

Guía del usuario de la interfaz web de la cámara IP

Modelos de cámara IP H6, H5 y H4 de alta definición Avigilon:

H6SL-xx	H6M-Dx-IR	H5EX-xx-BO1	H4A-ETD-KIT
H5A-xx	H6M-Dx	H5EX-xx-CO1	H4A-THC-BO
H5A-xx-IR	H5A-CR1-IR-xx	H4A-xx(-B)	H4A-G-B(-B)
H5SL-xx	H5A-CR2-IR-xx	H4M-D	H3A-xx
H5SL-xx-IR	H4A-G-xx-IR(-B)	H4F-DO	H3A-BO-IR
H5M-DO	H4A-xx-IR(-B)	H4SL-xx(-IR)	

Copyright

© 2016 - 2024, Avigilon Corporation. Todos los derechos reservados. AVIGILON, el logotipo de AVIGILON, HDSM SmartCodec, AVIGILON CONTROL CENTER, ACC, ACCESS CONTROL MANAGER y ACM son marcas comerciales de Avigilon Corporation. Android es una marca registrada de Google LLC. Apple, Safari y Mac son marcas comerciales de Apple Inc, registradas en los Estados Unidos y otros países. Firefox es una marca registrada de Mozilla Foundation en los Estados Unidos y otros países. Otros nombres o logotipos mencionados en este documento pueden ser marcas comerciales de sus respectivos propietarios. La ausencia de los símbolos ™ y ® junto a cada marca registrada mencionada en este documento o en todas no representa una renuncia a la propiedad de la marca comercial correspondiente. Cubierto por una o más reclamaciones de las patentes enumeradas en patentlist.hevcadvance.com.

Este documento se ha compilado y publicado mediante especificaciones disponibles y las descripciones del producto en el momento de la publicación. El contenido de este documento y las especificaciones de los productos en él tratados están sujetos a cambios sin previo aviso. Avigilon Corporation reserva el derecho de efectuar cambios mencionados sin previo aviso. Ni Avigilon Corporation ni ninguna de sus compañías afiliadas: (1) garantizan la exhaustividad o la precisión de la información contenida en este documento; o (2) es responsable del uso de, o la confianza en la información. Avigilon Corporation no será responsable de las pérdidas o daños (incluidos los daños indirectos) causados por su confianza en la información contenida en este documento.

Avigilon Corporation
avigilon.com

PDF-H4WebUI-G

Revisión: 3 - ES

20240221

Tabla de contenido

Introducción	1
Requisitos del sistema	1
Otras guías de la interfaz web	1
Acceso a la interfaz web de la cámara	2
Crear el usuario inicial e iniciar sesión	2
Iniciar sesión	3
Live View (Imagen en vivo)	4
Guardar una imagen fija	4
Setup (Configuración)	5
General	6
Red	7
Configurar la autenticación basada en puertos 802.1X	11
Conmutación de perfiles de autenticación 802.1X	11
Eliminación de un perfil de autenticación 802.1X	12
Configurar SNMP	12
Configuración de DSCP	13
IP Filter (Filtro de IP)	14
Configuración de seguridad	16
Activación de la transmisión SRTP	17
Requisitos	17
Administrar certificados	18
Descarga de certificados	18
Eliminación de certificados	18
Descarga de solicitudes de firma de certificados	18
Cargando certificados	18
Carga de certificados CA	19
Imagen y Visualización	19
Adjustments (Ajustes)	25
Compresión y velocidad de imagen	26
Activación de los ajustes de tecnología de HDSM SmartCodec™	28
Visualización de la URI de transmisión RTSP	28
Acceso a la URI de imagen fija	29
Ajustes avanzados de tecnología HDSM SmartCodec	29
Motion Detection (Detección de movimiento)	30

Tamper Detection(Detección de manipulación)	31
Configuración de análisis	32
Configuración ampliada	33
Zonas de privacidad	33
Ajuste de una zona de privacidad	34
Eliminación de una zona de privacidad	34
Configurar una zona de privacidad extraíble para usuarios específicos	34
Almacenamiento	35
Habilitar el almacenamiento interno	36
ONVIF Profile G	37
Descarga de vídeo grabado de la interfaz web	37
Descarga de vídeo grabado desde la tarjeta SD	38
Eliminación del vídeo grabado	38
Errores de la tarjeta SD	39
Entradas y salidas digitales	39
Arandela	41
Audio	41
Usuarios	42
Añadir a un usuario	42
Edición de usuarios y contraseñas	43
Eliminar un usuario	43
Cómo conservar nombres de usuario y contraseñas después de revertir el firmware	43
Sistema	44
Actualización del firmware de la cámara	45
Registro de dispositivos	45
Deshabilitar WebUI	46
About (Sobre)	47
Comprobación de la fuente de alimentación de una cámara	47
Cámara ACC™ ES	48
Comprobación del estado de la cámara ACC ES(ACC ES)	48
Configuración de los ajustes de administración de la cámara ACC ES	48
Reinicio del software ACC	48
Formateo de la unidad de vídeo grabado	48
Cambiar los puertos de comunicación	49
Anulación del límite de inicio de sesión	49
Habilitar Storage Management (Gestión de almacenamiento)	50

Revisión de registros del software ACC 50

Introducción

Todas las cámaras IP Avigilon de alta definición incluyen una interfaz web que le permite ver vídeo en directo y configurar la cámara a través de un navegador web.

Antes de acceder a la interfaz web, asegúrese de haber completado todos los procedimientos descritos en la Guía de instalación de la cámara.

Sugerencia: Las funciones y opciones no compatibles con la cámara están deshabilitadas.

Requisitos del sistema

Se recomiendan los siguientes navegadores para acceder a la interfaz web desde cualquier dispositivo Windows, Mac o móvil:

- Mozilla Firefox versión 96.0.2 (64 bit) o posterior
- Google Chrome™ versión 97.0.4692.71 (64 bits, versión oficial) o posterior
- Microsoft Edge versión 97.0.1072.76 (64 bits, versión oficial) o posterior

Nota: La interfaz web puede funcionar con navegadores más antiguos o no compatibles, pero esto no se ha probado.

