



# Security Spy

Manual de Usuario  
Cubre la versión 4.2.14

Escrito por Ben Bird – Ben Software Ltd  
Traducido por LCM Security México

# Contenido

- Introducción
- Iniciando
- Preferencias
  - General
  - Cámaras
  - Grupos
  - Planificación
  - Compresión
  - Email
  - Uploads
  - Web
- Browser
- Dispositivos de red
  - Pan/Tilt/Zoom (PTZ)
- SecuritySpy como software de visualización remota
- Configuración de SecuritySpy para funcionamiento autónomo
- Optimización del rendimiento
- Soporte y ayuda

# Introducción

SecuritySpy es un software de videovigilancia CCTV para Mac.

Con funciones como detección de movimiento, alertas por correo electrónico y iPhone, compatibilidad con ONVIF y control de panorámica / inclinación / zoom, SecuritySpy le permitirá configurar un sistema de CCTV completo y eficaz para su negocio o su hogar de forma rápida y sencilla.

SecuritySpy puede convertir cualquier Mac en una estación de videovigilancia (por ejemplo, con múltiples pantallas grandes en una sala de control de seguridad). También es ideal para la operación remota autónoma, ya que tiene una interfaz web segura con todas las funciones que le permite acceder y controlar su sistema de vigilancia desde Internet o una red local. Y, como software de Mac, es tan elegante y fácil de usar como cabría esperar, con una interfaz de usuario cuidadosamente diseñada. Si está construyendo un sistema de videovigilancia desde cero, todo lo que necesita es SecuritySpy, una Mac y algunas cámaras IP. Si tiene un sistema existente que usa cámaras analógicas, SecuritySpy puede usarlas junto con cámaras IP más modernas, lo que le permite realizar la transición a un sistema digital de última generación.

La flexibilidad de SecuritySpy le permitirá configurar un sistema que se adapte a sus necesidades individuales, ya sea que desee una sola cámara o cien.

Este manual describe cómo utilizar el propio software SecuritySpy. Para obtener información sobre cómo elegir, instalar y configurar el hardware de su sistema de CCTV, consulte el Manual de instalación de SecuritySpy.

## Las principales características de SecuritySpy son:

Muestra y captura video de varias cámaras simultáneamente.

Admite dispositivos de entrada de audio y video compatibles con Mac.

Admite cámaras de video IP (ONVIF, Axis, Sony, Canon, D-Link, Dahua Technology, Hikvision, etc.).

Modos de captura de detección de movimiento y continuo separados, para una grabación flexible.

Servidor web seguro integrado para visualización y administración remotas.

Soporte de Pan/Tilt/Zoom (PTZ) para cámaras de red.

Compresión H.264 acelerada por hardware para un almacenamiento eficiente del metraje capturado.

Función de carga FTP para la copia de seguridad automática fuera del sitio de las imágenes capturadas.

Notificaciones de iOS y correo electrónico activadas por movimiento.

Soporte de audio bidireccional.

Opción de pre-captura, para capturar video antes del momento del movimiento

Sincronice la reproducción multicámara del metraje capturado

## Empezando

Inicialmente, SecuritySpy detectará y mostrará todos los dispositivos locales (USB, Thunderbolt e integrados) conectados a su Mac. Si está utilizando cámaras IP, puede agregarlas en la ventana Preferencias.

## Ventanas de video

La ventana principal Todas las cámaras de SecuritySpy muestra transmisiones de video en vivo de todas las cámaras configuradas en una vista de cuadrícula.

También puede crear ventanas de grupo que contengan grupos particulares de cámaras. útil en instalaciones más grandes para organizar cámaras en colecciones lógicas.

Además, cada cámara se puede mostrar en su propia ventana de video individual. Puede abrir ventanas de video de cámaras individuales desde el menú Ventana, o haciendo doble clic en la imagen en vivo de una cámara en la ventana de video principal o en la ventana de grupo, o haciendo doble clic en el nombre de una cámara en la ventana Información de la cámara.

Todas las ventanas de video se pueden cambiar de tamaño a cualquier forma y tamaño arrastrando cualquier lado de la ventana.

SecuritySpy ofrece control digital Pan/Tilt/Zoom para cualquier cámara en cualquier ventana de video: mantenga presionada la tecla Comando (⌘) en su teclado y desplácese hacia arriba o hacia abajo en su mouse o trackpad (en un trackpad, use el gesto de dos dedos para desplazarse ).

Una vez ampliada, suelte la tecla Comando y desplácese en cualquier dirección para desplazarse por la imagen. Esto es útil para cámaras de alta resolución que brindan más detalles de los que se pueden mostrar en las ventanas de video.

## Grabación y acciones

Para grabar video desde una cámara, debe estar armada, y hay tres modos que pueden armarse de forma independiente:

**Captura continua** donde el video se captura continuamente.

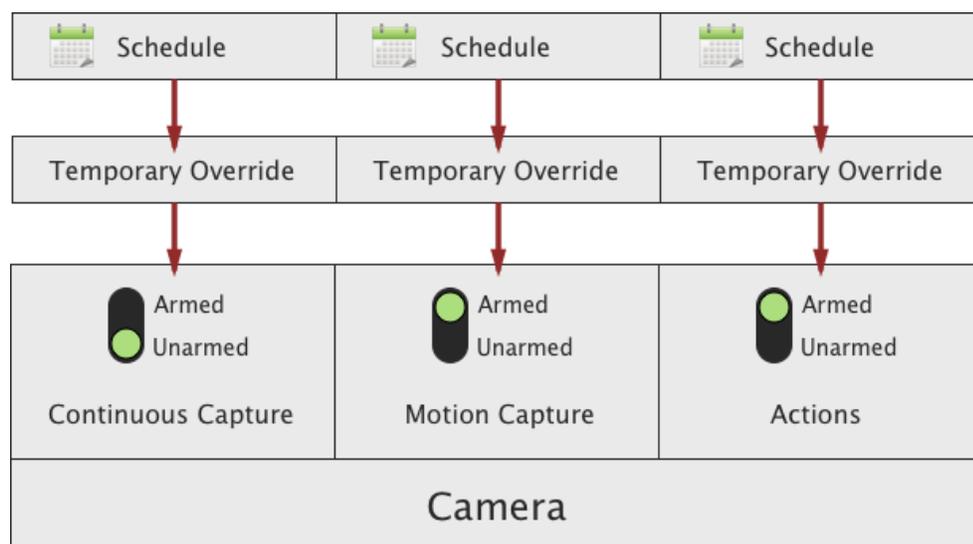
**Captura de movimiento** donde la captura de video se activa mediante detección de movimiento.

**Acciones** como correos electrónicos, scripts y sonidos, que se activan mediante la detección de movimiento.

## Scheduling

Los modos de cámara se activan y desactivan en función de horarios, que definen períodos de tiempo durante la semana en los que una cámara debe activarse o desactivarse.

Puede configurar sus propios horarios, o utilizar los dos básicos proporcionados, que son "**Armado 24/7**" y "**Desarmado 24/7**", lo que indica que un modo de cámara debe estar armado todo el tiempo o desarmado todo el tiempo respectivamente. Además, a veces es útil anular temporalmente las programaciones. Por ejemplo, si recibe muchas notificaciones debido a alguna actividad inusual en una cámara en particular, puede usar una anulación de programación para desarmar el modo de **Acciones** durante una hora para detener temporalmente las notificaciones. Esto se puede entender mejor mediante el siguiente diagrama que muestra la relación entre horarios, anulaciones de horarios y armado / desarmado de los modos de cámara:



Para establecer un horario o anular para una cámara en particular, haga clic con el botón derecho en su imagen de video (o en su nombre o estado en la ventana Información de la cámara) para obtener un menú emergente que le permite hacer esto, o use el menú Control en la parte superior de la pantalla.

## Ventana Camera Info

Esta ventana está disponible seleccionando Información de la cámara en el menú Ventana:



Camera Name	Status	Motion	Audio	FPS	Pixels	Size	Data Rate	CPU
Entrance	CMA	<input type="checkbox"/>	<input type="checkbox"/>	5 fps	0.3 MP	640x480	59 KB/s	1.3 %
Back Door	CA	<input checked="" type="checkbox"/>	<input type="checkbox"/>	7 fps	0.9 MP	1280x720	13.3 MB/s	5.5 %
Front Door	CMA	<input type="checkbox"/>	<input checked="" type="checkbox"/>	10 fps	0.3 MP	720x480	847 KB/s	4.1 %
Street	Online	<input type="checkbox"/>	<input type="checkbox"/>	4 fps	1.3 MP	1280x1024	43 KB/s	5.2 %

La ventana Información de la cámara muestra una gran cantidad de información sobre el funcionamiento de cada cámara:

**Camera Name:** el nombre que se utiliza para identificar la cámara en todo el software. **Status:** las letras C, M y A indican los tres modos que se pueden armar o desarmar por separado: **Captura continua**, **Captura de movimiento** y **Acciones**. El gris indica que un modo en particular está armado pero no está haciendo nada activamente, mientras que el rojo indica que el modo está armado y está haciendo algo (por ejemplo, grabar un video o ejecutar una acción). **Motion:** el nivel de movimiento que se detecta actualmente en la transmisión de video de la cámara. **Audio:** muestra el nivel de audio actual.

Haga clic en el icono del altavoz para reproducir el audio en vivo a través de los altavoces de la Mac. Además, si la cámara admite audio bidireccional, haga clic en el icono del micrófono para hablar y enviar ese audio a la cámara.

**FPS:** la velocidad de fotogramas actual de la transmisión de video. **Píxeles:** la resolución en términos de número de megapíxeles (MP). **Size:** la resolución en términos de píxeles de ancho por píxeles de alto. **Data Rate:** la cantidad de datos que se reciben por segundo. **CPU:** la cantidad aproximada de un núcleo de procesador de la CPU de Mac que se está utilizando. **Pérdida:** el porcentaje de paquetes de datos que se han perdido durante la transmisión a través de la red (lo ideal es que siempre sea cero; de lo contrario, esto indica un problema con la red o la cámara). **Formato de video:** el formato del flujo de video proporcionado por la cámara (por ejemplo, JPEG, MPEG, H.264).

**Audio Format:** el formato del flujo de audio proporcionado por la cámara (por ejemplo, PCM,  $\mu$ Law, AAC). **No:** el número de la cámara, que es un identificador único que se utiliza para hacer referencia a la cámara, principalmente a través de la interfaz web de SecuritySpy.

Para elegir qué columnas mostrar, haga clic en la barra de encabezado para obtener un menú emergente que le permite activar o desactivar cada uno de los elementos anteriores.

### **Full Screen Mode (Modo pantalla completa)**

Ingrese al modo de pantalla completa usando la opción en el menú Ventana, o presionando Comando-F en el teclado. Cada monitor conectado a su computadora se convierte en una pantalla completa independiente para las cámaras que elija. La primera vez que ingrese al modo de pantalla completa, SecuritySpy agregará todas las cámaras disponibles a la vista de pantalla completa; para cambiar esto, haga clic con el botón derecho (control-clic) en cualquier lugar de una pantalla y aparecerá un menú que le permitirá configurar qué cámaras mostrar en esa pantalla.

**Error** al reportar cuando SecuritySpy encuentra un error, informa el error en su archivo de registro y continúa ejecutándose. Por ejemplo, tales errores pueden incluir problemas con los dispositivos de entrada de video, errores de carga de FTP o errores al enviar correos electrónicos. Si encuentra algún tipo de problema mientras usa SecuritySpy, debe consultar el registro para obtener más información sobre lo que sucedió. Para abrir el archivo de registro, seleccione Abrir registro en el menú Archivo.

### **Preferences / Preferencias**

La ventana de Preferencias contiene todas las configuraciones para el software y se divide en las siguientes secciones:

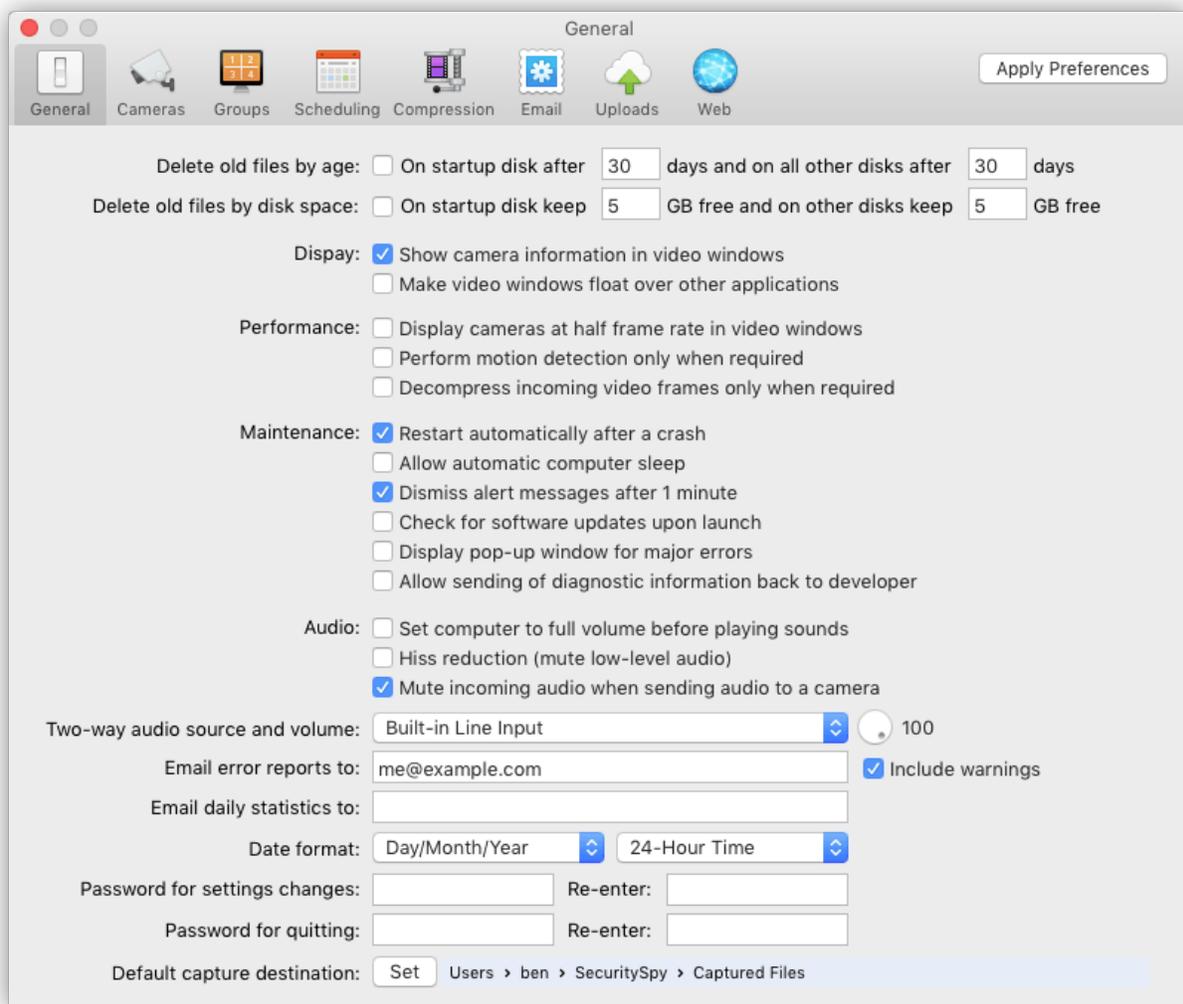
**General:** opciones de uso general como administración de archivos, rendimiento y seguridad **Cámaras:** agregue, elimine o configure cámaras **Grupos:** organice las cámaras en grupos lógicos para mostrarlas en ventanas de grupo **Programación:** configure horarios para armar automáticamente las cámaras durante ciertos momentos **Compresión:** configuración de compresión de video y audio **Correo electrónico:** configuración de correo electrónico para notificaciones e informes de errores **Cargas:** configure servidores FTP para realizar copias de seguridad de secuencias de video fuera del sitio **Web:** configuración de la interfaz web incorporada de SecuritySpy

Tenga en cuenta que los cambios en las Preferencias no se aplican inmediatamente cuándo interactúa con los controles en esta ventana, ya que esto podría interrumpir las grabaciones que se están realizando actualmente.

En su lugar, use la opción Guardar en el menú Archivo (Comando-S en el teclado), o haga clic en el botón "Aplicar preferencias" en la esquina superior derecha de la ventana, para aplicar los cambios que realice.

## Preferencias – General

Esta sección contiene configuraciones de propósito general para configurar el software, de la siguiente manera:



### **Eliminar archivos antiguos por tiempo / Delete old files by age**

Cuando está habilitado, los archivos capturados con una antigüedad superior a la cantidad de días que especifique se eliminarán automáticamente. Hay una configuración separada para el volumen de inicio (sistema) frente a otros volúmenes.

### **Eliminar archivos antiguos por espacio en disco / Delete old files by disk space**

Cuando está habilitado, los archivos capturados antiguos se eliminarán cuando el espacio en disco vaya por debajo del nivel que especifique. Esto no debe establecerse demasiado bajo, ya que los discos tienden a ralentizarse significativamente a medida que se quedan sin espacio; un valor de alrededor del 2% de la capacidad del disco es generalmente una buena configuración para usar (por ejemplo, 20 GB para una unidad de 1 TB). Si la computadora se está utilizando para otras aplicaciones además de SecuritySpy, se debe dejar mas espacio libre en el volumen de inicio (sistema), por lo tanto, hay una configuración separada para el volumen de inicio frente a otros volúmenes.

### **Pantalla: muestra la información de la cámara en las ventanas de video / Display – Show camera information in video windows**

Esta opción controla sí la información de la cámara, como el nombre de la cámara, los modos de armado y el estado de grabación se muestra en la parte superior de cada imagen de la cámara en las ventanas de video (pero no en el metraje capturado).

### **Pantalla: haga que las ventanas de video floten sobre otras aplicaciones / Display – Make video windows float over other applications**

Cuando está habilitado, todas las ventanas de video de SecuritySpy (la ventana Todas las cámaras, ventanas de grupo y ventanas de video de cámara individual) aparecerán sobre las ventanas de otras aplicaciones, incluso cuando SecuritySpy está en segundo plano.

**Rendimiento: muestra las cámaras a la mitad de la velocidad de fotogramas en ventanas de video / Performance – Display cameras at half frame rate in video windows**

Cuando está habilitado, todas las cámaras se mostrarán a la mitad de la velocidad de fotogramas en todas las ventanas de video. Si tiene muchas cámaras y / o muchas ventanas de video abiertas a la vez, habilitar esta opción puede resultar en un menor uso de la CPU (cuánto más bajo depende de la resolución y velocidad de cuadros de sus cámaras, y la velocidad del hardware de gráficos de su computadora). Esta opción afecta solo a la visualización; no afecta la captura de video.

**Rendimiento: realice la detección de movimiento solo cuando sea necesario / Performance – Perform motion detection only when required**

Cuando está habilitada, la detección de movimiento solo se realizará cuando sea necesario para activar la captura de movimiento o acciones, lo que resultará en un menor uso de la CPU cuando no sea necesario para estos fines.

Rendimiento: descomprima los fotogramas de video entrantes solo cuando sea necesario De forma predeterminada, SecuritySpy descomprimirá todos los fotogramas de video entrantes, ya sea que cada uno sea realmente necesario o no. La ventaja de hacerlo es que los fotogramas están disponibles en todo momento, por lo que si el video de una cámara se requiere repentinamente después de un período en el que no se requiere (por ejemplo, se abre una ventana de video después de haber sido cerrada previamente), entonces se mostrará un fotograma de video disponible inmediatamente; de lo contrario, puede haber un retraso significativo hasta que se pueda reanudar la descompresión y el siguiente cuadro esté disponible.

Para evitar una demora prolongada, asegúrese de que la velocidad de fotogramas clave de la cámara no esté configurada demasiado alta (esta es la frecuencia de los fotogramas clave autónomos en la transmisión de video comprimido, y se puede hacer referencia a los siguientes nombres por varios fabricantes: intervalo de fotogramas I, frecuencia de fotogramas I, longitud de GOV, período intra fotograma). Una buena configuración es aproximadamente el doble de la velocidad de fotogramas de la transmisión, lo que dará como resultado un retraso máximo de dos segundos (por ejemplo, si la cámara está transmitiendo video a 10 fps, establezca la velocidad de fotogramas clave en 20).

Habilitar esta opción podría resultar en un uso de CPU significativamente menor, especialmente si las funciones que requieren descompresión se usan con poca frecuencia. Dichas características incluyen detección de movimiento, visualización en ventanas de video, entrega a través de la interfaz web y grabación en disco donde SecuritySpy está realizando la recompresión de la transmisión de video.

**Mantenimiento:** se reinicia automáticamente después de una falla. Se hace todo lo posible para garantizar que SecuritySpy sea lo más estable posible; sin embargo, dado que se basa en otros componentes de software escritos por otras partes (como el software del sistema y el software del controlador para dispositivos de entrada de video), la estabilidad no se puede garantizar.

Por lo tanto, es posible, aunque poco probable, que SecuritySpy se bloquee ("se cierre inesperadamente"), y si la computadora puede quedar desatendida durante largos períodos de tiempo, esto es un problema potencial. Cuando esta opción está habilitada, se inicia una pequeña aplicación en segundo plano que monitorea SecuritySpy y la reinicia si falla. Esta aplicación se ejecuta de forma invisible y casi no utiliza recursos del sistema. Si SecuritySpy falla mientras se captura el video, como máximo se perderán solo unos minutos de video.

**Mantenimiento: permite la suspensión automática de la computadora /  
Maintenance – Allow automatic computer sleep**

La computadora debe estar activa para que SecuritySpy funcione, por lo que si desea un funcionamiento continuo, debe dejar esta opción desactivada. Utilice esta opción si desea que la computadora se suspenda automáticamente cuando no se esté utilizando (según la configuración en la preferencia del sistema Energy Saver).

**Mantenimiento: descarte los mensajes de alerta después de 1 minuto /  
Maintenance – Dismiss alert messages after 1 minute**

Si esta opción está activada, todos los mensajes de alerta (como los mensajes de error) se cerrarán después de 1 minuto. Esta opción debe estar habilitada si la computadora se va a dejar desatendida.

**Mantenimiento:** comprobar automáticamente si hay actualizaciones de software al iniciarse. Si hay una actualización disponible, se le ofrecerá la opción de instalarla; las actualizaciones nunca se instalan automáticamente sin su permiso.

### **Mantenimiento: muestra una ventana emergente para errores importantes / Maintenance – Display pop-up window for major errors**

Utilice esta opción para que aparezca una ventana en la pantalla para informarle de cualquier error importante (estos incluyen problemas que impiden que SecuritySpy obtenga secuencias de video o problemas de grabación).

**Maintenance / Mantenimiento:** envíe la información de diagnóstico al desarrollador Si esta opción está activada, SecuritySpy nos enviará información, los desarrolladores del software, una vez al día, para ayudarnos a diagnosticar problemas y mejorar el software. Esto incluye información de configuración del sistema, informes de errores y datos de rendimiento. Estos datos no se comparten con terceros y solo contienen información relevante para el desempeño de SecuritySpy.

### **Audio: configure la computadora al volumen máximo antes de reproducir sonidos / Audio – Set computer to full volume before playing sounds**

Cuando está habilitado, el volumen del altavoz principal de la computadora se establecerá automáticamente al máximo antes de reproducir sonidos, y luego volverá a su volumen original después de que se reproduzca el sonido.

### **Audio: reducción de ruidos / Audio – Hiss reduction**

Cuando está habilitado, el audio de bajo nivel se silenciará, eliminando el silbido y/o ruido de fondo de los micrófonos. Esto es útil para aplicaciones como el monitoreo de bebés, donde puede estar escuchando el audio por la noche o cuando varias cámaras están reproduciendo audio al mismo tiempo.

