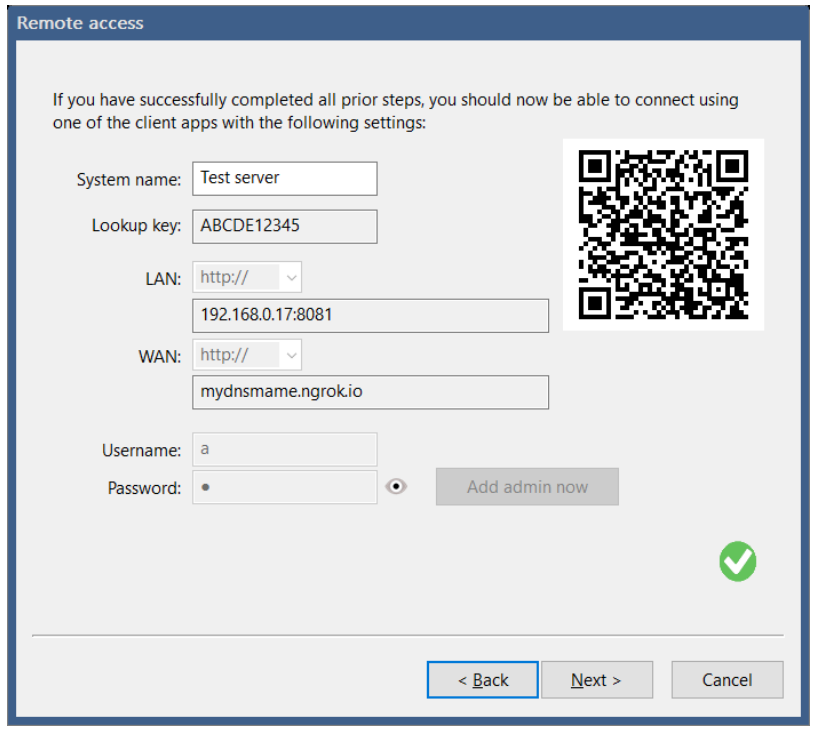
Finally, a test is performed to determine if your router/s have been properly configured:



The website canyouseeme.org offers similar functionality.

Client app login

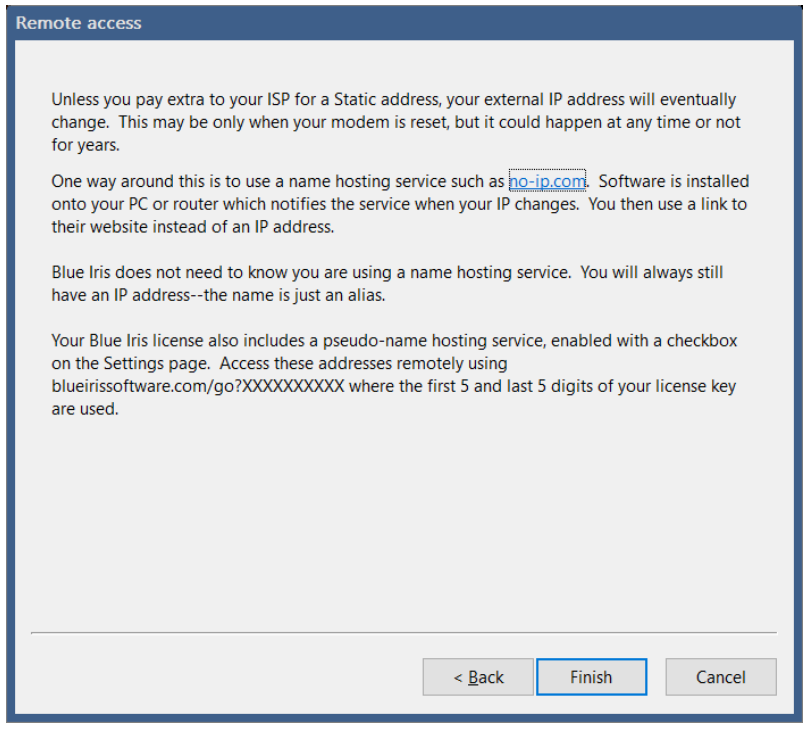
This page details what you need to use with the client apps for iOS and Android. All previous steps (or NGROK configuration) must first be completed.



If an *admin* account has not been created on the Users page in Settings, the software can automatically create one for you here.

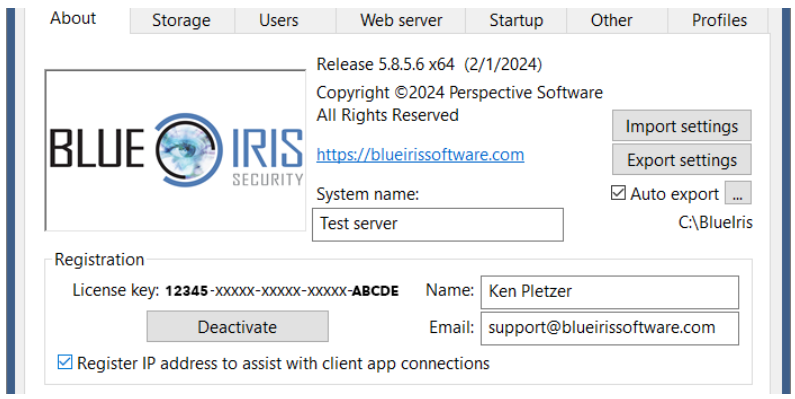
Dynamic IP

If your remote WAN address is often changed by your ISP, you may lose access to your system until you determine the new address. By using your license key, you can have the client phone apps “look up” the addresses for you if they were registered with Blue Iris on the About page in Settings. Also or instead, you may use a third party service to manage this.

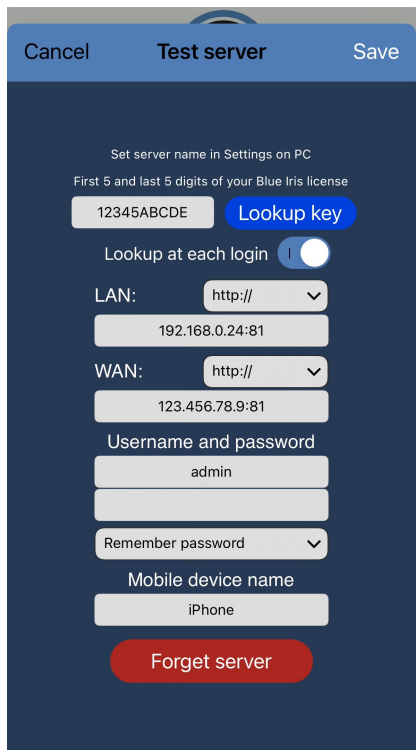


One popular service is no-ip.com, but others exist such as DynDNS.com. Also, if you are using NGROK, this may be included as well. These services allow you to use a *name* such as myserver.no-ip.com instead of a number. The way these services work is to install a small client software on your PC which sends your current WAN IP address to their website. Using your name remotely, the website "looks up" your current WAN address.

In order to have the phone apps look up your address, first, select to **Register IP address to assist with client app connections** on Settings/About:



Then in the app, enter the 1st and last 5 characters of your license:



You may use the **Lookup key** button to fetch the address manually, or you may select to **Lookup at each login**. Looking up the IP each time requires an extra connection which may add time to your login, so you should use this option only if your IP changes very frequently.

You may also perform this from a browser using this URL with the same characters from your license:

https://blueirissoftware.com/go?12345ABCDE

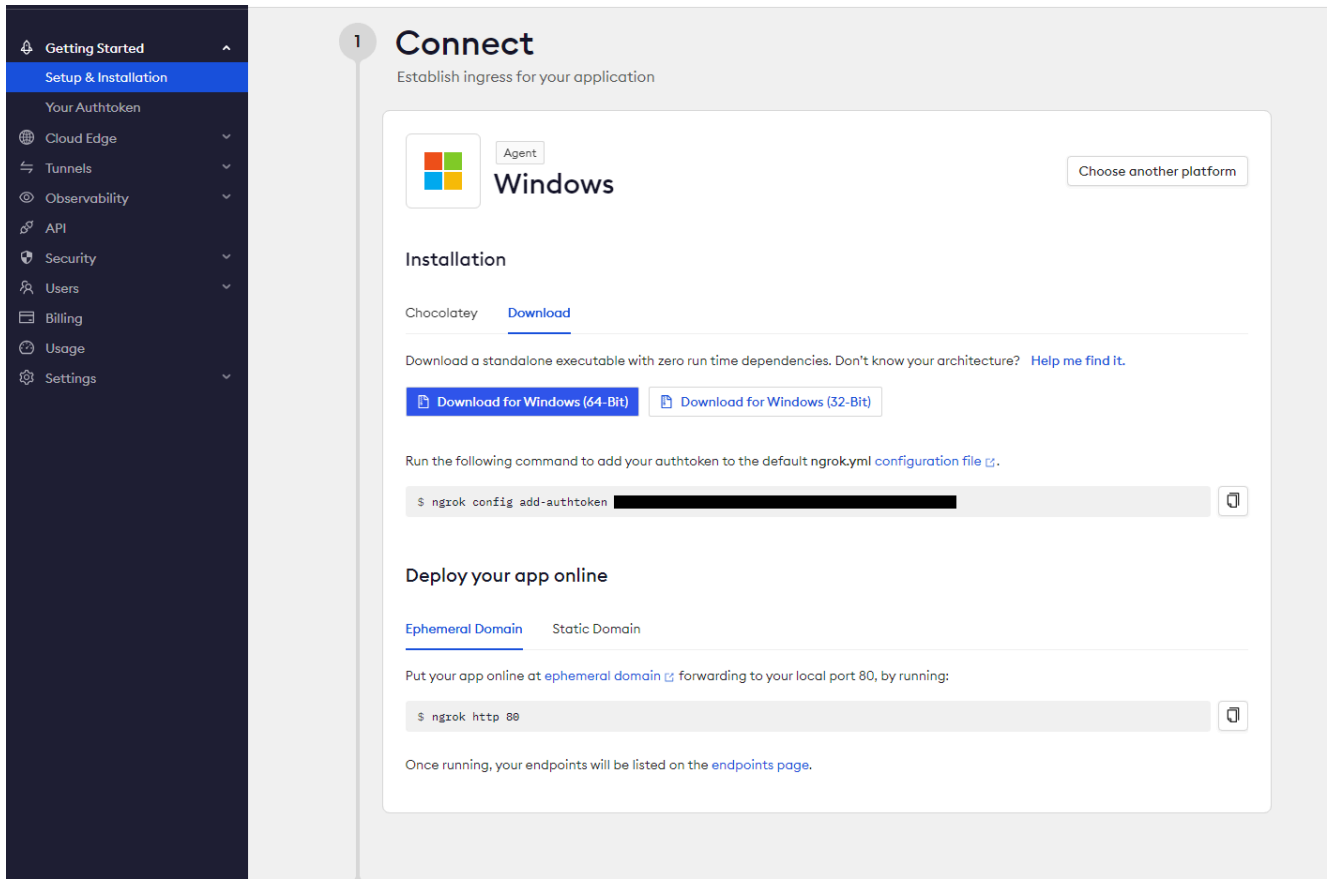
NGROK

If port forwarding is not (easily) configurable, you may instead choose to open a secure tunnel using the NGROK software. This method has many advantages over port forwarding:

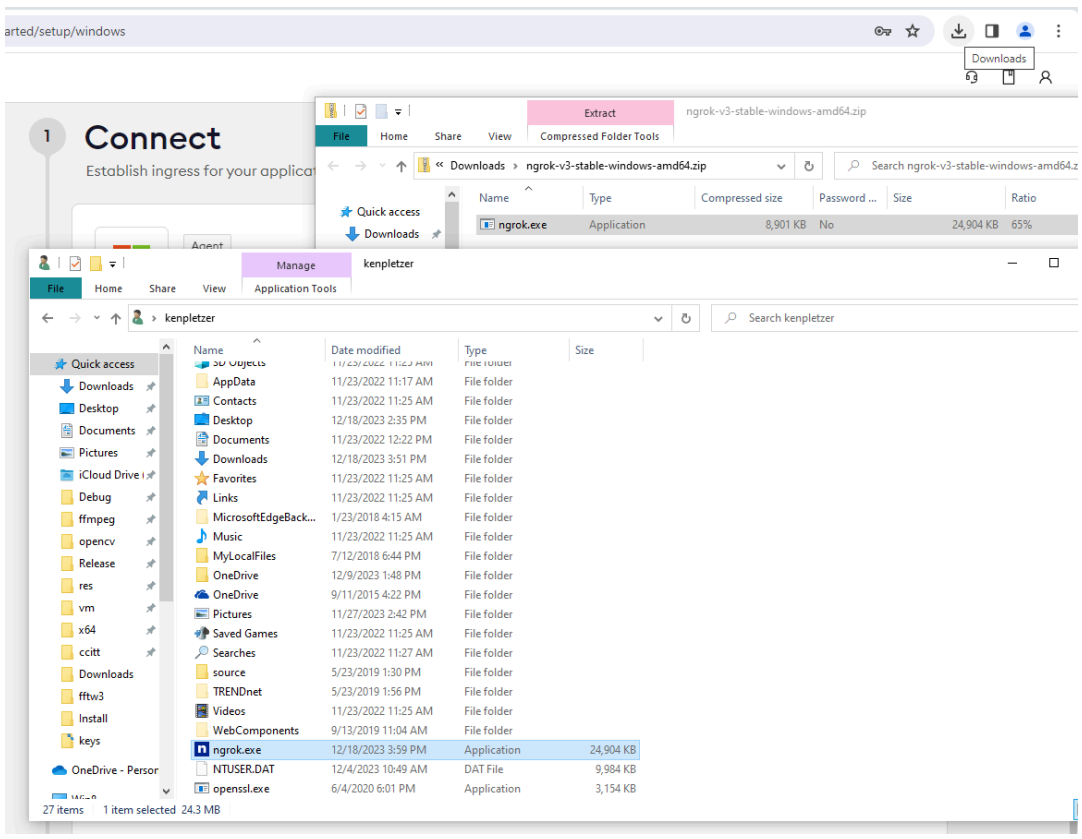
- *No router configuration!*
- SSL/HTTPS secure communication
- Not affected by incoming-connection blocks by your ISP, as your PC will now connect *out* to the NGROK "meet-up" server
- With a paid NGROK account, you may specify a *name* to use remotely instead of a possibly changing IP address

Here's how to configure it:

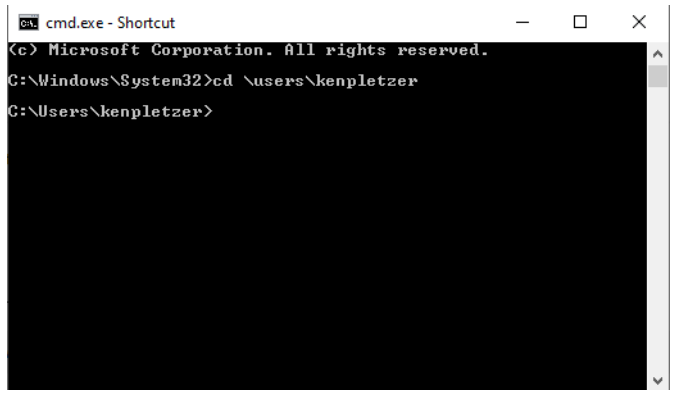
1. Create a free account at https://ngrok.com/
2. Locate and use the option to download for your OS



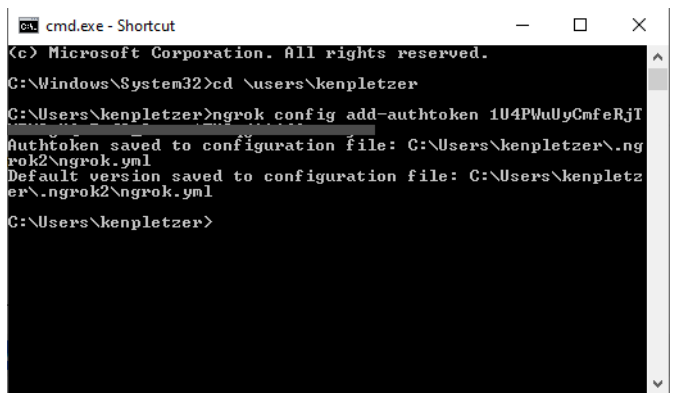
3. Download, open the zip, and drag the NGROK.exe to your Windows user folder (such as C:\users\kenpletzer for this example)



4. Run CMD from the Windows start bar, which should open to your user folder, or you may need to navigate there with a *cd* command as shown:



5. Highlight and copy the “Run the following command to add your authtoken to the default ngrok.yml configuration file” command from the NGROK page:

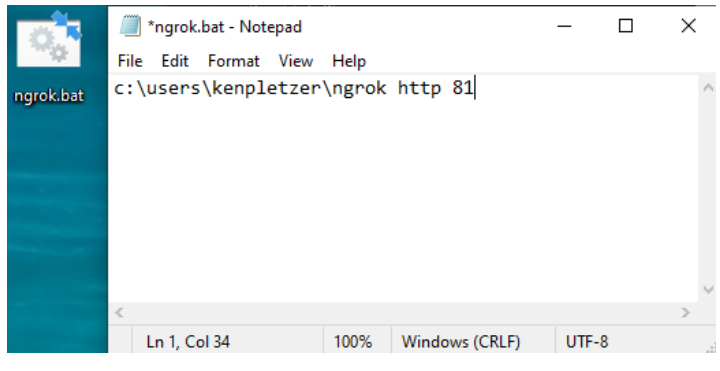


6. You should see a similar message as shown here if you have entered the command correctly. If you see **Access denied**, go back to the File Explorer window, right-click

the NGROK executable file and select to **Unblock** the file. You may also have to temporarily pause your antivirus in order to allow this file to run the first time.

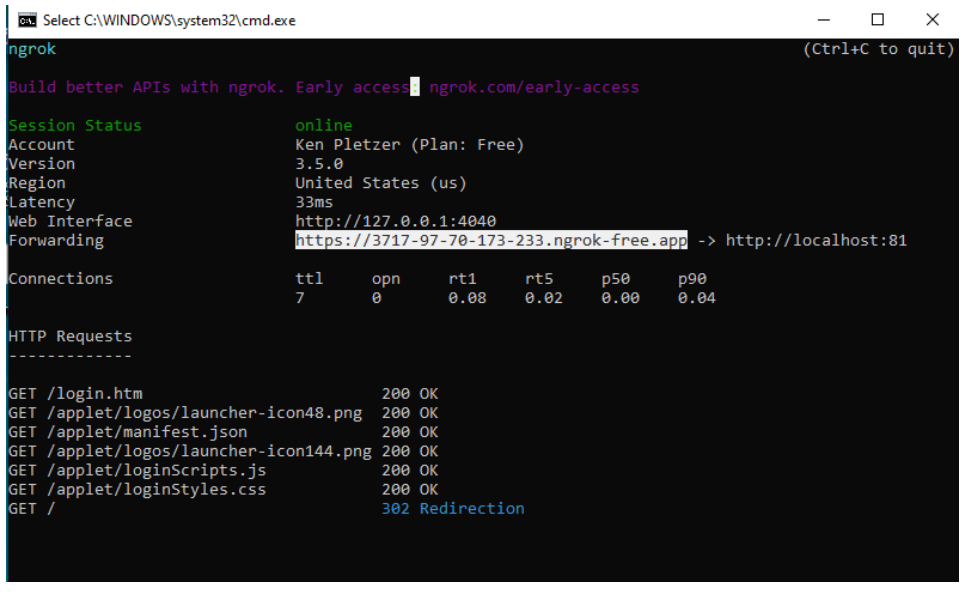
7. Create a server.bat file on your desktop by right-clicking to create a new text file. You must change the extension from .txt to .bat. If you don't have extensions enabled for visibility: in your File Explorer window, go to the View menu, then the Options drop down (far right), then select **Change folder and search options**. Go to the View tab, then UNCHECK the box for **Hide extensions for known file types**.

8. Add a single line to this file that runs the NGROK exe. You will need to use the full path. Follow this with **http** and then the Blue Iris port number, which has a default value 81.



9. Close and save the file.

10. When you then double click this file, it will run NGROK in a command window:



11. Your remote server address is then visible on this window, here highlighted in white. This is the address you can use to access your Blue Iris server from the Internet or phone app.

12. If you receive an error remotely stating "successfully tunneled to your NGROK client, but the client failed to establish a connection to the local address localhost:81" it may be that "localhost" is not resolvable for some reason. In this case you may use the full

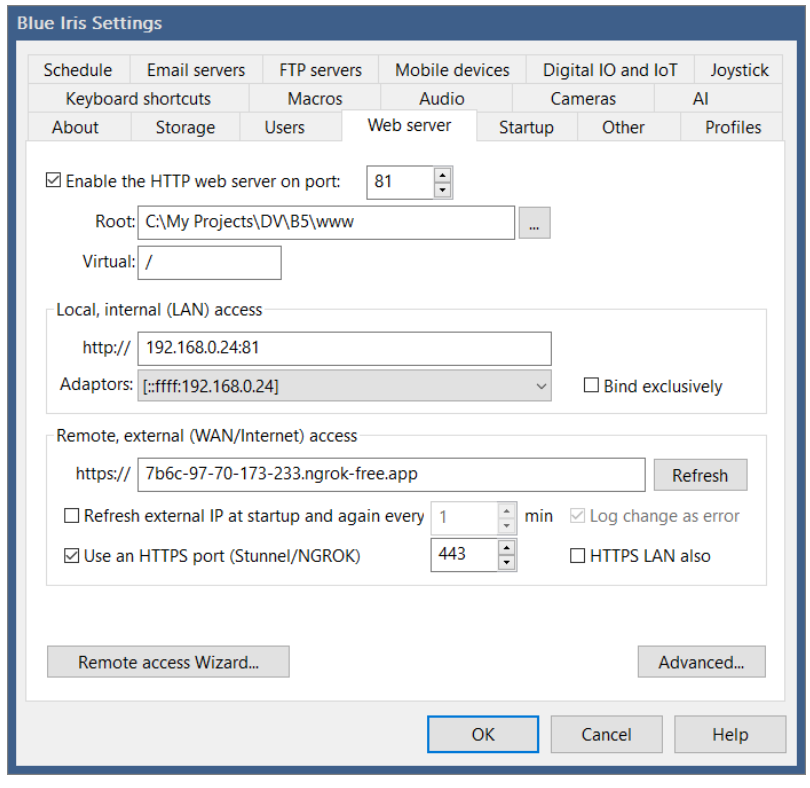
LAN IP address in the NGROK command. Edit the BAT file and change the 81 to your full LAN address such as 192.168.0.200:81 for example.

13. THE REMOTE ADDRESS WILL CHANGE each time you start NGROK. For a permanent address, they do offer to sell that service. You may then alter the .bat command to include a sub-domain:

ngrok http —subdomain=YourUniqueName 81

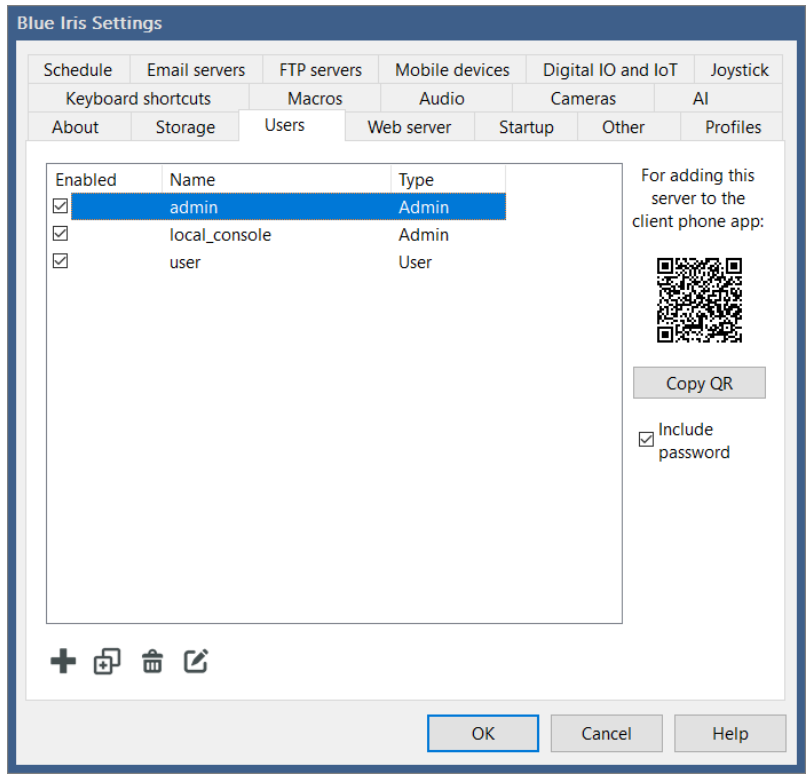
14. There are many ways to automatically run this when you login, PC restarts etc. One way is to open the shell:startup folder (press the Windows logo key + R, type shell:startup, then select OK) and then add the .bat file to this folder.

