SecuritySpy

Version 2.1.1

User Manual

Author: Ben Bird
Click here for web site
Click here for online store

Contents

Introduction

SecuritySpy is a multi-camera video surveillance application for the Macintosh.

This software will enable you to set up a comprehensive and effective surveillance system quickly and easily. The motion detection feature means that you can choose to capture footage only when there is some activity to record. In addition, you can use the timelapse feature to record continuously.

Unlike traditional analog CCTV systems, there is no need for bulky tapes to change nor for spending hours viewing the captured video. SecuritySpy also offers better image quality and much more convenient access to your captured footage.

A major advantage of using SecuritySpy is the Web Server feature, which allows you to access your surveillance system over the internet or over a local network using a web browser.

If you are building a video surveillance system from scratch all you need is SecuritySpy, a Macintosh computer, and one or more cameras (digital cameras, analog cameras with video input devices, or a combination of the two). If you have an existing system using analog cameras, SecuritySpy will enable you to upgrade to a computer-based digital system whilst still retaining your existing cameras and cabling.

SecuritySpy's flexibility will allow you to set up a system tailored for your individual needs. Whether you want a single camera or many dozens, SecuritySpy is ideal, for both domestic and business purposes.

This manual describes how to use the SecuritySpy software. For information about how to choose, install and set up the hardware of your video surveillance system, see the SecuritySpy installation manual.

The main features of SecuritySpy are:

- Displays and captures live video from multiple cameras simultaneously
- Supports Macintosh-compatible video and audio input devices
- Supports network video devices (Axis, JVC, Panasonic, Pixord, D-Link etc)
- Motion Detection and Timelapse capture features, with audio
- Built-in web server for remote viewing and administration
- Pan/Tilt/Zoom (PTZ) support for many network cameras

- Powerful real-time compression for efficient storage of captured footage
- Broadcasting support for powerful video delivery via QuickTime Streaming Server (QTSS)
- FTP upload feature for off-site storage of captured footage
- Motion-triggered email notifications
- Pre-capture buffer to capture video before the time of motion
- Browser feature for playback of captured footage, with synchronised multi-camera playback

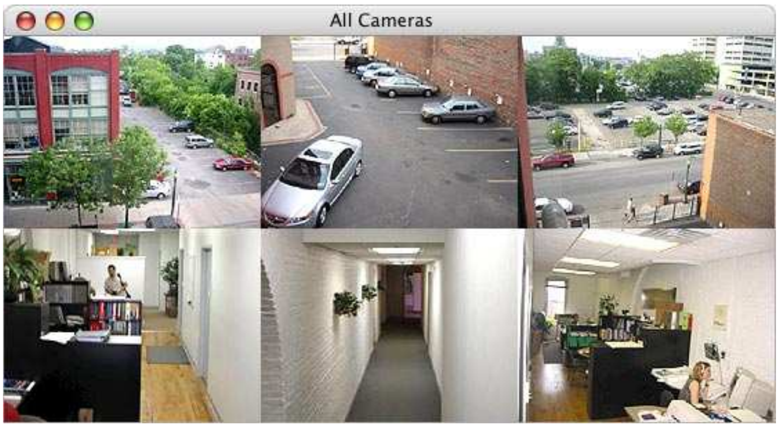
Getting Started

When you first open SecuritySpy it will display, in the main video window, video from all local video input devices that are connected to your computer. To adjust settings for the local video devices, or to add network video devices (such as network cameras and video servers), go to the Video Device Setup window (available from the Settings menu). From this window you can choose settings for the devices, such as video size and format.

SecuritySpy makes a distinction between "video devices" and "cameras", because there is not always a one-to-one relationship between the two. For example, when used with a quad processor, one video device can supply four separate cameras. Therefore the Video Device Setup window contains settings for the video input devices, while the Camera Setup window contains settings for each individual camera (motion detection, recording parameters, FTP uploading, email etc).

Each camera has two modes of operation: *passive mode* and *active mode*. Passive mode is basically preview only. When set to active mode, all the capture features as set up in the Camera Setup window are activated (such as movie/image capture, FTP uploading, actions etc). You can use the Control menu or the Camera Status window (below) to set the mode of a camera to active or passive. When set to active mode, the camera will remain in active mode (even across program restarts) unless there is some error that prevents it running in active mode. There is also a schedule feature available from the Camera Setup window to automatically activate a camera at specified times.

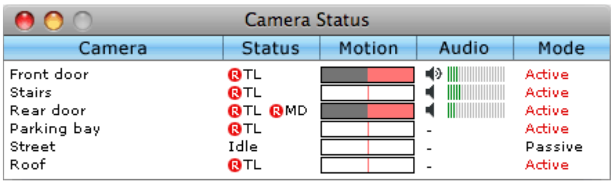
The main video window shows video from all the cameras - to open this select *Main video window* from the Window menu. Here is an example of the main video window displaying six cameras:



The main video window can be resized to any shape and size by clicking and dragging in the bottom right hand corner. As you resize the window it will snap to optimum sizes that are best for the speed and quality of the display (hold the Command key on the keyboard while resizing the window to disable this snapping). Click the green button in the title bar of the window and the window will be automatically resized for optimum display.

In addition, each camera can be displayed in its own individual video window. You can open an individual camera video window from the Window menu, or by double-clicking on a camera image in the main video window, or by double-clicking on a camera name in the Camera Status window.

The Camera Status window is available by selecting *Camera Status window* from the Window menu:


Camera Status

Camera	Status	Motion	Audio	Mode
Front door	Ⓡ TL		🔊	Active
Stairs	Ⓡ TL		🔈	Active
Rear door	Ⓡ TL Ⓡ MD		🔈	Active
Parking bay	Ⓡ TL		-	Active
Street	Idle		-	Passive
Roof	Ⓡ TL		-	Active

For each camera this window shows the camera name, the capture status, the motion bar, audio level, and the mode (active or passive). The capture status area shows any timelapse or motion detection captures in progress: "TL" indicates a timelapse capture and "MD" indicates a motion detection capture. If the status is "Idle" then no video is being captured.

Click the speaker icon (🔈) to the left of the audio level to play a camera's sound through the computer's speakers. In the above example, the first three cameras have audio and the "Front door" camera's audio is currently being played.

Click the mode of a camera and a menu will pop up allowing you to change the mode to active or passive.

To change the order of the cameras, click and drag the camera names in the above window. This affects the order in which the cameras are displayed in the main video window, in group windows, in the Camera Setup window, and through the built-in web server.

Error reporting

When SecuritySpy encounters an error that is not fatal it reports the error in a log file and continues to run. These include errors from video input devices, FTP upload errors, errors sending emails, and errors playing sounds. If you encounter an error you should check the error log to find out more information about what happened. To open the error log file, select *Open error log* from the File menu.

Settings

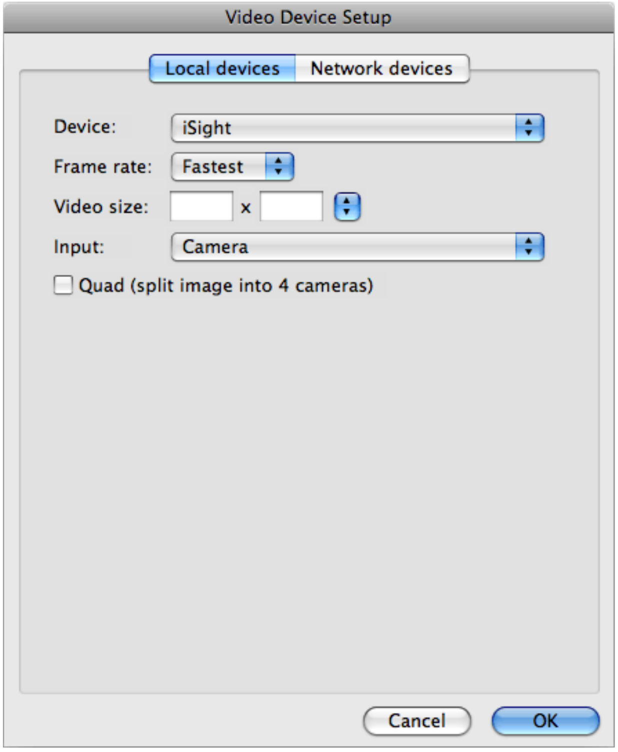
The main configuration windows are as follows:

Video Device Setup – settings for video input devices
Camera Setup – settings for cameras (motion detection, capture settings, actions etc)
Upload Destinations Setup – destinations for uploading images using FTP
Image Settings – settings such as brightness/contrast, and any custom settings for your local video input devices
Overlay Settings – configure the text overlay (for example date/time information) that is drawn onto video frames
Preferences – general settings
Compression Settings – compression used for video, still images, and audio
Schedules – create and edit schedules for automatic activation of cameras
Web Server Setup – settings for the built-in web server
Group setup – allows you to set up groups of cameras that can be displayed together

Video Device Setup

The Video Device Setup window is available from the Settings menu. It allows you configure the video input devices attached to your computer, connected either directly (locally) or over a network. Local devices include those connected by USB, FireWire, and PCI.

Local devices


Video Device Setup

Device: iSight
Frame rate: Fastest
Video size: x
Input: Camera
☐ Quad (split image into 4 cameras)

Click on any item to jump to the description below

Device
This menu contains a list of all local video input devices attached to the computer. Choose a device from this menu to adjust its settings.

Format
Allows you to choose the video format (NTSC, PAL, or SECAM) if the device uses analog video. When you first load SecuritySpy it will attempt to set the format automatically based on you location, although you may need to set this manually. Some devices automatically detect the format of the analog video themselves.

Frame rate
This is the frame rate that is requested from the device. Use it if you want a lower rate than the device's maximum rate - doing so may cause the device itself to switch to the lower rate, resulting in less of the computer's processor time required to process the video and therefore better performance.

Input
If the device has multiple inputs, this menu allows you to choose which input to use. If the device has only one input, this menu will be disabled.

Quad
This feature allows you to use a quad video processor device to enable the input of up to four analog cameras using a single video input device. The image from the device is split into four and each quadrant is treated as a separate camera. When this option is turned on, each camera will use a quarter of the video size supplied by the device. For more information about quad processor devices, click here.

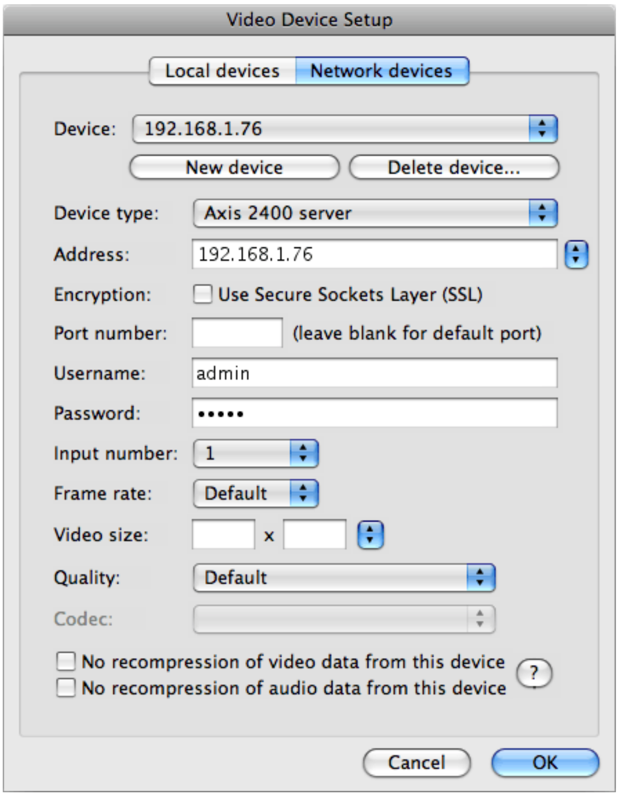
Video size
Allows you to choose a video size for the video input device. If you leave these fields blank, the maximum video size supported by the device will be used.

Generally, the smaller the resolution the better the capture performance and the less hard disk space used by the captured footage, however larger resolutions will result in better image detail.

If you are using an NTSC video source or a digital camera it will typically supply video as 640x480 or 320x240. If you are using a PAL video source it will typically supply video as 768x576, 752x576, 736x576, 704x576, or 352x288. In any case it is best to use either full size or half size - any sizes in between may cause scaling in software which uses CPU time and reduces quality. The popup menu to the right contains optimum sizes to use, including the maximum size available. Using sizes other than those listed in this menu may cause slower performance, or may not be supported by the device.

In the case of DV devices, the resolution is 720x480 for DV-NTSC or 720x576 for DV-PAL, however the pixels are not square and the signal is generally designed to be viewed at a width-to-height ratio of 4:3. Therefore DV-NTSC is usually viewed at 640x480 and DV-PAL is usually viewed at 768x576.

Network devices



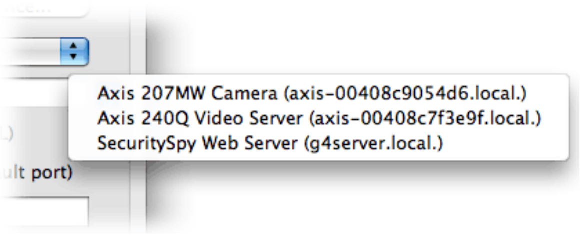
Device: 192.168.1.76
Device type: Axis 2400 server
Address: 192.168.1.76
Encryption: ☐ Use Secure Sockets Layer (SSL)
Port number: (leave blank for default port)
Username: admin
Password: •••••
Input number: 1
Frame rate: Default
Video size: x
Quality: Default
Codec:
☐ No recompression of video data from this device
☐ No recompression of audio data from this device

Device
This menu contains a list of all the network devices that have been set up. Choose one to configure its settings. For network video servers with multiple inputs, each input is treated as a separate network device, therefore you should create one network device for each input of the video server that you want to use.

Device type
Select the make and model of your network device in this menu. Select the *Manual configuration* option at the bottom of this menu if you wish to enter the HTTP request yourself (see below).

Address
Enter the IP address, hostname, or Bonjour name of the device.

Bonjour menu
This menu (to the right of the address text box) lists all Bonjour-enabled devices on your local network. If a device supports Bonjour, it can be found automatically by SecuritySpy and its name, along with its Bonjour address, will be displayed in this menu. Selecting a device in this menu automatically fills out the address and port number text boxes in the above window. For example, the menu will look something like this:


Axis 207MW Camera (axis-00408c9054d6.local.)
Axis 240Q Video Server (axis-00408c7f3e9f.local.)
SecuritySpy Web Server (g4server.local.)
lt port)

In this example, three network devices have been found: two Axis cameras and a SecuritySpy server running on a different computer on the network. For Axis devices, the Bonjour address includes the device's hardware (MAC) address, which is printed on the label on the device itself, making it easier to match up devices with their entries in the Bonjour menu. A MAC adddress is unique to each network device and consists of 12 hexidecimal digits.

Use Secure Sockets Layer (SSL)

SSL is a cryptography protocol that provides secure encrypted communication with network devices. For devices that support this feature, SSL provides additional security by preventing the decoding of intercepted data streams. Note that this may significantly slow down video transmission due to the extra processing required by the device. In order to use SSL you will have to set up the device with a certificate (either self-signed or from a certificate authority, although the latter is not really necessary since you are setting up the server yourself and there is therefore no question about its authenticity).