Otras guías de la interfaz web

Consulte estas otras guías de la interfaz web para otros tipos de cámaras de Avigilon:

- [Guía del usuario de la interfaz web de la cámara H6](#): para cámaras H6A y cámaras H6X.
- [Guía de la interfaz web de la cámara PTZ](#): para cámaras con desplazamiento, inclinación y zoom.
- [Guía de la interfaz web de la cámara multicabezal](#): para cámaras de doble cabezal y multisensor.
- [Guía de la interfaz web de las cámaras Pro H4 y H5](#): para las cámaras Pro de alta resolución.
- [Guía de la interfaz web de la cámara ojo de pez H5A](#): para las cámaras ojo de pez H5A.
- [Guía de la interfaz web de APD](#): para intercomunicadores de vídeo H4.
- [Guía de la interfaz web del sensor APD](#): para los detectores de presencia Avigilon.

Acceso a la interfaz web de la cámara

Una vez instalada la cámara, necesita su dirección IP para acceder a la interfaz web. La dirección IP se puede encontrar en las siguientes ubicaciones:

- Software Avigilon Control Center (ACC): abra la pestaña Configuración para ver los detalles de la cámara seleccionada.
- Herramienta Camera Configuration Tool (CCT) de Motorola Solutions: vaya a la pestaña Network (Red) para ver los detalles de las cámaras seleccionadas.

Una vez que tenga la dirección IP, complete el siguiente procedimiento para acceder a la interfaz web:

Nota: El navegador web debe configurarse para aceptar cookies. De lo contrario, la interfaz web de la cámara no funcionará correctamente.

1. En un ordenador con acceso a la misma red que la cámara, introduzca dirección IP de la cámara en un navegador web:
`http://<dirección IP de la cámara>/`
Por ejemplo: `http://192.168.1.40/`
2. Se le pedirá automáticamente que introduzca su nombre de usuario y contraseña para acceder a la cámara. Si el dispositivo está en el estado predeterminado de fábrica y se fabricó después del 1 de enero de 2020, se le pedirá que cree un usuario con privilegios de administrador antes de que el dispositivo esté operativo. Para más información, consulte *Crear el usuario inicial e iniciar sesión* abajo.

Crear el usuario inicial e iniciar sesión

Las cámaras nuevas no tienen un nombre de usuario y contraseña predeterminados y estarán en un estado predeterminado de fábrica.

Importante: Debe crear un usuario con privilegios de *administrador* antes de que la cámara esté operativa.

Al iniciar sesión en la cámara por primera vez, se le redirigirá a la página Add User (Agregar usuario) para crear un usuario administrador:

1. Introduzca un nuevo **Nombre de usuario** o mantenga el nombre de `administrador` predeterminado.
2. Introduzca un nuevo **Password(Contraseña)** para el usuario. Recomendamos utilizar una contraseña compleja y única. Evite utilizar contraseñas vacías, ya que no son compatibles con todas las plataformas y dispositivos.
3. Confirme la nueva contraseña.
4. Para el primer usuario, se debe seleccionar *Administrator (Administrador)* en el menú desplegable **Security Group (Grupo de seguridad)**.
5. Haga clic en **Apply (Aplicar)**. Después de crear el usuario, se le pedirá que inicie sesión.

Iniciar sesión

Las cámaras fabricadas antes del 1 de enero de 2020 tienen un nombre de usuario y una contraseña predeterminados que puede usar para iniciar sesión.

Se le pedirá automáticamente que introduzca su nombre de usuario y contraseña para acceder a la cámara.

- Si la cámara está en el estado predeterminado de fábrica y se fabricó después del 1 de enero de 2020, se le pedirá que cree un usuario con privilegios de administrador antes de que la cámara esté operativa. Use estas credenciales al iniciar sesión.
- El nombre de usuario por defecto para la mayoría de las cámaras es `administrador` sin contraseña.

Sugerencia: Le recomendamos que agregue una contraseña tras el primer inicio de sesión. Para obtener más información, consulte *Edición de usuarios y contraseñas* en la página 43.

Live View (Imagen en vivo)

Después de iniciar sesión, la primera página que verá es Live View (Imagen en vivo). La Vista en directo contiene un panel de imágenes que muestra la transmisión de vídeo en directo.

Use los enlaces del menú en la esquina superior izquierda para navegar por la interfaz web. Haga clic en **Live View (Imagen en vivo)** en cualquier momento para volver a esta página.

Sugerencia: Las funciones y opciones no compatibles con la cámara están deshabilitadas.

Guardar una imagen fija

Si ve el botón **Save Still to SD Card (Guardar imagen fija en la tarjeta SD)** en la página Live View (Imagen en vivo), la cámara admite la capacidad de capturar instantáneas de vídeo en directo desde la interfaz web.

Para usar esta función, se requieren las siguientes configuraciones para la cámara:

- Hay una tarjeta SD insertada en la cámara. Para obtener más información, consulte la guía de instalación de la cámara. Si está utilizando cifrado FIPS de nivel 3 con una microtarjeta CryptR insertada en la ranura para tarjetas SD, no podrá guardar una imagen en la tarjeta SD.
- La configuración de almacenamiento interno de la cámara está habilitada en la página Storage (Almacenamiento). Para obtener más información, consulte *Almacenamiento* en la página 35.
- El formato de vídeo de la cámara debe establecerse en MJPEG en la página Compression and Image Rate (Compresión y velocidad de imagen). Para obtener más información, consulte *Compresión y velocidad de imagen* en la página 26.

Una vez que se hayan cumplido todos los requisitos, puede hacer clic en **Save Still to SD Card (Guardar imagen fija en la tarjeta SD)** y la imagen que se muestra en la página Live View (Imagen en vivo) se guardará automáticamente en la tarjeta SD.

Para descargar la instantánea, consulte *Descarga de vídeo grabado de la interfaz web* en la página 37.

Setup (Configuración)

Nota: Algunas opciones no se muestran si no son compatibles con el modelo de cámara que está usando o si no tiene los permisos de usuario requeridos.

Los ajustes predeterminados de fábrica le permiten usar la cámara o el codificador inmediatamente después de la instalación. Si tiene requisitos especiales, puede personalizar la configuración a través de la interfaz web. En el área superior izquierda del menú, haga clic en **Setup (Configuración)** para mostrar todas las páginas de configuración disponibles.