15. The NGROK ".app" address becomes your WAN address and you may immediately use it remotely. However, in order for the Remote Access Wizard or the "lookup key" button on the phone apps to use this address, you need to now enter it into the WAN address box on Settings/Web server. Disable the option on that page to "refresh external IP" so that your NGROK address is not later overwritten:



USERS AND CONNECTIONS

Potential users of your Blue Iris server are managed on the Users page in Settings.



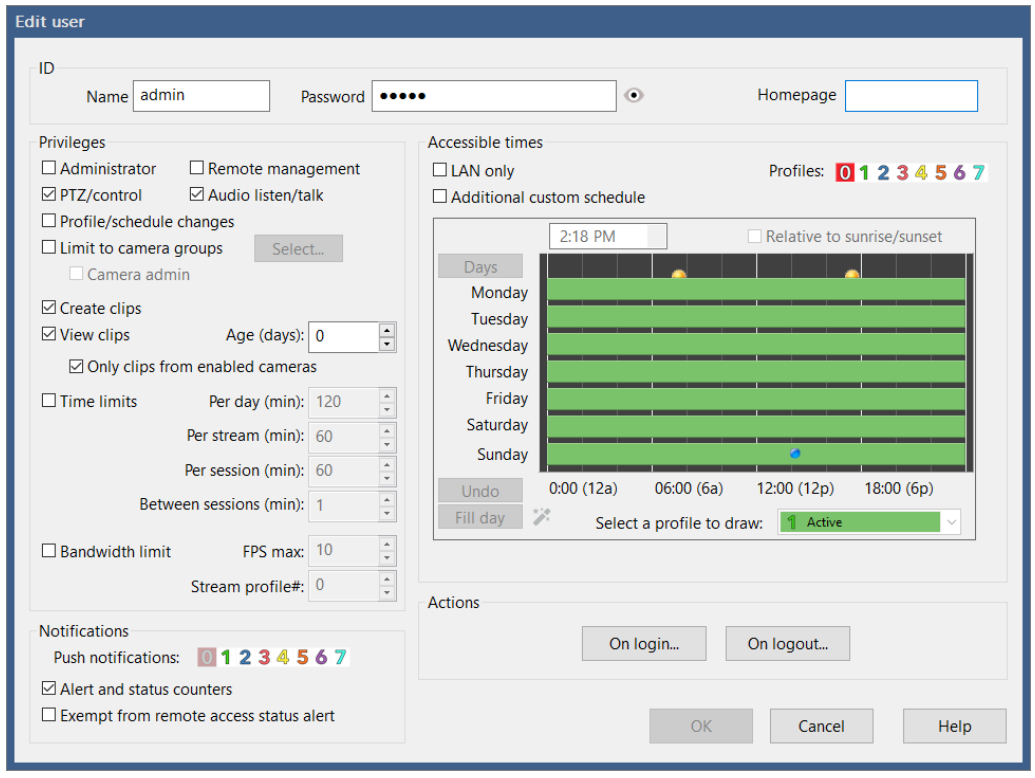
The **local_console** user is created automatically and is used only locally when you open the software. There are ways to login locally using another account in order to limit access, discussed in the Administration chapter.

The **Anonymous** user also is created automatically if you allow access without authentication (without a password) on either a LAN or WAN connection. This is covered in the Advanced topic below.

A **QR code** is generated for the selected user in order to assist with connection to the iOS or Android apps. You may direct your device's camera to the screen when prompted for the QR code by the app's Add New Server wizard, or you may copy it to the Windows clipboard for sharing in another way.

> Note: Use caution when including the password with the QR code if it is copied or otherwise distributed as it may be used for unauthorized access to your system if it is not used by the intended user.

Add or edit an existing user:



ID

A user should have a specified password in order to be used remotely.

Privileges

A remote user with **Administrator** access may make configuration changes to your system and delete video clips—please enable this with caution. IMPORTANT NOTE: If used in conjunction with the **Limit to camera groups** setting, the user may only administer the specified cameras.

Remote management allows a user to connect using another Blue Iris installation to remotely control this one. Only one user at a time may be connected in this way, and when connected it will not be possible to use the local console (it will be closed if currently open, but the software service will continue to run in the background).

The **PTZ/control** option allows the user to move the camera or to make other camera control changes such as brightness, IR lights, DIO output settings, etc.

The **Audio Listen/Talk** option may be disabled to prevent the user from listening to the audio from the camera or sending audio to the camera using a microphone.

The **Profile/Schedule changes** option may be used to allow a non-administrator access to change the global schedule or profile, including the run/lock button and shield.

The **Limit to camera groups** setting prevents a user (even an administrator) from accessing restricted cameras. Camera groups are managed using the *group layout edit mode* or may also be selected on the General pages in Camera Settings. Each camera may be a member of multiple groups for this purpose. Remote users have access only to recorded video which was recorded from an accessible camera.

When limited to specific camera groups, also select the **Camera admin** option to allow a user (even one with administrator access) to administer those cameras. This includes access to camera settings in the mobile app for enable/disable, current profile, pause, etc.

Select the number of historical days of video to which the user will have access (0 for unlimited). You may also unselect the **View clips** option to prevent access to any recorded video at all. You may also restrict the user to video associated with enabled cameras only. A user must have the **Create clips** privilege in order to create snapshots, create manual video recordings, or to crop and export video.

Specify a **homepage** for the user to override the default ui3.htm or default.htm page. This might allow you to force users to use specific custom views. Note that an adept user may still override this by specifically navigating to /ui3.htm in the browser address bar.

Accessible times

Select the profiles during which the user will be granted access.

The **LAN only** option attempts to discriminate between local and remote users. Note that if using Stunnel for HTTPS, all connections may appear to be local, as Stunnel and NGROK accept the connections and then forward these to Blue Iris.

If enabled, a custom schedule interface may be used to select the times during which the user may connect. Only the Inactive (clear) and Profile 1 (green) drawing is significant here. The user will be granted login only when the schedule shows active (green).

Other time restrictions

You may restrict the user to a specific number of minutes for each authenticated session, along with a specification of the number of minutes they must wait between successive connections. A per-day (24 hour calendar day) restriction is also possible.

A *per-stream* time limitation is available as well. This will automatically break a continuous streaming connection after a specified number of minutes. The user will need to re-initiate

a camera video stream when the timer expires. This exists to prevent a user from initiating a stream and then “walking away” from the PC while this is open.

Bandwidth limitations

You may restrict a user to a specific streaming profile which may be of lower quality. Streaming profiles are configured on the Advanced page from the Web server page in Settings.

Another possibility is to limit the number of FPS (frames per second) the user may receive from a video stream.

Notifications

You may select that a user receive push notification only when specific profiles are active. Note that in addition to this setting, the user’s device must also be enabled for push notifications on the Mobile Devices page in Settings.

By default, the software tracks the number of new alerts for each user, for each camera. This results in counters placed near camera icons on the client app. The alert counters are typically only reset when the user clicks on the associated camera for live streaming or plays a new clip recorded from the camera. This behavior may be disabled here.

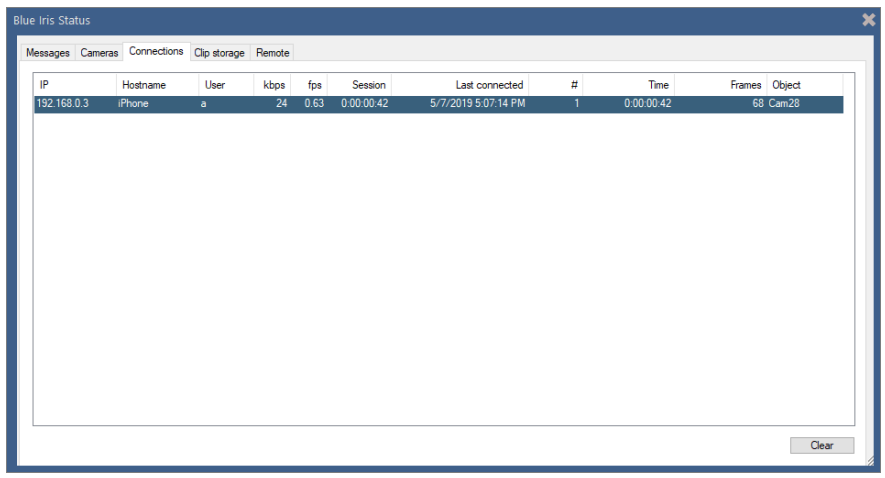
With an option on the Status Alerts page from the Log page in Status, notifications may be sent when users login remotely. However you may desire to defeat this behavior for specific users, and that may be done so here with a checkbox.

Actions

You may select any number of actions to perform upon user login or logout. Please see the chapter on Alerts and Actions for more information on configuring these actions.

Connections

Active connections are shown on the Connections page in Status.



Each connection shows an address, a hostname (the remote name, if it may be determined), the authenticated user, the bit rate (in kbps), the frame rate (fps), total number of frames served, the current "object" (typically a camera or clip) being streamed, and the duration of the session. The total number of times this connection entry has been re-used (possibly due to multiple logins over time) is shown in the # column, along with the total time session time for this and all previous connections.

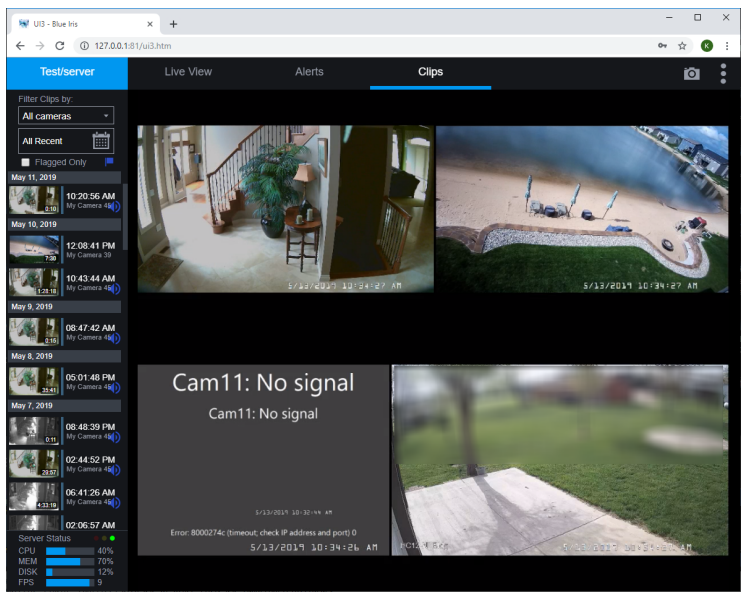
Note that a connection does not become a *login* until the connection has been authenticated (logged on with a valid user and password).

Previous connections from temporarily banned addresses are shown in red. Connection banning is managed on the Advanced page from the Web server page in Settings.

One or more connections may be cleared by highlighting them and using the **Clear** button. An active login will be logged out and disconnected.

BROWSER INTERFACE

The powerful UI3 browser interface may be used in place of a client phone app or remote management connection.



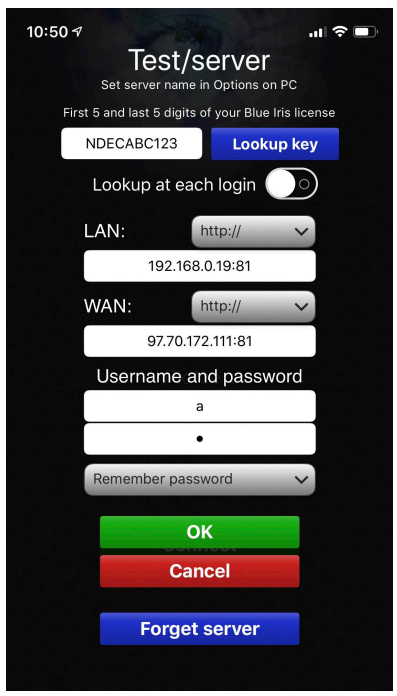
This client works best with a modern HTML5 browser such as Chrome. This interface was designed and built by a third party however—so separate help and support may be available via the “three dot” menu button at the top/right of the window.

You may find more information and release history here:

https://github.com/bp2008/ui3

MOBILE DEVICE ACCESS

Apps are available for both the iOS and Android device platforms which offer extended features such as geofencing and push notifications. Prior to using these apps, remote access must first be configured and working (see previous topics in this chapter). When you add a Blue Iris server to the app, you must complete a login page:

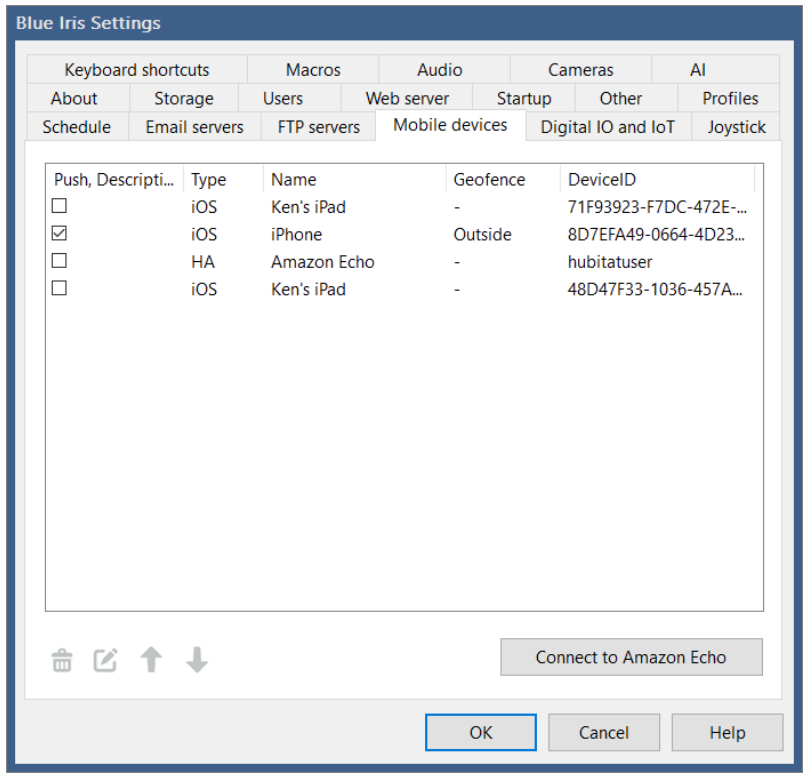


You may use part of your license key to “look up” your server addresses instead of entering them manually. If your WAN address changes frequently, you may wish to use the option to look up the address each time that you use the app. Using the option to look up the addresses requires use of the Blue Iris website and you must have registered your addresses with the website by using the checkbox on the About page in Settings. Use of the license key here to register and look up your addresses is *optional*.

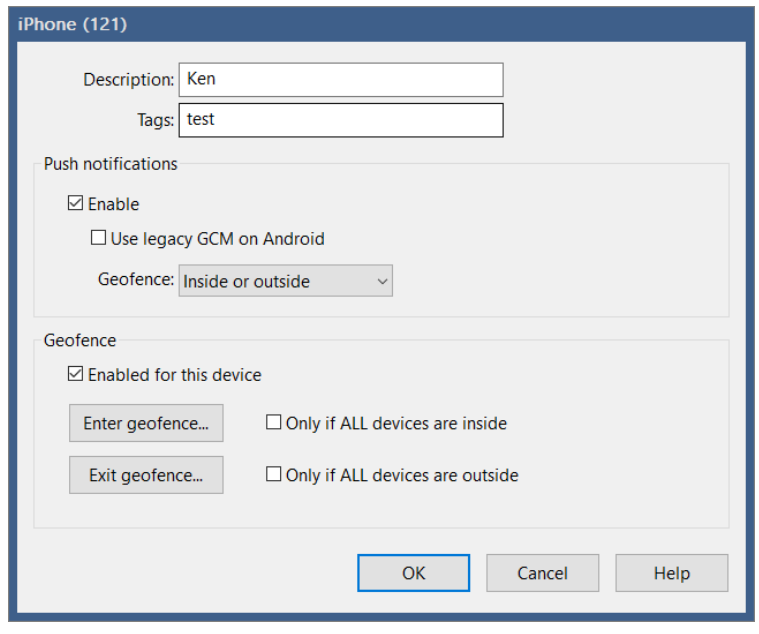
The app will attempt both the LAN and WAN addresses to make a connection, with preference for the LAN address (used when you are at home or in the office). While connected using the WAN address, the app occasionally attempts to revert to the LAN address if possible.

Mobile device management

Following a connection from the client app, the mobile device will be added to the Mobile Devices page in Settings:



Here, you may view the type of device, its name, and whether it's currently inside or outside of the fence if using geofencing. You may also select wether or not the device participates in push notifications and give it a description. For more device settings, highlight a device and use the **Edit** button or double-click the device in the table:



Here you may set the **description** and device **tags**. Multiple tags may be separated by semicolons. When configuring a push notification action, you may select to send the notification only to devices with a matching tag.

Some Android devices on older OS or on certain networks may require the use of the legacy GCM push notification format instead of the newer FCM format, and that may be selected here.

Geofencing

Geofencing provides a way for the Blue Iris to take action based on the position of your mobile devices, generally whether they are inside or outside of your home or office.

A geofence is primarily a phone *OS function* and is set on the phone app in the app's settings page. The geofence is set as a circular perimeter around a specific location. That location may be specified as either the phone's *current location* or the Blue Iris *server location*. Your phone's location is obvious, and may be used when the phone is inside the house near your Blue Iris PC. The Blue Iris server location is only known or accurate if you *set this location* on the Schedule page in Settings on the PC software. The location is specified as latitude and longitude coordinates. Following a change to this location, you must re-login to the phone app in order to download the coordinates to the app prior to setting the fence.

In response to a change in a device location, either moving into or out of the set geofence, you may perform any number of actions as defined by an action set (see that chapter). You may choose to perform these actions only when all other devices (that is, only those with the **Enabled for this device** checkbox selected) are also inside or outside of the fence.

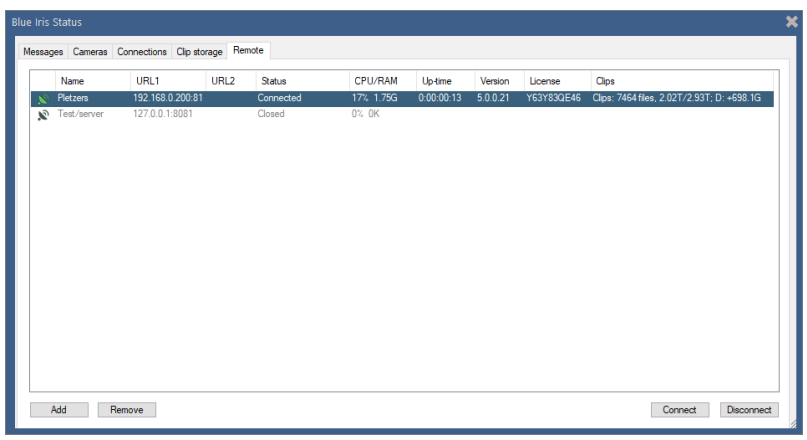
There are a number of moving parts when using geofencing, and many of them are device-specific. The device's location must be accurate via GPS and the phone OS must "wake" the app in order to notify the server. Often times battery or power-saving features on the device will limit geofence effectiveness. Further, the app must be able to use either the LAN or the WAN address to connect to your Blue Iris server to adjust the status on the Mobile Devices page in Settings.

Options exist in the client apps for notification upon both successful and unsuccessful attempts to notify the Blue Iris server of the change in geofence status.

REMOTE MANAGEMENT

Remote management allows you to use one Blue Iris installation to connect to potentially dozens of others and to administer and access features on those remote installations as though you were at those locations. Currently, this does require a full license on each PC.

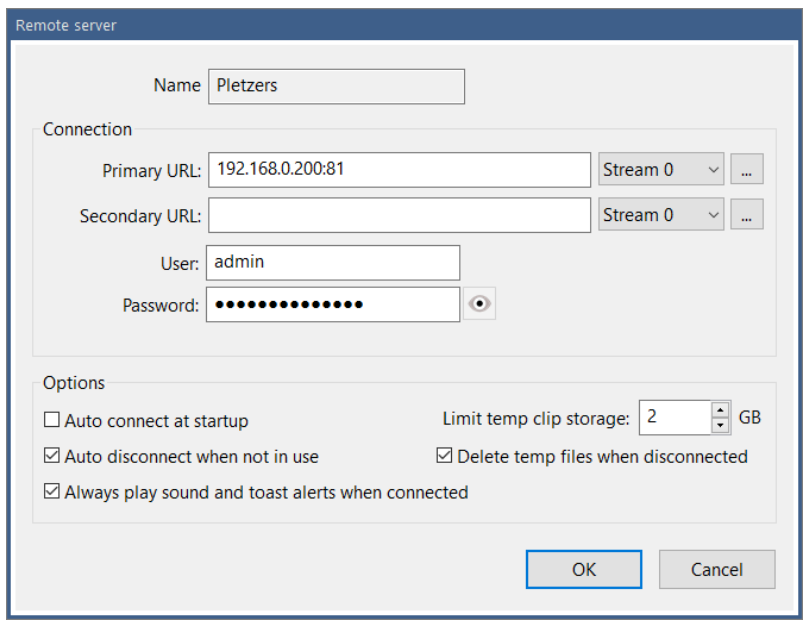
A list of remote systems is maintained on the Remote page in Status.



This list provides an overview of the status of each connected system including details such as CPU, RAM, up-time, software version, license, and clips storage details.

It's possible to connect and disconnect to each system from this interface without making that system the active system in local UI. While connected you may also right-click the server to force a download of the current Blue Iris software update. The update will proceed on the remote system and it will be automatically reconnected here when the remote system is restarted.

Add or edit (double-click) a system on the list to set additional preferences:



The system's *name* is set on each system's About page in Settings.

Connection

You may specify two addresses for the system. These may be LAN and WAN for example if you access it both locally and remotely. When making the connection and logging in, the software attempts the primary address first, and then rotates between the two if a connection cannot be immediately established.

For each URL, you may specify and edit the video encoding properties to be used. These are the same streaming profiles used by the browser and phone apps, editable on the Advanced page from the Web server page in settings, placed here for your convenience.

For each remote system managed, that system must be running as a service, and you must use a user account which has been granted the *remote management* privilege on the Users page in Settings on that remote system.

Options

You may choose to connect to each system automatically when you start Blue Iris. Note however that when connected via remote management, it is not possible to use the console at the remote system location—the console and remote management are mutually exclusive.

You may choose to automatically disconnect from the remote system when it is no longer the active system. The active system is the one selected with the control at the top of the main window UI.

You may choose the amount of local storage to devote to clips and other files downloaded from the remote system. For security or otherwise, upon disconnection, you may also choose to delete these files as well as all temporary files associated with the remote system.

When a remote system is connected and selected as the active system, the software will play sounds and popup notifications from the remote system. If you would like to receive these while connected even when it's *not the active system,* select the option here to do so. This allows you to receive these types of alerts from any combination or all managed systems simultaneously.

Operation

When the software is connected to the local cameras the remote management selection box shows Local:



When you select a remote system, this will show a green icon upon successful connection:



If your local system runs as a service, all local cameras and functions will continue to operate in the background. Note that it should be possible to also *add the local system as a remote connection* in order to continue monitoring its status along with the others if this is required.

It's possible to manage and to perform virtually all software functionality via the remote management connection with few exceptions, and those exceptions will likely be mitigated as this version of the software matures.