### **Audio: silencia el audio entrante al enviar audio a una cámara / Audio – Mute incoming audio when sending audio to a camera**

Para las cámaras que admiten audio bidireccional, esta opción controla si el audio entrante de esa cámara se silencia cada vez que envía audio a esa cámara. Esto evita una situación de retroalimentación en la que el audio puede pasar del micrófono de la Mac al altavoz de la cámara, al micrófono de la cámara, al altavoz de la Mac y de regreso al micrófono de la Mac en un bucle infinito.

## **Audio: fuente de audio bidireccional y volumen** **Audio – Two-way audio source and volume**

Esto define una fuente de entrada de audio conectada a su Mac que se utilizará para la transmisión de audio de computadora a cámara. Use la perilla de control redonda a la derecha para ajustar el volumen de audio.

## **Informes de errores por correo electrónico / Email error reports**

Utilice esta opción para que los informes de errores se envíen a una dirección de correo electrónico siempre que ocurra algún problema. Puede ingresar varias direcciones de correo electrónico, cada una separada por una coma. También tiene la opción de recibir mensajes de advertencia, que son mensajes de advertencia que le informan sobre problemas potenciales, como un uso excesivo de la memoria o de la CPU. En todos los casos, todos los errores se escriben en un archivo de registro, al que puede acceder desde el menú Archivo en SecuritySpy.

## **Estadísticas diarias de correo electrónico / Email daily statistics**

Cuando se utiliza esta opción, SecuritySpy recopilará varias estadísticas, incluida la cantidad de archivos creados, la cantidad de datos registrados y el tiempo de actividad de la cámara. A la medianoche, se enviará un informe por correo electrónico con un resumen de esta información. Esto es útil para confirmar rápidamente que su sistema está funcionando como se esperaba. Puede ingresar varias direcciones de correo electrónico, cada una separada por una coma.

## **Fecha de pedido / Date ordering**

Elija su formato de fecha preferido, que se utiliza siempre que se muestra una fecha (por ejemplo, en las marcas de tiempo de los fotogramas de vídeo y en los nombres de los archivos).

## **Estilo de reloj / Clock style**

Elija un formato de fecha y elija un reloj de 12 horas (p. Ej., "2 p. M.") O un reloj de 24 horas (p. Ej., "14:00").

## **Contraseña para cambios de configuración / Password for settings changes**

Aquí puede establecer una contraseña que será requerida por cualquier persona que intente acceder a la configuración o desarmar cámaras. También es recomendable, en la preferencia del sistema "SecuritySpy & Privacy", configurar la propia Mac para que requiera una contraseña después de un breve período de inactividad. Si bien esto no evita que alguien manipule físicamente la computadora, implementar estas precauciones de seguridad básicas proporciona una primera capa de protección útil .

## **Contraseña para salir / Password for quitting**

Aquí puede establecer una contraseña que será requerida por cualquiera que intente salir de SecuritySpy.

## **Destino de captura predeterminado / Default capture destination**

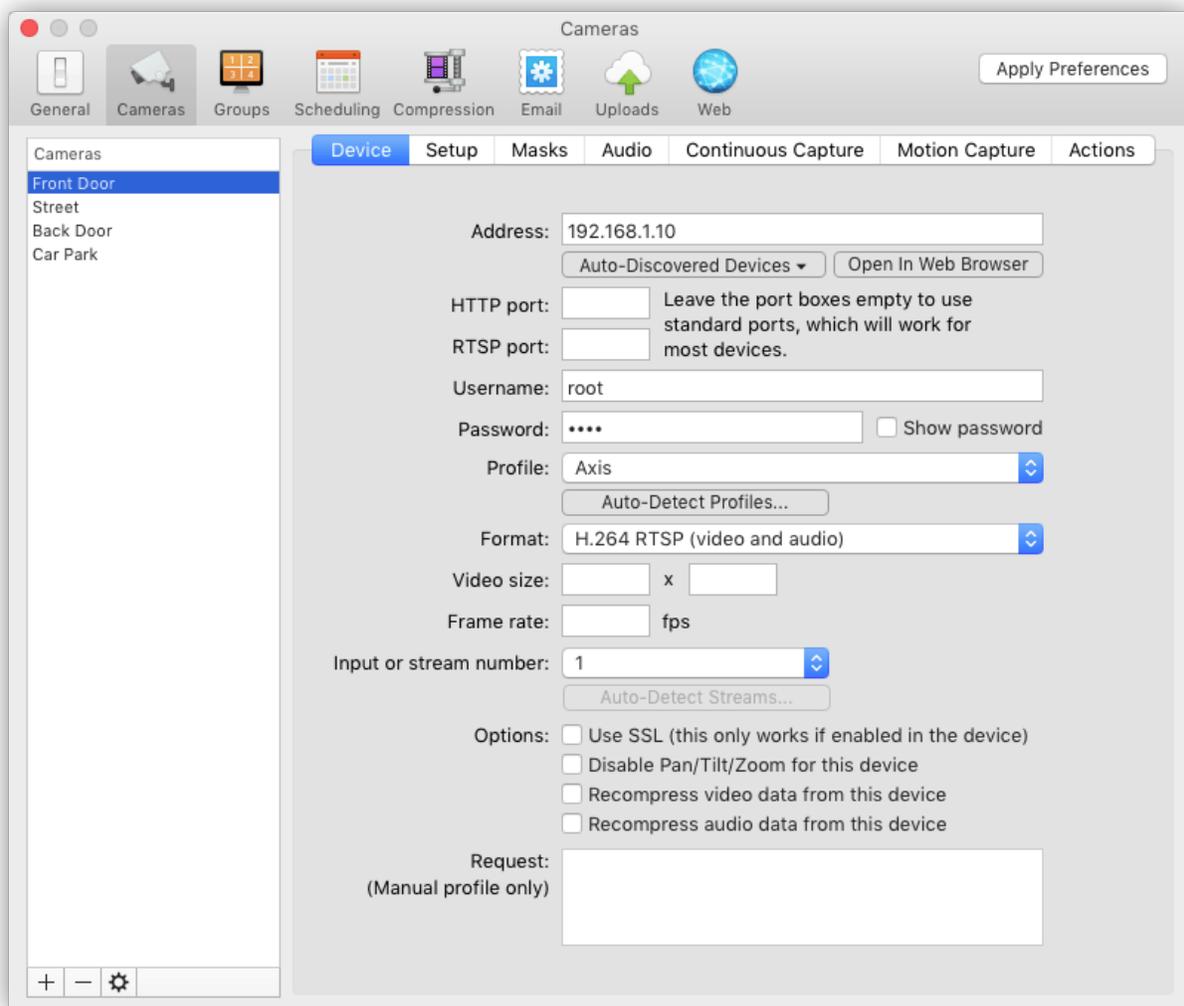
De forma predeterminada, los archivos de películas e imágenes se guardan en una carpeta de Archivos capturados, dentro de la carpeta SecuritySpy en su carpeta de inicio (es decir, ~/SecuritySpy/Captured Files/). Sin embargo, puede personalizar donde SecuritySpy guarda los archivos usando esta configuración, seleccionando un volumen o carpeta en cualquier lugar de su sistema de archivos. Importante: cuando utilice un dispositivo NAS (almacenamiento conectado a la red) como destino de la captura, asegúrese de que esté configurado para usar AFP (protocolo de archivos de Apple); de lo contrario, es posible que SecuritySpy no pueda eliminar automáticamente los archivos antiguos o mostrar los archivos correctamente en su navegador.

La mayoría de los dispositivos NAS son compatibles con AFP, aunque es posible que esta función no esté habilitada de forma predeterminada. Si desea elegir un destino de captura solo para cámaras específicas, puede hacerlo en [Preferences -> Cameras -> Setup](#).

## **Preferencias - Cámaras / Preferences - Cameras**

En la sección Cámaras, puede configurar todas las cámaras para que las utilice SecuritySpy. Esta sección se subdivide en las siguientes pestañas: [Device](#), [Setup](#), [Masks](#), [Audio](#), [Continuous Capture](#), [Motion Capture](#), and [Actions](#).  
Preferences - Cameras - Device

La pestaña dispositivo contiene configuraciones relacionadas con los dispositivos de video (la captura de pantalla a continuación muestra la configuración disponible para dispositivos de red; para dispositivos locales, es decir, aquellos conectados por USB, Thunderbolt o dispositivos integrados como cámaras FaceTime), hay muchas menos opciones disponibles como estos son dispositivos plug-and-play que no necesitan configurarse de la misma manera).



## Direcciones / Address

Ingrese la dirección IP, el nombre de host o la dirección Bonjour del dispositivo. Al hacer clic en el botón dispositivos descubiertos automáticamente debajo de este campo, SecuritySpy mostrará una lista de dispositivos que fueron descubiertos en su red local, por ejemplo:



Seleccione un dispositivo de esta lista y el campo Dirección se completará automáticamente con la dirección del dispositivo seleccionado. Este menú consta de dos secciones: Dispositivos ONVIF: esta sección enumera todos los dispositivos ubicados a través del mecanismo de descubrimiento automático de ONVIF.

Todas las cámaras compatibles con ONVIF conectadas a su red local se mostrarán aquí. Al seleccionar un dispositivo de esta lista, el campo Dirección se completará con la cadena de identificación única de la cámara ("UUID"). Al referirse a las cámaras por sus identificadores únicos, SecuritySpy puede localizar cámaras incluso si cambian sus direcciones IP subyacentes.

Dispositivos Bonjour: Bonjour es un protocolo para el descubrimiento automático y el direccionamiento que elimina la necesidad de utilizar direcciones IP. Todos los dispositivos compatibles con Bonjour se mostrarán aquí; al seleccionar uno de la lista, se completará el campo Dirección con la dirección Bonjour del dispositivo.

Ambos métodos de direccionamiento anteriores eliminan la necesidad de configurar sus cámaras con direcciones IP fijas: para una cámara que obtiene una dirección IP automáticamente a través de DHCP (que suele ser el caso), la configuración es simplemente un caso de conectarla a su red y seleccionarla en la lista anterior.

Muchas cámaras admiten tanto ONVIF como Bonjour, por lo que es posible que vea dos entradas en la lista para dichos dispositivos; en este caso, puede seleccionar cualquiera de las dos (aunque el uso de la dirección ONVIF puede ser un poco más rápido y más confiable en algunas circunstancias).

### **HTTP/RTSP ports**

Estos son los puertos de red que utiliza SecuritySpy para comunicarse con el dispositivo. Los puertos estándar son 80 para HTTP y 554 para RTSP (u 8000 en ambos casos si el dispositivo de red es otra copia de SecuritySpy). Si su dispositivo usa puertos estándar (la mayoría lo hace), puede dejar estos campos vacíos, pero si usa puertos no estándar, debe ingresarlos aquí.

### **Username / Password**

Si el dispositivo de red requiere autenticación, ingrese su nombre de usuario y contraseña aquí.

### **Perfil / Profile**

La mayoría de los productos de vigilancia IP vendidos en los últimos años implementan el protocolo ONVIF, que es una forma universal de comunicación con cámaras IP. Entonces, si su cámara admite esto, entonces debe usar el perfil ONVIF en SecuritySpy. Alternativamente, SecuritySpy tiene muchos perfiles diseñados específicamente para marcas y modelos de cámaras individuales, así que consulte esta lista para encontrar uno que coincida con su dispositivo. O, si desea ingresar la solicitud de transmisión HTTP / RTSP.

### **Opción de configuración manual / Manual configuration option.**

Si su dispositivo no es compatible con ONVIF y no está seguro de qué otro perfil usar, haga clic en el botón Detectar perfiles automáticamente. SecuritySpy luego probará cada perfil a su vez con su cámara y devolverá una lista de los que funcionan. Antes de ejecutar esta prueba, asegúrese de haber ingresado correctamente la dirección, los puertos, el nombre de usuario y la contraseña de la cámara.

## Formato / Format

Este menú enumera los formatos disponibles admitidos por el dispositivo de red, que será una combinación de los siguientes: Códecs de compresión de video:

**JPEG:** este es el códec mas simple, que le dará un bajo uso de CPU pero archivos de gran tamaño.

**MPEG-4:** este es un códec mas eficiente en el espacio que JPEG, pero usa mucho más tiempo de la CPU de Mac para procesar y ha sido reemplazado por H.264.

**H.264:** este es el códec mas eficiente y es el mejor para usar si es compatible con su cámara.

## Protocolos de transporte de red

**HTTP:** diseñado para páginas web, pero se puede usar para transmitir video JPEG; no admite audio.

**RTSP:** diseñado para video y generalmente se usa para transmisión MPEG-4 y H.264; tiene soporte para transmisión de video y audio.

**RTSP sobre HTTP:** tiene las ventajas de los dos formatos anteriores, ya que está diseñado para transmisión de video, admite video y audio y se transmite fácilmente a través de Internet junto con el tráfico web estándar.

Si se conecta a una cámara a través de una red local, el formato "**H.264 RTSP**" suele ser el mejor para usar. Si se conecta a través de Internet, entonces el formato "**H.264 RTSP-over-HTTP**" es el más apropiado, si su cámara lo admite.

## Tamaño de video / Video size

Ingrese un tamaño de video (resolución) para solicitar desde el dispositivo. Si deja estos campos vacíos, se utilizará el tamaño de video predeterminado del dispositivo de red. Esta configuración no está disponible para todos los dispositivos; por lo general, deberá configurar el dispositivo directamente para establecer su tamaño de video.

## **Cuadros por segundo / Frame rate**

Ingrese la velocidad de fotogramas a la que desea que el dispositivo envíe fotogramas de video. Esta configuración no está disponible para todos los dispositivos; por lo general, deberá configurar el dispositivo directamente para establecer su velocidad de fotogramas.

## **Número de entrada o flujo / Input or stream number**

Para dispositivos que tienen múltiples entradas o flujos, aquí puede especificar el que desea usar. Por ejemplo, algunos dispositivos tienen múltiples entradas físicas o sensores de imagen, mientras que otros tienen múltiples flujos con diferentes configuraciones de compresión. Esta opción solo estará disponible si el dispositivo admite esta función.

## **Opciones encriptación / Options – Use SSL**

SSL es un protocolo de criptografía que proporciona una comunicación cifrada segura con dispositivos de red. Para los dispositivos que admiten esta función, SSL proporciona seguridad adicional al evitar la decodificación de los flujos de datos interceptados. Por lo tanto, puede ser útil cuando se transmiten datos a través de Internet, pero normalmente no es necesario cuando se transmite a través de una red local. Tenga en cuenta que esto puede ralentizar significativamente la transmisión de video debido al procesamiento adicional requerido por el dispositivo. Para utilizar SSL, tendrá que configurar el dispositivo con un certificado (ya sea autofirmado o de una autoridad certificadora, aunque este último no es realmente necesario ya que está configurando el servidor usted mismo y, por lo tanto, no hay dudas sobre su autenticidad).

## **Opciones: deshabilitar la compatibilidad con Pan / Tilt / Zoom para este dispositivo / Options – Disable Pan/Tilt/Zoom support for this device**

Muchos perfiles de la lista anterior "Tipo de dispositivo" tienen habilitado el soporte PTZ para controlar cámaras con PTZ mecánico. Si su dispositivo no tiene funciones PTZ, o si desea deshabilitar la compatibilidad con PTZ para una cámara en particular, habilite esta opción. Esto simplemente elimina los controles PTZ asociados con la cámara de la interfaz de usuario de SecuritySpy.

### **Opciones: recomprime los datos de video de este dispositivo / Options – Recompress video data from this device**

Los dispositivos de red suministran datos de video en una variedad de formatos comprimidos (típicamente JPEG, MPEG-4 o H.264). De forma predeterminada, los datos de video proporcionados por la cámara se capturarán directamente desde el dispositivo a los archivos de película que crea SecuritySpy.

Esto garantiza una calidad, un rendimiento óptimos y un uso mínimo de la CPU. Sin embargo, si desea que SecuritySpy aplique una superposición de texto, una transformación (rotación / volteo) o una máscara de supresión de video (para ocultar secciones de la imagen), o si desea volver a codificar los datos a un espacio más eficiente formato, luego habilite esta opción y SecuritySpy utilizará la configuración establecida en la sección Compresión para volver a comprimir los datos durante la grabación.

Generalmente, si necesita una superposición de texto, una transformación o una máscara de supresión, debe aplicarse en la propia cámara (si está disponible allí), en lugar de SecuritySpy, para evitar la necesidad de que SecuritySpy vuelva a comprimir los datos de video.

### **Opciones: recomprime los datos de audio de este dispositivo/Options – Recompress audio data from this device**

Los dispositivos de red suministran datos de audio en una variedad de formatos comprimidos (generalmente G.711, G.726, AMR o AAC). De forma predeterminada, los datos de audio proporcionados por la cámara se capturarán directamente desde el dispositivo a los archivos de película que crea SecuritySpy.

Esto garantiza una calidad, un rendimiento óptimos y un uso mínimo de la CPU. Sin embargo, puede ser útil habilitar esta función para grabar con compresión de audio AAC si su cámara no es capaz de proporcionar este formato, porque cuando el formato de video es H.264 y el formato de audio es AAC, SecuritySpy puede crear archivos MP4. en lugar de archivos MOV.

Los archivos MP4 se reproducen en navegadores web, mientras que los archivos MOV generalmente no lo hacen, por lo que esto es importante si va a ver imágenes grabadas a través de la interfaz web de SecuritySpy.

## **Pedido / Request**

Esta configuración está disponible cuando selecciona Configuración manual como perfil.

Este es el texto de solicitud que se envía al dispositivo para indicarle que envíe datos multimedia. Esta configuración es útil si desea utilizar un dispositivo de red que no es compatible con ONVIF y no es compatible con un perfil existente.

Consulte la documentación o el fabricante de su dispositivo para obtener información sobre el formato de las solicitudes HTTP o RTSP que comprende.

Cuando los manuales de la cámara especifican esta información, normalmente lo hacen en forma de URL, por ejemplo: rtsp: // dirección-cámara: puerto / request.h264

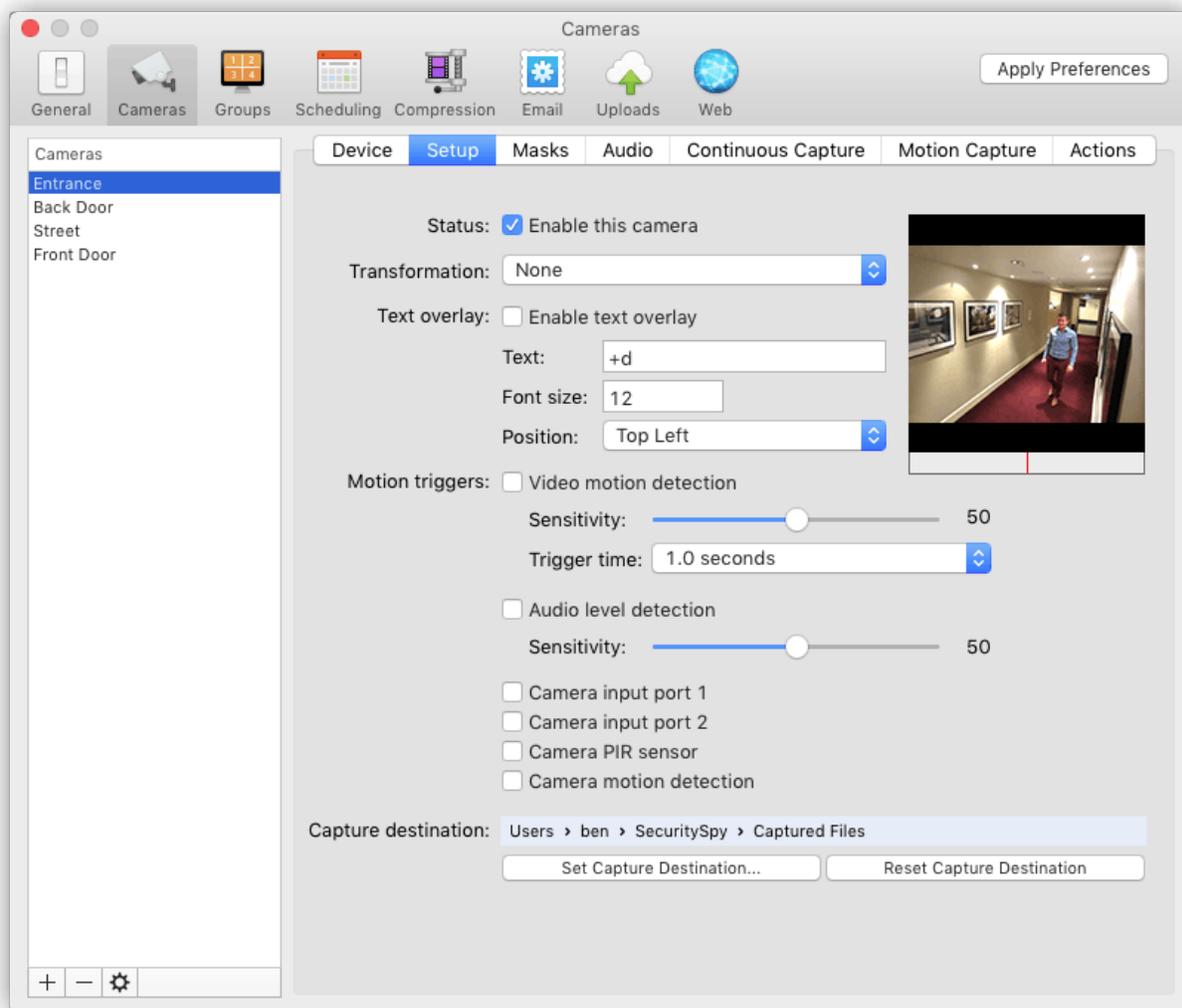
Esto indica que se debe usar el formato RTSP, con el puerto RTSP configurado en puerto y request.h264 como Request.

## **Elegir y configurar sus dispositivos de red / Choosing and configuring your network devices**

Consulte la sección Cámaras de red del Manual de instalación de SecuritySpy para obtener información completa sobre este tema.

## Preferencias - Cámaras - Configuración / Preferences - Cameras - Setup

Esta pestaña muestra las opciones de configuración generales para cada cámara, de la siguiente manera:



### Estado: habilita esta cámara / Status - Enable this camera

Esta casilla de verificación le permite apagar una cámara en particular sin eliminarla por completo del software. Si apaga una cámara, ya no se utilizará y no se podrá ver ni capturar.

## **Transformación / Transformation**

Este menú tiene varias opciones de transformaciones que se pueden aplicar a la imagen de video para compensar la posición de montaje de la cámara (por ejemplo, si está montada al revés o girada hacia un lado).

Las transformaciones disponibles son: rotación de 180 °, rotación de 90 ° en el sentido de las agujas del reloj, rotación de 90 ° en sentido antihorario, giro horizontal y giro vertical.

Tenga en cuenta que, para las cámaras de red, esta configuración solo está disponible si ha elegido volver a comprimir los datos de video de la cámara, en la sección Dispositivo.

## **Superposición de texto: habilitar la superposición de texto / Text overlay – Enable text overlay**

Utilice esta opción para dibujar una superposición de texto en todos los fotogramas de vídeo. Utilice los marcadores de posición + n, + d, + w y \ n para representar el nombre de la cámara, la fecha y la hora, el nombre del día y el salto de línea, respectivamente.

Tenga en cuenta que, para las cámaras de red, esta configuración solo está disponible si ha elegido volver a comprimir los datos de video de la cámara, en la sección Dispositivo.