Port number

If the network device is using a non-standard port, enter it here, otherwise leave this box blank to use the default port (which is 80 for most network video devices; 8000 for SecuritySpy; or 443 if SSL is being used).

Username / Password

If the network device requires authentication, enter your username and password here. If the device doesn't require authentication, leave these fields blank.

Input number

For devices that support multiple inputs (such as the Axis video servers), specify the input number here. This setting will only be available if this feature is supported by the device.

Frame rate

Enter the frame rate at which you want the device to send the video. This setting will only be available if this feature is supported by the device.

Video size

Enter a video size to request from the device. If you leave these fields blank, the default video size of the network device will be used. This setting will only be available if this feature is supported by the device.

Quality

This setting allows you to adjust the compression quality used by the device to encode the video that it sends. The choices are: Default (in which case the device will compress at its default quality), Low, Medium, High, and Maximum. Generally, if you will be capturing the raw data from the device (see below), the Medium setting is a good compromise between quality and data rate; if you will be compressing to a different format (such as MPEG-4 for example) you should use the High setting to ensure minimal image degradation due to this recompression. This setting will only be available if this feature is supported by the device.

Codec

This setting is only available if the network device is SecuritySpy running on another computer. The choices are JPEG, MPEG-4 and Apple Intermediate Codec. JPEG is a good all-round choice being quick to compress and decompress and offering reasonably good data rates; MPEG-4 is much more bandwith-efficient (typically 4 times lower data rates than JPEG at the same quality), however it uses significantly more CPU time to compress and decompress. Apple Intermediate Codec is quickest to compress and decompress and the highest quality of the three choices, however it has the highest bandwidth requirements. Therefore Apple Intermediate Codec is mainly useful on a fast local network where high image quality and low CPU usage are the most important criteria.

No recompression of video data from this device

Network devices generally supply video as a JPEG stream, which is a compressed video format. If this option is enabled, the JPEG-format video data will be captured directly to the movie files that SecuritySpy creates. If this option is not enabled, the video data will be compressed using the settings specified in the Compression Settings window. Enabling this option can significanly reduce the load on the computer's processor, resulting in increased performance, however the captured JPEG-format movie files will be larger compared to other compression formats such as MPEG-4 and H.264. Note that if you have enabled a text overlay or a transformation (rotation/flip) for the camera in the Camera Setup window, this setting will be ignored, as in this case the video must be recompressed.

No recompression of audio data from this device

Network devices generally supply audio data in a compressed format (such as G.711, G.726 or AAC). If this option is enabled and the audio is in a QuickTime-compatible format, the compressed audio data will be captured directly to the movie files that SecuritySpy creates. If this option is not enabled, the audio data will be compressed using the settings specified in the Compression Settings window. Enabling this option can reduce the load on the computer's processor, resulting in increased performance, however the captured movie files may be a bit larger (depending on the settings in the Compression Settings window).

HTTP Request

This setting is available when you select "Manual configuration" as the device type. This is the HTTP request that is sent to the device to instruct it to send video data. This setting is useful if you want to use a network device that isn't yet explicitly supported. Consult the documentation or manufacturer of your device for information about the format for HTTP requests it understands. The following methods of sending video data are supported:

- Multipart JPEG stream (sometimes called "server push", "MJPEG", or "Motion JPEG")
- Pure JPEG stream (usually no HTTP is used and the Request field is left blank)
- Separate JPEG images

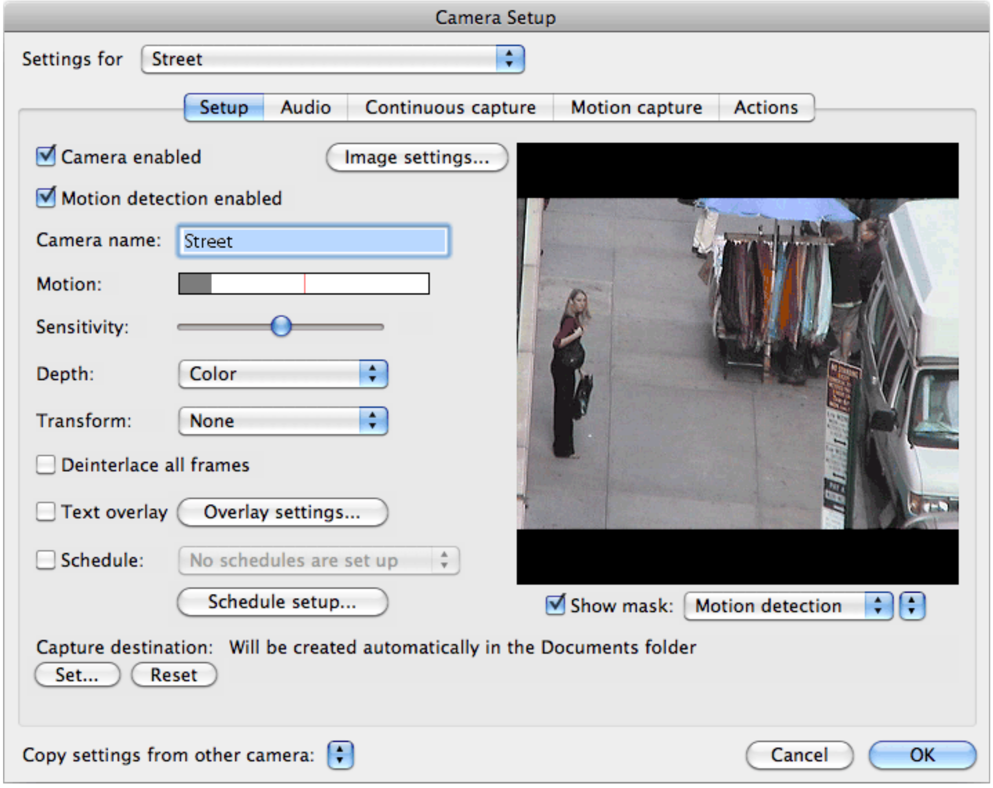
Choosing and setting up your network devices

Click here for comprehensive information on this topic.

Camera Setup

The Camera Setup windows allows you to define settings for each camera. To open this window choose *Camera setup...* from the Settings menu, or hold the Apple (command) key and double click on a camera's video image. The Camera Setup window is divided into four sections:

Setup



Camera Setup

Settings for: Street

Setup | Audio | Continuous capture | Motion capture | Actions

☑ Camera enabled

☑ Motion detection enabled

Camera name: Street

Motion:

Sensitivity:

Depth: Color

Transform: None

□ Deinterlace all frames

□ Text overlay

□ Schedule: No schedules are set up

☑ Show mask: Motion detection

Capture destination: Will be created automatically in the Documents folder

Copy settings from other camera:

Click on any item to jump to the description below

Settings for...
This popup menu contains a list of all cameras. Select a camera from this menu to change its settings.

Camera enabled
This allows you to turn a particular camera on or off. If you turn a camera off it will no longer be used and will not be viewed or captured from.

Motion detection enabled
If you do not need motion detection for a camera, this can be turned off, resulting in lower processor usage.

Camera name
This will be used for identifying the camera and for naming files when capturing video and still images, so you should choose a meaningful name for the camera such as it's location or view.

Motion
Displays the amount of motion currently in the video image. This is done by analyzing the image in software (no special hardware is required). Click within this bar to change the threshold value - when the camera is in active mode this threshold value determines when to capture video and still images, and when to perform actions (for example sounding an alarm, sending an email etc).

Sensitivity
Adjusts the sensitivity of the motion detection to allow for variations in lighting conditions and characteristics of different cameras. Generally this should be set so that there is a reasonable range of movement in the motion indicator when motion is detected, allowing you to set the threshold value accurately.

Mask
There are two masks available: motion detection and video blanking. The motion detection mask allows you to define areas of the image in which to ignore motion; the video blanking mask allows you to define areas of the image to blank out the video completely. Select a mask to edit from the menu, and click and drag in the video preview image to draw the mask, which will appear in green.

Depth
The depth at which to capture video and still images. There are two choices: grayscale and color. Generally, choosing grayscale results in lower file sizes of captured footage.

Transformation

This menu has several options for transformations that can be applied to the video image to compensate for the mounting position of the camera (for example if it mounted upside-down or rotated to one side). The available transformations are: 180° rotation, 90° rotation clockwise, 90° rotation counter-clockwise, horizontal flip, and vertical flip. ⇧

Text overlay on all frames
Use this option to draw a text overlay on all captured video frames and still images. This overlay can include the current date and time, camera name, and any other custom text - see below for more information. ⇧

Deinterlace all frames
This feature is useful if the video input source is supplying analog video (PAL, NTSC or SECAM). Analog video is interlaced, that is, each frame of video is made up of two fields on alternate horizontal lines (an "odd" field and an "even" field). DV video can also be interlaced. Since there is a time delay between the two fields, if there is motion in the frame this will show up as jagged lines in the area of the motion. This feature works by eliminating the odd field and creating a new odd field by interpolating pixels in the even field. Note that this removes some detail from the image and uses CPU time.

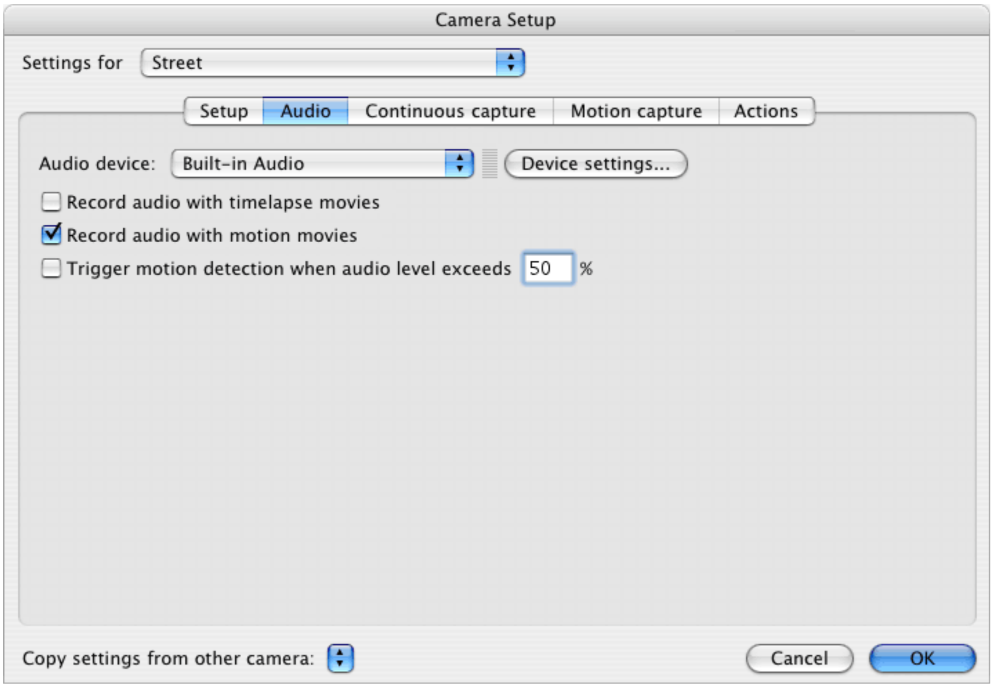
This feature should only be used if the video size is at the largest supplied by the video input device, otherwise the video has already been scaled and the fields are indistinguishable (and if the video size is half the largest size or less, normally only one field will be used and there will therefore be no interlace artifacts). ⇧

Schedule
Use these controls to set up a schedule for activating the camera automatically, for when you want the camera active at certain set times of the day or week. Click here for information about creating a schedule. ⇧

Capture destination
Each camera requires its own unique capture destination folder to which to capture movie and image files. By default, the capture destination is automatically created in the *Captured Files* folder on the main system volume (~/Documents/SecuritySpy/Captured Files/). To choose an alternative volume (for example an external USB or FireWire drive), click the *Set...* button and select the volume of your choosing - the capture destination will then be created automatically in a folder called *SecuritySpy Captured Files* at the root level of your chosen volume. You can alternatively select a particlar folder to use as the capture destination, but unless you want to do this, make sure to select the volume itself (root level), and not a particular folder within the volume. ⇧

Image settings
Click this button to define image settings such as brightness and contrast. This feature is only available for local devices (not for network devices). See below for more information. ⇧

Audio



Settings for: Street

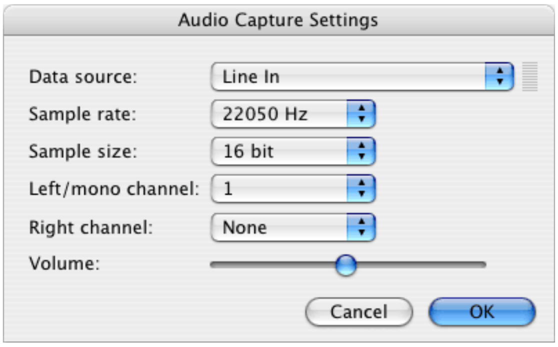
Audio device: Built-in Audio

□ Record audio with timelapse movies
☑ Record audio with motion movies
□ Trigger motion detection when audio level exceeds 50 %

Copy settings from other camera:

Audio Source
Choose an audio input device to associate with this camera. This menu lists all available devices attached to your computer. Supported devices include built-in audio inputs as well as any Mac-compatible USB, FireWire and PCI devices. Additionally, if the camera is a supported network camera, or from a supported network video server, there will be a "Network audio" option in this menu to get audio input from the network device. ⇧

Device settings
Click this button for the device settings window that allows you to adjust settings for the audio capture such as sample rate, sample size, and volume. These settings are set on a per-camera basis, so two different cameras can use the same audio device with different settings (this is useful if you are using an audio device with multiple inputs and want to assign each input to a different camera for example).



Audio Capture Settings

Data source: Line In

Sample rate: 22050 Hz

Sample size: 16 bit

Left/mono channel: 1

Right channel: None

Volume:

If the audio device has more than one data source, these are listed in the top menu. For example, most built-in audio inputs in Macintosh computers have two data sources: Line In and Digital In; if you were using an analog audio source you would select Line In, if you were using a digital source you would select Digital In.

The *Sample rate* and *Sample size* menus allow you to adjust the quality of the audio - the higher these settings the better the quality, but the larger the captured files. The following should give you some idea of how the sample rate and sample size affect the recording quality:

- Very high quality: 44100 Hz, 16 bit - CD quality audio, higher than you need for recording people speaking
- High quality: 22050 Hz, 16 bit
- Normal quality: 12000 Hz, 16 bit
- Low quality: 1200 Hz, 8 bit

Sample rates and and sample sizes that are supported in the hardware of the device are listed in these menus in bold; settings that are not listed in bold are achieved using software conversion (the disadvantage of software conversion being that it reduces audio quality and uses CPU time).

Each camera can use one or two of the audio device's channels. Using the left and right channel menus, you can select which channel on the device (numbered in the menu) is recorded to which channel in the captured movie (left or right). For example, if the audio device has 10 input channels and you want input 5 recorded to the movie as the left channel and input 6 recorded as the right channel, you would select 5 and 6 in these menus. Normally the object is to record people speaking, and this requires only mono (one channel) audio, in which case you should select "None" for the right channel. If you are using stereo audio (two channels), this doubles the size of the audio data, so use stereo only if you need to.