SSL AND HTTPS

Blue Iris authentication (login) is by default encrypted and secure already—no passwords are sent in "plaintext." Video however is only *encoded* and not *encrypted* by default. For an added layer of security, you can add an *SSL layer* to the web server. For this we recommend the Stunnel software (https://www.stunnel.org).

Stunnel runs a 2nd web server on your PC that listens for HTTPS requests (secure HTTP). These are then forwarded to your Blue Iris server as configured above. The default HTTPS port is 443, but you may use another (but not the same number as your Blue Iris server).

Once installed, you may edit the Stunnel configuration file, by default in a folder C:\Program Files (x86)\stunnel\config called **stunnel.conf**. Locate the [HTTPS] section in this file:

```
; TLS front-end to a web server
[https]
accept  = 443
connect = 81
cert = stunnel.pem
; "TIMEOUTclose = 0" is a workaround for a design flaw in Microsoft SChannel
; Microsoft implementations do not use TLS close-notify alert and thus they
; are vulnerable to truncation attacks
;TIMEOUTclose = 0
```

Edit the “connect” line to connect to your Blue Iris server port number, by default 81.

The lines beginning with ; are comments and have no effect.

For remote access exclusively using HTTPS, you may route (port forward) port 443 exclusively instead of port 81. If you are using an HTTPS port number other than the default 443, be sure to change this in all places (.conf file “accept” line, router port forwarding as described earlier, as well as the Web server page in Settings).

The default “self-signed” certificate that’s created by Stunnel is fine for your private access via browser (albeit with several security prompts informing you of this status because a self-signed certificate is not globally recognized). However, in order to use one of the client apps for iOS or Android, you will need a “real” certificate signed by a globally recognized Certificate Authority (CA). You may be able to obtain one at little or no cost from sources such as ZeroSSL or GoDaddy for example. These certificates must be combined with a domain name however, so you may also need to create a DynDNS or No-IP address. Once installed, you must inform Stunnel of the new .pem file location by altering the **cert=** line in the stunnel.conf file.

Use the following website to check your security configuration on your device:

https://www.sslshopper.com/ssl-checker.html

If you configured the certificates correctly on the device, this useful website should return all green checkmarks.

MORE ON SECURITY

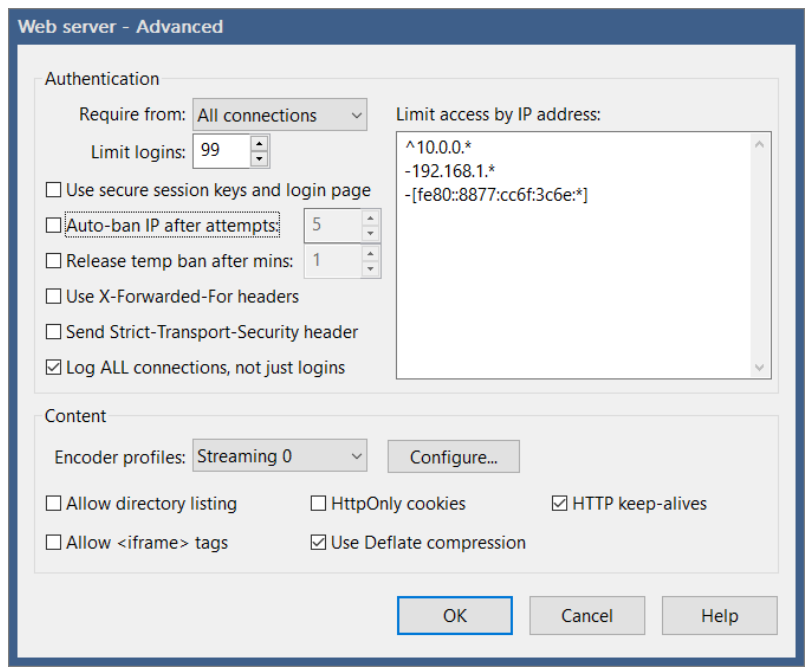
When using Blue Iris and its web server, it is then no longer necessary to open individual cameras for access from the Internet. Network IP cameras themselves have varying levels of security and in general should not be trusted in this way. This is a major feature of this software—a single point of network contact to your cameras without reliance on camera security or cloud security.

The Blue Iris access model is called *on-premises*. Your video and authentication is not reliant on outside cloud services. Because your video is stored locally, concerns of unauthorized access are limited to physical access to your PC or credentials.

When anonymous access is permitted, you will see a user *Anonymous* added automatically to the Users page in Settings. If you disable or limit this account, anonymous access will be denied. In order to prevent anonymous access, retain the default setting **Require from** *All connections* as discussed in the next topic.

The user *local_console* is automatically created whenever you connect via the console (the PC running Blue Iris). It is not possible to use this account remotely so that it cannot pose a security threat.

You may leave these settings at default for a typical installation.



Authentication

Authentication just means the requirement of a user and password to login. Without authentication, anyone can connect *anonymously*. You may choose to require authentication only from remote WAN users.

Note however that if you are using Stunnel or NGROK, all connections may appear to be coming locally from the LAN as these add-ons are actually receiving the remote connections and forwarding them to Blue Iris.

By default, authentication is made using secure (encrypted) methods with a separate login page. For some applications you may require "basic" authentication where the browser prompts for a login and you may enable this by unchecking **Use secure session keys and login page**. Although less secure, basic authentication is more flexible, allowing user names and passwords to also be used in URLs such as:

http://192.168.0.19:81?user=admin&pw=admin

The **Limit logins** box should be left at its default unless you are battling a system resource issue. One "real" user may be responsible for transiently adding multiple users to the connections list due to connectivity issues for example—and that user may be unable to re-connect until other connections time out.

Limit IP Adresses

This provides a basic firewall function. The list may contain multiple entries, one on each line. The first character defines the function:

+	allow this address
-	deny this address
=	*force* authentication for this address when it would otherwise connect anonymously
^	allow this address *without authentication* using the account 'admin'; this account must exist and it must be enabled (**use caution here**).

An address is either an IPv6 address (contain 8 segments of 4 hexadecimal digits each, always surrounded by [and]) or an IP4 address with 4 integers 0-255 separated by periods.

You may use CIDR subnet notation or add an asterisk (*) to the end of an address as a wildcard. These are equivalent:

```
+192.168.0.*
+192.168.0.0/24
+[::ffff:192.168.0.0]/120
```

Consecutive segments of 0000 in IPv6 addresses are removed by Blue Iris according to convention. For example, [ffff:0000:0000:0000:0000:1234:0777:0000] will be shown as [ffff::1234:0777:0000] (notice the double colon).

Depending on the first address's allow/deny character, all IP addresses are by default allowed or denied. That is, if you begin with +192.168.1.*, then all other IP addresses are considered denied unless otherwise allowed. The opposite applies if you begin with a denied address (all other addresses will be considered allowed unless specifically denied).

If an address is denied access on this list it is considered *permanently banned*. There is actually a second *temporary* "denied" list maintained by the software that is not visible here. If you choose to auto-ban an address after a specific number of failed login attempts, that address will be added to one of these lists. If you select the option to release the ban after a number of minutes, the banned IP address is added to the internal temporary list instead of the one visible and editable here.

Temporarily banned IP addresses may be identified with red text on the Connections page in Status.

More authentication options

You may limit the number of simultaneous users connected to the Blue Iris web server. All connected uses share your system resources, so it may become necessary limit these connections to maintain system stability.

By default only authentication connections are logged to the Log pages in Status. If you'd like to see each ping of your server, select the option to log all connections. A connection is *not* the same as a login. No video or other information is served to a connection unless it is authenticated.

The options for X-Forwarded-For and Strict-Transport-Security headers were added for users in enterprise environments requiring specific HTTP security features. You may read about them here:

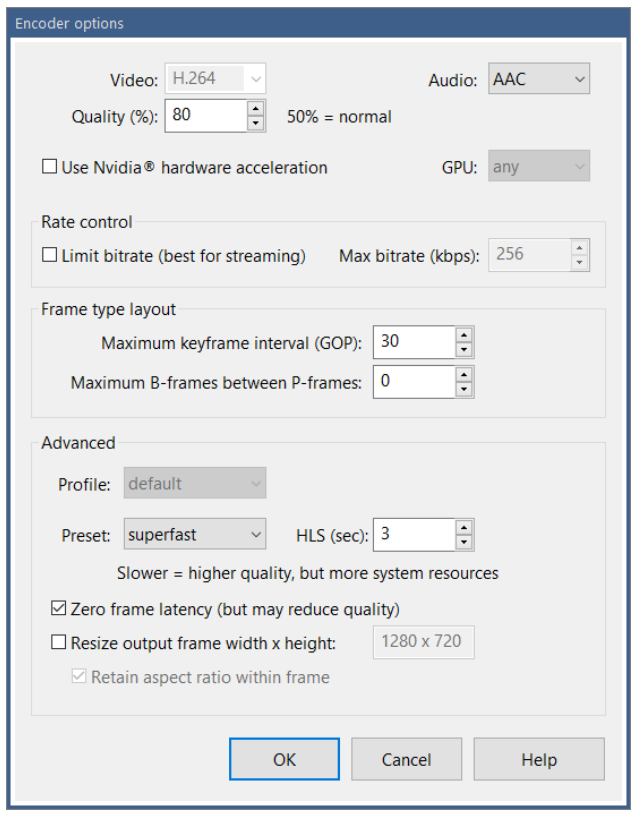
https://en.wikipedia.org/wiki/X-Forwarded-For

https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security

With X-Forwarded-For, a proxy server is considered trusted if it's a LAN address or if it's listed on Settings/Web server/Advanced as an elevated address (using the ^ directive).

Content

Video is compressed as it is sent to a remote client. You have control over the way the video is compressed in order to balance quality against bandwidth:



The important settings here are **Quality** and **Rate control**. If you use rate control (by default), the software attempts to keep a steady bit rate, which is ideal for streaming video. However, the downside of this is that the occasional larger (key) frames will be more compressed, potentially causing a "pulse" of pixelation each 5 seconds or so. When you remove bit rate limiting however, the bandwidth is variable and may not be suitable for a low-bandwidth connection—some larger (key) frames may require more time for transmission, causing pulses in the timing instead of the quality.

The spacing of these larger frames is controlled by the frame type layout. For streaming video, it's generally OK to space these longer, perhaps each 300 frames.

I-Frames are HTTP components where essentially one page is displayed within another page. Certain security requirements specify this not to be allowed.

HttpOnly may be added to cookies generated by Blue Iris and this may be a required setting for some PCI compliant networks. You may read about their function here:

https://www.owasp.org/index.php/HttpOnly

"Deflate" compression may be applied to images, HTML, and other data supplied by the Blue Iris server, greatly reducing transferred bandwidth at the expense of a a negligible amount of CPU time. You may read about this technology here:

https://en.wikipedia.org/wiki/DEFLATE

HTTP "keep-alives" provide a mechanism for the HTTP conversation to re-use existing connections between client and server. While this makes the server faster and more efficient, this may not be supported by all clients.

https://en.wikipedia.org/wiki/HTTP_persistent_connection

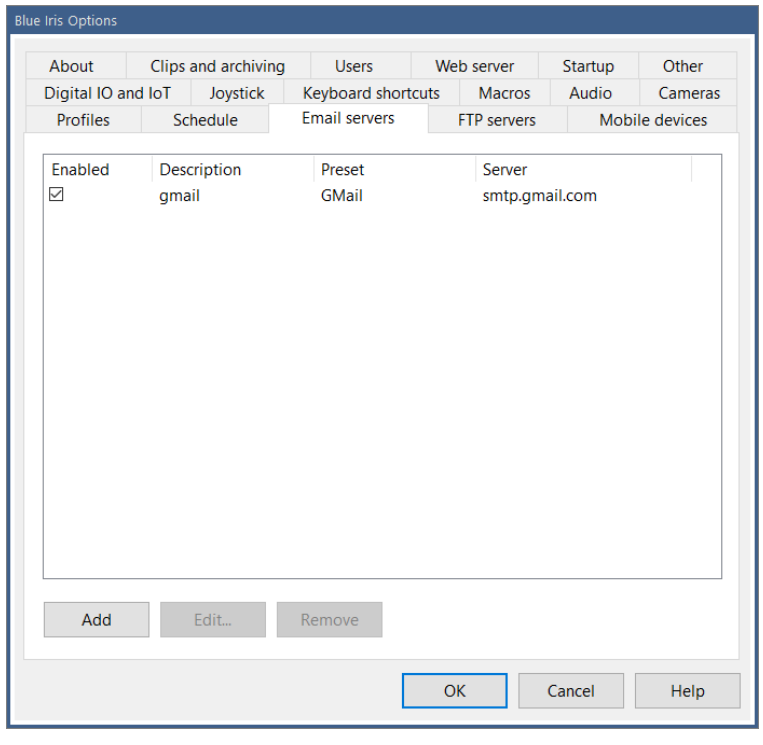
The **Allow directory listing** option should be disabled for all but very specialized cases. This will allow a remote user to see and directly download all files in managed folders such as /clips/ and /www/. Add &match=*x* to filter the results line-by-line using a case-insensitive pattern search—*x* may contain * and ? wildcards.

EMAIL AND FTP SERVERS

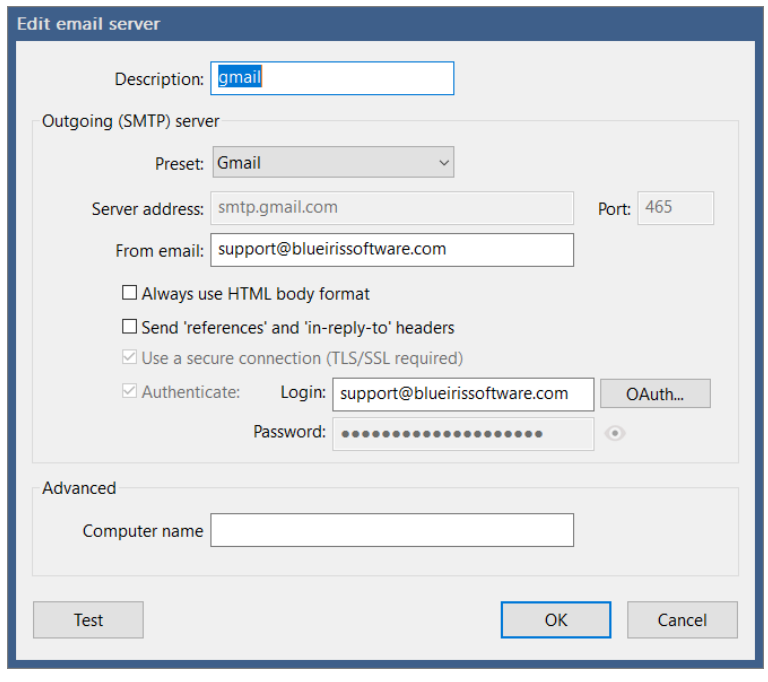
You may configure and test multiple Email and FTP server connections in Settings.

EMAIL

Email is used for alerts and notifications throughout the software.

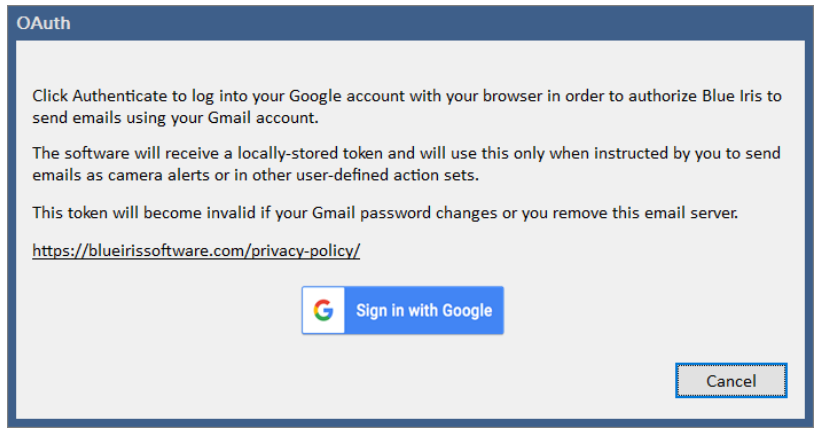


From this page, use the **Add** button to configure a new email server.



You may select from the limited list of presets, or obtain the server address and port from your email provider or ISP. Gmail is among the most commonly used email systems on the planet, so it will be used for demonstration here.

Enter your full email address with @gmail.com as the **Login**. With other email providers you will enter a **Password**, but for Gmail, you must complete the OAuth step instead:



When you click **Sign in with Google** your browser will open and you will need to login to Google and then authorize your account to be used by Blue Iris to send email on your behalf. Blue Iris receives an authorization token that is valid for 1 hour, but a "refresh token" is also used to continuously extend this connection to Gmail, until such time as your Gmail password is changed or you delete this server from Blue Iris.

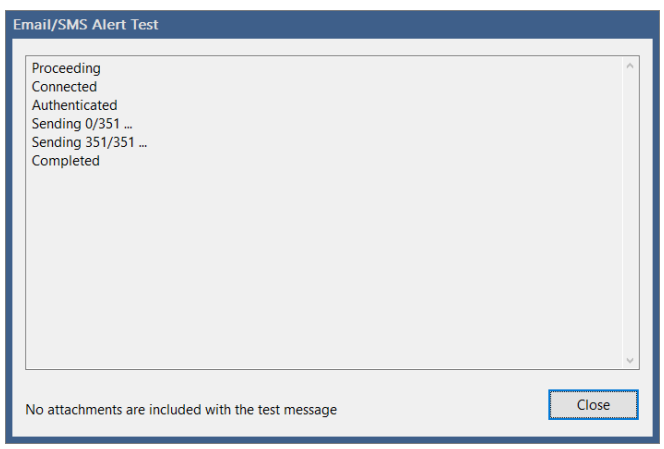
You're now ready to use the **Test** button. The **From** address will be used for all emails sent. If you require multiple from addresses, you may add the server multiple times with different descriptions.

Advanced

In SMTP, a domain name is required to identify your current computer. The default value is your current machine name. You may override this by entering a name into the **Computer name** field. Unless you have a specific reason for doing this, it is an unnecessary step.

Test

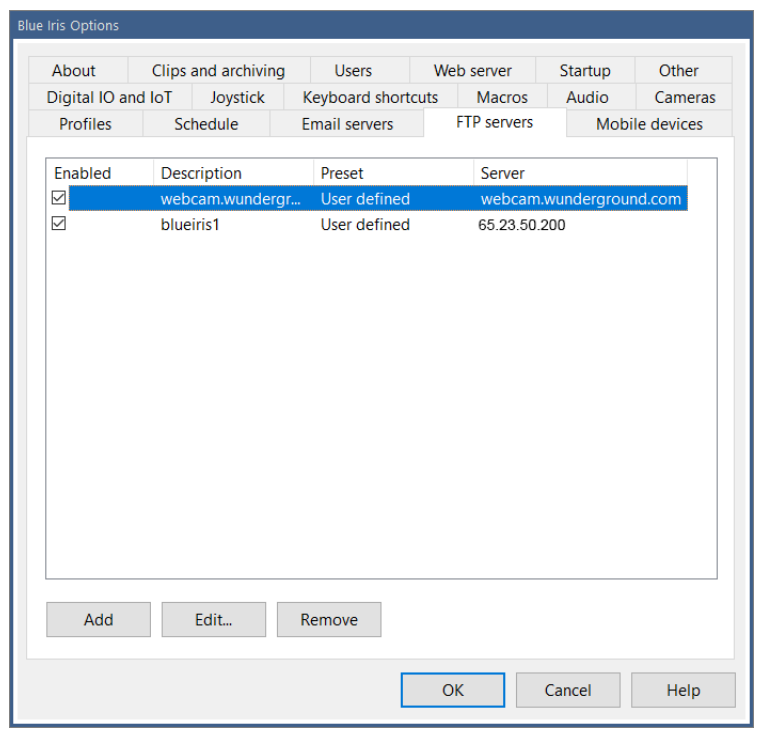
A short email is composed and sent both to and from the **From** address that you specified.



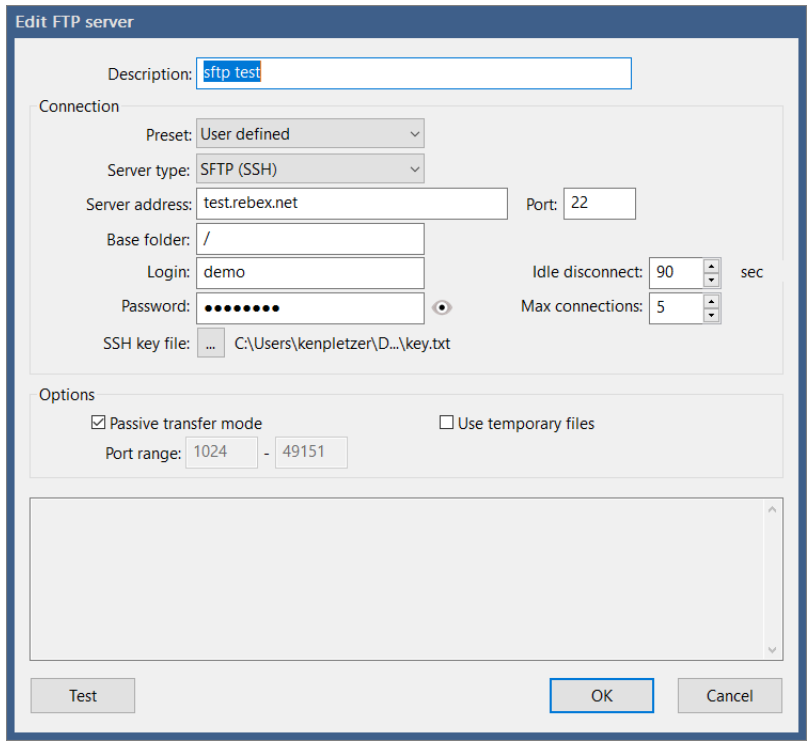
If successful, you are done! If you have trouble receiving an actual alert email that's sent when running as a service, please see instructions for properly configuring the service under that heading in the Administration chapter.

FTP

FTP is used for image posting and clip backup, but may also be used as an alert action. Please see those respective chapters for applications.



From this page, use the **Add** button to configure a new FTP server.



There are currently no presets defined—you must enter all server details. The server type, address, port, login and password should be provided your ISP. Some SFTP servers use SSH private keys in lieu of passwords and you may select a text file containing this key. If the private key is encrypted, a valid password is also required.

You must select the correct server type. The **Auth TLS** option enables **FTPS** or FTP over SSL/TLS for secure FTP transfers. **SFTP** (SSH) is also supported.

The base folder should always begin and end with a slash (/). Pages used to configure uploads in the software also have a folder setting. If that folder setting begins with /, that folder specification is considered **absolute from root** and is used in place of the base folder. If that folder does not begin with a slash, it is *appended* to the base folder:

Base folder	+ upload folder	FTP server folder
/		/
/temp/		/temp
/temp/	images	/temp/images
/temp/	/images	/images

Connections

You may select a number for the **Max connections** to make simultaneously to your server. Each connection has an **Idle disconnect** time, waiting for an additional file to be sent, before it is automatically closed. This time should be set to a value less than your server's automatic time-out period.

Options

In **Passive transfer mode**, the client makes all connections to the server. Otherwise in active mode, the server must be able to make connections to the client as well, and this is often problematic with firewalls and security software. You may select to not use passive transfer mode, but you must then open the ports that you specify on your router and forward them to your Blue Iris PC.

You may choose to **Use temporary files** when uploading. Files are uploaded using a temporary filename and then renamed upon completion. This will reduce the chances of someone downloading an incomplete file from the server.