## **Activadores de movimiento: detección de movimiento por video / Motion triggers – Video motion detection**

La función de detección de movimiento por video analiza la transmisión de video entrante para detectar movimiento. Cuando el nivel de movimiento excede el umbral (mostrado como la línea roja en la barra de movimiento debajo de la imagen de video), durante el tiempo especificado por la configuración de "tiempo de activación", se activarán la captura de movimiento y las acciones.

El ajuste de sensibilidad permite variaciones en las condiciones de instalación de la cámara y si desea que SecuritySpy capture el más mínimo movimiento o, en su lugar, limite la grabación a altos niveles de movimiento. Los valores altos aseguran que la detección de movimiento se active incluso con pequeñas cantidades de movimiento en la transmisión de video, sin embargo, esto también puede resultar en activadores falsos positivos.

La configuración de "tiempo de activación" especifica la duración mínima del movimiento continuo que dará como resultado un disparo. La configuración más sensible es "1 cuadro", que se activará si se detecta movimiento en un solo cuadro de video. Sin embargo, es probable que esto produzca muchos desencadenantes falsos positivos debido a la lluvia, los cambios de iluminación, los insectos y otros movimientos transitorios.

Normalmente, lo ideal es un tiempo de activación de entre 1 y 2 segundos: esto proporciona una tasa baja de disparos falsos positivos sin dejar de ser muy sensible al movimiento real. Tenga en cuenta que esta función funciona mejor cuando la velocidad de fotogramas del video entrante es de al menos 5 fps.

**Activadores de movimiento: detección de nivel de audio** Esta función activa la captura de movimiento y las acciones cuando el nivel de audio supera un cierto umbral. Cuanto mayor sea el ajuste de sensibilidad, más SecuritySpy se activará con sonidos muy silenciosos. Para utilizar esta función, se debe habilitar una fuente de audio para esta cámara (en la pestaña Audio).

#### **Activadores de movimiento: puertos de entrada de la cámara / Motion triggers – Camera input ports**

Esta función activa la captura de movimiento y acciones cuando se activa uno de los puertos de entrada de la cámara. Las cámaras IP suelen tener uno o más puertos de entrada (a veces llamados "puertos IO", "entradas de alarma", "entradas externas" o "entradas digitales") que se pueden conectar a sensores como sensores de movimiento PIR (infrarrojos pasivos), detectores de rotura, sensores de puertas / ventanas, etc. SecuritySpy actualmente admite los puertos de entrada de las cámaras Axis, D-Link, Canon y Hikvision.

#### **Activadores de movimiento: sensor PIR de la cámara / Motion triggers – Camera PIR sensor**

Esta función activa la captura de movimiento y acciones cuando el sensor PIR integrado de la cámara detecta movimiento. Actualmente, esto solo es compatible con las cámaras Hikvision.

**Activadores de movimiento: detección de movimiento de la cámara** esta función activa la captura de movimiento y las acciones cuando el algoritmo de detección de movimiento integrado de la cámara detecta movimiento.

## Destino de la captura

De forma predeterminada, los archivos de películas e imágenes se guardan en una carpeta de Archivos capturados, dentro de la carpeta SecuritySpy en su carpeta Inicio (es decir, ~ / SecuritySpy / Archivos capturados /).

Sin embargo, puede personalizar donde SecuritySpy guarda los archivos usando esta configuración, seleccionando un volumen o carpeta en cualquier lugar de su sistema de archivos. Importante: cuando utilice un dispositivo NAS (almacenamiento conectado a la red) como destino de la captura, asegúrese de que esté configurado para usar AFP (protocolo de archivos de Apple); de lo contrario, es posible que SecuritySpy no pueda eliminar automáticamente los archivos antiguos o mostrar los archivos correctamente en su navegador. característica. La mayoría de los dispositivos NAS son compatibles con AFP, aunque es posible que esta función no esté habilitada de forma predeterminada.

Cualquier destino de captura establecido aquí anulará el predeterminado establecido en Preferencias -> General

## Preferencias – Cámaras – Máscaras / Preferences – Cameras – Masks

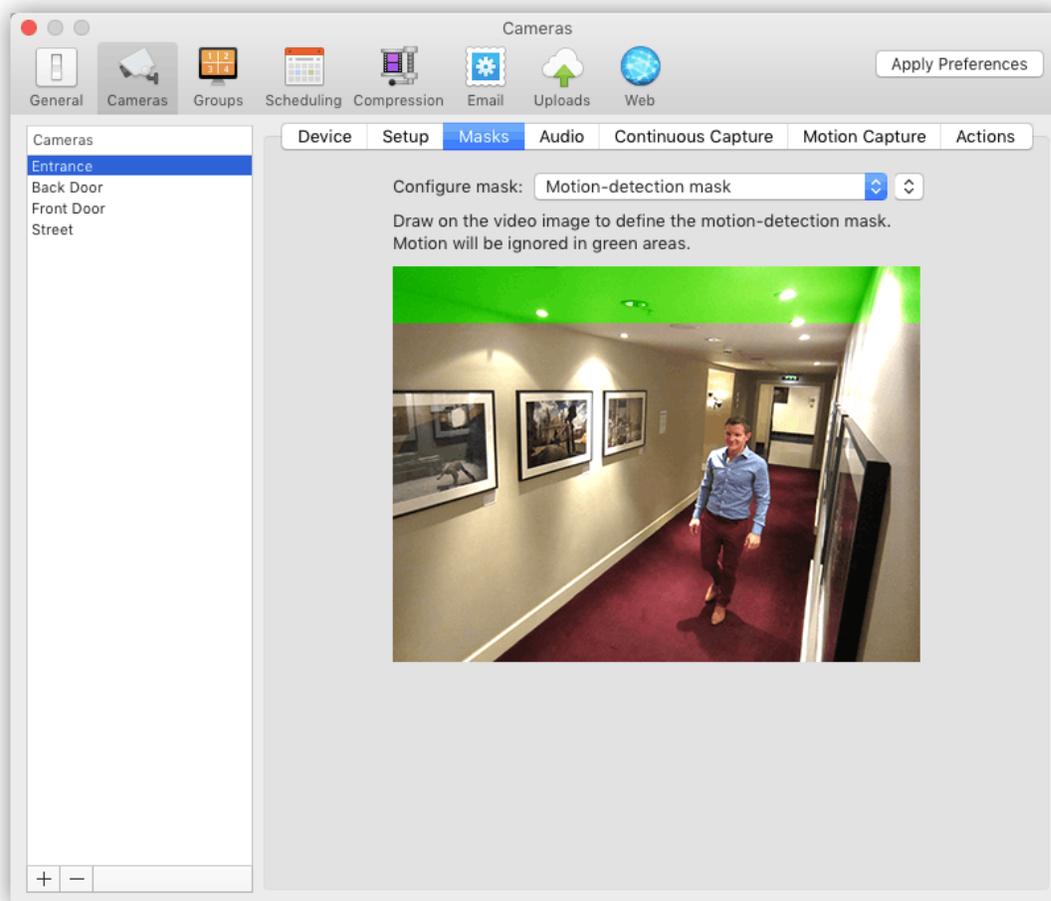
Hay dos máscaras que se pueden configurar en esta sección:

### Máscara de detección de movimiento / Motion Detection Mask

Esto define áreas en la imagen de video que el algoritmo de detección de movimiento de SecuritySpy debe ignorar.

### Máscara de supresión de video

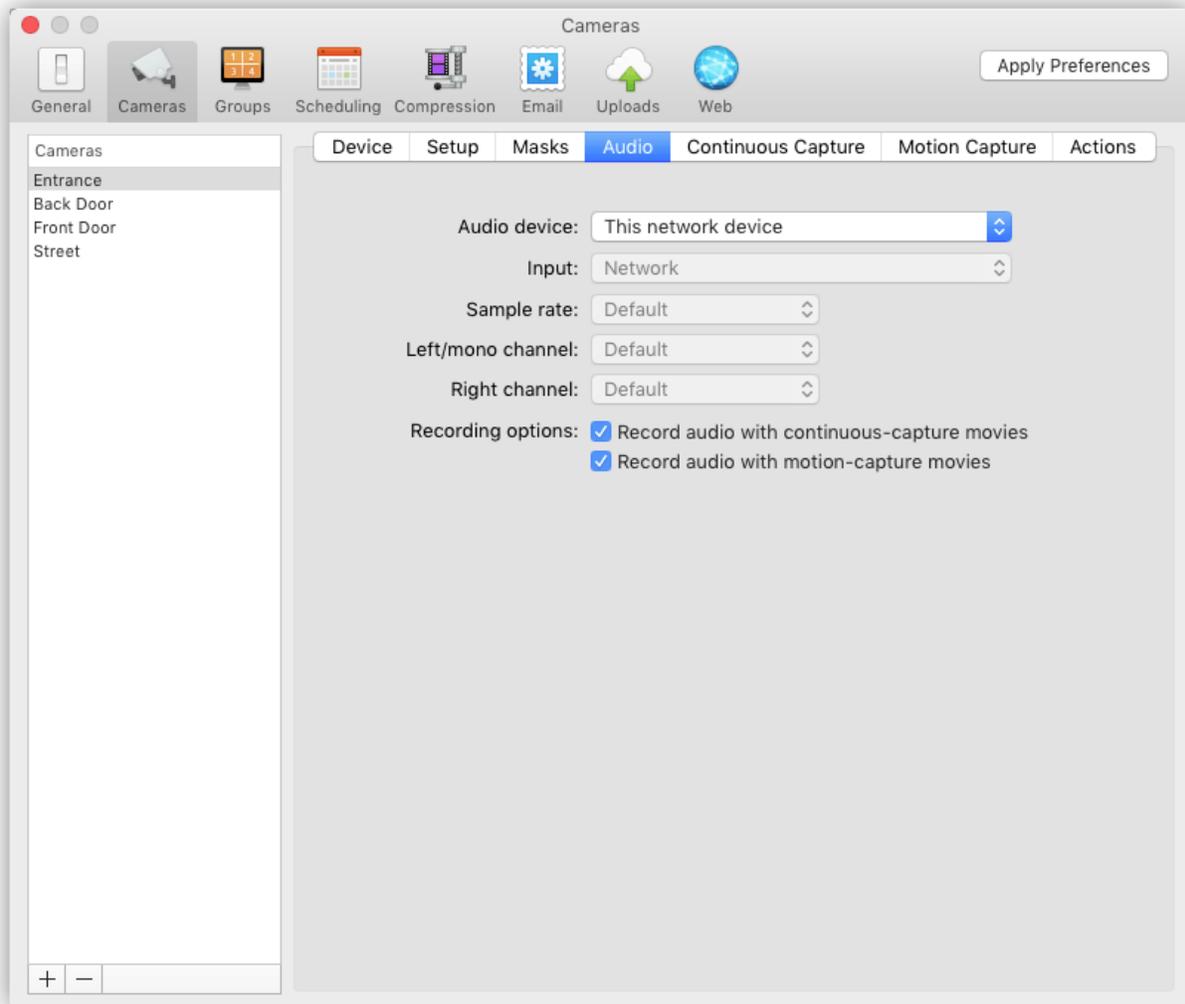
Esto define áreas en la imagen de video que se completarán oscurcidas (dibujadas en negro) en las secuencias de video en vivo y grabadas.



Elija la máscara que desea editar en el menú desplegable. A la derecha de este menú hay algunas opciones útiles para manipular la máscara (por ejemplo, para borrarla o invertirla). Tenga en cuenta que, para las cámaras de red, la máscara de supresión de video solo está disponible si ha elegido volver a comprimir los datos de video de la cámara, en la sección Dispositivo.

## Preferencias – Cámaras – Audio / Preferences – Cameras – Audio

Esta pestaña le permite especificar la configuración de audio para cada cámara:



### Fuente de audio / Audio Source

Elija un dispositivo de entrada de audio para asociarlo con esta cámara. Normalmente, para las cámaras IP, querrá utilizar la opción "Este dispositivo de red", que indica que SecuritySpy debe tomar la señal de audio de la propia cámara. Este menú también enumera todos los dispositivos de audio locales disponibles conectados a su computadora (entradas de audio incorporadas, USB, FireWire y Thunderbolt), y puede asociar cualquiera de estas entradas de audio con cualquier cámara.

## **Entrada / Input**

Si el dispositivo de audio tiene más de una fuente de datos, estas se enumeran aquí. Por ejemplo, la mayoría de las entradas de audio integradas en las computadoras Mac tienen dos fuentes de datos: Entrada de línea y Entrada digital; para usar una fuente de audio analógica, debe seleccionar Line In, o para usar una fuente digital, debe seleccionar Digital In.

## **Frecuencia de muestreo / Sample rate**

Este es el factor principal que determina la calidad del audio: cuanto mayor sea la frecuencia de muestreo, mejor será la calidad, pero mayores serán los archivos capturados.

Una frecuencia de muestreo de 8000 Hz suele ser adecuada para la videovigilancia, aunque si desea una mayor calidad, una configuración de alrededor de 16000–22050 Hz proporcionará una mejora significativa.

## **Canal izquierdo / mono, canal derecho / Left/mono channel, Right channel**

Cada cámara puede utilizar uno o dos de los canales del dispositivo de audio. Con los menús de canal izquierdo y derecho, puede seleccionar que canal del dispositivo (numerado en el menú) se graba en que canal de la película capturada (izquierdo o derecho).

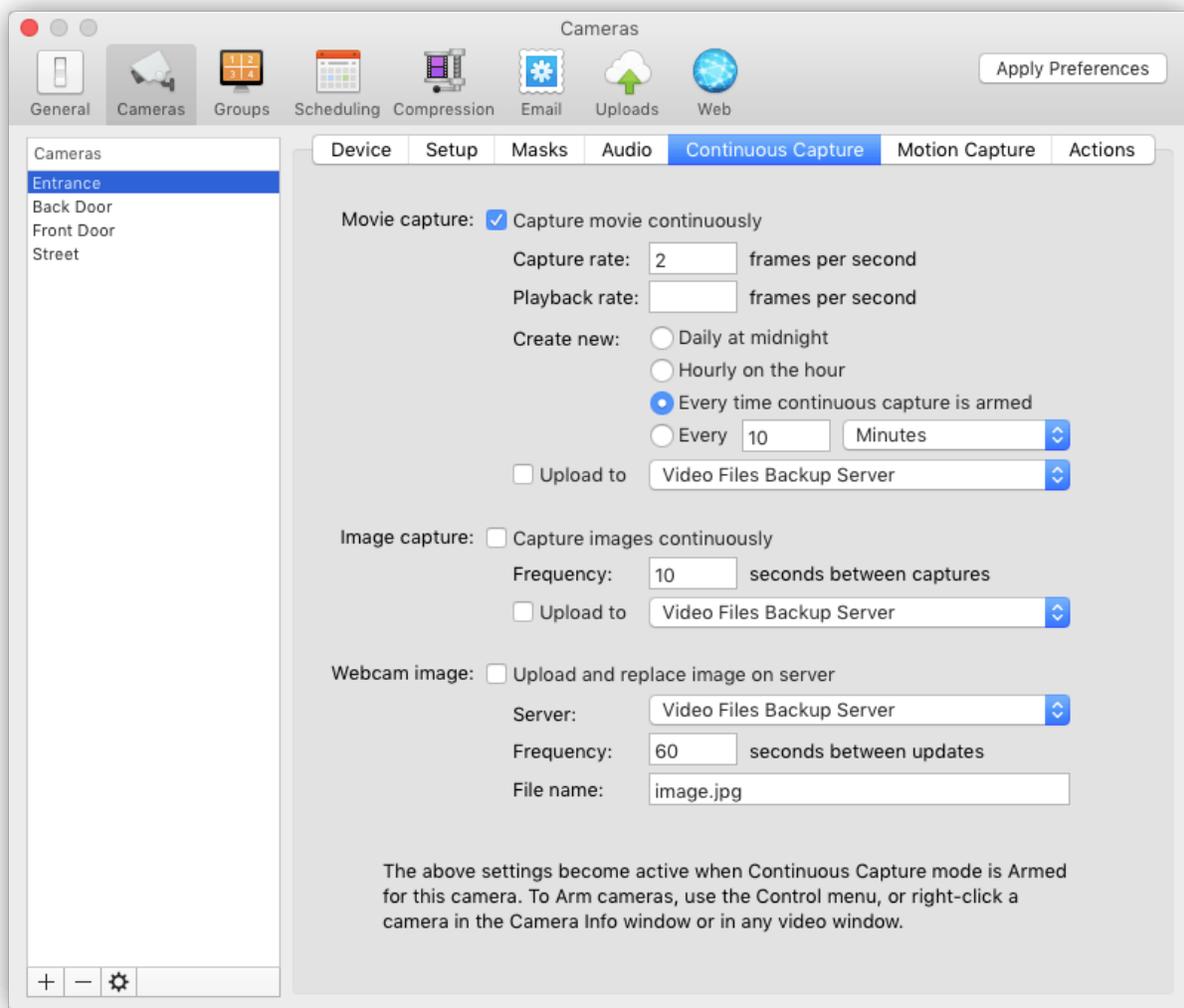
Por ejemplo, si el dispositivo de audio tiene 10 canales de entrada y desea que la entrada 5 se grabe en la película como el canal izquierdo y la entrada 6 se grabe como el canal derecho, debe seleccionar 5 y 6 en estos menús respectivamente. Para grabar simplemente a personas hablando, solo se requiere audio mono (un canal), en cuyo caso debe seleccionar "Ninguno" para el canal correcto. Si está utilizando audio estéreo (dos canales), esto duplica el tamaño de los datos de audio, así que utilícelo solo si es necesario.

## **Opciones de grabación / Recording options**

Puede elegir si desea incluir audio en grabaciones de captura continua y / o grabaciones de captura de movimiento. De forma predeterminada, ambas opciones están habilitadas.

## Preferencias – Cámaras – Captura continua / Preferences – Cameras – Continuous Capture

Esta pestaña le permite especificar la configuración para el modo de grabación de Captura continua:



### Captura de películas: captura películas de forma continua/ Movie capture – Capture movie continuously

Habilite esta opción para capturar un archivo de película siempre que se active el modo de grabación de captura continua.

## **Captura de películas: tasa de captura / Movie capture – Capture rate**

Esta es la velocidad a la que se capturan fotogramas de la película (déjelo en blanco para la velocidad máxima). Sin embargo, tenga en cuenta que si el video entrante está en formato MPEG-4 o H.264, y ha elegido no volver a comprimir el video (consulte la Configuración del dispositivo), SecuritySpy no podrá cambiar la velocidad de fotogramas del video y lo hará. por lo tanto, se grabará a la velocidad que suministre la cámara.

## **Captura de películas: tasa de reproducción / Movie capture – Playback rate**

Esta función es útil para capturar películas a intervalos, donde puede especificar una velocidad de reproducción que sea diferente (generalmente significativamente más alta) que la velocidad de captura.

## **Captura de película – Crear nueva / Movie capture – Create new**

Aquí puede especificar cuándo crear nuevos archivos de película; hay cuatro opciones: Diariamente a la medianoche: se creará un nuevo archivo de película a la medianoche todos los días. Todo el metraje capturado durante el día se agregará al mismo archivo de película, incluso si el modo de captura continua está desarmado y armado durante este tiempo.

Cada hora (a la hora): se creará un nuevo archivo de película al comienzo de cada hora. Todo el metraje capturado durante cada hora se agregará al mismo archivo de película incluso si el modo de captura continua está desarmado y armado durante este tiempo.

Esta es una alternativa útil a la opción Diaria anterior, que produce archivos más pequeños y, por lo tanto, mas manejables que se pueden descargar fácilmente a través de Internet. Cada vez que se arma la captura continua: se creará un nuevo archivo de película siempre que se active el modo de captura continua, y se continuará capturando hasta que se desactive.

Cada x Minutos / Horas / Días: se creará un nuevo archivo de película con la frecuencia que especifique. Siempre que el modo de captura continua se desarma y luego se arma, también se creará una nueva película.

### **Captura de película: subir a / Movie capture – Upload to**

Habilite esta opción para cargar todos los archivos de película de captura continua a un servidor FTP. Si el ajuste "crear nuevo" se establece en Diariamente a la medianoche, las películas se cargarán al final del día; de lo contrario, las películas se cargarán tan pronto como estén terminadas.

### **Captura de imágenes: captura imágenes de forma continua / Image capture – Capture images continuously**

Esta función captura un archivo de imagen en el disco en formato JPEG a la velocidad que especifique.

### **Captura de imágenes: subir a / Image capture – Upload to**

Habilite esta opción para cargar todos los archivos de imágenes de captura continua a un servidor FTP.

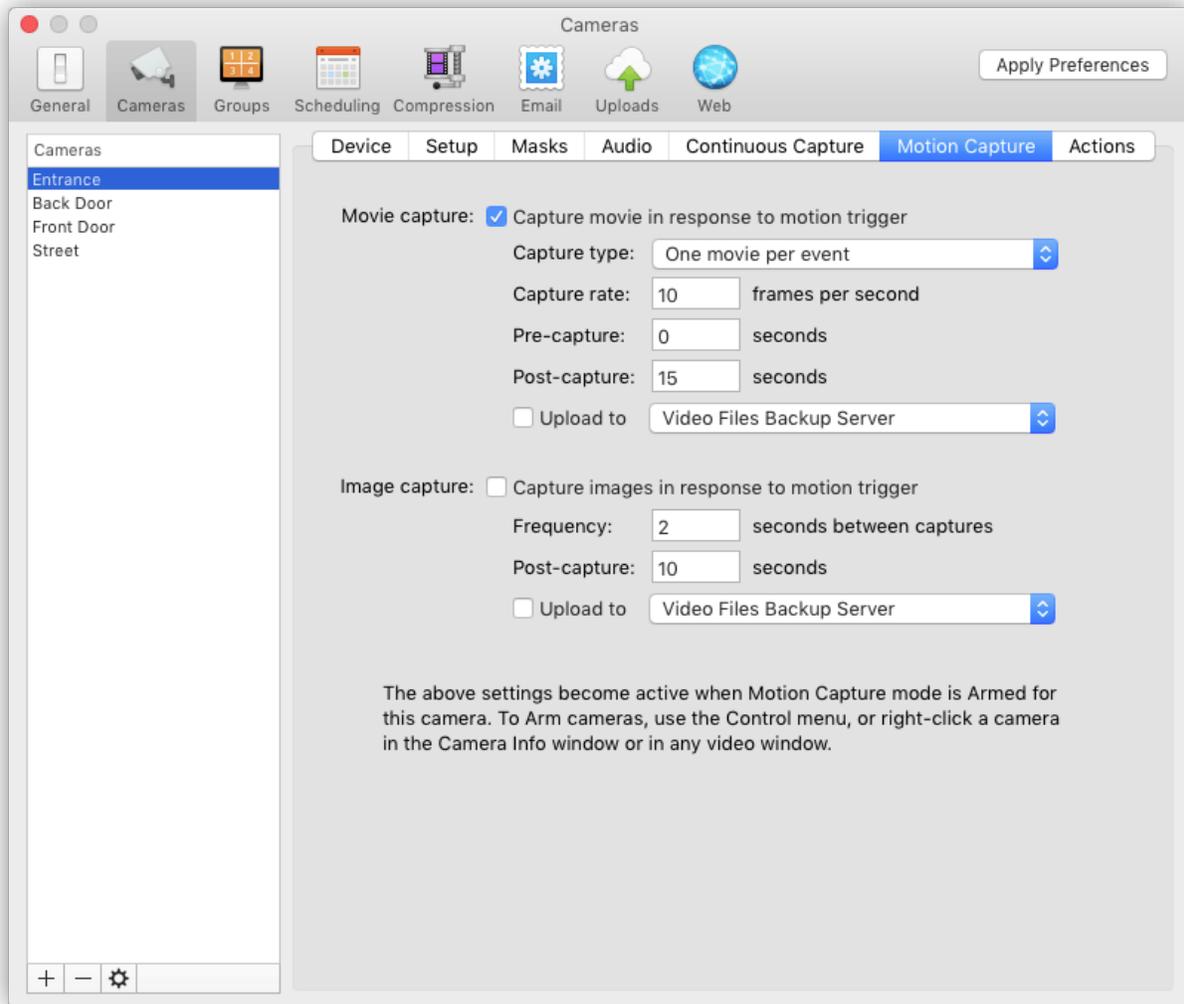
### **Imagen de la cámara web: cargue y reemplace la imagen en el servidor / Webcam image – Upload and replace image on server**

Utilice esta opción para cargar periódicamente un archivo de imagen JPEG con un nombre fijo a un servidor FTP, reemplazando el archivo anterior cada vez.