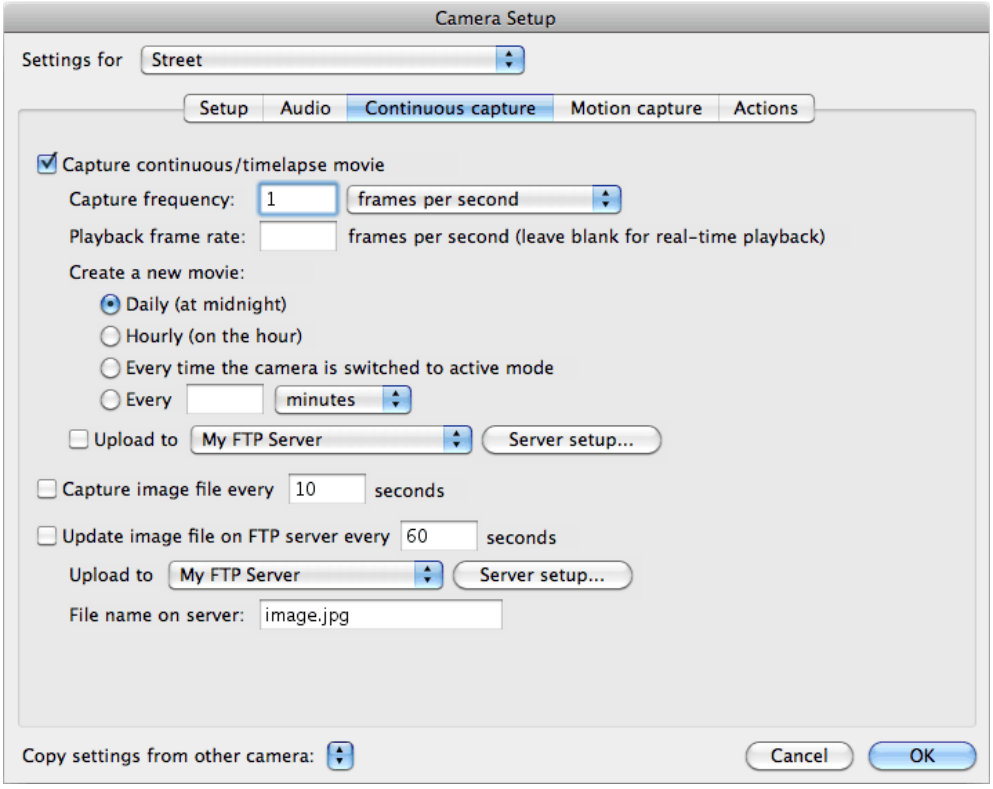
The range of the volume control depends on the device. To obtain the best recording quality, adjust the volume so that loud sounds register high without going into the top two red bars of the volume indicator.

Record audio with timelapse movies
Enable this option to record audio with timelapse movies. Note that if you enable this option, timelapse movies will play back in real time.

Record audio with motion movies
Enable this option to record audio with movies triggered by motion detection.

Trigger motion detection when audio level exceeds x %
This feature triggers motion detection capture when the audio level exceeds a certain value (1-99). To use this feature, motion detection capture must be enabled (see below).

Continuous capture



Camera Setup

Settings for: Street

☑ Capture continuous/timelapse movie

Capture frequency: 1 frames per second

Playback frame rate: frames per second (leave blank for real-time playback)

Create a new movie:

● Daily (at midnight)

○ Hourly (on the hour)

○ Every time the camera is switched to active mode

○ Every minutes

□ Upload to My FTP Server

□ Capture image file every 10 seconds

□ Update image file on FTP server every 60 seconds

Upload to My FTP Server

File name on server: image.jpg

Copy settings from other camera:

Capture continuous/timelapse movie
This feature captures timelapse movies at the frame rate you specify, irrespective of whether motion is detected or not. Timelapse movies are named with a "TL" label in the file name (as well as the current date) so that you can tell them apart from the movies triggered by motion detection. Timelapse capture will take place whenever the camera is in active mode.

The *Capture frequency* specifies how often to capture new frames (leave this setting blank to capture as fast as possible - video will be captured at full frame rate if your computer is fast enough).

The *Playback frame rate* specifies the frame rate that will be used for playback of the movie (it doesn't affect the capture at all). Use this setting if you want the movie to be played back faster than real time (if you leave this setting blank the movie will be played back in real time).

You can specify when to create a new timelapse movie - there are four options:

Daily (at midnight): a new movie will be created at midnight each day. All video captured during each day will be added to the same movie file even if the camera is switched between active and passive mode. The file name of the movie will contain just the day, month and year.

Hourly (on the hour): a new movie will be created at the beginning of each hour. All video captured during each hour will be added to the same movie file even if the camera is switched between active and passive mode. The file name of the movie will contain just the day, month, year and hour. This is a useful alternative to the *Daily* option above, producing smaller and therefore more manageable files that can be downloaded more easily over an internet connection, for example.

Each time the camera is switched to active mode: a new movie will be created whenever the camera is switched to active mode and will continue to be created until the camera is next switched to passive mode.

Every x Minutes/Hours/Days: a new movie will be created at the frequency you specify. Whenever the camera is switched to passive mode and then back to active mode a new movie will also be created. ⇧

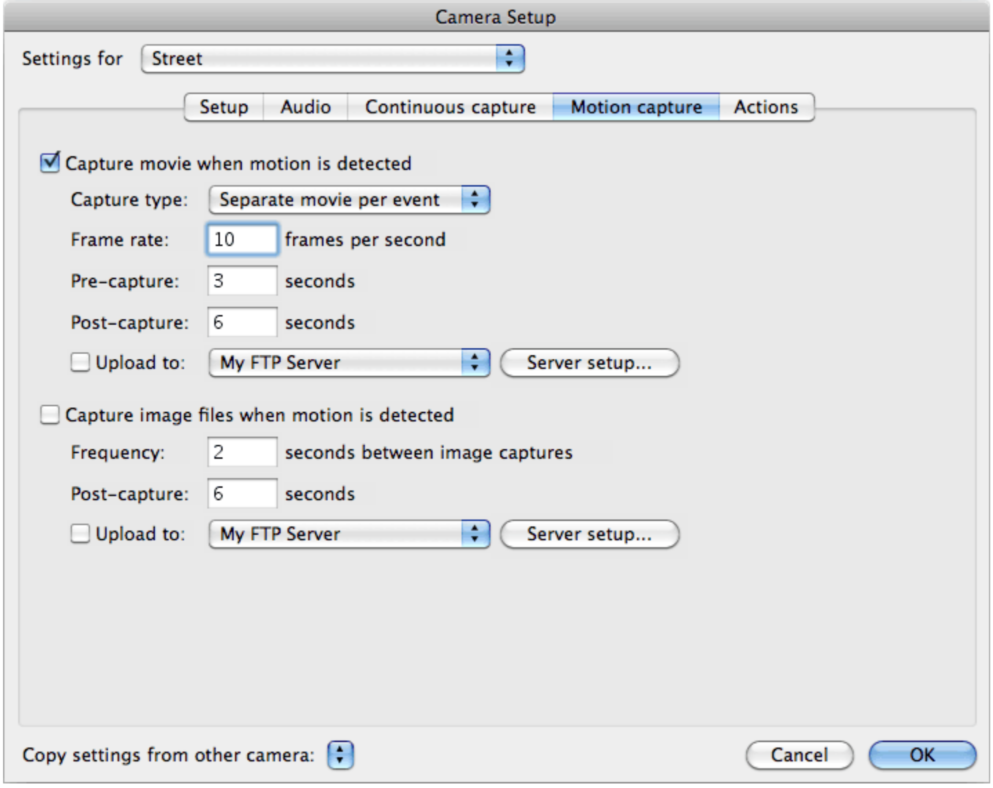
Upload to...
Turn this option on to upload all captured continuous/timelapse movie files to an FTP server. If the create setting is set to *Daily at midnight*, movies will be uploaded at the end of the day; otherwise movies will be uploaded as soon as they have been captured. Click the *Server setup* button to set up the upload destinations (see below for more information on this). ⇧

Capture image file every x seconds
This feature captures an image file to disk in JPEG format at the rate you specify. ⇧

Update image file on FTP server every x seconds
Turn this option on to upload an image with a fixed name to an FTP server periodically, replacing the previous file on the server each time. This can be used, for example, to continuously update an image on a web site. Click the "Server setup" button to set up the upload destinations. See below for more information. ⇧

File name on server
The name of the file on the server. Each time an image is uploaded this name is used and the new file replaces any existing file of the same name. ⇧

Motion capture



Settings for: Street

☑ Capture movie when motion is detected

Capture type: Separate movie per event

Frame rate: 10 frames per second

Pre-capture: 3 seconds

Post-capture: 6 seconds

☐ Upload to: My FTP Server

☐ Capture image files when motion is detected

Frequency: 2 seconds between image captures

Post-capture: 6 seconds

☐ Upload to: My FTP Server

Copy settings from other camera:

Capture movie when motion is detected
Turn on this option to capture a movie when motion is detected. Video is captured at the frame rate specified and saved to disk as a QuickTime movie using the current compression settings (JPEG, MPEG-4 etc). A name for the movie file is generated automatically based on the camera name and time of capture. ⇧

Capture type (movie capture)
There are two options for the type of movie triggered by motion detection:

Separate movie per event: a separate movie will be created for each motion detection event. This may result in a large number of individual movie files but it is then easy to see the time of each motion detection event and find the movie you are looking for.

One movie per day: one movie will be created each day containing all the motion detection events of that day. One large file is easier to manage than lots of smaller files. If you use this option it is useful to enable the Text Overlay feature with a timestamp so that you will be able to see the capture time of each frame in the movie. ⇧

Frame rate (movie capture)
Specifies the frame rate for the movie capture. The lower the frame rate the less hard disk space used by the captured footage and the less CPU time used to compress the video, although low frame rates result in jerky video. ⇧

Pre-capture (movie capture)
It is often useful to have video from both before and after a motion event – in the time before and after, even though the motion is not high enough to trigger recording, there is often something interesting happening that is worth capturing. This is the purpose of the Pre-capture and Post-capture features. The pre-capture feature uses a buffer of video in memory so that when motion is detected the video before the time of motion is also captured. ⇧

Post-capture (movie capture)
Specify the number of seconds to continue capturing the movie after motion has dropped below the threshold level. This should be set to at least a few seconds to avoid many small movie files being captured for one longer period of motion. ⇧

Upload to... (movie capture)
Turn this option on to upload all captured motion-detected movie files to an FTP server. If the capture type is set to *One movie per day*, movies will be uploaded at the end of the day; if the capture type is *Separate movie per event*, movies will be uploaded as soon as they have been captured. Click the *Server setup* button to set up the upload destinations (see below for more information on this). ⇧

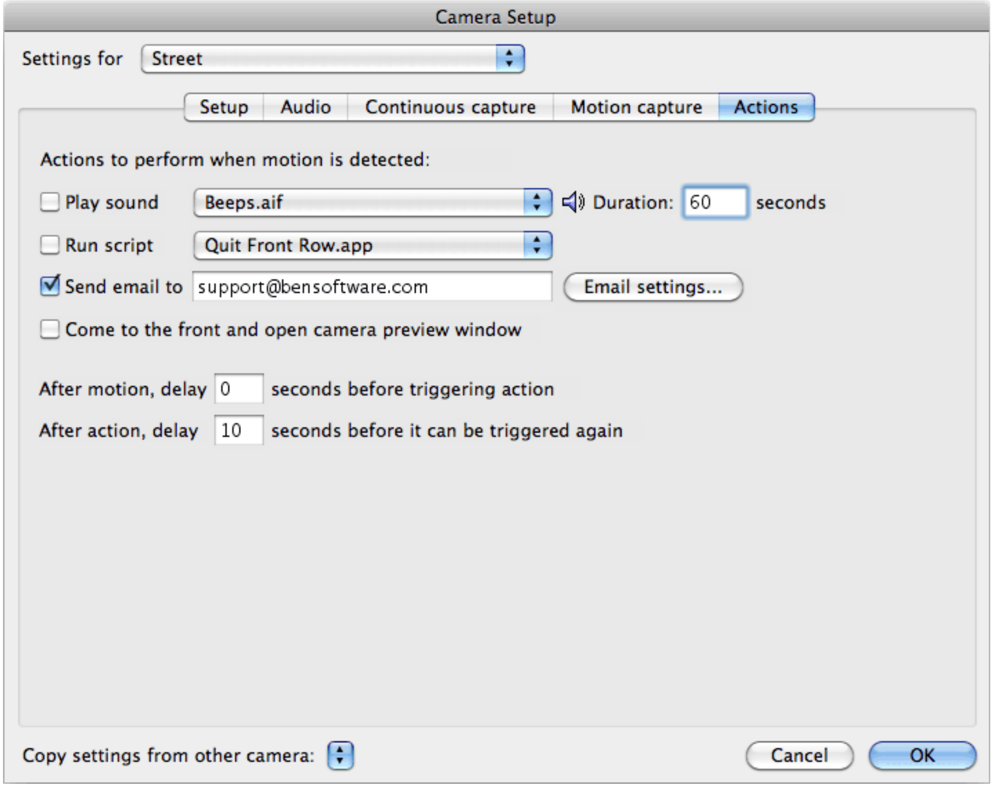
Capture image files when motion is detected
Turn this option on to periodically capture image files when motion is detected. Image files are saved in JPEG format and named based on the camera name and time of capture. ⇧

Frequency (image file capture)
Specify the capture frequency in terms of the number of seconds between image file captures. ⇧

Post-capture (image file capture)
Specify the number of seconds to continue to capture image files after motion has stopped. ⇧

Upload to... (image file capture)
Turn this option on to upload all captured motion-detected image files to an FTP server. Click the *Server setup* button to set up the upload destinations (see below for more information on this).

Actions



Settings for: Street

Actions to perform when motion is detected:

☐ Play sound: Beeps.aif — Duration: 60 seconds

☐ Run script: Quit Front Row.app

☑ Send email to: support@bensoftware.com

☐ Come to the front and open camera preview window

After motion, delay 0 seconds before triggering action

After action, delay 10 seconds before it can be triggered again

Play sound...
Turn this option on to play a sound when motion is detected. There are several sounds designed to scare off intruders, and you can add your own by placing sound files in the Sounds folder (~/Documents/SecuritySpy/Sounds/). To open the Sounds folder, select *Sounds* from the File menu. Most sound formats are supported (including AIFF, WAV, MP3, and AAC).

Duration
Specifies the duration in seconds to play the sound after motion has stopped.

Run script...
Turn this option on to run an AppleScript when motion is detected. You can create your own scripts and place them the Scripts folder (~/Documents/SecuritySpy/Scripts/). To open the Scripts folder, select *Scripts* from the File menu. When using Script Editor to create an AppleScript for this purpose, make sure to save it as a run-only application with no startup screen (these options are available when you come to save the script).

Send email...
This feature sends an email, optionally with attached images, to an address you specify (to send the email to multiple addresses enter them separated by commas). Click the Email settings button to specify settings for sending emails. Images sent with emails are always compressed in JPEG format.