Test

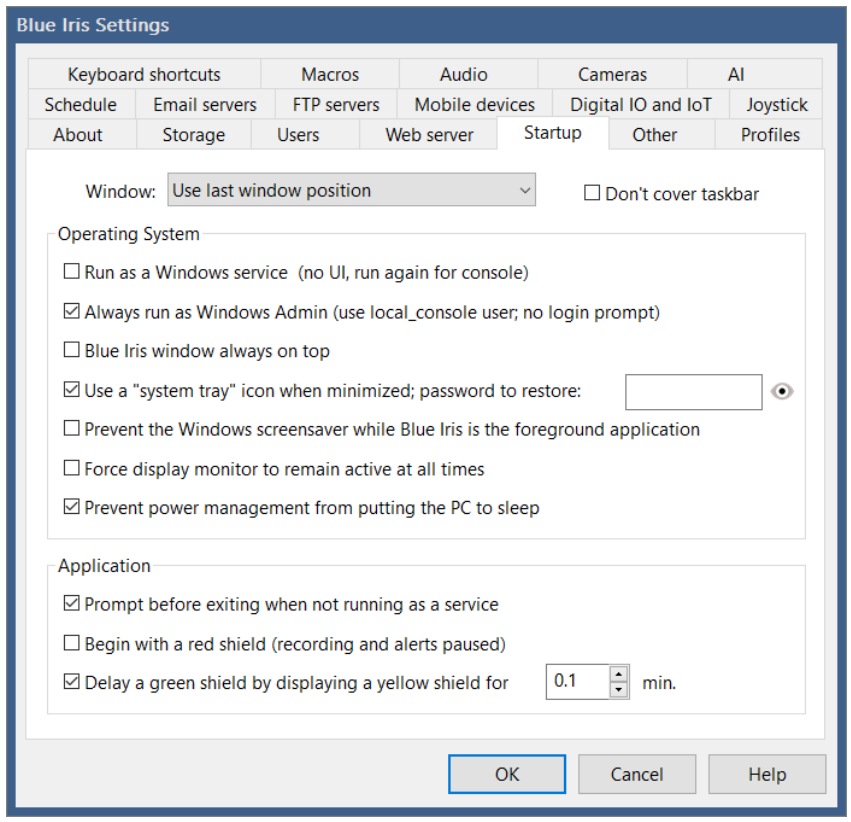
Use the Test button to test the connection by uploading a short file.

If successful, you are done! If you have trouble uploading during normal software operation while running as a service, please see instructions for properly configuring the service under that heading in the Administration chapter.

MORE OPTIONS

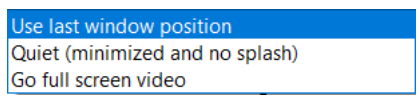
STARTUP

Many startup options control the way in which Blue Iris works with the operating system.



By default the software will re-open its main window with the same position and size.

However you may also select to (minimized and no splash screen)

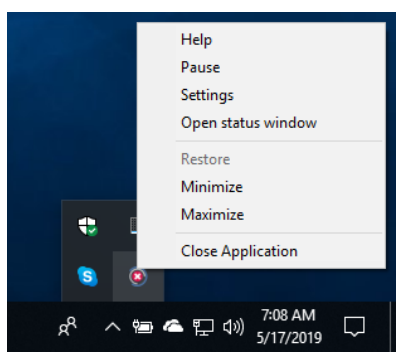


have it always open **Quietly** or to have it immediately **Go full screen video**. Some prefer to retain the Windows **taskbar** on the screen as well.

Running as a **service** or without **Windows Admin** privileges is quite an important topic, so it is covered in the next chapter on Administration.

You can force the software window to be **Always on top** of other windows on the screen.

You may have the operating system place a Blue Iris icon in the “system tray” notification area rather than the taskbar.



You may also specify a password which must be used to reopen the window. The icon has a right-click popup menu however only if there is no password set.

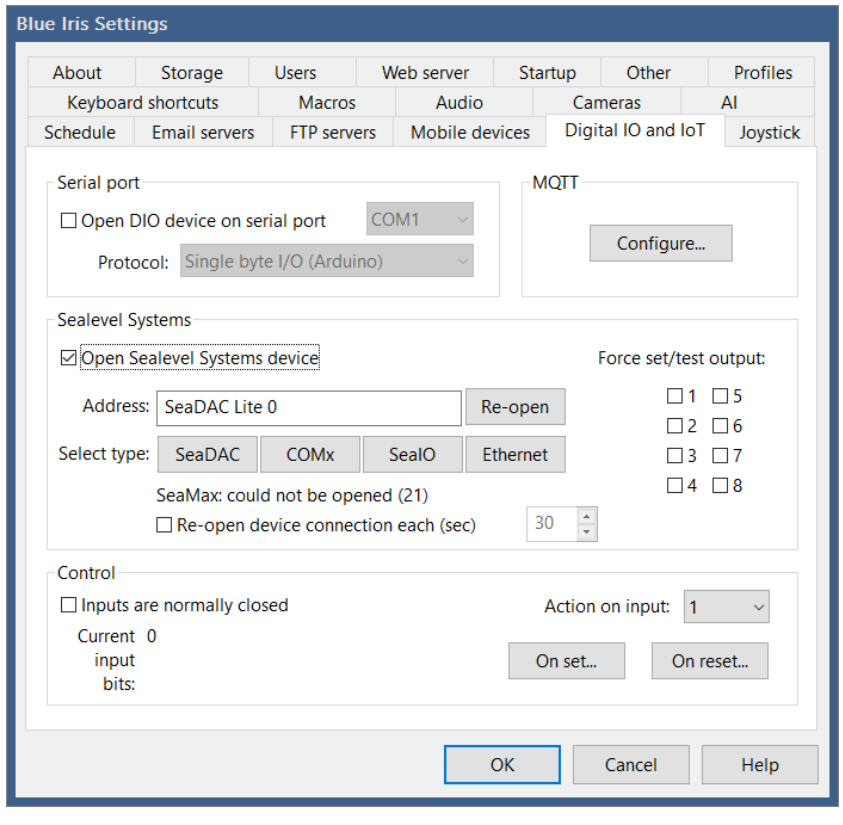
Three additional options exist to help prioritize the Blue Iris window on your desktop. You may prevent the **Windows screensaver**; you may **prevent the monitor from sleeping** due to a power saving setting; you may prevent power-saving features from **sleeping the PC** entirely.

Unless you are running as a service, by default you will be prompted for confirmation when attempting to close the software.

If you choose to **begin with a red shield**, you must manually arm the software by clicking the shield icon. Before turning green, by default the shield goes through a yellow state if the **delay green shield** option is set.

DIGITAL I/O AND IOT

Digital Input/Output and the “Internet of Things” options here provide additional ways in which Blue Iris is able to interact with external systems or hardware devices.



Serial port

This option provides simple serial port connectivity to an Arduino box, a GCE electronics controller, or similar. In addition to the COM port, assumed to be configured for **9600 baud, No parity, 1 stop bit**, you must specify the protocol to use.

A "single byte" protocol was implemented in very early versions of the software for the **Arduino**.

For setting the output signal, the software sends a *single ASCII number character* equal to the output number. That is '0', '1', '2' etc. No corresponding character is sent when the output signal is reset.

For reading input signals, the software looks at each byte received from the serial port as a set of 8 input bits—the input bits are *binary* encoded.

The **GCE electronics** protocol implemented offers more flexibility, and may still be used with an Arduino with the appropriate sketch.

For setting the output signal, the software sends *3 bytes*, always the letter 'S' followed by the ASCII output number '0', '1', '2' etc., and then either a '1' or '0' character depending on whether the signal is being set or reset.

As with the Arduino protocol selection, bytes received from the serial port are interpreted as sets of 8 bits each for 8 input signals.

Sealevel Systems

You can avoid having to work with Arduino or other device programming and scripting by using a piece of hardware more dedicated to digital I/O. We have had great success with the ease of operation and integration of Sealevel Systems devices.

https://www.sealevel.com

The software supports both USB and Ethernet variants of these devices. Devices are available with a range of inputs and outputs. Known compatible models are those that use SeaMAX such as the 8112 for USB, SeaIO such as the 8206, or 120E or 130E for Ethernet.

SeaLevel offers many other models compatible with these as well—as long as the *SM_ReadDigitalOutputs* and *SM_WriteDigitalOutputs* or *SeaIo_ReadBytes* and *SeaIo_WriteBytes* calls are supported through their driver, the device will be compatible.

The option to **Re-open the device** on a timed basis may be required if the connection is unreliable.

The **Address** field may be populated in FOUR ways depending on the driver and technology used to connect to your specific SaeLevel device:

> An **IP Address** for an Ethernet port 502 device, like the 120E.
>
> The phrase **SeaDAC Lite** followed by the device number (default **0**) for devices using SeaMax USB connections, like the 8112.
>
> The COM port, such as **COM1** or **COM3**, for devices like the 8222.
>
> The COM port number **alone**, such as **0** or **3**, for devices using legacy SeaIO drivers.

Use one of the buttons **SeaDAC**, **COMx**, **SeaIO** or **Ethernet** to select the address format and automatically search for the device.

Control

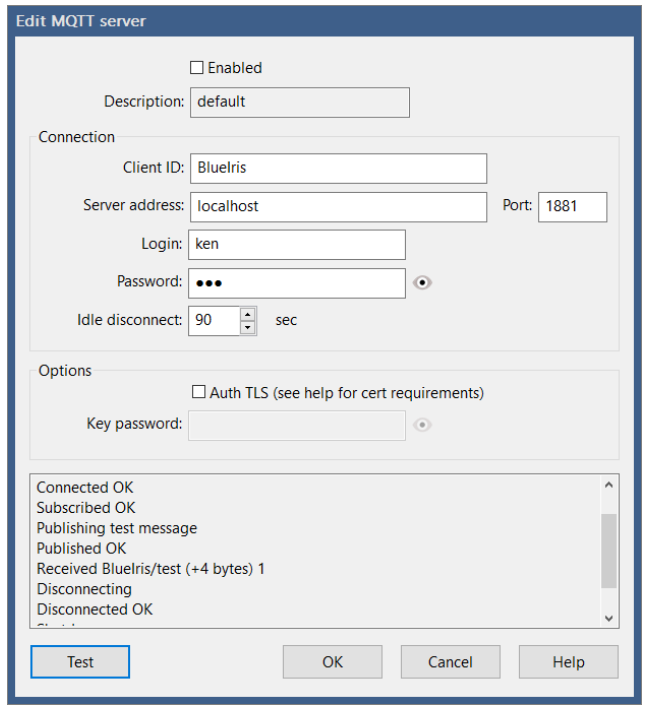
You may select whether input circuits are normally “closed” or “open” as the normal “reset” state in the software. In other words, generally when the LED is *lit* on the SeaLevel device, this is a “set” condition, but you may reverse this sense.

You may define a complete *Action set* to be executed as any input signal is set or reset. Please see the Alerts and Actions chapter for details on configuration.

A camera may be triggered based on the state of these global input bits—see the Trigger page in camera settings. Also, any action set may be configured to set these global output bits.

MQTT

MQTT is a “machine to machine” protocol for “the Internet of Things” connectivity. Please see http://mqtt.org for details.



MQTT works by having a *broker* accept connections from *clients*. Clients subscribe to or listen for traffic relevant to their function. Blue Iris is one such client. Eclipse Mosquito is one such broker that can be installed and ran on Windows, but the software can be configured to connect to a broker anywhere on the Internet. Please see https://mosquitto.org/download/ for details.

An MQTT message has a *topic* and a *payload*. A topic may have an additional sub-topic by using a slash. The software sends these *retained* messages:

Topic	**Payload**	
BlueIris/app	*starting*	
BlueIris/app	*running*	
BlueIris/app	*stopping*	
BlueIris/app	*stopped*	
BlueIris/app	*unexpected stop*	… this is the *Last Will message*

BlueIris/status	*signal=X\n* *profile=Y\n* *lock=Z\n* *schedule=ScheduleName\n*

where

X=0, 1, 2	… the state of the Shield icon
Y=0, 1, …, 7	… the active global profile
Z=0, 1, 2	… the state of the profile lock, 0=run, 1=temp, 2=lock
ScheduleName	… the current schedule name or *Default*

The software responds to these messages received:

BlueIris/admin	*camera=cam1&trigger*	… for example
BlueIris/status	responds by publishing the current global status	
BlueIris/status/cam1	responds by publishing the current status for a specific camera	

Possible */admin* commands are identical to those offered by the web server, documented in the Administration chapter.

Options

Select to use **Auth TLS** only if this is required by your broker. You **must** install a PEM file containing your CA root certificate path in the Blue Iris program file folder, by default:

C:\program files\Blue Iris 5\mqtt_ca.pem

Optionally, you may also specify client certificate and key PEM files and password if required:

C:\program files\Blue Iris 5\mqtt_cert.pem

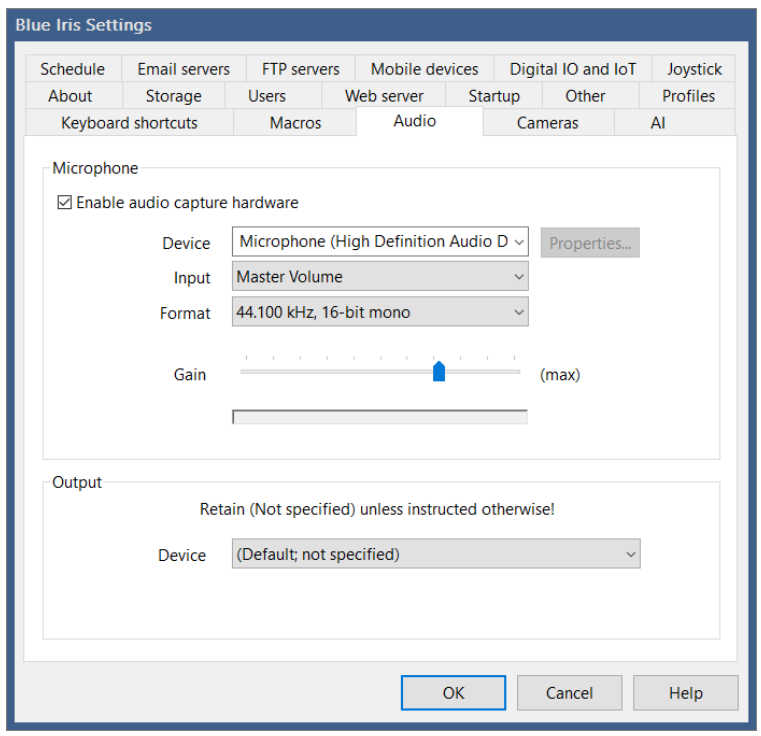
C:\program files\Blue Iris 5\mqtt_key.pem

These files must be secure and valid CA certificates, not self-signed.

The **Test** button will setup a loopback, both publishing and requesting the same topic in order to check 2-way connectivity to the broker.

AUDIO AND MICROPHONE

A microphone may be configured primarily for use with the camera *Talk* function. You must specify the device, input line, and format. A *mono* format should be selected, and generally 8000 or 11025 Hz is a sufficient sampling rate for this application.



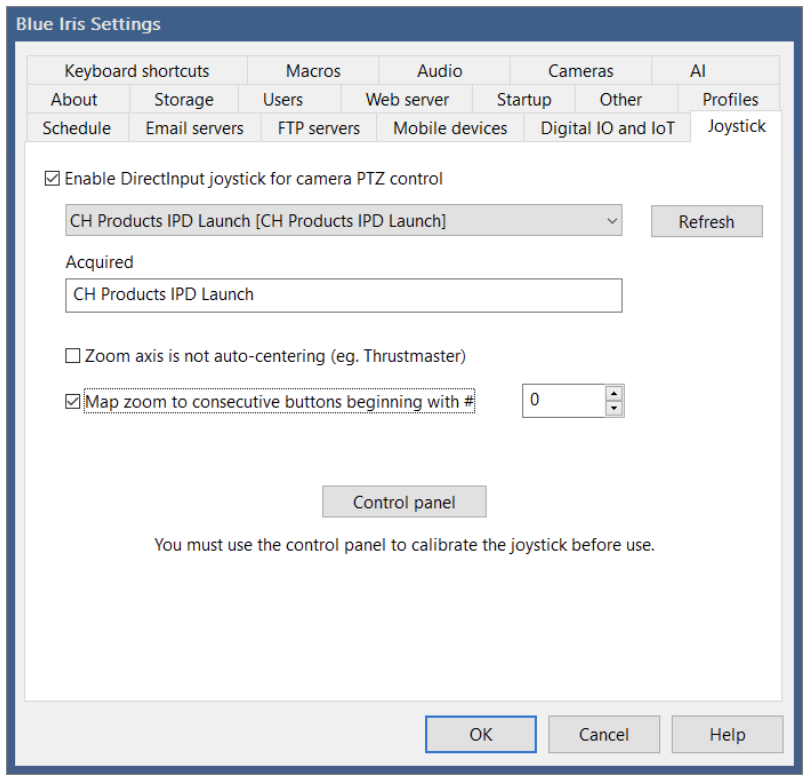
Adjust the gain so that when you speak naturally the audio power bar occupies the majority of its control window without hitting the right-hand side. When the audio power reaches this level, sample "clipping" will occur and there may be audible clicking or other quality loss as a result.

Output

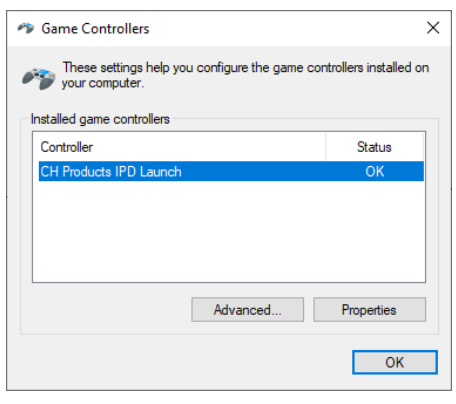
You should not have a need to change this setting unless your system has multiple sound cards and you do not wish to use the primary sound card for audio playback by Blue Iris.

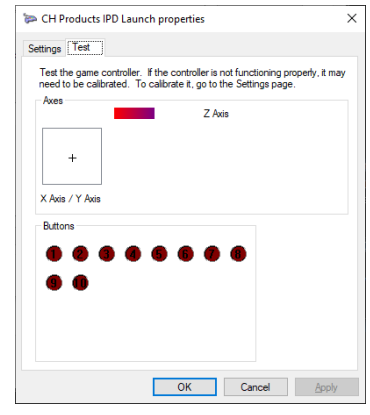
JOYSTICK

A joystick may be used for camera PTZ operation. If a compatible Windows DirectInput joystick has been attached and its driver is functioning, you will see it on this page.

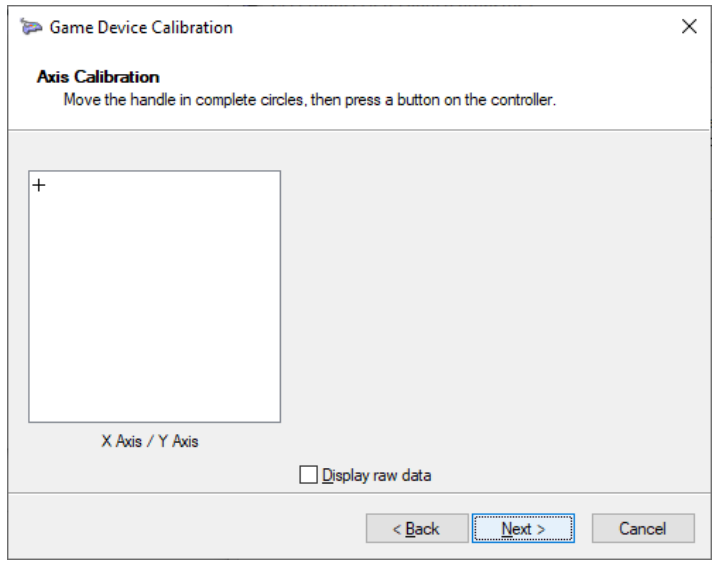


You must use the **Control panel** button to get to the joystick driver's properties page.





From here you can test functionality of the X and Y movements, as well as Z which will be used for Zoom level. The joystick buttons, if available, will be mapped to PTZ preset positions. Switch to the Settings tab to find the **Calibration** button.



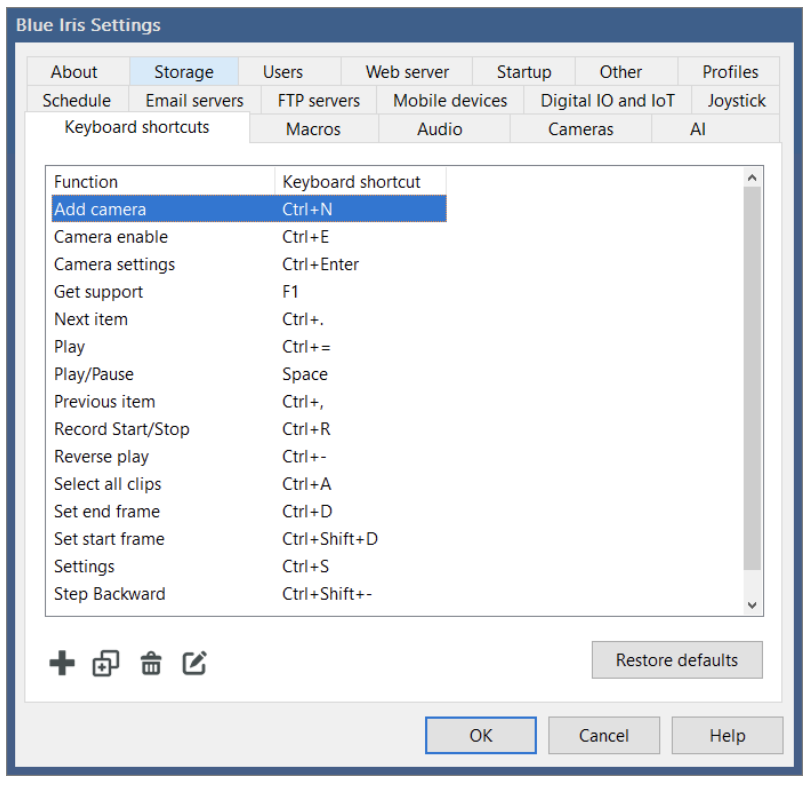
Once you have completed this calibration you can test the joystick function once again through the control panel before trying it with an actual camera window.

For joysticks without a third dimension (usually twist) for zoom, you may map two consecutive buttons for this purpose. That is, button 1 for zoom in and button 2 for zoom out for example.

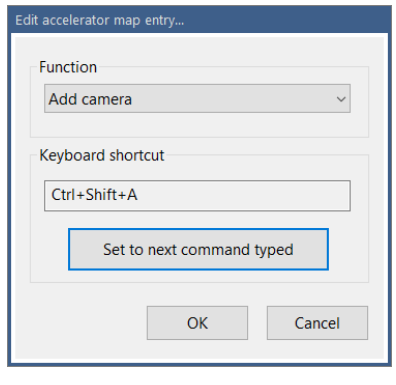
You may also map joystick buttons to software commands. Add a keyboard shortcut (see the next help topic) for Control+Shift+*x*, where *x* is a button number 1, 2, etc. When the joystick button is pressed, the associated command will be issued.

KEYBOARD SHORTCUTS

The software can memorize a number of **keyboard shortcuts** for your commonly used functions or commands.



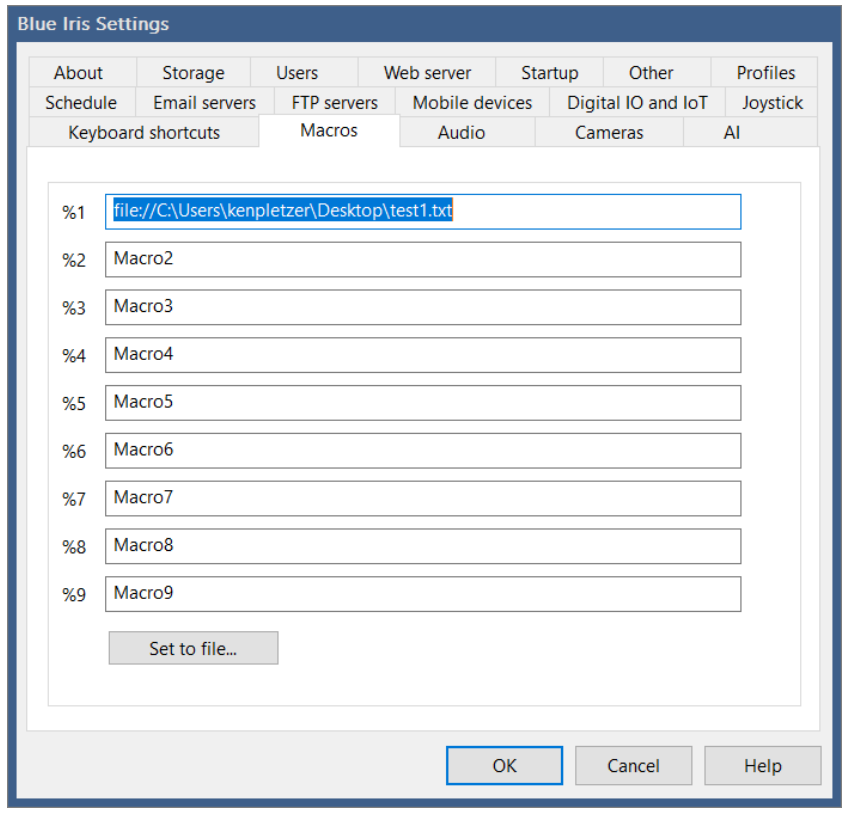
Use **Add** or **Edit** and you will be prompted



Select a function from the list and then use the **Set to next command typed** button to set the keyboard combination by example.