Esto es útil para actualizar continuamente una imagen en una página web.

## Preferencias – Cámaras – Captura de movimiento / Preferences – Cameras – Motion Capture

Esta pestaña contiene configuraciones para el modo de grabación de captura de movimiento, qué captura películas o imágenes en respuesta a los activadores de movimiento configurados en la pestaña. Configuración:



### Captura de película: captura la película en respuesta al disparador de movimiento. / Movie capture – Capture movie in response to motion trigger

Habilite esta opción para capturar una película en respuesta a un disparador de movimiento. Los activadores de movimiento incluyen detección de movimiento por video, detección de audio y puertos de entrada de cámara, que se pueden habilitar a través de la pestaña Configuración.

## **Captura de película: tipo de captura / Movie capture – Capture type**

Hay dos opciones para la película de captura de movimiento: Una película por evento: se creará un archivo de película independiente para cada evento de detección de movimiento. Esto puede resultar en una gran cantidad de archivos de película individuales si hay eventos frecuentes, sin embargo, ofrece más resistencia a los problemas de la computadora o la manipulación.

Una película por día: se creará un archivo de película cada día que contendrá todos los eventos de detección de movimiento de ese día. Un archivo grande puede ser más fácil de administrar que muchos archivos más pequeños.

## **Captura de películas: tasa de captura / Movie capture – Capture rate**

Especifique la velocidad a la que se capturarán los fotogramas de la película (déjelo en blanco para la velocidad máxima). Sin embargo, tenga en cuenta que si el video entrante está en formato MPEG-4 o H.264, y ha optado por no volver a comprimir el video (consulte la Configuración del dispositivo), SecuritySpy no podrá cambiar la velocidad de fotogramas del video y lo hará. por lo tanto, se grabará a la velocidad que suministre la cámara.

## **Captura de películas: captura previa / Movie capture – Pre-capture**

A menudo es útil tener videos antes y después de un evento de movimiento; en el tiempo antes y después, aunque el movimiento no es lo suficientemente alto como para activar la grabación, a menudo sucede algo interesante que vale la pena capturar. Este es el propósito de las funciones de captura previa y posterior. La función de captura previa utiliza un búfer de fotogramas de video en la memoria, de modo que cuando se activa la captura, también se captura algo de video antes del disparador.

## **Captura de películas: poscaptura / Movie capture – Post-capture**

Especifique el número de segundos para continuar capturando la película después de que se detenga el disparador de movimiento. Esto debe establecerse en al menos unos segundos para evitar que se capturen muchos archivos de película pequeños durante un período de movimiento más largo.

### **Captura de película: subir a / Movie capture – Upload to**

Habilite esta opción para cargar todos los archivos de películas de captura de movimiento a un servidor FTP para realizar copias de seguridad fuera del sitio. Si el tipo de captura se establece en Una película por día, las películas se cargarán al final del día; si el tipo de captura es Una película por evento, las películas se cargarán tan pronto como terminen.

### **Captura de imágenes: captura imágenes en respuesta al disparador de movimiento / Image capture – Capture images in response to motion trigger.**

Habilite esta opción para capturar periódicamente archivos de imagen JPEG cuando se detecte movimiento.

### **Image capture – Frequency / Image capture – Frequency**

Especifique la frecuencia de captura en términos de la cantidad de segundos entre capturas de archivos de imagen.

### **Captura de imágenes: poscaptura / Image capture – Post-capture**

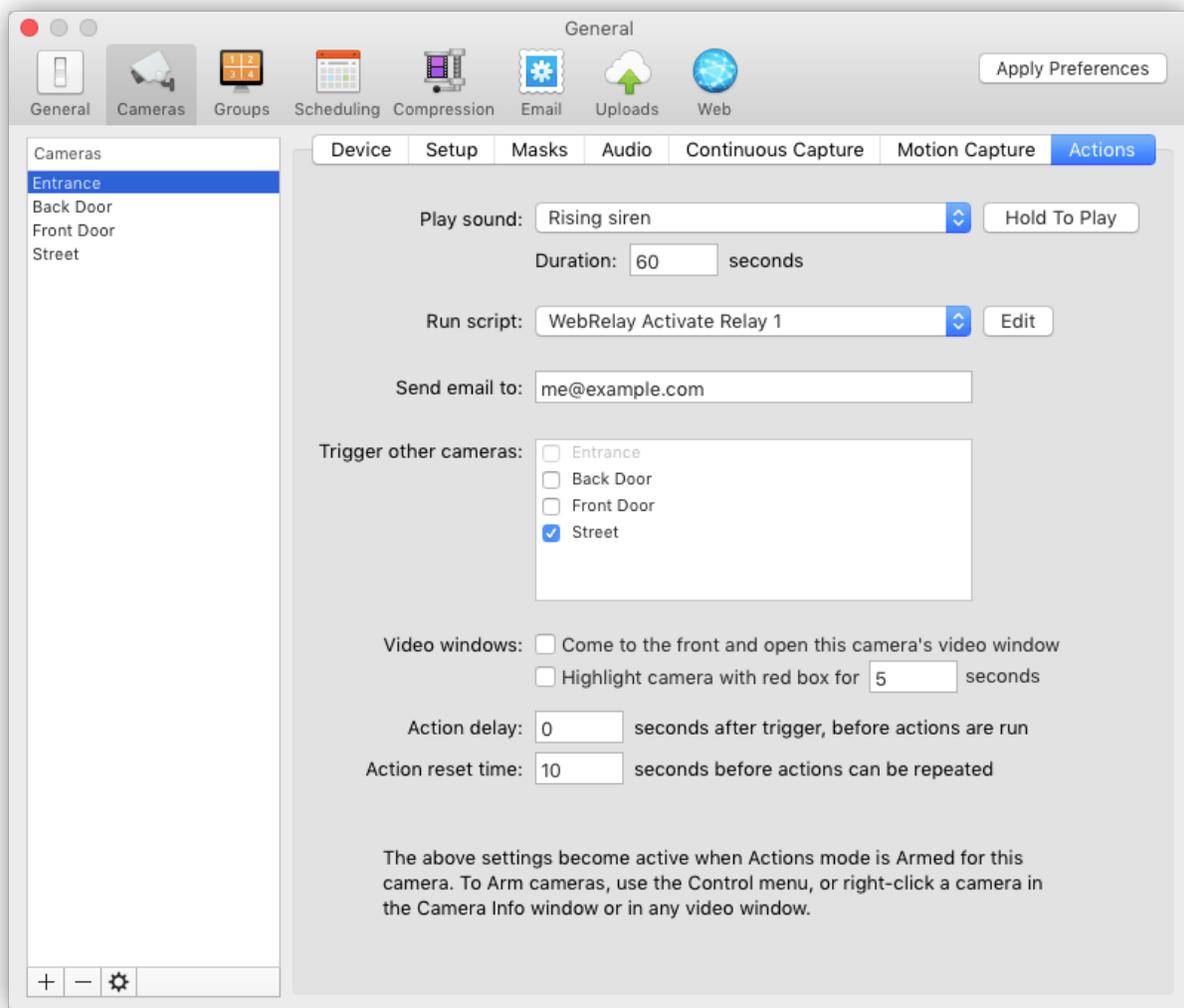
Especifique la cantidad de segundos para continuar capturando archivos de imagen después de que se detenga el disparador de movimiento.

### **Captura de imágenes: subir a / Image capture – Upload to**

Utilice esta opción para cargar todos los archivos de imágenes de captura de movimiento a un servidor FTP para realizar una copia de seguridad fuera del sitio.

## Preferencias - Cámaras - Acciones / Preferences - Cameras - Actions

Esta pestaña contiene la configuración de las acciones que se realizarán en respuesta a los activadores de movimiento configurados en la pestaña de configuración:



## **Reproducir sonido / Play sound**

Seleccione un sonido para reproducir cuando se activa el movimiento. Además de los sonidos estándar del sistema, hay varios sonidos incorporados diseñados para ahuyentar a los intrusos, y puede agregar los suyos propios colocando archivos de sonido en la carpeta Sonidos de SecuritySpy (para ubicar esta carpeta, haga clic en el menú Archivo y seleccione Revelar Carpeta en Finder / Sonidos). Se admiten la mayoría de los formatos de sonido, incluidos AIFF, WAV, MP3 y AAC.

## **Reproducir sonido – Duración/ Play sound – Duration**

Especifica la duración en segundos para reproducir el sonido después de que se detenga el disparador de movimiento.

## **Ejecutar guión / Run script**

Puede seleccionar una secuencia de comandos para ejecutar cuando se activa el movimiento. Para crear sus propios scripts, use la aplicación Script Editor que viene con macOS (esta aplicación se llama AppleScript Editor en versiones anteriores del sistema). Coloque sus scripts en la carpeta Scripts de SecuritySpy para que estén disponibles para invocarlos como acciones (para ubicar esta carpeta, haga clic en el menú Archivo y seleccione Mostrar carpeta en Finder / Scripts). Se incluyen algunos scripts con SecuritySpy, incluidos los que controlan los dispositivos de conmutación / relé que pueden activar dispositivos externos como luces y alarmas. Los scripts integrados funcionan con dispositivos WebRelay y Web-i IO.

## **Enviar el email a / Send email to**

Esta función envía un correo electrónico, opcionalmente con imágenes JPEG adjuntas, a una dirección que especifique. Para enviar el correo electrónico a varias direcciones, introdúzcalas separadas por comas.

## **Activar otras cámaras / Trigger other cameras**

Esta configuración le permite activar la grabación en una cámara en función de un activador de movimiento en otra. Esto podría ser útil cuando tiene varias cámaras que cubren la misma área y desea que la grabación se lleve a cabo en todas las cámaras cuando alguna detecta movimiento, lo que aumenta las posibilidades de capturar algo interesante.

### **Mostrar video: pase al frente y abra la ventana de video de esta cámara / Show video – Come to the front and open this camera's video window**

Si esta opción está habilitada, siempre que suceda un disparador de movimiento para esta cámara, SecuritySpy pasará al frente, sobre todas las demás aplicaciones, y mostrará la ventana de video de la cámara.

### **Retraso de acción / Action delay**

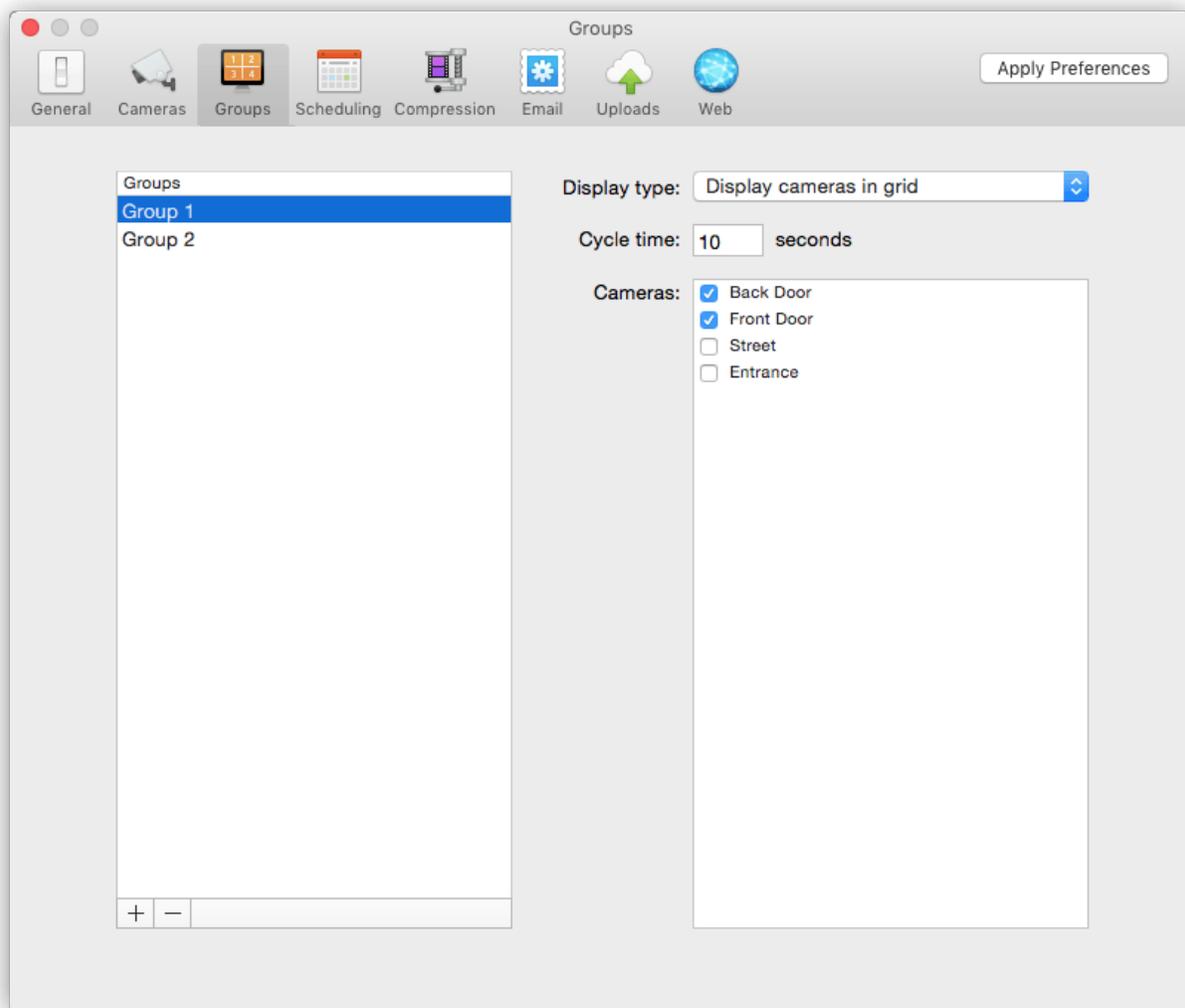
Esta opción le permite especificar un retraso en segundos después de un disparo de movimiento, antes de realizar cualquiera de las acciones.

### **Tiempo de restablecimiento de la acción / Action reset time**

Una vez que se activan las acciones, este retraso especifica el tiempo mínimo antes de que se puedan activar de nuevo. Sin este retraso, una acción podría invocarse muchas veces en rápida sucesión si hay mucho movimiento, lo que generalmente no es deseable. Por lo tanto, es aconsejable especificar aquí un retraso de al menos la duración de un evento típico de detección de movimiento.

## Preferencias – Grupos / Preferences – Groups

Esta sección le permite especificar grupos de cámaras que se pueden mostrar a través de sus propias ventanas de grupo. Para instalaciones grandes, organizar las cámaras en grupos lógicos de esta manera hace que verlas sea mucho más manejable.



## **Tipo de visualización / Display type**

Elija cómo desea que aparezcan las cámaras en la ventana del grupo: Mostrar cámaras en cuadrícula: al igual que la ventana Todas las cámaras, la ventana de grupo mostrará todas sus cámaras miembro a la vez, en una disposición de cuadrícula.

Ciclo entre cada cámara: esta opción mostrará una cámara a la vez, de forma secuencial.

## **Tiempo del ciclo / Cycle time**

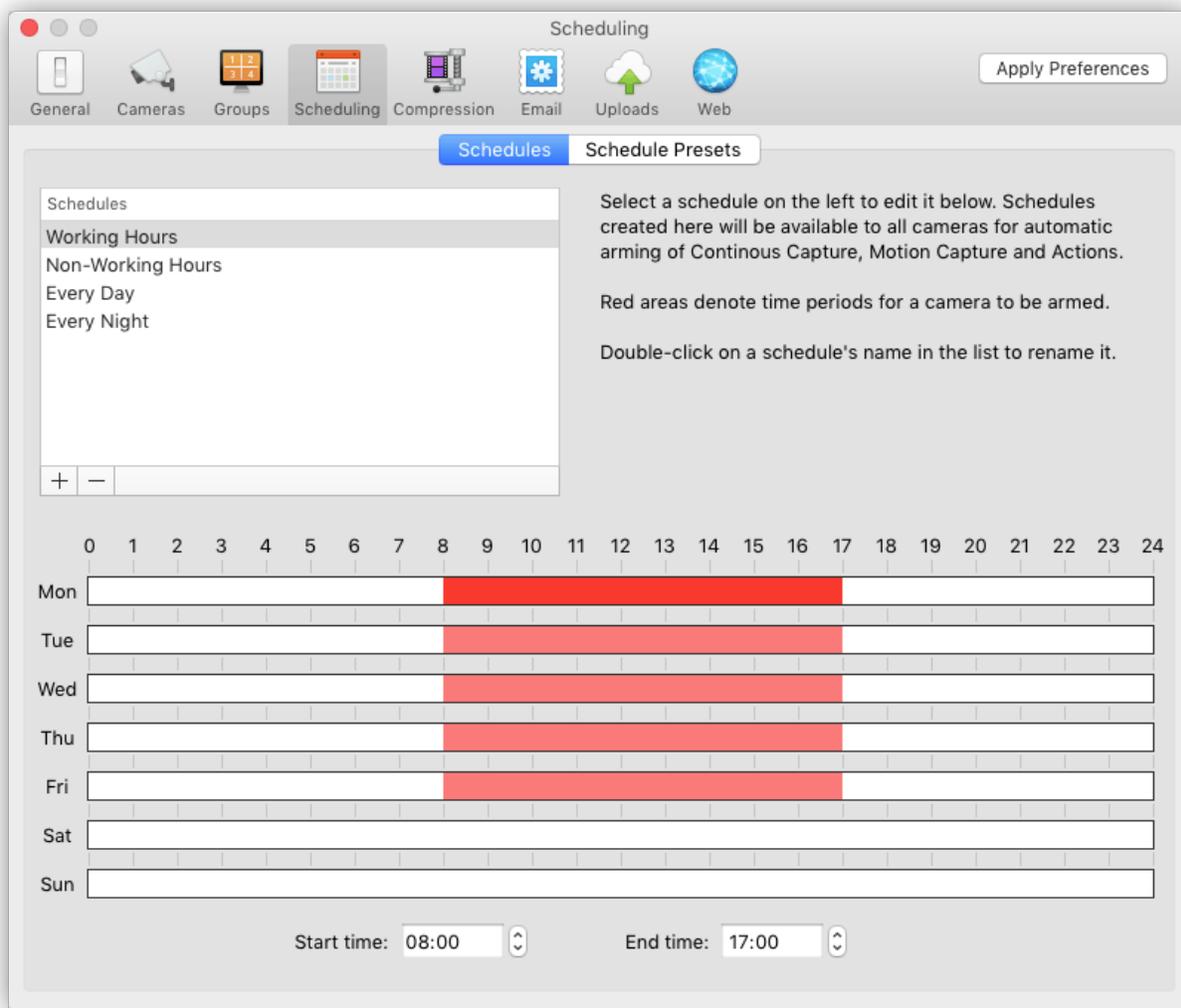
Especifique el número de segundos entre ciclos, cuando utilice cualquiera de las opciones de visualización de Ciclo.

## **Cameras / Cameras**

Simplemente habilite la casilla de verificación junto a cada cámara que desee incluir en el grupo.

## Preferencias – Programación – Horarios/ Preferences – Scheduling – Schedules

Los horarios definen cuando las cámaras deben estar armadas y desarmadas durante la semana. Todos los horarios creados aquí estarán disponibles para todas las cámaras y se pueden usar para armar sus modos de captura continua, captura de movimiento y acción de forma independiente.



Los momentos en que las cámaras estarán armadas se representan como "objetos de tiempo" rojos. Cada objeto de tiempo tiene una hora de inicio y finalización, que define cuando la cámara se armará automáticamente y luego se desarmará automáticamente. Haga clic y arrastre para crear nuevos objetos de tiempo o para mover o editar objetos de tiempo existentes. Para eliminar un objeto de hora, selecciónelo y presione la tecla Suprimir en el teclado.



Para cada cámara, puede definir un horario o puede especificar "Sin cambios" para indicar que el horario de una cámara en particular no debe cambiarse cuando se aplica el ajuste preestablecido. Los ajustes preestablecidos de programación se pueden invocar desde el menú Control.

### **Preferencias: compresión / Preferences – Compression**

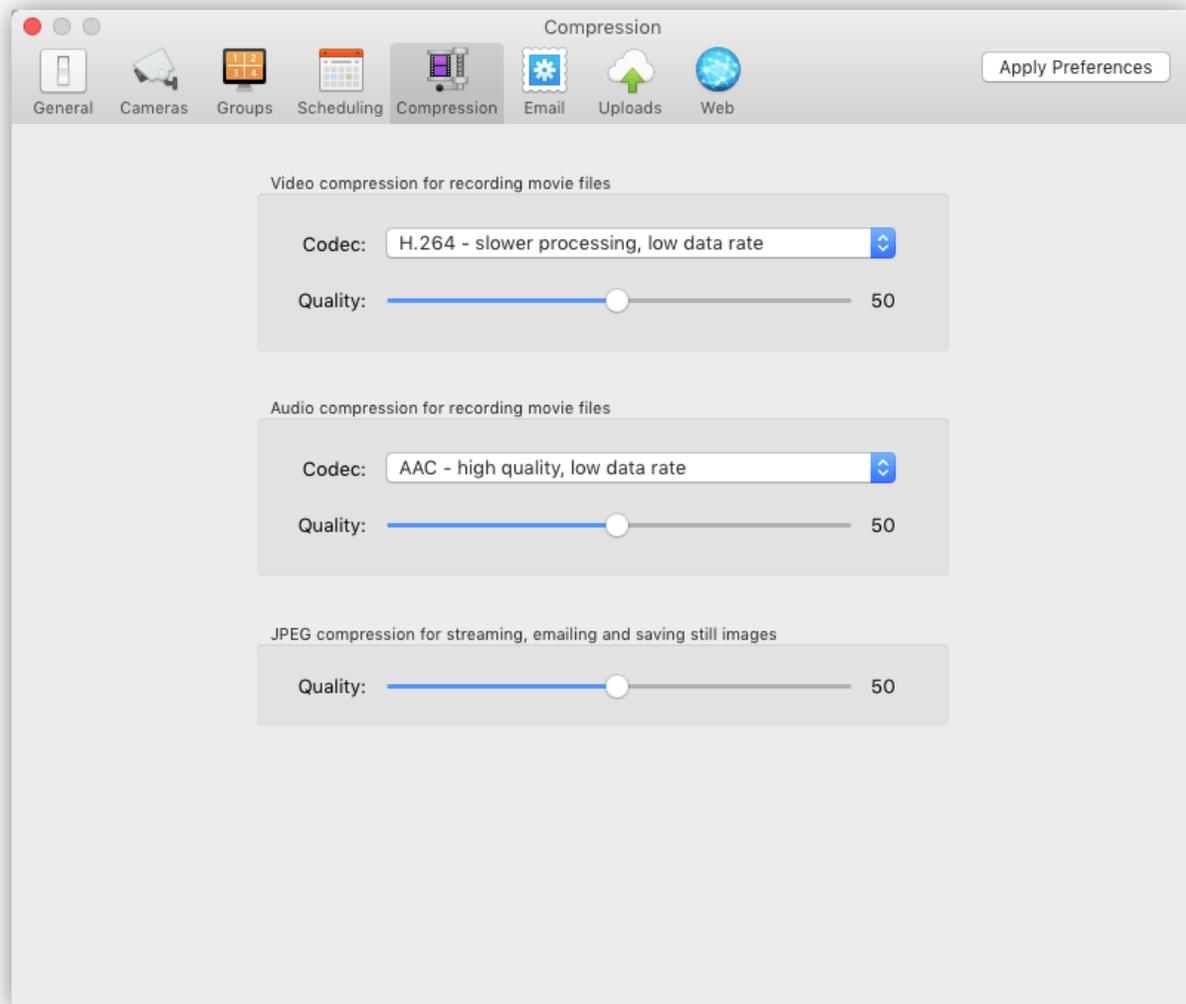
Esta sección le permite especificar la compresión de video y audio que se realizará para que SecuritySpy comprima cualquier conjunto de cámaras. Esto se aplica en los siguientes casos: Los dispositivos de video locales, como los dispositivos USB, FireWire y Thunderbolt, y las cámaras FaceTime integradas, proporcionan video sin comprimir, que SecuritySpy debe comprimir para grabar en archivos de película.