En cada página de configuración hay un botón **Restore Defaults (Restaurar predeterminados)** para restaurar los ajustes predeterminados de fábrica.

Tenga presente que algunos ajustes solo están disponibles a través de la interfaz web de la cámara y no se pueden cambiar en el software de gestión de vídeo en red.

Para obtener información específica sobre las cámaras H4 Edge Solution (ES), consulte *Cámara ACC™ ES* en la página 48.

Para conocer los ajustes específicos de las cámaras de detección térmica de temperatura elevada H4, consulte la [Guía del usuario de la cámara de detección térmica de temperatura elevada H4](#).

General

Al seleccionar Setup (Configuración), la primera página que aparece será la página de General (General). La página General (General) le permite establecer la identidad de la cámara.

Sugerencia: Las funciones y opciones no compatibles con la cámara están deshabilitadas.

Nota: Si traslada o ajusta una cámara con análisis de vídeo o una detección de movimiento inusual, o cambia el nivel de zoom o de enfoque, restablezca el progreso de aprendizaje para obtener resultados más precisos. Si se actualiza la configuración de velocidad y compresión o de visualización de la cámara, puede que el progreso de aprendizaje se restablezca automáticamente.

1. En el campo **Name (Nombre)**, asigne un nombre significativo a la cámara.
2. En el campo **Location (Ubicación)**, describa la ubicación de la cámara.
3. Seleccione la casilla de verificación **Disable device status LEDs (Desactivar los LED de estado del dispositivo)** para desactivar los indicadores LED situados en la cámara.
4. Seleccione la casilla **Lens Distortion Correction (Corrección de distorsión de lente)** para activar la corrección automática de la distorsión del objetivo basada en algoritmos. La cámara se reiniciará al aplicar este ajuste.
5. En la lista desplegable **Mode (Modo)**, seleccione el modo en el que va a funcionar la cámara.
Esa opción solo se muestra en aquellas cámaras que emplean un ancho de banda superior.
 - **Full Feature (Función completa):** este es el modo de funcionamiento estándar. Ofrece la funcionalidad completa de la cámara.
 - **High Framerate (Alta velocidad de fotogramas):** este modo utilizará la máxima velocidad de imagen posible, pero deshabilitará el análisis de vídeo con autoaprendizaje, la Unusual Motion Detection (UMD) y la detección de manipulación y WDR (rango dinámico amplio) en las cámaras ES.

Modelos	Características impactadas por High Framerate (Alta velocidad de fotogramas)
Cámaras analíticas 4K (8 MP) H4 HD: 8.0-H4A-x	<ul style="list-style-type: none">◦ Velocidad de fotogramas máxima aumentada◦ Manipulación y análisis de vídeo con autoaprendizaje deshabilitados◦ Unusual Motion Detection (UMD) deshabilitada◦ Transmisión de vídeo terciaria de menor resolución◦ Secuencia de vídeo secundaria deshabilitada

Modelos	Características impactadas por High Framerate (Alta velocidad de fotogramas)
---------	--

Cámaras analíticas H4 HD ES: xx-H4A-xG-x	<ul style="list-style-type: none">◦ Velocidad de fotogramas máxima aumentada◦ WDR desactivado
--	--

- **Sin análisis de vídeo:** este modo deshabilitará el análisis inteligente. Esta opción es para implementaciones en las que el análisis de vídeo basado en cámaras interferiría con otras integraciones de análisis.

6. Marque cualquiera de las casillas de verificación **Overlay Setting (Ajuste de superposición)** para mostrar y marcar esa información en la transmisión de vídeo de la cámara. Las opciones son:

- **Display Date (Mostrar fecha)**

La selección de la casilla de verificación **Display Date (Mostrar fecha)** también habilita la lista desplegable **Date Format (Formato de fecha)**. En la lista, elija el formato de fecha que se usará para mostrar la fecha.

- **Display Time (Mostrar hora)**
- **Display GMT Offset (Mostrar desplazamiento de GMT)**
- **Display Name (Mostrar nombre)**
- **Display Location (Mostrar ubicación)**

7. En el área **Time Settings (Configuración de hora)**, seleccione cómo establece la hora la cámara.

- Si prefiere establecer manualmente la fecha y la hora de la cámara, introduzca la zona horaria en esta página.
- Seleccione la casilla de verificación **Automatically adjust clock for Daylight Savings Time (Ajustar automáticamente el reloj en el horario de verano)** si es necesario.
- Si prefiere sincronizar automáticamente la fecha y la hora de la cámara con un servidor NTP, éste debe estar configurado. Haga clic en el enlace (**Configurar servidor NTP**) en la parte inferior de la página para ser redirigido a la página de Red.

Para obtener más información sobre cómo configurar el servidor NTP, consulte el Paso 7 en *Red* abajo.

PRECAUCIÓN: El ajuste de la hora siempre debe estar actualizado o el software ACC rechazará la transmisión de vídeo de la cámara. Para asegurarse de que la hora esté siempre actualizada, debe realizar una de las siguientes acciones:

- Configure NTP en el servidor DHCP utilizado por el software ACC.
- Utilice un servidor NTP público válido.
- Establezca manualmente la hora correcta en los campos **Time Settings (Configuración de hora)**.

8. Haga clic en **Apply (Aplicar)** para guardar los ajustes.

Red

En la página **Network (Red)**, puede cambiar cómo se conecta la cámara a la red del servidor y elegir cómo la cámara mantiene la hora.

1. En la parte superior de la página, seleccione la manera en que la cámara obtiene una dirección IP:
 - **Obtain an IP address automatically (Obtener una dirección IP automáticamente):** seleccione esta opción para conectarse a la red a través de una dirección IP asignada automáticamente. La dirección IP se obtiene de un servidor DHCP. En caso contrario, la dirección IP pasará al valor predeterminado de direcciones del rango 169.254.
 - **Use la siguiente dirección IP:** seleccione esta opción para asignar manualmente una dirección IP estática.
 - **IP Address (Dirección IP):** introduzca la dirección IP que desea usar.
 - **Subnet Mask (Máscara de subred):** introduzca la máscara de subred que desea usar.
 - **Default Gateway (Puerta de enlace predeterminada):** introduzca la puerta de enlace predeterminada que desea usar.
2. Seleccione la casilla de verificación **Disable setting static IP address through ARP/Ping method (Desactivar la configuración de dirección IP estática a través del método ARP/Ping)** para deshabilitar el método ARP/Ping para configurar una dirección IP.
3. Si la cámara admite IPv6, seleccione la casilla de verificación **Enable IPv6(Habilitar IPv6)** para configurar los siguientes ajustes.

