



VERSION 5

**PERSPECTIVE
SOFTWARE**

143 Cadycentre #86 • Northville Michigan 48167 • USA

Copyright ©2020 Ken Pletzer, All Rights Reserved

Last revision: July 9, 2020

- Introduction.....6**
- System Requirements.....6
- Activation6
- Quick Start.....6
- What’s New7
- Update notes11
- User Interface20
- Cameras28**
- Adding a new camera.....28
- Video Settings.....29
- More Video Settings33
- Audio Settings35
- PTZ/Control.....37
- Advanced Video Topics40
- General settings.....44
- The Camera Context Menu46
- Screen layout and frames47
- Camera Groups48
- Triggering and Motion Detection51
- Artificial Intelligence.....53
- The Motion Sensor55
- Alerts61
- Schedule and Events63
- Webcasting65
- Image Posting67
- Watchdog68
- Configuration synchronization.....69
- Global Camera Settings70
- Camera Status Window.....73
- Recording and Clips.....75**
- Recording options75
- Encoder options.....80
- Manual recording82

Clip folders.....	82
The Database and Clips list.....	85
Clip Playback and The viewer window	90
The speed slider	93
Timeline playback	94
Trim, Convert, Export	96
FTP Clip Backup	99
Global viewer options	100
Alerts and Actions.....	101
Sound.....	101
Push notification	102
Run a program or script.....	103
Web request or MQTT	104
Send email.....	104
Send SMS	106
Make a phone call	106
Set DIO bits	108
Popup toast.....	108
FTP upload	109
Change shield	110
Change schedule/profile.....	110
Do command	111
Wait.....	111
Timecode and other Macros.....	113
Testing the Action Set.....	115
Shield, Profiles and Schedules	116
The Shield	116
Camera Pause	116
Profiles	117
Schedules.....	119
Run, Hold and Temporary Profiles	121
Camera Profile and Schedule Override.....	121
Remote access	122

The Web Server	122
Networking and Router Configuration	124
Remote Access Wizard	125
NGROK.....	131
Users and connections	133
Browser interface	137
Mobile device access	138
Remote management	141
SSL and HTTPS.....	143
More on Security	144
Other Advanced Web Server Topics.....	146
Email and FTP Servers	150
Email.....	150
FTP	152
More Options	155
Startup	155
Digital I/O and IoT.....	156
audio and microphone.....	160
Joystick	161
Keyboard Shortcuts	162
Macros.....	163
Other	164
Administration.....	165
Running as a Service	165
Security Software Exemptions	166
Windows Administrator Access.....	169
CPU management	170
Status messages, logs and Alerts	176
Backups.....	178
Registration, Support and Maintenance	179
HTTP Interface.....	182
JSON interface	187
DDE Interface	201

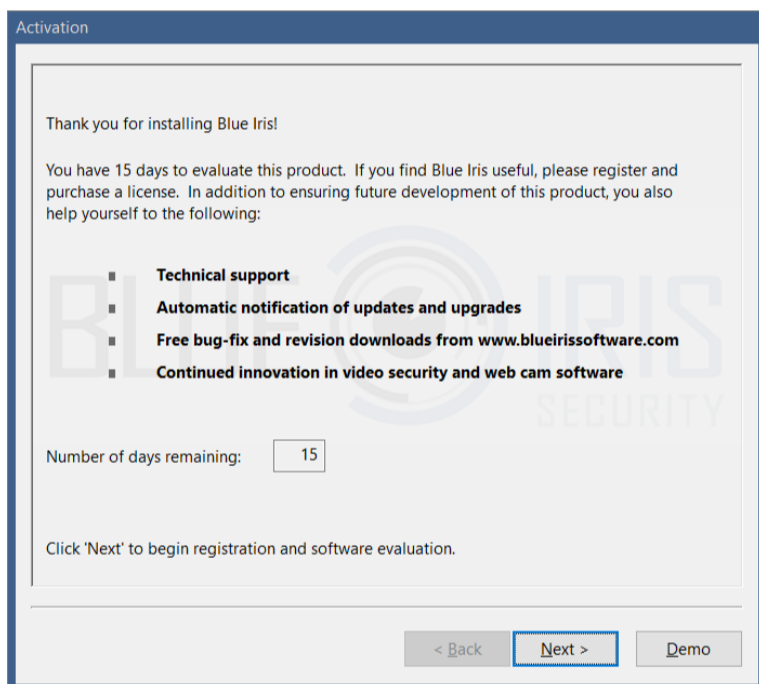
INTRODUCTION

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. 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 camera* topic in the Cameras chapter for details.

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

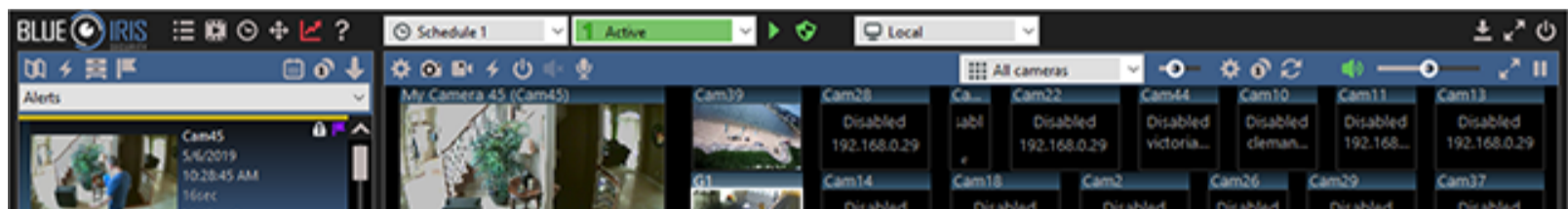
Refer to the chapter on Administration for tips on overall software operation.

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.



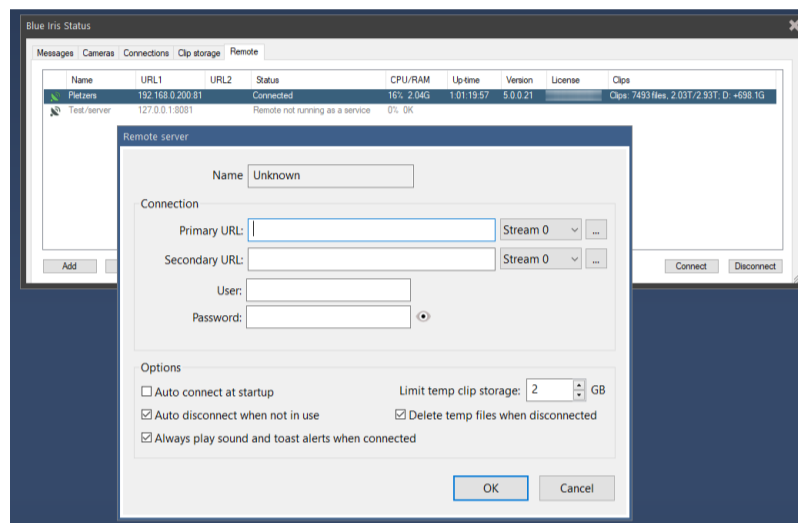
High DPI display awareness

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

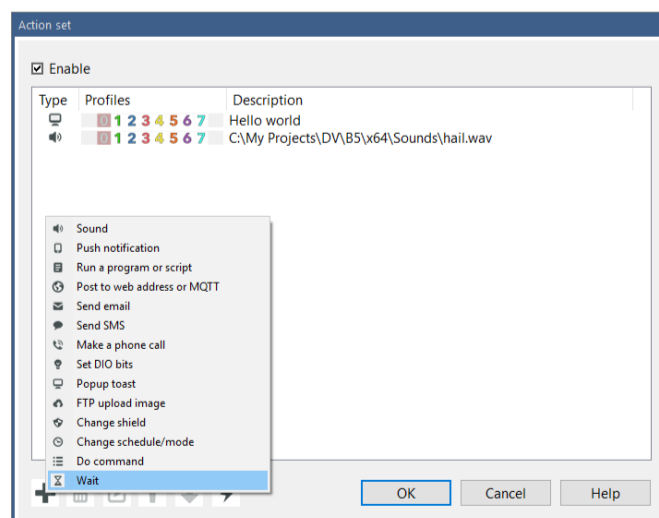
This is perhaps the most significant upgrade in terms of software power and flexibility—you may now use one Blue Iris installation to manage many others simultaneously.

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.

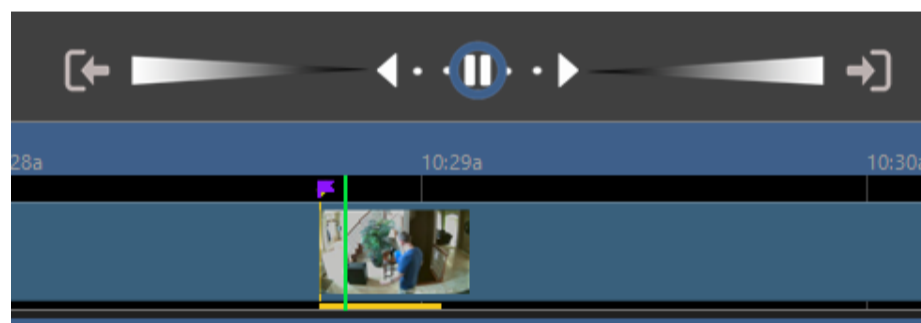
Clip management updates

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.

5.3.0 - July 9, 2020

When recording direct-to-disc 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-disc 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-disc 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/messages 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 disc” 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 disc” 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.

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 “require admin run-as administrator” 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 it 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/Messages 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 cancelled 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 Trigger 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

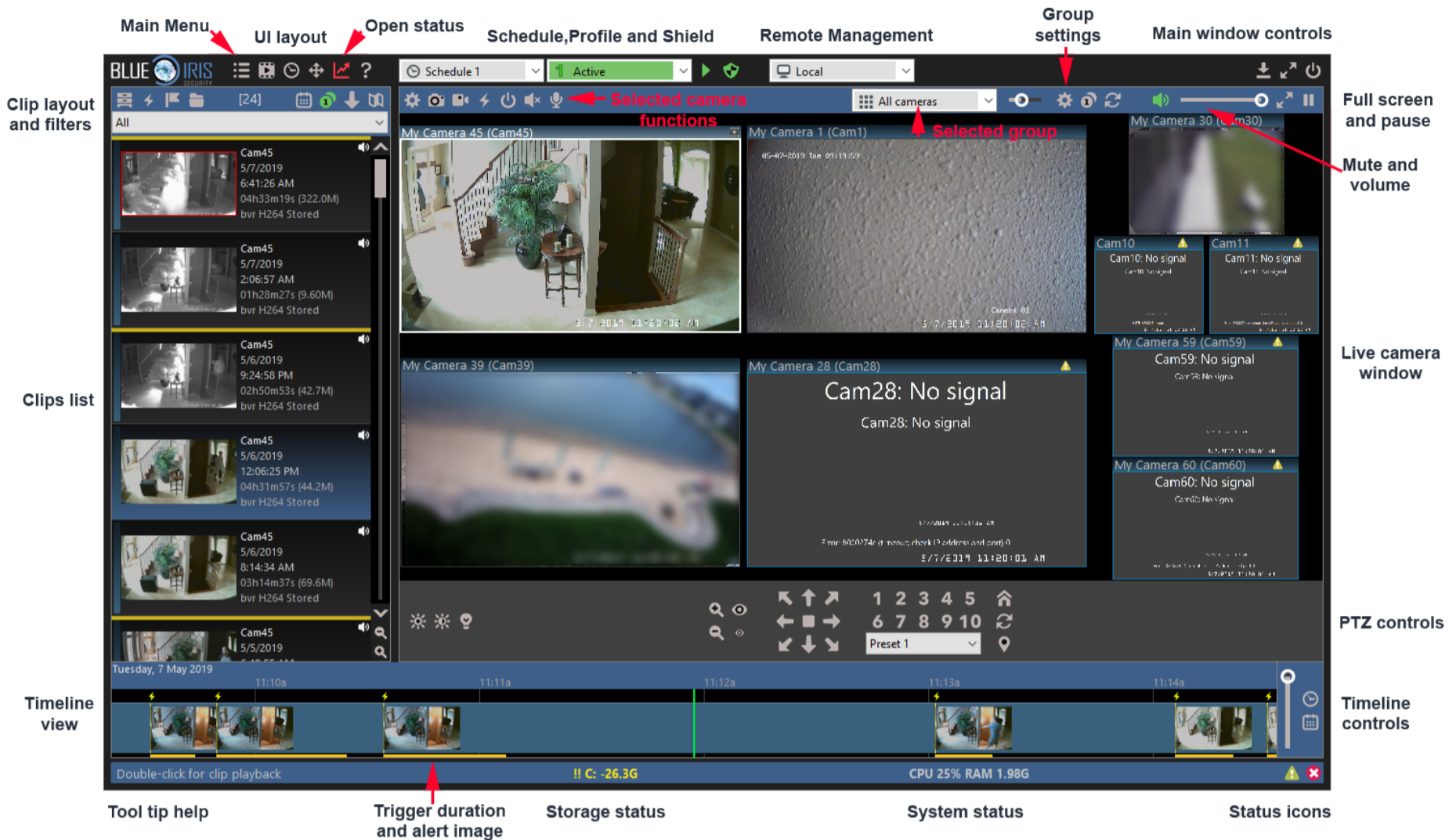
After a couple of months spent focusing solely on bug fixes and minor usability enhancements, we have reached a point of stability that now allows us to continue with more significant development.

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.

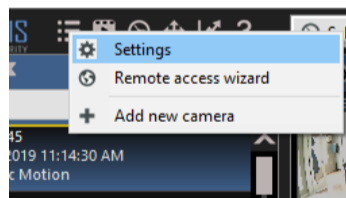
USER INTERFACE

The main window



Main menu

- ☰ Use this button to reveal a menu that allows you to access 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.

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.
-  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.

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 camera's groups 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.



Layout slider. Quickly adjust the relative size of the camera/s in the top-left position relative to the others. It’s also possible to bring either 1, 2, or 4 cameras into larger size windows at the top-left of the live video window—this requires an option on the right-click menu in the live video window under “layout.”



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



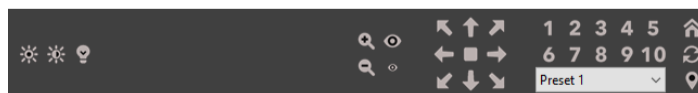
Single-camera or “solo” the selected camera. When in this mode, use the arrow keys on the keyboard to rotate between other cameras in the selected group.



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.

 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.



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 calendar icon to jump immediately to a date of interest.

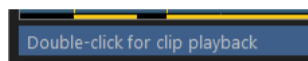


Use the time icon to force the timeline view to always display the current time at the right-hand edge.

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

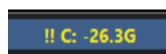
Tool tip help

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.



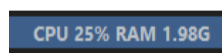
Storage status

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 disc 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 Messages page in Status contains one or more error condition messages.
-  The Messages 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 or a push webcasting error.
-  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.
-  One or more alert actions is setting DIO output bits.
-  A remote system is connected and active in the main window UI.

CAMERAS

ADDING A NEW CAMERA

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

The screenshot shows a 'New camera' dialog box with the following fields and options:

- Name:**
 - Full name: My Camera 3
 - Short name: Cam3 (for URLs and filenames)
 - Names must be unique among all cameras and groups
- Type:**
 - Network IP
 - USB, Analog, other
 - Import from exported .reg file
 - Copy from another camera
 - My Camera 23 (dropdown menu)
- Options:**
 - Enable audio
 - Enable motion detector
 - Direct to disc recording (no re-encoding)

Buttons: OK, Cancel

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 some 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:

The screenshot shows the 'Network IP camera configuration' dialog box. It is divided into several sections: 'Address' with a protocol dropdown (http://) and an IP address field (192.168.0.105), a 'Find/inspect...' button, and fields for 'User' (admin) and 'Password' (masked); 'Make' (Generic/ONVIF) and 'Model' (RTSP H.264/H.265/MJPEG/MPEG4) dropdowns; 'Media/video/RTSP port' (554) and 'Discovery/ONVIF port' (80) spinners; 'Video' section with 'Main stream' (/Streaming/Channels/101), 'Params' (transportmode=unicast&profile=Profile_1), 'Camera' (1), and 'Sub stream (+params)' (/Streaming/Channels/{CAMNO}02?transportmode=unicast&profile=Profile_1); 'Audio' section with 'Path' and 'Format' (64 kbps G.711 u-law) fields, and a checkbox for 'Setup RTSP back-channel for talk support (PCM-U format)'; and 'Network options' with a 'Receive buffer (MB)' spinner (6.0), checkboxes for 'Use RTP/UDP ports' (7000), 'Send RTSP keep-alives', 'Use RTSP/stream timecode', 'Skip initial HTTP DNS and reachability tests', 'Decoder compatibility mode', and 'Get ONVIF trigger events', and a 'Media profile' dropdown (Profile_1). 'OK', 'Cancel', and 'Help' buttons are at the bottom.

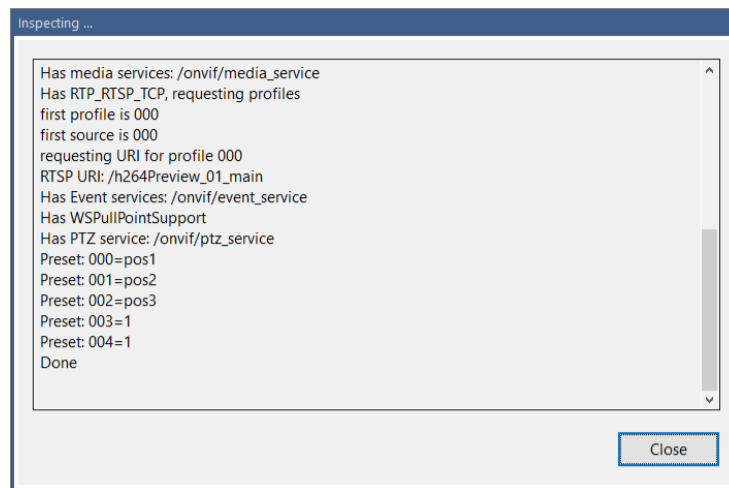
Address

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 UPnP to discover cameras connected to the same LAN segment as your PC. Here's an example of what it might find:

The screenshot shows the 'Camera discovery' dialog box with a list of discovered cameras. The list has two columns: 'Address' and 'Name'. At the bottom, there is a 'Refresh' button, a text prompt 'Select or double-click an entry to inspect', and 'OK' and 'Cancel' buttons.

Address	Name
http://192.168.0.100/onvif/device_service	AXIS M1054
http://192.168.0.102/onvif/device_service	AXIS M5014
http://192.168.0.103/onvif/device_service	AXIS M1004-W
http://192.168.0.106/onvif/device_service	AXIS M5014
http://192.168.0.107/onvif/device_service	DCS-2132LB1
http://192.168.0.108:888/onvif/device_service	IPC-model
http://192.168.0.109/onvif/device_service	HIKVISION DS-2CD2132F-I
http://192.168.0.111/onvif/device_service	AXIS M1034-W
http://192.168.0.123:80/onvif/device_service	ONVIF_IPNC

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>

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.

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.

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.

Video and audio paths

These typically will be populated automatically.

If you are using a high-megapixel camera (4MP or higher) with an RTSP stream along with direct-to-disc 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 of 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.

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.

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 *Doorbird* doorbell camera.

Network 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.

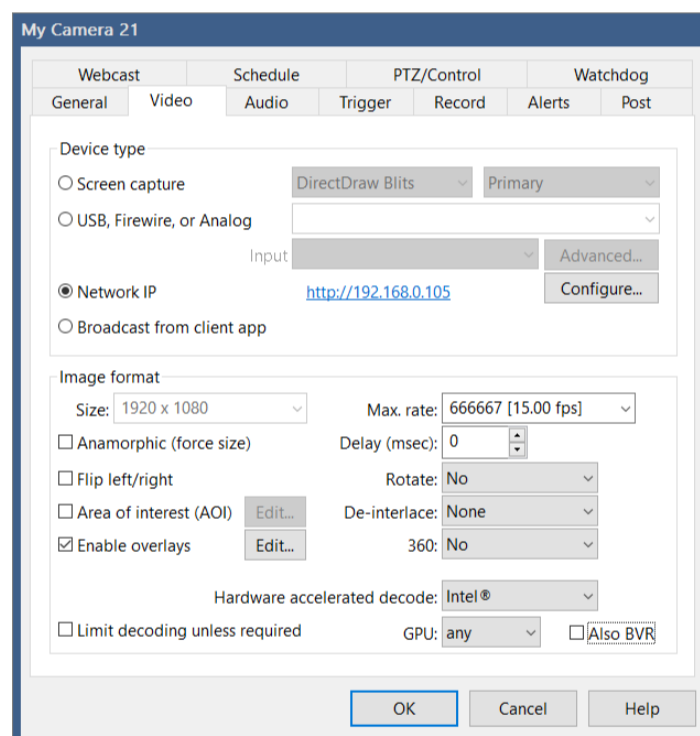
The software by default first verifies the camera is online by “pinging” its HTTP port before continuing on to video streaming. This allows a check for address redirection, and possibly a session key or cookie as well that may be required for other functionality on some models. You may elect to bypass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

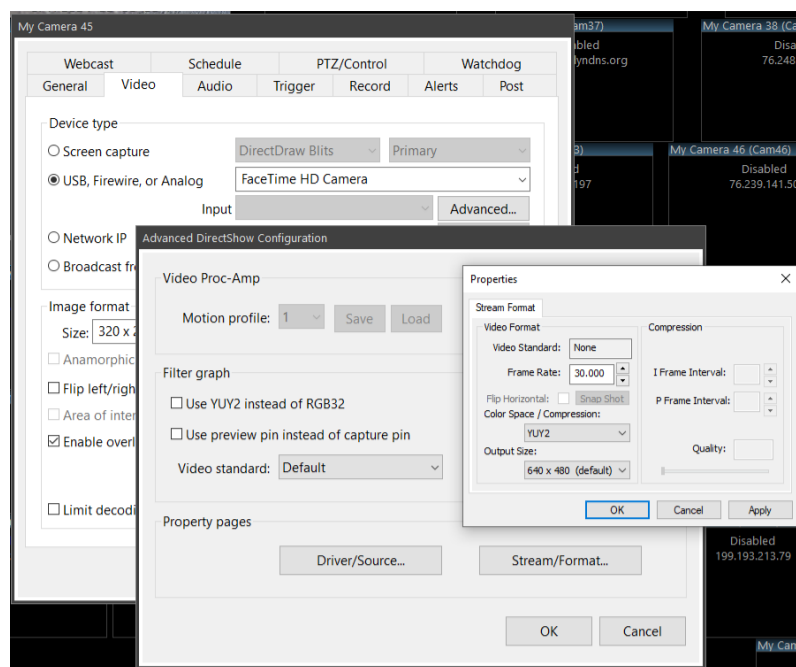
MORE VIDEO SETTINGS

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. As the service process generally cannot interact with the desktop UI, it may not be possible to use this option 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 always adjust higher, never lower. This value is used internally by Blue Iris to allocate buffers only, and is not "settable" for network IP cameras. However it is used to adjust the FPS (frames per second) on USB and other camera types.

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.

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.

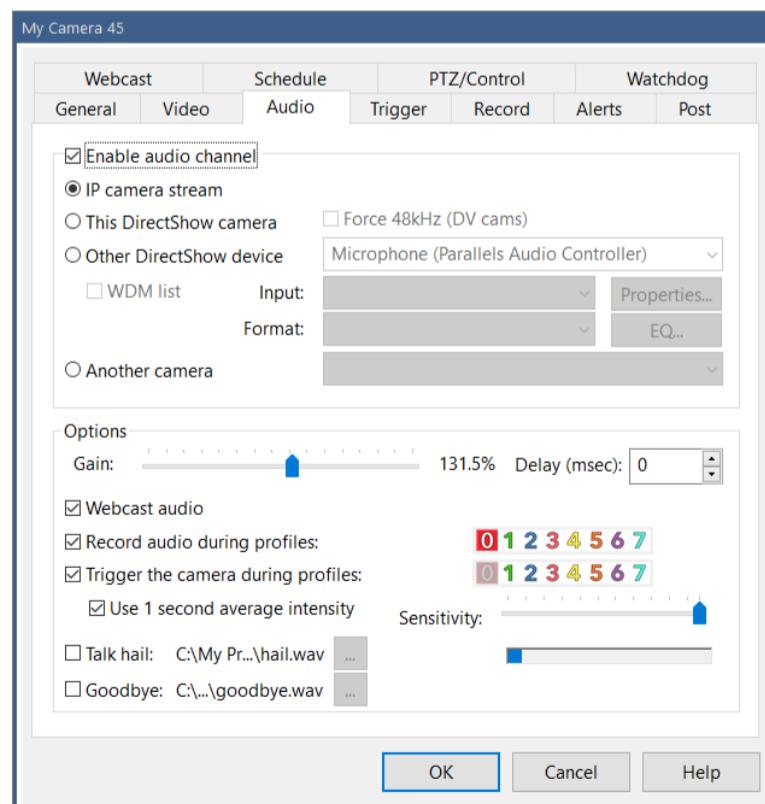
A video **Delay** setting may be used if video arrives much earlier than audio in an attempt to force audio-video synchronization. This is specified in milliseconds (ms).

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.

Audio triggering

You may wish to trigger the camera for recording and alerts based on loud-enough sounds. By default, an average sound level is measured over a one second time period and this is used to compare to a sensitivity threshold value. Without the averaging it's possible that a single sound sample of sufficient amplitude may trigger the camera. The overall sensitivity of the trigger also may be adjusted using a slider control. For testing, a level meter is shown. The camera will trigger when this peaks—and the meter will turn red to show this condition.

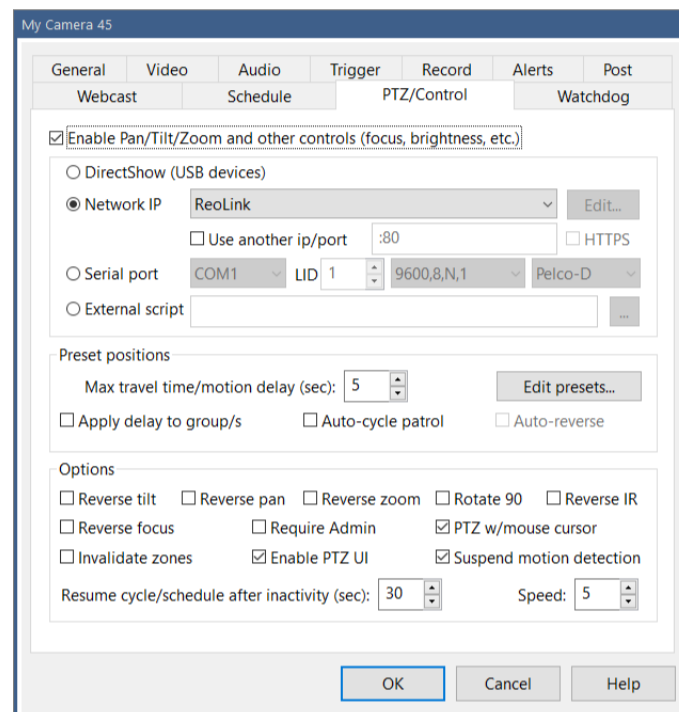
Talk

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.

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 send 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.

Select **PTZ w/mouse cursor** to allow the user to adjust camera position by clicking directly on the camera window. This applies only when the camera is solo or in a full-screen mode. You may also un-select the option to **Enable PTZ UI**. If disabled, it will not 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.

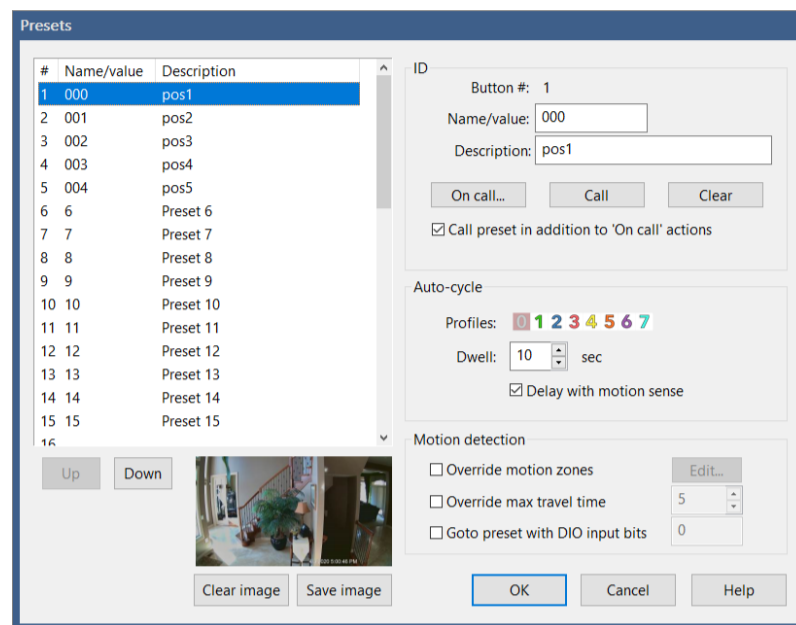
For cameras which support PTZ speed, you may select an initial value here. You may then adjust this using the right-click menu over a camera window.

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 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 **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 **Call preset in addition to ‘On call’ 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. 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.

Each preset may have its own motion zone map to override the one defined for the camera on the Motion Detection page from the Trigger page. Keep in mind that these maps are

resolution-dependent—if the camera image size changes, the map will also change. If a custom preset map is in use and another preset is called without a custom map, the software will reload the map from the Motion Detection page. See that topic later in this chapter for instructions on defining a motion zone map.

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.

Position images

Each preset position may have an associated camera image saved to disc. 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.

ADVANCED VIDEO TOPICS

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 to the CPU or 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-decode-gpu-support-matrix>

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 will be seen to *decline* from the camera, 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 Messages page in Status. For the best chance at compatibility, you should ensure that the stream is encoded as “simple” 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**. 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.

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 “#” in the Pixels column on Status/Cameras. 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.

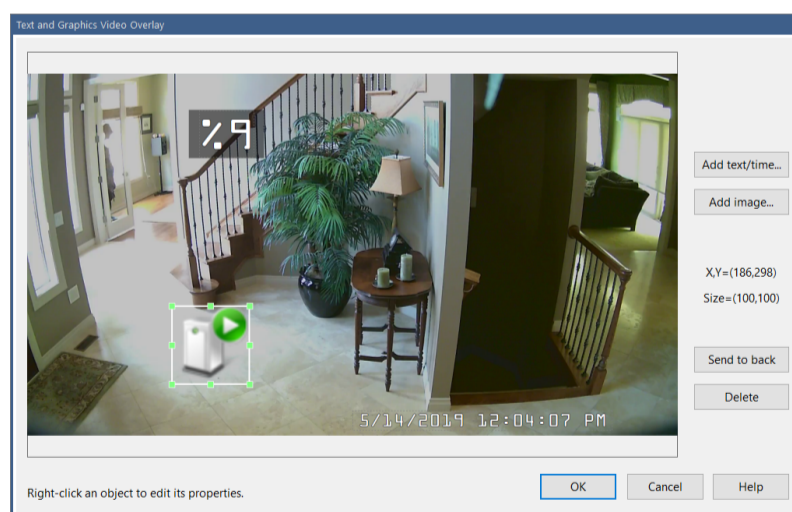
Limit decoding

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.