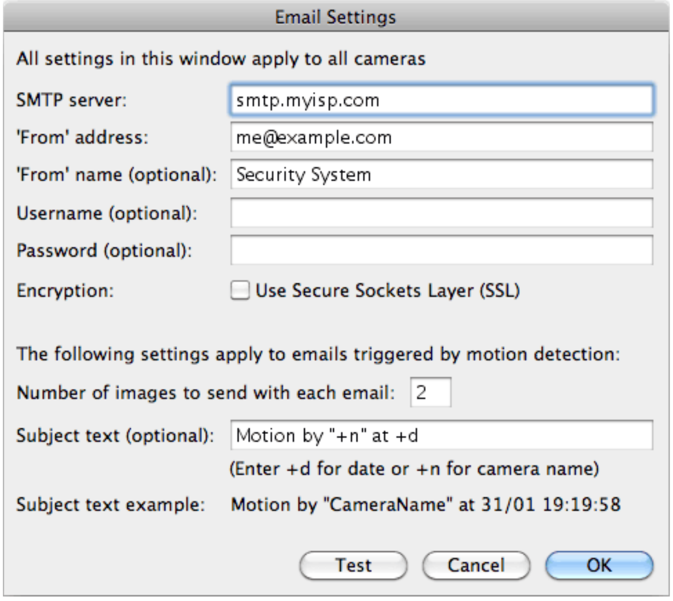
Come to the front and open camera video window
If this option is enabled, whenever motion is detected in this camera, SecuritySpy will come to the front, above all other applications, and will display the camera's video window.

After motion, delay x seconds before triggering action
This option allows you to specify a delay in seconds before performing any of the actions after motion is detected.

After action, delay x seconds before it can be triggered again
Once an action is triggered, this delay specifies the minimum time before the same action can be triggered again. Without this delay, an action could be triggered many times in quick succession if there is lots of motion, which is usually undesirable. Therefore, it is advisable to specify a delay here of at least the length of a typical motion detection event.

Email Settings

This window allows you to specify settings for sending emails. It is available by clicking the *Email settings* button in the Camera Setup window. The Email Settings window looks like this:



Email Settings

All settings in this window apply to all cameras

SMTP server: smtp.myisp.com

'From' address: me@example.com

'From' name (optional): Security System

Username (optional):

Password (optional):

Encryption: □ Use Secure Sockets Layer (SSL)

The following settings apply to emails triggered by motion detection:

Number of images to send with each email: 2

Subject text (optional): Motion by "+n" at +d

(Enter +d for date or +n for camera name)

Subject text example: Motion by "CameraName" at 31/01 19:19:58

SMTP server
The address of the server used to send mail. This is normally provided by your ISP (Internet Service Provider).

If your ISP uses a non-standard port, you can specify this here using a colon and then the port number. For example, if your ISP uses port 28, you would enter "smtp.myisp.com:28". Most SMTP servers operate on standard ports (25 for non-encrypted communication; 465 for encrypted SSL communication), so if you have not been told by your ISP to use a particular port, don't specify a port number and the standard one will be used automatically.

'From' address
This is the return address sent with emails to identify the sender. You should always use a valid email address here as some spam filters block messages without a valid return address. Note that many SMTP servers will not accept just any return address: often the return email address must be from the same provider as the SMTP server.

'From' name
This is the name associated with the return address. It is optional, however if you don't specify a name here, there is a higher chance of the email being blocked by anti-spam software at the receiving email server, therefore it is recommended that you provide one.

Username and password
Some SMTP servers require authentication - if yours does, enter your username and password here.

Secure Sockets Layer (SSL)
SSL is a protocol that provides secure encrypted communication over the internet. If you would prefer to use SSL for sending email, or if your SMTP server requires it, you should enable this option. Note that while some SMTP servers require the use of SSL (notably Google Mail), most SMTP servers do not support it, and therefore enabling this feature when using such servers will prevent emails being sent. Therefore, only enable this feature if you are sure that your email server supports SSL.

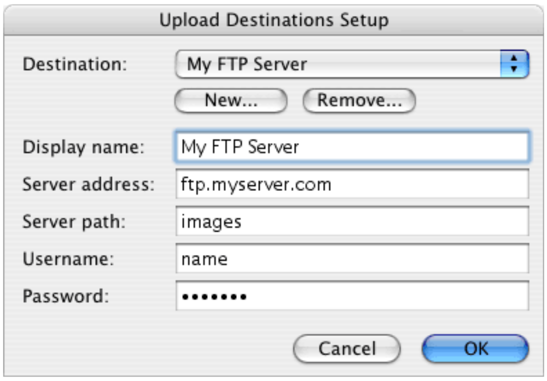
Number of images to send with each email
This defines how many JPEG images to attach to each email triggered by motion detection. For this purpose images are captured at 4fps to allow for reasonably fast stream of images without a large amount of data.

Subject text
This is the subject field that is used for emails triggered by motion detection. If you leave this blank, a subject will be created automatically. If you want to add the date or camera name to your custom subject text, enter "+d" or "+n" respectively (without the quotes) and the appropriate text will be inserted in place of these markers.

Test button
Once you have set up the email settings, you can test them by clicking the *Test* button. This is a feature that attempts to send a test email and reports back any problems with your email settings.

Upload Destinations Setup

This feature allows you to upload captured files to FTP servers. To set up the upload destinations click the *Server setup* button in the Camera Setup window. The Upload Destinations Setup window looks like this:


Upload Destinations Setup

Destination: My FTP Server

Display name: My FTP Server

Server address: ftp.myserver.com

Server path: images

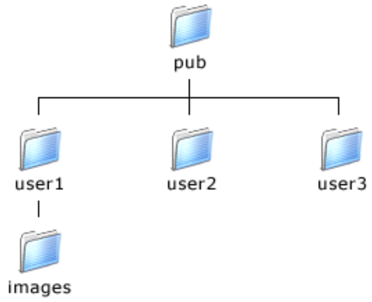
Username: name

Password: •••••••

You can use this window to define destinations that are used to upload files. The same FTP server with different paths may be used for different upload destinations, so one camera can be set to upload to a particular directory on the server and another camera to a different directory on the same server. To check directory paths and download or delete files, you will need to use a graphical FTP client utility such as Transmit.

If you specify a path that starts with a forward slash character, this denotes an absolute path from the server's root directory. A path that does not begin with a forward slash character denotes a relative path from the default directory. The default directory depends on the FTP server - generally each user has a folder on the server which is used as the default directory and set automatically by the server when that user logs in.

For example, consider the following directory layout:



If you were to log in as user1, the FTP server will most likely set the initial directory as /pub/user1/. To have images uploaded to the user1 directory, you would not specify anything for the server path in the Upload Destinations Setup window, or you could specify "/pub/user1/" to be explicit. To have images uploaded to the "images" folder within the "user1" folder, you could specify either "/pub/user1/images/" or simply "images" for the path (in all cases it doesn't matter whether you put a forward slash at the end of the path or not). Generally, you should let the FTP server decide the default directory and use a relative path, unless you have a specific reason to use an absolute path.

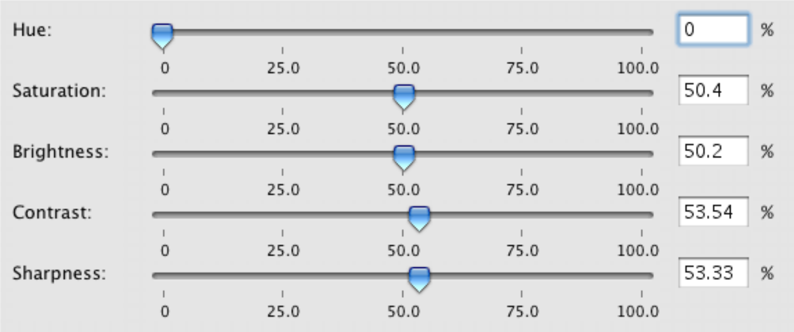
If the directory that you specify does not already exist on the FTP server, SecuritySpy will attempt to create it.

Technical information: SecuritySpy uses passive (PASV) FTP which works in most setups, even when there is a firewall at the client side. However, passive FTP may not work when there is a firewall at the server side. In this case, the firewall and FTP server need to be configured to use a set range of high ports for the FTP data connection. This effectively introduces a small "tunnel" through the firewall that can be used for FTP transfers (see the documentation of your FTP server and firewall for more information).

To see the status of current uploads at any time select *Upload Status window* from the Window menu.

Image Settings

To get this window click the *Image settings* button in the Camera Setup window. This window contains controls for local video input devices such as saturation, brightness, contrast, and any other control that is supported by the device such as flip horizontal/vertical, backlight compensation and manual exposure. Not all controls are available for all devices; the Image Settings window shows all available controls that are supported by the device. Note that for cameras that are part of a quad view from a video processor device, image settings set for one camera will apply to all four cameras. This is because these controls adjust settings for the video input device itself, which is shared by all the cameras.



Hue: 0 %

Saturation: 50.4 %

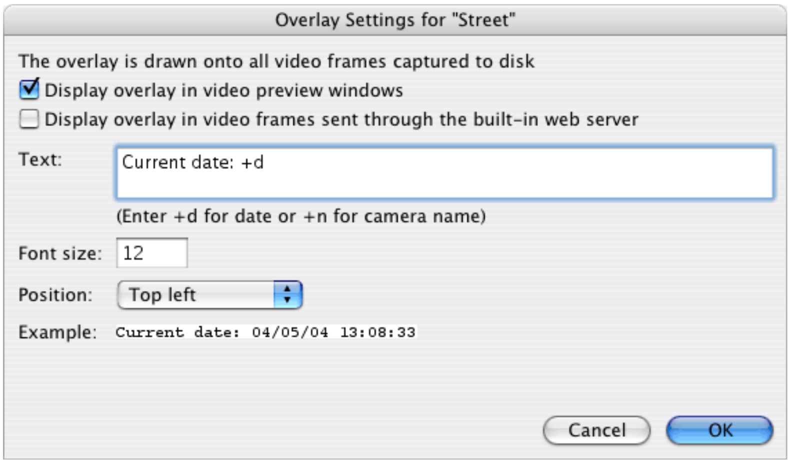
Brightness: 50.2 %

Contrast: 53.54 %

Sharpness: 53.33 %

Overlay Settings

To set up the text overlay settings click the *Overlay settings* button in the Camera Setup window. The Overlay Settings window looks like this:



Overlay Settings for "Street"

The overlay is drawn onto all video frames captured to disk

☑ Display overlay in video preview windows

□ Display overlay in video frames sent through the built-in web server

Text: Current date: +d

(Enter +d for date or +n for camera name)

Font size: 12

Position: Top left

Example: Current date: 04/05/04 13:08:33

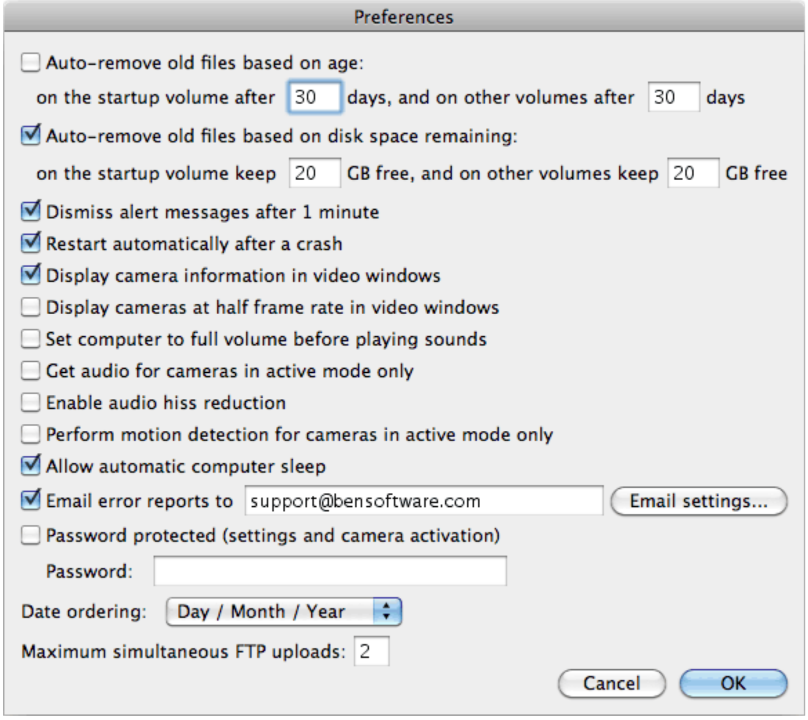
In this window you can specify the text to overlay onto video frames. If you want to add the date (timestamp) or camera name to the overlay, enter "+d" or "+n" respectively (without the quotes) and the appropriate text will be inserted in place of these markers. If you want to add a time difference to the date (perhaps the camera is in a different time zone, connected over the internet), you can add the time zome difference after the date marker, for example "+d+5" for 5 hours ahead the current local time; "+d-5" for 5 hours behind.

When enabled, the overlay is added to all recorded images and video. There are two options that control where else the overlay is shown: in video windows and/or in images sent through SecuritySpy's built-in web server.

You can also adjust the overlay's font size and position in the video image. The space at the bottom of the window displays the overlay as it will look in the video image.

Preferences

The preferences are available from the Settings menu. The Preferences window looks like this:



Preferences

□ Auto-remove old files based on age:

on the startup volume after 30 days, and on other volumes after 30 days

☑ Auto-remove old files based on disk space remaining:

on the startup volume keep 20 GB free, and on other volumes keep 20 GB free

☑ Dismiss alert messages after 1 minute

☑ Restart automatically after a crash

☑ Display camera information in video windows

□ Display cameras at half frame rate in video windows

□ Set computer to full volume before playing sounds

□ Get audio for cameras in active mode only

□ Enable audio hiss reduction

□ Perform motion detection for cameras in active mode only

☑ Allow automatic computer sleep

☑ Email error reports to support@bensoftware.com

□ Password protected (settings and camera activation)

Password:

Date ordering: Day / Month / Year

Maximum simultaneous FTP uploads: 2

Auto-remove old files based on age
If this option is on, captured files older than the number of days you specify will be deleted automatically. There is a separate setting for the startup (system) volume vs other volumes.

Auto-remove old files based on disk space remaining
If this option is on, old captured files will be deleted when disk space drops below the level you specify. If the computer is only being used to run SecuritySpy, a low level of 0.5 GB can be used; if the computer is being used for other applications as well, more free space should be left on the startup (system) volume, hence there is a separate setting for the startup volume vs other volumes.

Dismiss alert messages after 1 minute
If this option is on, all alert messages (such as error messages) will be dismissed after 1 minute. This option should be enabled if the computer is left unattended.

Restart automatically after a crash
Every effort is taken to ensure that SecuritySpy is as stable as possible, however since SecuritySpy relies on other software components written by other parties (such as system software and driver software for video input devices), stability cannot be guaranteed. Therefore it is possible, although unlikely, for SecuritySpy to crash ("unexpectedly quit"), and since the computer may be left unattended for long periods of time this is a potential problem.

If this option is enabled, an auxiliary application is launched that monitors SecuritySpy and will restart it if it crashes. The auxiliary application runs invisibly in the background and uses practically no CPU time. If SecuritySpy crashes while video is being captured, at most only a few minutes of video will be lost.

Display camera information in video windows
If this option is turn on, camera information such as the camera name, mode, and recording status is displayed at the top of each camera image in video windows (but not in captured footage).