MACROS

A macro is text that is substituted for a shorter “token” of some sort. The macro tokens %1 - %9 may be used in camera video overlays, as well as throughout the software for things like email, push notification and SMS body and subject fields.



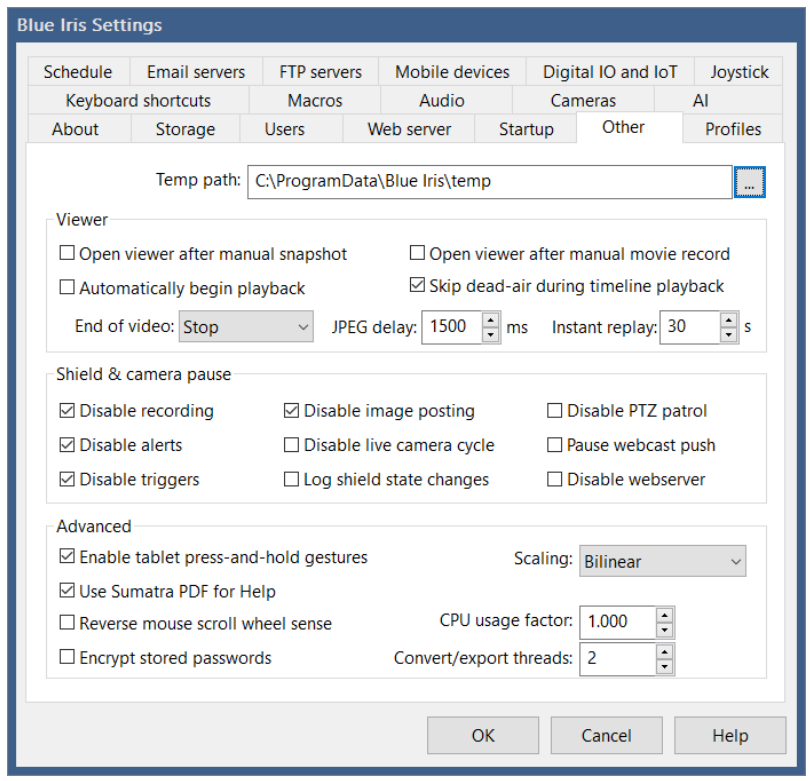
Although only 9 may be set here, the software actually supports up to 99 of these. You will find a section in the Windows registry:

HKEY_LOCAL_MACHINE\SOFTWARE\Perspective Software\Blue Iris\Macros

Other software, scripts or the HTTP/JSON interfaces may be used to write to this location and Blue Iris will immediately adopt the new text. It’s also possible to link a macro to a text file, perhaps generated in realtime by a weather app for example. The file may contain multiple lines separated with new line (hex 0x0A) characters.

OTHER

The majority of what you will find on this page has been discussed in-context in other sections. There are a few exceptions:



The **temp path** is used by the software for temporarily saving JPEG images for upload, as well as temporary files for remote management. You may select a target maximum to retain for each remote system under management, however the folder can grow quite large when clips are viewed remotely. Please ensure that this location is chosen appropriately and will not result in a *disk-full* condition on a disk used for the database or recording.

Shield & camera pause

You may control what is disabled when the shield icon is red or yellow. By default, this is recording, image posting, triggers and alerts.

Camera pause functions like the shield icon, but for individual cameras. A camera may be paused temporarily or indefinitely using options on the camera's right-click menu or through the phone client apps.

Advanced

By default the Sumatra PDF reader is used for the help file. This provides the ability to jump to context-sensitive bookmarks and a consistent user experience. However, you may uncheck this option to use the default PDF reader on your system. Your reader may or may not understand the "-nameddest *topic*" parameter.

By default, scrolling *down* with the mouse wheel is used to zoom-in, and scrolling *up* is used to zoom-out. You may be accustomed to an OS or interface which has an opposite sense, so the option to reverse this is provided here.

Your options for video **Scaling** are *Fast*, *Bilinear* and *Bicubic*. *Bilinear* will provide better quality than *Fast* and *Bicubic* will provide better quality than *Bilinear*. There is of course an increasing CPU cost. This setting does not affect the way that video is recorded, only the way in which it is drawn onto the display.

The **CPU usage factor** can be used to adjust the way in which Blue Iris displays the CPU utilization in the status bar and as is reported for remote management. If Blue Iris shows 20%, but your task manager shows 40%, please set this value to 2.00.

Select **Encrypt stored passwords** to perform an encryption on all passwords stored by Blue Iris (they are otherwise still Base-64 encoded). While this does provide strong security for your passwords in the event someone obtains access to your PC registry, the major disadvantage of password encryption is that if you must transfer your .REG settings to another PC, you will need to re-enter all of your passwords, as they may only be decrypted on the PC on which they were encrypted—not ideal for a backup/restore unless they are done on the same PC.

Note: Changing this setting does not immediately affect stored passwords until they are next loaded and re-saved.

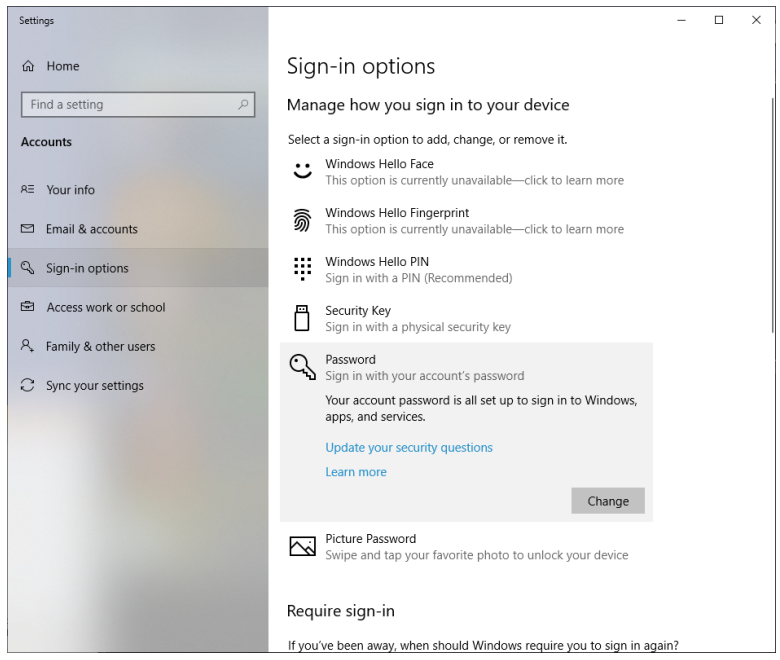
ADMINISTRATION

Management topics for getting the most out of the software.

RUNNING AS A SERVICE

The software offers the very powerful feature of **running as a service** on your PC. This means a couple of important things—when you close the main window, the software continues to run *in the background* and the software will automatically restart in the event of a PC, OS, or software crash or restart.

Enable the service on the Startup page in Settings. You will be prompted for a Windows login user and password—by default the current user. This account must have administrator rights. The software will check the password for accuracy and then add the necessary system privileges to the account. If you have not previously set a password for your Windows login, you may do that in the control panel:



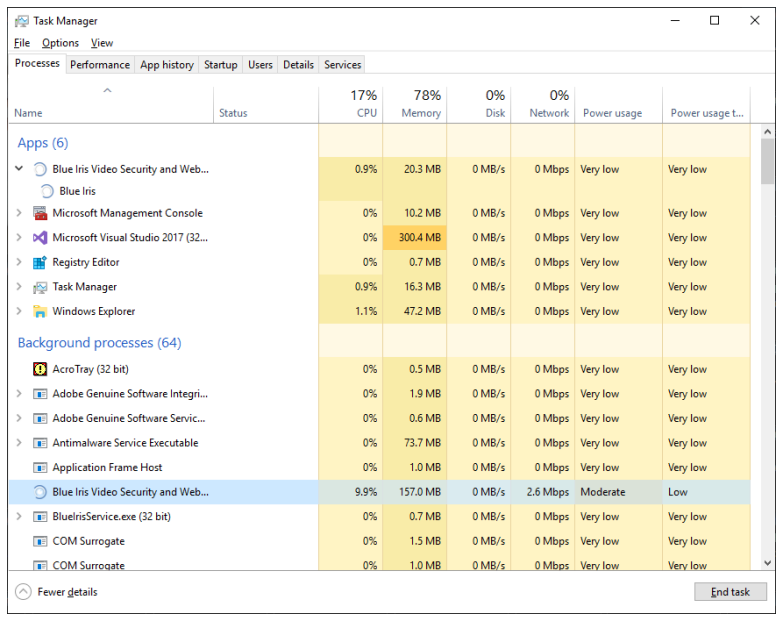
By default Windows does not allow services to run on accounts without passwords (blank passwords). You may override this with a registry setting:

> https://stackoverflow.com/questions/432570/how-to-get-a-user-token-from-logonuser-for-a-user-account-with-no-password

Although discouraged, you may instead force the software to use the *LocalSystem* account for the service by specifying a blank user name and password. The *LocalSystem* may not have the same system access as a standard Windows administrator account, leading to issues with antivirus and storage access.

Once the service is installed, you may monitor or administer its status by entering "services" in the Windows search bar to open the Windows Service Manager.

Running the software again now opens a *console* window. This second instance of the software does not actually interact with any cameras etc., it merely interacts with the service. If you open the Windows Task Manager you will see two processes:



The console shows under *Apps*, but the service shows under *Background processes*. The console generally uses negligible system resources as the heavy lifting is done by the service process. It may also be useful to use this task manager view to track software resource consumption over time to identify possible stability issues.

Service Considerations

When configuring the software—the many Test options for email servers, FTP servers and action set functions all run in the *console* process. A true test only occurs when one of these functions is accessed by the service. In general, the service will post any access issues to the Log page in Status.

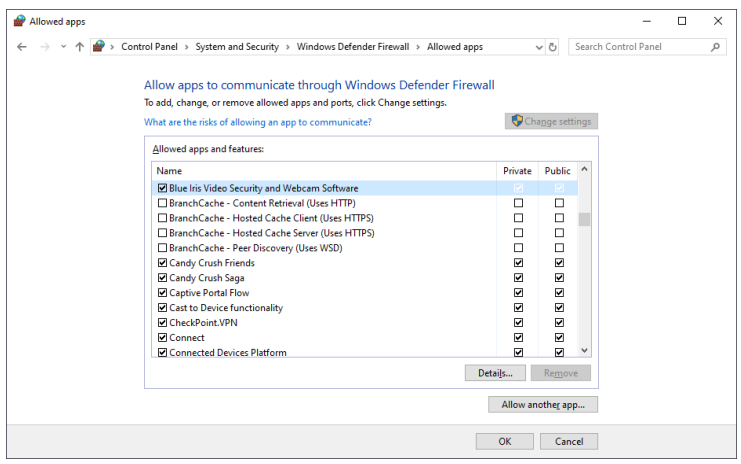
If you are using a NAS or other remote storage device, you should use a username and password on that device that is identical to your service login. This will allow the service seamless access to the device.

SECURITY SOFTWARE EXEMPTIONS

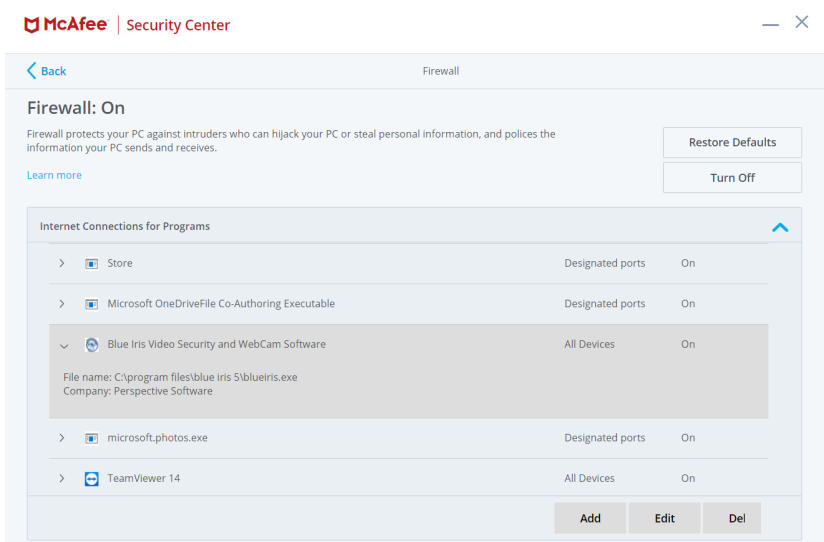
The importance of this step cannot be overemphasized. There are four categories of security software to address:

Firewall. These stand between software and use of the network or Internet. Blue Iris requires network access to pull video from network IP cameras. Blue Iris also uses an occasional connection to the Blue Iris Software website to check for software updates, license activation, and changing WAN address if this is configured on the About page in Settings.

Here's what the firewall exemption looks like in Windows firewall:



Here's what the firewall exemption should look like in McAfee:

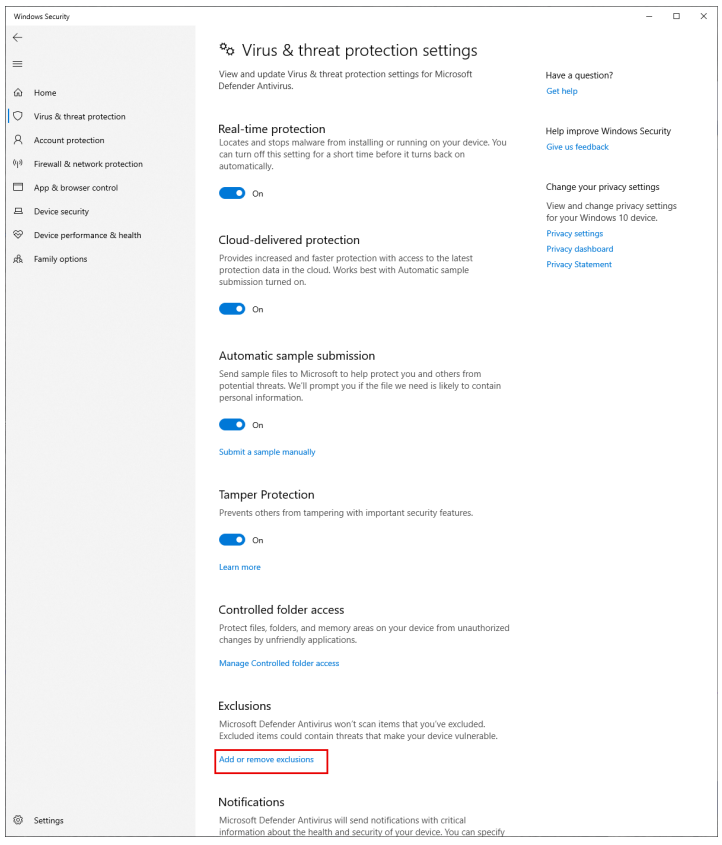


Antivirus. These monitor files or folders for changes, looking for threats. These may interfere by locking files which Blue Iris is actively modifying or attempting to delete. For smooth and efficient software operation, you should exempt the database and clips storage folders. Blue Iris never creates or uses executable code in these folders.

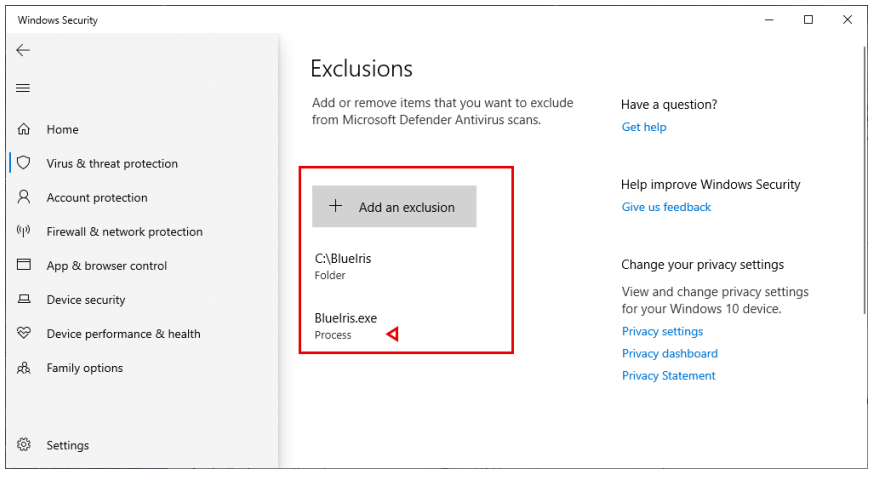
Application and process scanning. These monitor actively running software and every byte of information sent or received for suspicious activity. These are by-far the most intrusive and

can greatly affect software performance. For proper efficient software operation it is highly recommended that you exempt the *BlueIris.exe* executable as well as the supporting file *BlueIrisAdmin.exe* from this type of scanning. In the past, this type of "security" software has been responsible for otherwise unexplained memory leaks and broken camera streams. These software like to "cache" network communication, and in the case of a camera video stream, this can be gigabytes of information each day, often overwhelming memory or disk resources with endless "temp" files.

Here are the critical exemptions shown in Windows Security:



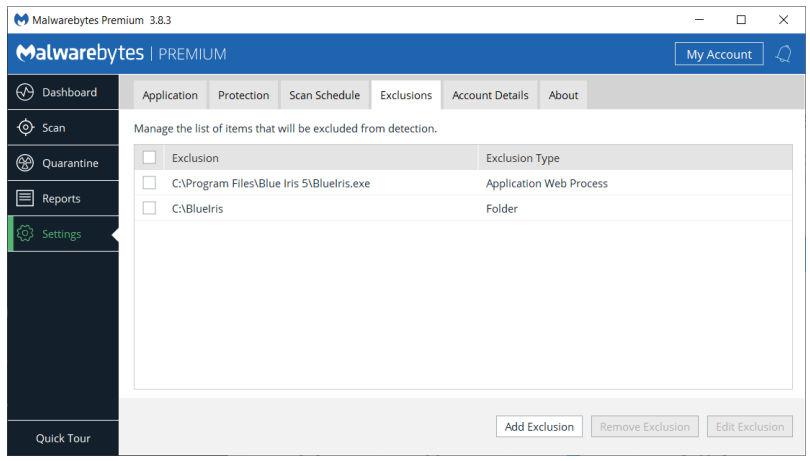
Under Virus & thread protection settings, find Exclusions and use the *add or remove exclusions* link:



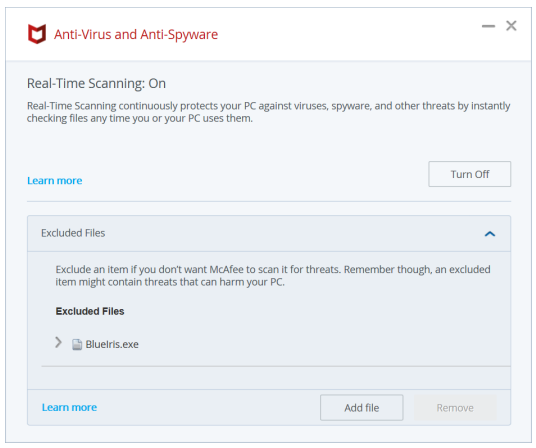
BlueIris.exe should be added as a *Process* exclusion, while the C:\BlueIris folder should be excluded as a *Folder*.

Note that some security software packages replace the links on this page with links to their software's own custom settings pages.

Here's what the exemption should look like in Malwarebytes:



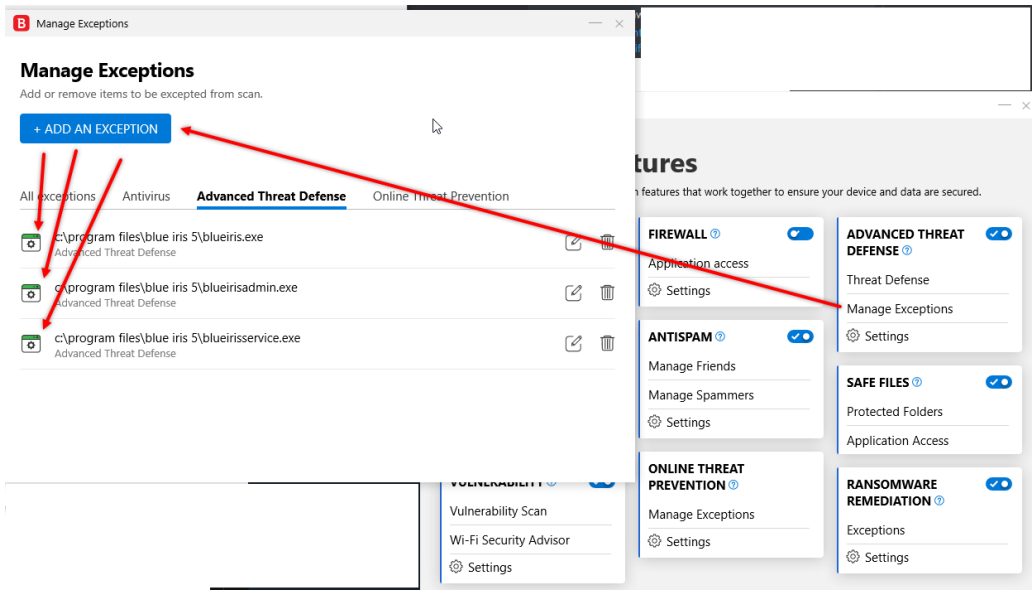
and in McAfee:



Here's what to do in Sophos (you may have a crash in Hit Man Pro); add a "local exclusion":

https://support.home.sophos.com/hc/en-us/articles/360000501206-Adding-local-exclusions-Allowing-Installations-and-or-applications-to-run

Here's what to do in Bit Defender:



Registry cleaners. Problems here are two-fold. Sometimes these like to "back out" changes, which mean that your Blue Iris settings may be completely rolled-back or un-done. Also as was notoriously the case with Kaspersky, a shadow copy of each registry change was maintained *within* the Blue Iris registry key—soon leading to gigabytes used for the registry and making settings backups painful, if possible at all. If it is not possible to exempt specific software or registry keys, it is recommended not to use such software at all.

All of these software will use CPU time and other system resources and should be added or used thoughtfully.

WINDOWS ADMINISTRATOR ACCESS

Blue Iris is security software, and as such requires Windows Administrator access to the PC. All settings are also stored in the Windows system registry under a location only accessible by a PC administrator. It is possible to configure the software to allow access by non-administrators in a couple of ways.

First, when running as a service, you can *un-check* the default option on the Startup page in Settings to **Always run as Windows Admin.** You must also:

- Configure a user/password on the Users page in Settings. The user will be prompted for this when running the software. Although you may select Admin access for this account, the user will only truly have Admin access if they are a Windows system administrator.

- Provide a desktop icon link to BlueIris.exe instead of BlueIrisAdmin.exe

Instead, you may alter the access rights on the registry key used by Blue Iris to include non-administrators. The software checks writability to this key when determining if Administrator access is allowed. Open REGEDIT and locate the key.

HKEY_LOCAL_MACHINE\SOFTWARE\Perspective Software\Blue Iris

You may edit the permissions on this key to provide *full control* to the *Everyone* user or to a specific user or group.

You must still run BlueIris.exe instead of BlueIrisAdmin.exe to avoid the Windows UAC authentication prompt.