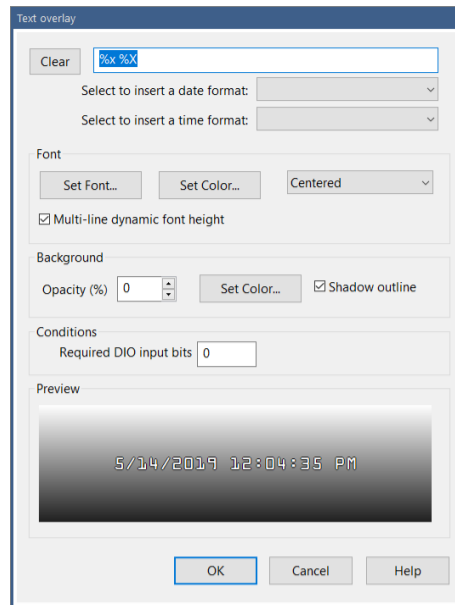
Overlays

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:

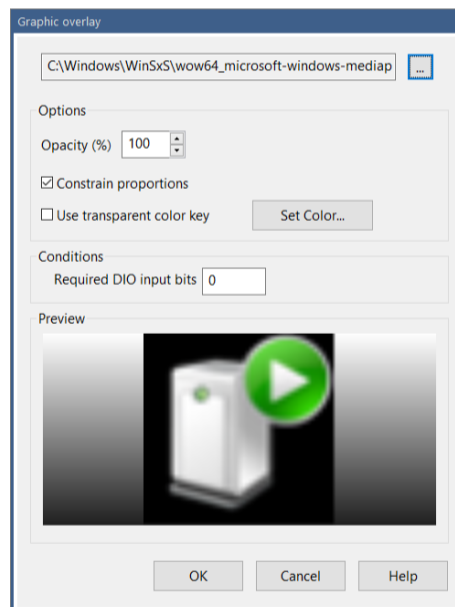


You may choose a preset time or date macro or enter your own. Please see the topic at the end of the Alerts and Actions chapter for a complete list of possible macros.

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.

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.

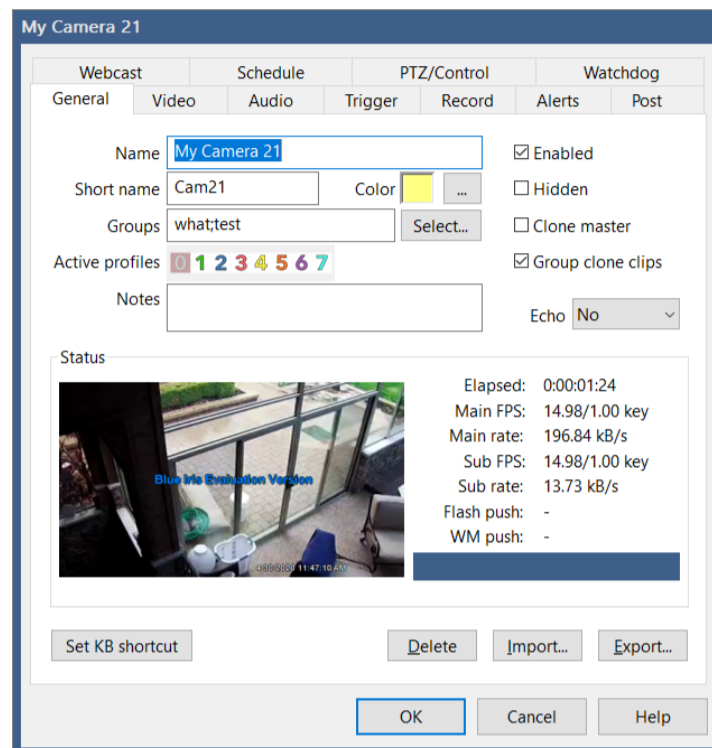
As with text overlays, the use of opacity and transparency here will result in higher CPU demand.

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.

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.

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. You will find an option in the main window UI right-click menu to **Hide disabled cameras**.

You may mark a camera as Hidden, however it may still be visible in the main window UI with a right-click menu option to **Show hidden cameras**.

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 video, unless that too is disabled on the Schedule page.

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, an 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.

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.

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.

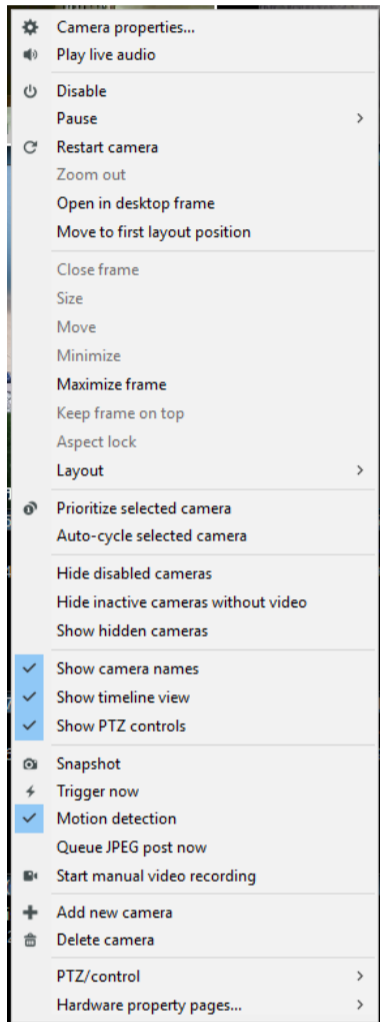
Keyboard shortcut

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 many are available from here alone.

Camera windows may be moved to the desktop by dragging and dropping, or you may use the **Open in desktop frame** command.

Camera windows may be dragged/dropped to rearrange them in the main window UI, or you may select **Move to first layout position**.

The option to **Drag lock** prevents cameras from accidentally being moved with random mouse clicks. Note that drag and drop may not be possible at all with some remote desktop software.

Additional frame commands are available such as **Keep frame on top** and **Aspect lock**.

Inactive cameras are not normally hidden, but you have the option to hide them if you also un-selected the option on the Schedule page to **Continue to display and stream video when inactive**.

De-select **Show camera names** to remove camera window headers and to make more space available for camera video.

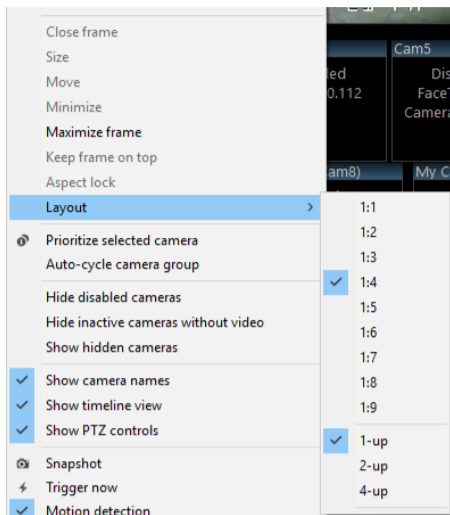
Use **Queue JPEG post now** to immediately upload an image using the destination set on the Post page in camera settings.

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.

SCREEN LAYOUT AND FRAMES

Right-click in the live cameras window to find the Layout menu:



You may choose to prioritize either 1, 2, or 4 cameras together in the top-left of the live video window. The remainder of cameras will be arranged to fit to the right and beneath these.

The ratio options 1:1 through 1:9 define the height of this group of cameras relative to the others. This ratio may also be adjusted by using the slider found at the top of the main window UI next to the group selection box.

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

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 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.

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

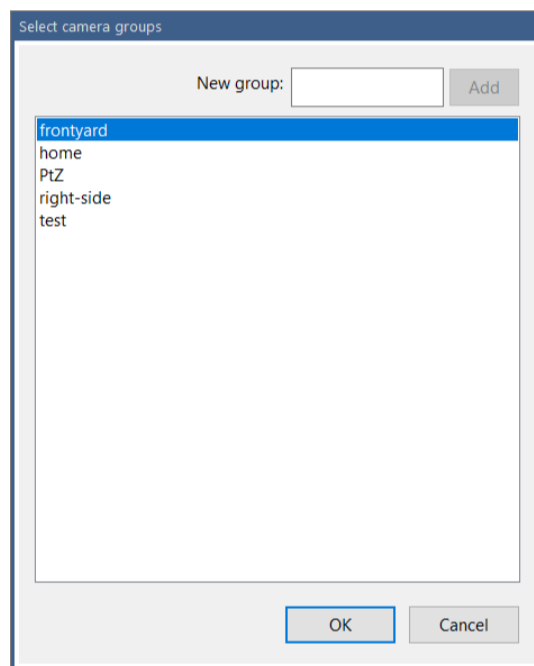
A camera group is used for viewing a subset of cameras. It's also used to provide users access to a subset of cameras on the Users page in Settings.



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.

Adding and removing groups

The Groups field on the General page in camera settings is used to place the camera into one or more *groups*.



A group exists when at least 1 camera is a member. One caveat however is that a group will not appear for viewing remotely by the client app or browser unless it has more than 1 member camera.

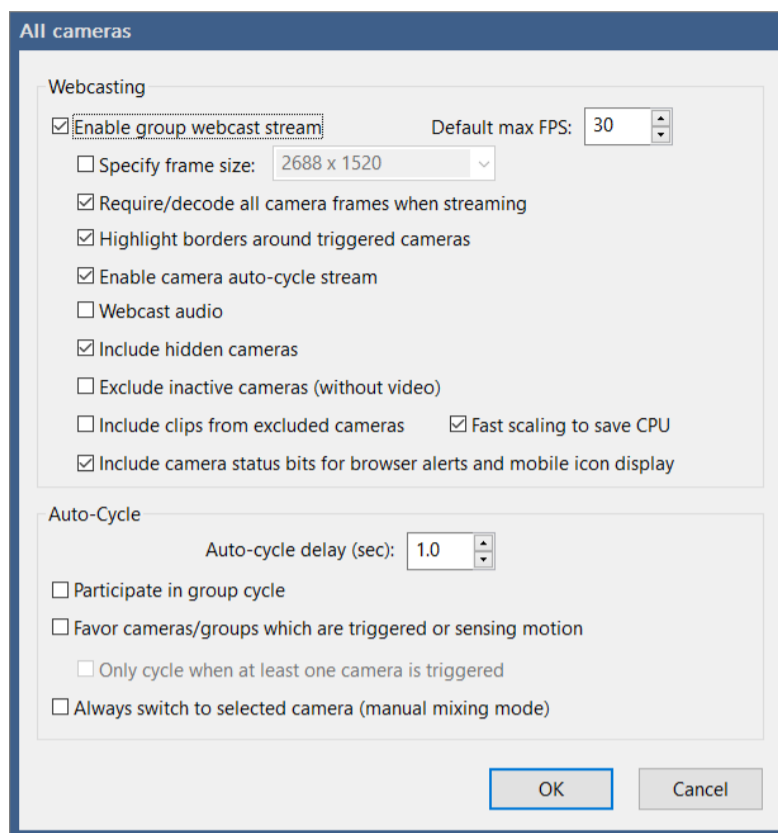
A group is only *deleted* when all cameras are removed from the group.

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.



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 for this view. 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 Cameras page in Settings just for this stream.

If **Limit decoding unless required** is enabled for any of the cameras in the group, the option here to **Require/decode all camera frames when streaming** will provide a more fluid view of these cameras when viewing remotely.

You have the option of drawing the orange borders around cameras currently in the triggered state with the **Highlight borders** option.


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 and internally is the '@' symbol followed by the group name.

You have the options to include or exclude **Audio**, **Hidden cameras**, and **Inactive cameras (without video)** in these remote views.

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 **Participate 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 triggered or sensing motion** will cause some cameras or groups to be skipped in the cycle if there are others where there is motion activity. Furthermore, there is an option to **Only cycle if there is at least one camera triggered**. 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 triggered.

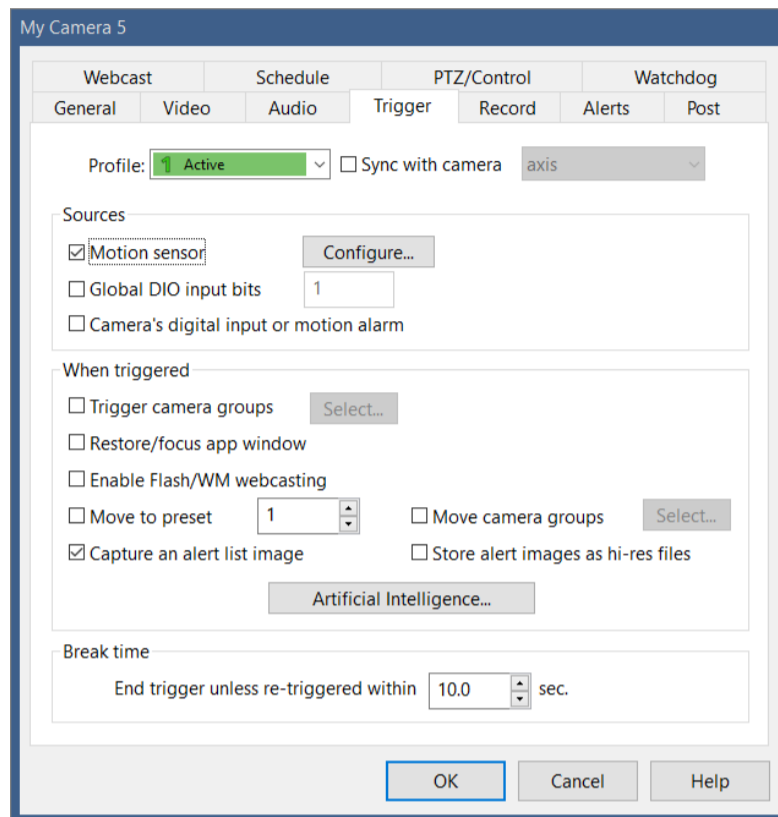
Note that in the case of camera auto-cycle, you must also select one *enabled* camera in the group to begin the cycle *unless* **Only cycle if there is at least one camera triggered** is also used.

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.



Settings on this page as well as on the Record and Alerts 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.

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.

The camera itself may have DIO terminals which may be used as a trigger source. Also classified as a **camera DIO** source for our purposes are signals received from ONVIF *GetEvents PullPointSubscriptions*.

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.

The camera may be triggered by other *External* means, possibly via menu command or 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:

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.

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 images

An alert image is a special kind of clips 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. 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 **full-resolution** JPEG files for alert images along with the "postage stamp" size images in the database. When this option is used, the alerts folder may be configured to actually move these to another folder instead of deleting them after a period of time, and at that point they become regular JPEG snapshots in the database rather than special "alert images."

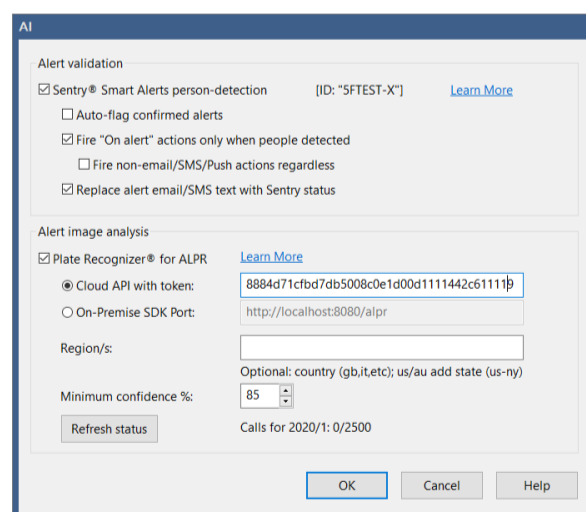
Break time

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.

ARTIFICIAL INTELLIGENCE

Artificial intelligence may be used to make the motion detector "smarter" and to reduce the incidence of false-alerts.



Alert validation

It's possible to have an alert image first analyzed by an external service prior to executing any alert actions. Blue Iris has 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 are alerts fired; if not, the trigger and its alert actions are considered *cancelled* and alert images are marked accordingly in the clips and timeline views. Click the *learn more* link for more information.

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 Sentry-confirmed alerts.

By default, Sentry screening is used to cancel alerts. By un-checking the **Fire “On alert” actions only when people detected** option, you can override this behavior and receive alerts regardless. As a compromise, you may also select to only **Fire non-Email/SMS/Push actions**.

The default behavior for Sentry alerts is to **Replace alert email/SMS text Sentry status** information.

Alert image analysis

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.

Use the **Regions** box to specify your country code for optimal plate recognition. Users in the USA and Australia may further specify a state or province.

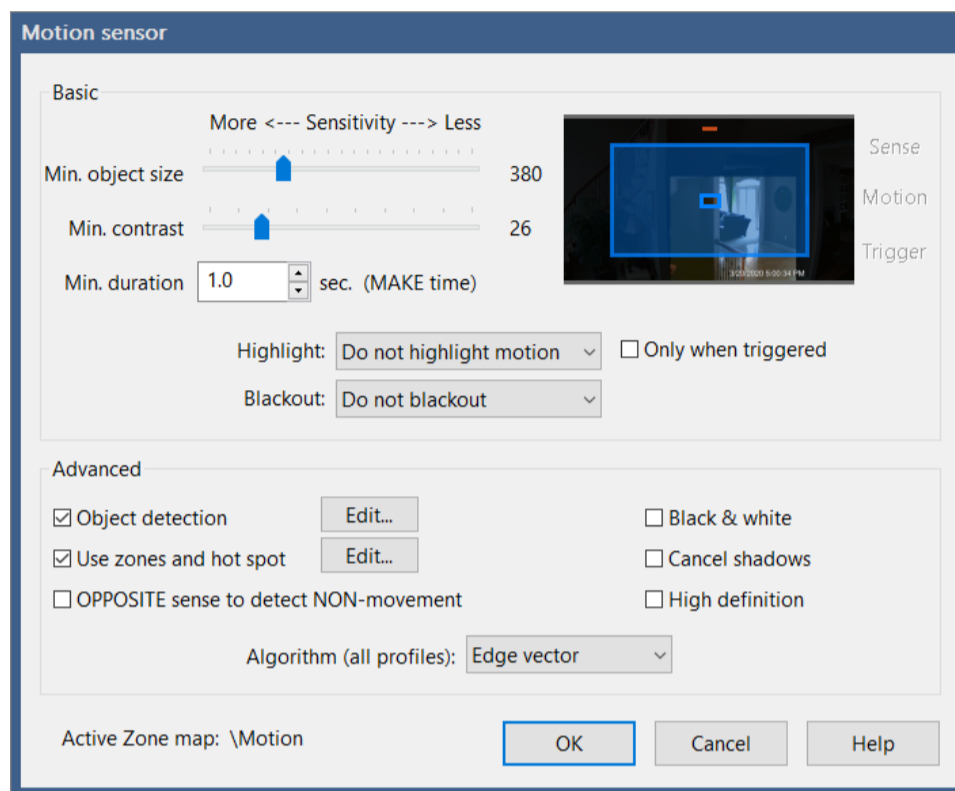
A successful plate number reading will appear on the alert image entry in the database as well as in the Status Messages log.

Active development

Additional services for AI person, pet, object, vehicle, license plate recognition, both built-in and external will be offered as version 5 development continues.

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.

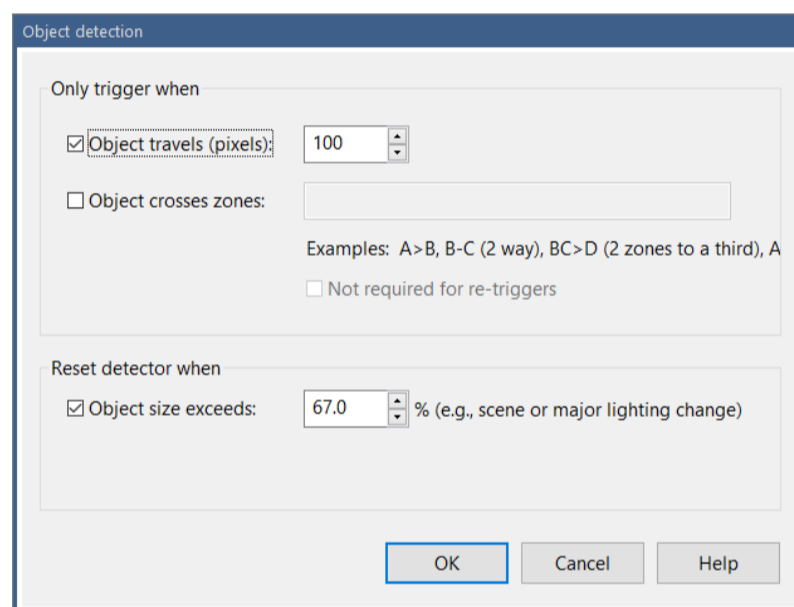
By moving either slider to the left, you will make the motion detection more sensitive, as there will be lower thresholds to overcome. The software attempts to show this visually with a small box in the center of a camera preview window to represent the *minimum* object size. There may also be a larger 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 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 **black-out** 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.

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 “hot spot” zone. There is a special syntax to use when specifying zone crossing:

- A Object must only have entered zone A
- AB Object must have entered both zones A *and* B, overlapping or not
- A>B Object must start in zone A, traveling to zone B

A-B Object must travel between zones A and B in either direction

AB>C Object must travel from zone A *and* B to zone C

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. It is possible to specify more than two zones together, for example *ABC>D*.

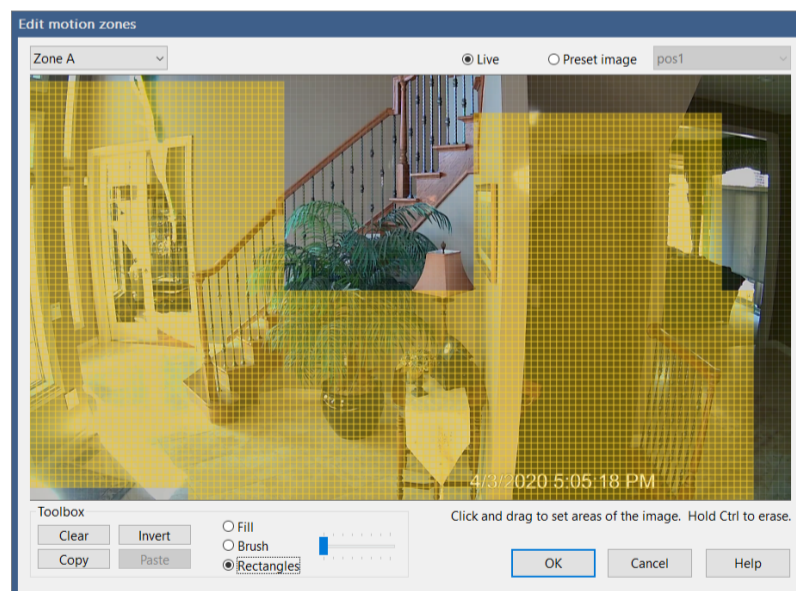
Or conditions may be specified by adding multiple zone crossing rules separated by commas.

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 hot spot

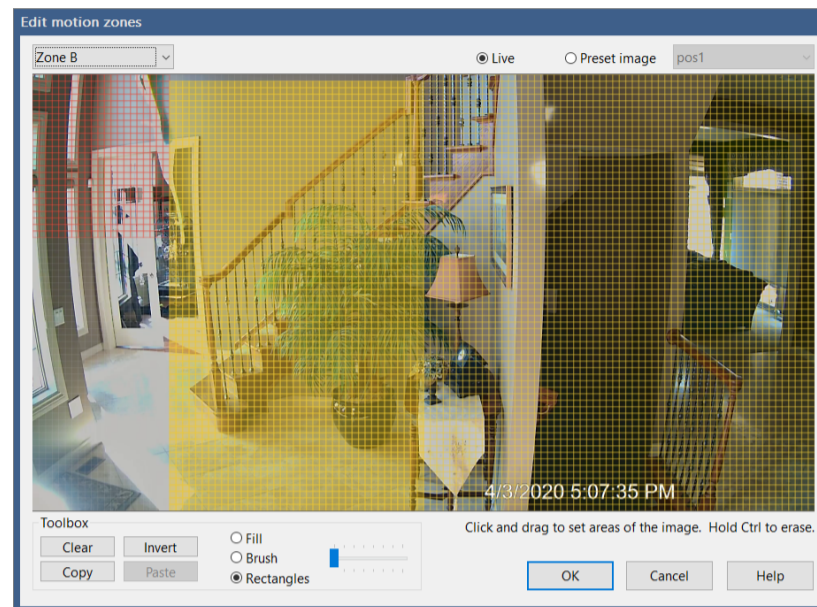
Zones allow you to identify parts of the image for consideration by object detection. They are also noted with an alert image in the clips list so that you may know more specifically the source of motion.

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 A is shown with hatch marking in yellow. Zone H (the Hot spot zone) is shown with red 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 Hot Spot 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 feature 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 movements 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*.

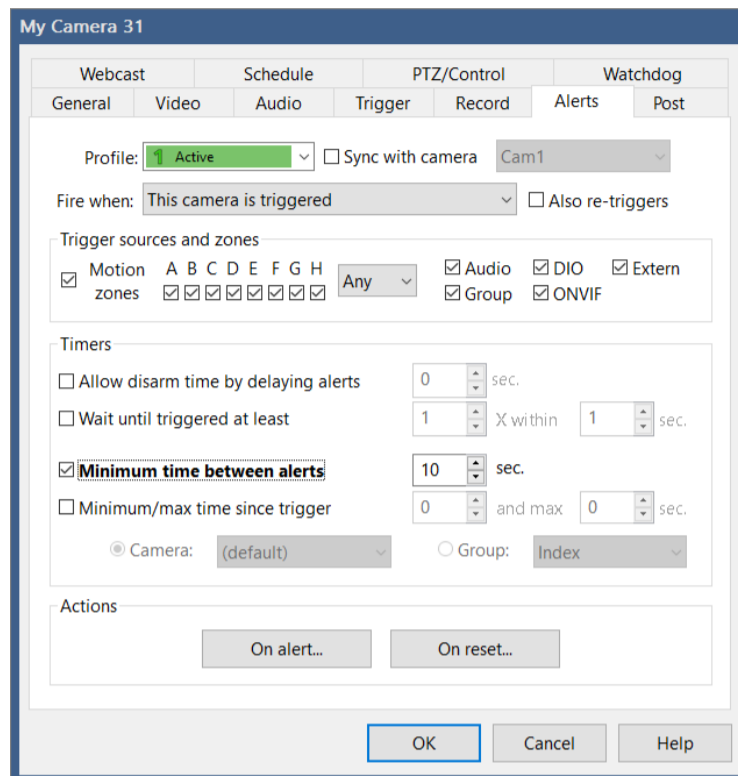
The goal here is to reduce false positives and to provide more meaningful input to more advanced AI.

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.

Triggered zone/s	Any	All	=
A	No	No	No
B or AB	Yes	No	No
ABC	Yes	Yes	No
BC	Yes	Yes	Yes

ALERTS

OK the camera has been triggered. Now what? In addition to recording, you may fire any number of actions.



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

When to fire

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 a group, or all cameras on the system in this regard.

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:

By default, an alert occurs only at the *leading-edge* of the camera's trigger state. 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.

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 alerts** setting basically gives you time to prevent an alert, perhaps as you enter the home or building where the camera would normally be triggered. If you are using the Sentry Smart Alerts, this is basically what is employed—the camera still triggers for recording, but the alerts are delayed until the Sentry service makes a determination on the accuracy of the detection.

One measure to prevent false-alerts is to employ the **Wait until triggered at least X times** feature. Generally if there's a break-in or anything else of concern, this will cause multiple triggers over a short period of time. This feature allows you to ignore short-lived motion events which may be of no consequence.

The **Minimum time between alerts** is used simply to reduce the number of consecutive alerts. Following an alert, you may not be interested in receiving alerts in quick succession as motion and triggering continue.

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

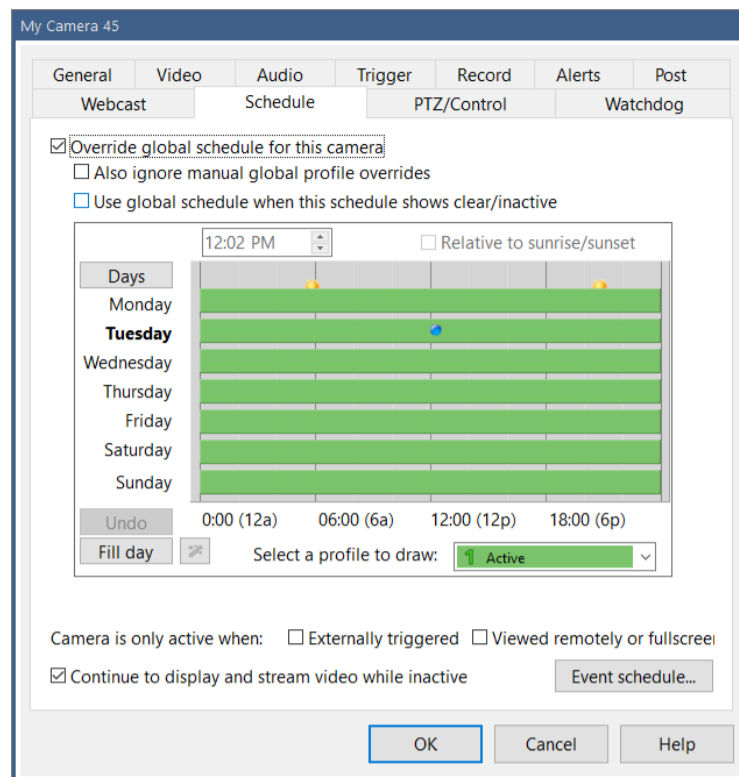
Actions

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.

SCHEDULE AND EVENTS

The global schedule has the Shield, Profiles and However, although not as it makes keeping the much more difficult, it's schedule on a per-



already been covered in Schedules chapter. generally recommended active profile straight possible to override the camera basis:

By default, an override of the global schedule (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 schedule. You may override this behavior with the setting here to **Also ignore manual global profiles overrides**.

By default, when the camera schedule shows inactive (profile 0, clear), the camera is inactive. However, you may override this so that the effective camera profile becomes the active global profile whenever it would otherwise be Inactive.

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.