Nota: La activación de IPv6 no deshabilita la configuración de IPv4.

- a. Asegúrese de que la casilla **Accept Router Advertisements(Aceptar anuncios de enrutador)** si utiliza la configuración automática de direcciones sin estado.
- b. En la lista desplegable **DHCPv6 State(Estado de DHCPv6)**, seleccione una de las siguientes opciones:
 - **Auto(Automático):** el estado DHCPv6 se determina por los anuncios del enrutador (RA).

Nota: La configuración Accept Router Advertisements(Aceptar anuncios de enrutador) debe estar habilitada para que esta configuración funcione como se espera.
 - **Stateful(Seguimiento de estado):** la cámara recibe información de dirección IP, DNS y NTP del servidor DHCPv6.
 - **Stateless(Sin estado):** la cámara recibe solo la información de DNS y NTP del servidor DHCPv6. No acepta una dirección IP del servidor DHCPv6.
 - **Off (Inactivo):** la cámara no se comunica con el servidor DHCPv6.
- c. En el campo **Static IPv6 Addresses(Direcciones IPv6 estáticas)**, introduzca la dirección IPv6 preferida.
 - Haga clic en + para obtener direcciones adicionales.
 - Haga clic en - para eliminar una dirección.

Para cambiar la longitud del prefijo, introduzca la dirección IPv6 preferida utilizando la notación de enrutamiento entre dominios sin clase (CIDR). Por ejemplo, `2001:db8::1/32` indicaría que el prefijo de la dirección tiene 32 bits de longitud.

Por defecto, la longitud del prefijo se establece en `/64`.

Nota: La longitud de prefijo configurada podría no verse correctamente en la interfaz web, pero el prefijo utilizado por la cámara tendrá la longitud configurada.

- d. En el campo **Default Gateway (Puerta de enlace predeterminada)**, introduzca la puerta de enlace predeterminada que prefiere usar. Solo puede asignar una puerta de enlace predeterminada si RA está deshabilitado.

Las direcciones IPv6 que se pueden usar para acceder a la cámara se enumeran en el área **Current IPv6 Addresses (Direcciones IPv6 actuales)**.

4. Si necesita personalizar el nombre de host, introdúzcalo en el campo **Hostname (Nombre de host)**.
5. En el área DNS Lookup (Búsqueda de DNS), seleccione cómo la cámara obtendrá una dirección de servidor de sistema de nombre de dominio (DNS).
 - **Obtain DNS server address automatically (Obtener dirección de servidor DNS automáticamente):** seleccione esta opción para buscar automáticamente un servidor DNS.
 - **Use the following DNS server addresses (Usar las siguientes direcciones de servidor DNS):** seleccione esta opción para configurar manualmente las direcciones del servidor DNS. Puede configurar hasta tres direcciones:
 - **Preferred DNS server (Servidor DNS preferido):** asigne la dirección del servidor DNS preferido en este campo.
 - **Alternate DNS server 1 (Servidor DNS alternativo 1):** asigne la dirección de un servidor DNS alternativo en este campo (opcional). En el caso de que el servidor preferido no esté disponible, la cámara intentará conectarse a este servidor.
 - **Alternate DNS server 2 (Servidor DNS alternativo 2):** asigne la dirección de otro servidor DNS alternativo en este campo (opcional). En el caso de que tanto el servidor preferido como el primer servidor alternativo no estén disponibles, la cámara intentará conectarse a este servidor.
6. En el área Control Ports (Puertos de control), puede especificar qué puertos de control se van a usar para acceder a la cámara. Puede introducir cualquier número de puerto entre 1 y 65 534. Los números de puerto predeterminados son:
 - **HTTP Port (Puerto HTTP): 80**

Si desea limitar el acceso a la cámara sólo a conexiones seguras, desactive la casilla de verificación **Enable HTTP connections (Habilitar conexiones HTTP)** HTTP Port (Puerto HTTP) está activado por defecto.
 - **HTTPS Port (Puerto HTTPS): 443**
 - **RTSP Port (Puerto RTSP): 554**
 - **RTSP Replay Port (Puerto RTSP de reproducción): 555**

7. En el área NTP Server (Servidor NTP), indique si desea que la cámara utilice un servidor NTP para conservar la hora.
 - a. Seleccione la fuente NTP para conservar la hora:
 - **Always use Avigilon Control Center NTP Server(Utilizar siempre el servidor NTP de Avigilon Control Center).** Seleccione esta opción si desea que la cámara conserve la hora solo a través del software Avigilon Control Center™.
 - **Always use external NTP server(Utilizar siempre servidor NTP externo).** Seleccione esta opción si desea usar solo un servidor NTP externo. A continuación, configure el servidor NTP para usarlo.
 - **Use NTP server when not connected to an external Avigilon Control Center Server (Utilizar el servidor NTP cuando no se esté conectado a un servidor externo de Avigilon Control Center).** De forma predeterminada, las cámaras Avigilon conservan la hora vez a través del software Avigilon Control Center y utilizarán un servidor NTP externo cuando no está conectada a un servidor ACC, si hay uno configurado.
 - b. Si está utilizando un servidor NTP externo, seleccione cómo está configurado el servidor:
 - **DHCP(DHCP:).**
 - **Manual: (Manual:).** Seleccione esta opción e introduzca la dirección del servidor en el campo **NTP Server (Servidor NTP).**
8. En el área MTU(MTU), configure el tamaño de la unidad máxima de transmisión (MTU) en bytes. Introduzca un número entre el rango disponible que se muestra a la derecha. Es posible que desee reducir el tamaño de MTU si su conexión de red es lenta.
9. En el área Ethernet Setting (Configuración de Ethernet), configure el parámetro **Speed & Duplex (Velocidad y dúplex)** para su conexión de red. La configuración Auto-negotiation (default) (Negociación automática (predeterminado)) es la configuración preferida para la mayoría de las cámaras y negociará la velocidad óptima y la configuración dúplex para su conexión de red. Si es necesario, puede seleccionar manualmente la configuración de velocidad y dúplex para su conexión.
10. En el área Security (Seguridad), configure el **Minimum TLS version (Versión mínima de TLS)** que debe usar la cámara para cifrar la comunicación entre la cámara y el servidor, y bloquee las versiones anteriores de TLS que no deban usarse.
 - Se recomienda **TLS 1.3** para una mayor seguridad.