CPU MANAGEMENT

It's common to struggle to find balance between software demand and CPU capability. If you find your system is sluggish, you may be asking too much of the CPU. If the Windows Task Manager shows consistently high CPU usage (at or near 100%) for extended periods of time, this should be addressed to maintain system stability. It is advisable to leave some "head room" here as well, perhaps shooting for an average CPU utilization over time of no more than 60-75%.

In order to understand how to maximize your CPU performance with Blue Iris, you must understand where CPU demand originates.

Decoding

By default, all video received from each camera is *decoded*. This means the bytes received are used to reconstruct an image or video frame for display or further analysis. This may be performed in software or in hardware if you have a compatible Intel chip or Nvidia graphics card. Please see *Advanced video topics* in the Cameras chapter for details. When this is performed by software, it is preferable that the video was *encoded* as simply as possible to save CPU cycles when decoding. See your camera's internal web-based settings to manage this—you want to select H.264 "main" profile without any "high" or "+" or "smart" modes enabled—all of these are designed to save *bandwidth* at the *expense* of CPU.

It's also possible to instruct the software to *not* decode each and every video frame. This is done with the **limit decoding** option on the Video page in camera settings. Please see discussion of that topic in the Cameras chapter for proper use of this feature—a minimum rate of key frames in the video stream is required.

Just as software decoding has intrinsic limits, so too does hardware decoding. If you begin to see frames/second throughput by your cameras begin to *decline* from expected values over time, this may indicate the hardware decoding is saturated and you should remove one or more cameras from hardware decoding.

Encoding

By default, Blue Iris uses software to *re-encode* each video frame that's written to disk. This refers to conversion of each image into a *compressed* set of bytes, and this can be much more CPU-intensive than video decoding as the software works to create the smallest set of bytes

possible for each image in a series of images. Fortunately there are two technologies which will greatly reduce the CPU's role in this process:

Direct-to-disk recording. Video is already received from the camera in an encoded format—why not just use this for recording as well? Please see the various pros and cons for using this under the *Video file format and compression* topic in the Recording and Clips chapter. For example, as with *limit decoding,* there is also an optimal key-frame rate for use of this feature.

Hardware encoding. Some Nvidia hardware may also be leveraged for video *encoding*. Please see the same matrix in the *Advanced video topics* in the Cameras chapter for details. Hardware encoding is enabled on the various *Video encoder settings* pages provided on the Format page from the Record page in camera settings and elsewhere. One obvious "con" with this technology is that it often sets up a "pipeline" of video for encoding, which translates to a delay in getting video out of the encoder, which translates to initial "blackness" in playback.

Webcasting

When you connect to the server with a browser or phone app and stream the All cameras view, video is *required* from all cameras (meaning it must be decoded), resized and composited into a single image, and then *re-encoded* according to client specifications. This often results in a perfect storm in terms of CPU demand. Here are a few strategies to avoid saturating the CPU:

- Create groups with fewer cameras.
- Consider disabling webcasting of the "all cameras" group altogether.
- Lower the FPS on the group image, typically 5 is adequate for a group image. This is done on the group settings page using the gears icon found next to the group selection box.
- Lower the resolution of the group image.

Drawing to the screen

The more that is drawn to the screen directly translates to more CPU time used. Whenever possible, keep the console minimized or completely closed if running as as service. There are also options to control the rate and quality of drawing to the screen. **Limit live preview rate** is found on the Cameras page and **Scaling** is found on the Other page in settings. These adjustments do *NOT* affect the quality of video that is recorded or viewed remotely.

Drawing onto the video

By default the software draws the date and time to each frame, which will use typically a nominal amount of CPU time. If this has been made more complex, possibly adding shading or transparency or graphic images, the CPU usage may ramp up, potentially saturating the thread. You can identify this situation when the frames/second throughput for the camera begins to *decline* from its expected value as you increase overlay complexity.

For ultimate CPU performance, you can completely eliminate video overlays via an option on the Video page in camera settings. Note that when in demonstration mode, a banner is drawn to each video frame to this effect, which may contribute to initial CPU utilization before license activation. If you counter-intuitively see CPU usage go UP when the software is licensed, this may indicate a higher frame throughput when the overlay is removed.

Writing to the hard drive

With properly efficient hardware, this is not always a concern, but it does have the capability to severely slow things down. You should always use a local, fast drive for the database and *New* folders to prevent OS lag as these locations are accessed frequently. These folders should also specifically be exempted from antivirus software which may be constantly scanning them for changes. Finally, a failing drive often first manifests itself by causing excessive CPU time for operations, as the OS struggles to find areas on the media without errors. Significant *fragmentation* may also be a concern as well, causing the drive to work overtime accessing locations across the media for a single file. If you suspect an issue with a recording volume there are many Windows utilities for testing and optimizing these.

Use of a high-speed drive will also help if your system is recording from many cameras simultaneously. For example, a high-speed SSD drive or 7,000-10,000 RPM hard drive will offer performance gains over a standard 5,000 RPM drive.

Moving memory

Not surprisingly, CPU time is consumed with many basic memory move operations, and these can be significant with video streaming and playback software. A video image with 1920x1080 resolution in 32-bit RGB format occupies 8MB of memory for example and copying or moving this memory around is not trivial when it is done with frequency. The easiest way to combat this is with more CPU cycles—a faster CPU. However there are other efficiencies gained by newer CPU technology. The overall QuickSync score given to chips on

the ark.intel.com page also impacts the efficiency of the chip allocating and moving large blocks of memory.

Video analysis

By default, Blue Iris analyzes 1-2 frames per second of video from each camera to look for motion. The algorithms employed are fairly simple and not in general CPU-intensive. However, when motion is detected, the rate of analysis goes up to at least 8 frames per second in order to more accurately follow objects. If you do have a number of cameras with a considerable amount of activity, this may begin to contribute (still in a small way) to the overall CPU demand of the software. There are a couple of ways to mitigate this:

- Do not use the "high-def" setting on the Motion detector page. This uses up to 4x the number of pixels as input to the algorithms.
- Don't use the "Gaussian" algorithm.
- Consider using camera-based motion detection if offered by your camera. This does require that the camera supports and is configured to use ONVIF *GetEvents* via *PullPointSubscription* and that the software understand the type of events the camera is sending (this is not standardized). You can view what the camera sends in response to motion or other triggers using the *Events* page in the ODM (ONVIF device manager) software.

Dual streaming

If your camera offers multiple streams, you may instruct the software to use one for recording and audio (the "main" stream) and one for everything else (the "sub" stream). This may be done for RTSP cameras by specifying a second video path on the Network camera configuration page from the Video tab in camera settings. You must also have recording configured as "direct-to-disk."

Dual streaming saves CPU time with video decoding, encoding, as well as video analysis for motion detection. The only downside is the increased bandwidth used to pull two streams from the camera, as well as the associated increase in potential signal loss now with two points of failure.

PC and Windows considerations

Many PCs, especially laptops, offer power-saving modes which have the effect of lowering overall system performance. You may manage these settings via the system BIOS typically, a special key combination used as your PC starts up. You will want to favor performance over battery or power consumption for most video software applications.

Many PCs also employ something called *thermal management*, where the CPU is intentionally handicapped if the temperature is such that it might cause hardware failure. While in general it seems like a good idea to protect your hardware in this way, it is wise to check for adequate PC and CPU ventilation in order to prevent these "features" from activating and slowing down your system.

Not all device drivers are of equal quality. Your SSD device may have impressive stats, but you may need to run a performance test on the device to determine exactly how fast it's able to read and write given the OS and its drivers.

You will want to disable CPU and disk-intensive OS features such as *file indexing* via the Windows Settings page.

How to measure and compare relative CPU utilization

If you have a CPU utilization issue, the first thing to do is to determine a *baseline*. With Blue Iris *not running* you want to open Windows Task Manager and see 0% used by the system most of the time. Various things like Windows updates and file indexing may use some transient CPU cycles. However there may be other even less-efficient services installed for the various other hardware and software you may have installed on the PC. This is a good time to audit what's installed and to analyze the amount of CPU each might potentially consume.

Now with Blue Iris running with *all cameras disabled,* you again should be at or near 0% CPU utilization. There may be Blue Iris features such as the web server or file management still operating, as well as occasional screen updates to draw the status icons, etc., but these should consume negligible CPU at this point.

Now with the Shield icon *RED*, you may enable one camera and then *minimize the window* to evaluate the amount of CPU simply to stream and decode that single camera. You can try this with each camera in-turn, or with groups of cameras. It may be possible to identify cameras with inefficient encoding/decoding in this way.

Finally you may enable other software features such as recording by setting the shield icon to green, with one or more cameras enabled for further analysis.

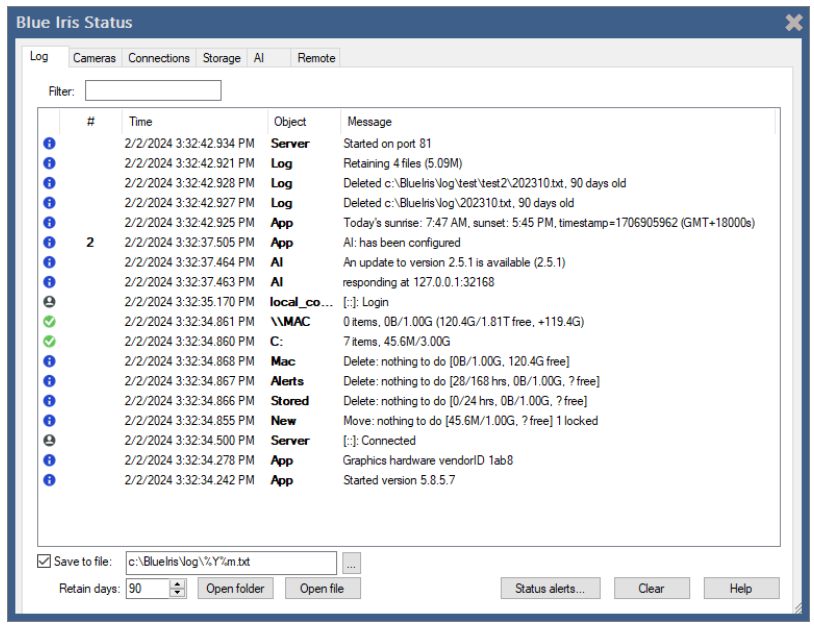
The Bottom Line

The bottom line is that the software *will* attempt to do all that you ask of it until there are just no more CPU cycles to consume, and at that point, something must give. Ultimately the best way to handle a CPU time shortage may be to either (1) process fewer MP/s (megapixels/second, a function of both FPS and frame size) or (2) get a faster CPU and/or one with better graphics capabilities if possible.

If you write to support about a CPU issue, please always include an image of your Cameras page in Status. This will give an overview of the FPS, kbps and MP/s consumed by each camera and in total for the system.

STATUS MESSAGES, LOGS AND ALERTS

The Log page in Status is where you will find warnings, errors, and other communication from the software that does not otherwise appear in any type of popup message box.



If there are errors or warnings on this list, a corresponding status icon will appear in the software's status bar at the lower-right of the main window.

The first column contains an icon representing the "severity" of the log entry—informational (i), warning (yellow caution triangle), or error (red X). The # column acts to "roll-up" multiple recent (occurring within 30 minutes of one another) and repetitive entries. The *Object* column may be a camera "short name" or a storage folder name, but may also be a more general system component like Clips or App. If the Message contains a colon, only the portion of the message that comes before the colon must match another message in order to cause it to replace that message and increment the # column.

For a more permanent record of what's added to this list, you may use the **Log to file** option. By default, a new log file is created each month to prevent it from growing too large. For your convenience, buttons are provided for **Open folder** and **Open file**.

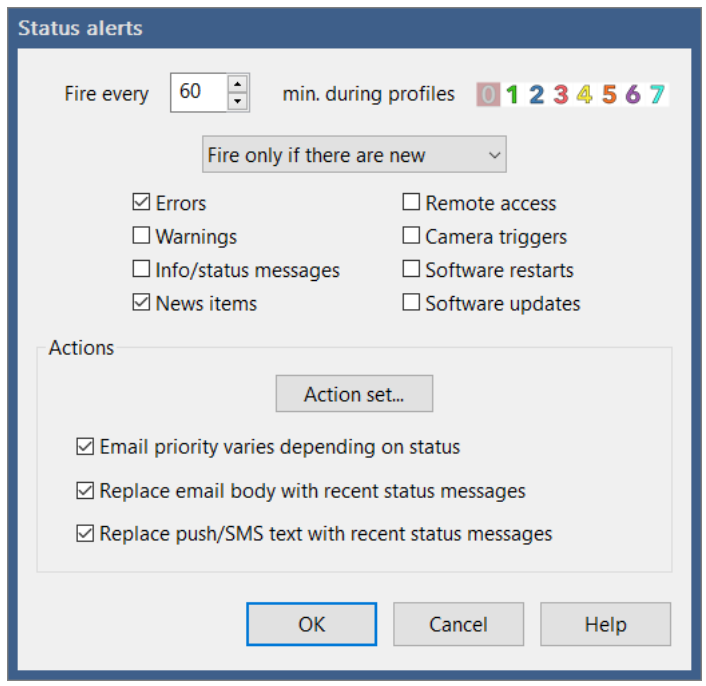
The default log filename format and location is

C:\BlueIris\Log\%Y%m.txt

The %Y macro becomes the 4 digit year and the %m macro becomes the 2 digit month.

Any .txt file in this folder (and its subfolders if you add them to the format) will be pruned automatically at the beginning of each day once that file's age exceeds your **Retain days** specification.

Use the **Status alerts** button to configure periodic status messages via email, push, or otherwise.



You may select the rate at which these may be sent, along with which the active profiles.

Always fire

> You may wish to receive periodic messages simply as a “health” notice.

Fire only if there are new

> Typically however you are interested in receiving messages only when there are new items of interest added to the Log page in Status, and you may choose which types are of interest.

ALSO fire each minute if there are new

> Combines the previous two options so that you receive period notifications regardless, but more timely notifications for specific items of interest.

Actions

The types of messages used to communicate these status alerts are configured with an action set. Please see the Alerts and Actions chapter for details on this configuration.

Typically you will want set all of the options here to **vary the email priority**, **Replace email body** and **Replace push/SMS text** with recent status messages.

Important note: text/body replacement requires that the action’s text/body is blank or remains set to its default value.

BACKUPS

Software Settings

Options to **Export** and **Import** software settings may be found on the About page in Settings. The complete software settings reside within a .REG registry keys file and may also be found via REGEDIT at the key

HKEY_LOCAL_MACHINE\SOFTWARE\Perspective Software\Blue Iris

If you select the **Auto export** option, you may select a folder location for these files. The software maintains a rolling set of three files, always from three different days. These are updated only when the software service is restarted. Restarting the software multiple times on a single day results only in the replacement of just one of the backup files.

The default registry export format is compressed and this format is required in order to use the Import button. However if you hold the Shift key while clicking Export, the file will be saved in a human-readable text format. To re-import this type of registry file, you must double-click it from Windows; it may not be imported with the Import button.

It's also possible to manually Export/Import individual camera settings via buttons on the General page in camera settings.

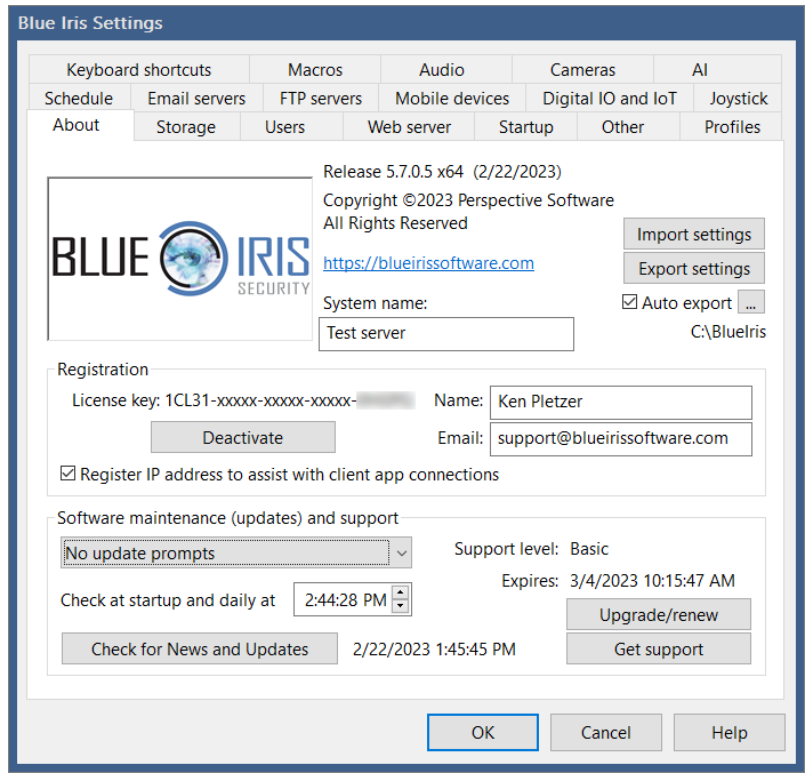
Recorded Video

Using the Backup settings on the Clips page in settings, you may choose an FTP service to be used to upload marked clips. Clips may be automatically marked for backup by using settings on the Record page in camera settings.

Some users prefer to synchronize one or more of their recording folders with a cloud service and this is certainly possible. Management of this type of backup is beyond the scope of Blue Iris support however.

REGISTRATION AND SOFTWARE MAINTENANCE

Open the Settings About page by using the menu icon at the top-left of the main window:



The software is licensed *per-PC (or VM)*. You may re-install and move the license to new hardware up to 10 times before it must be manually reset by an email to support. A license includes *basic* maintenance which means access to email support and software updates for one year from first activation.

Please *register* your software. This is done simply by adding your **name** and **email** on this page. This information is *never* shared with others, but may be used to assist with the look-up of your license key if you have misplaced it. Registration details here override any purchase records. Registration of your **IP address** is optional, but it helps when using the remote client apps to look-up the (possibly changing) address using only a portion of your license key.

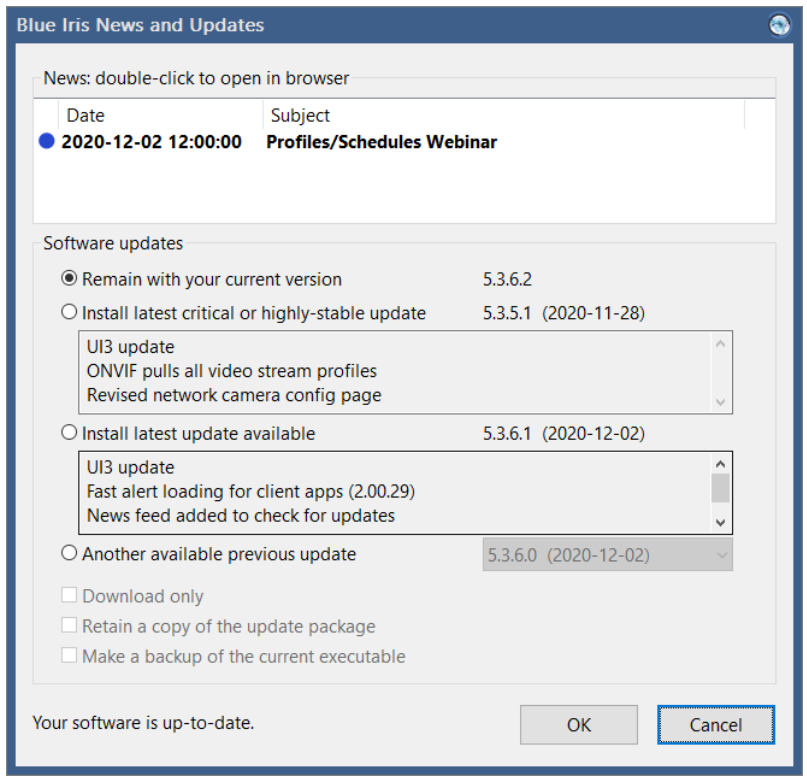
For continued access to software maintenance (all updates, including free major-version *upgrades* as well) including email support, there is an *optional* annual maintenance program. For details please visit:

https://blueirissoftware.com/support/

Although continuous Internet access is not required, the software either must be connected to the Internet occasionally to check for updates and licensing, or the license must be re-entered at least once each year using offline methods as the maintenance date expires.

If expiring soon, please use the **Upgrade/Renew** button to either purchase a new plan, or to enter the maintenance key that you will receive via email each year.

It's also possible to check manually for software updates, or automatically to install them at a particular time of the day when running as a service. For automatic updates, you may choose to install only occasional critical and known highly-stable updates, or you may choose to install all available updates, which may occur very frequently as daily development occurs. To explore all available updates, use the **Check for News and Updates** button.



If you choose to **Download only** or to **Retain a copy of the update package**, it will be placed into a new folder Updates found in the Blue Iris 5 program files folder. If you choose to **Make a backup of the current executable** that will appear in the Blue Iris 5 program files folder alongside BlueIris.exe.

For your own security, please do not attempt to download or install updates when the software license is not covered by a maintenance plan. If you do download versions for which your license is unauthorized (those released while your license was not covered by maintenance), the software will run in an evaluation mode.

When writing for support, you must include basic software and license details. For your convenience you will find an **Email support** button on this page. This button will copy important information to the Windows clipboard. In order to make use of this information, you must them open an email to send to support@blueirissoftware.com. Please make the subject descriptive in order to prevent our mail server from combing it with others of the same subject. In the *BODY* of the message (not the subject), use the Windows *PASTE* command (control-V) to insert your support information at the beginning of your message.

Please take advantage of our user group support channels as well, as often you will find others with similar hardware, conditions, or questions, who will offer assistance as well. The official forum may be found at the address:

https://blueirissoftware.com/forum/

The new Blue Iris Support YouTube channel will contain archives of support webinars beginning October 2020 as well as other valuable content:

https://www.youtube.com/c/BlueIrisSupport

And there's even a Blue Iris Facebook page. Please note that the developers may not actively monitor these pages.

Although you may stumble upon other camera forums online, you are advised to proceed with caution. Specifically, please know that we are not directly associated with the IPCamTalk Forum.

HTTP INTERFACE

In addition to Digital I/O and MQTT services, Blue Iris also offers significant opportunity to interact with and to manage the software through a web server interface.

HTML Macros

Blue Iris pre-processes all files ending in *.htm* before they are served. If you're using a dynamic IP address, Blue Iris will substitute %%SERVERNAME%% for your WAN server address wherever it appears. Other available macros include the following:

%%AUTHEXEMPT%%	unknown, no, user, admin
%%AUTHSTATUS%%	unknown, user, admin, anonymous
%%SERVERNAME%%	Current host name and port used to access the server
%%SERVER%%	Current host name without the port number
%%SESSION%%	Current session key
%%VERSION%%	The software version in the format 5.0.8.2
%%SHOWALERTS%%	0, or 1 if there are new alert images for the current user
%%SYSNAME%%	System name as defined on the Settings page
%%AUTHORIZATION%%	If basic authentication is used, the base-64 encoded USER:PASSWORD
%%CAMLIST%%	A list of HTML <OPTION> tags containing the available cameras and groups
%%CAMLIST2%%	An alternate/simpler version of CAMLIST
%%CLIPLIST%%	A list of HTML <OPTION> tags describing the clips currently displayed in the Clip List. HTML parameters are supported: &cam= a camera or group short name &days= x500, the beginning clip number on the list (days=3 to begin 1500 into the list) &alerts= 0 for all, 1 for alerts, 2 for flagged
%%CLIPn%%	A virtual path to the actual "nth" clip currently displayed in the Clip List using the cam and alerts parameters
%%THUMBn%%	A virtual path to a thumbnail image for the "nth" clip currently displayed in the Clip List using the cam and alerts parameters
%%CAMNAME0%%	DEPRECATED. The first camera's name
%%CAMPORT0%%	DEPRECATED. The first camera's webcasting port number

Direct image and video requests

There are a number of methods for retrieving images and video from the Blue Iris web server for use on mobile devices, converting a USB camera into a web camera, or for any other purpose. Here are the paths to these methods:

/image/{cam-short-name} A single JPEG image from a specific camera or group, with optional parameters (see below). You may also add *&clean=1* to provide an image without overlay text or graphics.