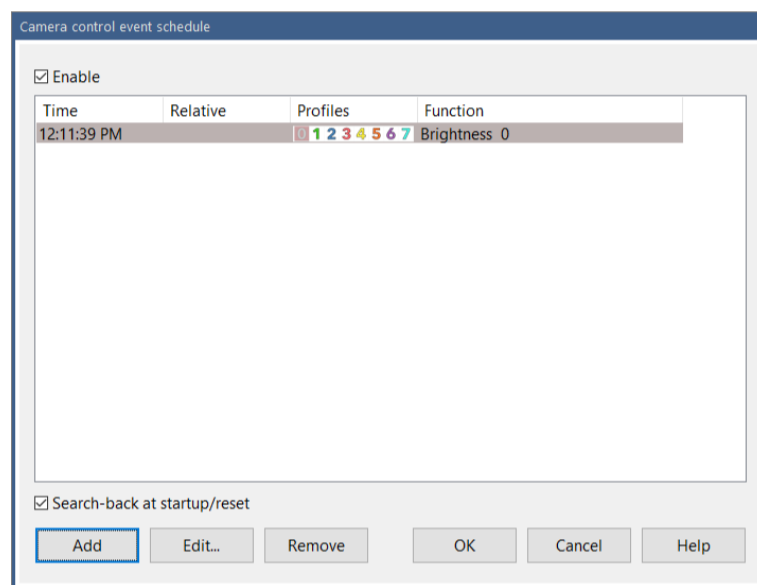
There are options here to force the camera into the inactive state (profile 0) unless the camera is currently **externally triggered**, being **viewed remotely**, or is in **full-screen display**.

By default, the camera continues to **display and stream live video when inactive**. However if you'd rather 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.

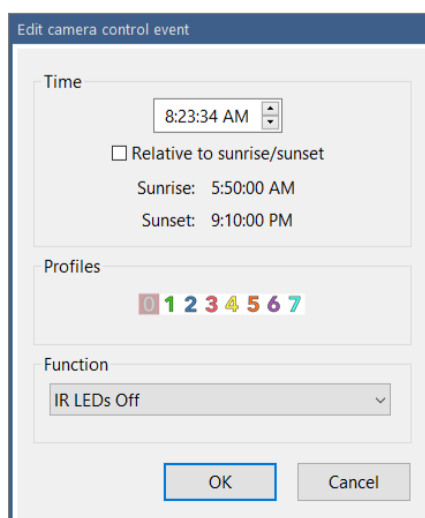


Events are executed at the specified times throughout the day. By selecting the **Search-back at startup/reset** option, the software will send the most recent event of each type when the software is first started or the camera is reset. That is, if you have a PTZ preset position 0 at 12 noon, and a 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 schedule PTZ preset position after a period of time without manual PTZ control.

When adding or editing an event

you have these options:

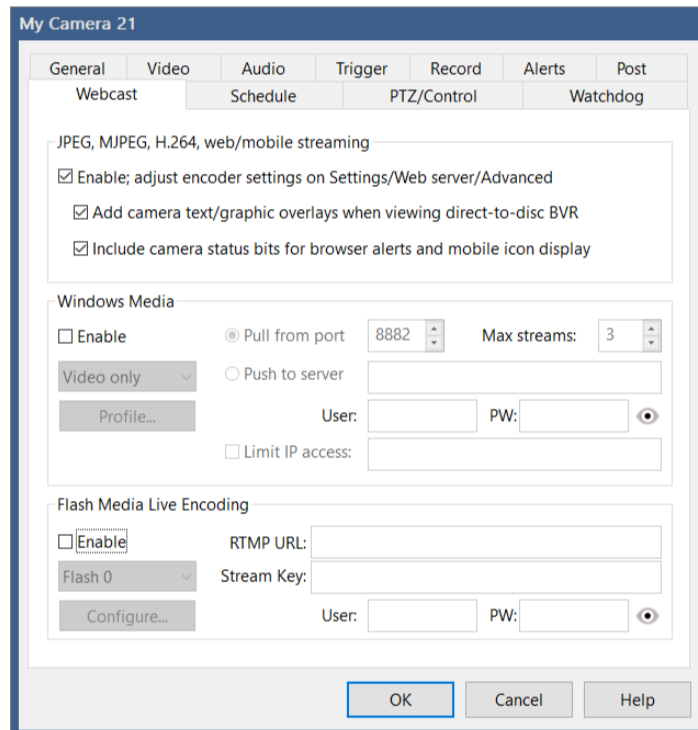


If the time is set with proximity to either sunrise or sunset, you may instruct the software to maintain this offset and move the event accordingly as the seasons change. Sunrise and sunset are only accurate if you have set your latitude and longitude on the Schedule page in global Settings.

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

WEBCASTING

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

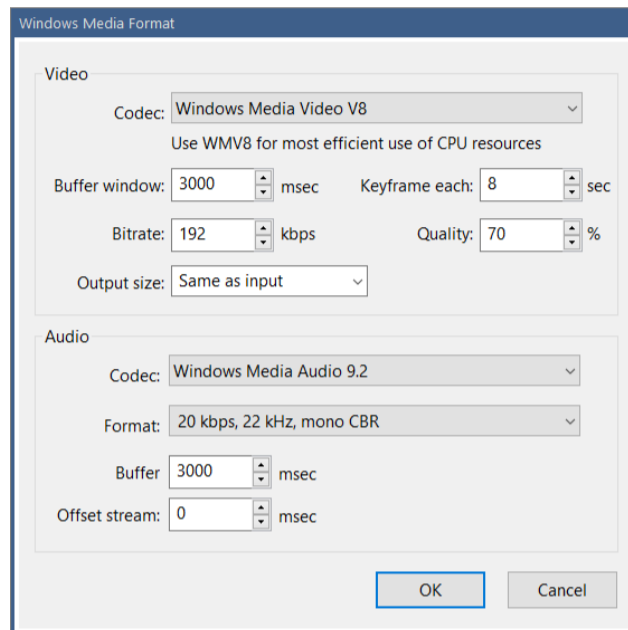


Direct-to-disc recording (by definition) does not include video overlays from Blue Iris such as the date and time. However, you may select here to automatically draw these items to captured video frames as they are served to remote clients.

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.

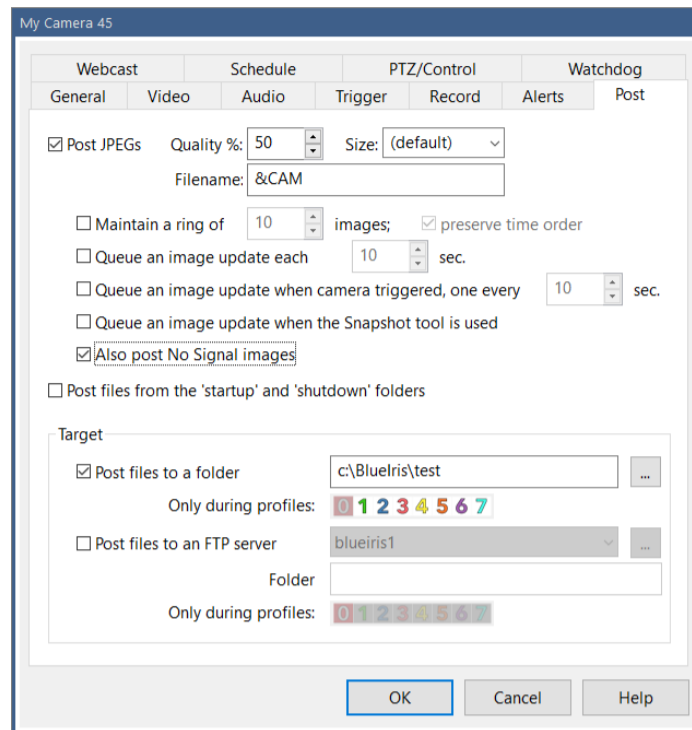
If you are hosting a video stream with a number of viewers, it will be more efficient (and maybe only possible) to serve the video in this way, rather than having a large number of clients attempting to connect to your Blue Iris server directly.

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.

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.

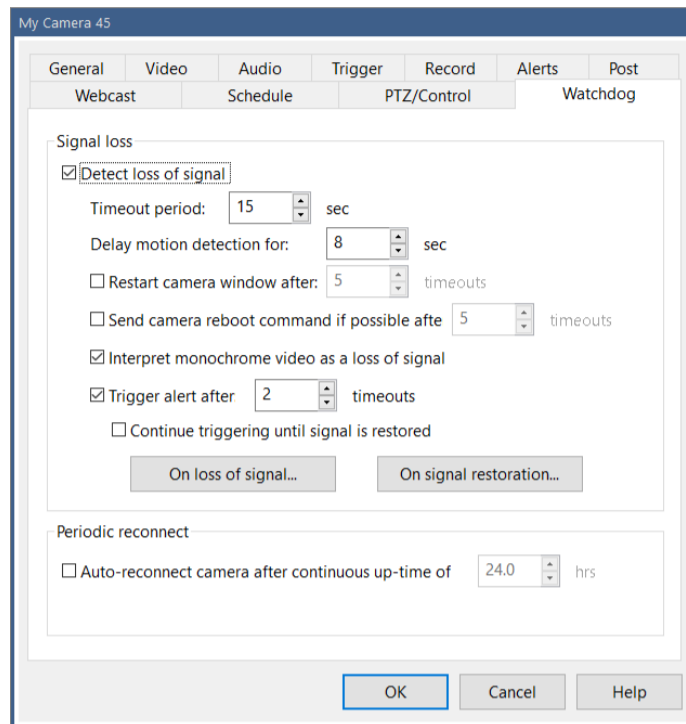
Images may be uploaded on a **timed** basis, and/or only in response to a camera **trigger** or use of the **snapshot** command. It's also possible to queue an upload manually via a command on the camera's right-click menu.

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.

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.



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.

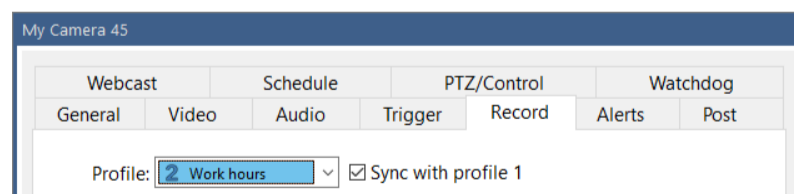
CONFIGURATION SYNCHRONIZATION

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, and Record pages the option to synchronize the page. This replaces the functionality found in older versions where copy and paste buttons were tediously used.

Profile synchronization

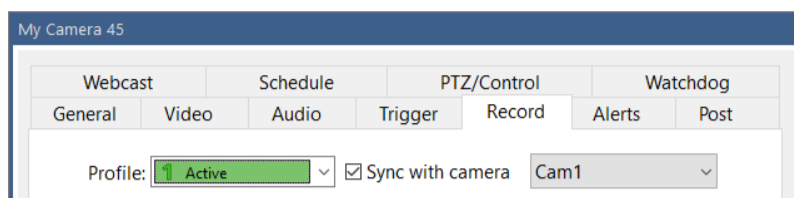
When a profile other than 1 is selected, you have the option to synchronize that profile with Profile 1 and *this is the default setting*.



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.

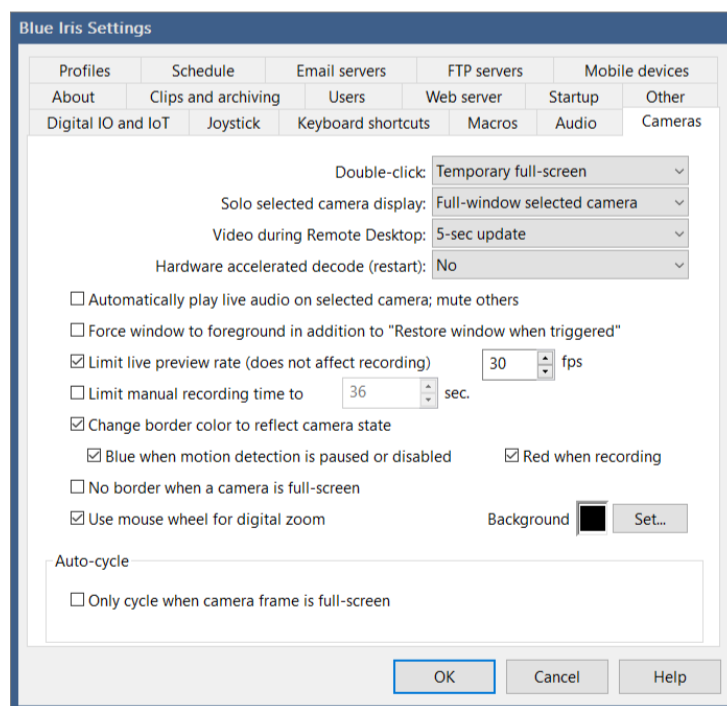


This will apply to all profiles on the camera unless you have selected to not synchronize specific individual profiles (by unchecking their **sync with profile 1** boxes). That is, if profile 2 is active and camera A's profile 2 syncs with profile 1, and camera A's profile 1 syncs with camera B, camera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

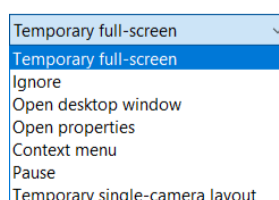
Yes it is possible to synchronize cameras in a "chain" sequence, each referencing another camera, but this is not recommended for efficiency or sanity. A settings loop will be detected and discontinued after 10 "hops."

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.

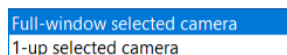


You may define what happens when you **double-click** a camera window.



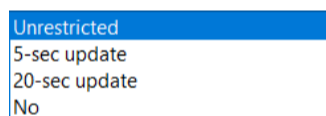
By default a double-click will open the camera individually temporarily **full-screen**. While in temporary full-screen mode, use the arrow keys to select another camera. Use Esc or the right-click menu options to exit full-screen. Use **Pause** to toggle between paused indefinitely and to cancel pause—this 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.

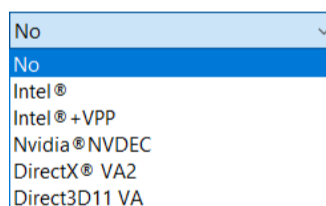


By default, a “soloed” camera is shown alone in the live video window. It’s also possible to select it to be at the “1-up” position. This means it is displayed larger than the other cameras, at a size determined by the camera layout slider at the top of the cameras window.

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**.

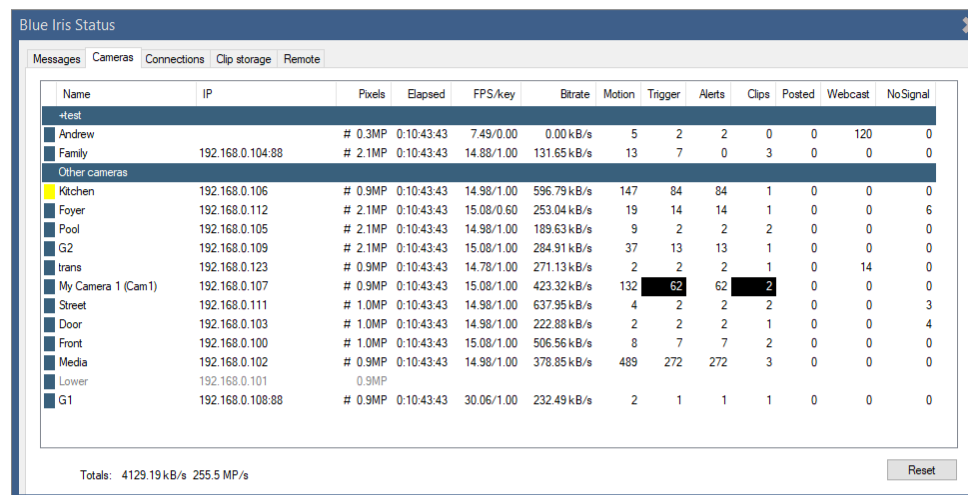
The color of the live video window behind all cameras windows may be set here.

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.



The screenshot shows the 'Blue Iris Status' window with a 'Cameras' tab selected. It displays a table with columns for Name, IP, Pixels, Elapsed, FPS/key, Bitrate, Motion, Trigger, Alerts, Clips, Posted, Webcast, and NoSignal. The table lists various cameras including 'Andrew', 'Family', and several 'Other cameras' like 'Kitchen', 'Foyer', 'Pool', 'G2', 'trans', 'My Camera 1 (Cam1)', 'Street', 'Door', 'Front', 'Media', 'Lower', and 'G1'. A 'Totals' row at the bottom shows 4129.19 kB/s and 255.5 MP/s. A 'Reset' button is located at the bottom right.

Name	IP	Pixels	Elapsed	FPS/key	Bitrate	Motion	Trigger	Alerts	Clips	Posted	Webcast	NoSignal
-test												
Andrew		# 0.3MP	0:10:43:43	7.49/0.00	0.00 kB/s	5	2	2	0	0	120	0
Family	192.168.0.104:88	# 2.1MP	0:10:43:43	14.88/1.00	131.65 kB/s	13	7	0	3	0	0	0
Other cameras												
Kitchen	192.168.0.106	# 0.9MP	0:10:43:43	14.98/1.00	596.79 kB/s	147	84	84	1	0	0	0
Foyer	192.168.0.112	# 2.1MP	0:10:43:43	15.08/0.60	253.04 kB/s	19	14	14	1	0	0	6
Pool	192.168.0.105	# 2.1MP	0:10:43:43	14.98/1.00	189.63 kB/s	9	2	2	2	0	0	0
G2	192.168.0.109	# 2.1MP	0:10:43:43	15.08/1.00	284.91 kB/s	37	13	13	1	0	0	0
trans	192.168.0.123	# 0.9MP	0:10:43:43	14.78/1.00	271.13 kB/s	2	2	2	1	0	14	0
My Camera 1 (Cam1)	192.168.0.107	# 0.9MP	0:10:43:43	15.08/1.00	423.32 kB/s	132	62	62	2	0	0	0
Street	192.168.0.111	# 1.0MP	0:10:43:43	14.98/1.00	637.95 kB/s	4	2	2	2	0	0	3
Door	192.168.0.103	# 1.0MP	0:10:43:43	14.98/1.00	222.88 kB/s	2	2	2	1	0	0	4
Front	192.168.0.100	# 1.0MP	0:10:43:43	15.08/1.00	506.56 kB/s	8	7	7	2	0	0	0
Media	192.168.0.102	# 0.9MP	0:10:43:43	14.98/1.00	378.85 kB/s	489	272	272	3	0	0	0
Lower	192.168.0.101	0.9MP										
G1	192.168.0.108:88	# 0.9MP	0:10:43:43	30.06/1.00	232.49 kB/s	2	1	1	1	0	0	0
Totals: 4129.19 kB/s / 255.5 MP/s												

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). A hash tag (#) before the MP value indicates that the camera is currently using *hardware decoding*.

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 1.00 is desirable for optimal use of the *direct-to-disc recording* option as well as the *limit-decoding unless required* functionality. Adjust this rate within the camera's web browser interface.

Direct-to-disc 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 disc 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 Messages page in status.

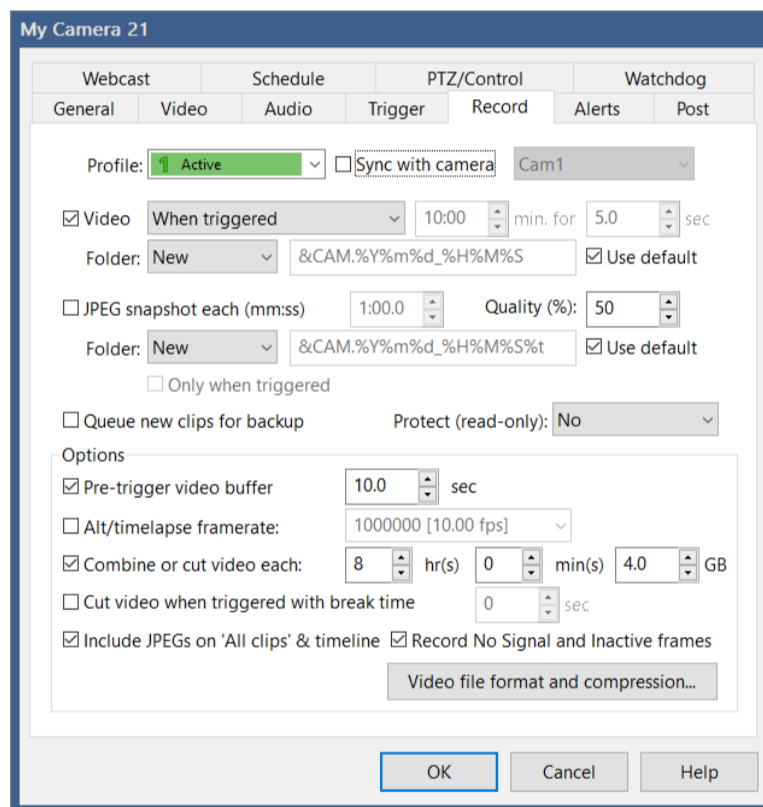
RECORDING AND CLIPS

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 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.

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 the triggered state.

Triggered + continuous. Records video in an interval manner where playback gaps are *retained*—playback will appear to pause between recorded segments. All frames are recorded when the camera is the triggered state, however.

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 conflicting 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 video buffer** applies only to *when triggered* recording. This is a useful feature for capturing the moments leading up to a trigger event. There are a couple of considerations when using this however, depending on whether or not you are using “direct to disc” recording (discussed in the format and compression topic below). Without direct to disc, all pre-trigger frames will be encoded at once upon trigger. As this has the potential to require time and CPU resources, you should keep the pre-trigger time to a minimum, ideally just a few frames. If you are using direct to disc recording, this is not a concern, as the frames are pre-encoded—however you must be mindful that recording can only begin on a

key frame and not an arbitrary time in the stream. Key frames are generally spaced at 1 second intervals, but you should take a look at Cameras in Status to see what your camera is sending.

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.

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 *when 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 equally divides a day, such as 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.

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.

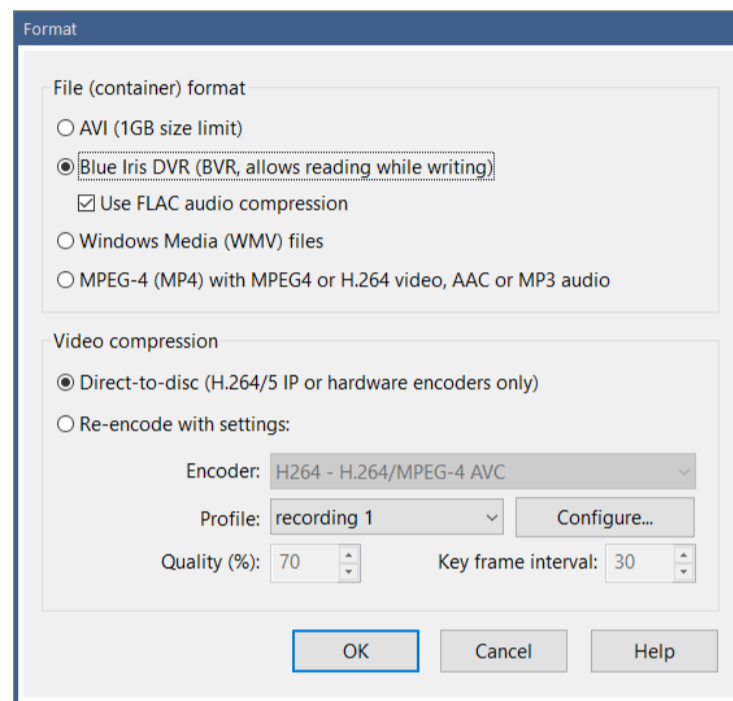
There’s an option to save an image only when triggered. Depending on your timing for trigger break time and snapshot interval, one or more images may be saved.

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-disc

This option may be used to save considerable CPU time. Video taken from a network IP camera stream is directly saved to disc 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.


- Video overlays are not saved. This includes the time/date stamp as well as others you may have added.
- 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 disc. 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.

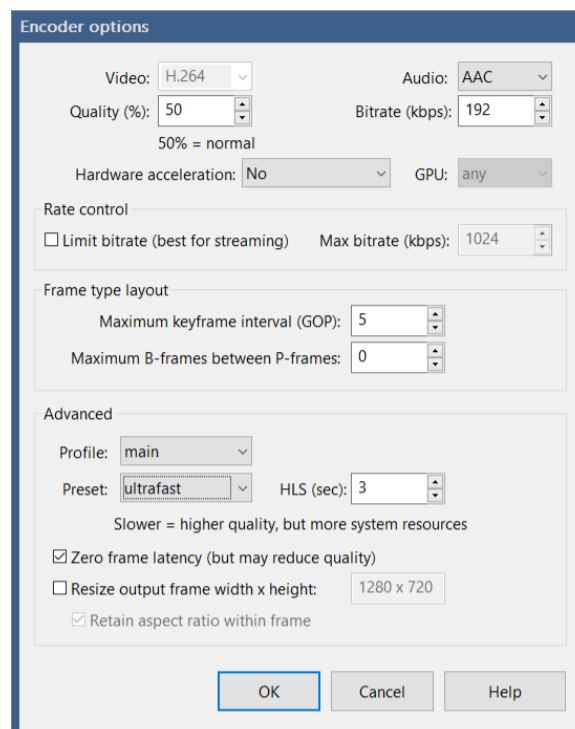
More options

 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 disc 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-disc* or when video is exported from BVR format to MP4 without alteration, these 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 Messages page in Status, and the software “falls back” to software-based encoding.

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.

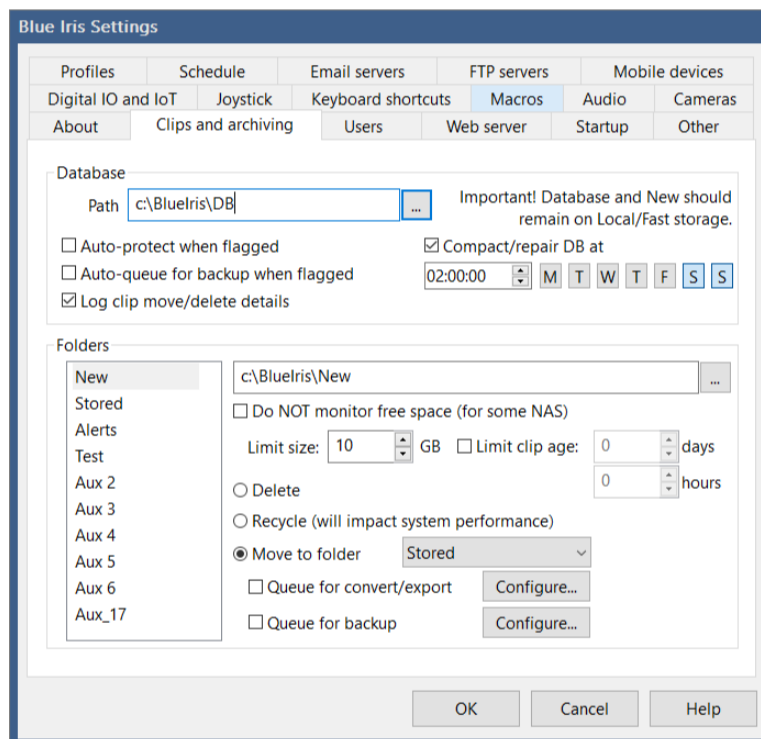
The option is provided to **Resize the output frame**. If not used, the video output resolution will equal the input resolution. You may be necessary for instance to take your 5MP camera video and resize it for consumption online where videos are typically only 640x480, 1280x720, 1920x1088 etc.

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 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 folders, and the *Alerts* folder will remain empty unless you have asked for **hi-res alert images** on the Record 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.”

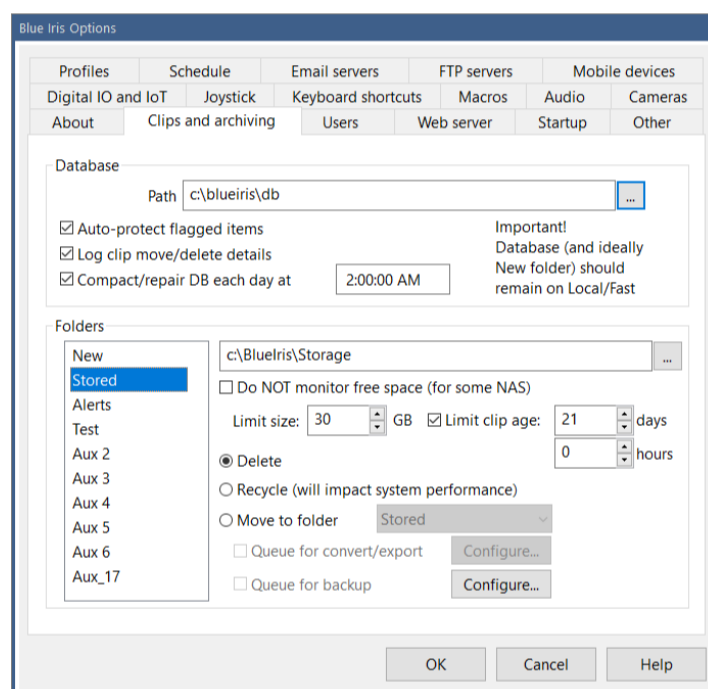
Each folder may be configured to reference a different volume or drive entirely—excluding the *Alerts* folder, that is a total of nine possible drives. Although *New* and *Database* should remain on your fastest storage possible because of frequent access, the only other requirement is that these folders 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**.

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*.

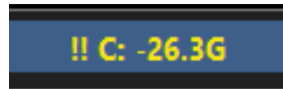


Each folder is given a **size** (in gigabytes) and an **age** (in days and hours). Once a folder reaches either occupancy limit, always the *oldest* clips in that folder are moved or deleted in sequence until order is restored.

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.

It is important to 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

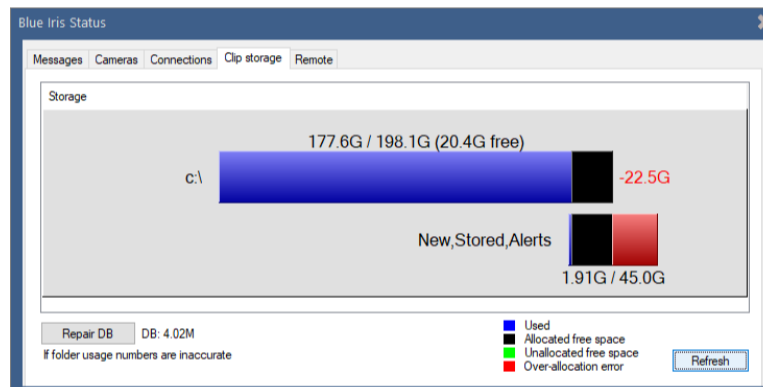
addressed, the drive *will* run out of space, and that will lead to other complications and instability.



It is important to know that the **age** is 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.

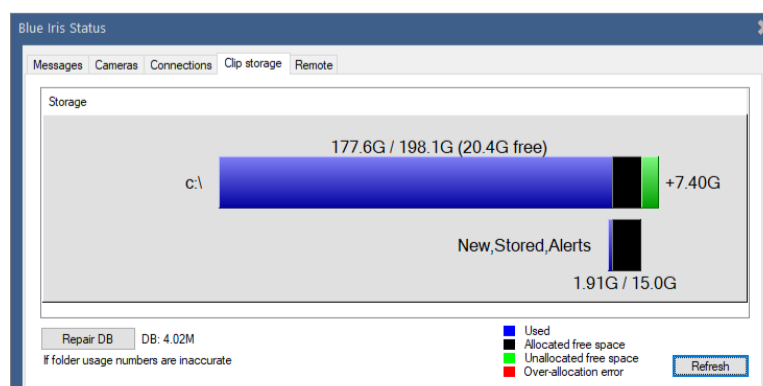
Use the option to **Recycle** instead of **Delete** cautiously. This requires more system resources, and can be Windows user-specific. If you are running as a service, you should be running with a named user account, not *Local Service* if you are considering use of the *Recycle* bin. The option to **Not monitor free space** should also be used on rare occasion—if the software has trouble reading free space from a drive, it may also indicate a problem with accessibility due to running the service improperly.