Nota: Antes de activar esta opción, compruebe que su VMS la admite.

- Se puede seleccionar **TLS 1.2 (TLS 1.2)** si es necesario para contar con compatibilidad con versiones anteriores.

Nota: Algunas cámaras también pueden tener las opciones **TLS 1.1 (TLS 1.1)**, que se pueden seleccionar si es necesario para la compatibilidad con versiones anteriores.

11. Haga clic en **Apply (Aplicar)** para guardar los ajustes.

Configurar la autenticación basada en puertos 802.1X

Si su conmutador de red requiere autenticación 802.1X basada en puerto, puede configurar las credenciales de cámara adecuadas para que la transmisión de vídeo no se bloquee por la conmutación.

1. En el recuadro del menú de la izquierda, seleccione **Network (Red) > 802.1X(802.1X)**.
2. En la página Configure 802.1X Profiles (Configurar perfiles 802.1X), seleccione el método de autenticación preferido. Puede configurar varios perfiles. Tenga en cuenta que solo puede habilitar un perfil a la vez.

En la lista desplegable **EAP Method (Método EAP)**, seleccione una de las opciones siguientes y complete los campos relacionados:

- Seleccione **PEAP(PEAP)** para autenticar el nombre de usuario y la contraseña.
 - **Configuration Name (Nombre de configuración):** asigne un nombre al perfil.
 - **EAP Identity (Identidad EAP):** introduzca el nombre de usuario que se utilizará para autenticar la cámara.
 - **Password(Contraseña):** introduzca la contraseña que se utilizará para autenticar la cámara.
 - **Autenticar servidor:** marque esta casilla si necesita añadir un certificado.
- Seleccione **EAP-TLS(EAP-TLS)** para autenticar el certificado.
 - **Configuration Name (Nombre de configuración):** asigne un nombre al perfil.
 - **EAP Identity (Identidad EAP):** introduzca el nombre de usuario que se utilizará para autenticar la cámara.
 - **TLS Client Certificates (Certificados de cliente TLS):** seleccione el archivo de certificado con codificación PEM para autenticar la cámara.
 - **Private Key (Clave privada):** seleccione el archivo de llave privada con codificación PEM para autenticar la cámara.
 - **Private Key Password (Contraseña de clave privada):** si la clave privada tiene una contraseña, introduzca la contraseña aquí.
 - Haga clic en **Upload Files (Cargar archivos)** y el certificado de cliente TLS y la clave privada se cargarán en la cámara. Los archivos cargados se utilizan para generar un certificado único para autenticar la cámara. El certificado único se muestra en el campo Uploaded Certificate (Certificado cargado).

3. Haga clic en **Save Config (Guardar configuración)** para guardar el perfil de autenticación.

Si este es el primer perfil que se agrega a la cámara, se activará de forma automática.

Las configuraciones guardadas se muestran en **Saved 802.1X Configurations (Configuraciones 802.1X guardadas)**.

Conmutación de perfiles de autenticación 802.1X

Para usar un perfil de autenticación diferente, seleccione la configuración guardada y, a continuación, haga clic en **Enable (Activar)**.

Eliminación de un perfil de autenticación 802.1X

Para eliminar uno de los perfiles de autenticación, seleccione la configuración guardada y, a continuación, haga clic en **Remove (Suprimir)**.

Configurar SNMP

Puede usar el Protocolo simple de administración de redes (SNMP) para ayudar a administrar las cámaras que están conectadas a la red. Cuando el SNMP está habilitado, la información del estado de la cámara se puede enviar a una estación de administración del SNMP.

En la página SNMP(SNMP), puede configurar los ajustes del SNMP de la cámara y elegir la información de estado que se envía a la página de la estación de administración. Para obtener más información sobre la información de estado o las capturas que se enviarán, consulte el archivo de la Base de información de gestión (MIB) de la cámara en el sitio web de Avigilon: <http://avigilon.com/support-and-downloads>.

1. En el recuadro del menú de la izquierda, seleccione **Network (Red) > SNMP(SNMP)**.
2. En la página SNMP(SNMP), seleccione la casilla de verificación **Enable SNMP (Activar SNMP)**.
3. En la lista desplegable **Version (Versión)**, seleccione la versión de SNMP que prefiera. Tenga en cuenta que ambas versiones se pueden configurar, pero solo se puede habilitar una a la vez:
 - **SNMP v2c(SNMP v2c)**: con SNMP v2c, puede realizar una solicitud a la cámara para obtener información de estado a través de una solicitud SNMP Get y recibir notificaciones de captura de la cámara.

En el área **SNMP v2c Settings (Configuración de SNMP v2c)**, seleccione la casilla de verificación **Enable Traps (Activar capturas)** para activar las capturas de la cámara.

- a. **Read Community (Comunidad de lectura)**: introduzca el nombre de comunidad de lectura de la cámara. El nombre se usa para autenticar el tráfico SNMP. Solo las estaciones de administración de SNMP con el mismo nombre de comunidad de lectura recibirán una respuesta de la cámara.
- b. **Trap Destination IP (IP de destino de captura)**: introduzca la dirección IP de la estación de administración donde se enviarán las capturas.

En el área Available Traps (Capturas disponibles), seleccione las capturas que se enviarán:

- **Temperature Alert (Alerta de temperatura)**: se enviará una notificación de captura cuando la temperatura de la cámara esté por arriba o por debajo del umbral admitido. También se enviará una notificación cuando la temperatura de la cámara vuelva a la normalidad.
- **Camera Tampering (Manipulación de cámaras)**: se enviará una notificación de captura cuando la cámara de análisis de vídeo de la cámara detecte un cambio de escena repentino.
- **Edge Storage Status (Estado de almacenamiento de borde)**: se enviará una notificación de captura cuando cambie el estado de la tarjeta SD.