Los dispositivos de vídeo en red proporcionan vídeo comprimido y, de forma predeterminada, SecuritySpy lo grabará directamente en los archivos de película capturados. Sin embargo, para cualquier cámara para la que haya habilitado las opciones Recomprimir datos de video y / o Recomprimir datos de audio en Cámaras -> Configuración del dispositivo, SecuritySpy comprimirá sus datos de video y / o audio usando las opciones de compresión de video y compresión de audio configuradas. en esta sección.

Para cualquier cámara de red que suministre datos de video H.264, para una calidad y un rendimiento óptimos, no debe habilitar la opción Volver a comprimir datos de video en Cámaras -> Configuración del dispositivo a menos que necesite hacerlo por alguna razón específica (por ejemplo, si desea SecuritySpy para agregar una superposición de fecha / hora en la transmisión de video y la cámara no puede hacer esto).

Limitar el uso de la recompresión de audio es menos importante, porque requiere mucho menos tiempo de CPU que la recompresión de video. Idealmente, sus cámaras pueden suministrar audio en formato AAC, pero para cualquier cámara que no pueda, es posible que desee configurar SecuritySpy para que vuelva a codificar en formato AAC.

La ventaja de grabar audio AAC es que SecuritySpy puede crear archivos de película MP4 (en lugar de archivos de película MOV), que son mucho más compatibles para su reproducción en navegadores web. Si no necesita reproducir los archivos capturados en navegadores web, es mejor dejar desactivada la opción Recomprimir datos de audio.



## Compresión de video – Códec / Video Compression – Codec

Elija entre los siguientes códecs de compresión de video: JPEG: produce video de alta calidad y se comprime rápido, por lo que el rendimiento con este códec es muy bueno; sin embargo, el tamaño de los archivos de película capturados será grande. MPEG-4: produce video a velocidades de datos más bajas que JPEG. Es bastante rápido de comprimir y ofrecerá un buen rendimiento en una computadora razonablemente rápida. Este es un códec algo obsoleto, que solo está disponible cuando se ejecuta la versión de 32 bits de SecuritySpy.

H.264: este es un códec muy eficiente que producirá archivos de tamaño pequeño. En las Mac modernas con capacidades de compresión de video por hardware integradas, esto será rápido de comprimir, pero la cantidad de cámaras que se pueden comprimir por hardware variará entre los modelos de Mac. En Mac mas antiguas sin capacidades de compresión de video por hardware, esto usa un tiempo de CPU significativo para comprimir. Utilice esta opción sí necesita SecuritySpy para crear archivos de películas MP4 que se reproduzcan en los navegadores web.

MPEG-4 y H.264 admiten la compresión temporal. Dependiendo del contenido, el video puede tener un alto nivel de redundancia temporal, es decir, muy a menudo un fotograma es similar al último fotograma. La compresión temporal aprovecha esta redundancia para reducir el tamaño del archivo del video resultante. La compresión temporal funciona mediante el uso de "fotogramas clave" a intervalos regulares, seguidos de varios "fotogramas delta". Los fotogramas clave contienen la imagen de video completa; los fotogramas delta contienen solo las partes de la imagen que han cambiado desde el último fotograma clave.

Las imágenes de las cámaras de vigilancia a menudo tienen un alto nivel de redundancia temporal porque, por lo general, la mayor parte de la imagen es constante y solo una pequeña parte cambia. Por lo tanto, el uso de la compresión temporal puede disminuir significativamente el tamaño de los archivos capturados sin degradar significativamente la calidad.

### **Compresión de video – Calidad / Video Compression – Quality**

Cuanto mayor sea el ajuste de calidad, mejor será la calidad visual de los archivos de película resultantes. Sin embargo, una configuración de mayor calidad dará como resultado archivos más grandes. Una configuración de alrededor de 50-60 es normalmente ideal.

### **Compresión de audio – Códec / Audio Compression – Codec**

Elija entre los siguientes códec de compresión de audio: Ninguno: sin compresión: esta configuración ofrece la mejor calidad y el menor uso del procesador. Dado que la velocidad de datos del audio es generalmente mucho más baja que la del video, a menos que requiera tamaños de archivo muy pequeños, no usar compresión de audio puede ser una buena opción.

Si elige esta opción, debe establecer una frecuencia de muestreo baja y audio mono para minimizar la velocidad de datos (estas opciones se configuran de forma independiente para cada dispositivo, a través de Cámaras -> Configuración de audio).

Apple Lossless: esto proporciona una calidad igual a ninguna compresión (ya que es un códec sin pérdidas), aproximadamente a la mitad de la velocidad de datos, y es bastante rápido de comprimir.  $\mu$ -Law: Este es un códec muy eficiente diseñado específicamente para comprimir voz rápidamente a una velocidad de datos muy baja (64 kbps).

AAC: produce audio de alta calidad a velocidades de datos bajas, pero es el códec disponible con él procesador más intensivo. Utilice esta opción si necesita SecuritySpy para crear archivos de películas MP4 que se reproduzcan en los navegadores web.

### **Compresión de audio – Calidad / Audio Compression – Quality**

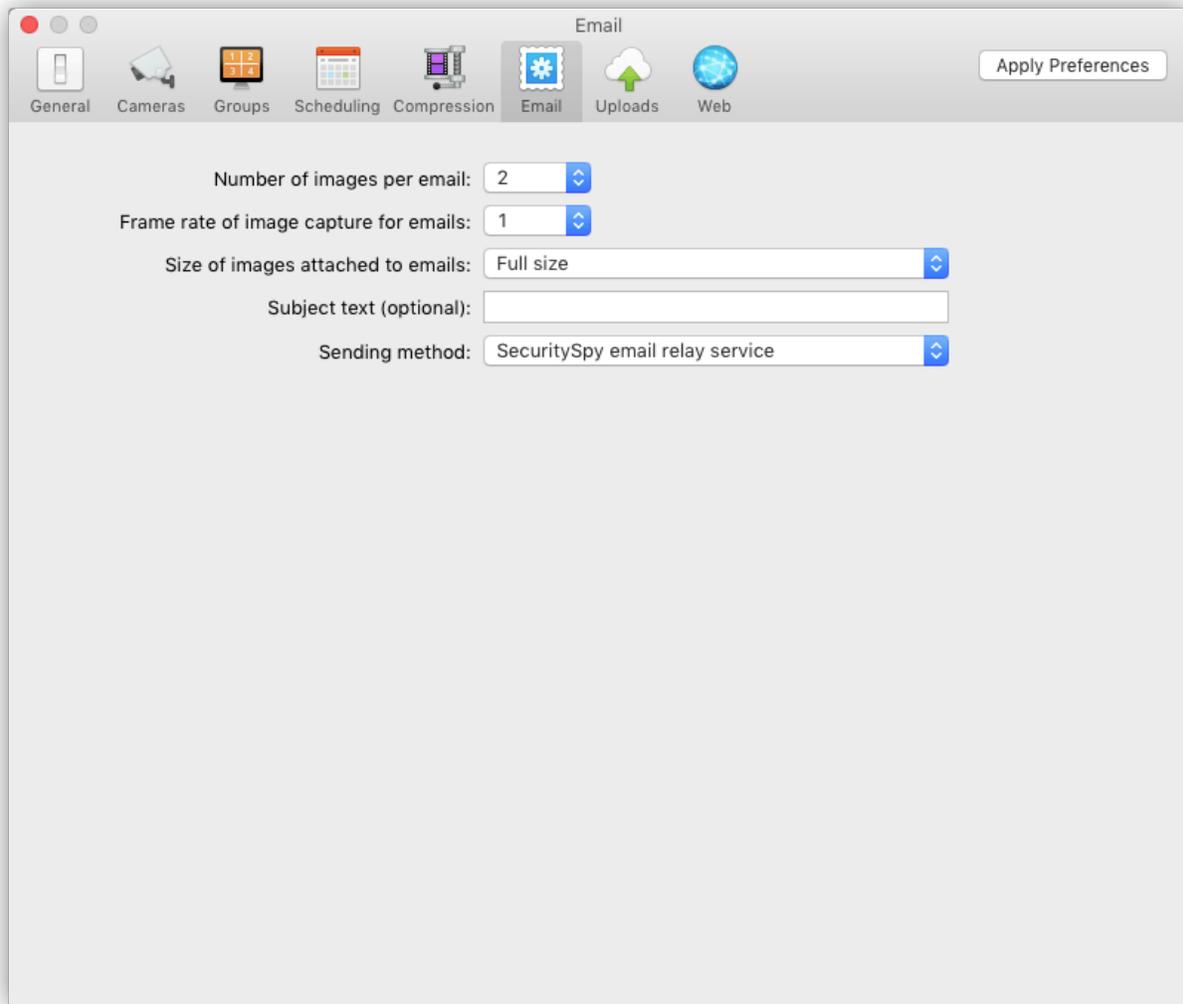
Para el códec AAC, puede establecer un nivel de calidad, que determinará la tasa de bits de los datos de audio codificados (la tasa de bits exacta utilizada dependerá de la frecuencia de muestreo del audio de origen, que puede variar de una cámara a otra). Un valor de alrededor de 50 proporciona un audio de calidad razonablemente buena a una tasa de bits eficiente.

### **Compresión JPEG / JPEG Compression**

Siempre que SecuritySpy necesite crear una imagen JPEG fija, utilizará esta configuración de calidad para la codificación. Esto se aplica a las imágenes fijas capturadas en el disco, las imágenes adjuntas a los correos electrónicos y las imágenes enviadas a través de la interfaz web.

## Preferencias: correo electrónico / Preferences – Email

Esta sección le permite especificar la configuración para enviar correos electrónicos:



### Número de imágenes por correo electrónico / Number of images per email

Cuando se envía un correo electrónico en respuesta a un disparador de movimiento en una cámara en particular, esta configuración define ahora que muchas imágenes JPEG de la cámara se adjuntarán al correo electrónico.

### Velocidad de fotogramas de captura de imágenes para correos electrónicos / Frame rate of image capture for emails

Esto define la velocidad de fotogramas a la que se agregan las imágenes a los correos electrónicos activados por movimiento.

## **Tamaño de las imágenes adjuntas a los correos electrónicos / Size of images attached to emails**

Puede enviar imágenes a tamaño completo, pero con cámaras de alta resolución esto da como resultado correos electrónicos grandes que tardan en transferirse. Para mantener los tamaños de correo electrónico pequeños y las velocidades de transferencia altas, elija un tamaño mas pequeño de una de las opciones disponibles.

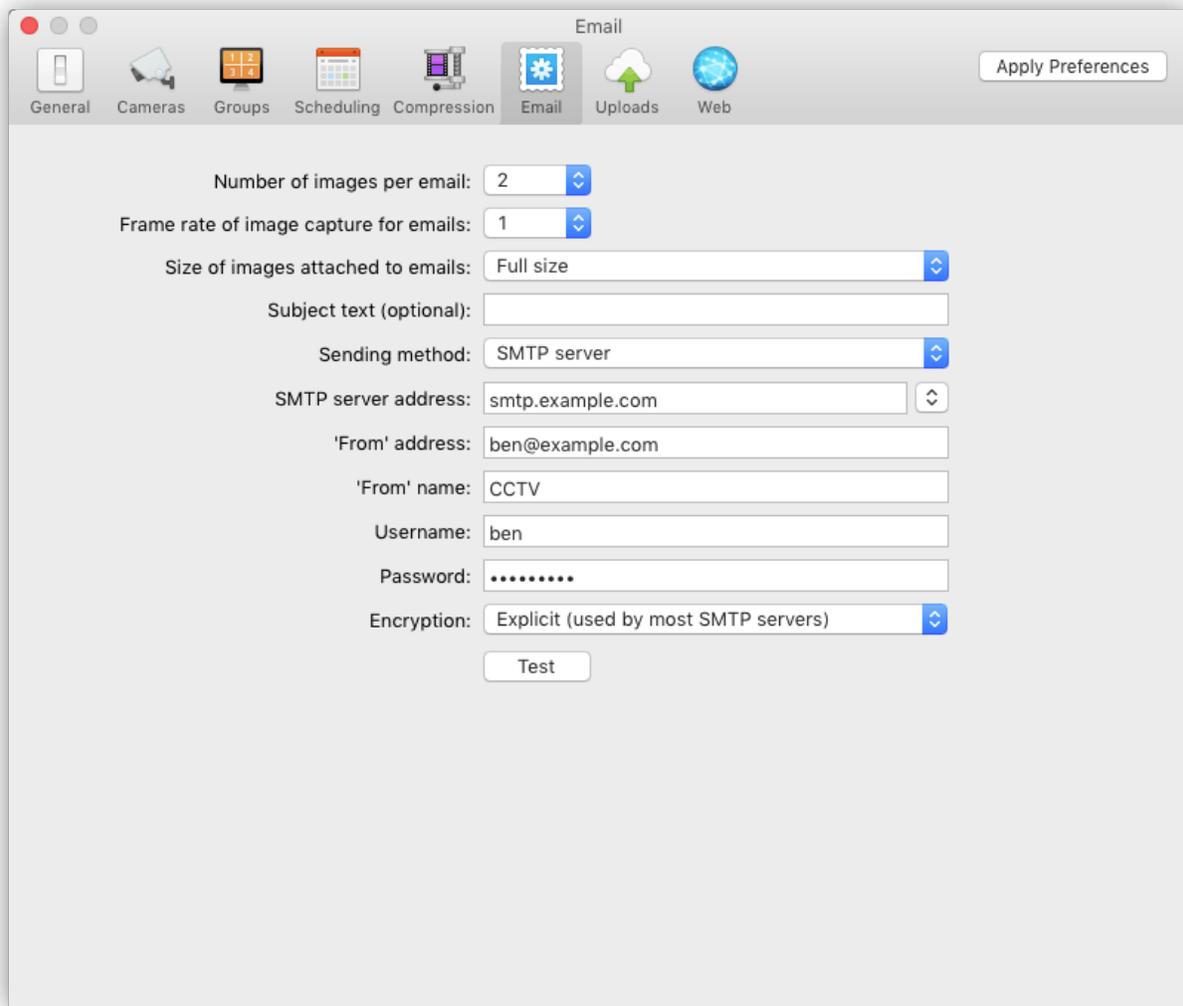
## **Texto del asunto / Subject text**

Este es el campo de asunto que se utiliza para los correos electrónicos activados por detección de movimiento. Si deja este espacio en blanco, se creará un asunto automáticamente. Al especificar un tema personalizado, puede ingresar + d para la fecha y hora actuales, y + n para el nombre de la cámara.

## **Método de envío / Sending method**

De forma predeterminada, SecuritySpy utilizará su propio servicio de retransmisión de correo electrónico, que no requiere configuración alguna. Este servicio lo proporcionamos nosotros y su uso es gratuito para todos los usuarios de SecuritySpy (aunque limitamos el tamaño y la frecuencia de los correos electrónicos para garantizar un buen rendimiento para todos los usuarios).

La otra opción es usar su propio servidor SMTP; esto requiere la siguiente configuración:



### Dirección del servidor SMTP / SMTP server address

La dirección del servidor utilizado para enviar correo. Esto normalmente lo proporciona su ISP (proveedor de servicios de Internet). Si su servidor usa un puerto no estándar, puede especificarlo aquí usando dos puntos y luego el número de puerto. Por ejemplo, si su servidor usa el puerto 28, debe ingresar "smtp.example.com:28". La mayoría de los servidores SMTP operan en puertos estándar (25 para comunicación no cifrada y 465 para comunicación SSL cifrada), por lo que si su ISP no le ha dicho que use un puerto en particular, no especifique un número de puerto y el estándar lo hará. ser utilizado automáticamente.

El pequeño menú emergente a la derecha de este campo contiene algunos ajustes preestablecidos para cuentas de correo electrónico comunes; seleccione uno y la dirección del servidor, cualquier otra configuración apropiada se establecerá automáticamente.

### **'De la Dirección / 'From' address**

Esta es la dirección de devolución que se envía con los correos electrónicos para identificar al remitente. Siempre debe usar una dirección de correo electrónico válida aquí, ya que los filtros de spam bloquearán los mensajes que no tengan una. Además, muchos servidores SMTP no aceptan cualquier dirección de retorno: normalmente debe ser del mismo proveedor que el servidor SMTP.

### **'De' nombre / 'From' name**

Este es el nombre asociado con la dirección de retorno. Es opcional, sin embargo, si no especifica un nombre aquí, existe una mayor probabilidad de que los filtros de correo no deseado bloqueen los correos electrónicos.

### **Nombre de usuario y contraseña / Username and password**

La mayoría de los servidores SMTP requieren autenticación; si el suyo lo requiere, ingrese aquí su nombre de usuario y contraseña. El nombre de usuario suele ser su dirección de correo electrónico.

### **Cifrado / Encryption**

Puede elegir entre sin cifrado, cifrado implícito o cifrado explícito (si su servidor de correo utiliza cifrado, probablemente utilizará el método explícito). Un número cada vez mayor de servidores de correo electrónico admiten el cifrado (algunos incluso lo requieren), sin embargo, muchos servidores no lo admiten, y habilitar esta función cuando se utilizan dichos servidores evitará que se envíen correos electrónicos. Por lo tanto, debe consultar las instrucciones proporcionadas por el proveedor del servidor SMTP y habilitar esta función solo si su servidor de correo electrónico la admite.

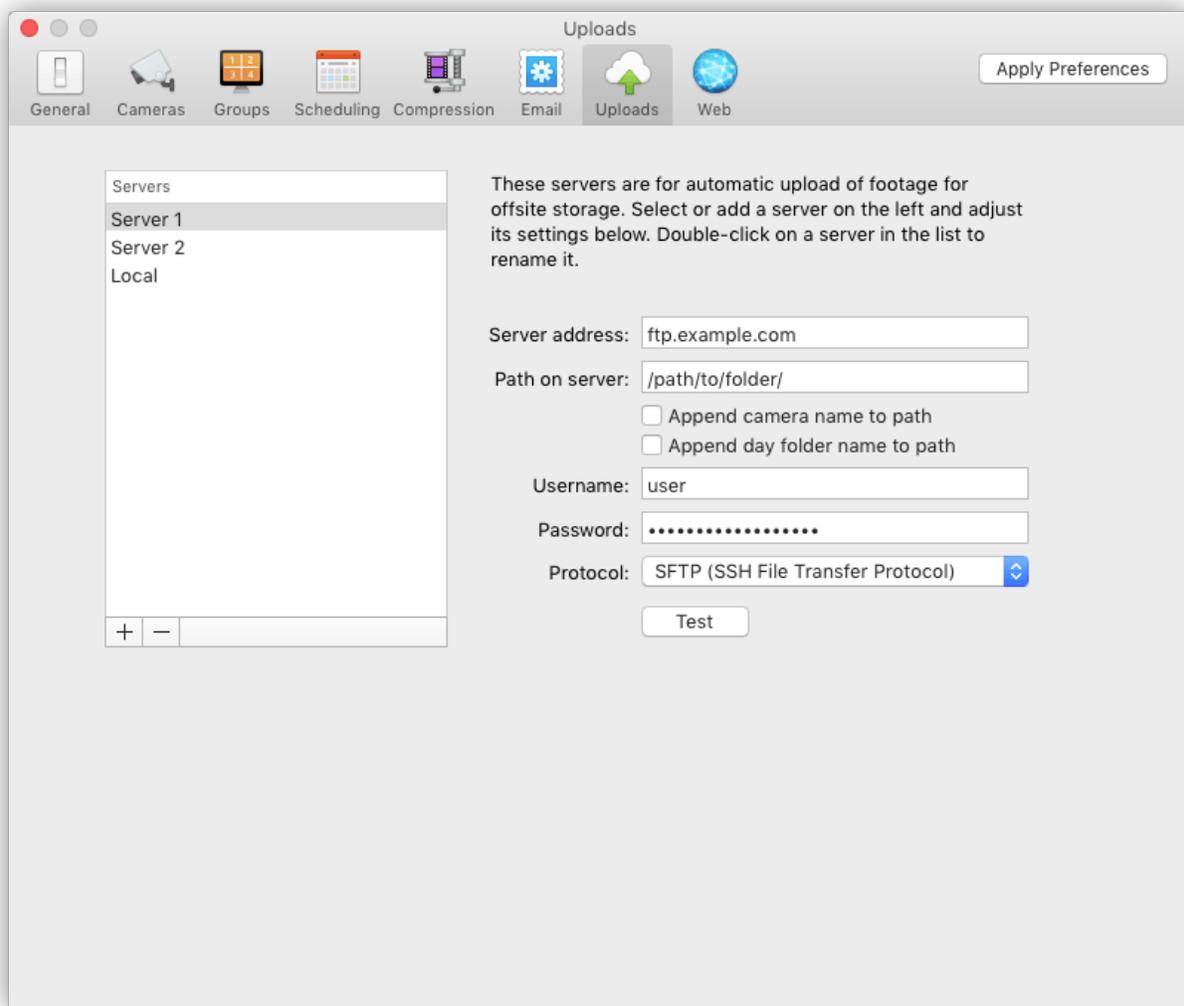
### **Botón de prueba / Test button**

Una vez que haya configurado los ajustes de correo electrónico, puede probarlos haciendo clic en este botón. SecuritySpy intentará enviar un correo electrónico de prueba e informará cualquier problema que encuentre

## Preferencias: subidas / Preferences – Uploads

Esta sección le permite especificar la configuración para cargas FTP a servidores remotos, lo cual es útil para la copia de seguridad de metraje fuera del sitio. El mismo servidor FTP con diferentes rutas se puede utilizar para diferentes destinos de carga, por lo que una cámara se puede configurar para cargar en un directorio particular en el servidor y otra cámara en un directorio diferente en el mismo servidor.

Para comprobar las rutas de directorio y descargar o eliminar archivos, deberá utilizar una utilidad gráfica de cliente FTP como Cyberduck.