The Clip storage page in Status offers a visual overview of your storage settings:



Here we see an overallocation as we've selected 15 GB for the New folder and 30 GB for Stored. This will not fit on the drive by over 22GB. The first line shows the drive's size, used space (in blue) and free space (in black). The next line shows your Blue Iris folders which are configured to use this drive—used space is blue, unused space is black, but the *red* indicates requested space which will not fit onto the drive. This must be corrected to prevent the drive from eventually running out of space as new clips are created.

By lowering the total requested space to 15GB, here is the new chart:



The green space on the C: drive 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!**

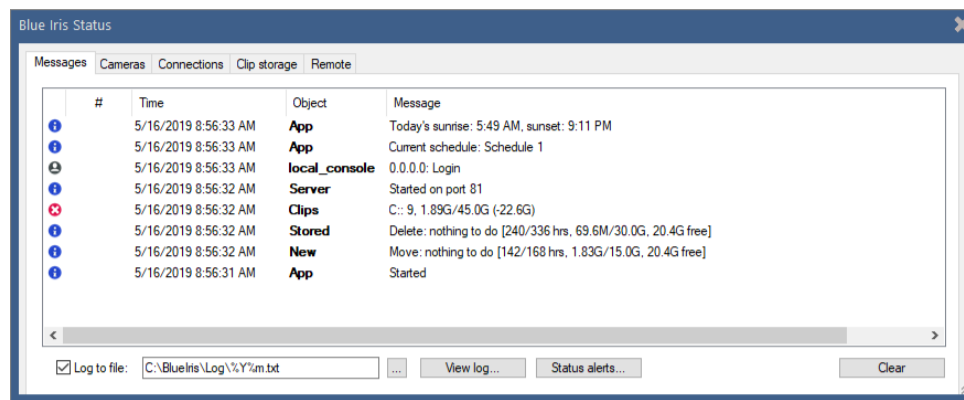
THE DATABASE AND CLIPS LIST

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*.

Database compact/repair 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/Repair*. If you disable this option yet neglect to perform it manually, the database will grow unbounded and performance will suffer.

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**.



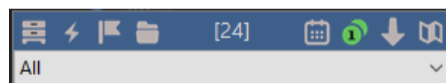
Each folder’s statistics appear in the format *240/336 hrs, 69.6M/30.0G, 20.4G free*. This indicates:

- 240* the oldest file in the folder (hours).
- 336* the maximum age set for the folder
- 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 configured to use on the drive
- 22.6G* the amount of the overallocation

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.



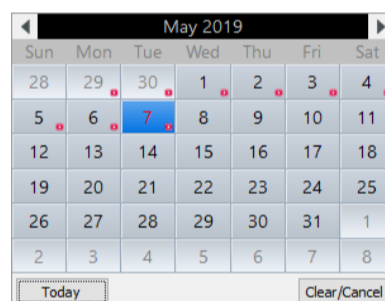
Show flagged items. Flagged items may include a combination of clips (files) and triggered alert images. Flagged items are marked with purple flags in both the clips list and the timeline view.



Select another view of the database. You may choose to view only alerts that have been either confirmed or cancelled by Sentry Smart Alerts.



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.



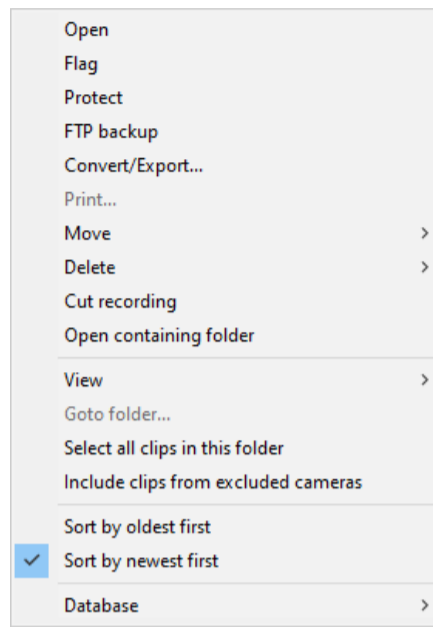
Use the **Solo** icon to filter the clips list to display only items from one particular camera—the selected camera. If you are using the live view’s camera solo function, the clips list will already be filtered, and it is unnecessary to use this option as well.



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

Clips list context menu

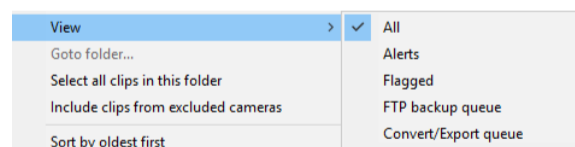
Several options are repeated on this menu, however many are available here solely.



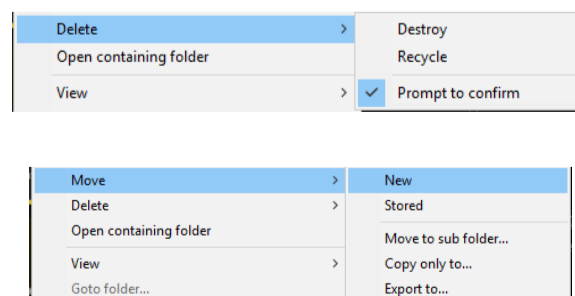
You may just double-click an item on the clips list, or click once and then use the *Enter* key to **Open** it in the viewer window.

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 disc 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. The *View* menu may be used to select a managed folder or one of these queues.



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.

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.

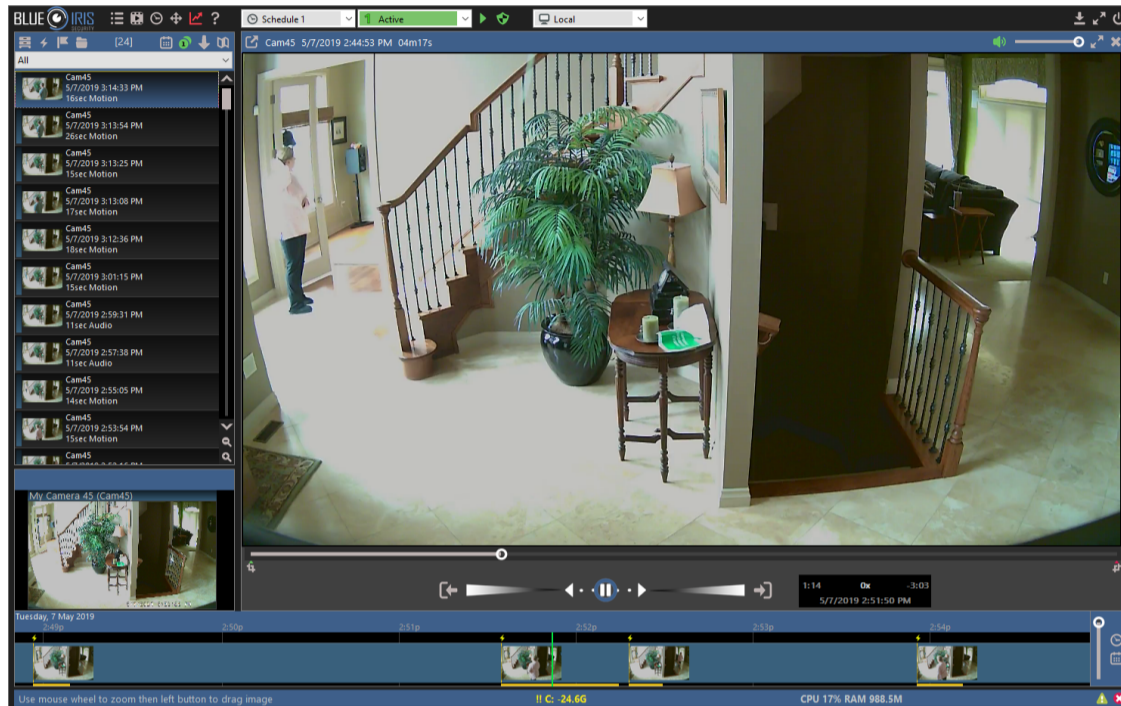
Note that an *alert image* cannot be moved, copied, or exported here unless it has an associated JPEG file created using the **hi-res** option on the Trigger tab in camera settings. Recall that an alert image is normally just a database entry referencing an actual clip. Furthermore, deleting an alert 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.

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.
- ✂ 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

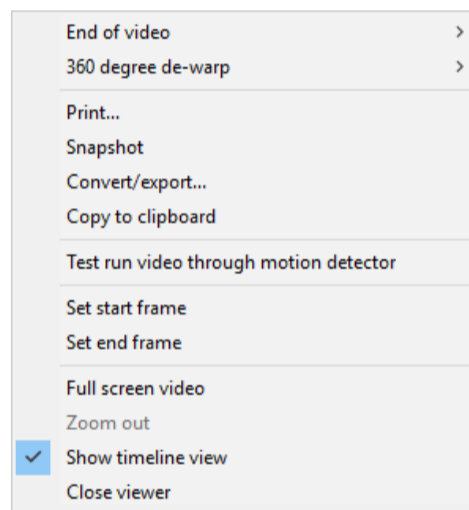
Use the mouse wheel over a camera window to zoom in digitally (the camera lens does not actually move). When zoomed in, the mouse cursor will become a “hand” icon and may be used to pan around.

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.

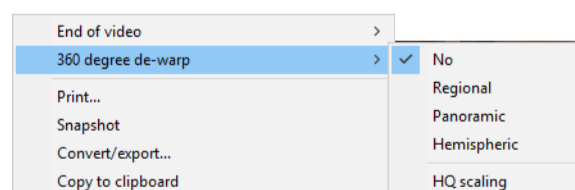
Viewer context menu

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).

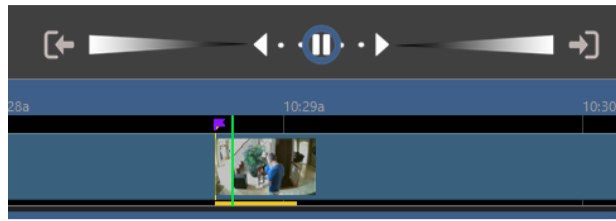
You may copy the current viewer image **to the clipboard** at the maximum resolution of the source regardless of how it's scaled for display.

The **Test run video through motion detector** feature can 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 disc” recording or ones without added motion highlighting
- 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.
- Don't forget to turn off this mode when you are finished with it!

If you ask 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.

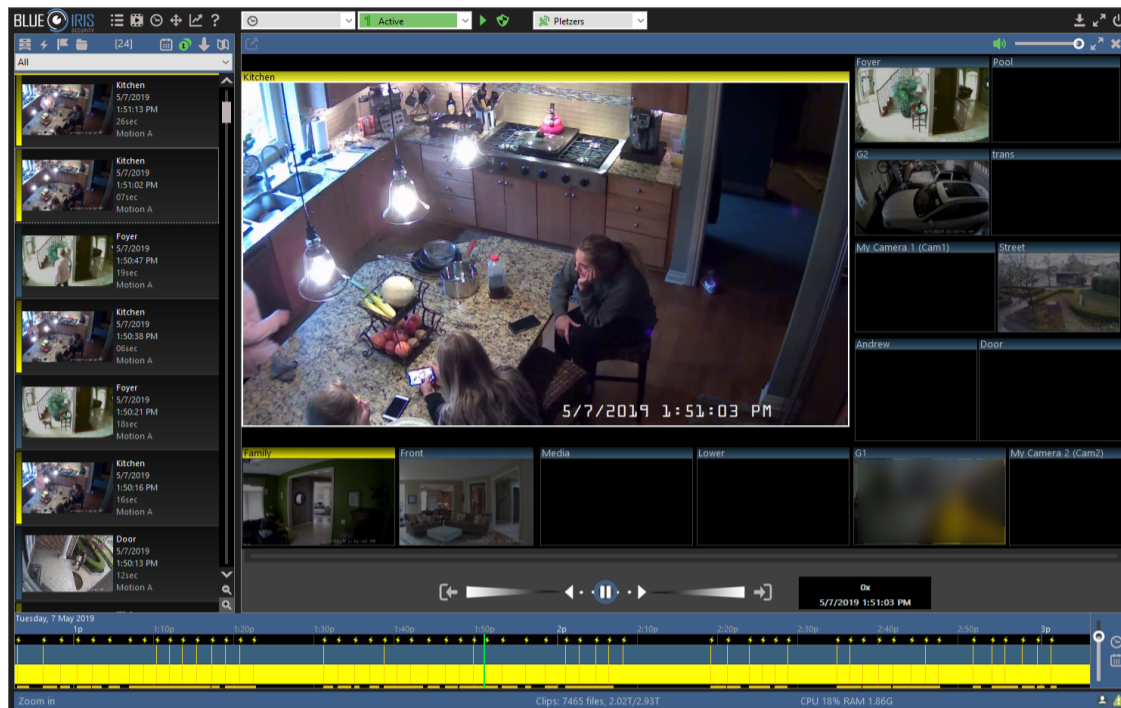
Click anywhere on the control further to the left or right for high-speed playback in either direction, up to 256x.

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 either jump forward or backward by 30 seconds, or to move to the next or previous alert, discontinuity, or file (whichever comes first), depending on the mode and type of file that is open for playback. Hold the Control key before clicking to force a movement to the next alert or clip on the current list.

TIMELINE PLAYBACK

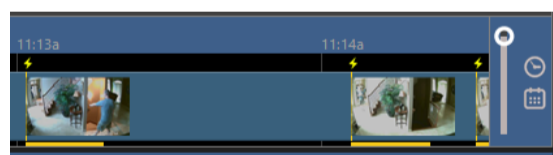
Double-click anywhere in the timeline view to enter *timeline playback*. Use the Esc key or the X icon to close timeline playback.



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.

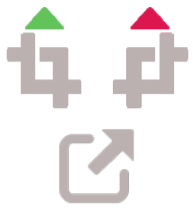
- Use these icons to jump to the previous or next alert position respectively. If there are no alerts currently visible on the timeline, these buttons will jump backward or forward by a time equal to 1/2 of the visible timeline (a page jump).

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

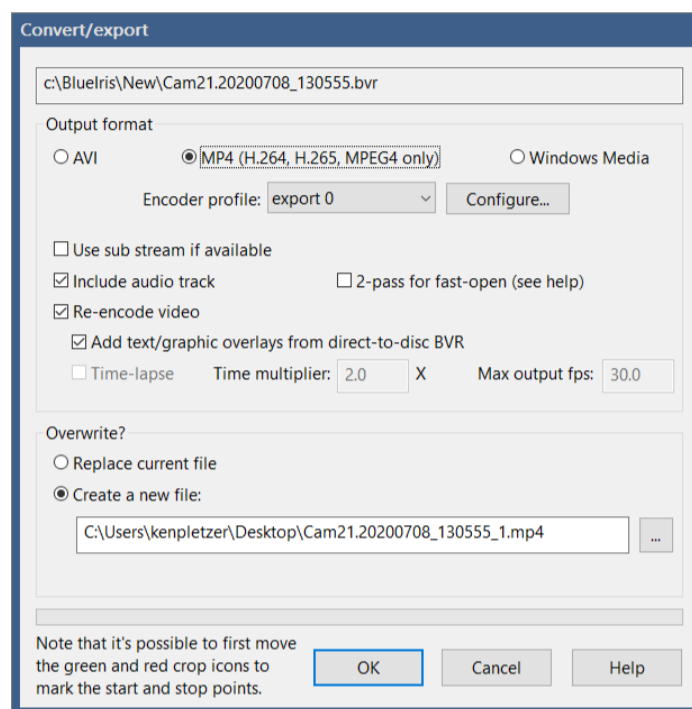
If audio is enabled, audio is played from the selected camera's video when the playback speed is 1x forward. **Click** a camera's video window to select that camera.

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 Trim/Export. Return to timeline playback by using the *Esc* key, or completely close the viewer window by using the X icon.

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:



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-disc 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-disc* 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
- if you desire to change the frame size or the video quality

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 to output.

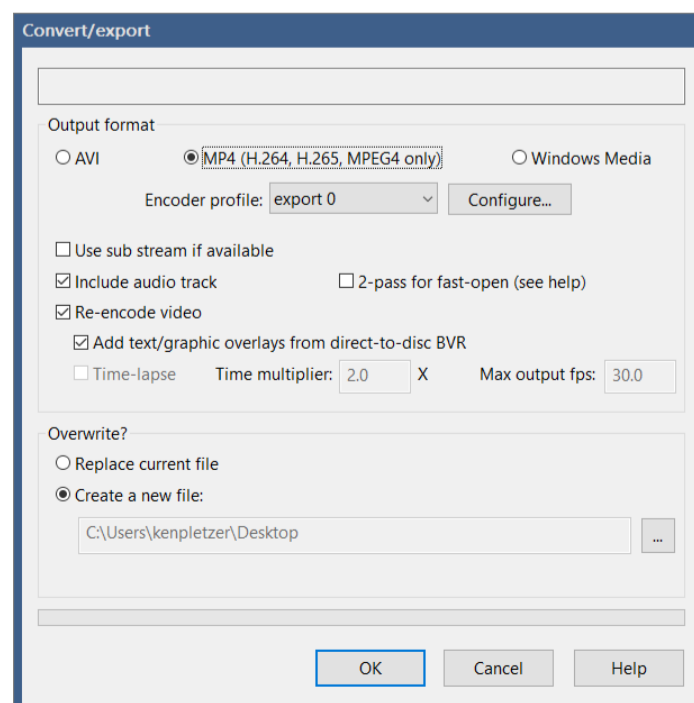
Output file

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 added to the database as a “new” item at the top of the list—it may be possible to re-sort the list to move it to the correct position in the timeline by running the database repair (right-click in the clips list).

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. This folder must *not* be a folder managed by the software.

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

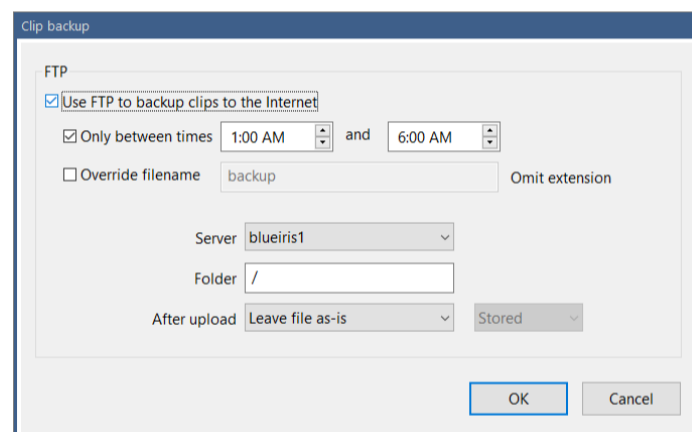
Only the *basic* install is required, without additional software it may attempt to install.

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.

GLOBAL VIEWER OPTIONS

These are found on the Other page in Settings.

Viewer

<input type="checkbox"/> Open viewer after manual snapshot	<input type="checkbox"/> Open viewer after manual movie record
<input checked="" type="checkbox"/> Automatically begin playback	At end of video: <input type="text" value="Stop"/>
<input checked="" type="checkbox"/> Skip dead-air during timeline playback	



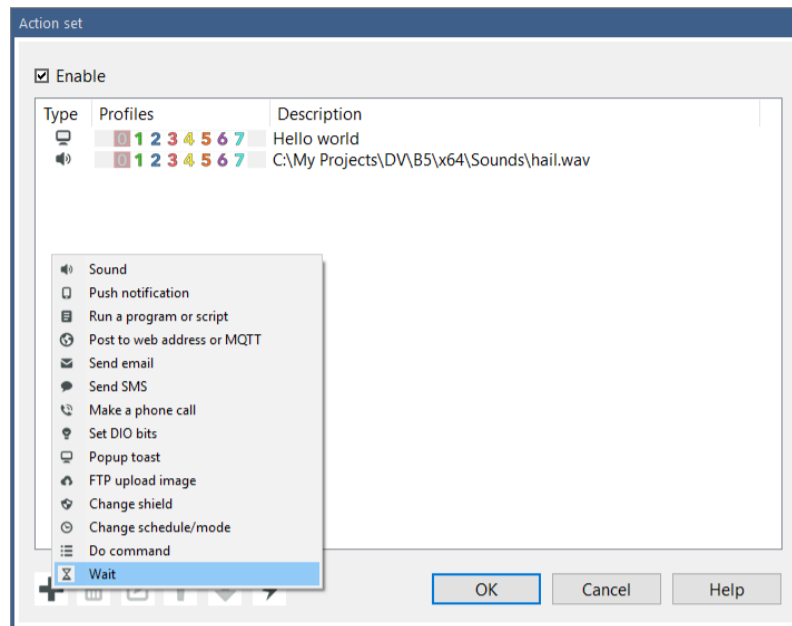
Upon use of either the Snapshot or Video buttons, the viewer window may be immediately opened.

You may select whether to **begin playback automatically**. 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.

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 by enabling this **Skip dead-air** option.

ALERTS AND ACTIONS

In response to a camera trigger or other alert, you may define a set of actions to be executed.

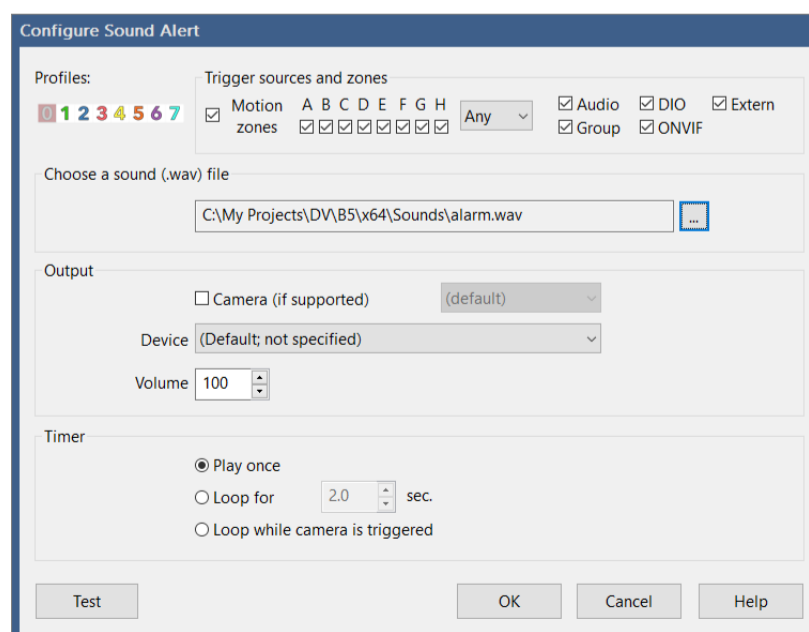


Action items on this list are executed in order from top to bottom. Alerts of different type may execute simultaneously however. That is, push notifications, sounds, and emails execute in order, but these all have separate queues and threads.

The action set will be executed only if the Enable box is checked. Each action item also has an associated profile control, 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.

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.

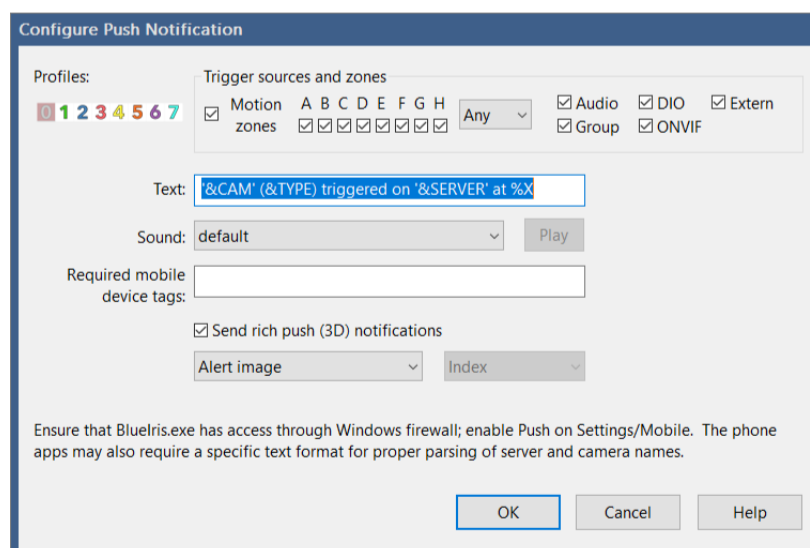
Use the volume setting to change the playback volume by percentage. A value of 100 is full volume.

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.



Although you may override the default text format, the apps are designed to parse the text in this format using the apostrophes and parentheses.

You may specify any of the 50+ sounds that have been pre-installed on both the PC software and the apps.

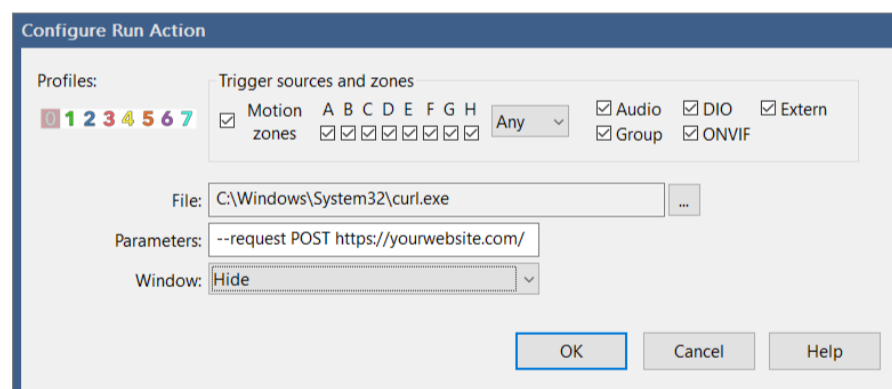
If you would like to send this notification to only a subset of connected mobile devices, you may specify one or more “tags.” Separate multiple tags with semicolons. A mobile device must have any one of the specified tags in order to receive the alert. Please see the Mobile devices tab in Settings.

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.

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 SCRIPT

You may select any executable (generally .EXE) or batch (Windows .BAT script) file to be executed.



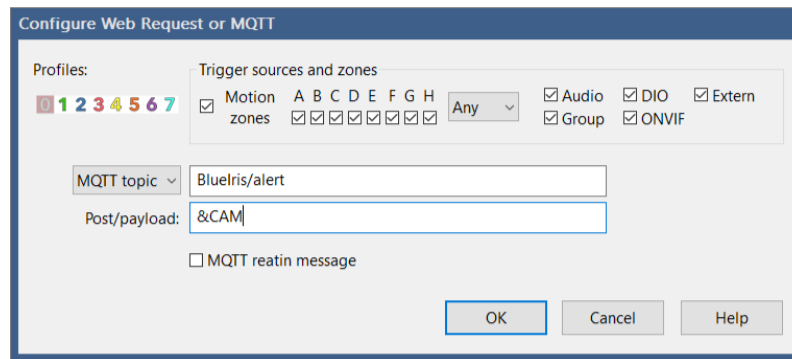
Parameters may be used as required by the file that you specify. For example, you may send the camera’s short name to a script by specifying &CAM.

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.

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.



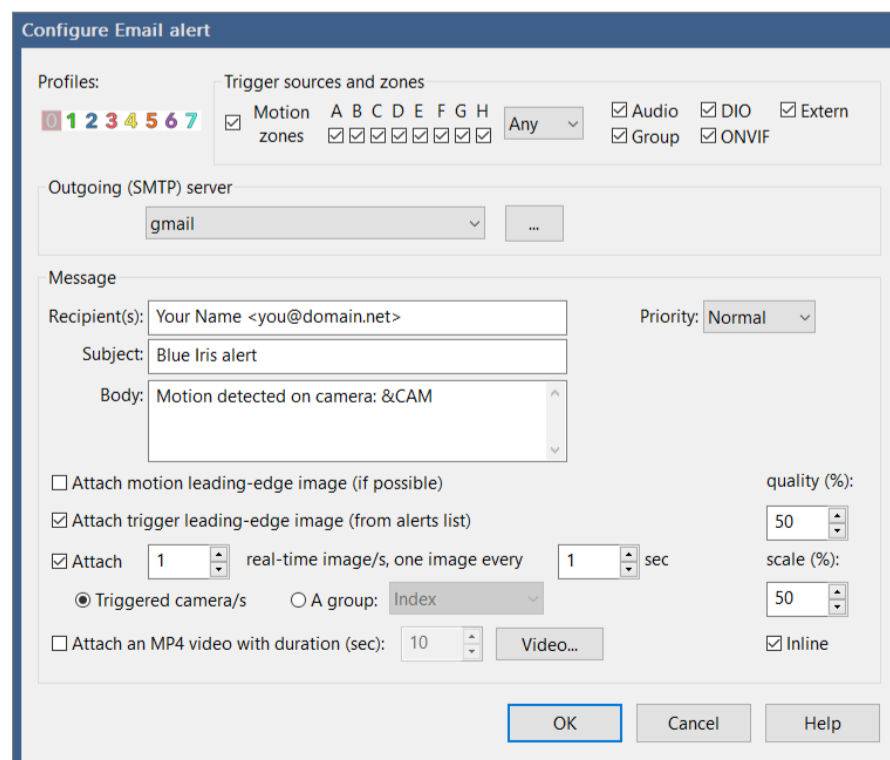
For HTTP or HTTPS requests, you must omit the `http://` or `https://` in the address box. HTTP GET semantics will be used if the post/payload box is empty, otherwise POST semantics will be used.

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.

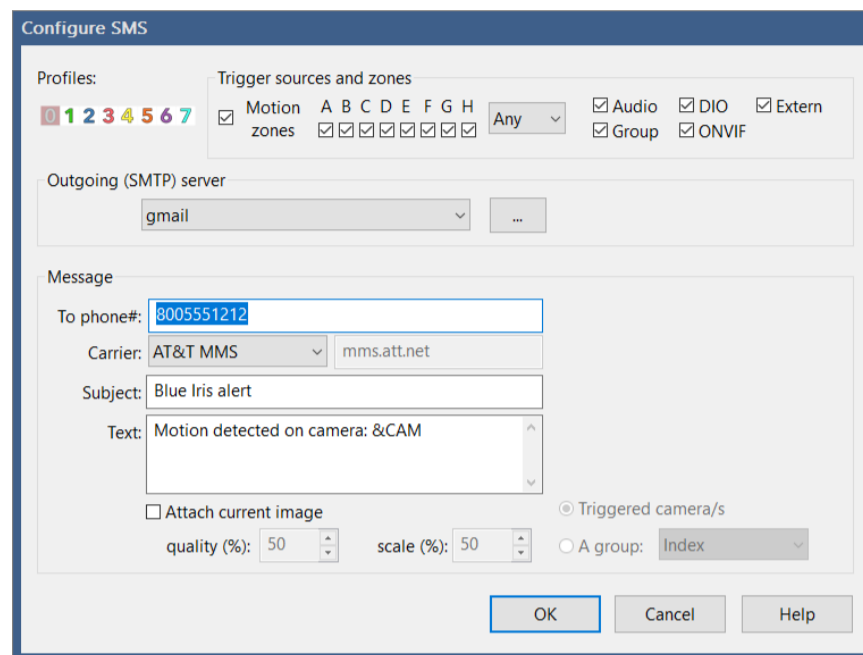
In addition to motion leading-edge and trigger leading-edge (alert) images, you may specify a number of additional real-time images, each spaced by a number of seconds.