Display cameras at half frame rate in video windows
If this option is enabled, all cameras will display at half frame rate in all video windows. If you have many cameras and/or many video windows open at once, enabling this option may result in lower CPU usage (how much lower will depend on the resolution of your cameras and the speed of your computer's graphics card). This option affects display only; it doesn't affect video capture.

Set computer to full volume before playing sounds
If this option is enabled, the computer's main speaker volume will be automatically to maximum before playing sounds.

Get autio for cameras in active mode only
If you do not need to listen to the audio from cameras that are in passive mode, enable this option as it will reduce CPU usage.

Enable audio hiss reduction
When enabled, low-level audio will be silenced, eliminating hiss and background noise from microphones. This is useful for applications such as baby monitoring, where you may be listening to the audio at night, or when multiple cameras are playing audio at the same time.

Perform motion detection for cameras in active mode only
If this option is enabled, motion detection will not be performed for any camera in passive mode. This will reduce CPU usage while any cameras are in passive mode.

Allow automatic computer sleep
If you want SecuritySpy to operate continuously, the computer must be awake, therefore you should disable this option. If however you would like the computer

to sleep automatically when it is not being used (as per the settings in the Energy Saver system preference), enable this option.

Email error reports to...
Use this option to have error reports sent to an email address. Whenever an error occurs, an email that describes the error will be sent to the specified address. Click the Email settings button to specify settings for sending emails.

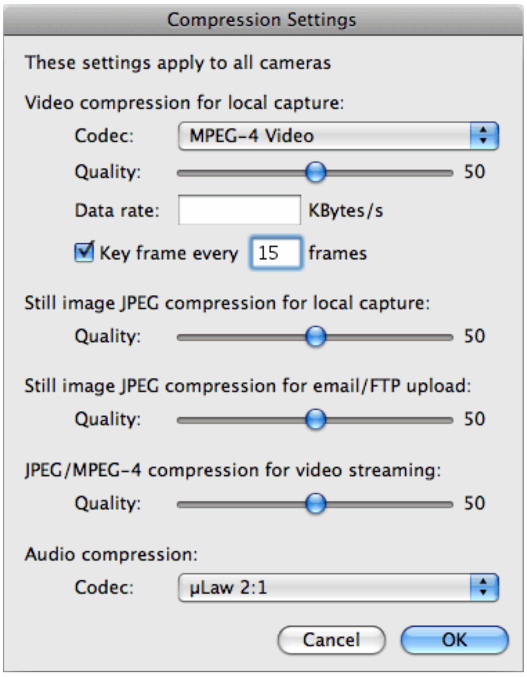
Password protected
You can set a password here that will be required by anyone attempting to change the mode of any camera (passive/active) as well as access settings or quit. Unfortunately it is not possible to prevent someone from manually switching off the computer but requiring a password provides a basic level of security.

Date ordering
Choose your desired ordering of the date. This is used whenever a date is displayed (for example in the timestamps in video frames and file names).

Maximum simultaneous FTP uploads
This setting defines how many uploads will be performed simultaneously to different FTP servers (multiple uploads to the same server will not be performed simultaneously, as there is no advantage in doing so).

Compression Settings

To set up the compression settings select *Compression settings* from the Settings menu. The Compression Settings window looks like this:



Compression Settings

These settings apply to all cameras

Video compression for local capture:

Codec: MPEG-4 Video

Quality: 50

Data rate: KBytes/s

☑ Key frame every 15 frames

Still image JPEG compression for local capture:

Quality: 50

Still image JPEG compression for email/FTP upload:

Quality: 50

JPEG/MPEG-4 compression for video streaming:

Quality: 50

Audio compression:

Codec: µLaw 2:1

Video compression for local capture
There are several video compression codecs available for you to choose from:

None: No compression - produces the highest quality video possible but with the largest file size. In most cases, Apple Intermediate Codec or high-quality JPEG is preferable because of the huge data sizes of uncompressed video files. Using no compression is not suitable for typical video surveillance applications.

Apple Intermediate Codec: produces very high quality video and is very quick to compress but with high data rates. This codec is useful if speed of compression is a priority, or as an alternative to no compression when the quality must be virtually lossless. It is not suitable for typical video surveillance applications.

JPEG: Produces high quality video and is fast to compress so performance with this codec is very good. JPEG is reasonably efficient in terms of file size, but not as efficient as MPEG-4 or H.264. JPEG is significantly quicker to compress than MPEG-4 or H.264.

MPEG-4: Produces high quality video at low data rates. It is reasonably quick to compress and will give good performance on a reasonably fast computer. This is the codec that is the best choice for the majority of video surveillance applications.

H.264: This codec produces the lowest file sizes out of all the standard QuickTime codecs, however it uses a lot of processing power (many times more than MPEG-4) due to it's very complex compression algorithm. It also uses vast amounts of memory: for a single camera at a video size of 640x480 for example, around 120MB of real memory is required. With multiple cameras or large video sizes, memory requirements can easily increase to many GB. If you use H.264 compression on a computer with too little memory, you will experience program or computer crashes. If this happens, switch to MPEG-4 instead.

MPEG-4 and H.264 support temporal compression. Depending on the content, video can have a high level of temporal redundancy, that is, very often one frame is similar to the last frame. Temporal compression exploits this redundancy to reduce the file size of the resulting video. Temporal compression works by using "key frames" at regular intervals, followed by several "delta frames". The key frames contain the complete video image; the delta frames contain only the portions of the image that have changed since the last key frame.

Images from surveillance cameras often have a high level of temporal redundancy because usually most of the image is constant and only a small portion is changing. Therefore the use of temporal compression will usually significantly decrease file sizes of captured video without significantly degrading quality. For MPEG-4 and H.264 you can enter a key frame rate in the Compression Settings window (key frame rates of 10 to 15 are typical).

Still image JPEG compression for local capture
Here you can set the compression quality for saving still JPEG images to the hard drive.

Still image JPEG compression for email/FTP upload
Here you can set the compression quality for sending JPEG image by email or uploading them to an FTP server.

JPEG/MPEG-4 compression for video streaming
Here you can set the compression quality for video streaming through the web server.

Audio compression
There are several audio compression codecs available for you to choose from, including:

None
No compression - this setting gives optimum quality and lowest processor usage. Since the data rate of audio is generally much lower than that of video, unless you need very small file sizes, no audio compression can be a good option. If you are not using audio compression, you should use a low sample rate and mono audio to minimise the data rate (these options are set independently for each device in the Audio Device Settings window available from the Camera Setup window).

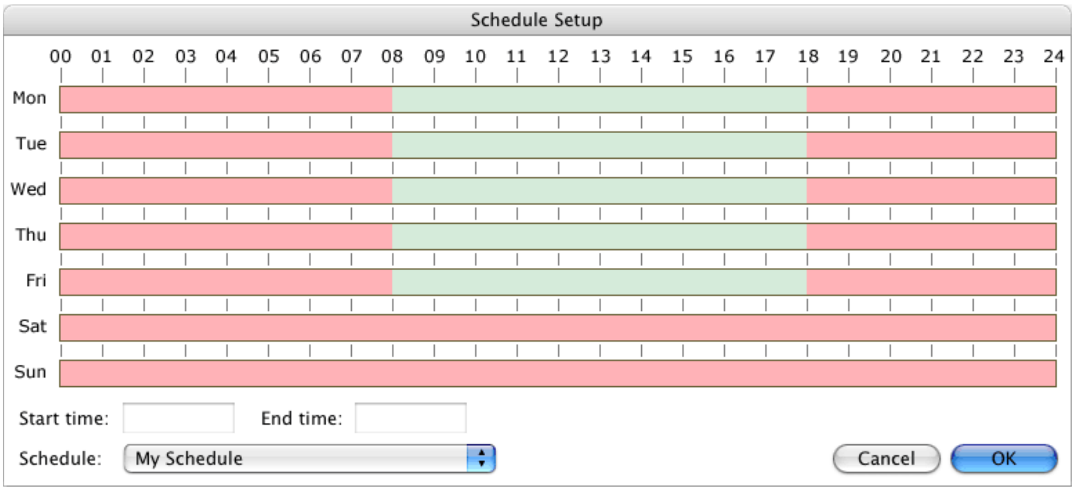
Apple Lossless
This gives quality equal to no compression (since it is a lossless codec), at roughly half the data rate, and is reasonably quick to compress.

μ-Law
This is the codec we recommend as the best in most circumstances. It is a very efficient codec designed specificallly for compressing speach quickly at a very low data rate (the data rate is fixed at just under 8 KB per second).

AAC
This produces high quality audio at very low data rates, but is the most processor-intensive of the available codecs.

Schedule Setup

This feature allows you to set up weekly schedules for activating cameras automatically. Any schedules created here are available to all cameras in the Camera Setup window. Select *Schedule setup...* from the Settings menu:



Start time:

End time:

Schedule: My Schedule

Times when cameras will be activated are represented as red "time objects". Each time object has a start time and end time, and defines a range of time when the camera will be automatically activated. Click and drag using the mouse to draw new time objects, or to move or edit existing time objects. To remove a time object, click on it and press the delete key on the keyboard. In the above example, the camera will be set to active mode from 18:00 to 08:00 on weekdays, and all weekend. SecuritySpy doesn't need to be running before the start time of a time object - if you launch it at any time marked in red on the schedule, all cameras using the schedule will be activated.

You can set up multiple schedules from the popup menu at the bottom of the window - in this menu there are options to add a new schedule, or rename or delete an existing schedule.

Web Server Setup

SecuritySpy features a built-in web server that allows you to view live video and audio, download captured footage, change settings and control the software, all from a remote location over a network (either a local network or the internet).

There are may ways to receive and play the live streams at the remote location (client side). The main methods are as follows (the first three use a web browser, the last three use other client software):

- "Server push" in a web browser: this is supported directly in the Netscape, Safari and FireFox web browsers, and is therefore the default streaming format in these browsers. It is efficient and offers high performance, although it uses JPEG compression so it most suited for streaming over a local network rather than the internet due to its high data rate. This method supports video only (no audio).

- Java applet in a web browser: a Java applet is a small application that runs within the browser on the client computer. Java is a cross-platform technology, so this method works in both Mac and PC browsers. It is efficient and you additionally have the option to choose the compression codec: either JPEG (good for viewing over a local network) or MPEG-4 (best for viewing over the internet, due to its lower data rate). Note that you will have to set Safari to 32-bit mode in order to use the Java applet in Safari on Mac OS X 10.6 and later (click here for more information). This method supports both video and audio.

- JavaScript in a web browser: JavaScript is a scripting language used in web browsers. This method is inefficient as it displays one frame at a time rather than a stream, however it is included for compatibility with browsers that don't support the above methods, such as some browsers on portable devices. This method supports video only (no audio).

- Using SecuritySpy as the client software: this offers the best streaming performance and viewing environment for live video and audio.

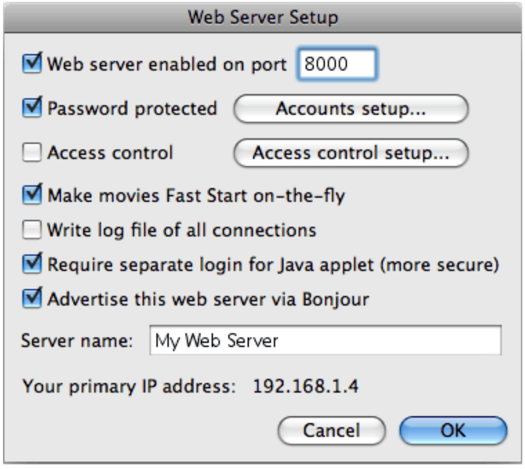
- Dashboard widget: this is simple and convenient, although offers a small viewing size and low frame rate. This method supports video only (no audio). Can also be used on Windows and Linux computers with the Kludget Engine software.

- PC software such as Webcam Watcher. You will have to set up Webcam Watcher with an appropriate HTTP request to receive video from SecuritySpy. See the Appendix 2 for the format of HTTP requests. Some PC software may also be able to receive the audio stream, but this depends on the capabilities of the particular PC software used.

When using a web browser, you will have a choice of which viewing method to use (server push, Java, JavaScript), and an explanation of the pros and cons of each method. To view captured footage, change settings and control SecuritySpy, you will need to use a web browser.

You can make any file available through SecuritySpy's web server by adding it to the Web folder (~/Documents/SecuritySpy/Web/) - to open this folder, select *Web* from the File menu. To customise the web interface, you can add your own "index.html" file in this Web folder and it will override the default index.html file.

To set up the Web Server feature, go to *Web server setup...* from the Settings menu:



Web Server Setup

☑ Web server enabled on port 8000

☑ Password protected

☐ Access control

☑ Make movies Fast Start on-the-fly

☐ Write log file of all connections

☑ Require separate login for Java applet (more secure)

☑ Advertise this web server via Bonjour

Server name: My Web Server

Your primary IP address: 192.168.1.4

Port number
This defines the TCP/IP port number that is used for connections. A port number represents an endpoint or "channel" for network communications and allows different applications on the same computer to use the network without interfering with each other. On Mac OS X, it is not possible to use ports below 1024 unless you are logged in as root (you can do this by enabling the root account using Netinfo Manager), however this is not advisable for security reasons. You access the web server from another computer on the same local network by typing the server's IP address and port number into a web browser, for example:

http://192.168.1.4:8000

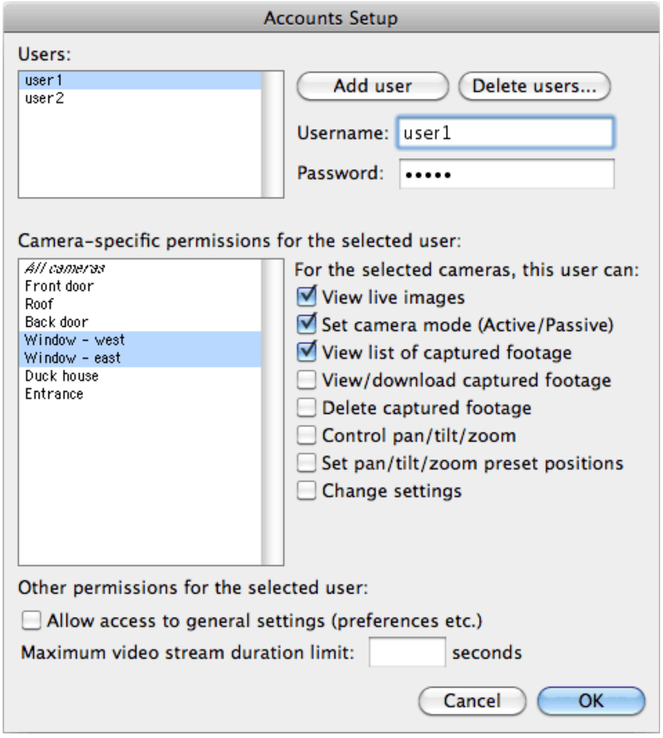
An alternative to using the IP address to access web servers running on your computer from within your local network, you can use the computer name, as set up in the Sharing system preference (provided you have not set up the Mac OS X firewall feature on the computer). So, if your computer name is set as "Mac Pro" for example, you could access SecuritySpy's web server from another computer using this address:

http://mac-pro.local.:8000

The advantage of using the computer name in this way is that you don't have to set up your computer with a fixed IP address on the local network - no matter what IP address it has, you can access it using the computer name. Note however that if you want to access your SecuritySpy web server from the internet, you will need to set up your computer with a fixed IP address on your local network in order to use port forwarding - see here for more information. ⇧

Password protected
If this option is on, anyone accessing the web server will be required to enter a username and password.