/mjpg/{cam-short-name}/video.mjpg. An M-JPEG stream. This stream is compatible with Blue Iris's "MJPEG stream request." Note that *{cam-short-name}* may be a group name or @ followed by the group name for auto-cycle.

/h264/{cam-short-name}/temp.h264. Pull a raw H.264 stream (MIME type video/H264). This stream will play in a tool like VLC. Note that *{cam-short-name}* may be a group name or @ followed by a group name for auto-cycle.

/h264/{cam-short-name}/temp.ts. Pull an MPEG-2 transport stream (MIME type video/MP2T).

/h264/{cam-short-name}/temp.m or *.m3u8*. Pull a virtual M3U8 file (MIME type application/vnd.apple.mpegurl). This will play in QuickTime, iPad and the iPhone using the Apple HLS (HTTP Live Streaming) format.

/audio/{cam-short-name}/temp.wav. Pull a raw audio stream (MIME type audio/x-wav).

/time/{group-name or cam-short-name}. Pull a timeline playback stream. The following options are available:

w	viewport width
h	viewport height
speed	playback speed in percentage (100=normal playback speed)
pos	playback time in milliseconds since January 1, 1970
solo	prioritize the selected camera, either 1-up or solo as configured
addmotion=1	include direct-to-disk BVR motion rectangles
addoverlay=1	include direct-to-disk BVR overlays
isolate	use a unique/dedicated playback object for this request
jpeg	return a single JPEG image instead of a stream

/time/set. Change parameters for current */time/* stream. The following options are available:

sel	change camera selection: *sel={cam-short-name}*
pos	playback time in milliseconds since January 1, 1970
jump	1 or -1 to skip to the next or previous alert or clip
speed	playback speed in percentage (100=normal playback speed)

/video/{cam-short-name}. Used by client apps to pull an H.264-encoded video stream with proprietary formatting.

/file/clips/{filename}?mode=mjpeg&speed=100. An M-JPEG stream of a clip from your New clips folder. You may include additional subdirectory names in the filename. The speed parameter is optional, a percentage of normal playback speed. For a direct-to-disk BVR, you may also add optional parameters *&addmotion=1* and *&addoverlay=1* if you would like motion rectangles or text/graphic overlays added, respectively.

/thumbs/{filename}. A thumbnail image for a specific file. You may use a database record number (@record) in place of the filename.

/alerts/{filename}. An alert image. You may use a database record number (@record) in place of the filename. HTTP parameter *&fulljpeg* will return the high-definition version of the image or MP4 file if it was saved to disk.

Optional parameters for many of the above:

&w=	width, use with or without height
&h=	height, use with or without width
&s=	scale 1-100 in place of width and/or height
&q=	quality 1-100
&fps=	frames/second
&kbps=	kilobits per second
&cache=1	include cache-control: no-cache in the reply
&stream=x	x= 0..2; select an encoder preset from settings/web server/advanced
&decode=x	x= 0 for automatic (default), -1 for sub-stream, 1 for main-stream
&connection=close	do not re-use this connection
&dl=1	request the browser to download rather than play the content

Dynamic group layout options

When requesting a group stream that's configured for dynamic layout (no forced aspect ratio), you may customize the display as follows:

&h=height	if the layout does not force a specific height
&w=width	use with height if the layout does not force a specific aspect ratio
&cams=camlist	a comma-delimited list of camera short names (e.g., cam1,cam2,cam3)
&flags=x	1=names 2=borders 4=show hidden 8=hide disabled 16=hide inactive
&mask=x	bits corresponding to the flags to adjust

Admin commands

/admin?actionset=x (x=1..8) Run one of the custom action sets defined via the Settings/ Keyboard shortcut commands

/admin?camera=x&actionset=y&enabled=0 or 1. Where *y* is one of OnTrigger, OnReset or OnPreAI. Optionally, include a specific ordinal action on the action set with the syntax OnTrigger\0, OnTrigger\1 etc.

/admin?camera=x&autocycle=1 or 0 Automates the auto-cycle function for camera x's frame

/admin?camera=x&alerts=[-1..2] Sets the "when" value on the Alerts tab for camera x (short name). For "never" use alerts=-1.

/admin?camera=x&enable=1 or 0 Enable or disable camera x (short name)

/admin?camera=x&escape Equivalent to using Esc key on camera window to exit full screen or other temporary modes.

/admin?camera=x&flagalert=x&memo=text&jpeg=path&flagclip

x = 0 mark the most recent alert as *canceled* (if not previously confirmed).
x = 1 mark the most recent alert as *flagged*.
x = 2 mark the most recent alert as *confirmed*.
x = 3 mark the most recent alert as *flagged and confirmed*.
x = -1 reset the *flagged, confirmed, and canceled* states

when *x* is 1-3, you may add 4 to mark the alert as a confirmed person and/or 8 to mark the alert as a confirmed vehicle.

Use of *memo, jpeg, flagclip* are optional. If supplied, the *jpeg* will replace any existing hi-res image for this alert in the alerts folder; however it will not replace the thumbnail used in the database alerts list. You may use this in conjunction with a camera's **Allow disarm time by delaying alerts** setting to allow an external system to validate an alert or to prevent an alert from firing.

/admin?camera=x&flash=1 or 0 Enable or disable Flash broadcasting on camera x (short name). A camera reset will also be required (&reset)

/admin?camera=x&fullscreen=1 or 0

/admin?camera=x&hide=1 or 0 Hide or show camera x (short name)

/admin?camera=x&manrec=1 or 0 Start or stop manual recording on camera or group x (short name)

/admin?camera=x&mdelay=x Delay motion detection on camera x (short name)

/admin?camera=x&motion=1 or 0 Enable or disable motion detection on camera x (short name)

/admin?camera=x&output=n&msec=t Set or reset the digital output n (1-10) on camera x (short name). Use msec=0 to reset the output and any other value to set it.

/admin?camera=x&pause=n Pause camera x (short name). n=-2,-1,0,1,2... for toggle, infinite, 0,+30s,+5min,+30m,+1h,+2h,+3h,+5h,+10h,+24h,+15m

/admin?camera=x&preset=n Goto PTZ preset n on camera x (short name)

/admin?camera=x&preset=n&set Set PTZ preset n on camera x (short name); optionally use *set=new description* to update the preset's description.

/admin?camera=x&priority=n 1: temporarily move camera x to the top-left position, 0: return it to its normal position.

/admin?camera=x&profile=n[&lock=0/1] Temporarily force profile n on camera x (short name). Add *&lock=1* to "hold" the the profile indefinitely. Use *&profile=-1* to unlock and revert to the normally scheduled profile.

/admin?camera=x&ptz=n PTZ command n on camera x (short name). n=0,1... for left,right,up,down,center,zoom+,zoom-

/admin?camera=x&ptzcycle=1 or 0 Enable or disable PTZ preset cycle on camera x

/admin?camera=x&reboot Reboot camera x (short name) (as supported)

/admin?camera=x&reset Reset camera x (short name)

/admin?camera=x&resetnew Reset new alerts counter for the connected user on camera x (short name)

/admin?camera=x&schedule=1 or 0 Enable or disable schedule on camera x (short name)

/admin?camera=x&select Select camera x (short name). Omit the camera name (x is empty) to de-select all cameras.

/admin?camera=x&snapshot Snapshot on camera x (short name)

/admin?camera=x&trigger&memo=text&jpeg=path Trigger camera or group x (short name) as an External source; optionally add *text* to the memo field in the database; optionally use the JPEG at *path* as the alert image in both the database and the alerts folder.

/admin?camera=x&trigger=1&zones=z Trigger camera or group x (short name) as a Motion source. Zone bits *z* are combined powers of 2 … the zone A value is 1, zone B is 2, zone C is 4 … zone H is 128.

/admin?camera=x&trigger=-1 Trigger camera (short name) as a *bistable* ONVIF source

/admin?camera=x&trigger=0 Reset trigger on camera (short name)

> **NOTE:** The ONVIF source will cause the camera to *remain triggered* until the &trigger=0 command is used and the break time has expired.
>
> **NOTE**: With a supplied JPEG or memo, a new alert list image will be generated even if the camera is already triggered.

/admin?camera=x&webcast=1 or 0 Enable or disable webcasting on camera x (short name)

/admin?console={group name} (&fullscreen=1 or 0) Select the specified group for display on the console, "index" is All cameras.

/admin?db=rebuild, compact, maintain, status Initiates the specified database operation.

/admin?ai=x Restarts the AI with mode=0,1,2 for low, medium, high. Omit the x value to restart using the current mode.

/admin?input=x Manually sets the state of the global DIO input bits

/admin?log=message&level=x Adds message to the log with severity level x (0: info, 1: warn, 2: error)

/admin?macro=x&text={text} Set macro number x=1-999 to value {text}

/admin?output=x&msec=y or &force=true Set DIO output x=0-31 on for y msec, or force on indefinitely

/admin?profile=x&lock=y. Set the active profile to x. Use x=-1 to toggle the lock status, or set the lock=y, 0=run, 1=temp, 2=hold

/admin?schedule=1 or 0 or schedule name. x=0 or 1 to disable/enable Options/Schedule, or a name to set the current schedule

/admin?sendkeys=w:x Emulates keyboard input. w=target window, one of cams, clips, main, or a camera short name. x=a string of keys to send such as {LEFT}{ENTER}{ESC}. This functionality is based on the project found here: https://www.codeproject.com/Articles/6819/SendKeys-in-C. The ability to arbitrarily run programs and use the Windows keys has been removed for security.

/admin?signal=x Changes the shield icon state and returns the current state. x=0 for red, x=1 for green, x=2 for yellow. This requires admin authentication.

/admin?camera=x&solo=1 or 0 Automates the frame window single-camera "solo" icon and function. You must specify any one of the cameras' short name in the frame as *x*.

/admin?transport=x Automates the clip viewer window; x may be one of play, rplay, next, prev, pause, step, or rstep.

x may also be a UTC time value with millisecond precision to position the video slider.

x may be an integer power of 2 in the range [-256,256] to set the playback speed directly.

The current UTC position and playback speed is now also returned.

Camera commands

/cam/{cam-short-name}/pos=x Performs a PTZ command on the specified camera, where x=0=left, 1=right, 2=up, 3=down, 4=home, 5=zoom in, 6=zoom out

/cam/{cam-short-name}/pos=100 Causes a snapshot image to be captured from the specified camera.

/cam/{cam-short-name}/preset=x Moves the camera to PTZ preset position x

RTSP server

You may request an RTSP stream from your HTTP port as well with the URI format */{cam-short-name}* or */{group-name}*. Stream and image parameters may be added just as they are available for */image*. For example:

rtsp://yourip:81/cam1

rtsp://yourip:81/index (all camera group)

rtsp://yourip:81/@index (all camera group cycle)

As with /image and other video requests, you may add parameters to select image size, quality, etc. For example:

rtsp://yourip:81/cam1?decode=-1 select the sub stream

rtsp://yourip:81/cam1?h=720 encode to 720p

Authentication

You may add &user=*username*&pw=*password* to any HTTP request, but only if **use secure session keys and login page** is disabled on the Advanced page in Settings/Web server. It's also possible to exempt or elevate connections from specific IP addresses.

JSON INTERFACE

The JSON (JavaScript Object Notation) interface is used by the client apps as well as the UI3 browser interface.

For a description of JSON, see http://www.json.org/. It's simply a block of text which is sent by HTTP-POST to the Blue Iris web server page */json*. Blue Iris will respond with a JSON formatted response (*Content-Type: application/json*).

Each JSON object sent to Blue Iris must have a *cmd* value, for example, *"cmd":"login"*. Additional values will depend upon the type of command sent.

login
Here's an example command and response conversation for authentication:

{"cmd":"login"}

Blue Iris will respond with a "result" value of "fail' and a "session" value.

{"result":"fail","session":"182c8a04f7d4ab042ff8e4a2"}

Respond with this session value combined with a userid and password MD5 hash encoded as MD5("userid:session:password"):

{"cmd":"login","session":"182c8a04f7d4ab042ff8e4a2","response":"56e72abc7019c6b43a761e9"}

parameter	value
session	the session key that was supplied with the initial login command
response	a string created via MD5("userid:session:password")
uuid	optional, a unique identifier used to identify a mobile device
devicename	optional, a description of the device
devicetype	optional, for example, "iOS"
token	optional, a code used to send push notifications

If a correct response is received from the client, Blue Iris will respond:

parameter	value
result	success
session	the session key that was supplied with the initial login command
data	an array with the following objects:
system name	as defined on the Settings page

parameter	value
admin	true/false; full system admin
changeprofile	true/false; may change the shield, profile, schedule without full admin access
ptz	true/false
audio	true/false
clips	true/false
clipcreate	true/false; may take snapshots, start manual recording, export/convert clips
timelimits	true/false
sessionlimit	seconds allowed per session (most recent login)
streamlimit	seconds allowed per stream
daylimit	seconds allowed per calendar day
dayused	seconds used for current day
dio	true/false
version	PC software version, eg., 5.0.0.26_x64 (or w32)
license	PC software license key
support	PC software maintenance status or expiration
tzone	time zone bias in minutes from GMT
streams	an array of video encoding stream names
sounds	an array of available sound files in the Sounds folder in the Blue Iris installation folder
www_sounds	an array of available sound files in the Sounds folder in the WWW root folder
profiles	an array of profile names as defined on the Profiles page in Settings
schedules	an array of schedule names as defined on the Schedules page in Settings

If result is “false” then a data value “reason” will be returned.

More commands

alertlist

get a list of alert images

parameter	value
session	the session key that was supplied with the initial login command
camera	a camera's short name or a group name
startdate	UTC, expressed as the integer number of seconds since January 1, 1970
enddate	UTC, expressed as the integer number of seconds since January 1, 1970
tiles	true/false, return a single entry per-day only
delete	true/false, delete all items instead of returning the list
reset	true, reset new alert counters for current user on all or select camera/s

parameter	value
view	(optional) a specific database view; one of: `all, new, stored, alerts, aux1, aux2, aux3, aux4, aux5, aux6, aux7, flagged, export, archive, people, vehicles, confirmed, or canceled`
search	(optional) text that must appear within the memo field of each record, case-insensitive, similar to the search box above the alerts list in the PC software.

the following information is returned in an array, and for each entry:

parameter	value
camera	camera short name
newalerts, newalerttime	only sent for the 1st alert on each camera, user specific new alert counter
path	@record.extension for the alert
clip	@record.extension for the referenced clip
file	the JPEG filename in the alerts folder, if alerts are saved as JPEGs for this camera
memo	the alert's memo field typically containing AI results
plate	only sent when a license plate number was added
offset	the offset within the clip in milliseconds
flags	database flags field
res	string XxY resolution representation
zones	a bit representation of the motion zones, 1==A, 2==B, 4==C, etc.
date	UTC, expressed as the integer number of seconds since January 1, 1970
color	the camera's set RGB color
filesize	a formatted string with both duration and size on disk

camconfig

get (and optionally set) the state of many camera properties:

parameter	value
session	the session key that was supplied with the initial login command
camera	camera short name
rename	string, change camera long name
resetnew	true, reset new alert counter for selected camera for current user
audio	true/false, enable audio processing
reset	true, reset camera window
reboot	send PTZ/control reboot command to camera
output	true/false, set or reset the camera's first DIO output
profile	set the camera's active profile (override global)
lock	true/false, also "hold" the profile if true, otherwise it's temporary
manrec	true/false, start or stop manual recording

parameter	value
pause	adjust the camera's pause state. a list of values is available upon request from support
hide	true/false
enable	true/false
motion	true/false, enable/disable the motion detector for the currently effective profile
schedule	true/false, enable/disable schedule override for this camera
ptzcycle	true/false
ptzevents	true/false, enable/disable events list (schedule page)
alerts	set the alerts scope for the currently effective profile. -1==disable, 0==this camera, 1==groups, 2==any camera
record	-1==manual, 0==periodic, 1==continuous, 2==triggered, 3==motion+periodic, 4==continuous+alerts, 5==alerted
setpost	an array of image post settings; currently only "timed":bool and "timed_interval":seconds are defined.
setmotion	an array of motion detection parameters as defined in the response to this command

replies with the current state of these settings.

camlist

returns a list of cameras on the system ordered by group. Cameras not belonging to any group are shown beneath the "all cameras" group. Disabled cameras are placed at the end of the list.

parameter	value
session	the session key that was supplied with the initial login command
reset	1: reset stat counts, 2: reset new alerts; 3 or true: reset both

An array of objects is returned in *data* (note the [] surrounding a JSON array), each describing a camera or a camera group. For each of these objects, the following values are defined:

parameter	value
optionDisplay	the camera or group name
optionValue	the camera or group short name, used for other requests and commands requiring a camera short name
notes	the user notes field from the General tab in camera settings
number	the camera serial number, used internally to match database records
admin	true/false; user has access to administer this camera
audio	is audio supported, true or false
ptz	is PTZ supported, true or false
color	24-bit RGB value (red least significant) representing the camera's display color
clipsCreated	the number of clips created since the camera stats were last reset

parameter	value
webcast	true/false, is webcasting enabled
hidden	true/false
tempfull	true/false, is camera temporarily full screen
active	true/false, camera is currently displaying live video
type	4==network IP, 5==broadcast
pause	0==not paused, -1==paused indefinitely, else the number of seconds remaining
isEnabled	true/false
isOnline	true/false
isMotion	true/false, current sensing motion
isNoSignal	true/false
isPaused	true/false
isTriggered	true/false
isAlerting	true or false; currently sending an alert
isRecording	true/false
isManRec	true/false, manually recording
ManRecElapsed	msec since manual recording began
ManRecLimit	msec limit for a manual recording
isYellow	true/false
profile	the camera's current profile, or as overridden by the global schedule or the UI profile buttons
profiles	bits representing the camera's active profiles; by default 254, all profiles but 0
ptz	is PTZ supported, true or false
audio	is audio supported, true or false
nTriggers	number of trigger events since last reset
nAlerts	number of alerts since last reset
nNoSignal	number of no signal events since last reset
nClips	number of no recording events since last reset
xsize	for a group, the default number of cameras across
ysize	for a group, the default number of cameras tall
group	for a group, an array of the default camera short names in the group
rects	for a group, an array of the default camera rectangles within the default group image
newalerts	per camera, per user number of new alerts
lastalert	database record locator for most recent alert image
lastalertutc	UTC timecode (msec precision) for most recent alert image
bps	bytes/second for main (or only) stream
bps2	bytes/second for sub stream
fps	frames/second for main (or only) stream

parameter	value
fps2	frames/second for sub stream
width	frame pixel width for main (or only) stream
height	frame pixel height for main (or only) stream
width2	frame pixel width for sub stream
height2	frame pixel height for sub stream
error	formatted string with camera error condition

camset

camera window manipulation, added recently for Remote Management

parameter	value
session	the session key that was supplied with the initial login command
camera	camera short name
click	perform camera "click" function, which is to select the camera and then reset new alerts for the current user
audio	true/false, play live audio
delete	true, delete the camera window
ptz	a string in the format "*id*:*args*". a list of ids is available upon request from support 2201 - 2240: call preset position 1-40 2301 - 2340: SET preset position 1-40
trigger	true, trigger the camera
reset	true, reset the camera window
enable	true/false, enable or disable the camera
video	toggle manual video recording
zoom	an array of 5 floats defining the zoom factor and X,Y,X2,Y2 zoom view rectangle within the image rectangle
snappreset	integer x 1-40, the preset number; capture a preset position image
clearpreset	integer x 1-40, the preset number; clear a preset position image
uppreset	integer x 2-40, the preset number; exchange preset values & settings with the one previous (x-1)
down preset	integer x 1-39, the preset number; exchange preset values & settings with the one following (x+1)
target	a target camera short name for use by *move*
move	0: swap selected camera with target camera window
	1: insert selected camera at target camera window position

cliplist

get a list of clips from the database

parameter	value
session	the session key that was supplied with the initial login command
camera	a camera's short name or a group name

parameter	value
startdate	expressed as the integer number of seconds since January 1, 1970
enddate	expressed as the integer number of seconds since January 1, 1970
view	a specific database view; one of: `all, new, stored, alerts, aux1-5, flagged, export, archive, confirmed, or canceled`
search	(optional) text that must appear within the memo field of each record, case-insensitive, similar to the search box above the alerts list in the PC software.
tiles	true/false, return a single entry per-day only
delete	true/false, delete all items instead of returning the list

the following information is returned in an array, and for each entry:

parameter	value
camera	camera short name
path	primarily used to parse the extension
offset	for an alert, the offset within the clip
clip	for an alert, the @record.extension for the referenced clip
date	UTC value in seconds
color	the camera's set RGB color
flags	database flags field
res	string XxY resolution representation
msec	playable duration (although clip may cover a longer time range)
file	the item path relative to its folder
filesize	string, a formatted representation of the clip duration
filetype	a string with the file's extension, compression type, and folder name

clipstats

return information about a specific database record

parameter	value
session	the session key that was supplied with the initial login command
path	@record, the database locator for the item

the following information is returned:

parameter	value
camera	camera short name
path	for an alert, the DB locator for the associated clip with extension
file	the item path relative to its folder

parameter	value
offset	for an alert, the offset within the clip (in milliseconds)
alertmsec	if an alert, the alert duration in milliseconds
date	UTC value in seconds
color	the camera's set RGB color
flags	database flags field
zones	bitwise trigger zones (1=A, 2=B, 4=C, 8-=D, 16=E, 32=F, 64=G, 128=H)
memo	for an alert, AI results, otherwise user settable
plate	license plate captured with ALPR if configured
res	string XxY clip resolution representation
msec	playable duration of the entire clip (although the clip may cover a longer time range when using cut/combine)
campreset	the most recently called PTZ preset at the time of alert
camprofile	active profile at time of alert: 0-7
camschedule	camera schedule overriding global at time of alert: true/false
camsmart	AI in use at time of an alert: 0=none, 1=Sentry, 2=AI
camzones	was a motion zone map in force at the time of alert: true/false
filesize	string, a formatted representation of the clip duration
filetype	a string with the clip's extension, compression type, and folder name

console

manipulate the layout of the PC software

parameter	value
session	the session key that was supplied with the initial login command
selcam	optional, select a camera window using its short name
group	optional, select a group by name. The All Cameras group has an internal short name of "index".
fullscreen	optional, true/false

delalert

removes the specified alert from the database

parameter	value
session	the session key that was supplied with the initial login command
path	@record, the database locator for the alert to be removed from the database; multiple @records may be specified separated by either ; or ,

delclip

deletes the specified clip

parameter	value
session	the session key that was supplied with the initial login command
path	“@record”, the database locator for the alert to be removed from the database; multiple @records may be specified separated by either ; or ,
flags	1: recycle 0: delete normally

devices

returns an array of mobile devices

parameter	value
session	the session key that was supplied with the initial login command
reset	reset statistics on the Mobile Devices page in Settings
push	0: no push notifications 1: normal push notifications sent to this device -X: a number of seconds to pause push notifications, expressed here as a negative number

Each device entry in the array contains:

parameter	value
date	date of last login, UTC in seconds
count	there number of logins since this statistic was reset
id	phone identifier or GUID
name	more descriptive name, such as Sam’s iPhone
type	iOS, Android, Win, etc.
push	0: disabled 1: normal operation -X: a number of seconds push notifications have been paused
inside	inside, outside, or “-” for unknown

export

create a video file suitable for download and sharing

parameter	value
session	the session key that was supplied with the initial login command
path	“@record”, the database locator for the clip to export; alert records will resolve to clips automatically; omit this value for a status array of all items in the export queue; send an export record for status on a specific item
startms	starting position in milliseconds; the actual starting frame is determined by the nearest key frame
msec	duration in milliseconds; omit to go to the end of the file
audio	optional, true/false, default true
overlay	optional, true/false, default false
format	optional, 0==AVI, 1==MP4, 2==WMV, default MP4
profile	optional, encoding parameters, 0-2 as configured through convert/export dialog on console

parameter	value
reencode	optional, true/false, default true; use false for “direct-to-disk” export, which is much quicker; “false” is incompatible with WMV, overlay:true or time-lapse options
timelapse	optional, “2.0@30.0” for example to create a file using 2 frames per second from the source video to create a 30 frames per second output video; incompatible with audio:true or reencode:false
delete	optional, true/false, default false; when combined with a path record for an existing export item, the item will be removed from the export queue and deleted.

replies with

parameter	value
path	“@record”, the database locator for the export product
status	queued, active, error, or done
msec	status, the duration of the export in milliseconds
progress	0-100 (%) when status is “active”
uri	status, the file path relative to the New folder; use /clips/{uri} for direct access to the file once status=done
utc	status, the original clip start time, expressed as the integer number of seconds since January 1, 1970
error	the error text, when status is “error”
filesize	a formatted file size when status is “done”

Send only a *path* with a previously obtained *path* to obtain status on a single item. Send only the *export* command without a *path* to receive an array of items in the export queue.