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.

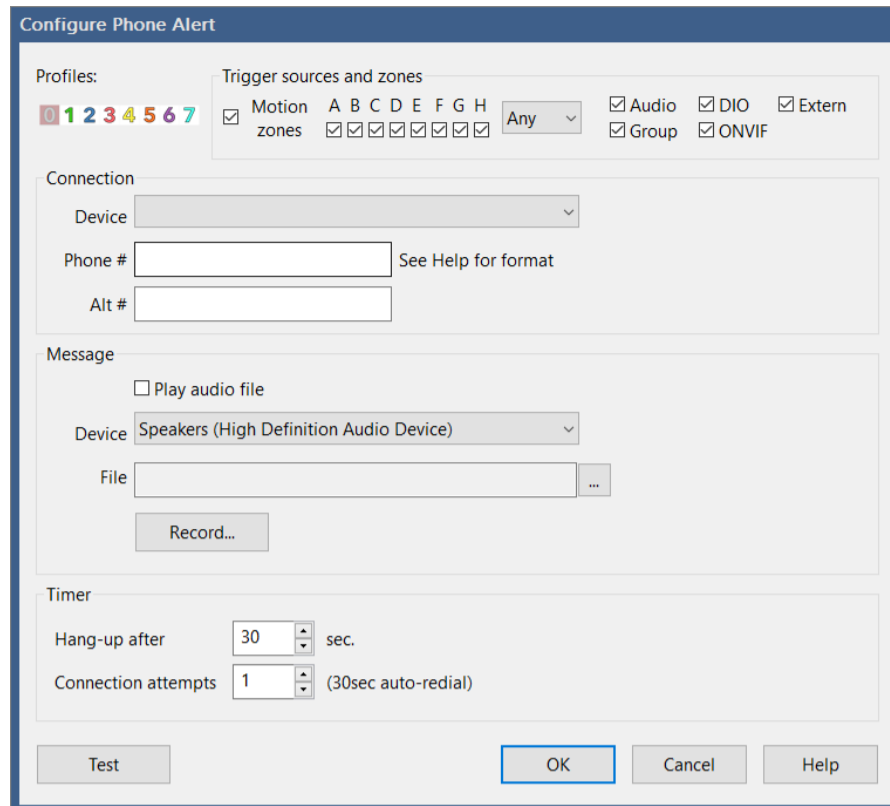
The email that is sent goes to (your phone number)@(your carrier's gateway). Using any other email client, you may test this outside of Blue Iris to verify function and compatibility. Many popular carriers are preconfigured for you, however if your carrier is not listed, you may select "other" and manually 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.

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.

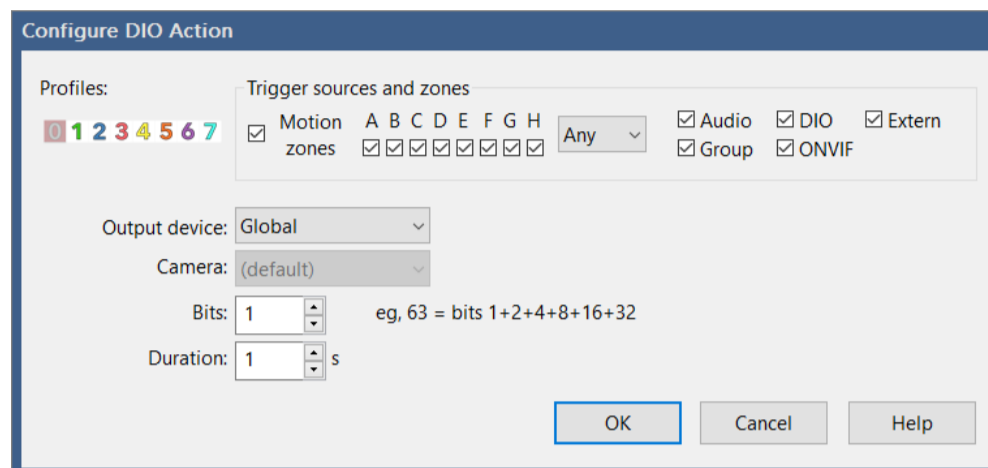
The device specified is for your sound hardware which will have a cable (internal to the PC) running from the sound card to the modem.

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.



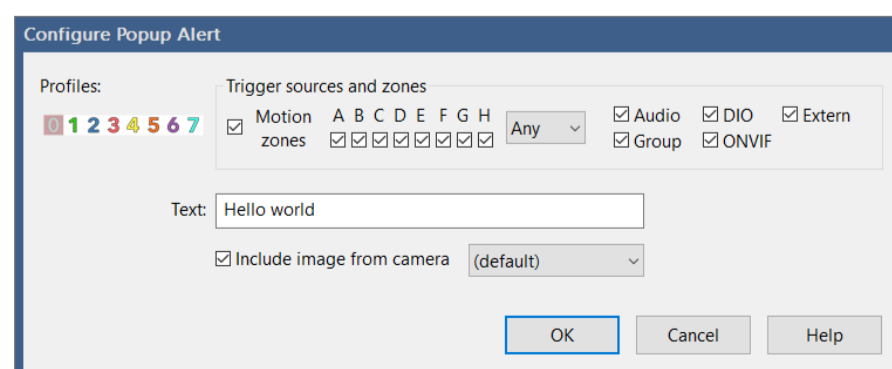
The output device may be set to Global or Camera. The Global DIO device is set on the DIO and IoT page in Settings. Many cameras however also offer DIO input/output terminals which may be used instead. Blue Iris must support the use of camera DIO based on its PTZ/control setting.

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.

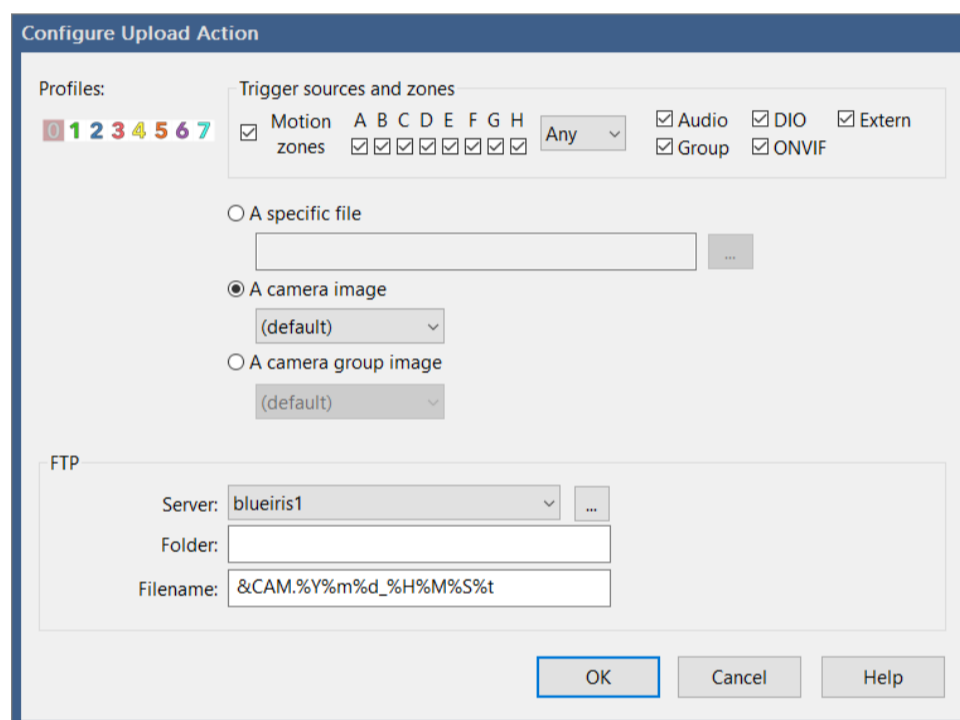


You may specify the text to be displayed along with the inclusion of a current camera image.

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.

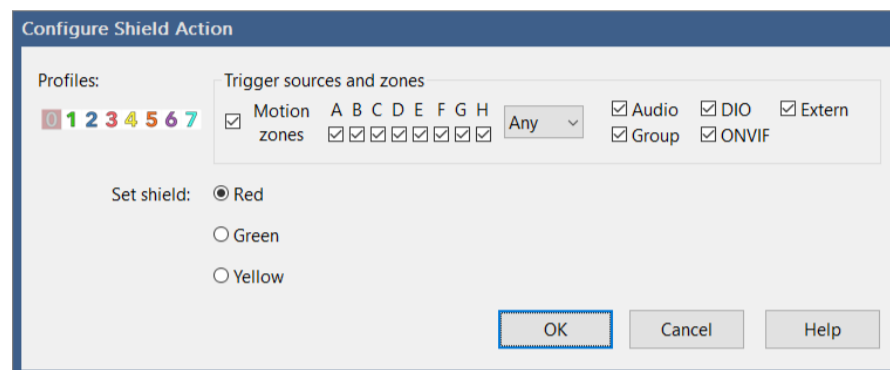


If a destination folder is not specified, the FTP server’s default folder is used. If the folder specified here begins with a / (forward slash), this is considered a root or absolute folder. Otherwise, the folder is appended to the server’s default folder.

Please see the chapter on Email and FTP servers for more information on configuration of the FTP server.

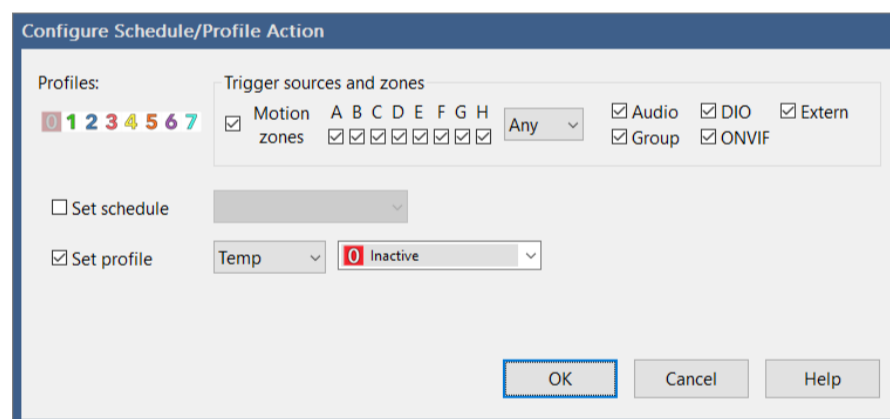
CHANGE SHIELD

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

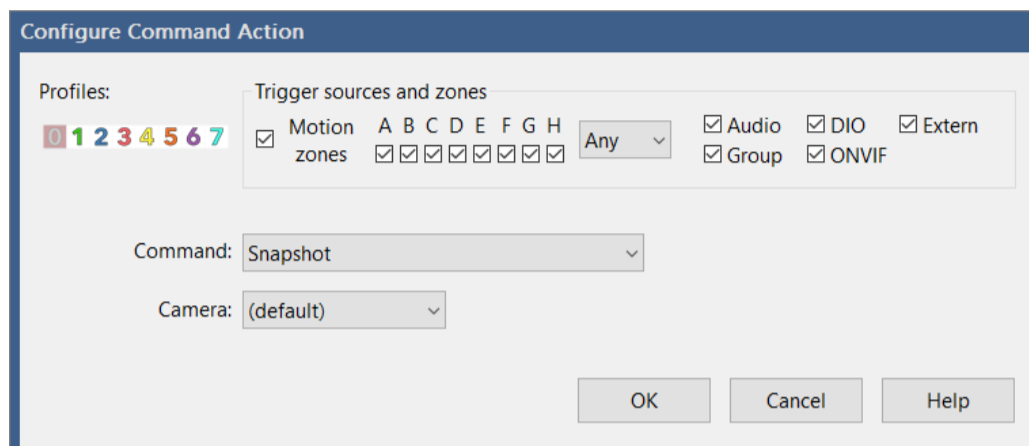
The current schedule and profile are also displayed at the top of the main window UI alongside the shield icon. Please see the chapter on Schedule and Profiles for descriptions of these settings.



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.

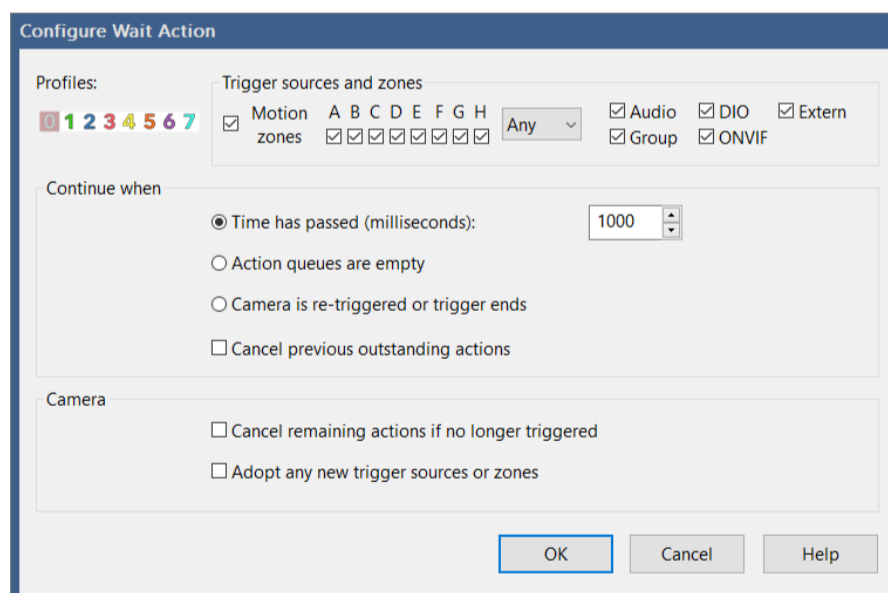
DO COMMAND

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.



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 milliseconds or 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 yet 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.

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	
&ALERT_DB	The DB record locator for the most recent alert image for the camera.
&ALERT_PATH	The path to the most recent alert image on the camera. Note that alert images are not saved to disc by default; this is controlled with a setting on the Trigger page in camera settings.
&CAM	Camera's short name
&FILE	The path to the currently recording clip on the camera
&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)
%f	Frames/second (FPS) for camera
%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)
%k	Kilobytes/second (kB/s) for camera
%m	Month as decimal number (01 - 12)
%M	Minute as decimal number (00 - 59)

Macro	
%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)
%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

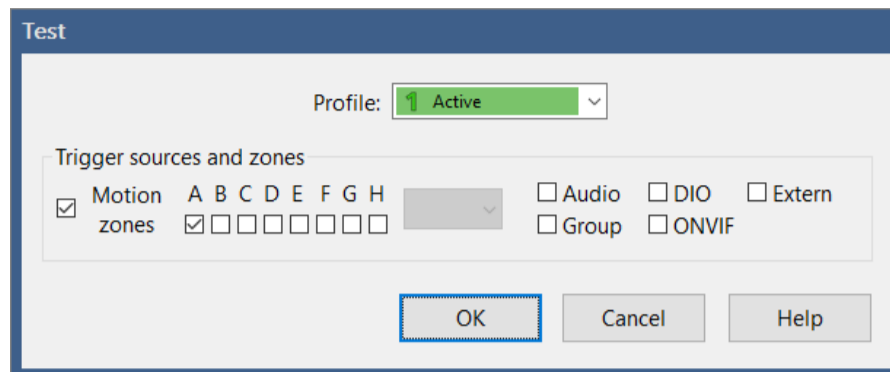
For time zone correction in a text object overlay, add the special sequence {+n} to the beginning of the string, where n is a number 1-23, and the sign is either + or -. For example, a text overlay of {+3}%c will display the time 3 hours ahead of local time.

Additional special macros

Macro	
%0-99	A numbered macro on the Macros page in Settings
%f	The camera's current FPS
%k	The camera's current bit rate in kbps
%n	The camera's most recent PTZ preset position
%P	The camera's current profile number and description, such as 1: Work hours
%D	The current day's ordinal indication, either st, nd, rd, or th, as in the 1st, 2nd, 3rd, 4th.
%t	The current time's millisecond value, 0-999

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.

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.

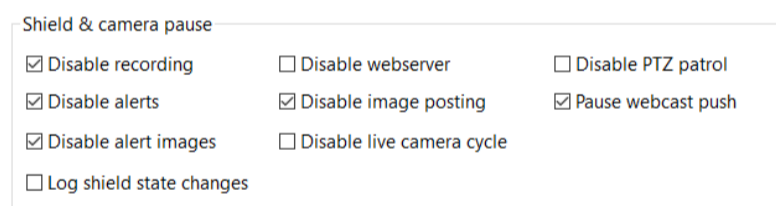



THE SHIELD

 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.

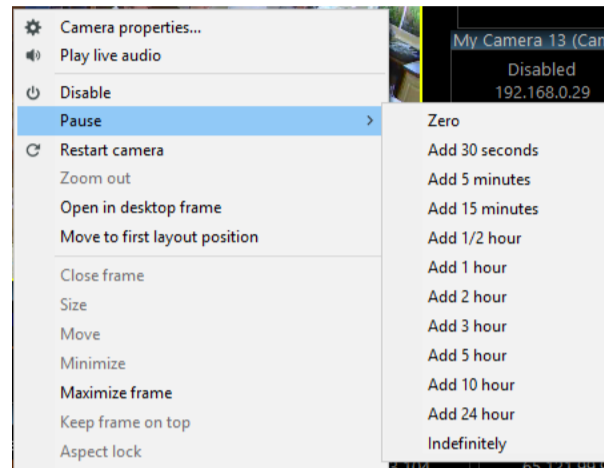
CAMERA PAUSE

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.

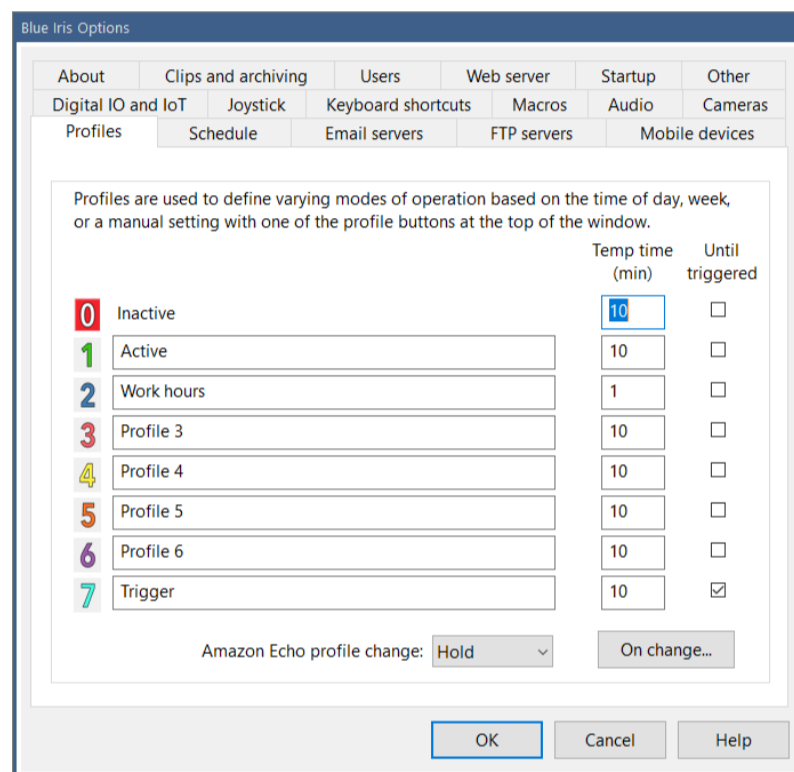
The original use for profiles in Blue Iris version 1 was to allow you to configure the motion detection differently based on the time of day. Generally at night, cameras operate in black and white, and trigger much differently than they do during the day. So in another example, you might use profile 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 title the remaining profiles 1-7 on the Profiles page in Settings:



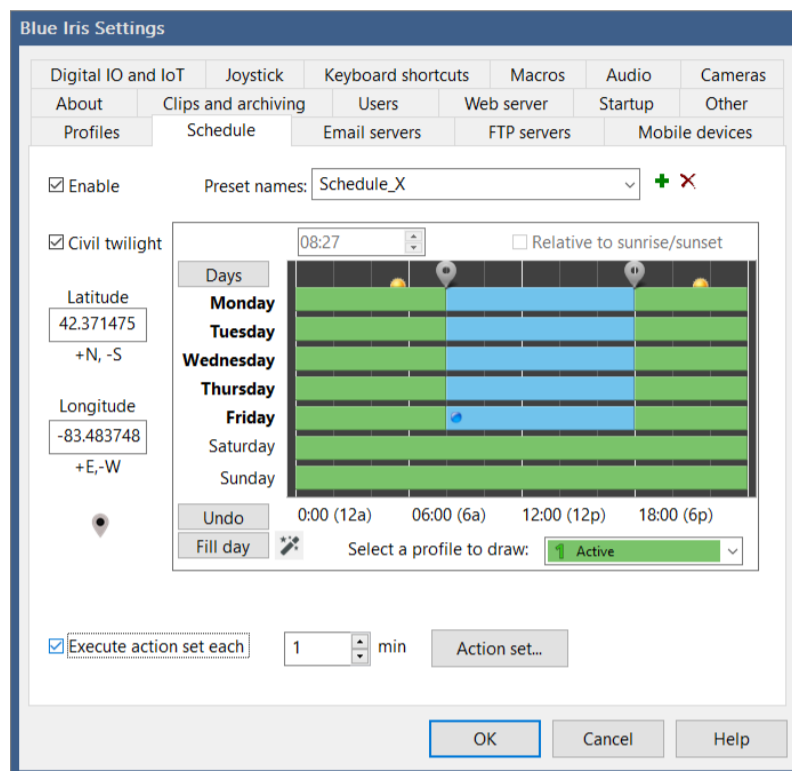
Each profile may be assigned a time to remain temporarily active before returning to the normally active profile (as defined by a schedule, see below). You may select that the temporary state is immediately cancelled when a camera is triggered.

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.

Execute action set

You may configure an action set to be executed 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.

RUN, HOLD AND TEMPORARY PROFILES

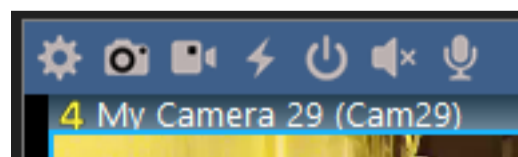
- ▶ When a schedule is running normally and the active profile is set automatically, this is called the “run” state and a green play icon is shown.
- ▬▬ When the active profile is overridden in some way, this is considered a temporary or transient state and a yellow pause icon is shown. The active profile 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.



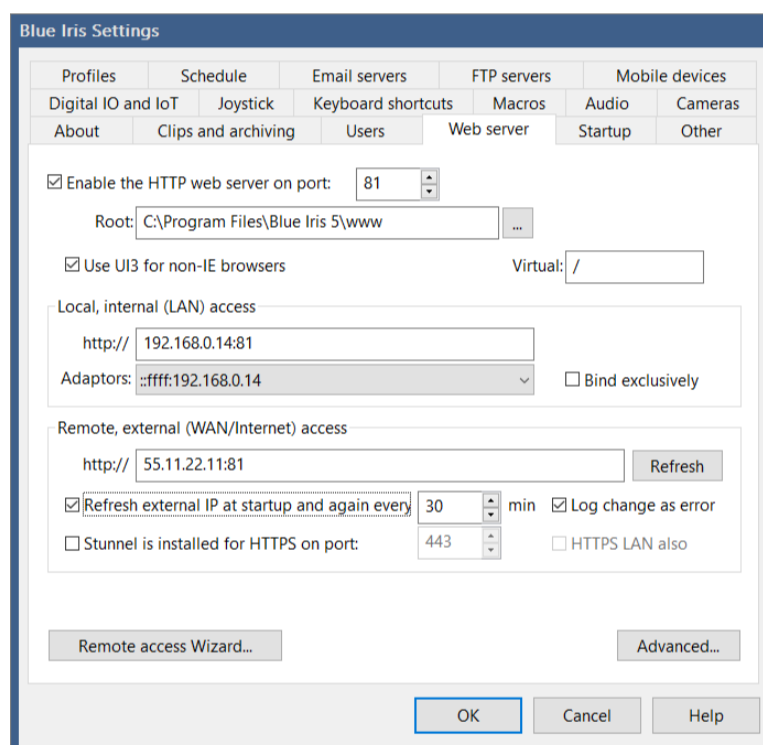
When a camera’s effective active profile differs from the global profile, the active profile number will be shown in the camera’s header.

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 (although the image shown here has had this changed to 8081). 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, 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 Messages page in Status, possibly with “error” status so that it can be pushed to you using the Status Alerts in Messages.

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. This 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*.

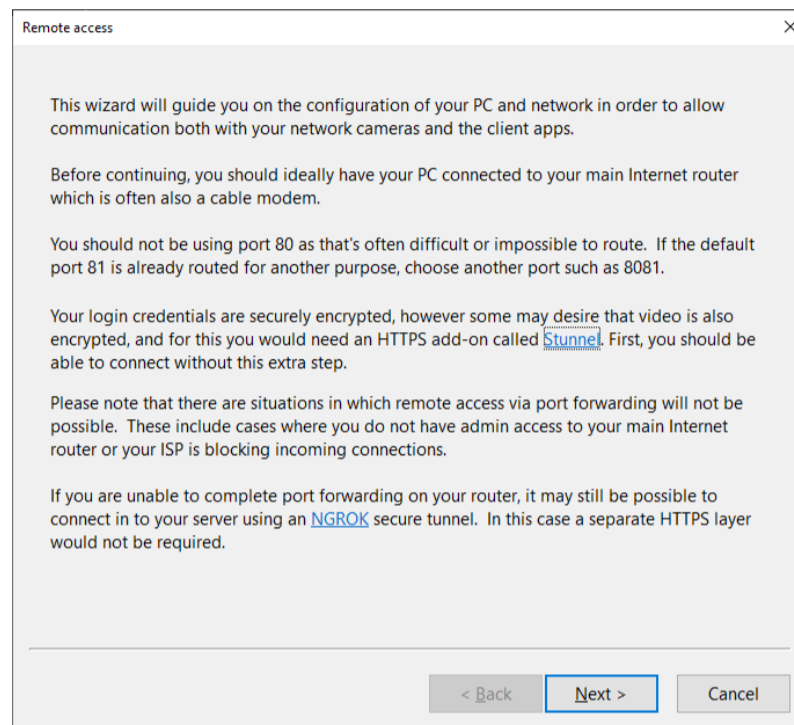
A secure tunnel is what something like a Nest thermostat or Rachio sprinkler system uses to provide you access to your home devices without configuring any of your router or other network hardware—the local devices and your remote clients (phone apps) “meet up” at a designated website (typically operated 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

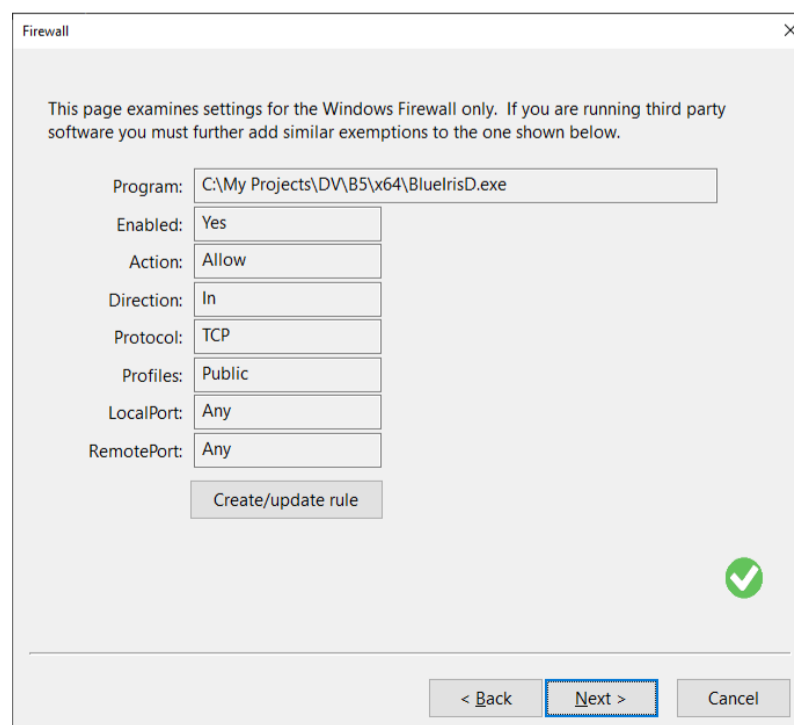
The Remote Access Wizard covers many topics which must be addressed for remote access regardless of the type of connection you will be making. It is accessed either from the main menu or from a button on the Web server page in Settings.

Introduction



Firewall and antivirus

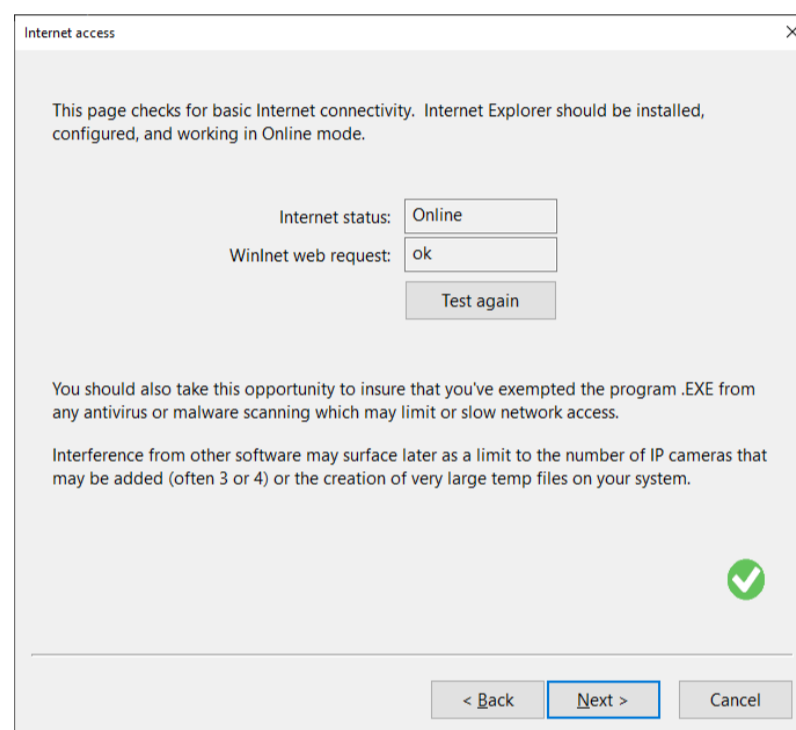
The first step is to ensure there is no local firewall or antivirus software restricting access to the Blue Iris server port. If you do not see a green check mark, use the **Create/update rule** button. When you first launched Blue Iris, you would have been queried by the operating system on whether 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.