Click the *Accounts setup...* button to get this window:



Accounts Setup

Users:

user1
user2

Add user | Delete users...

Username: user1

Password: •••••

Camera-specific permissions for the selected user:

All cameras
Front door
Roof
Back door
Window - west
Window - east
Duck house
Entrance

For the selected cameras, this user can:

- ☑ View live images
- ☑ Set camera mode (Active/Passive)
- ☑ View list of captured footage
- □ View/download captured footage
- □ Delete captured footage
- □ Control pan/tilt/zoom
- □ Set pan/tilt/zoom preset positions
- □ Change settings

Other permissions for the selected user:

□ Allow access to general settings (preferences etc.)

Maximum video stream duration limit: seconds

Cancel | OK

For each user you can choose which features of the web server they are allowed to access. Such permissions can be selected on a per-camera basis. So, for example, a particular user may be allowed to view live images for certain cameras, but not all cameras.

To set permissions for a particular user, first select the user from upper list. Next, in the lower list, select the camera(s) for which you want to allow certain actions, and set the permissions accordingly. Select the *All cameras* option to set permissions that will apply to all cameras. This makes it easy to give a particular user a certain level of access for all cameras, while still being able to apply further permissions for individual cameras.

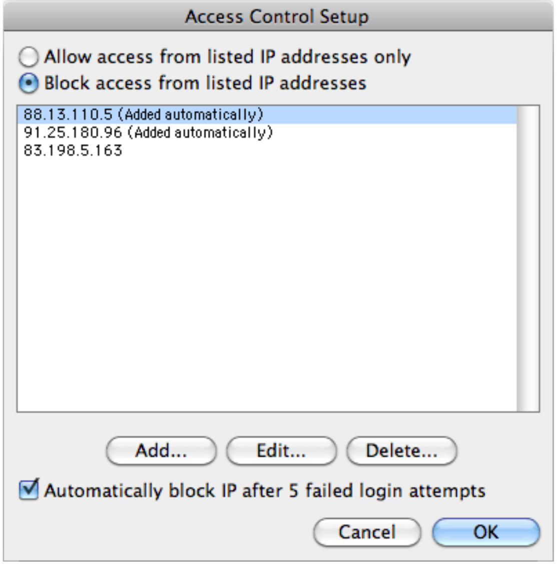
Enable the *Allow access to general settings* option to give a user access to general settings such as preferences and compression settings.

Note: the username is not case sensitive, but the password is. Both the username and password can be up to 31 characters in length and can contain any character.

Access control

This feature allows you to limit the access to the web server to specific IP addresses, or to ban specific IP addresses from access. This adds another level of security on top of password protection, and is especially useful when you have just a small group of people with fixed IP addresses who are allowed access to the web server, or when you want to automatically ban people when they repeatedly try to gain access without authentication.

Click the *Access control setup...* button to get this window:



Access Control Setup

○ Allow access from listed IP addresses only
● Block access from listed IP addresses

88.13.110.5 (Added automatically)
91.25.180.96 (Added automatically)
83.198.5.163

Add... | Edit... | Delete...

☑ Automatically block IP after 5 failed login attempts

Cancel | OK

There are two modes for this access control feature. If you select *Allow access from listed IP addresses only*, then only the IP addresses you specify in the list will be allowed access; connection attempts from any other IP addresses will be blocked.

If you select *Block access from listed IP addresses* (as in the above example), connection attempts from the listed IP addresses will be blocked, while connections from any other IP address will be allowed (but password protection still applies if you have enabled this feature).

If you enable the *Automatically block IP after 5 failed login attempts* option at the bottom of the window, after five consecutive failed connection attempts within five minutes (attempts to access the web server with incorrect login details), the IP address where the connection originated will be automatically added to the list, and no further connection attempts will be accepted from that IP address. This will stop someone from trying to guess your password by repeatedly attempting to access the web server.

You can use the wildcard character * in an address you specify to indicate a whole subnet. For example if you specify 192.168.1.*, this will allow or block access for the entire 192.168.1 subnet.

Make movies Fast Start on-the-fly

Normally, QuickTime movies have a movie resource at the end of the file (the movie resource holds necessary information about all the frames in the movie and therefore has to be written to the file last, after all the frames have been written). This works well when the movie is on a local drive because the movie resource is instantly accessible, however if the movie is being received from a slower source such as the Internet the whole movie must be downloaded before it can be played, which may take some time. In Fast Start movies, the movie resource is at the beginning of the file so that the movie can start to play before it has completely downloaded.

If this option is enabled the movie resource will be read from the end of the file and sent first, so the movie will be Fast Start when it is received by the client computer.

Write log file of all connections

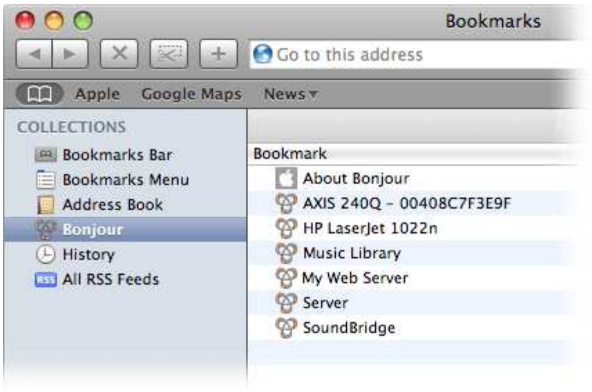
If this option is enabled, a text file called "WebLog.txt" will be written to the Web folder (~/Documents/SecuritySpy/Web/) - this file contains information about every connection to the web server. For each connection this log file will list the time, the client's IP address, and the requested page of each connection. Since this file is created in the Web folder it can be accessed through the web server using a browser just like any other file in the Web folder.

Require separate login for Java applet

A Java applet is used to display live video in certain web browsers (such as FireFox and Internet Explorer for example, but not Safari). This is a small application that runs within the browser, getting video from SecuritySpy and displaying it in the browser window. If this option is on, the Java applet will ask for login details if password protection is enabled for the web server. This means that you will have to enter login details twice: first for the web browser and then again for the Java applet. If this option is off, the login details you entered into the browser are passed to the Java applet, so the applet doesn't have to ask again. This is slightly less secure, but you will still have to enter login details to get access to the web server in the first place, so it generally isn't a security problem. It becomes a security problem only when you use the Java applet on one of your own web pages that doesn't have password protection (see Appendix 2 in this manual for more information on this).

Advertise this web server via Bonjour

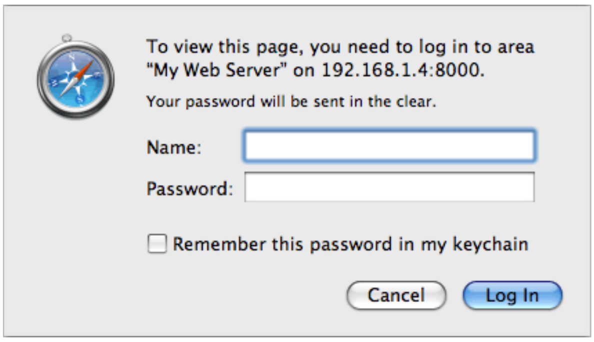
Bonjour is a method of "zero configuration" network setup, which makes it easy to attach and find devices on a network. To discover Bonjour-advertised network devices in Safari, you need to go to Bookmarks and click on the Bonjour section - the following image shows the Safari Bookmarks window which has discovered several devices on the network, including the SecuritySpy web server which is entitled "My Web Server":



SecuritySpy uses the server name text (see below) as its Bonjour name. Note that if you have enabled the Mac OS X firewall feature on the computer running SecuritySpy, this may prevent Bonjour from working properly. Therefore you may have to disable the firewall if you want to use Bonjour to connect to SecuritySpy servers. The firewall settings are accessible in the System Preferences.

Server name

You can enter any text here in order to customise the name of the web server. As well as being used as the Bonjour name (see above), this name gets displayed by a web browser when it requests authentication. For example, here is the message displayed by the Safari web browser when it connects to a password-protected server with the name "My Web Server" (other web browsers display similar messages):



To view this page, you need to log in to area "My Web Server" on 192.168.1.4:8000.

Your password will be sent in the clear.

Name:

Password:

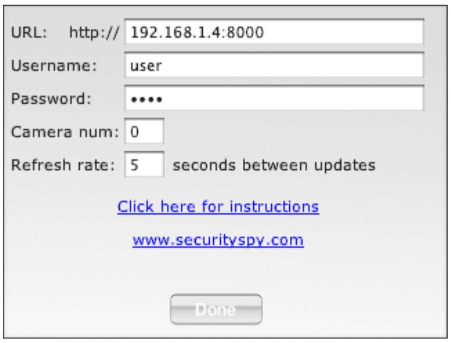
□ Remember this password in my keychain

Your primary IP address
This shows the computer's main IP address. From another computer on the local network, you enter the this IP address (along with the port number) into a web browser to connect to the web server. Your computer may have more than one network interface and therefore may have more than one IP address, in which case your web server is available to all attached networks at its respective IP addresses. Only the first (main) IP address is shown here. You can see all your network interfaces in the "Network" system preference. ⇧

Accessing SecuritySpy from the internet
If you want to access SecuritySpy from the internet, you will need to configure your router to allow this. In addition, if you have a dynamic IP address, you will need to use a dynamic DNS service to give yourself a static host name on the internet. For more details click here.

Dashboard Widget

SecuritySpy comes with its own Dashboard widget for easy remote viewing of video streams over a local network or the internet. Click here to download the widget - it will be installed automatically into your widgets folder and will be immediately available in Dashboard. The first time you load the widget it will be blank - you will first need to set up the settings so that it knows where the SecuritySpy web server is. To open the settings window click the info button (the "i" symbol in the bottom right hand corner of the widget). The settings look like this:



URL: http:// 192.168.1.4:8000

Username: user

Password: ••••

Camera num: 0

Refresh rate: 5 seconds between updates

Click here for instructions

www.securityspy.com

The widget has the following controls on the back:

- URL: the IP address or host name of the SecuritySpy server including any port number - in the above example it is "192.168.1.3:8000".
- Username/Password: if the SecuritySpy server has password protection you need to enter the username and password here.
- Camera num: to see the camera numbering open the *Device map* window in SecuritySpy on the server (from the Window menu).
- Refresh rate: the frequency at which you want the image to update (the image will be refreshed only when the widget is actually visible).

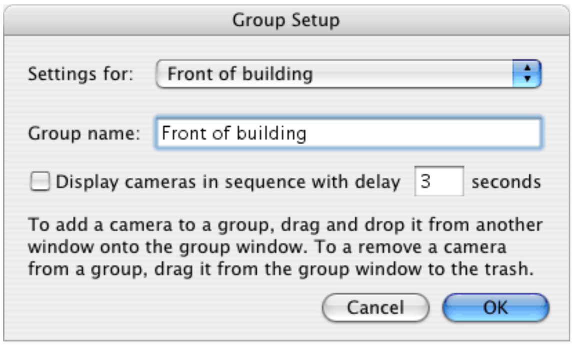
If, instead of the image, you get a question-mark icon, it means that the widget wasn't able to get the image. Check the URL, username/password and camera number settings to make sure they are correct.

In order to view several different cameras at the same time, you can open one instance of the SecuritySpy widget for each camera you want to view. The widget can be used without restriction on as many computers as you like.

This widget can also be used on Windows and Linux computers with the Kludget Engine software.

Group Setup

When you have many cameras, the main video window can get cluttered and difficult to view, so it is useful to set up groups of cameras that can be displayed in separate windows. For example, if you have four cameras at the front of your building and four cameras at the back, you can set up two groups: "Front of building" and "Back of building". Each group contains the four appropriate cameras, and can be displayed independently in its own window. To set up groups, select *Group Setup...* from the Settings menu:



Settings for: Front of building

Group name: Front of building

□ Display cameras in sequence with delay 3 seconds

To add a camera to a group, drag and drop it from another window onto the group window. To a remove a camera from a group, drag it from the group window to the trash.

From the menu at the top of the window, you can add a new group or delete an existing one. By default, all cameras are displayed at the same time in the group window, but if you enable the *Display cameras in sequence* option, then each camera will be displayed in sequence with the delay you specify.

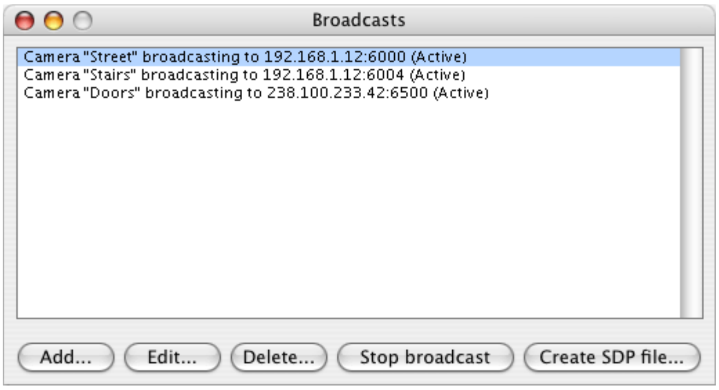
Once you create a group, click the OK button in the above window and the new group window will be opened. To add a camera to a group window, drag it from another video window or from the Camera Status window to the group window. To remove a camera from a group window, drag it from the group window to the trash in the Dock.

If a group window is closed, you can open it again from the *Group video windows* section of the Window menu.

Broadcasting

SecuritySpy has broadcasting features for streaming real-time video over a network, using the standard Real-Time Transport Protocol/Real-Time Streaming Protocol (RTP/RTSP). The video can be viewed using Apple's QuickTime Player application, or sent to Apple's QuickTime Streaming Server (QTSS) for large-scale delivery. The use of compression such as MPEG-4 makes SecuritySpy's broadcasting a powerful and efficient method of real-time content delivery. Multiple simultaneous streams from multiple cameras are supported, as well as both unicast and multicast streams. You can even create multiple simultaneous streams from the same camera, with different compression and bandwidth settings.

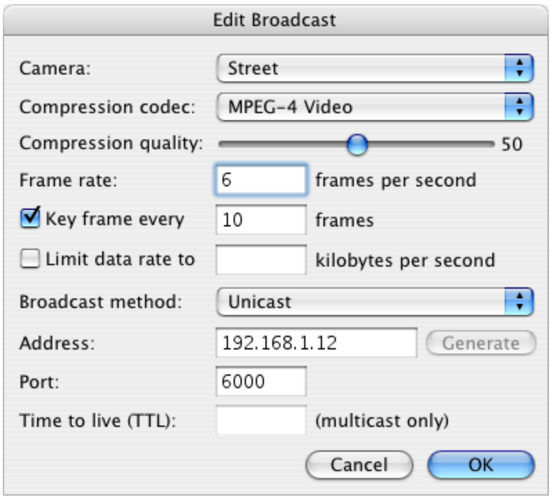
Streams are created and managed from the Broadcasts window, available by selecting *Broadcasts* from the Window menu:



Camera "Street" broadcasting to 192.168.1.12:6000 (Active)
Camera "Stairs" broadcasting to 192.168.1.12:6004 (Active)
Camera "Doors" broadcasting to 238.100.233.42:6500 (Active)

This window lists all current broadcasts, showing the camera name and the destination IP address and port number. In the above example, all three broadcasts are active - to stop a broadcast, select it in the list and click the *Stop broadcast* button (this button is also used to start broadcasts that have been stopped). To delete a broadcast, select it in the list and click the *Delete...* button.