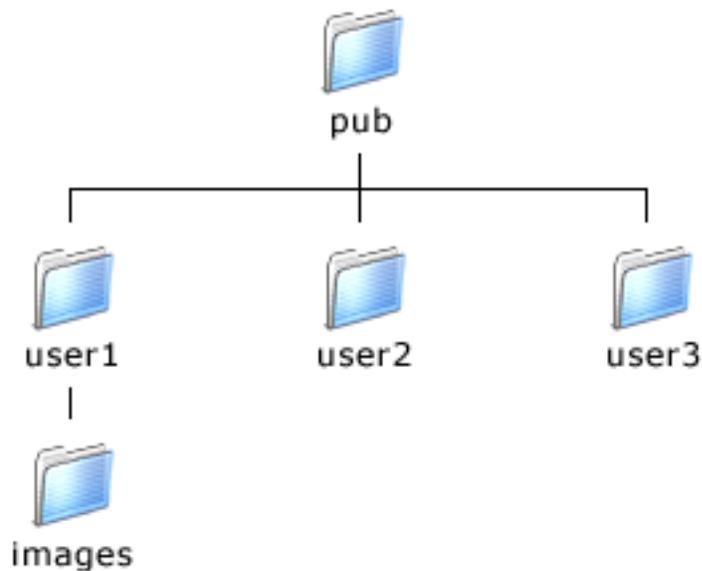
## Dirección del servidor / Server address

Ingrese la dirección IP (por ejemplo, 192.168.1.1) o el nombre de host (por ejemplo, ftp.example.com) del servidor FTP.

## Ruta en el servidor / Path on server

Si especifica una ruta que comienza con un carácter de barra inclinada, esto denota una ruta absoluta desde el directorio raíz del servidor. Una ruta que no comienza con un carácter de barra inclinada denota una ruta relativa desde el directorio predeterminado. El directorio predeterminado depende del servidor; por lo general, cada usuario tiene una carpeta en el servidor que se utiliza como directorio predeterminado y el servidor la configura automáticamente cuando ese usuario inicia sesión.

Por ejemplo, considere el siguiente diseño de directorio:



Si tuviera que iniciar sesión como usuario1, lo más probable es que el servidor establezca el directorio inicial como / pub / usuario1 /. En este caso, para que las imágenes se carguen en el directorio user1, puede dejar el campo de ruta vacío o puede especificar que "/ pub / user1 /" sea explícito. Para que las imágenes se carguen en la carpeta "images" dentro de la carpeta "user1", puede especificar "/ pub / user1 / images /" o simplemente "images" para la ruta (en todos los casos, no importa si coloca una barra diagonal al final de la ruta o no). Generalmente, debe dejar que el servidor decida el directorio predeterminado y usar una ruta relativa, a menos que tenga una razón específica para usar una ruta absoluta.

Si el directorio especificado aún no existe en el servidor, SecuritySpy intentará crearlo.

### **Agregar el nombre de la cámara a la ruta / Append camera name to path**

Habilite esta opción para agregar automáticamente los nombres de las cámaras a la ruta del servidor, de modo que cada cámara se cargue en una carpeta separada en el servidor.

### **Agregar el nombre de la carpeta del día a la ruta / Append day folder name to path**

Habilite esta opción para agregar automáticamente los nombres de las carpetas del día a la ruta del servidor, de modo que los archivos de cada día se coloquen en carpetas separadas en el servidor. Los nombres de las carpetas de días comprenden la fecha en la que se creó el archivo, con el formato AAAA-MM-DD.

### **Protocolo / Protocol**

Elija entre los siguientes protocolos:

FTP: este es el protocolo estándar de transferencia de archivos no cifrados. Tiene un amplio soporte y es confiable, sin embargo, no estar cifrado no es tan seguro como los dos protocolos siguientes. FTPS: a veces llamado FTP-SSL, esta es la versión encriptada segura del protocolo FTP. Desafortunadamente, no cuenta con un apoyo muy amplio. SFTP: a veces llamado Protocolo de transferencia de archivos SSH, se trata de un protocolo de transferencia de archivos seguro ampliamente admitido que proporciona una comunicación cifrada segura. Este es generalmente el que debe usar cuando desea cifrado.

### **Copia local / Local Copy**

Para copiar los archivos a una unidad local, en lugar de un servidor remoto, ingrese local como la dirección del servidor y especifique la ruta de una carpeta en su sistema de archivos local (arrastre la carpeta desde el Finder al cuadro Ruta para completar la ruta salir automáticamente).

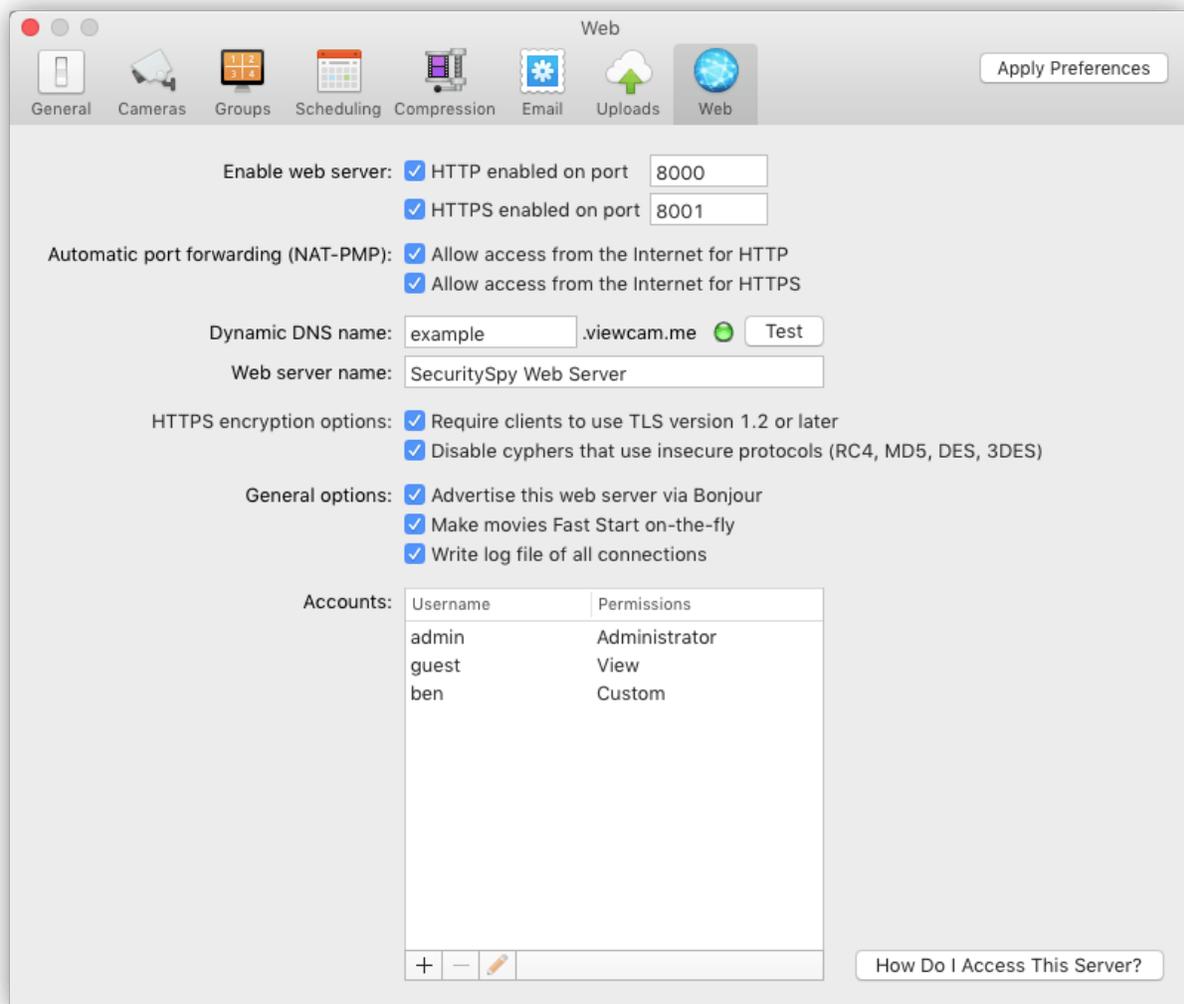
Las rutas a las carpetas en el sistema de archivos local normalmente comienzan con / Volumes / VolumeName /... para referirse a una carpeta en un volumen adjunto, o / Users / UserName /... para referirse a una carpeta dentro de su directorio de usuario.

## Status

Para ver el estado de las cargas actuales en cualquier momento, seleccione Cargas en el menú Ventana.

## Preferencias – Web / Preferences – Web

SecuritySpy cuenta con un servidor web incorporado que le permite ver transmisiones de cámara en vivo, descargar imágenes capturadas, cambiar configuraciones y controlar el software, todo desde una ubicación remota a través de una red local o Internet.



## Habilitar servidor web / Enable web server

SecuritySpy incluye una interfaz web HTTP estándar y una interfaz web HTTPS segura cifrada. HTTP estándar envía y recibe datos en su forma sin procesar, lo que es adecuado para redes locales pero no es seguro para comunicarse a través de Internet, donde los datos podrían ser interceptados por un tercero.

Por el contrario, HTTPS es un protocolo seguro que emplea cifrado, lo que dificulta enormemente que alguien descodifique los datos interceptados. Por lo tanto, se prefiere HTTPS para enviar información confidencial a través de Internet, como contraseñas y metraje de cámaras CCTV.

Los servidores HTTP y HTTPS operan cada uno en su propio puerto de red. Un número de puerto representa un "canal" para la comunicación de red y permite que diferentes aplicaciones en el mismo dispositivo utilicen la red sin interferir entre sí. Tenga en cuenta que en macOS, no es posible que una aplicación como SecuritySpy use puertos por debajo de 1024 (a menos que lo ejecute específicamente como un proceso raíz, lo cual no es recomendable). Los puertos predeterminados de SecuritySpy son 8000 y 8001 para HTTP y HTTPS respectivamente.

Desde otra computadora en su red local (LAN), puede acceder al servidor con un navegador web utilizando la dirección IP y el número de puerto del servidor:

Bonjour nombre y número de puerto, por ejemplo:

```
http://192.168.1.4:8000  
https://192.168.1.4:8001  
http://mac-pro.local:8000  
https://mac-pro.local:8001
```

Cuando utilice la función DDNS junto con las opciones de reenvío automático de puertos (consulte a continuación las explicaciones de estas funciones), podrá acceder a SecuritySpy desde Internet de esta manera:

```
http://example.viewcam.me:8000  
https://example.viewcam.me:8001
```

Tenga en cuenta que las direcciones de red local no funcionarán desde Internet, y es posible que las direcciones de Internet no funcionen desde su red local (dependiendo de su enrutador).

Haga clic en [¿Cómo accedo a este servidor?](#) para obtener una lista de las direcciones que puede utilizar para acceder a su servidor SecuritySpy desde su red local y desde Internet. Si necesita configurar la dirección IP de LAN de su Mac, puede hacerlo a través del panel Red de las Preferencias del sistema.

## **Certificados y claves HTTPS / HTTPS Keys and Certificates**

Los servidores seguros requieren una clave privada y un certificado para realizar el cifrado e identificar el servidor. Hay dos tipos de certificado que puede utilizar: un certificado autofirmado o un certificado firmado por una autoridad de certificación. Ambos proporcionan el mismo nivel de cifrado, sin embargo, los certificados autofirmados no proporcionan el mismo nivel de garantía al cliente con respecto a la autenticidad del servidor, por lo que un navegador web que se conecte a dicho servidor mostrará una advertencia a tal efecto. Sin embargo, para SecuritySpy, usted es quien configura el servidor y, por lo tanto, puede estar seguro de su autenticidad. Por lo tanto, el uso de un certificado autofirmado para SecuritySpy es totalmente adecuado; simplemente ignore la advertencia que muestra el navegador web.

Aquí hay una advertencia, ya que iOS se negará a reproducir archivos de películas entregados por un servidor HTTPS con un certificado autofirmado. Por lo tanto, si desea reproducir películas en un iPad o iPhone, deberá usar la interfaz HTTP estándar o deberá comprar un certificado oficial para usar con SecuritySpy.

La dirección que utiliza para acceder a SecuritySpy debe coincidir con el nombre de host del certificado; de lo contrario, recibirá una advertencia adicional del navegador web sobre una discrepancia en el nombre de host. Por lo tanto, para conectarse a SecuritySpy a través de Internet, le recomendamos que utilice la función de DNS dinámico de SecuritySpy (ver más abajo), configure esto como el nombre de host en el certificado y lo use para acceder a SecuritySpy a través de Internet.

Para utilizar un certificado autofirmado con SecuritySpy, simplemente habilite la opción "Servidor HTTPS habilitado" en la ventana anterior: SecuritySpy generará una clave y un certificado automáticamente. La dirección DNS dinámica que ha configurado se utilizará como el nombre de host del certificado, así que asegúrese de crearlo y utilizarlo para acceder a SecuritySpy.

Para utilizar un certificado obtenido de una autoridad de certificación, primero deberá generar una clave privada y una solicitud de firma de certificado (normalmente, utilizando OpenSSL a través de la Terminal; la autoridad de certificación debe proporcionar las instrucciones).

Envía la solicitud de firma del certificado a la autoridad de certificación y esta le devuelve un certificado firmado. Coloque la clave privada, el certificado principal y cualquier certificado intermedio en la carpeta SecuritySpy dentro de la carpeta Inicio (es decir, ~ / SecuritySpy /), y luego salga y reinicie SecuritySpy.

Al suministrar una clave privada, debe ser la siguiente: El nombre del archivo debe ser "server.key" El formato debe ser PEM o DER binario La clave no debe tener ningún requisito de contraseña.

Al suministrar un certificado, debe ser el siguiente: El nombre del archivo debe ser "server.crt" El formato debe ser PEM o DER binario.

Certificados intermedios: Su certificado puede venir con certificados intermedios, que forman la "cadena de certificados". Si se le ha proporcionado un archivo "ca-bundle", colóquelo en la carpeta SecuritySpy De lo contrario, coloque todos los archivos de certificado .crt y .pem intermedios en la carpeta SecuritySpy Asegúrese de no incluir ningún archivo .crt o .pem que no esté vinculado a su certificado principal

### **Reenvío automático de puertos / Automatic port forwarding**

Para permitir el acceso a SecuritySpy desde Internet, su enrutador debe estar configurado para reenviar las conexiones entrantes a SecuritySpy. Utilice estas opciones para habilitar el reenvío automático de puertos para el puerto HTTP y / o HTTPS. Para que esto funcione, su enrutador debe admitir y tener habilitado el Protocolo de asignación de puertos NAT (NAT-PMP) o Universal Plug and Play (UPnP).

Casi todos los enrutadores admiten al menos uno de estos protocolos y la mayoría tiene esta función habilitada de forma predeterminada.

**IMPORTANTE:** al utilizar esta función, su sistema se vuelve mucho más fácil de acceder desde Internet, por lo que debe crear al menos una cuenta de servidor web, con una contraseña segura, para proteger su servidor web SecuritySpy.

## Dynamic DNS name (DDNS)

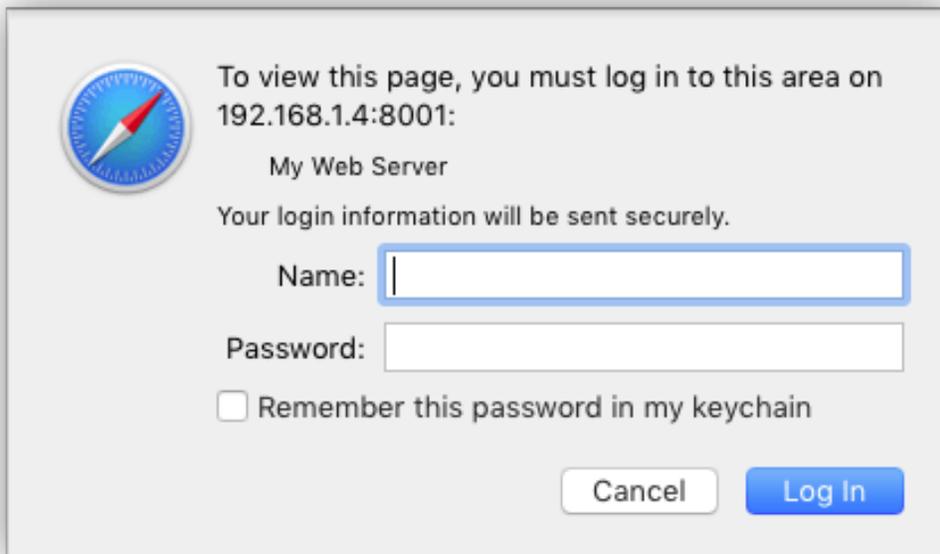
La mayoría de las conexiones a Internet proporcionan una dirección IP pública dinámica, que puede cambiar de vez en cuando. Si desea acceder a su sistema a través de Internet, necesitará una dirección estática, que es lo que proporciona el sistema DDNS de SecuritySpy.

Simplemente ingrese el nombre DDNS que desea usar y haga clic en el botón Probar; el indicador se volverá verde para indicar éxito o rojo para indicar un problema (por ejemplo, si el nombre que solicitó no está disponible). Una vez habilitada, la dirección de Internet `example.viewcam.me` siempre apuntará a su dirección IP pública, incluso cuando cambie.

**IMPORTANTE:** con DDNS habilitado, su sistema se vuelve más fácil de acceder desde Internet, por lo que debe crear al menos una cuenta de servidor web, con una contraseña segura, para proteger su servidor web.

## Nombre del servidor web / Web server name

Puede introducir aquí cualquier texto para personalizar el nombre del servidor web. Además de ser utilizado como el nombre Bonjour (ver más abajo), un navegador web muestra este nombre cuando solicita autenticación. Por ejemplo, este es el mensaje que muestra el navegador web Safari cuando se conecta a un servidor protegido con contraseña con el nombre "Mi servidor web" (otros navegadores web muestran mensajes similares):



The image shows a Safari login dialog box. On the left is the Safari compass icon. The text reads: "To view this page, you must log in to this area on 192.168.1.4:8001: My Web Server". Below this, it says "Your login information will be sent securely." There are two input fields: "Name:" and "Password:". Below the password field is a checkbox labeled "Remember this password in my keychain". At the bottom right are two buttons: "Cancel" and "Log In".

Exigir a los clientes que usen TLS versión 1.2 o posterior (opción disponible en macOS 10.9 o posterior) Esto requiere que los clientes web HTTPS utilicen la versión más reciente y segura de TLS (el protocolo criptográfico subyacente a HTTPS). Deje esta opción habilitada a menos que necesite que el servidor web sea accesible para los clientes más antiguos que no son compatibles con TLS 1.2. Tenga en cuenta que las versiones del sistema macOS anteriores a la 10.9 no son compatibles con TLS 1.2, por lo que la mayoría del software que se ejecuta en estos sistemas no podrá conectarse al servidor si esta opción está habilitada.

Deshabilite los cifrados que usan protocolos inseguros (opción disponible en macOS 10.8 o posterior) Existe una variedad de protocolos criptográfico diferentes que se pueden utilizar para una conexión HTTPS; estos se negocian entre el cliente y el servidor cada vez que se establece una nueva conexión. Se ha encontrado que muchos protocolos más antiguos (como RC4, MD5 y DES) tienen fallas de seguridad y, por lo tanto, deben evitarse si es posible. Habilitar esta opción asegura que no se utilizarán estos protocolos inseguros; sin embargo, esto puede evitar que los clientes más antiguos puedan conectarse al servidor web.

### **Anuncie este servidor web a través de Bonjour / Advertise this web server via Bonjour**

Bonjour es un método de configuración de red de "configuración cero", que facilita la búsqueda de dispositivos. Habilitar Bonjour permite que Safari, las aplicaciones de iOS y otras instancias de SecuritySpy encuentren fácilmente su servidor SecuritySpy en la red.

### **Haz películas Fast Start sobre la marcha / Make movies Fast Start on-the-fly**

Normalmente, las películas QuickTime y los archivos MP4 tienen un recurso de película al final del archivo (el recurso de película contiene la información necesaria sobre todos los fotogramas de la película y por lo tanto, debe escribirse en el archivo en último lugar, después de que se hayan escrito todos los fotogramas).

Esto funciona bien cuando la película está en una unidad local porque el recurso de la película es accesible instantáneamente; sin embargo, si la película se recibe de una fuente más lenta, como Internet, debe descargarse toda la película antes de que pueda reproducirse, lo que puede llevar un tiempo. En las películas de inicio rápido, el recurso de la película se encuentra al principio del archivo para que la película pueda comenzar a reproducirse antes de que se haya descargado por completo.

Si esta opción está habilitada, el recurso de la película se leerá desde el final del archivo y se enviará primero, por lo que la película se iniciará rápidamente cuando la reciba la computadora cliente.

### **Escribir archivo de registro de todas las conexiones / Write log file of all connections**

Cuando está habilitado, SecuritySpy creará un archivo de texto que contiene información sobre cada conexión al servidor web, incluido el tiempo de conexión, la dirección del cliente y la página solicitada.

Para ver el registro, seleccione la opción "Abrir registro web" del menú Archivo en SecuritySpy. SecuritySpy usa el texto del nombre del servidor (ver arriba) como su nombre Bonjour. Tenga en cuenta que si ha habilitado la función de firewall de macOS en la computadora que ejecuta SecuritySpy, esto puede impedir que Bonjour funcione correctamente.

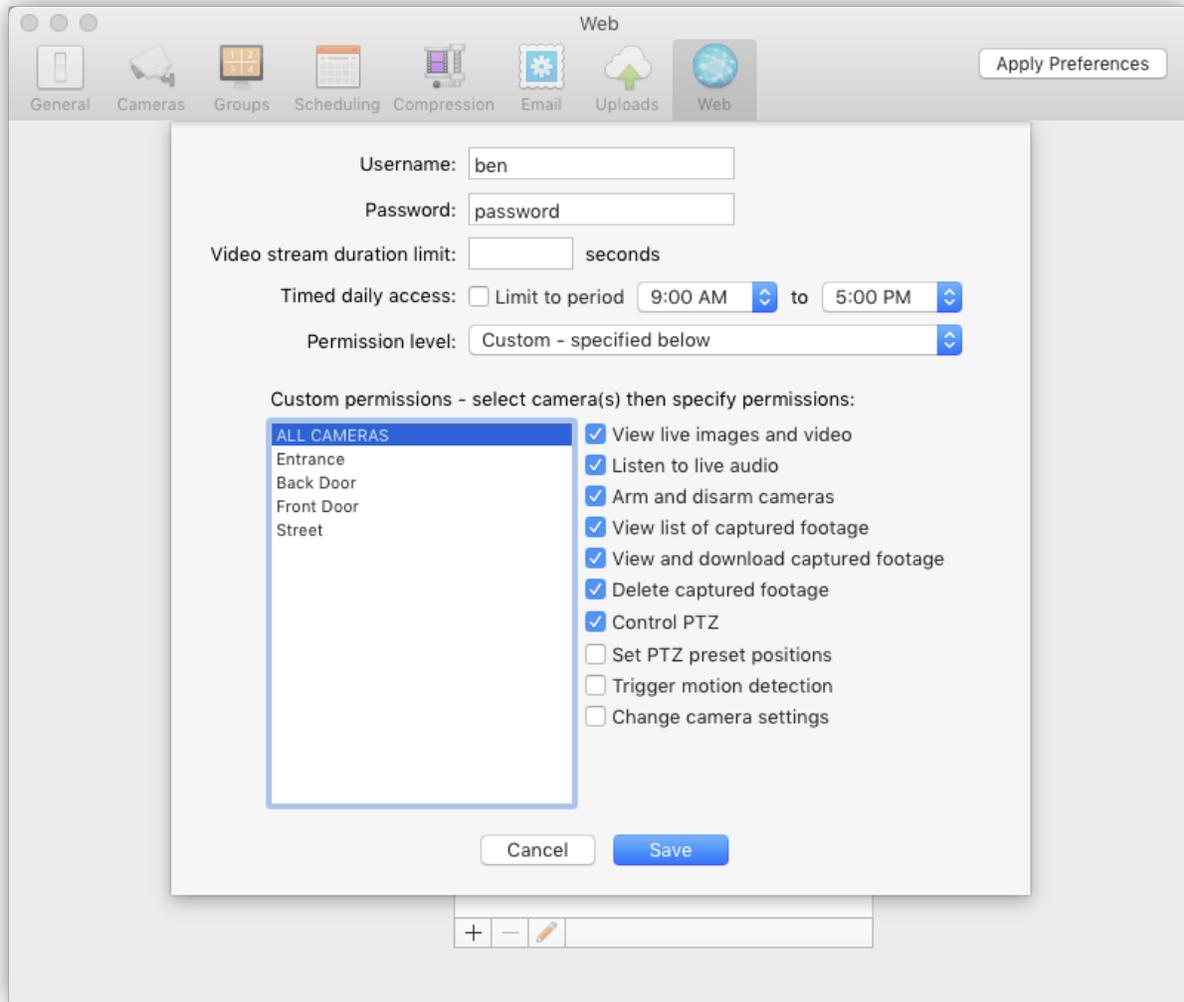
Por lo tanto, es posible que deba deshabilitar el firewall si desea utilizar Bonjour para conectarse a los servidores SecuritySpy. Se puede acceder a la configuración del firewall en las Preferencias del sistema de seguridad y privacidad.