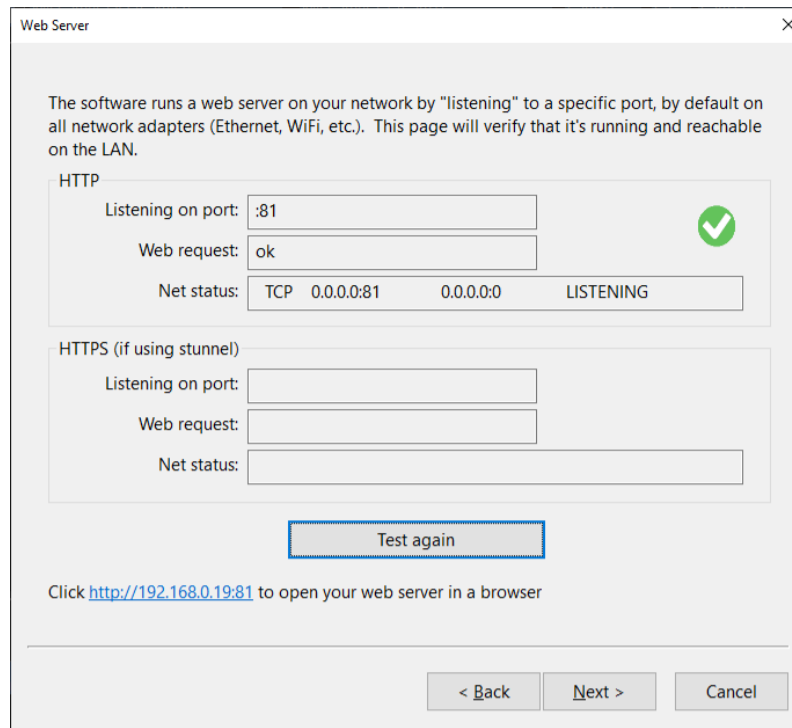
Internet access

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

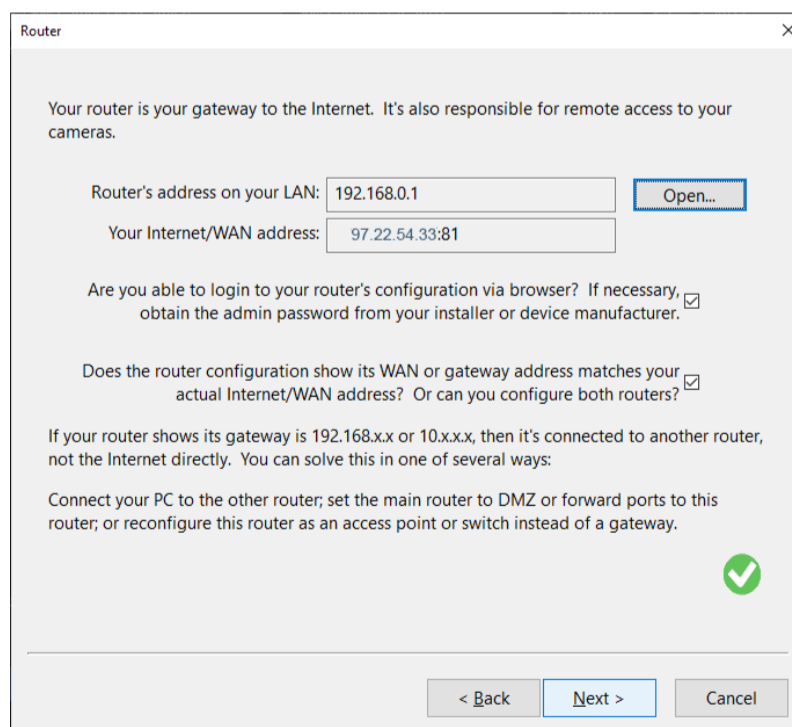
This step verifies that the Blue Iris service is actually running (listening) on the specified port. If all steps are successful to this point, you should have local access to your Blue Iris server from any other PC on the LAN (same home or office network). If you are unable to access the Blue Iris server 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 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.”

Port Forwarding

Port forwarding opens an external port on your network. The router will send requests on this port to your PC running this software.

Router's address on your LAN: 192.168.0.1 Open...

Port forwarding rule

Port: 81 LAN address: 192.168.0.19
Protocol: TCP LAN port: 81

Use UPnP to automatically add this rule

Can you enable UPnP in your router and then use it to add this rule or otherwise manually add the port forwarding rule?

For more on port forwarding, see portforward.com

< Back Next > Cancel

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:

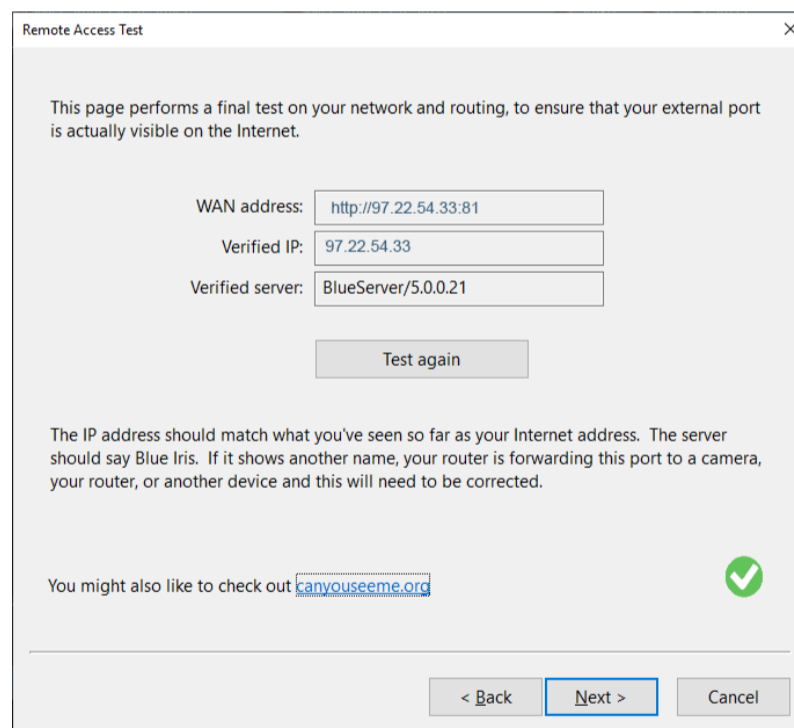
Internet —> Router 1 —> Router 2 —> Blue Iris PC
66.22.11.11 —> 192.168.0.1 —> 192.168.0.2 —> 192.168.1.6
(and 192.168.1.1)

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. instead of .0. 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.

Client app login

If you have successfully completed all prior steps, you should now be able to connect using one of the client apps with the following settings:

Lookup IPs by license: NDEC0BK3NE


LAN: http://
192.168.0.19:81

WAN: http://
97.22.54.33:81

Username: a

Password: Add admin now

If you have not yet created a login for yourself on Options/Users, you may do so now by completing these fields.



< Back Next > Cancel

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 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.

Dynamic IP

Unless you pay extra to your ISP for a Static address, your external IP address will eventually change. This may be only when your modem is reset, but it could happen at any time or not for years.

One way around this is to use a name hosting service such as no-ip.com. Software is installed onto your PC or router which notifies the service when your IP changes. You then use a link to their website instead of an IP address.

Blue Iris does not need to know you are using a name hosting service. You will always still have an IP address--the name is just an alias.

Your Blue Iris license also includes a pseudo-name hosting service, enabled with a checkbox on the Options page. Access these addresses remotely using blueiris.pro/go?XXXXXXXXXX where the first 5 and last 5 digits of your license key are used.

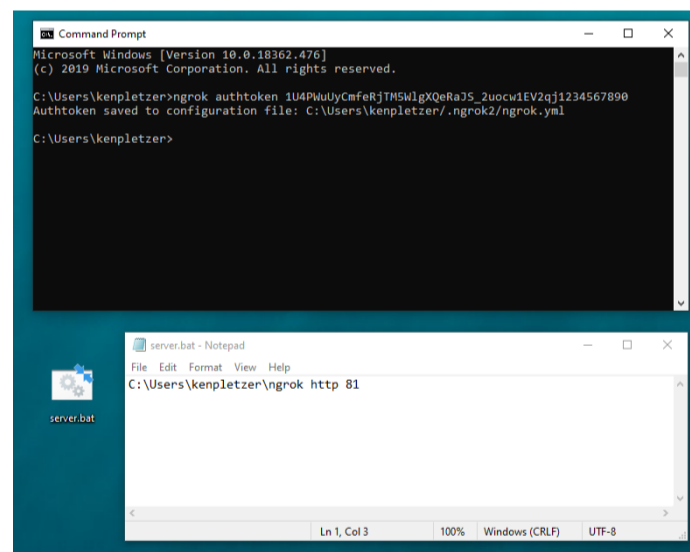
< Back Finish Cancel

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.

NGROK

If port forwarding is not (easily) configurable, you may instead choose to open a secure tunnel using the NGROK software. Here’s how to configure it:

- Create a free account at <https://ngrok.com/>
- Download and unzip the NGROK.exe to your Windows user folder (such as C:\users\kenpletzer for this example).
- Run CMD from the Windows start bar, which should open to your users folder.
- Highlight and copy the “connect your account” command from the NGROK page. Leave off the ./ at the beginning, that’s just for UNIX.



- You should see a similar message as shown here if you have entered the command correctly.
- 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.
- 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.
- Close and save the file.

- When you then double click this file, it will run NGROK in a command window:

```
C:\Users\kenpletzer\Desktop\ngrok.exe - ngrok http 81
ngrok by @inconshreveable (Ctrl+C to quit)

Session Status      online
Account             Ken Pletzer (Plan: Free)
Version             2.3.35
Region             United States (us)
Web Interface       http://127.0.0.1:4040
Forwarding          http://8a62aa39.ngrok.io -> http://localhost:81
                   https://8a62aa39.ngrok.io -> http://localhost:81

Connections        ttl   opn   rt1   rt5   p50   p90
                   51    1     0.50  0.15  0.32  0.36

HTTP Requests
-----
GET /video/Index/2.0      200 OK
POST /json                200 OK
POST /json                200 OK
POST /json                200 OK
GET /ui3/ui3-local-overrides.js 404 Not Found
GET /ui3/ui3-local-overrides.css 404 Not Found
GET /ui3.htm              200 OK
POST /json                200 OK
POST /json                200 OK
POST /json                200 OK
```

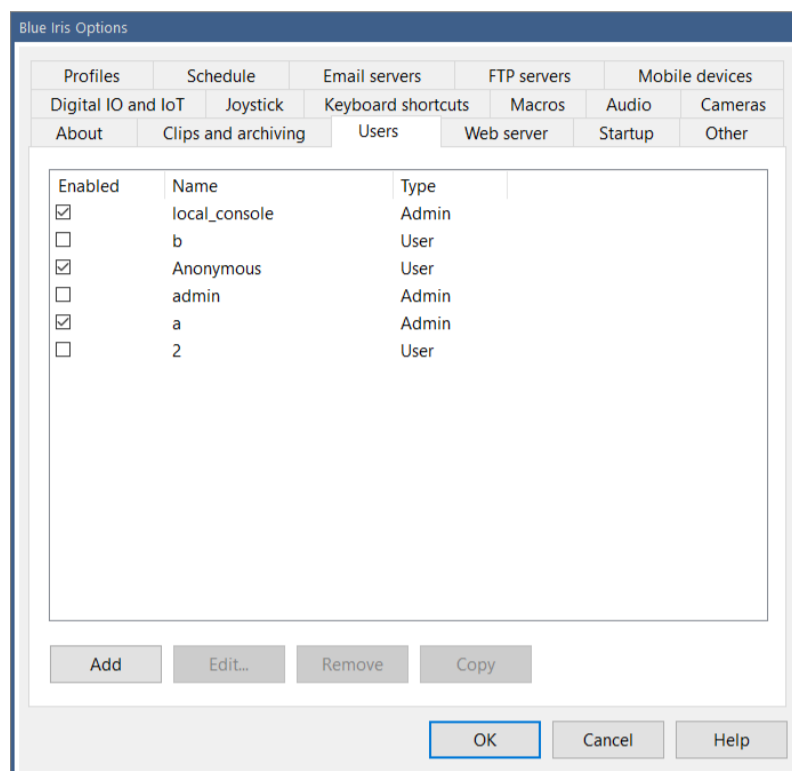
- Your remote server address is then visible on this window, here designated with a red arrow. This is the address you can use to access your Blue Iris server from the Internet or phone app.
- If you receive an error remotely stating “successfully tunneled to your NGROK client, but the client failed 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.
- 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

- There are many ways to automatically run this when you login. One way is to run shell:startup and then add the .bat file to this folder.

USERS AND CONNECTIONS

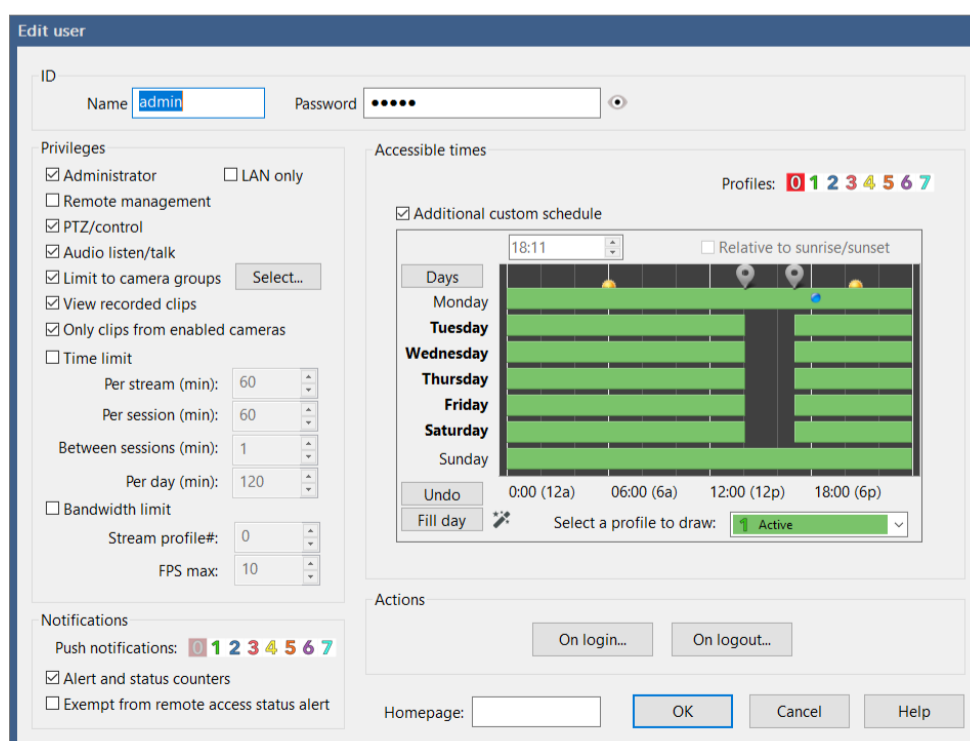
Potential users of your Blue Iris server are managed on the Users page in Settings.



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 (a password) on either a LAN or WAN connection. This is covered in the Advanced topic below.

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. **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 **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 accepts the connections and then forwards these to Blue Iris.

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 **Limit to camera groups** setting prevents users from accessing restricted cameras. Camera groups are set on their General pages in Camera Settings. Each camera may be a member of multiple groups for this purpose. A camera group is deleted only when all cameras are removed from that group. Remote users have access only to recorded video which was recorded from an accessible camera.

Unselect the **View recorded clips** option to prevent access to any recorded video at all. You may also restrict the user to video associated with enabled cameras only.

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.

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.

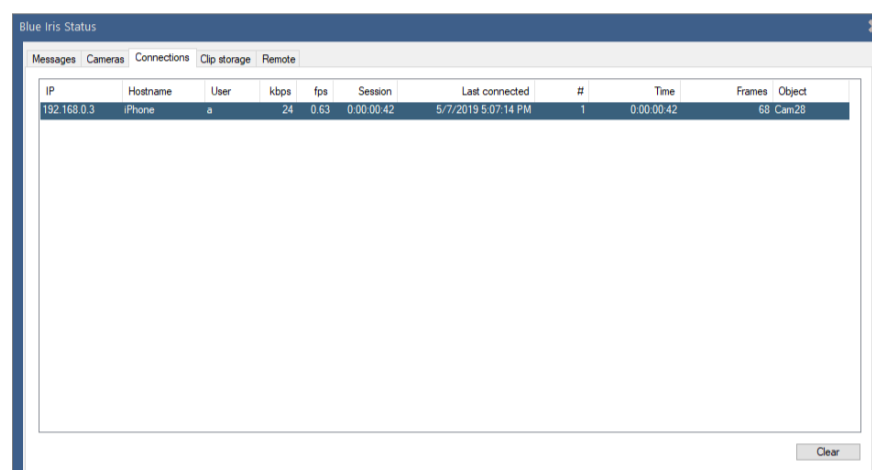
With an option on the Status Alerts page from the Messages page in Status, notifications may be sent when users login remotely. However you may desire to defeat this behavior for specific users, and that may be done so here with a checkbox.

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.



The screenshot shows the 'Connections' tab in the Blue Iris Status application. The table displays the following data:

IP	Hostname	User	kbps	fps	Session	Last connected	#	Time	Frames	Object
192.168.0.3	iPhone	a	24	0.63	0:00:00.42	5/7/2019 5:07:14 PM	1	0:00:00.42	68	Cam28

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.

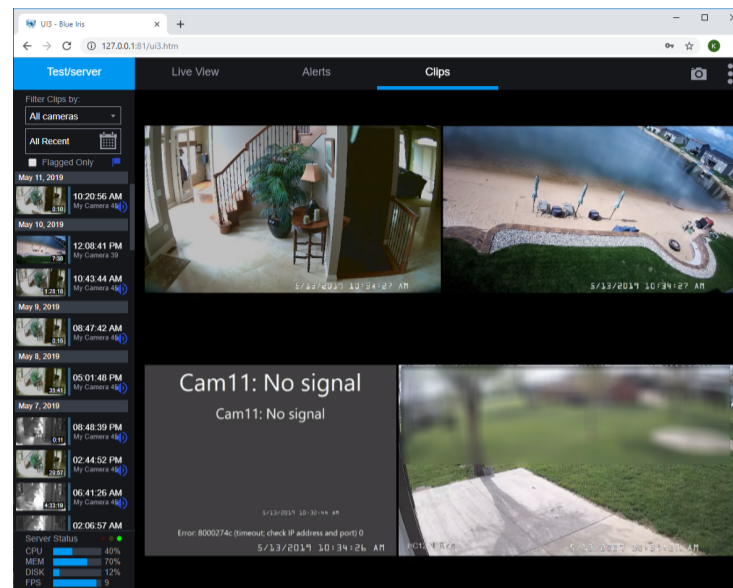
Note that a connection does not become a *login* until the connection has been authenticated (logged on with a valid user and password).

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.

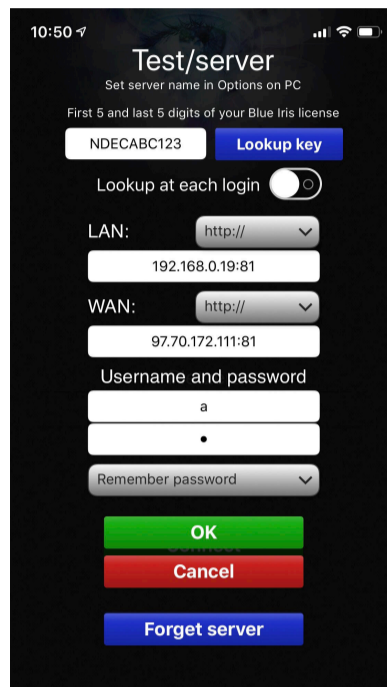


This client works best with a modern HTML5 browser such as Chrome. This interface was designed and built by a third party however—so separate help and support may be available via the “three dot” menu button at the top/right of the window.

You may choose to use the legacy Blue Iris server pages by unchecking the option on the Web server page in Settings.

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:

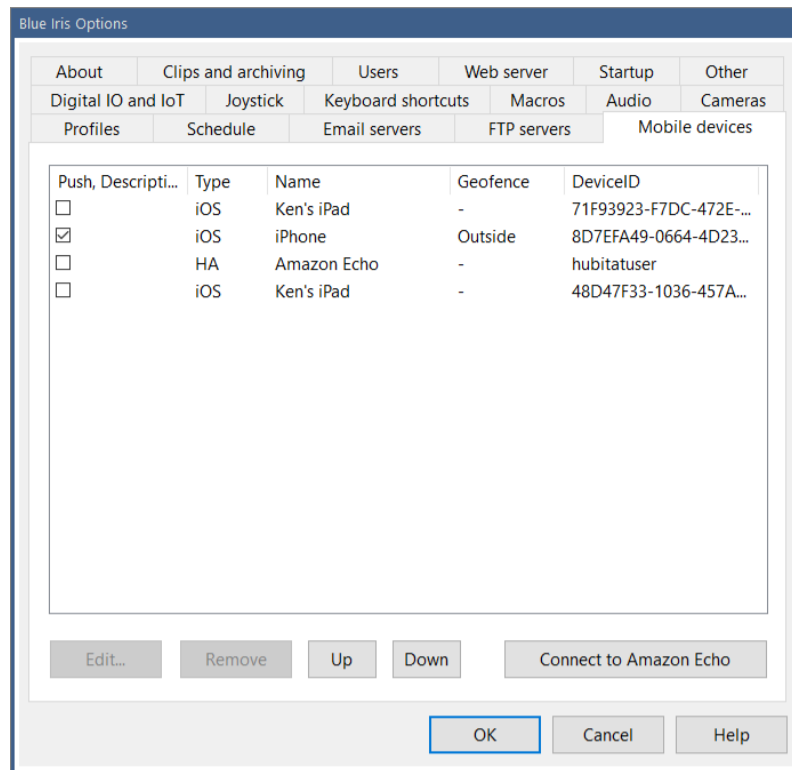


You may use part of your license key to “look up” your server addresses instead of entering them manually. If your WAN address changes frequently, you may wish to use the option to look up the address each time that you use the app. Using the option to look up the addresses requires use of the Blue Iris 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*.

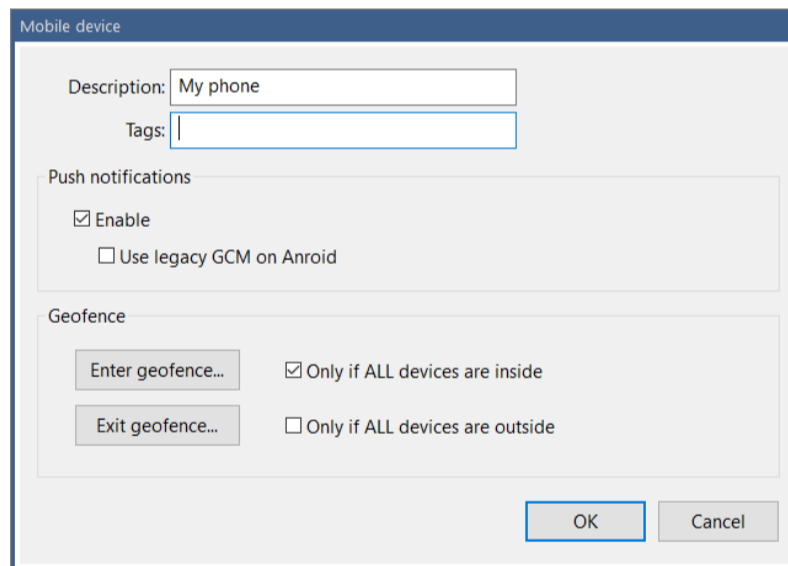
The app will attempt both the LAN and WAN addresses to make a connection, with preference for the LAN address (used when you are at home or in the office). While connected using the WAN address, the app occasionally attempts to revert to the LAN address if possible.

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 whether 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 are also inside or outside of the fence.

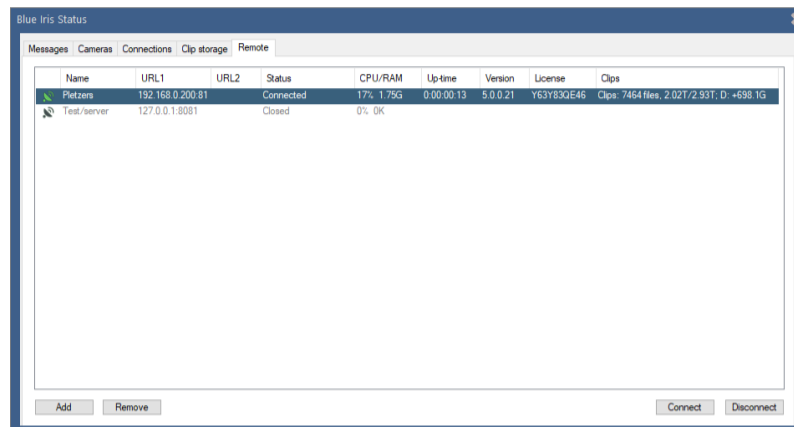
There are a number of moving parts when using geofencing, and many of them are device-specific. The device's location must be accurate via GPS and the phone OS must "wake" the app in order to notify the server. Often times battery or power-saving features on the device will limit geofence effectiveness. Further, the app must be able to use 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.

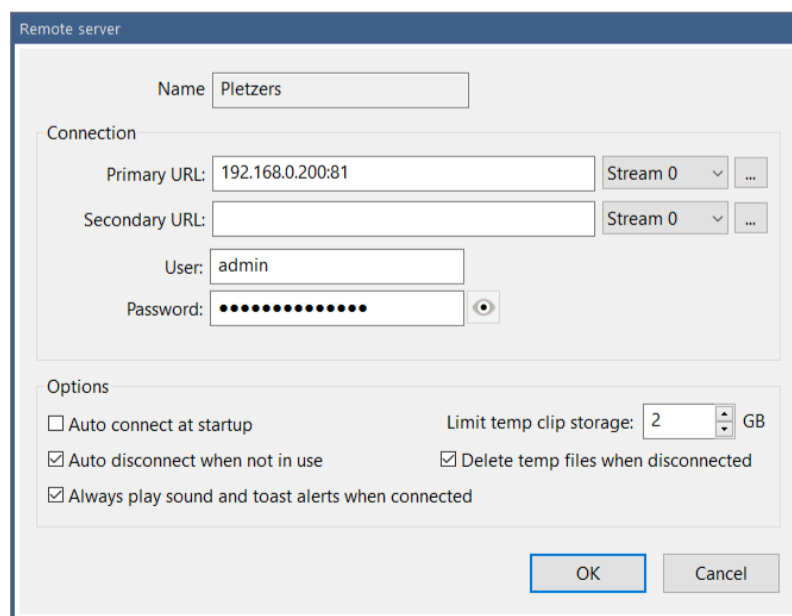
A list of remote systems is maintained on the Remote page in Status.



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.

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.

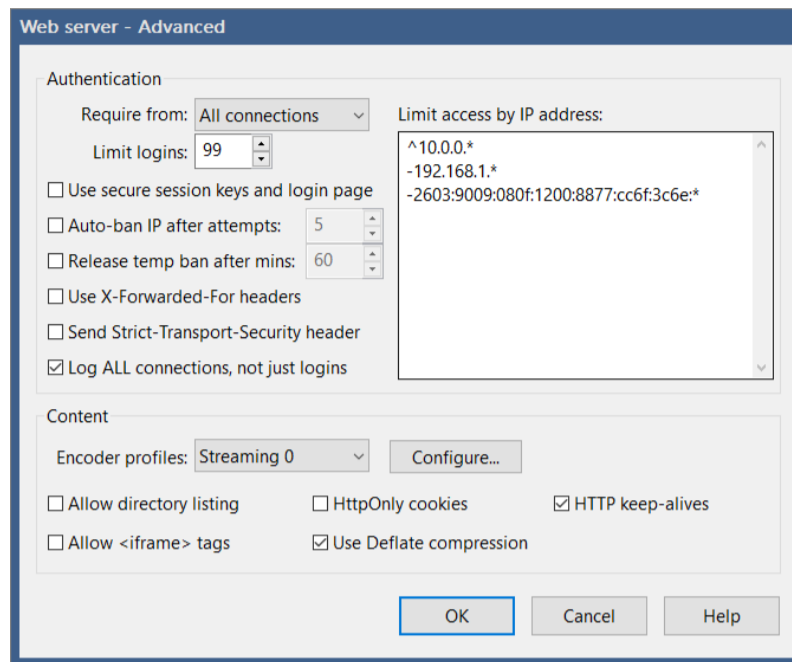
The Blue Iris access model is called *on-premises*. Your video and authentication is not reliant on outside cloud services. Because your video is stored locally, concerns of unauthorized access are limited to physical access to your PC or credentials.

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.

OTHER ADVANCED WEB SERVER TOPICS

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, all connections may appear to be coming locally from the LAN as Stunnel is actually receiving the remote connections and forwarding these 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 un-checking **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 the URL 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 separated by semicolons. The first character defines the function:

+ allow this address

- deny this address

^ allow this address with *admin* privileges (**use caution here**)

An address is an IPv6 address or an IP4 address with 4 integers 0-255 separated by periods. As a wildcard, an asterisk (*) may be used at the end of an entry.

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 this 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 users share your system resources, so it may become necessary to limit these connections to maintain system stability.

By default only authentication connections are logged to the Messages 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.