To add a new broadcast, click the *Add...* button or to edit an existing broadcast, select it in the list and click the *Edit...* button - this window will appear, allowing you to add or edit a broadcast:



Edit Broadcast

Camera: Street

Compression codec: MPEG-4 Video

Compression quality: 50

Frame rate: 6 frames per second

☑ Key frame every 10 frames

□ Limit data rate to kilobytes per second

Broadcast method: Unicast

Address: 192.168.1.12

Port: 6000

Time to live (TTL): (multicast only)

The settings are as follows:

Camera
Select the camera from which you want to broadcast live video.

Compression codec
This is the compression type used for the video stream. MPEG-4 is the most efficient and will give you the best quality at the lowest data rates of all the codecs currently available.

Compression quality
The higher the quality the higher the data rate of the stream. A quality of 50 typically represents a reasonable balance between image quality and data rate.

Frame rate
The frame rate of video sent on this broadcast.

Key frame every...
If the compression codec you select supports temporal compression, you should specify a key frame rate here. Using temporal compression will significantly reduce the data rate of the video stream. A key frame rate of between 10 and 20 is typical.

Limit data rate to...
Use this setting if you require a particular data rate for the video stream. This is useful if you are streaming over the internet and have only a limited bandwidth available. If you use this setting, the compression quality is automatically adjusted in order to achieve the specified data rate.

Broadcast method
There are two broadcast methods available: unicast and multicast. See below for more information on this.

Address
This is the address the stream is sent to. In unicast mode, this defines the client computer's address. In multicast mode this defines the multicast address. This multicast address can be generated randomly by clicking the *Generate* button or, if you are streaming over the internet, you may have to use a particular multicast address assigned to you by your service provider.

Port
The port number for the stream. Each broadcast must be on a unique port.

Time to live (TTL)
This setting specifies the number of times a stream can be passed from one router to another before the stream is no longer transmitted. The value can be any number between 1 and 255. A value of 1 reaches client computers on the local area network. The larger the number, the farther the multicast packets will travel.

How to stream video

There are two broadcast methods: unicast and multicast. In unicast mode, each client requests its own stream from the server. As more clients request the stream, more sessions will become active on the server. As the number of sessions grows, the load on the server and the bandwidth required to support these clients will increase accordingly.

In multicast mode, one stream is sent that can be received by multiple clients. The advantage of multicast is that clients can "tune in" to this single stream with no extra load on the server or increase in required network bandwidth. This method allows for very efficient distribution of video to a large number of clients, however it requires networks that support multicasting.

A client computer connects to a stream broadcast by SecuritySpy through the use of an "SDP" file, which contains information about a broadcast. Select a broadcast from the list, click the *Create SDP file...* button, and save the file somewhere (to your desktop for example). You need to transfer this file to the client computer to be used by the software that is to receive the stream (such as QuickTime Player, QuickTime Streaming Server (QTSS), or some other software that can receive RTP/RTSP streams). The software on the client computer will use the information contained in the SDP file to connect to the stream.

Depending on your audience size and broadcast method, you may or may not need to use Apple's QuickTime Streaming Server (QTSS) software.

If you are streaming unicast to a single client, you don't need QTSS: the client computer can connect directly to SecuritySpy to receive the stream by opening the SDP file in QuickTime Player.

If however you are streaming unicast to multiple clients, you will need to use QTSS. Place the SDP file created by SecuritySpy into the /Library/Quicktimestreaming/Movies/ folder on the computer running QTSS. The stream will then be available to users by connecting to QTSS using QuickTime Player, by using the following URL:

rtsp://<QTSS address>/<SDP file name>.sdp

For example, if the address of the computer running QTSS is 192.168.1.1 and the SDP file name is "mystream.sdp", the URL would be:

rtsp://192.168.1.1/mystream.sdp

If you are streaming multicast to users on a local network or the internet, you don't need to use QTSS, however each client computer will need a copy of the SDP file in order to receive the stream. A more convenient setup is to use QTSS, in which case each client will simply connect to a URL (same as above in the unicast case).

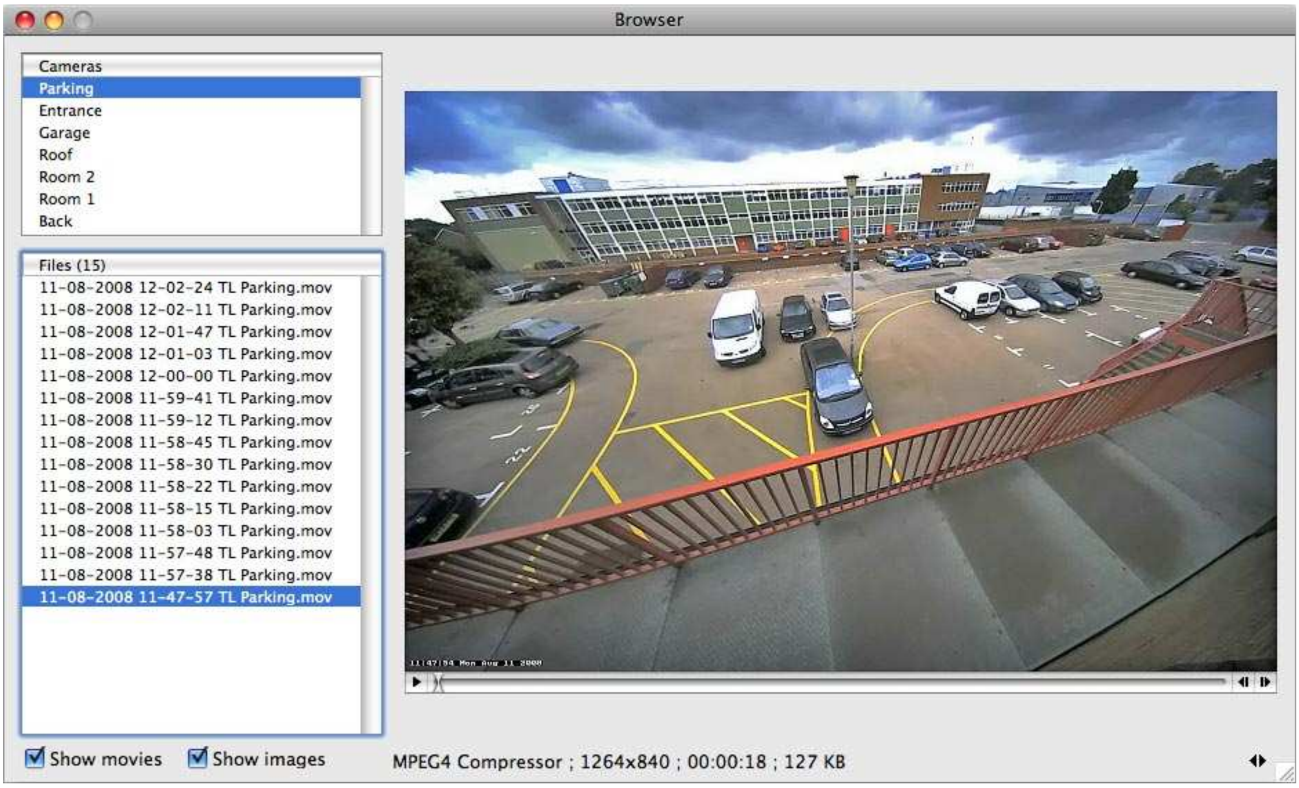
Broadcasting multicast streams over a local network requires that you have a network that supports multicasting - if you are unsure about your network equipment, contact your equipment manufacturer/supplier to find out if multicast is supported and how to enable it.

Broadcasting multicast streams over the internet requires a connection to the multicast backbone ("MBone"). Some internet service providers offer this service, but not all - check with your service provider if you are unsure. Client computers doesn't need to have access to the MBone to receive your multicast stream: if they don't, they will receive a unicast stream from the closest edge router (ie the last router in the chain that supports multicast).

It is possible to run both SecuritySpy and QTSS on the same computer - for a small audience size (100 or so) this normally yields acceptable performance. For best performance or for larger audiences, you should use two separate computers: one running SecuritySpy and the other running QTSS.

Browser

SecuritySpy has a Browser feature that allows you to view and manage captured footage. Choose *Browser* from the Window menu to open the Browser:


Browser
Cameras
Parking
Entrance
Garage
Roof
Room 2
Room 1
Back
Files (15)
11-08-2008 12-02-24 TL Parking.mov
11-08-2008 12-02-11 TL Parking.mov
11-08-2008 12-01-47 TL Parking.mov
11-08-2008 12-01-03 TL Parking.mov
11-08-2008 12-00-00 TL Parking.mov
11-08-2008 11-59-41 TL Parking.mov
11-08-2008 11-59-12 TL Parking.mov
11-08-2008 11-58-45 TL Parking.mov
11-08-2008 11-58-30 TL Parking.mov
11-08-2008 11-58-22 TL Parking.mov
11-08-2008 11-58-15 TL Parking.mov
11-08-2008 11-58-03 TL Parking.mov
11-08-2008 11-57-48 TL Parking.mov
11-08-2008 11-57-38 TL Parking.mov
11-08-2008 11-47-57 TL Parking.mov
11:47:54 Mon Aug 11 2008
☑ Show movies
☑ Show images
MPEG4 Compressor ; 1264x840 ; 00:00:18 ; 127 KB

The Browser has two modes: single-file and multi-file. In single-file mode, the Browser displays a list of captured files for the camera(s) you select, as in the picture above. In multi-file mode, the Browser displays a single 24-hour long movie for each day that contains all footage captured by the camera(s) you select, allowing you to play back synchronised footage from multiple cameras. You switch between these two modes from the Browser Settings window, available from the Browser menu (see below).

Controlling movie playback
To play a movie, click the play button in the bottom left hand corner of the movie. To the right of this play button is the movie controller that allows you to move forwards and backwards in the movie. The arrows in the bottom right hand corner of the movie allow you to step forwards and backwards by one frame at a time (the right and left arrow keys on the keyboard do the same thing). The icon with the arrows in the bottom right corner of the Browser window is a mouse-operated scrub control: click in this control and drag the mouse left and right to scrub backwards and forwards in the movie (each pixel moved by the mouse advances the movie by one second). Hold the alt key on the keyboard to slow down the scrub speed for very fine control (holding down the alt key makes the

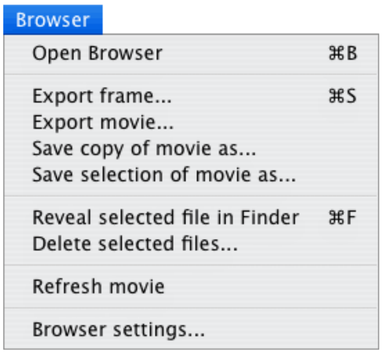
scrub speed 30 times slower).

The Browser also supports "JKL" keyboard shuttle controls: pressing "L" causes the movie to speed up in the forward direction by a factor of 2; "J" causes the movie to speed up in the reverse direction by a factor of 2; "K" pauses the movie playback. If you press L while holding K, the movie will step forwards one frame; if you press J while holding K, the movie will step backwards one frame.

Single-file mode
In this mode, there are two lists on the left of the window: one that shows all available cameras and another that shows a list of files. Select one or more cameras in the top list, and all captured files for the selected cameras will be shown in the lower list. Click on any file in the lower list to display it. You can use the movie controller to play a single movie, or click the play button above the file list to play through all files in sequence. Movies that are currently being captured appear in the list in italics, and every time you click on such a movie in the list, it will update to reflect the changes that may have occurred since the last update.

Multi-file mode
In this mode, there is only one list: the camera list in the top left of the window. There is also a date control that allows you to select a particular day. Select one or more cameras from this list (hold the shift key down to select multiple cameras) to display all footage captured by the cameras for the day you select. All captured movies files (both timelapse and motion-triggered) are collated into a single movie covering the whole day.

The Browser menu
The Browser menu at the top of the screen contains the following functions:



Export frame...
Exports an image file of the current movie frame. The image file can be saved in a variety of formats (including TIFF, JPEG and PNG) - for most purposes JPEG is a good choice as it offers good quality at low data sizes. The quality is adjustable, so choose high quality if this is important.

Export movie...
Exports the current movie as a new file, allowing you to change the compression format and other parameters (such as video size and frame rate).

Save copy of movie as...
Saves an exact copy of the current movie as a new file.

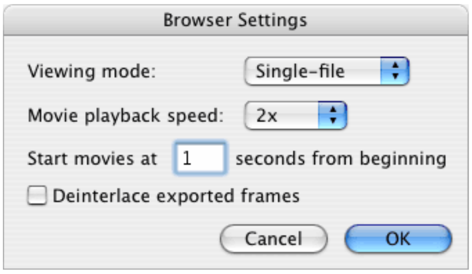
Save selection of movie as... (single-file mode only)
You can select a portion of the movie by holding the shift key on the keyboard and dragging the movie controller. Once you have set a selection, you can use this command to save the selection as a separate movie.

Reveal selection in Finder (single-file mode only)
Show the current file in the Finder.

Delete selected files... (single-file mode only)
Permanently deletes the files that are currently selected in the file list.

Refresh movie
Reloads the movie from disk. Useful when you are viewing a file that is currently being captured, to update the Browser display with the latest data.

Browser settings...
Shows the browser settings window:


Browser Settings

Viewing mode: Single-file

Movie playback speed: 2x

Start movies at 1 seconds from beginning

☐ Deinterlace exported frames

Viewing mode
Allows you to choose between single-file and multi-file viewing modes.

Movie Playback speed

Use this option to play the movies back at a multiple of their normal speed. This is useful for saving time while viewing lots of movies.

Start movies at x seconds from beginning
If you use this option movies will be automatically started a number of seconds from the beginning. This is useful when you are using the pre-capture feature, since in this case the motion event that triggers recording occurs some time after the start of the movie.

Deinterlace exported frames
This is useful for exporting frames from full-size analog video to remove any interlacing artifacts, however this also reduces the amount of detail in the image.

Network Devices

These devices connect to the computer over a wired or wireless ethernet network. There are two kinds of network device: network cameras and network video servers. They are similar in the way that they send video over the network, but whereas a network camera is a self-contained (often all-digital) unit, a network video server has one or more analog inputs for connecting analog cameras.

Network devices can connect over long distances, ethernet wiring is relatively cheap and easy to set up, and a large number of devices can be used simultaneously (the number of devices is only limited by network bandwidth, speed of computer, and performance required). Network devices generally provide high quality video and good performance.

SecuritySpy supports devices that can send video in "multipart JPEG" format (sometimes called "server push" or "motion JPEG"), as well as those that can send individual JPEG images. For a comprehensive list of supported network devices, click here.

You set up network devices in the Video Device Setup window.