- **SNMP v3(SNMP v3):** al utilizar SNMP v3, puede solicitar información de estado a través de una solicitud SNMP Get. SNMP v3 no admite capturas.

SNMP v3 ofrece una mayor seguridad, ya que le permite configurar un nombre de usuario y una contraseña para la cámara. Esta cámara utiliza autenticación de tipo SHA-1 y cifrado de tipo AES.

En el área SNMP v3 Settings (Configuración de SNMP v3), complete los siguientes detalles:

- a. **Username (Nombre de usuario):** introduzca el nombre de usuario que debe usar la estación de administración al enviar la solicitud SNMP Get a la cámara.
- b. **Password(Contraseña):** introduzca la contraseña que la estación de administración debe usar con el nombre de usuario elegido.

4. Haga clic en **Apply (Aplicar)** para guardar los cambios.

Configuración de DSCP

Los servicios diferenciados o DiffServ es una arquitectura de red informática que especifica un mecanismo simple y escalable para clasificar y gestionar el tráfico de red y proporcionar calidad de servicio (QoS) en las redes IP modernas. DiffServ puede, por ejemplo, usarse para proporcionar baja latencia al tráfico de red crítico, como voz o transmisión de medios, al tiempo que proporciona un servicio simple de mejor esfuerzo a servicios no críticos, como tráfico web o transferencias de archivos.

DiffServ utiliza un punto de código de servicios diferenciados (DSCP) de 6 bits en el campo de servicios diferenciados (campo DS) de 8 bits del encabezado IP para clasificar los paquetes. El campo DS sustituye al anticuado campo TOS de IPv4. Cada valor DSCP representa una clase de QoS, también conocida como agregado de comportamiento. DiffServ es un mecanismo de gestión del tráfico de granularidad gruesa basado en clases.

En la página DSCP puede activar la función DSCP, elegir valores para los tipos de tráfico enumerados a continuación y restablecer los valores predeterminados.

1. En el panel izquierdo del menú, seleccione **Red > DSCP**.
2. En el área DSCP, la casilla **Activar función** está seleccionada por defecto. Desactive la casilla **Activar función** y haga clic en **Aplicar** para desactivar DSCP.
3. En el menú desplegable **protocolo ONVIF**, haga clic para seleccionar una de las opciones:
 - a. DF (0)
 - b. CS2 (16) (Esta es la opción predeterminada).
4. En el menú desplegable **Interfaz web**, haga clic para seleccionar una de las opciones:
 - a. DF (0)
 - b. AF21 (18) (Esta es la opción predeterminada).
5. En el menú desplegable **Protocolo SNMP**, haga clic para seleccionar una de las opciones:
 - a. DF (0)
 - b. CS2 (16) (Esta es la opción predeterminada).
6. En el menú desplegable **Transmisión en secuencia principal**, haga clic para seleccionar una de las opciones:

- a. CS3 (24)
 - b. AF31 (26)
 - c. CS4 (32)
 - d. AF41 (34) (Esta es la opción predeterminada).
7. En el menú desplegable **Transmisión en secuencia secundaria**, haga clic para seleccionar una de las opciones:
 - a. CS3 (24)
 - b. AF31 (26)
 - c. CS4 (32)
 - d. AF41 (34) (Esta es la opción predeterminada).
8. En el menú desplegable **Transmisión en secuencia terciaria**, haga clic para seleccionar una de las opciones:
 - a. CS3 (24) (Esta es la opción predeterminada).
 - b. AF33 (30)
9. En el menú desplegable **Retransmisión**, haga clic para seleccionar una de las opciones:
 - a. CS3 (24) (Esta es la opción predeterminada).
 - b. AF33 (30)
 - c. CS4 (32)
 - d. AF43 (38)
10. Haga clic en **Aplicar** para guardar los cambios.
11. Haga clic en **Restaurar valores predeterminados** y, a continuación, en **Aplicar** para restaurar los valores DSCP a sus valores predeterminados.

Nota: En caso de transmisión en flujo primario, secundario, terciario y de repetición, es muy importante preparar y configurar el tráfico de transmisión. En caso de transmisión a través de TCP (un socket común con RTSP), el valor DSCP se tomará de la transmisión en secuencia principal y se propagará a las otras transmisiones. La configuración de un flujo a través de UDP permite al usuario especificar diferentes valores DSCP para todos los flujos.

IP Filter (Filtro de IP)

En la página IP Filter (Filtro de IP) puede controlar qué direcciones IP pueden conectarse a su cámara.

Si está habilitada, podrá limitar las direcciones IP de dos formas:

- Deny Access (Denegar acceso) a direcciones IP específicas o rango de direcciones.
- Allow Access (Permitir acceso) solo a direcciones IP específicas o rango de direcciones.

Importante: Si opta por filtrar el acceso de IP utilizando la opción **Allow Access (Permitir acceso)**, asegúrese de configurar las direcciones correctas que se permitirán o es posible que no pueda acceder a su cámara.

1. En el panel de menú izquierdo, seleccione **Network (Red) > IP Filter (Filtro de IP)**.
2. Seleccione la casilla de verificación **Enable IP Filter (Habilitar filtro de IP)** para habilitar el filtrado de IP.
3. En la parte superior de la página, seleccione la manera en que la cámara debe filtrar las direcciones IP:
 - **Allow Access (Permitir acceso):** seleccione esta opción para permitir solo el acceso a las entradas de direcciones IP específicas que realizará a continuación. Asegúrese de agregar las entradas de dirección IP correctas o es posible que no pueda acceder a su cámara.
 - **Deny Access (Denegar acceso):** seleccione esta opción para denegar el acceso a las entradas de direcciones IP específicas que realizará a continuación. Este es la opción predeterminada.
4. Agregue las IP Filter Entries (Entradas de filtro de IP) cuyo acceso desea denegar o permitir:
 - a. En el campo **IPv4, IPv6 or CIDR range (Rango de IPv4, IPv6 o CIDR)** que aparece, introduzca el rango de direcciones IP IPv4, IPv6 o CIDR que desea filtrar.
 - b. Haga clic en + para añadir entradas adicionales a la lista de filtros IP y continúe añadiendo entradas adicionales a la lista hasta que haya añadido todas las direcciones IP necesarias para ser filtradas.