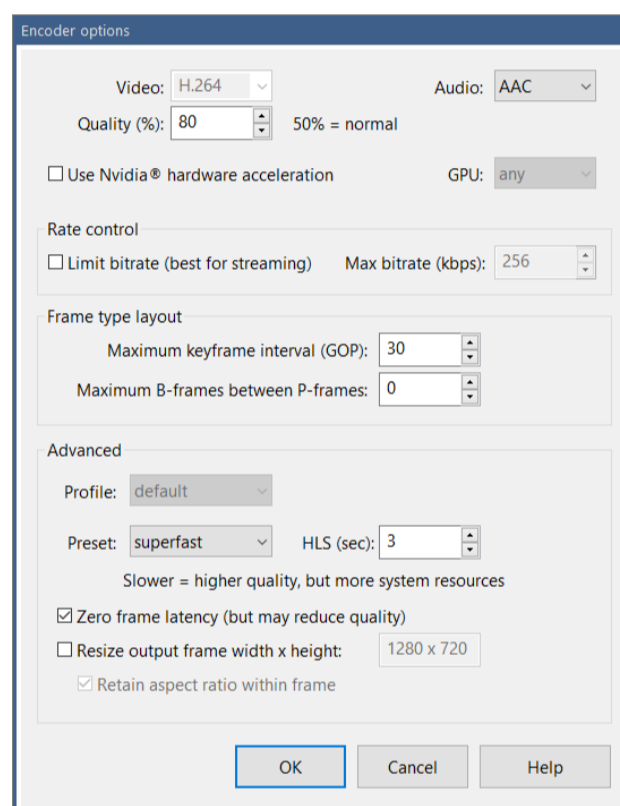
The options for X-Forwarded-For and Strict-Transport-Security headers were added for users in enterprise environments requiring specific HTTP security features. You may read about them here:

<https://en.wikipedia.org/wiki/X-Forwarded-For>

https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security

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 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

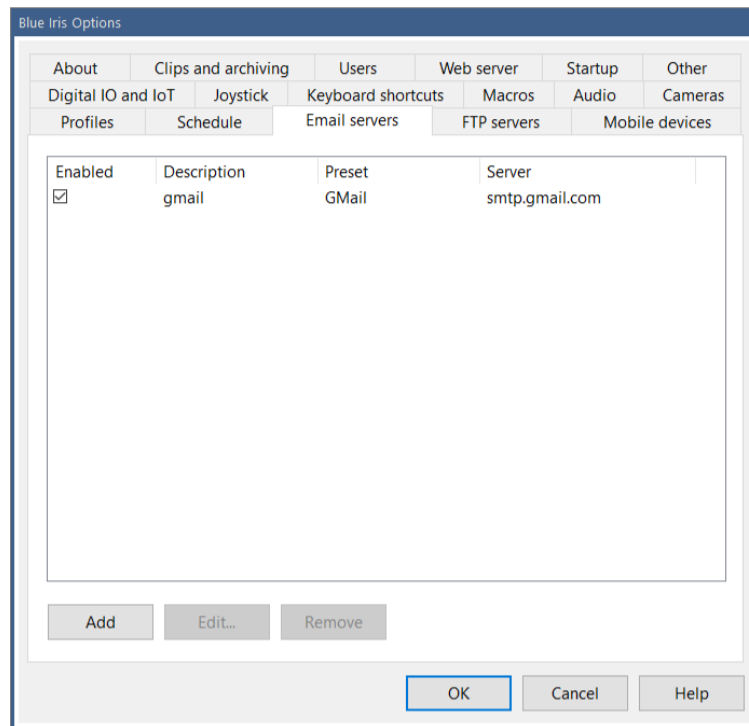
The **Allow directory listing** option should be disabled for all but very specialized cases. This will allow a remote user to see and directly download all files in managed folders such as /clips/ and /www/. Add &match=*x* to filter the results line-by-line using a case-insensitive pattern search—*x* may contain * and ? wildcards.

EMAIL AND FTP SERVERS

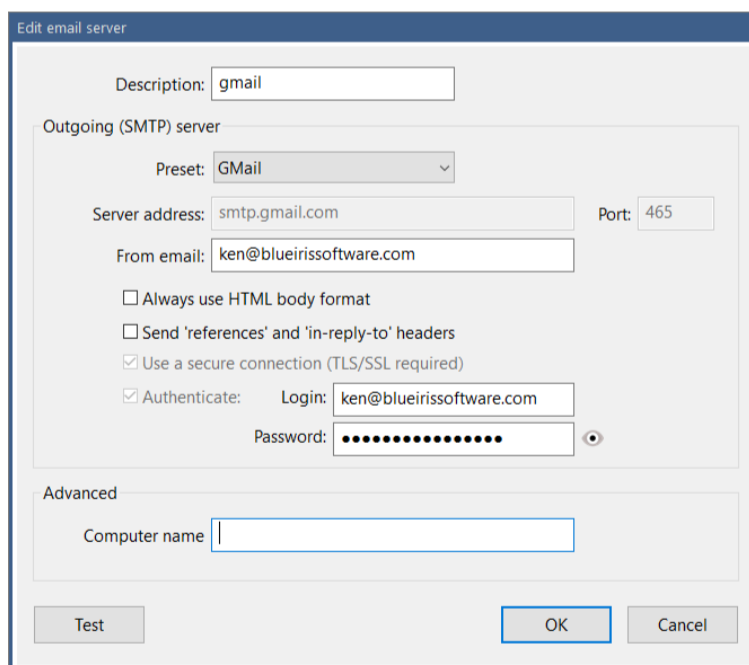
You may configure and test multiple Email and FTP server connections in Settings.

EMAIL

Email is used for alerts and notifications throughout the software.



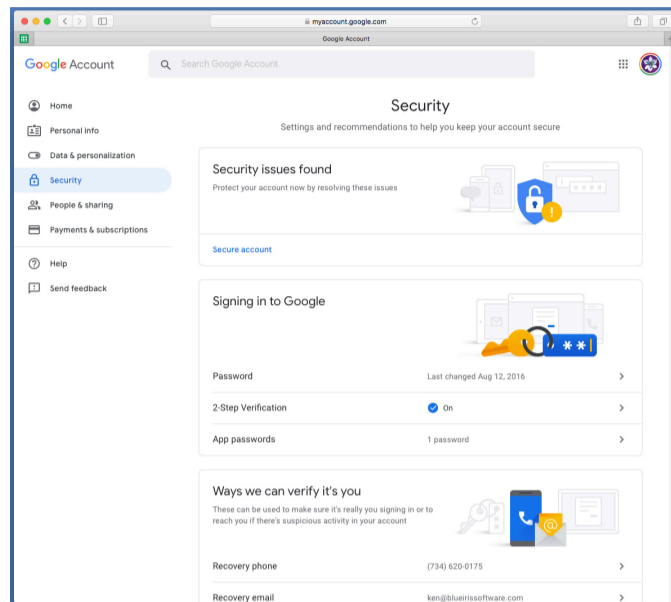
From this page, use the **Add** button to configure a new email server.



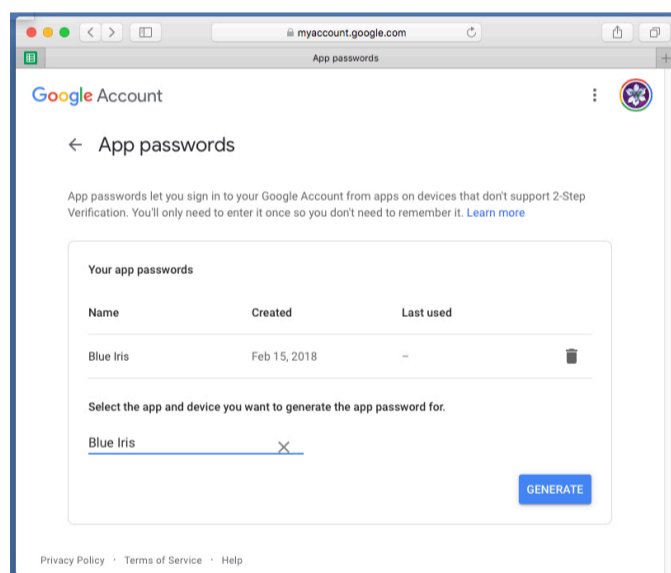
You may select from the limited list of presets, or obtain the server address and port from your email provider or ISP. Gmail is among the most commonly used email systems on the planet, so it will be used for demonstration here.

For Gmail and other systems which use 2-step authentication, you need to first generate an app-specific password for Blue Iris to use, as your normal email password will not work. There is no need to disable 2-step authentication.

Go to myaccount.google.com and select Security from the menu on the left.



Locate the App passwords link and click this.



Select to add an “other” app and name it Blue Iris and then click **Generate**. You will receive a 16 character password and instructions for its use.

Enter your full email address with @gmail.com as the **Login** in Blue Iris. Enter the newly generated password in the **Password** box. You’re now ready to use the **Test** button.

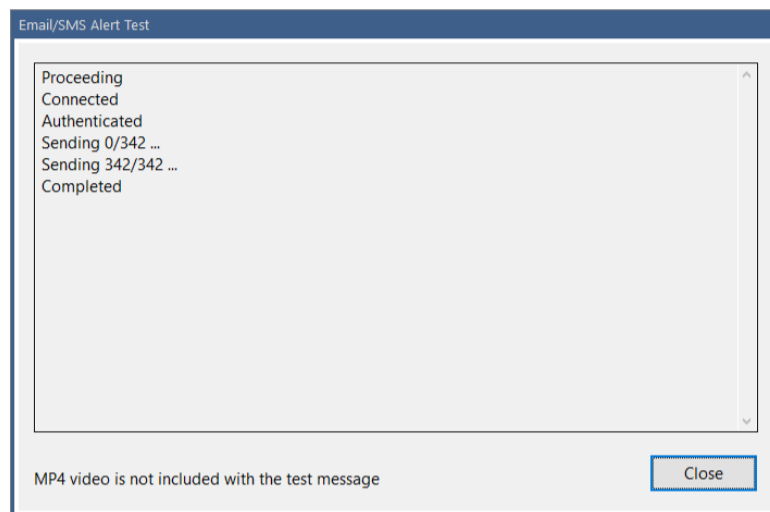
The **From** address will be used for all emails sent. If you require multiple from addresses, you may add the server multiple times with different descriptions.

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

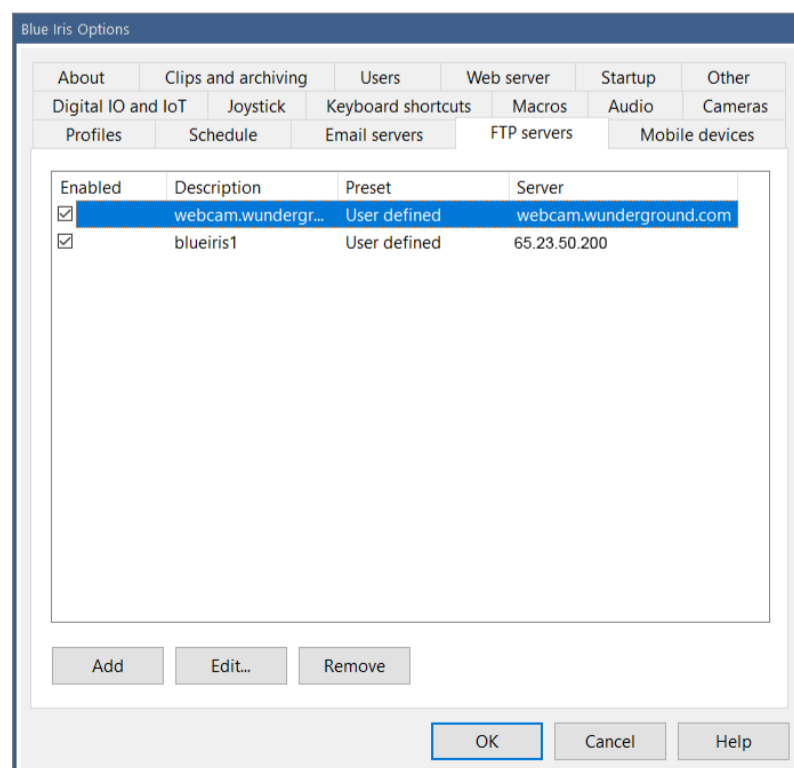
A short email is composed and sent both to and from the **From** address that you specified.



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.

The screenshot shows the 'Edit FTP server' dialog box. The 'Description' field is set to 'blueiris1'. Under the 'Connection' section, the 'Preset' is 'User defined', 'Server address' is '65.23.50.200', 'Port' is '21', 'Base folder' is '/temp/', 'Login' is 'Administrator', and 'Password' is masked. 'Idle disconnect' is set to 1 second and 'Max connections' is set to 1. In the 'Options' section, 'Passive transfer mode' is checked, and the 'Port range' is 1024-49151. The log area shows a successful connection and upload. Buttons for 'Test', 'OK', and 'Cancel' are at the bottom.

There are currently no presets defined, you must enter all server details. The server address, port, login and password should be provided your ISP.

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 a slash, that folder specification is used in place of the base folder. If that folder does not begin with a slash, it is *appended* to the base folder.

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.

The **Auth TLS** option enables **FTPS** or FTP over SSL/TLS for secure FTP transfers. The software does not currently support **SFTP** (SSH File Transfer Protocol). Although FTPS is the more common of the two, it may not be supported by your server.

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

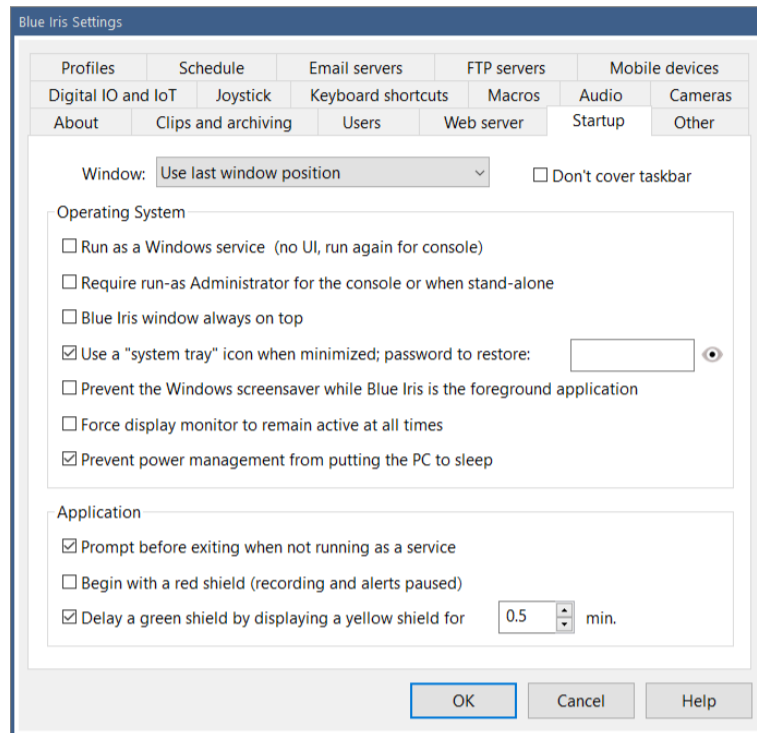
Use the Test button to test the connection by uploading a short file.

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.

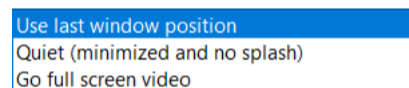
MORE OPTIONS

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.

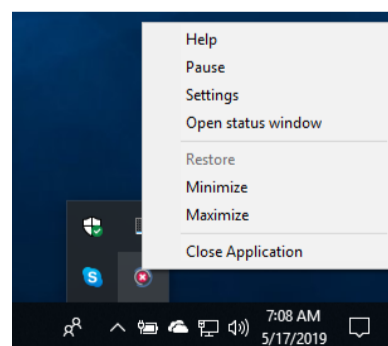


However you may also select to have it always open **Quietly** (minimized and no splash screen) or to have it immediately **Go full screen video**. Some prefer to retain the Windows **taskbar** on the screen as well.

Running as a **service** or without **Administrator** 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.

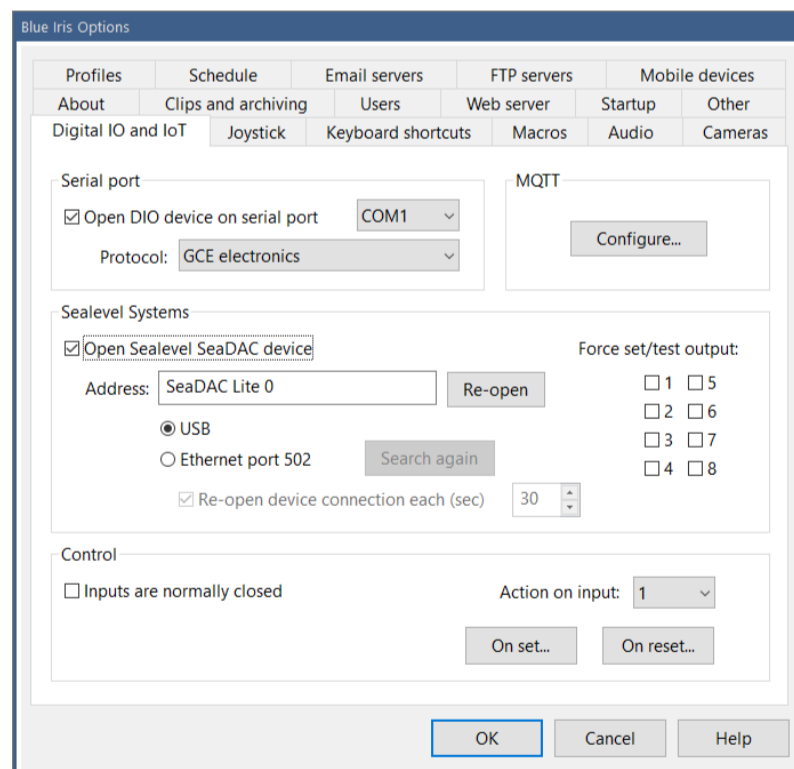
Three additional options exist to help prioritize the Blue Iris window on your desktop. You may prevent the **Windows screensaver**; you may **prevent the monitor from sleeping** due to a power saving setting; you may prevent power-saving features from **sleeping the PC** entirely.

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 the 8206, 8209, 8222, 8223, 8232, 8221, 8113 and 8112 for USB, or 120E or 130E for Ethernet. They offer many other models compatible with these as well—as long as the *SM_ReadDigitalOutputs* and *SM_WriteDigitalOutputs* 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.

Control

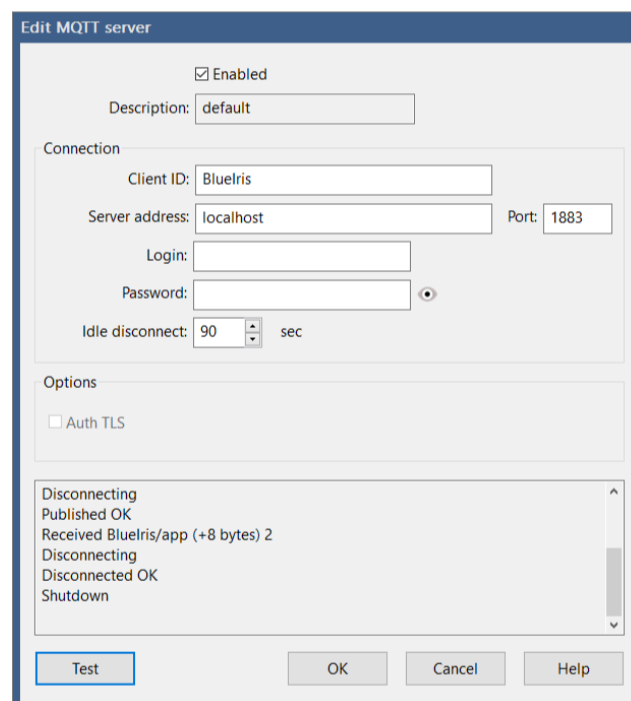
You may select whether input circuits are normally “closed” or “open” as the normal “reset” state in the software. In other words, generally when the LED is *lit* on the SeaLevel device, this is a “set” condition, but you may reverse this sense.

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 “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 Mosquitto 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	
<i>BlueIris/app</i>	<i>starting</i>	
<i>BlueIris/app</i>	<i>running</i>	
<i>BlueIris/app</i>	<i>stopping</i>	
<i>BlueIris/app</i>	<i>stopped</i>	
<i>BlueIris/app</i>	<i>unexpected stop</i>	... this is the <i>Last Will message</i>
 <i>BlueIris/status</i>	 <i>signal=X\n</i>	
	<i>profile=Y\n</i>	
	<i>lock=Z\n</i>	
	<i>schedule=ScheduleName\n</i>	

where

<i>X=0, 1, 2</i>	... the state of the Shield icon
<i>Y=0, 1, ..., 7</i>	... the active global profile
<i>Z=0, 1, 2</i>	... the state of the profile lock, 0=run, 1=temp, 2=lock
<i>ScheduleName</i>	... the current schedule name or <i>Default</i>

The software responds to these messages received:

<i>BlueIris/status</i>	responds by publishing the current status
<i>BlueIris/admin</i>	<i>camera=cam1&trigger</i> ... for example

Possible */admin* commands are identical to those offered by the web server, documented in the Administration chapter.

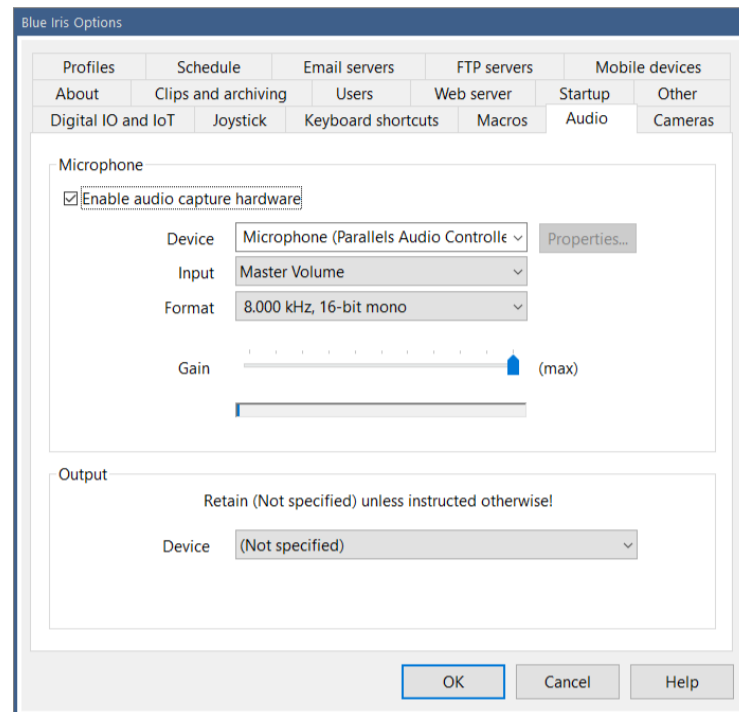
Options

Select to use **Auth TLS** only if this is required by your broker.

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.



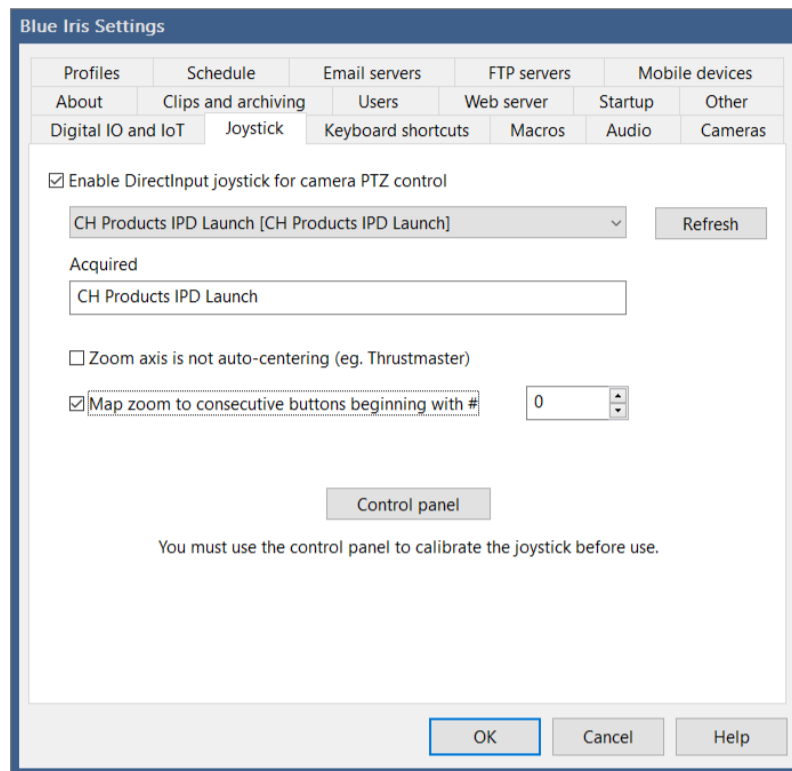
Adjust the gain so that when you speak naturally the audio power bar occupies the majority of its control window without hitting the right-hand side. When the audio power reaches this level, sample “clipping” will occur and there may be audible clicking or other quality loss as a result.

Output

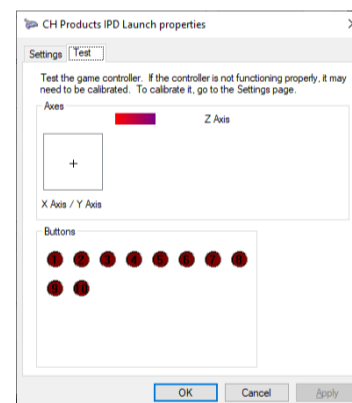
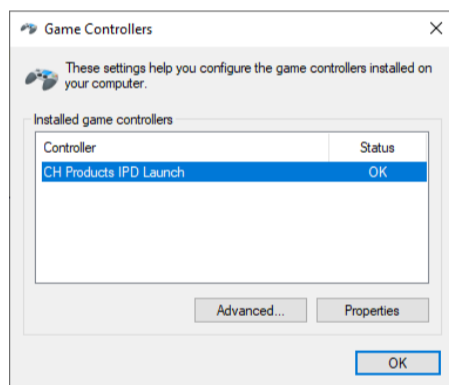
You should not have a need to change this setting unless your system has multiple sound cards and you do not wish to use the primary sound card for audio playback by Blue Iris.

JOYSTICK

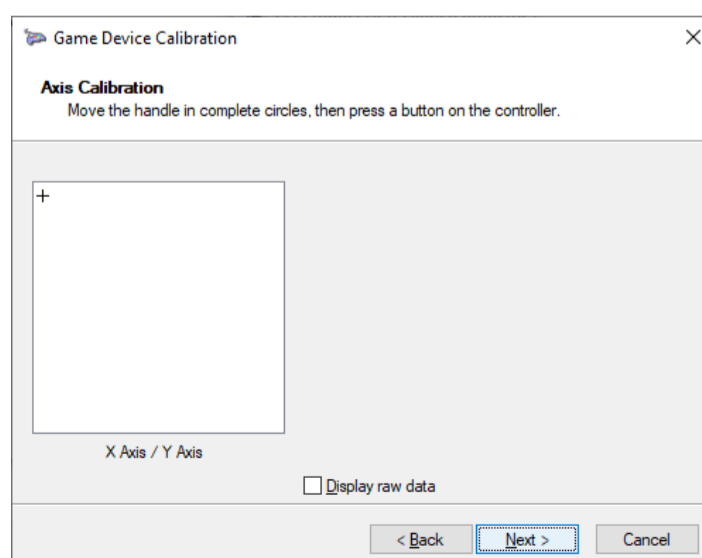
A joystick may be used for camera PTZ operation. If a compatible Windows DirectInput joystick has been attached and its driver is functioning, you will see it on this page.



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.



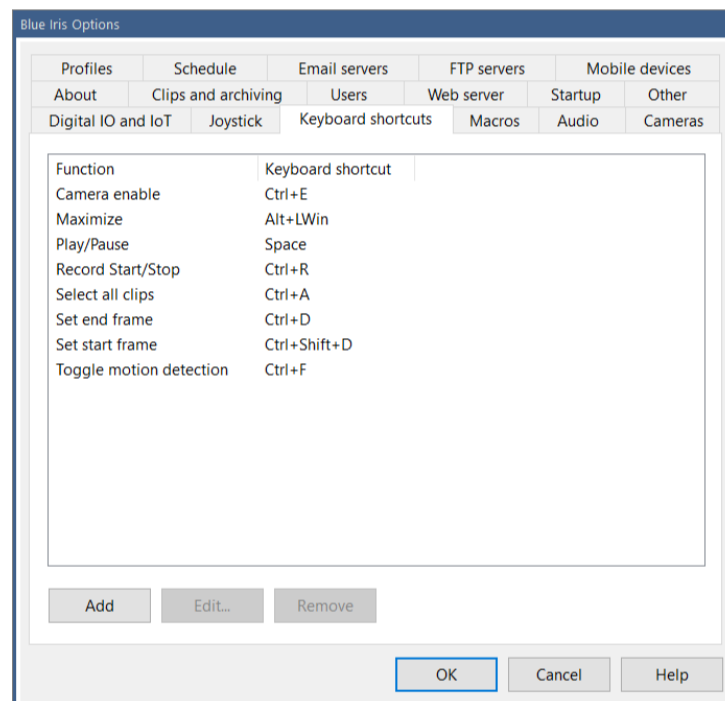
Once you have completed this calibration you can test the joystick function once again through the control panel before trying it with an actual camera window.

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.

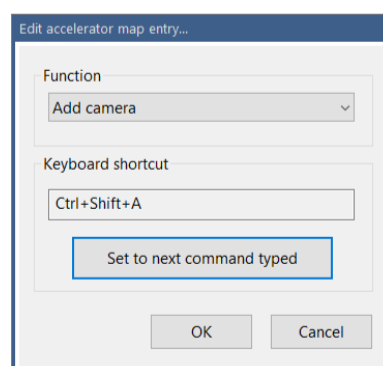
You may also map joystick buttons to software commands. Add a keyboard shortcut (see the next help topic) for Control+Shift+x, where x is a button number 1, 2, etc. When the joystick button is pressed, the associated command will be issued.

KEYBOARD SHORTCUTS

The software can memorize a number of **keyboard shortcuts** for your commonly used functions or commands.



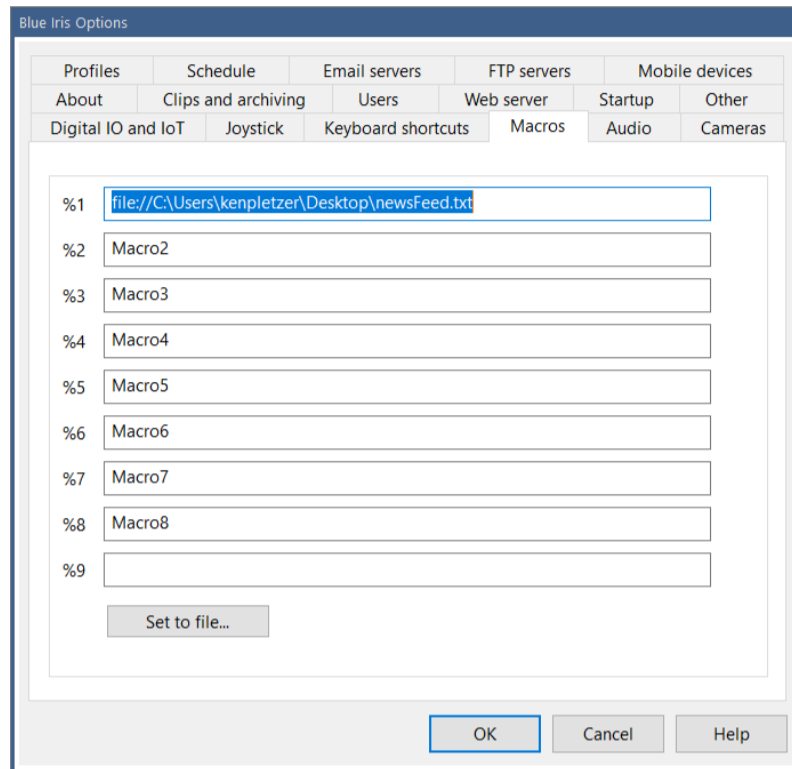
Use **Add** or **Edit** and you will be prompted



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.