Connecting to network devices

When you open SecuritySpy it will attempt to connect to all network devices. While the connection is in progress you will see a flashing icon like this:

⇄

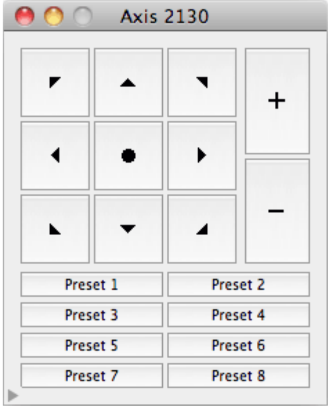
If the connection fails for any reason, the icon will change to a red cross:

✕

Connections can fail for a number of reasons such as an incorrect username/password, incorrect IP address, or network problem. If a connection fails, check the error log (select *Open error log* from the File menu) as it should give you more information about what the problem is. SecuritySpy will repeatedly attempt to connect at 30 second intervals - this will ensure reliability if there is just a temporary problem with the network or device.

Pan/Tilt/Zoom (PTZ)

SecuritySpy supports PTZ control for certain network devices (see this list for more details). To open the PTZ control window for a particular camera, select it from the Window menu or hold down the option (alt) key and double-click on the camera's video display. The PTZ window looks like this:



The arrow buttons control pan and tilt, the + and - buttons control zoom and the circle button resets the device to the "home" position. If a particular function is not supported by the device the corresponding button will not be available in the above window (for example some devices support pan and tilt but not zoom).

If your camera supports preset positions, the eight lower buttons will also be available. To save the current position as one of the presets, hold the <alt> key on the keyboard and click one of the preset buttons. To specify names for the preset positions, click the small disclosure triangle in the bottom left hand corner of the window to reveal these settings.

When a PTZ window is at the front, it be controlled using the numeric keypad on the right of standard keyboards: 1 on the keypad corresponds to down-left; 2 corresponds to down etc. These keyboard controls also work in video windows - simply click once on the video image of the camera you want to control and you can use these keypad commands to control it.

In addition, if you press the Caps Lock key on the keyboard, you can control the pan and tilt of the camera by clicking directly in the video image of a particular camera - a click in the right hand side of the video image will move the camera right etc.

Note: devices often require username/password details for controlling PTZ so make sure these have been entered correctly in the Video Device Setup window. Authentication details required for simply viewing video may not be the same as those required for controlling PTZ.

Using SecuritySpy as a video server

It is possible to use one computer running SecuritySpy as a network video server, sending video to another computer running SecuritySpy. In this way you can set up a distributed video surveillance system with multiple computers over an ethernet network, each with their own local video input devices, all sending video back to a central computer that records and stores all the video.

One advantage of this approach is its sheer flexibility when it comes to numbers and types of video input device you can use. For example, in a large organization with several departments, each can have a video server with one or more local video input devices (a built-in iSight camera for example), sending video back to a central control room, possibly over long distances, using an ethernet network. Depending on the requirements for each department, low-spec computers may be used for the video servers, therefore enabling a low cost and very flexible solution compared to purpose-built hardware video servers. Another advantage of such a system is that all the motion detection processing is done on the remote computer, which sends back this information to the central computer, thus reducing the processor load on the central computer and resulting in better performance (note that with such a setup the "central computer" is not always well defined; since each computer is running SecuritySpy each has the same capabilities. For example, one computer could record some of its cameras locally while sending the video from other cameras to a different computer for display and capture somewhere else - this capability makes the setup very flexible).

Another use for this feature is remote viewing of cameras over a local network or the internet. Although this can be done using a web browser, you will find that using SecuritySpy gives you better performance and a nicer interface. Of course, you can only do this on a Mac whereas web browsers are available for other platforms (Windows and Linux).

To set up one computer (the server) to transmit video to another computer (the client), do the following:

On the server computer
• Turn on SecuritySpy's web server feature in the Web Server Setup window. If you have set a static address for the server computer, note the server's IP address and port number as displayed in this window. If you haven't set up the server with a static IP address, make sure that the "Advertise this web server via Bonjour" setting in the Web Server Setup window is enabled so that the client computer can automatically find the server. Give the server a name in the *Server name* text box.

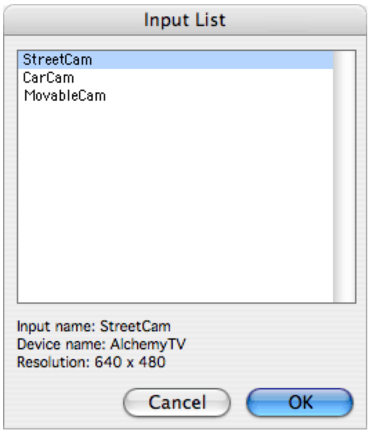
On the client computer
• Go to the Video Device Setup window (under the Settings menu) and add a new network device.

• If the server has a static IP address, enter enter it in the *Address* field; otherwise click the Bonjour menu to the right of the *Address* field and select the server computer, which should have been found automatically. Select *SecuritySpy* from the *Device type* popup menu, and select an input number corresponding to a camera on the server computer (each camera connected to SecuritySpy has a unique number - this is the number you enter in the Video Device Setup window of the client computer as the *Input number*).

• If you have enabled password protection for the web server you need to enter your username and password on the client computer.

• You have three options for the video compression codec used for the video stream: JPEG, MPEG-4, and Apple Intermediate Codec (AIC). JPEG is a good general-purpose codec due to its high quality at reasonable data rates, and relatively quick compression and decompression. MPEG-4 is ideal for transmission over a low-bandwidth connection such as the Internet, as it offers much lower data rates than JPEG, however it uses more CPU time to compress and decompress. AIC is the fastest and highest quality of all three codecs, therefore it is a good choice for transmission over a local network, especially if the video is to be recompressed on the client computer, however it uses significantly more network bandwidth than JPEG and MPEG-4. Also, AIC is not part of the system software; it is installed by Apple's iLife suite, and both the client and server computers need AIC installed in order for SecuritySpy to use it.

To find out which input number corresponds to which camera on the server computer, click the *Get input list* button in the Video Device Setup window on the client computer. The client will ask the server for a list of available cameras and will display the list in a window, like this:


Input List

StreetCam
CarCam
MovableCam

Input name: StreetCam
Device name: AlchemyTV
Resolution: 640 x 480

This window lists all available cameras on the server computer. To choose a particular camera, select it in the list and click the OK button - the input number in the Video Device Setup window will then be set for you. If instead of this list you get an error message, make sure that you have correctly entered the IP address and port number of the server.

In the above case, the camera "MovableCam" is actually a network camera attached to the server. If the client requests video from this input, it will get video from the network camera, retransmitted through the server computer. Having multiple users access the network camera through another computer running SecuritySpy instead of directly from the camera itself in this way reduces the load on the camera and therefore may increase performance, and also the number of users who can then access the camera is not restricted by the camera's limit. If you do this it is advisable to enable the *Don't recompress images from this device* option in the Video Device Setup window on the server computer, otherwise video will be recompressed as it is retransmitted through the server, which reduces quality and uses more of the server's processing power. If this option is enabled, the server computer retransmits the video in its raw form, preserving the original quality.

Setting up SecuritySpy for autonomous operation

Here are the steps required to set up your video surveillance system to operate autonomously:

Set SecuritySpy to open whenever the computer starts up
Open System Preferences and click on *Accounts*. Click on your account and click the *Startup Items* tab on the right hand side of the window. Drag the SecuritySpy application into the list of startup items. Alternatively, open SecuritySpy and click and hold the mouse button on the SecuritySpy icon in the Dock. From the menu that pops up, select *Open at Login*.

Set the computer to never sleep
Open System Preferences and click on *Energy Saver*. Click on the *Sleep* tab and where it says *Put the computer to sleep when it is inactive for*, drag the slider all the way to the right, where it says *Never*. It is also recommended for best performance to disable the setting *Put the hard disk to sleep when possible*. Display sleep should be enabled to save power and prevent monitor "burn-in".

Set the computer to restart after a power failure
Open System Preferences and click on Energy Saver. Click on the *Options* tab and enable the setting labeled *Restart automatically after a power failure*.

Enable remote monitoring and administration
See the Web Server Setup settings in this manual for details.

Close all video windows
Video windows are not required if there is no one operating the computer, and they will use CPU time resulting in lower performance.

Optimising Performance

Using multiple cameras simultaneously involves moving, calculating and storing large amounts of data. To get the most out of your computer you should:

- In the Options section of the Energy Saver System Preference, set the *Processor Performance* setting to *Highest*. This setting is not available on all computers, but where it is, it should speed up the computer significantly.
- Disable sleep mode in the Energy Saver System Preference. SecuritySpy cannot operate when the computer is in sleep mode.
- Disable hard disk sleep in the Energy Saver System Preference if you get movie files with a long pause at the beginning. If the hard disk is sleeping, frames will be lost at the start of the next movie capture due to the time taken to spin up the disk. SecuritySpy automatically disables hard disk sleep when any camera that is set to capture video on motion is active, but if there are periods when there are no cameras active the disk(s) may spin down.
- Enable the *Display cameras at half frame rate* option in the Preferences, and close the video windows when you are not using them. Display of video to the screen can take a significant amount of CPU time and can therefore result in lower capture performance. When resizing video windows they will snap to certain optimum sizes - this will result in better performance than previewing at odd sizes.
- Enable the *Disable motion detection for cameras in passive mode* option in the Preferences.
- In the Video Device Setup window, specify the lowest frame rate you require for each device. If a device is sending frames faster than they need to be recorded, CPU time is wasted processing these extra frames.
- If you are using a network device and don't require very low data rates for captured video (as provided by a codec such as MPEG-4 or H.264), enable the *Don't recompress images from this device* option in the Video Device Setup window. This causes the video to be captured in the raw JPEG format directly from the device, which ensures best performance as well as best quality (although certain features then won't be available - click here for more information).
- Quit all applications other than SecuritySpy.
- A fast hard disk is likely to improve performance when capturing video, depending on the number of cameras capturing simultaneously and the video compression settings used. With high ratio compression such as MPEG-4 performance is most limited by processor speed, whereas with no compression performance is most limited by hard disk speed.

Support / Help

For information about how to choose, install and set up the hardware of your video surveillance system, see the SecuritySpy installation manual.

For up to date troubleshooting and help please see the SecuritySpy online help pages.

If your question is not answered in the online help pages, please email it to support@bensoftware.com.

Click here for an online calculator that gives a guide to the specification of computer required for a particular setup.

Appendix 1: Error codes

When SecuritySpy encounters an error it will display an error code, or write one to the log file. Click here for a list of Apple-defined error codes.

There are also the following SecuritySpy error codes:

800 - The operation timed out
801 - Data from network device not as expected
802 - Error initializing a network device
803 - Invalid network device
804 - The network device unexpectedly closed the connection
805 - Response from FTP server not as expected
806 - Network device has not yet initialised
807 - Invalid camera number
808 - Data size from local device not as expected

Appendix 2: Built-in web server HTTP interface

This section describes the HTTP requests that SecuritySpy's built-in web server understands. You can use this information to include images and video in your own web pages, or to set up remote viewing software such as Webcam Watcher.

Still JPEG image

http://<*servername*>/++image?cameraNum=<*camera*>[&width=<*width*>][&height=<*height*>][&quality=<*quality*>]

<*camera*> is the number of the camera, as displayed in the Device Map window (select *Show device map* from the Window menu)
<*width*> is the width of the image in pixels (this parameter is optional)
<*height*> is the height of the image in pixels (this parameter is optional)
<*quality*> is the compression quality in the range 0 to 100 (this parameter is optional)

For example:

http://192.168.1.1/++image?cameraNum=1&width=640&height=480&quality=50

Multipart-JPEG "server push" video stream

http://<*servername*>/++video?cameraNum=<*camera*>[&width=<*width*>][&height=<*height*>][&quality=<*quality*>][&req_fps=<*fps*>]

<*camera*> is the number of the camera, as displayed in the Device Map window (select *Show device map* from the Window menu)
<*width*> is the width of the image in pixels (this parameter is optional)
<*height*> is the height of the image in pixels (this parameter is optional)
<*quality*> is the compression quality in the range 0 to 100 (this parameter is optional)
<*fps*> is the FPS of video that SecuritySpy will attempt to send (this parameter is optional)

For example:

http://192.168.1.1/++video?cameraNum=1&width=640&height=480&quality=50&req_fps=10

Audio (encoded as G.711 μ-law)

http://<*servername*>/++audio?cameraNum=<*camera*>

<*camera*> is the number of the camera, as displayed in the Device Map window (select *Show device map* from the Window menu)

For example:

http://192.168.1.1/++audio?cameraNum=1

Java applet

To use SecuritySpy's Java applet in your own web page for display of live video, use this HTML code:

```
<applet code="CamViewerApplet" archive="CamViewerApplet.jar" width=640 height=480>
<param name="CameraNum" value="1">
</applet>
```

In this example, live images from camera 1 will be displayed at a resolution of 640x480. You will need to substitute your own values for width, height and CameraNum as appropriate to your setup (to find out which camera corresponds to which camera number, select *Show device map* from the Window menu). To make your web page available through SecuritySpy's built-in web server, place it in the Web folder (~/Documents/SecuritySpy/Web/). If you want to put your web page on a different server, you need to include an additional "codebase" parameter that describes the location of the SecuritySpy web server, like this:

```
<applet codebase="http://myServer.dyndns.org/" code="CamViewerApplet" archive="CamViewerApplet.jar" width=640 height=480>
```

If you have enabled password protection for SecuritySpy's web server, the Java applet will ask for authentication details before displaying images. To avoid this, do the following: in the Web Server Setup window, disable the *Require separate login for Java applet* option. Log on to the SecuritySpy web server using a web browser, select *Java applet* as the viewing method, and click the *Go* button to display the live images. Then use your browser to view the HTML source code for the live images page (in Safari, this option is in the View menu). You will notice an extra "Auth" parameter in the code for the Java applet, for example:

<param name="Auth" value="YmVuOnRlYXBvdA==">

If you include this parameter in your own web page, the applet won't need to ask for authentication details. Beware though that if your web page is not protected by a password, anyone can access it and see the authentication details. Therefore, to minimise this security risk, you should create a separate account for the SecuritySpy web server that has limited permissions (live image access only for example) and use this to log on to SecuritySpy in order to get the Auth parameter.

The default compression used in the Java applet is JPEG. JPEG is high quality and fast to compress and decompress so it is a good option for viewing video over a local network, since bandwidth is not a problem. When viewing video over the internet however, using MPEG-4 compression will give much better frame rates, as it is a much more efficient codec. To tell the applet to use MPEG-4 compression, add this line of code:

<param name="Codec" value="mp4v">

Setting a camera to Active or Passive mode

http://*<servername>*/++ssControlActiveMode?cameraNum=*<camera>*
http://*<servername>*/++ssControlPassiveMode?cameraNum=*<camera>*

<camera> is the number of the camera, as displayed in the Device Map window (select *Show device map* from the Window menu)

For example:

http://192.168.1.1/++ssControlActiveMode?cameraNum=1

Additional features

The request "++scripts" displays a page showing all the available scripts: clicking on one opens it on the server computer. Likewise the request "++sounds" displays a page showing all the available sounds: clicking on one plays it on the server computer. Scripts are stored in the ~/Documents/SecuritySpy/Scripts/ folder; sounds are stored in the ~/Documents/SecuritySpy/Sounds/ folder - you can add your own scripts and sounds to these folders to make them available in SecuritySpy. To open the Scripts or Sounds folder in the Finder, select it from the list of folders in the File menu).

More information

Full specifications of the HTTP interface to SecuritySpy's web server can be found here.