Sugerencia: Puede agregar hasta 256 IP Filter Entries (Entradas de filtro de IP).

5. Haga clic en **Apply (Aplicar)** para guardar los ajustes.

Nota: Si ha denegado o no ha permitido el acceso a la dirección IP que está utilizando actualmente para conectarse a su cámara, la conexión de su interfaz web se cerrará cuando haga clic en **Apply (Aplicar)**.

6. Haga clic en **Restaurar valores predeterminados** y, a continuación, en **Aplicar** para restaurar la configuración predeterminada del filtro IP.

Configuración de seguridad

Para una mayor seguridad en las comunicaciones de red, puede habilitar el cumplimiento de los Requisitos de seguridad de nivel 1 o nivel 3 del Estándar federal de procesamiento de información (FIPS) 140-2 para módulos criptográficos para la comunicación de cámaras y servidores.

Nota:

- El nivel 1 del FIPS 140-2 requiere la compra de una licencia de cámara FIPS.
- FIPS 140-2 Nivel 3 en cámaras con un TPM integrado requiere la compra de una licencia de cámara FIPS.
- FIPS 140-2 Nivel 3 en cámaras sin TPM integrado requiere la compra de una microtarjeta CRYPTR. La tarjeta CRYPTR debe insertarse en la ranura para tarjetas SD de la cámara antes de poder habilitarla.

1. En el panel de menú de la izquierda, seleccione **Red > Seguridad** para navegar a la página Configuración de Security (Seguridad).
2. En la lista desplegable Encryption Engine (Motor de cifrado), seleccione el tipo de cifrado que vaya a utilizar:

- **OpenSSL** es la opción predeterminada para el cifrado.
- **FIPS 140-2 (FIPS 140-2)** habilita el cifrado de nivel 1 del FIPS 140-2.
- **NXP TPM** permite que el módulo de plataforma de confianza (TPM) integrado almacene sus claves de cifrado de forma segura. Solo las cámaras que vienen con NXP TPM integrado mostrarán esta opción.
- **CRYPTR micro (CRYPTR micro)** permite que la tarjeta CRYPTR instalada almacene de forma segura sus claves cumpliendo con los requisitos de nivel 3 del FIPS 140-2.

Tenga en cuenta que las cámaras H6SL vienen con la opción TPM integrado y no son compatibles con las tarjetas CRYPTR.

Importante: Si cambia la configuración a CRYPTR micro (CRYPTR micro), la cámara generará una nueva clave y un certificado autofirmado. Es posible que se requiera cierta administración de certificados y claves cuando habilite esta configuración. Si una autoridad de certificación (CA) firmó sus claves anteriores, las claves nuevas que se generen también deberán contar con la firma de la CA para mantener la seguridad de la conexión a su cámara.

La Camera Configuration Tool (CCT) se puede utilizar para generar una solicitud de firma de certificado (CSR) desde la cámara y volver a cargar el certificado firmado en la cámara. Para obtener más información, consulte la *Guía del usuario de la Camera Configuration Tool*.

3. Haga clic en **Apply (Aplicar)** para guardar los ajustes.

Importante: Si cambia esta configuración en su cámara, deberá reiniciar su cámara y perderá la transmisión de vídeo durante ese tiempo. Avigilon recomienda aplicar esta configuración durante los momentos de funcionamiento no críticos.

Cuando habilite el cifrado CRYPTR, podrá acceder a la página **CryptR Log (Registro de CryptR)** seleccionándola en el menú lateral. Cuando el registro de auditoría interno de la microtarjeta CRYPTR alcanza el 80 % de su capacidad, las entradas se extraen automáticamente de la tarjeta, se registran en el registro del sistema de la cámara y se borra el registro de audio de la microtarjeta CRYPTR. En la página **CryptR Log (Registro de CryptR)** solo verá las entradas que aún no se hayan registrado en el registro del sistema de la cámara.

Nota: Si la microtarjeta CRYPTR se expulsa o se vuelve inutilizable mientras está insertada en la cámara y habilitada, la cámara se reiniciará en modo FIPS 140-2 (FIPS 140-2). Si la tarjeta se vuelve a insertar en la cámara, deberá volver a seleccionar CRYPTR micro (CRYPTR micro) como Encryption Engine (Motor de cifrado) para continuar usando la microtarjeta CryptR para almacenar sus claves.

Activación de la transmisión SRTP

La transmisión SRTP permite a la cámara transmitir mediante cifrado SRTP a sistemas de gestión de vídeo que también admitan SRTP. Para activar la transmisión SRTP, la cámara debe tener instalado el firmware correcto.

Nota: El uso de SRTP para integraciones de terceros puede requerir pasos adicionales. Para obtener información sobre la configuración de la transmisión SRTP cuando se utilizan integraciones de terceros, consulte la documentación del fabricante.

Requisitos

- La transmisión SRTP requiere una conexión HTTP.
Puede activar las conexiones HTTP en la interfaz web de la cámara. Para obtener instrucciones, consulte *Red* en la página 7.
- La transmisión SRTP requiere una conexión con la biblioteca OpenSSL y no funciona con FIPS 140-2 o NXP TPM.
Puede cambiar el motor de cifrado para utilizar OpenSSL en la página Seguridad de la interfaz web de la cámara. Para obtener instrucciones, consulte *Configuración de seguridad* en la página anterior.
- La transmisión SRTP requiere una conexión unidifusión y multidifusión sobre UDP.

Administrar certificados

En la página de Certificados, los administradores pueden gestionar los certificados. Los certificados se utilizan para autenticar dispositivos y cifrar la comunicación en la red.

En el área de Certificados, puede ver la siguiente información:

- **ID del certificado:** se utiliza para identificar de forma única el certificado.
- **Sujeto:** la entidad a la que pertenece un certificado: una máquina, un individuo o una organización.
- **Emisor:** la entidad que verificó la información y firmó el certificado.
- **Algoritmo:** contiene un algoritmo hash y un algoritmo de firma digital.
- **Fecha de caducidad:** la fecha de caducidad del certificado.
- **Tipo:** el tipo de certificado, es decir, de confianza o no de confianza.