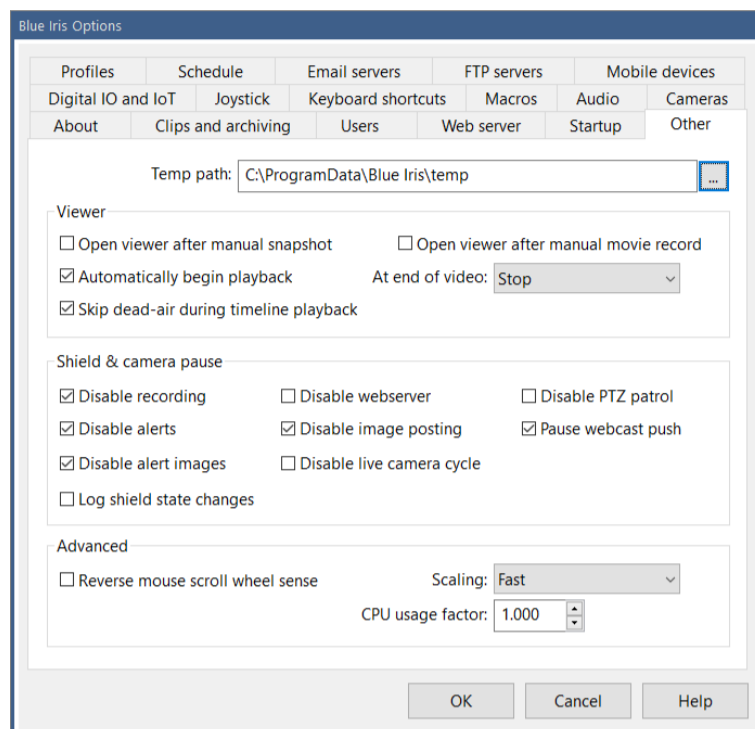
Although only 9 may be set here, the software actually supports up to 99 of these. You will find a section in the Windows registry:

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 *disc full* condition on a disc used for the database or recording.

Advanced

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, and 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.

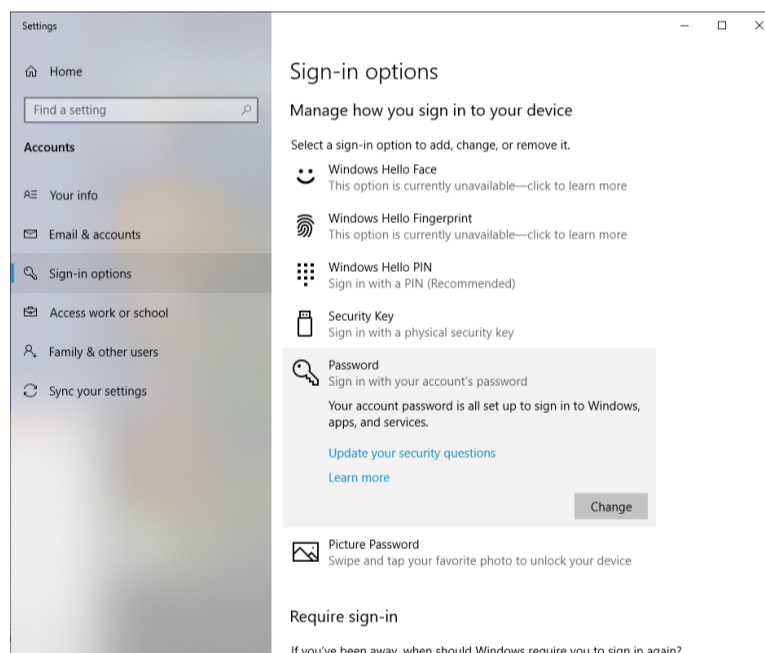
ADMINISTRATION

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.

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:

Name	Status	17% CPU	78% Memory	0% Disk	0% Network	Power usage	Power usage t...
Apps (6)							
Blue Iris Video Security and Web...		0.9%	20.3 MB	0 MB/s	0 Mbps	Very low	Very low
Blue Iris							
Microsoft Management Console		0%	10.2 MB	0 MB/s	0 Mbps	Very low	Very low
Microsoft Visual Studio 2017 (32...		0%	300.4 MB	0 MB/s	0 Mbps	Very low	Very low
Registry Editor		0%	0.7 MB	0 MB/s	0 Mbps	Very low	Very low
Task Manager		0.9%	16.3 MB	0 MB/s	0 Mbps	Very low	Very low
Windows Explorer		1.1%	47.2 MB	0 MB/s	0 Mbps	Very low	Very low
Background processes (64)							
AcroTray (32 bit)		0%	0.5 MB	0 MB/s	0 Mbps	Very low	Very low
Adobe Genuine Software Integri...		0%	1.9 MB	0 MB/s	0 Mbps	Very low	Very low
Adobe Genuine Software Servic...		0%	0.6 MB	0 MB/s	0 Mbps	Very low	Very low
Antimalware Service Executable		0%	73.7 MB	0 MB/s	0 Mbps	Very low	Very low
Application Frame Host		0%	1.0 MB	0 MB/s	0 Mbps	Very low	Very low
Blue Iris Video Security and Web...		9.9%	157.0 MB	0 MB/s	2.6 Mbps	Moderate	Low
BlueirisService.exe (32 bit)		0%	0.7 MB	0 MB/s	0 Mbps	Very low	Very low
COM Surrogate		0%	1.5 MB	0 MB/s	0 Mbps	Very low	Very low
COM Surrogate		0%	1.0 MB	0 MB/s	0 Mbps	Very low	Very low

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 Messages 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.

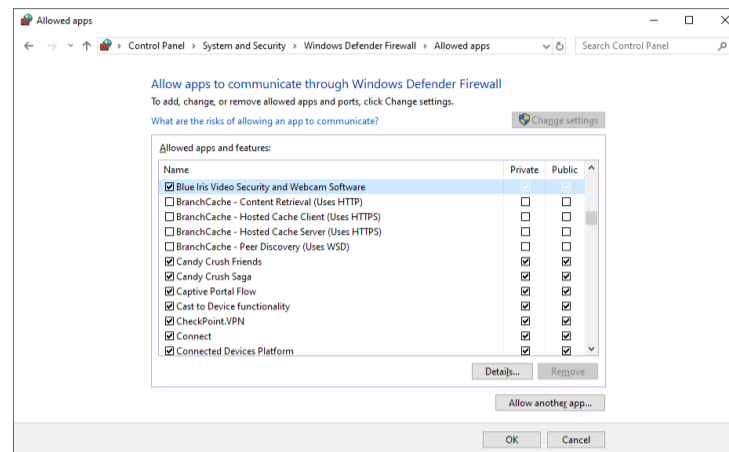
SECURITY SOFTWARE EXEMPTIONS

The importance of this step cannot be overemphasized. There are four categories of security software to address:

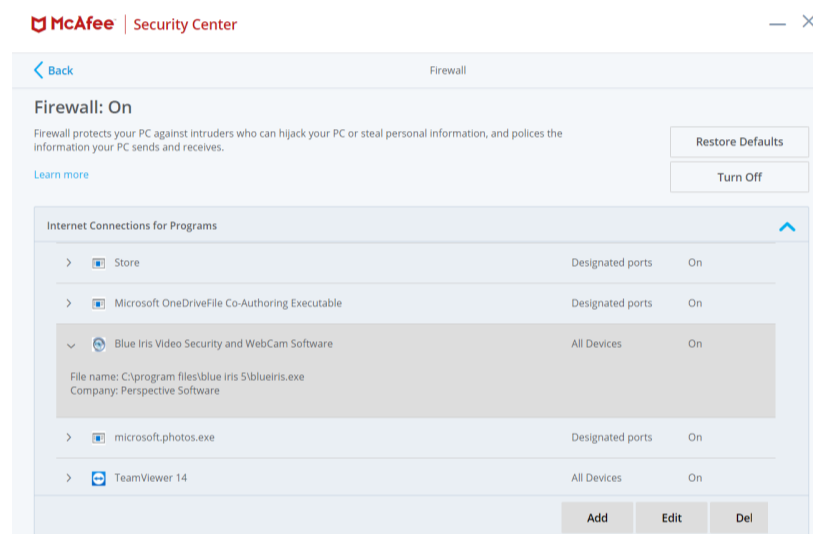
Firewall. These stand between software and use of the network or Internet. Blue Iris requires network access to pull video from network IP cameras. Blue Iris also uses an occasional connection to the Blue Iris Software website to check for software updates,

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:



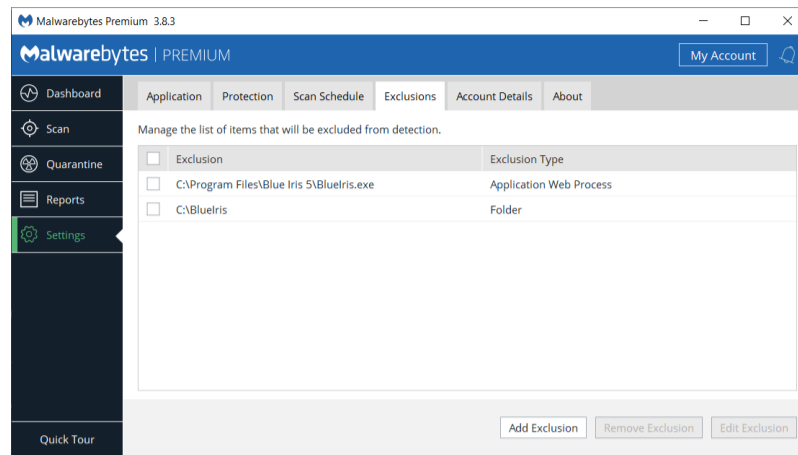
Here's what the firewall exemption should look like in McAfee:



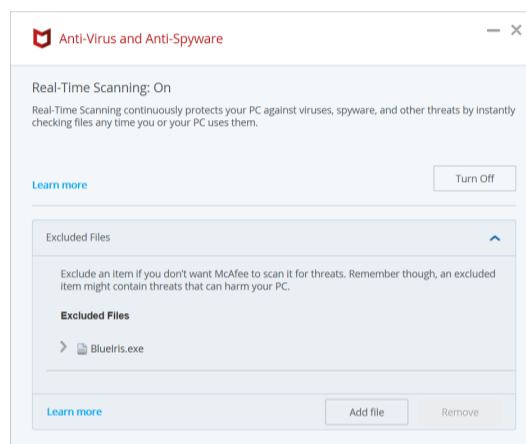
Antivirus. These monitor files or folders for changes, looking for threats. These may interfere by locking files which Blue Iris is actively modifying or attempting to delete. For smooth and efficient software operation, you should exempt the database and clips storage folders. Blue Iris never creates 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 files *BlueIrisAdmin.exe* and *BlueIrisService.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 disc resources with endless “temp” files.

Here's what the exemption should look like in Malwarebytes:



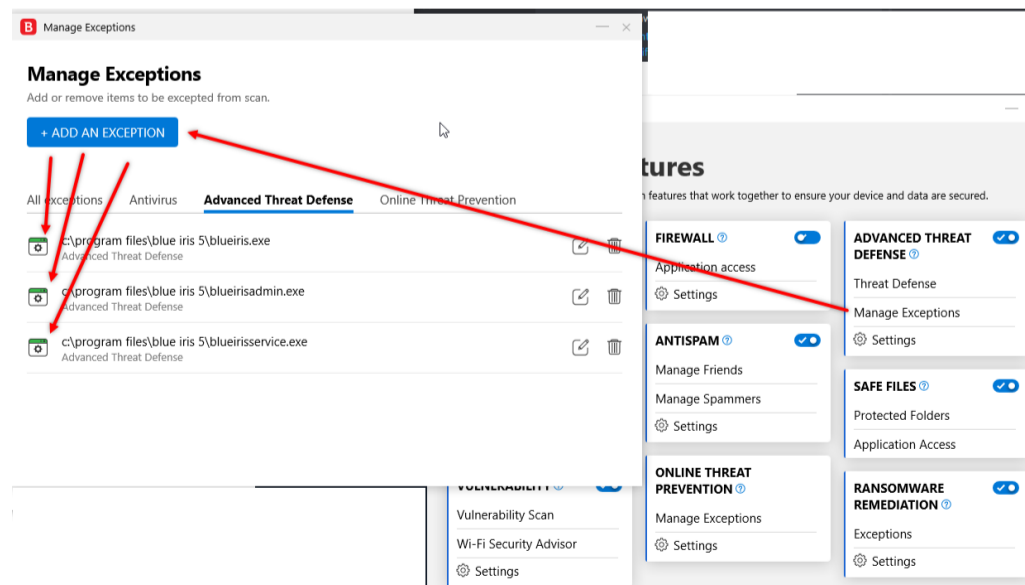
and in McAfee:



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 **Require run-as Administrator**. 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 disc. 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-disc 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 a 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 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 disc.”

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 disc-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.

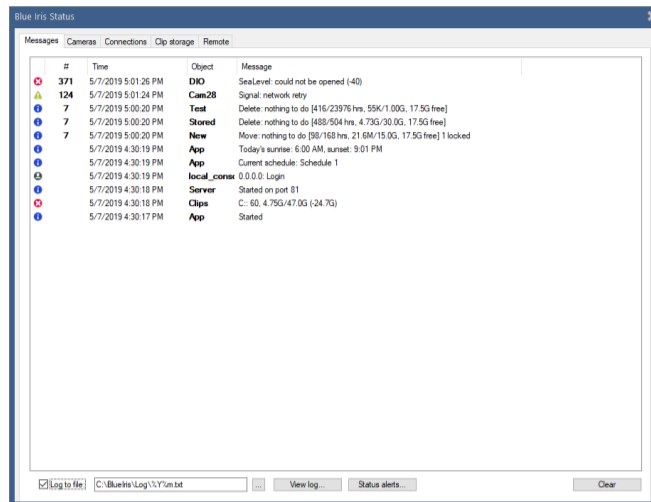
The Bottom Line

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 Messages 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.

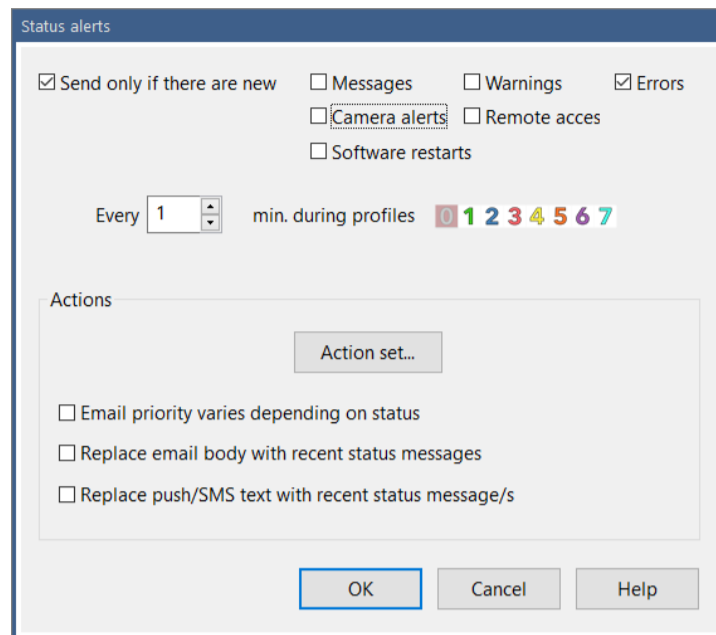


If there are errors or warnings on this list, a matching status icon will appear in the software's status bar at the lower-right of the main window.

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 a **View log** button is provided. These files *are not otherwise managed* and will eventually use considerable disc space. Please be sure to prune this folder on occasion as required.

Use the **Status alerts** button to configure periodic status messages via email, push, or otherwise.



You may wish to receive periodic messages simply as a “health” notice. Typically however you are interested in receiving messages only when there are new items of interest added to the Messages page in Status, and you may choose which types are of interest.

You may select the rate at which these may be sent, along with which the active profiles.

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.

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.

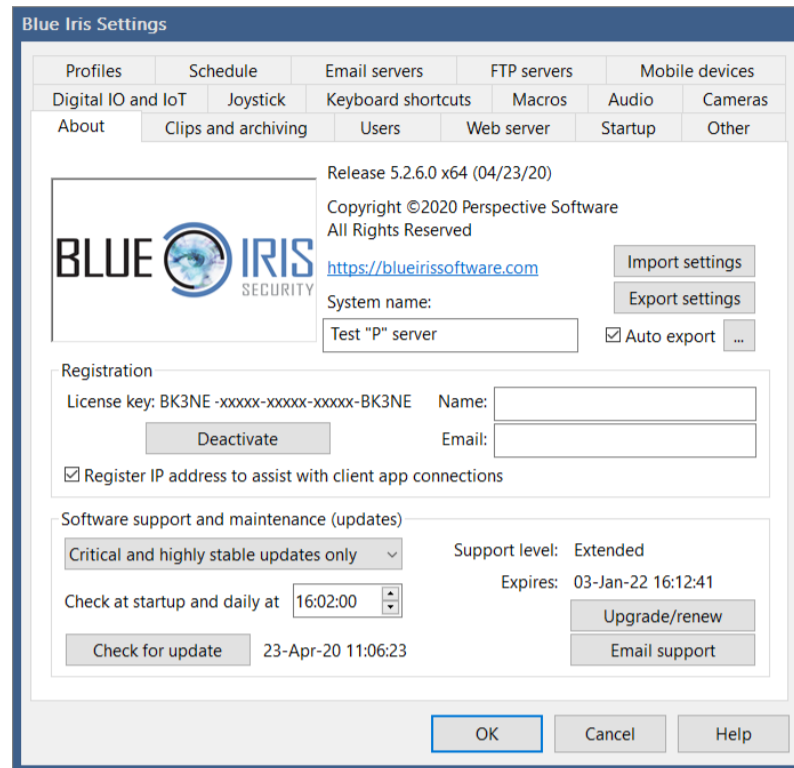
Recorded Video

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, SUPPORT AND 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* support and maintenance which means access to email software support and same-version 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.

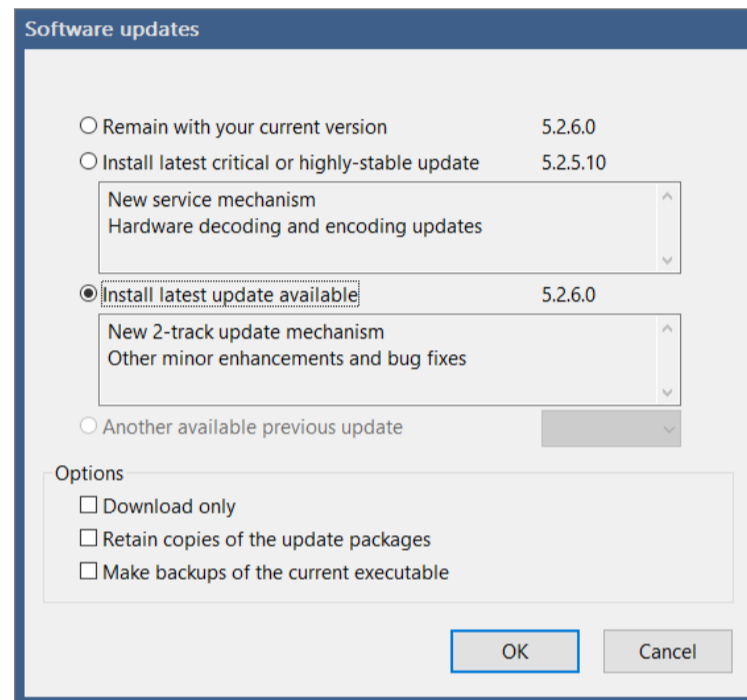
For continued access to email support and software maintenance (all updates, including free major-version *upgrades* as well), there is an *optional* annual support and maintenance program. For details please visit:

<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 support and maintenance date expires.

If expiring soon, please use the **Upgrade/Renew** button to either purchase a new plan, or to enter the support and 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. 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 update** 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 support and maintenance plan. You may only download versions for which your license is authorized (those released while your license was covered by support and maintenance).

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 then 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, 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/>

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, we do NOT support and are NOT affiliated with the "IPCamTalk" forum and have in fact received many complaints from users concerning the way in which they have been treated—the forum's moderators are known to be intolerant of beginners and in many cases provide profanity-laden and unprofessional replies.

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:

<code>%%SERVERNAME%%</code>	Current host name and port used to access the server
<code>%%SERVER%%</code>	Current host name without the port number
<code>%%SESSION%%</code>	Current session key
<code>%%VERSION%%</code>	The software version in the format 5.0.8.2
<code>%%SHOWALERTS%%</code>	0, or 1 if there are new alert images for the current user
<code>%%SYSNAME%%</code>	System name as defined on the Settings page
<code>%%AUTHORIZATION%%</code>	If basic authentication is used, the base-64 encoded USER:PASSWORD
<code>%%CAMLIST%%</code>	A list of HTML <code><OPTION></code> tags containing the available cameras and groups
<code>%%CAMLIST2%%</code>	An alternate/simpler version of CAMLIST
<code>%%CLIPLIST%%</code>	A list of HTML <code><OPTION></code> 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
<code>%%CLIPn%%</code>	A virtual path to the actual "nth" clip currently displayed in the Clip List using the cam and alerts parameters
<code>%%THUMBn%%</code>	A virtual path to a thumbnail image for the "nth" clip currently displayed in the Clip List using the cam and alerts parameters
<code>%%CAMNAME0%%</code>	DEPRECATED. The first camera's name
<code>%%CAMPORT0%%</code>	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."

/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, and may be used in future versions of the ActiveX control.

/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).

/video/{cam-short-name}. Used by client apps to pull an H.264-encoded video stream with proprietary formatting.

/file/clips/{filename}&mode=jpeg&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.

/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 if it was saved to disc.

Optional parameters for many of the above:

<i>&w=</i>	width, use with or without height
<i>&h=</i>	height, use with or without width
<i>&s=</i>	scale 1-100 in place of width and/or height
<i>&q=</i>	quality 1-100
<i>&fps=</i>	frames/second
<i>&kbps=</i>	kilobits per second
<i>&cache=1</i>	include cache-control: no-cache in the reply
<i>&connection=close</i>	do not re-use this connection

Admin commands

`/admin?camera=x&autocycle=1 or 0` Automates the auto-cycle function for camera x's frame

`/admin?camera=x&alerts=x` Enable or disable alerts on camera x (short name)

`/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` Use x=1 to mark the most recent alert as flagged in the clips database and timeline; *memo* is optional. Use x=0 to mark the most recent alert as *cancelled*. 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&priority=x` 1: temporarily move camera to top-left position, 0: return to normal position.

`/admin?camera=x&profile=n` Force profile *n* on camera *x* (short name)

`/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&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` Trigger camera or group *x* (short name) as an External source; optionally add *text* to the memo field in the database.

`/admin?camera=x&trigger=1` Trigger camera or group *x* (short name) as a Motion source

`/admin?camera=x&trigger=-1` Trigger camera (short name) as an ONVIF source

`/admin?camera=x&trigger=0` Reset trigger on camera (short name)

NOTE: With the ONVIF source, the camera will *remain triggered* until the `&trigger=0` command is used and the break time has expired.

`/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, or maintain` Initiates the specified database operation.

`/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*=1-99 to value {*text*}

/admin?output=x&msec=y or &force=true Set DIO output x=0-7 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?solo=1 or 0 Automates the main window single-camera “solo” icon and function

/admin?transport=x Automates the clip viewer window; x may be one of play, rplay, next, prev, pause, step, or rstep

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

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
ptz	true/false
audio	true/false
clips	true/false
streamtimelimit	true/false
dio	true/false
version	PC software version, eg., 5.0.0.26_x64 (or w32)
license	PC software license key
support	PC software support and 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	expressed as the integer number of seconds since January 1, 1970
enddate	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 all users on all cameras

the following information is returned in an array, and for each entry:

parameter	value
camera	camera short name
newalerts	only sent for the 1st alert on each camera, user specific new alert counter
path	primarily used to parse the extension

parameter	value
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
filetype	a string with the file's extension, compression type, and folder name
zones	a bit representation of the motion zones, 1==A, 2==B, 4==C, etc.

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
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
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
FPS	the current number of frames/second delivered from the camera
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
isAlerting	true or false; currently sending an alert
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
isRecording	true/false
isManRec	true/false, manually recording
ManRecElapsed	msec since manual recording began
ManRecLimit	msec limit for a manual recording
isYellow	true/false

parameter	value
profile	the camera's currently active profile, or as overridden by the global schedule or the UI profile buttons
ptz	is PTZ supported, true or false
audio	is audio supported, true or false
width	frame pixel width
height	frame pixel height
nTriggers	number of trigger events 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 number of cameras across
ysize	for a group, the number of cameras tall
group	for a group, an array of the camera short names in the group
rects	for a group, an array of the camera rectangles within the 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
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)

parameter	value
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 <i>move</i>
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
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
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)
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	primarily used to parse the extension
offset	for an alert, the offset within the 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)
filesize	string, a formatted representation of the clip duration
filetype	a string with the file'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
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 disc" export, which is much quicker; "false" is incompatible with WMV, overlay:true or timelapse 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

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

parameter	value
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.
	0: Pan left
	1: Pan right
	2: Tilt up

parameter	value
	3: Tilt down
	4: Center or home (if supported by camera)
	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
	if a button value is not sent, the current PTZ settings are returned
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	install current software update
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

parameter	value
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
memload	a percent formatted version of RAM
discs	an array of disc information, each disc 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
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 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

parameter	value
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

trigger

trigger the selected camera

parameter	value
session	the session key that was supplied with the initial login command
camera	camera short name

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
flags	adjusted flags are returned by <i>cliplist</i> or <i>alertlist</i>
mask	which flags to adjust
exportprofile	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
enabled	optional, true/false
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

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 <i>log</i> 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	showhidden	N/A	toggle show hidden command in live camera window
	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
		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	1-99	(text)	set macro number to specified text

TROUBLESHOOTING AND FAQ

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.

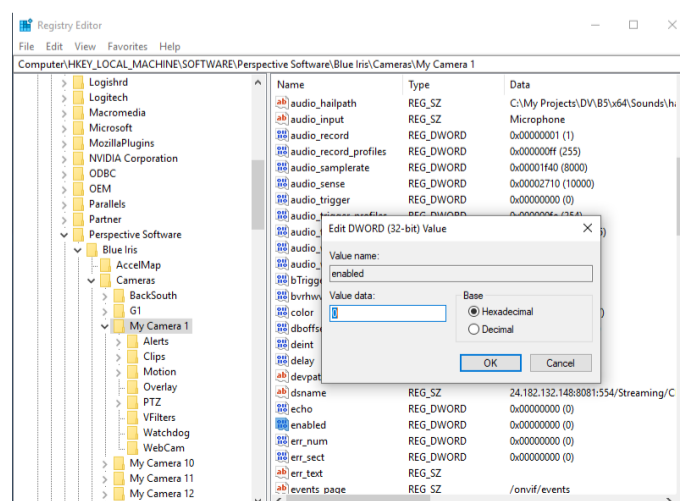
An issue may be related to a recent settings change. If you are creating automatic settings backups as configured on the About page in settings, you may try reverting to one of these if you are able to get to that page without a crash.

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:

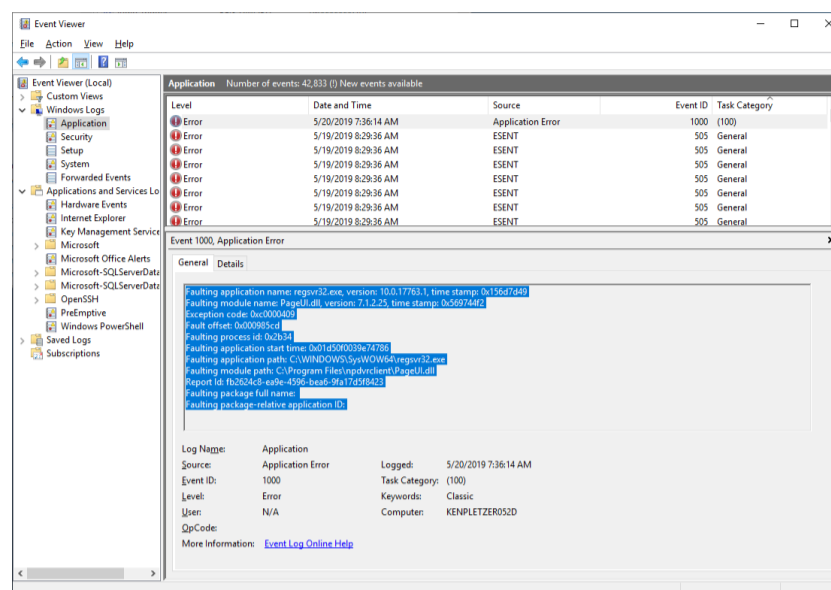
HKEY_LOCAL_MACHINE\SOFTWARE\Perspective Software\Blue Iris

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” 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 handling. 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-disc*, 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:

$$\frac{\frac{2048\text{kbps}}{(10\text{bits/byte})} * 86400\text{seconds/day}}{(1024\text{KB/MB})}$$

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 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 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 storage 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 lengthy 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 Web server 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.

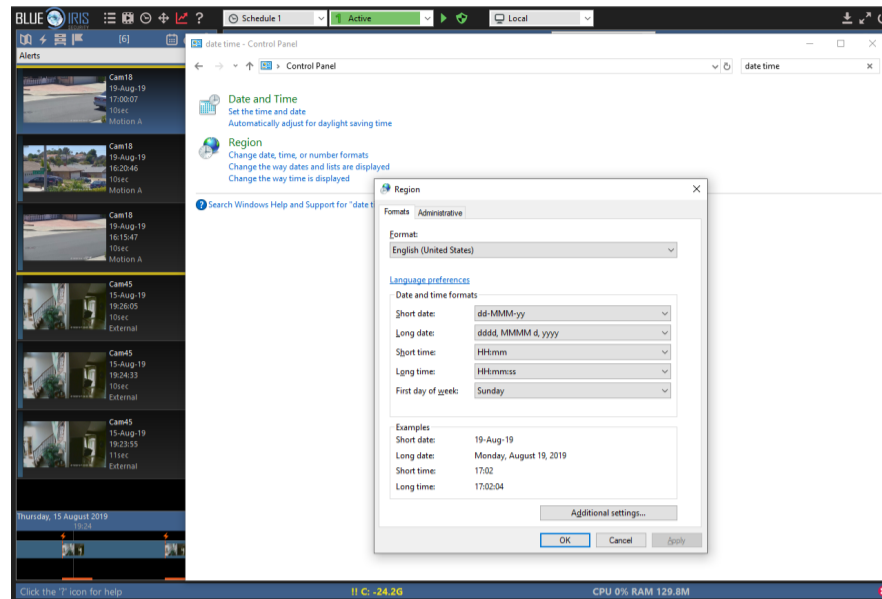
Use another firewall (software or hardware) to allow access only from specified IP addresses.

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-disc* 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 “non-USA” date formats?

This is done in the Windows 10 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