### **Cuentas / Accounts**

Para habilitar la protección con contraseña para restringir el acceso a su servidor SecuritySpy, debe agregar al menos una cuenta de servidor web; si no agrega ninguna cuenta, no habrá protección por contraseña. Si se podrá acceder a su servidor SecuritySpy desde Internet, le recomendamos encarecidamente que habilite la protección con contraseña.

## Preferencias – Web – Cuenta / Preferences – Web – Account

Este panel le permite especificar la configuración de una cuenta de servidor web:



### Username / Password

Ingrese el nombre de usuario y la contraseña necesarios para iniciar sesión con esta cuenta. El nombre de usuario no distingue entre mayúsculas y minúsculas, pero la contraseña sí; ambos pueden tener hasta 31 caracteres.

### Límite de duración de la transmisión de video / Video stream duration limit

Especifique una cantidad de segundos después de los cuales cortar cualquier transmisión de video en vivo que se esté viendo a través de esta cuenta.

## **Acceso diario programado / Timed daily access**

Esta configuración le permite restringir el acceso al servidor web a través de esta cuenta a ciertas horas del día.

## **Nivel de permiso / Permission level**

Hay algunos niveles de permisos preestablecidos y uno completamente personalizable, como se indica a continuación: Ver: el usuario puede ver videos en vivo desde cualquier cámara. Ver, descargar: el usuario puede ver videos en vivo y descargar imágenes capturadas previamente para cualquier cámara. Ver, descargar, controlar PTZ: el usuario puede ver video en vivo, descargar metraje capturado previamente y controlar Pan / Tilt / Zoom para cualquier cámara.

Administrador: el usuario tiene acceso completo a todas las funciones del servidor web. Personalizado: en esta configuración, puede especificar a qué funciones tiene acceso el usuario. Seleccione las cámaras para las que desea permitir determinadas acciones y configure los permisos en consecuencia.

Seleccione la opción Todas las cámaras para configurar los permisos que se aplicarán a todas las cámaras; esto hace que sea fácil otorgar a un usuario en particular un cierto nivel de acceso para todas las cámaras, al mismo tiempo que puede aplicar permisos adicionales para cámaras individuales.

## **Acceso a SecuritySpy desde Internet / Accessing SecuritySpy from the Internet**

La configuración del acceso a su sistema desde Internet requiere la configuración de su enrutador. Para obtener instrucciones, consulte la sección Supervisión remota del Manual de instalación de SecuritySpy.

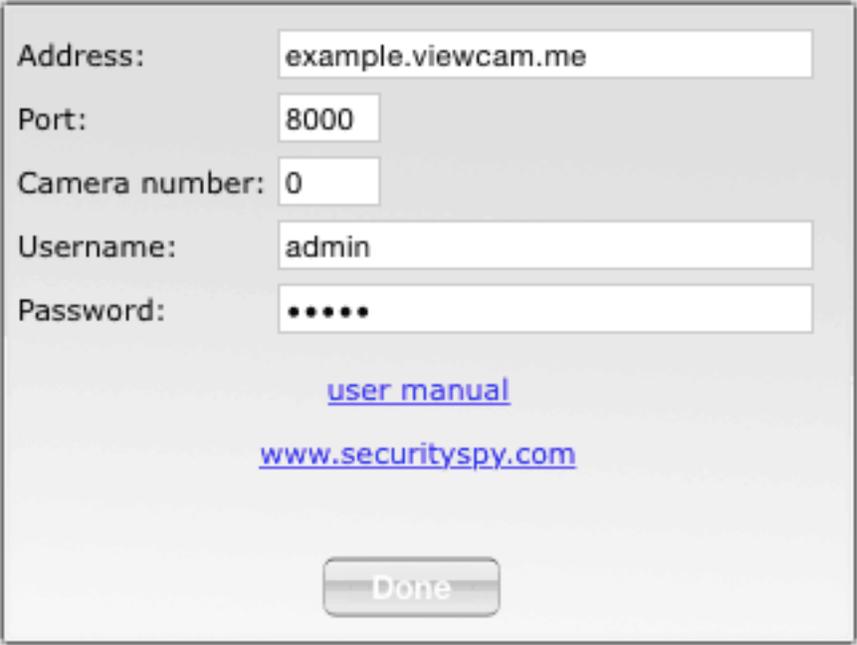
## **Widget del panel / Dashboard Widget**

SecuritySpy viene con su propio widget Dashboard para una fácil visualización remota de transmisiones de video desde su servidor SecuritySpy a través de una red local o Internet.

Haga clic aquí para descargar el widget SecuritySpy; se instalará automáticamente en su carpeta de widgets y estará disponible de inmediato en Dashboard.

La primera vez que cargue el widget, deberá especificar algunas configuraciones para que sepa dónde está el servidor web SecuritySpy. Para abrir la ventana de configuración, haga clic en el botón de información (el símbolo i en la esquina inferior derecha del widget).

La configuración se ve así:



The image shows a configuration window for SecuritySpy. It contains the following fields and options:

- Address:** example.viewcam.me
- Port:** 8000
- Camera number:** 0
- Username:** admin
- Password:** masked with five dots

Below the fields, there are two blue underlined links:

- [user manual](#)
- [www.securityspy.com](http://www.securityspy.com)

At the bottom center, there is a button labeled "Done".

El widget tiene la siguiente configuración: Dirección: la dirección IP o el nombre de host del servidor SecuritySpy. Si desea conectarse mediante HTTPS seguro, anteponga la dirección con el especificador de protocolo "https://"; de lo contrario, el widget se establecerá de forma predeterminada en HTTP estándar.

Puerto: este es el puerto de red utilizado para conectarse a SecuritySpy. Los puertos predeterminados de SecuritySpy son 8000 y 8001 para HTTP y HTTPS respectivamente. Número de cámara: puede obtenerlo a través de la ventana Información de la cámara en SecuritySpy. Nombre de usuario / contraseña: ingrese el nombre de usuario y la contraseña de la cuenta del servidor web SecuritySpy que tiene permiso para acceder al video en vivo de la cámara en cuestión.

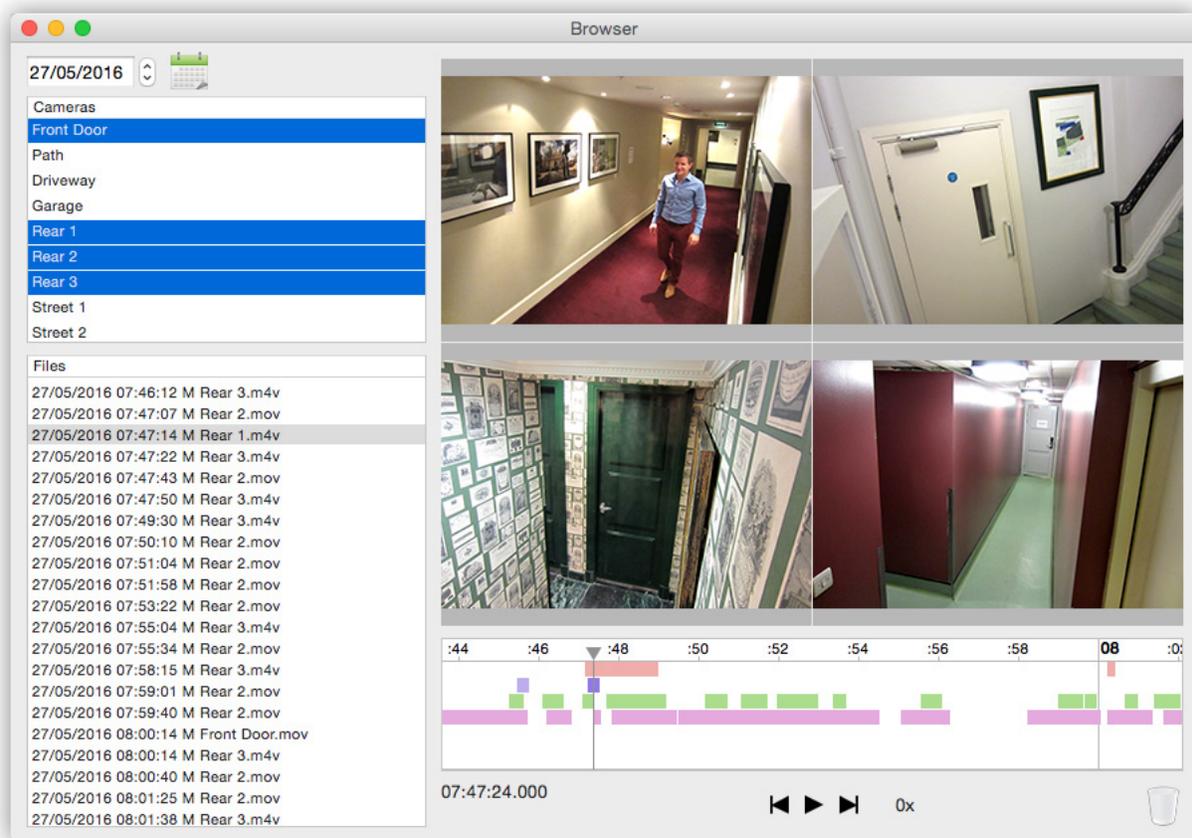
Sí, en lugar de la imagen, aparece un icono de signo de interrogación, significa que el widget no pudo obtener la imagen. Verifique la dirección, el número de la cámara, el nombre de usuario y la contraseña para asegurarse de que sean correctos.

Puede crear varias instancias del widget para ver varias cámaras diferentes al mismo tiempo, y el widget se puede utilizar sin restricciones en tantas computadoras como desee.

Este widget también se puede utilizar en computadoras con Windows y Linux con el software Kludget Engine.

## Navegador / Browser

La función del navegador de SecuritySpy le permite ver y administrar el metraje capturado. Elija Navegador en el menú Ventana para abrir el Navegador:



Seleccione una o más cámaras y especifique una fecha, y el navegador mostrará todos los archivos que coincidan con estos criterios. Los principales componentes del navegador son:

## **Control de fecha / Date control**

Para la fecha que especifique, el navegador muestra todas las imágenes capturadas durante ese día. Haga clic en el ícono de calendario para obtener un calendario gráfico emergente, lo que facilita la elección de la fecha deseada.

## **Lista de cámaras / Camera list**

Esta lista muestra todas las cámaras activas en SecuritySpy. Seleccione hasta seis cámaras para ver imágenes de todas ellas, sincronizadas juntas. Para seleccionar varias cámaras, presione Mayús y haga clic o comando y haga clic en las entradas de la lista.

## **Lista de archivos / File list**

Esta lista muestra todos los archivos que han sido capturados por todas las cámaras seleccionadas en el día especificado. Haga clic en cualquier archivo de esta lista para saltar al inicio de ese archivo en la línea de tiempo, o haga doble clic en un archivo para comenzar a reproducirlo inmediatamente.

Mantenga presionada la tecla alt (opción) en el teclado al seleccionar un archivo de captura de movimiento, y la línea de tiempo saltará al primer movimiento real en el archivo, en lugar de al principio. Esto es útil cuando se usa la función de captura previa de SecuritySpy para comenzar a grabar algunos segundos antes del disparo por movimiento.

## **Cronología / Timeline**

La línea de tiempo muestra una representación gráfica de los períodos de tiempo durante el día que han capturado imágenes de video para cada cámara seleccionada. Haga clic en cualquier parte de la línea de tiempo para cambiar la hora actual del cursor, y haga clic y arrastre hacia la izquierda y hacia la derecha para desplazarse hacia atrás y hacia adelante a través de las imágenes de video.

Mantenga presionada la tecla Mayús en el teclado mientras arrastra el cursor de la línea de tiempo para seleccionar un período de tiempo, que luego puede exportar. Todos los archivos capturados desde el último escaneo se agregarán en rojo, lo que indica que aún no se han puesto en cola para mostrarse en el área de películas. Para reproducir estos archivos, use la opción Volver a explorar en el menú del navegador (ver más abajo) para agregarlos a la visualización de la película. Los archivos de la papelera se muestran en gris, pero aún se podrán reproducir hasta que la vacíes.

## Área de películas / Movie area

Esta es el área que realmente muestra el metraje capturado. Si ha seleccionado varias cámaras, se mostrarán en una cuadrícula, en la disposición más óptima para el tamaño de la ventana del navegador y la resolución de cada cámara seleccionada.

## Menú del navegador / Browser Menu

El menú del navegador en la barra de menú contiene las siguientes opciones:

Export File	
Export Selection	
Export Current Frame	
Rescan	⇧ ⌘ R
Reveal in Finder	⇧ ⌘ F
Move to Trash	⌘ ⌫
Empty Trash	⇧ ⌘ ⌫
Zoom In Timeline	⌘ +
Zoom Out Timeline	⌘ -
Clear Selection	⇧ ⌘ D
Increase Speed Backwards	J
Stop	K
Increase Speed Forwards	L

## Menú del navegador – Exportar archivo / Browser Menu – Export File

Esta opción le permite exportar cualquier archivo que esté seleccionado actualmente en la lista de archivos. Los datos de video y audio se copian directamente en el archivo exportado, por lo que no hay pérdida de calidad.

Al exportar un archivo, tiene la opción de establecer la velocidad de fotogramas de reproducción. De esta manera, puede crear películas a intervalos que se reproducen a velocidades mucho más rápidas que en tiempo real. Tenga en cuenta que al hacerlo, se eliminarán las pistas de audio de la película.

### **Menú del navegador: Exportar selección / Browser Menu – Export Selection**

Haga una selección en la línea de tiempo arrastrando el cursor mientras mantiene presionada la tecla Mayús. Luego, para cualquier cámara que esté seleccionada actualmente en la lista de cámaras, esta opción le permite exportar el metraje de video contenido dentro del período de tiempo seleccionado. Los datos de video y audio se copian directamente en el archivo exportado, por lo que no hay pérdida de calidad.

### **Menú del navegador – Exportar fotograma actual / Browser Menu – Export Current Frame**

Para cualquier cámara que haya seleccionado en la lista de cámaras, esta opción le permite exportar una imagen fija de la hora actual como un archivo JPEG. Esta opción está disponible solo si hay algún metraje válido para la cámara especificada en el momento actual.

### **Menú del navegador – Volver a explorar / Browser Menu – Rescan**

Esto vuelve a escanear archivos para la (s) cámara (s) actualmente seleccionada (s) y la fecha. Esto es útil para agregar a la visualización de la película cualquier archivo que haya sido capturado desde el último escaneo, con el fin de reproducirlos.

### **Menú del navegador: mostrar en el Finder / Browser Menu – Reveal in Finder**

Esta opción le dice al Finder que muestre todos los archivos que están seleccionados actualmente.

### **Menú del navegador: mover a la papelera / Browser Menu – Move to Trash**

Esto mueve todos los archivos seleccionados a la papelera del navegador. El navegador guarda su propia papelera, separada de la papelera del Finder.

### **Menú del navegador: Vaciar papelera / Browser Menu – Empty Trash**

Utilice esta opción para eliminar permanentemente todos los archivos de la papelera del navegador.

## **Menú del navegador – Línea de tiempo para acercar / alejar / Browser Menu – Zoom In/Out Timeline**

Utilice estas opciones para acercar o alejar la vista de la línea de tiempo. Amplíe para ver la posición de los objetos de tiempo en detalle, o reduzca el zoom para obtener una imagen más general de las imágenes capturadas a lo largo del día.

### **JKL control**

El navegador también es compatible con los controles de lanzadera del teclado JKL: presionar L hace que la reproducción se acelere en la dirección de avance en un factor de 2, J hace que la reproducción se acelere en la dirección de retroceso en un factor de 2 y K pausa la reproducción.

### **Reproducción de video para acercar / alejar / Zoom In/Out Video Playback**

Para acercar o alejar el metraje capturado durante la reproducción, mantenga presionada la tecla Comando (⌘) y desplácese hacia arriba o hacia abajo en su mouse o trackpad (en un trackpad, use el gesto de dos dedos para desplazarse). Una vez ampliada, suelte la tecla Comando y desplácese en cualquier dirección para desplazarse por la imagen.

### **Dispositivos de red / Network Devices**

Los dispositivos de red se conectan a la computadora a través de una red Ethernet cableada o inalámbrica. Hay dos tipos de dispositivos de red: cámaras de red y servidores de video en red (a veces denominados cámaras IP y servidores de video IP). Son similares en la forma en que envían video a través de la red, pero mientras que una cámara de red es una unidad autónoma totalmente digital, un servidor de video en red tiene una o más entradas analógicas para conectar cámaras analógicas. Debido a las importantes limitaciones del video analógico, toda nueva instalación debe utilizar exclusivamente cámaras IP.

Para encontrar una cámara adecuada para su sistema, consulte nuestra lista completa de búsqueda de cámaras de red compatibles. Incluso si una cámara en particular no está en esta lista, es muy probable que funcione con SecuritySpy usando el protocolo ONVIF, o con la cadena de solicitud HTTP o RTSP correcta (esto generalmente se puede obtener de la documentación de la cámara o solicitando esta información directamente del fabricante).

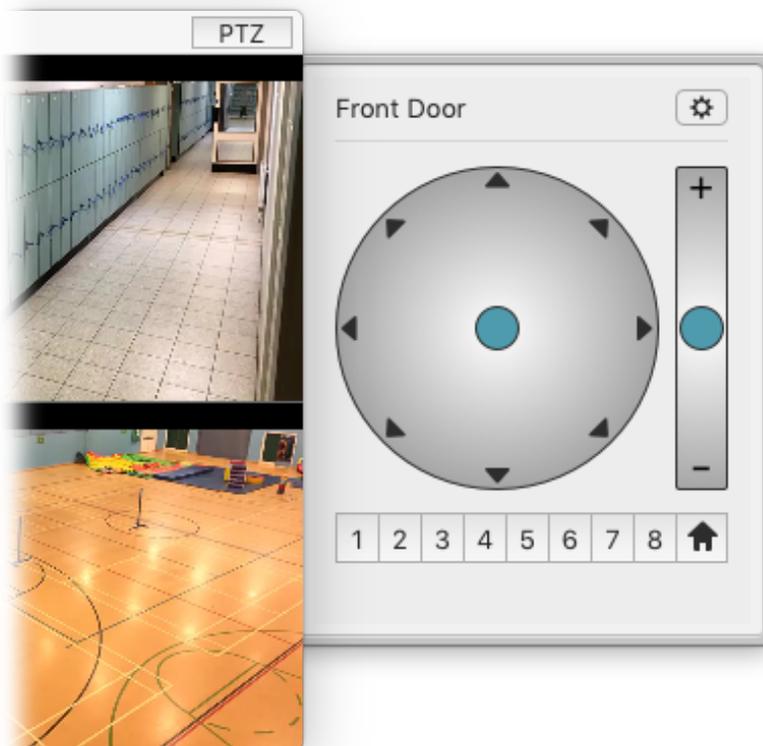
SecuritySpy admite todos los principales formatos de transmisión de video producidos por cámaras de red (protocolos HTTP y RTSP; formatos de video JPEG, MPEG-4 y H.264; formatos de audio AAC, G.711, G.726, PCM y AMR). Mientras SecuritySpy intenta conectarse a un dispositivo de red, muestra un icono de conexión parpadeante.

Si, por cualquier motivo, falla la conexión, verá un icono de una cámara con una cruz que lo atraviesa y un mensaje para informarle del problema. Las conexiones pueden fallar por varias razones, como un nombre de usuario / contraseña incorrectos, una dirección IP incorrecta o un problema de red.

Si falla una conexión, verifique el registro (seleccione Abrir registro en el menú Archivo), ya que le dará más información sobre cuál es el problema. SecuritySpy intentará repetidamente conectarse a dispositivos de red para garantizar la confiabilidad en caso de un problema temporal con la red o el dispositivo.

### Pan/Tilt/Zoom (PTZ)

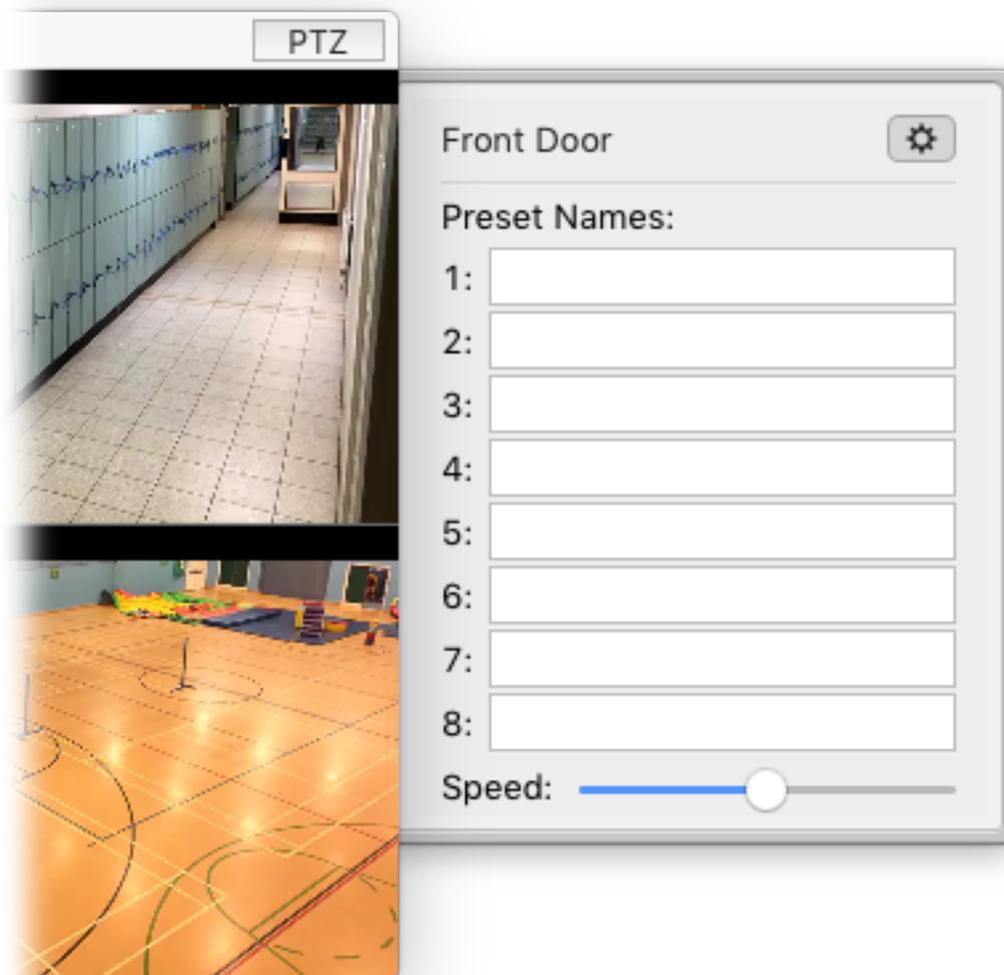
Cada ventana de video que contenga una cámara que admita PTZ tendrá un botón PTZ en el lado derecho de la barra de título de la ventana: haga clic en este botón y un cajón PTZ se deslizará hacia afuera, permitiéndole controlar las cámaras en la ventana:



Los controles PTZ actúan como un "joystick virtual", lo que le permite controlar la dirección, así como la velocidad de movimiento, para las cámaras que admiten movimiento de velocidad variable (cuanto más se mueven los indicadores azules desde el centro de sus respectivas áreas de control, el más rápido el movimiento).