The Convert/Export queue may be viewed via the PC software clips list as well. Items created through this API are physically located in the New folder and remain in the queue until they are deleted manually or through normal database maintenance operations.

geofence

set the current status of the connected mobile device; the JSON login must have included the device uuid.

parameter	value
session	the session key that was supplied with the initial login command
inside	0: outside
	1: inside
	anything else: unknown

log

returns an array of status messages

parameter	value
session	the session key that was supplied with the initial login command
aftertime	The earliest time to display, UTC time in seconds
reset	reset the Message page in Status

Each log entry in the array contains:

parameter	value
object	current camera or clip stream
date	date of last login, UTC in seconds
count	sent only if not 0, the number of entries this represents
obj	the software object writing to the log
msg	the message
level	a severity level, 0==info, 1==warn, 2== error, 10==user

logout

closes the current user session

parameter	value
session	the session key that was supplied with the initial login command

moveclip

move a clip to another managed folder

parameter	value
session	the session key that was supplied with the initial login command
path	@record, the database locator for the item
folder	the target folder, 0==New, 1==Stored, 3==Aux 1, etc.

ptz

operate a camera's PTZ functionality

parameter	value
session	the session key that was supplied with the initial login command
camera	camera short name
button	this value determines the PTZ operation performed; omit this value to receive the PTZ status.

parameter	value
	0: Pan left
	1: Pan right
	2: Tilt up
	3: Tilt down
	4: Center or home (if supported by camera) add “xperc”:x, “yperc”:y, and optionally “zperc”:z where x and y are normalized coordinates (floating point 0-1) and z represents the relative amount to zoom (again 0-1).
	5: Zoom in
	6: Zoom out
	8..10: Power mode, 50, 60, or outdoor
	11..26: Brightness 0-15
	27..33: Contrast 0-6
	34..35: IR on, off
	101..120: Go to preset position 1..20
	-1 and -2: focus near and far
updown	non-zero: the command will be sent a 2nd time to “stop” the movement
description	if sent with a preset position command, the preset will be SET instead of called

status

get (and optionally set) the state of the shield, active global profile as well as the schedule's hold/run state and other system vitals

parameter	value
session	the session key that was supplied with the initial login command
remote	assert remote management status; session is closed if inaccurate
admin	execute any admin command, see the /admin documentation in HTTP above
update	*“version, flags”* install current software update. *version* is the HEX formatted number, for example 0x05030906 (5.3.9.6), converted to decimal (84084998 for this example). *flags* should be 0.
reboot	reboot the PC
play	play a specific sound in the Sounds folder in the installation folder
dio	set an output according to additional parameters supplied in an array: “output” number, “force” (true/false) and “msec”
signal	set the shield icon, 0 for red, 1 for green, 2 for yellow.
profile	a single digit 0-7 for the profile number to set temporarily, send again to hold; or -1 to toggle the hold/run state
schedule	set the current global schedule by name
macro	set a specific global macro accounting to parameters supplied in a set: “number” and “value” (string)

replies with

parameter	value
profile	active global profile
lock	the state of the schedule run/hold button: 0 for run, 2 for temp, 1 for hold
signal	the state of the shield icon, 0 for red, 1 for green, 2 for yellow.
cxns	the number of active server connections
cpu	the CPU utilization %
ram	string value representing RAM used by the software
bits	status bits, definitions upon request from support
mem	a formatted version of RAM used by the main BlueIris.exe process
memphys	a formatted version of the total physical RAM installed on the system
memload	a formatted version of the percentage of physical RAM in use on the system
folders	an array of folder names as configured on settings/clips; a name is blank if the folder is unused
discs	an array of disk information, each disk with name, allocated, used, free and total space
schedule	active global schedule
dio	an array of output states; 0 for reset, -1 for indefinitely set, else a number of msec remaining
uptime	a formatted representation of the software up-time
clips	formatted strings representing clip and storage statistics
tmessage	the timestamp of the last message added to Messages in Status
warnings	current number of warnings in Messages for the current user
alerts	current number of new camera alerts for the current user
time	the current server time in milliseconds GMT
tzone	the time zone bias in minutes from GMT for the server

sysconfig

get and set system configuration settings—admin access required

parameter	value
session	the session key that was supplied with the initial login command
mreset	0: reset all messages on the Messages page in Status
	X: the lower-32 bits of the time code for a specific message to remove
clearcxns	clear the connections list, open connections will remain
dio	0: shutdown
	1: startup
	string X:Y set output X for Y msec
mqtt	0: shutdown
	1: startup
kick	a numeric value, close a specific connection using an internal PTR value

parameter	value
	a string value, close connections with a specific user name
permban	toggle permanent ban/un-ban for a specified IP address
tempban	toggle temporary ban/un-ban for a specified IP address
archive	true/false, enable FTP backup function configured on Clips in Settings
schedule	true/false, toggle use of global schedule
manrecsec	0: unlimited manual recording time
	X: set the number of seconds for a manual record start/stop

replies with

parameter	value
archive	true/false, enable FTP backup function configured on Clips in Settings
schedule	true/false, use of global schedule
manrecsec	the number of seconds for a manual record start/stop

timeline

get a formatted list of alerts, flags, and clips over a specified time range

session	the session key that was supplied with the initial login command
camera	a camera's short name or a group name
startdate	expressed as the integer number of seconds since January 1, 1970
enddate	expressed as the integer number of seconds since January 1, 1970; must follow start date
msecpp	item display x position quantization in milliseconds per pixel, minimum 128. The values used in the Blue Iris UI are (450000,240000,180000,144000,120000,90000,72000,60000,45000,22500,11250,5625,1875,625,256,128). For optimal performance, this number should evenly divide a day (86400000 milliseconds), no remainder.

replies with

parameter	value
colors	an array of RGB values corresponding to the tracks in the timeline from top to bottom; used to determine the number of tracks
alerts	an array of items in the format {"x1":*x1*,"x2":*x2*,"type":*flags*,"record":"@*recno*","tracks":*tracks*}; *x1* and *x2* are the display x positions, *flags* may be used to determine the type of alert (confirmed, person, vehicle, sound, etc., or flagged), and bits in *tracks* are used to determine the display y positions
clips	an array of items in the format {"x1":*x1*,"x2":*x2*,"track":*track*}; *x1* and *x2* are the display x positions, *track* is used to determine the display y position of the clip rectangle

Note that in order to represent *x* positions as 32-bit numbers, they are relative to the start date. To convert an *x* position to an absolute time, you would use *utc=startdate + x•msecpp*.

trigger

trigger the selected camera

parameter	value
session	the session key that was supplied with the initial login command
camera	camera short name
memo	optional ... set the memo field in the database for this alert
jpeg	optional ... use a supplied JPEG image for this alert (fully qualified path)

> **NOTE**: With a supplied JPEG or memo, a new alert list image will be generated even if the camera is already triggered.

update

adjust database entry

parameter	value
session	the session key that was supplied with the initial login command
path	@record, the database locator for the item in the database
memo	up to 35 characters to reflect AI findings or custom text to associate with this record
flags	adjusted flags are returned by *cliplist* or *alertlist* ; available flags (may be 'or'ed): 2 flagged 4 protected 64 archive 512 export
mask	which flags to adjust ('or'ed from list above)
date	milliseconds since Unix epoch (January 1, 1970 GMT)
exportfolder	internal use, corresponding to a folder number at HKEY_LOCAL_MACHINE\SOFTWARE\Perspective Software\Blue Iris\Defaults\exportfolder
exportprofile	adjusted encoded bits for item export status
timelapseprofile	adjusted encoded bits for item export status

userconfig

update a specific user's settings

parameter	value
session	the session key that was supplied with the initial login command
user	user name
pw	optional, reset the user's password
enabled	optional, true/false

parameter	value
admin	optional, true/false
schedule	optional, true/false, use the schedule for timed access
push	optional, true/false, enable push notifications for the currently active profile

The current state of these settings is returned.

users

returns an array of all users

parameter	value
session	the session key that was supplied with the initial login command
reset	true, reset statistics on the Users page in Status
remove	the user name to remove
add	the user name to add; the following values will be used:
pw	required, the new user's password
admin	optional, true/false

Each user entry in the array contains:

parameter	value
isOnline	true/false
object	current camera or clip stream
date	date of last login, UTC in seconds
obj	the user name
msg	access description such as Admin,Enabled,camera groups
level	always 10. the users list is an extension of the *log* messages list for client app compatibility.

DDE INTERFACE

A technology that is largely deprecated, yet a part of Blue Iris. A DDE service name *BlueIris* is created to listen for commands:

topic	item	data	function
global	signal	0, 1, or 2	set the shield icon to red, green, or yellow
camera	(shortname)	ptzpreset=x	move to PTZ preset position x
		trigger	trigger the camera
		snapshot	single snapshot to the database
		record	toggle manual recording

topic	item	data	function
		recstart	start manual recording
		recstop	stop manual recording
		reset	reset camera
		enable	enable camera
		disable	disable camera
		schedule=1 or 0	enable or disable camera schedule override
		profile=x	temporarily set camera override profile
macro	1-999	(text)	set macro number to specified text

IOS APP DEEPLINKING

You may launch the Blue Iris on the iPhone or iPad using the following browser schema:

blueiris://?

You may go directly to a camera or group by specifying its short name. Optionally, go to the most recent alert on the camera or group.

blueiris://?camera=xxx[&alerts]

You may instead go directly to a specific tab or page in the app:

blueiris://?tab=(home,cameras,alerts,status,info)

Pinpointing a source of instability can be frustrating for sure—the most basic of strategies is to isolate a problem by narrowing the focus. If things were working fine yesterday, you may also ask yourself "what changed?"

An issue may be coincidental with a software update. If you suspect the update, you can always try "rolling back" to an older version if possible. Please use the **Check for update** button on the Settings About page for the availability of previous releases.

An issue may be coincidental with Windows or other security software updates. If other measures fail, you can always try reverting these to older versions as well. Also double check your *security software exemptions* as discussed in a topic toward the beginning of this chapter. It's possible one of these has come "undone" as the result of a software update.

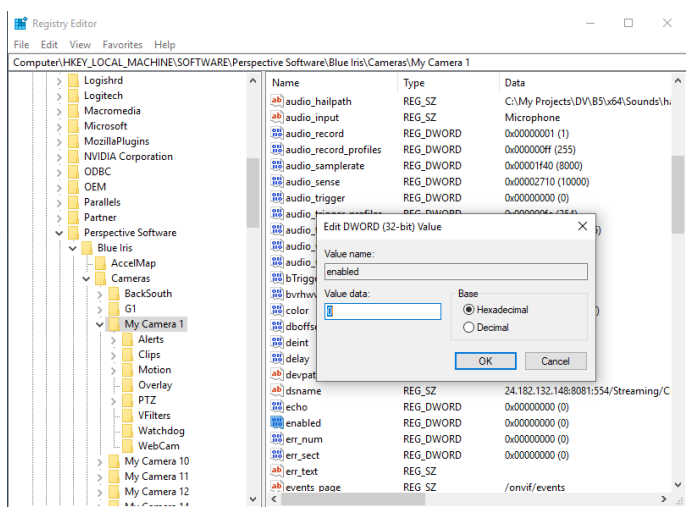
An issue may be related to a recent settings change. If you are creating automatic settings backups as configured on the About page in settings, you may try reverting to one of these if you are able to get to that page without a crash.

All settings for Blue Iris are stored in a registry key. Enter REGEDIT into the Windows search box to open the registry editor. Search for:

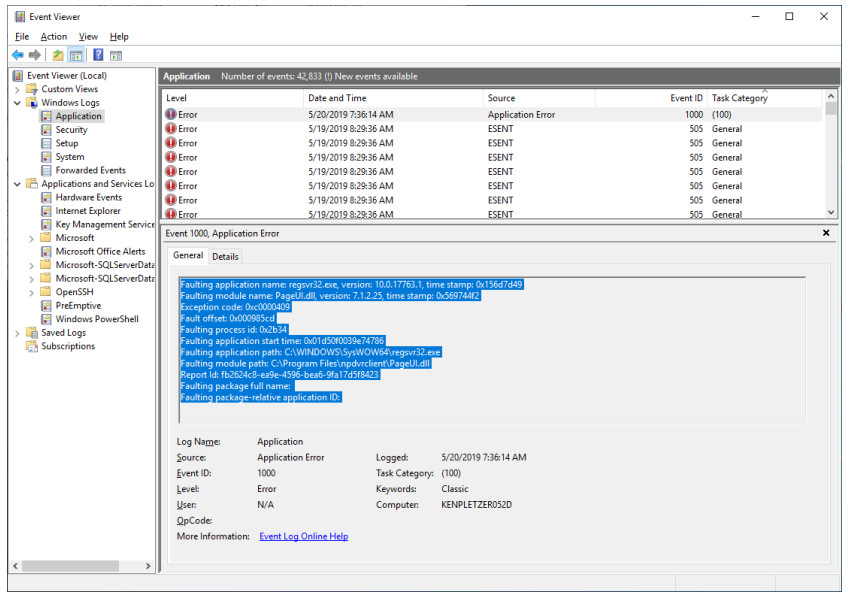
HKEY_LOCAL_MACHINE\SOFTWARE\Perspective Software\Blue Iris

Deleting or renaming this key will allow you to test a startup without any cameras and with other default settings. It's also possible to rename particular sub-keys, for example changing Cameras to CamerasX. To disable individual cameras, open the camera's key and change the *enabled* value to 0.

If the service is crashing, it may be necessary to startup without the service in order to find the issue. Do this by first setting the service to a "manual" startup state in the Windows Service Manager (search for *services*). Then in the Options sub-key in REGEDIT, set the *service* value to 0.



For an application crash, this is logged to the Windows Event Viewer (search for *event viewer*).



Locate the most recent crash event under *Windows Logs, Application* which shows **Faulting application name BlueIris.exe** in the *General* box. Copy and paste the information shown in blue in the image above into your support email—please do not send *.evtx* files as your email may be read on a non-Windows PC.

Please note that a Windows "blue screen" (BSOD) error or system "hang" where the mouse cursor is stuck may not be caused by application software directly, but may be due to a faulty device driver, OS component, even a virus etc. These should be logged to the Windows Event Viewer as well and should identify the particular device driver causing the issue.

Use Windows Task Manager (search for *task*) to monitor CPU and RAM usage by the BlueIris.exe process. If CPU is at or near 100% for extended periods, or RAM used by the application appears to be growing over time without "leveling out" this could be the cause of the instability or crashing. Please see topics earlier in this chapter for CPU management techniques and security software exemptions (security software, along with faulty device drivers are leading causes of memory leaks).

For efficient service when writing to support, please send your license key along with any information learned through your troubleshooting efforts. Please also send an individual camera settings export or the full settings export as may be required to attempt to replicate an issue.

FAQ

Can I add more than 64 cameras?

The software was designed for 64 cameras. The best way to handle a requirement for more than this is to split the load among multiple PCs and then to link them using the new Remote Management features.

What type of system or CPU do I need for X cameras?

First, the number of cameras, although a consideration, is *not* the most important factor—rather it's the overall MP/s (megapixels per second) that your system is handing. The two factors which contribute to MP/s are the frame size (the camera's resolution) and the number of frames per second. Lowering either of these will directly lower the CPU demand. The software will actually run a large number of cameras on a fairly modest system if you put thought into this and other *CPU management*—there's an entire section in this chapter devoted just to this topic.

Is camera X compatible with Blue Iris?

Most network IP cameras on the market today will be compatible using standard methods or protocols such as RTSP, RTMP, ONVIF, MJPEG, or just regular JPEGs. However, there are many models (especially DVRs) still using proprietary authentication and streaming—please check with the manufacturer specifications for availability of one of the standard protocols. *Ring* is a prime example of a camera that is *not* compatible, as that company purposely does not play well with others—they want you all to themselves.

If you can send a WAN address with the required ports forwarded to the camera, we can evaluate it for compatibility and advise on the best settings.

For a USB or PC card device, check manufacturer specifications for standard Windows DirectShow drivers. Too often manufacturers of these devices choose to implement proprietary drivers, requiring that you use their software exclusively.

How much storage space do I need?

Most network IP cameras will have a setting for bandwidth or kbps (kilobits per second) or Mbps (megabits per second). If you are recording *direct-to-disk*, which is almost always the case with larger systems, you may simply multiply this number out by the amount of time for which you want to save video. Unlike a storage byte, a network *byte* actually has *10 bits* so this simplifies the calculation:

$$\frac{\frac{2048 kbps}{(10 bits/byte)} * 86400 seconds/day}{(1024 KB/MB)}$$

will give you the number of MB per day for a 2048 kbps camera stream, 17280 MB, or about 17 Gigabytes (GB). However, by default, Blue Iris only records video when cameras are triggered, so this greatly reduces the amount of storage necessary.

Will you ever create a version for Mac or Linux?

We have chosen to strongly focus on one OS rather than diluting development effort. However, the Parallels virtual machine for Mac (Intel, not M chips as of this writing) supports Blue Iris well—use a second monitor just for Blue Iris or run within a window right on your Mac desktop.

How can I stop my camera addresses from changing when the power goes out, or randomly?

Once you have your cameras working, you can force them to continue to use specific addresses indefinitely by turning off DHCP in their settings. You can either use a range of addresses which the router will not re-use, or you can *reserve* the addresses in the router's settings to prevent them from being given to other devices.

Why am I getting an email every hour that's coming from my system?

These may be *status alerts*—check your settings on the Messages page in Status with the **Status Alerts** button.

I don't see my videos on the clips list, where did they go?

The default storage is only 30GB and with many cameras recording often it's possible to quickly overrun this. Please see the Recording chapter to learn how to make adjustments.

If the files are physically on the drive but not appearing on the list, repair the database by selecting Database/Repair from the right-click menu in the clips list.

Another thing to consider is that *Alert images* and *Clips* are often confused. Clips are the files —alerts are just images captured at the time of trigger. You may be looking at the wrong list. Check this and the other clip list filter options at the top of the clips list.

Why aren't my files being moved to Stored and the New folder is overflowing?

Most likely, you are running as a service, but under the Local Service user, and that user has insufficient rights. Please see the related topic at the beginning of this chapter. Also, you may need to use a UNC name (like *server**share*) for your NAS rather than a drive letter.

Please see the Messages log in Status for the error that is encountered when the software attempts to move or delete files.

Why is my hard drive constantly running out of space?

If you see only green, no red, on the Storage page in Status, maybe it's the Windows temp folder that is filling up. This folder may be used by antivirus software to "cache" network traffic for analysis. Please see the *security software exemptions* topic in this chapter.

I lost my license key, can you tell me what it is?

If you purchased from Blue Iris directly, we should be able to look this up by email. If you purchased from a reseller, we only have a record of the sale if you registered your name and email on the About page in Settings. Otherwise, you will need to inquire with the reseller for the key.

Why doesn't the profile selection "stick" on a schedule page?

The profile selection box is not a setting—it only exists to allow you to select the profile you want to *draw* onto the schedule. It is the schedule that determines the active profile, and only one profile is ever active at a time. Please see the chapter on Shield, Schedule and Profiles.

Why doesn't the FPS setting "stick" on the Video page in camera settings?

The **max FPS** box is not a setting for network IP cameras. It merely reflects the maximum rate which has been observed from the camera and may be used internally to size a receive buffer. You must control the FPS and kbps that your camera is sending by adjusting this in the camera's own web browser based settings.

Why can't I login remotely using a browser or client app?

Please see the lengthly discussion on this topic in the Remote Access chapter. If you are unable to configure your security software and router(s) port forwarding for remote access, there is a service called NGROK which allows access in almost any networking situation.

Why does my security software show network intrusion attempts from foreign countries?

The Internet is a global resource. This is what allows you to view your Blue Iris and cameras anywhere in the world. However, network crawlers, "bots" and potentially malicious actors may attempt to connect as well. First, a "connection" is not the same as a "login" and these entities will gain no access to your system without the appropriate credentials. Check these security settings (they are defaults):

> On the Advanced page from the Web server tab in Settings, please be sure you retain the setting for authentication of *all connections*. This means no anonymous access.
>
> Also on that page, retain use of the *Use secure session keys and login page* option. This means that login information is encrypted and never visible in plaintext to avoid both "man in the middle" and "replay" attacks.

For even *more* security, you may consider:

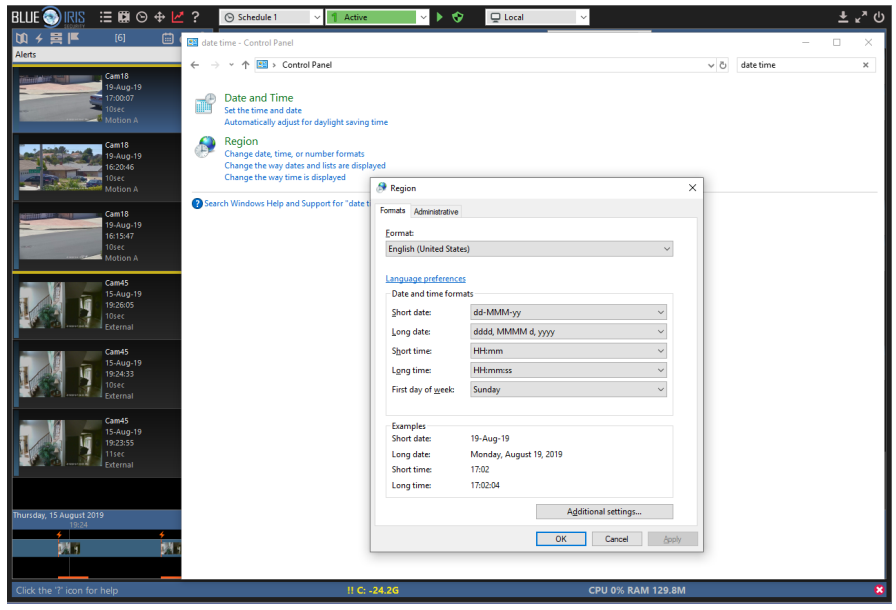
> Use the *Limit IP addresses* box on the Advanced page. The software will not reply even with a login page to addresses blocked using this feature.
>
> Use another firewall (software or hardware) to allow access only from specified IP addresses.

Why when I have alert images captured on the clips list, but attempt to play one of them I get a file not found message?

The alert image is captured at the moment of trigger. However, recording may *not* be able to begin at this precise moment if you are using *direct-to-disk* recording. In this case, recording can only begin on a *key frame boundary* and this is the essential reason to ensure that your camera is sending an adequate number of key frames. On the Cameras page in Status, you should see a key frame rate of about 1.00 (this is the number after the FPS, like 15.0/1.00). Anything lower than 0.50 is undesirable and should be remedied via settings in the camera's internal web interface.

How can I display 24 hour time or international (localized) date formats?

This is done in the Windows control panel under Region, "change the way time is displayed."



This may be set in Windows *per-user,* so if you are running as a service, this may be another reason to insure the service runs with your own Windows account, not Local System.

How can I start Blue Iris automatically when Windows starts?

The best way to do this is to run *as a service*. Please see the Administration chapter for details. However, you may want to also or instead run the GUI on the desktop. For this, you should use the Windows Task Scheduler. Methods for this are described here:

https://tinkertry.com/how-to-run-an-elevated-program-shortcut-at-startup-with-uac-prompt

There are also free-ware utilities that may be used as well:

https://www.toms-world.org/blog/start-program-at-startup-without-uac-prompt/

Why can't I open MP4 files in the viewer or see them remotely?

Many PCs lack the appropriate components that are required to open, parse and play MP4 files programatically. To enable this functionality, we recommend installing the K-Lite codec pack. You need only the "basic" version:

https://codecguide.com/download_kl.htm