Si su cámara admite posiciones preestablecidas, los ocho botones preestablecidos estarán disponibles. Para guardar la posición actual de la cámara como uno de los ajustes preestablecidos, mantenga presionada la tecla alt (opción) en el teclado y haga clic en un botón preestablecido (la posición de inicio, si está disponible, suele estar preestablecida por el fabricante y no se puede cambiar) .

Haga clic en el botón de engranaje en la parte superior derecha del cajón PTZ para revelar estas configuraciones:



Aquí puede nombrar cada posición preestablecida, así como especificar la velocidad máxima a la que se moverá su cámara (si su cámara admite movimiento de velocidad variable).

### **Atajos de teclado PTZ / PTZ Keyboard Shortcuts**

También puede controlar PTZ desde el teclado, utilizando las teclas de flecha o el teclado numérico a la derecha de los teclados estándar (1 en el teclado corresponde a abajo a la izquierda y así sucesivamente). Para las cámaras que admiten movimiento de velocidad variable, mantener presionada la tecla Mayús mientras usa estos atajos de teclado mueve la cámara un 50% más rápido que la velocidad estándar.

Puede recuperar preselecciones presionando una tecla numérica en la parte superior del teclado; mantenga presionada la tecla alt (opción) con una tecla numérica para guardar un ajuste preestablecido. Incluso si no tiene el cajón PTZ abierto, simplemente haga clic una vez en la imagen de video de la cámara que desea controlar, y luego podrá usar estos atajos de teclado.

### **Accesos directos del mouse PTZ / PTZ Mouse Shortcuts**

Mantenga presionada la tecla Mayús (o habilite el bloqueo de mayúsculas) y haga clic directamente en la imagen de una cámara en cualquier ventana de video para controlar su giro e inclinación: un clic en el lado derecho de la imagen de video moverá la cámara hacia la derecha y así sucesivamente. Si su cámara admite movimiento de velocidad variable, la distancia de su clic desde el centro de la imagen define la velocidad del movimiento.

### **Permisos de control PTZ / PTZ Control Permissions**

Tenga en cuenta que los dispositivos generalmente requieren detalles de nombre de usuario / contraseña de administrador para controlar PTZ, así que asegúrese de que se hayan ingresado correctamente en la ventana Preferencias -> Cámaras -> Dispositivo. Es posible que los detalles de autenticación que no sean de administrador necesarios para simplemente ver videos no sean suficientes para controlar PTZ.

## SecuritySpy como software de visualización remota / SecuritySpy as remote viewing software

Puede usar una instancia de SecuritySpy ejecutándose en una Mac para ver las cámaras conectadas a otra instancia de SecuritySpy ejecutándose en una Mac diferente. De esta manera, puede utilizar SecuritySpy como software de visualización de clientes, proporcionando una mejor experiencia de usuario que la visualización a través del navegador web.

A efectos de solo visualización, SecuritySpy se puede utilizar de forma gratuita en su estado sin licencia. Para configurar una Mac (el servidor) para transmitir video a otra Mac (el cliente): En el servidor Mac Habilite la función del servidor web de SecuritySpy en Preferencias -> Ventana web.

Para conexiones a través de una red local, asegúrese de que la opción Anunciar este servidor web a través de Bonjour esté habilitada, para que la computadora cliente pueda encontrar el servidor automáticamente. Para conexiones a través de Internet, configure el acceso al servidor a través de Internet según la sección de Monitoreo Remoto del Manual de Instalación de SecuritySpy.

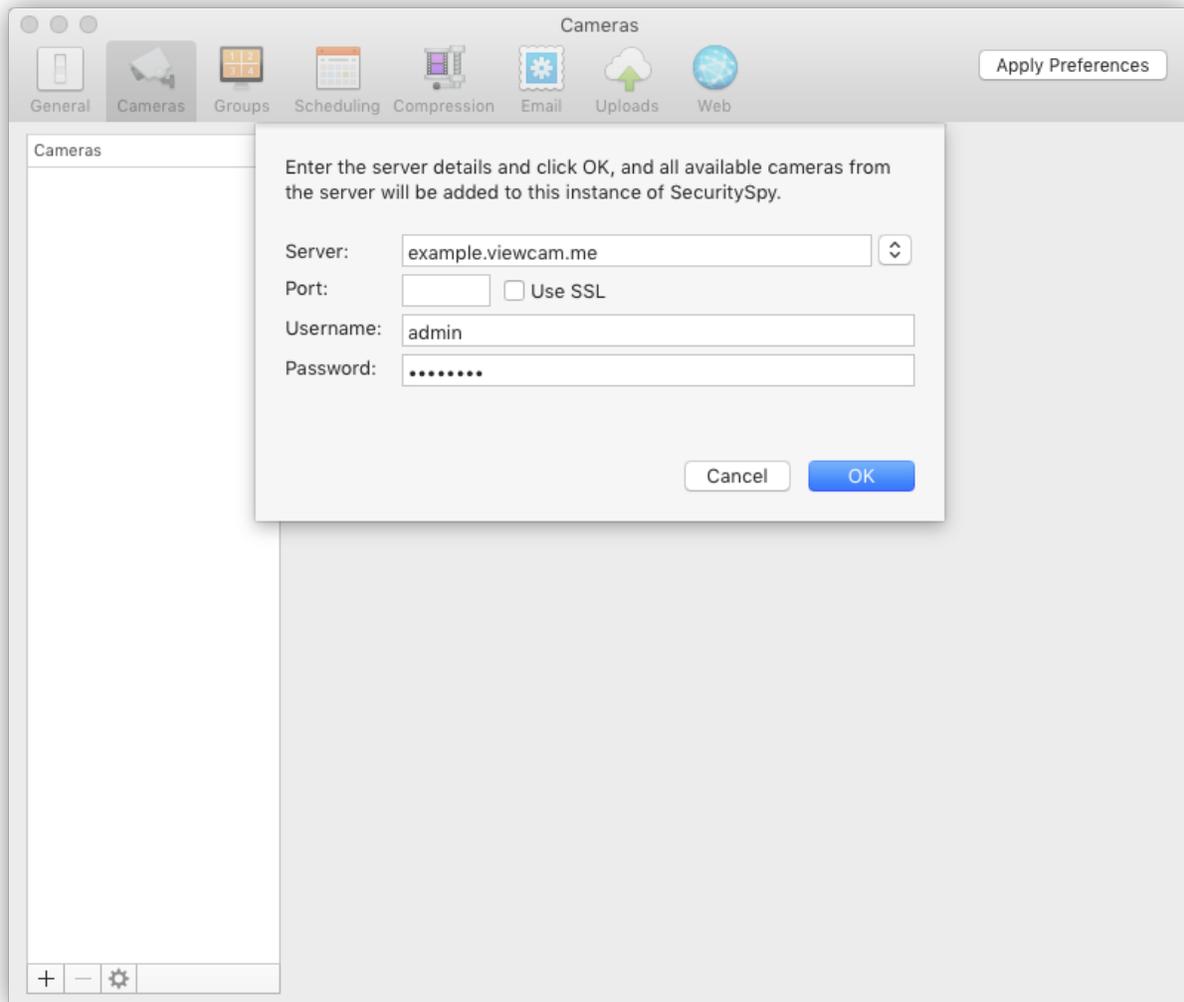
Esto le proporcionará su propio nombre de dominio DDNS (por ejemplo, [example.viewcam.me](http://example.viewcam.me)) con el que acceder al servidor a través de Internet.

Hay dos formas de agregar cámaras a la instancia del cliente SecuritySpy: En el cliente Mac: agregar todas las cámaras de una vez

Vaya a Preferencias -> Cámaras, haga clic en el botón más (+) en la parte inferior izquierda y seleccione Agregar todas las cámaras desde SecuritySpy Server.

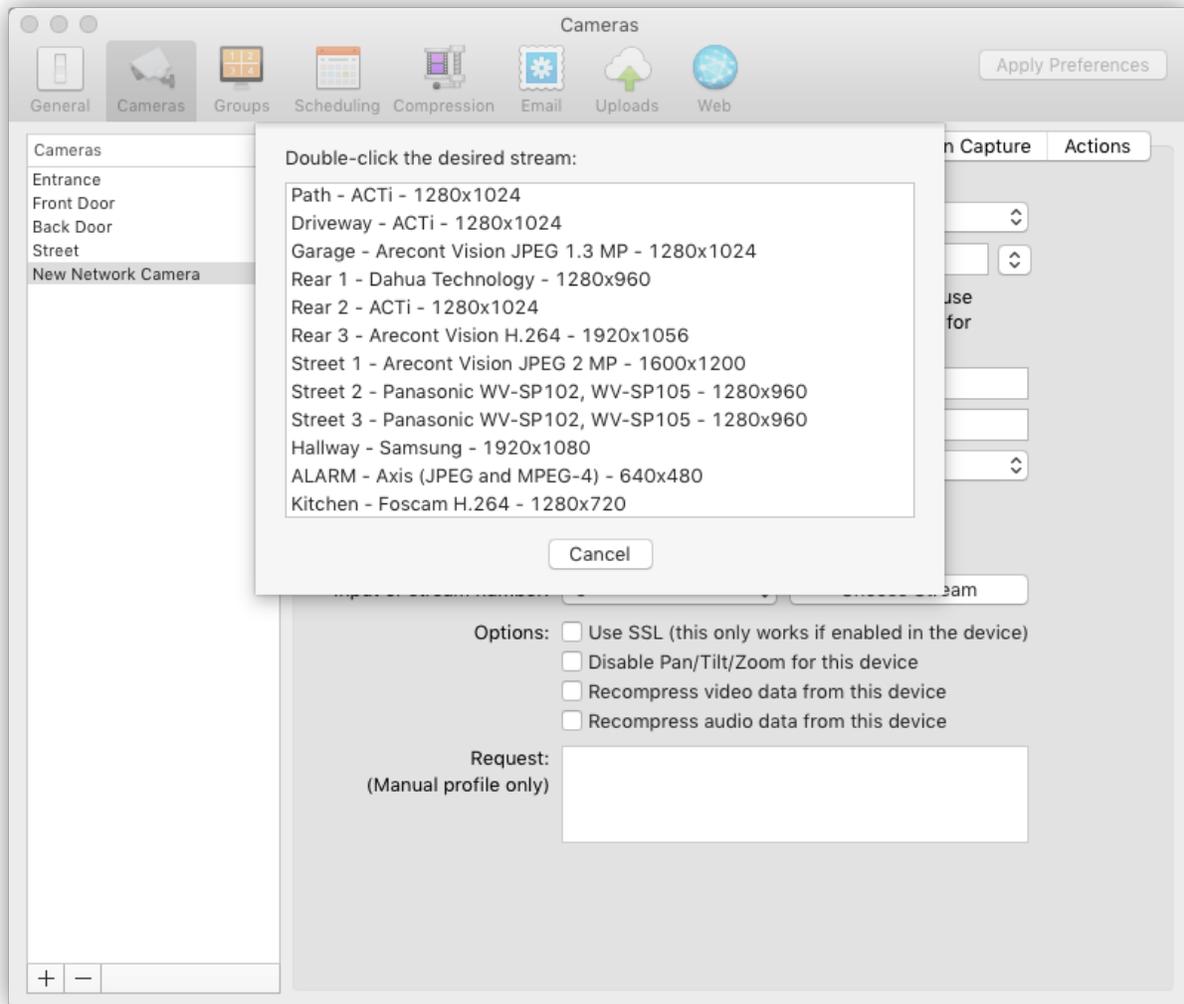
Si se está conectando a través de una red local, haga clic en el menú Bonjour a la derecha del campo Dirección y seleccione la computadora del servidor; Si se conecta a través de Internet, ingrese la dirección DDNS que creó anteriormente (por ejemplo, [example.viewcam.me](http://example.viewcam.me)).

Sí ha habilitado la protección por contraseña en el servidor, ingrese el nombre de usuario y la contraseña. Si utiliza puertos estándar (8000 y 8001), no es necesario que ingrese un número de puerto. Haga clic en Aceptar y se agregarán todas las cámaras:



En el cliente Mac: agregar cámaras individualmente Vaya a Preferencias -> Cámaras, haga clic en el botón más (+) en la parte inferior izquierda y seleccione Agregar dispositivo de red. Si se está conectando a través de una red local, haga clic en el menú Bonjour a la derecha del campo Dirección y seleccione la computadora del servidor; Si se conecta a través de Internet, ingrese la dirección DDNS que creó anteriormente (por ejemplo, example.viewcam.me). Seleccione SecuritySpy como perfil del dispositivo y, si ha habilitado la protección con contraseña en el servidor, ingrese el nombre de usuario y la contraseña.

Para la configuración de Formato, elija entre JPEG HTTP o H.264 RTSP. JPEG es adecuado para la transmisión a través de una red local, mientras que H.264 es más adecuado para la transmisión a través de Internet debido a su menor velocidad de datos. Haga clic en Elegir transmisión y aparecerá una ventana que presenta todas las cámaras disponibles en la computadora servidor; haga doble clic para seleccionar uno:



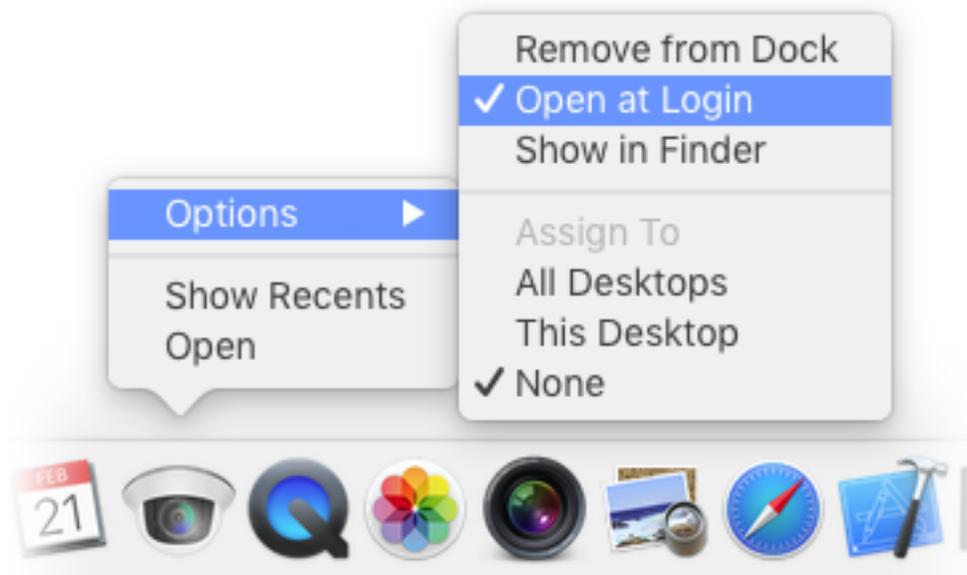
Tenga en cuenta que cada instancia de visualización coloca una carga de procesamiento adicional en el servidor.

Puede reducir esta carga especificando una velocidad de fotogramas baja en la ventana anterior y / o utilizando la compresión JPEG en lugar de la compresión H.264 (pero tenga en cuenta que la compresión JPEG utiliza más ancho de banda).

## Configuración de SecuritySpy para funcionamiento autónomo / Setting up SecuritySpy for autonomous operation

Estos son los pasos que recomendamos para configurar su sistema SecuritySpy para que funcione de forma autónoma:

Configure SecuritySpy para que se abra cada vez que se inicie la computadora. Abra SecuritySpy y haga clic y mantenga presionado el botón del mouse en el ícono de SecuritySpy en el Dock. En el menú que aparece, seleccione Opciones -> Abrir al iniciar sesión:



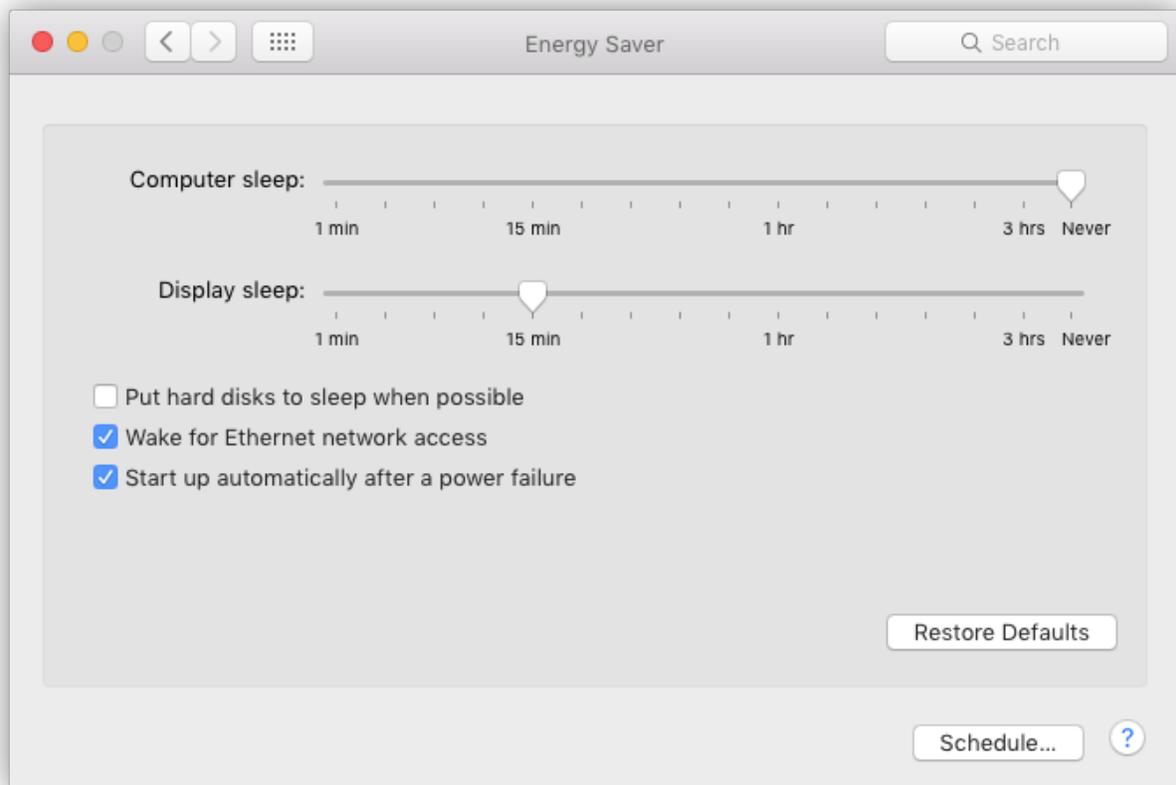
### Set the computer to never sleep

Abra Preferencias del sistema y haga clic en el elemento Ahorro de energía. Arrastre el control deslizante de suspensión de la computadora completamente hacia la derecha, donde dice Nunca.

También se recomienda para un mejor rendimiento deshabilitar la configuración Poner los discos duros en reposo cuando sea posible. La suspensión de la pantalla debe estar habilitada para ahorrar energía y evitar daños en el monitor.

## Configurar la computadora para que se reinicie después de un corte de energía / Set the computer to restart after a power failure

Abra Preferencias del sistema y haga clic en el elemento Ahorro de energía. Active la opción Iniciar automáticamente después de un corte de energía. Para mayor protección, haga clic en el botón Programar ... y configure la Mac para que se inicie automáticamente todos los días.



Habilite la supervisión y la administración remotas Consulte la sección Preferencias -> Web de este manual para obtener más detalles.

## Cerrar todas las ventanas de video / Close all video windows

Las ventanas de video no son necesarias si no hay nadie operando la computadora, y usarán el tiempo de la CPU, lo que reducirá el rendimiento.

## Optimización del rendimiento / Optimising Performance

El uso de varias cámaras simultáneamente implica mover, calcular y almacenar grandes cantidades de datos. Para aprovechar al máximo su computadora, debe: Cuando utilice dispositivos de red, no habilite las opciones de Recomprimir en Preferencias -> Cámaras -> Ventana Dispositivo, a menos que tenga una buena razón para hacerlo. Dejar desactivada la opción Recompress video data significa que no podrá usar las funciones de superposición y transformación de texto de SecuritySpy, pero afortunadamente la mayoría de las cámaras admiten estas funciones, por lo que si las necesita, puede activarlas directamente en la configuración de la cámara. . En la preferencia del sistema Energy Saver, si la configuración de Rendimiento del procesador está disponible, establézcala en la configuración más alta. Desactive el modo de suspensión en la preferencia del sistema Energy Saver. SecuritySpy no puede funcionar cuando la computadora está en modo de suspensión. Desactive la suspensión del disco duro en la preferencia del sistema Ahorro de energía si obtiene archivos de película con una pausa larga al principio. Si el disco duro está inactivo, los fotogramas se perderán al comienzo de la siguiente captura debido al tiempo necesario para hacer girar el disco (esto solo se aplica a los discos duros mecánicos, no a los de estado sólido o híbridos). Habilite la opción Mostrar cámaras a la mitad de la velocidad de fotogramas en las ventanas de video en las Preferencias y cierre todas las ventanas de video cuando no las esté usando. La visualización de video en la pantalla puede consumir un tiempo de CPU significativo y, por lo tanto, puede resultar en un rendimiento más bajo en general.

Habilite la opción Realizar detección de movimiento solo cuando sea necesario en las Preferencias.

Habilite la opción Descomprimir fotogramas de video entrantes solo cuando sea necesario en las Preferencias, sin embargo, tenga en cuenta que esto puede resultar en un retraso de unos segundos cuando se requiere video, después de un período en el que no se requiere (por ejemplo, al abrir una ventana de video).

En la ventana Preferencias -> Cámaras -> Dispositivo, configure la velocidad de fotogramas de cada dispositivo a la velocidad más baja que necesite. Si esta opción no está disponible aquí, configúrela directamente en las cámaras. Si una cámara envía fotogramas más rápido de lo necesario, se pierde tiempo de CPU procesando estos fotogramas adicionales.

Es probable que un disco duro rápido mejore el rendimiento, según la cantidad de cámaras que capturen simultáneamente y la compresión de video utilizada. Si se utiliza una unidad externa, Thunderbolt es la mejor interfaz, aunque USB 3.0 también ofrece mucha velocidad. Aunque significativamente más lento, USB 2.0 funcionará bien para sistemas pequeños a medianos, especialmente cuando se graba en formato H.264, que tiene una velocidad de datos baja.

Cierre todas las aplicaciones que no sean SecuritySpy.

### **Soporte / Ayuda / Support / Help**

Para obtener información sobre cómo elegir, instalar y configurar el hardware de su sistema de videovigilancia, consulte el Manual de instalación de SecuritySpy. Para obtener ayuda y solución de problemas actualizada, consulte las páginas de ayuda en línea de SecuritySpy.

Para averiguar qué especificación de computadora se requiere para una configuración de cámara en particular, consulte la Calculadora de requisitos del sistema de SecuritySpy