Descarga de certificados

1. Para descargar un certificado, selecciónelo en la lista.
2. Haga clic en el botón **Download(Descargar)**.

Los certificados se descargan como archivos .pem.

Eliminación de certificados

1. Para eliminar un certificado, haga clic en el botón **Remove (Suprimir)**.
2. Haga clic en el botón **Aceptar**.

Descarga de solicitudes de firma de certificados

1. Para descargar la solicitud de firma de certificado (CSR), haga clic en el **botón CSR** de descarga e introduzca la siguiente información:
 - **Nombre común:** el nombre de host principal del servidor.
 - **Nombre alternativo:** los valores alternativos asociados al certificado, por ejemplo, dirección de correo electrónico, direcciones IP, URI, nombres DNS.
 - **(Opcional) Organización:** el nombre de la organización que solicita los certificados.
2. Haga clic en el botón **Download(Descargar)** para descargar el CSR.

Cargando certificados

1. Para cargar un certificado, haga clic en **Cargar certificado**.
 - a. **Certificado:** haga clic en **Elegir archivo** para cargar un certificado.
 - b. **Clave privada:** haga clic en **Elegir archivo** para cargar una clave privada.
 - c. **Contraseña de la clave privada:** introduzca la contraseña de la clave privada.
2. Haga clic en el botón **Cargar** para cargar el certificado.

Carga de certificados CA

1. Haga clic en el botón **Cargar** para cargar el certificado.
2. Para cargar un certificado de CA, haga clic en **Cargar certificado de CA**.
 - a. Certificado CA: haga clic en **Elegir archivo** para cargar un certificado CA.
 - b. ID de certificado CA: introduzca el ID de certificado CA.
3. Haga clic en el botón **Cargar** para cargar el certificado CA.

Imagen y Visualización

Sugerencia: Las funciones y opciones no compatibles con la cámara están deshabilitadas.

Nota: Si traslada o ajusta una cámara con análisis de vídeo o una detección de movimiento inusual, o cambia el nivel de zoom o de enfoque, restablezca el progreso de aprendizaje para obtener resultados más precisos. Si se actualiza la configuración de velocidad y compresión o de visualización de la cámara, puede que el progreso de aprendizaje se restablezca automáticamente.

En la página Image and Display (Imagen y Visualización), puede controlar los ajustes de exposición y de día/noche de la cámara.

La página Image and Display (Imagen y Visualización) incluye un panel de imágenes que muestra la transmisión de vídeo en directo de la cámara. Al hacer clic en **Apply (Aplicar)** para guardar los cambios, la transmisión de vídeo se actualiza para usar los nuevos ajustes.

Debajo del panel de imagen, se muestra la información siguiente en el lado derecho:

- Current Exposure (Exposición actual)
- Current Gain (Ganancia actual)
- Current Iris (Diafragma actual)
- Last Known Light Level (Último nivel de luz conocido)

Las cámaras IP Avigilon de alta definición disponen de controles de enfoque y zoom electrónicos, por lo que también puede establecer el zoom y el enfoque de la cámara desde esta página.

1. Para las cámaras H6SL, puede cambiar el tamaño y la ubicación de la **Zona de enfoque automático** haciendo clic y arrastrando el cuadro naranja de la **Zona de enfoque automático** en el campo de visión de la cámara.

Sugerencia: Las zonas de enfoque automático son visibles por defecto. Si la Zona de enfoque automático no es visible en el campo de visión de la cámara, asegúrese de que la casilla **Mostrar zonas de enfoque automático** esté seleccionada.

2. Utilice el control deslizante **Zoom (Zoom)** para ajustar la posición de zoom de la cámara.
 - Para ampliar, desplace el control deslizante hacia la derecha.
 - Para alejar, desplace el control deslizante hacia la izquierda.
3. Para enfocar manualmente la cámara, utilice los botones **Focus (Enfoque)**:
 - Para enfocar hacia cero:
 - Haga clic en << para dar un paso grande.
 - Haga clic en < para dar un paso pequeño.
 - Haga clic en **0** para enfocar en cero.
 - Para enfocar hacia el infinito:
 - Haga clic en >> para dar un paso grande.
 - Haga clic en > para dar un paso pequeño.
 - Haga clic en **Inf (Infinito)** para enfocar en infinito.
 - Si está disponible, haga clic en **Auto Focus (Enfoque automático)** para permitir que la cámara se enfoque.

Nota: Una vez que el enfoque se establece manualmente, no cambiará.

4. Si la cámara se desenfoca mientras está en modo monocromo por la noche, ajuste el control deslizante **IR Focus Offset (Corrección del enfoque por IR)** para compensar el cambio de enfoque causado por los iluminadores IR integrados o externos.
5. Utilice el selector **Image Rotation (Rotación de imagen)** desplegable para girar la imagen de vídeo. La opción predeterminada es **None (Ninguno)**. La imagen se puede girar 90 grados, 180 grados o 270 grados. La cámara se reiniciará al aplicar este ajuste y algunos ajustes de codificación volverán a su configuración predeterminada.

Nota: La rotación de imagen no debe combinarse entre la configuración de rotación de imagen de la cámara y VMS. Realice la rotación de imagen en la cámara o en el VMS, pero no en ambos.

6. Si están disponibles, seleccione la casilla para habilitar [[[Undefined variable webUI_ camera.TempRefocus]]]. Cuando está habilitada, la cámara se reenfocherà automáticamente a medida que la temperatura fluctúe.

Importante: Las zonas de enfoque automático se utilizan para enfocar automáticamente la cámara a medida que la temperatura fluctúa. Asegúrese de que la zona tenga suficiente contraste tanto de día como de noche.

7. Para establecer cómo la cámara compensa las condiciones de iluminación ambiental, defina los siguientes ajustes:
- **Day/Night Mode (Modo día/noche):** Use la lista desplegable Day/Night Mode (Modo día/noche) para establecer la forma en que la imagen de vídeo cambia entre el modo de día y el de noche.
 - **Automatic (Automático):** cuando el nivel de luz esté por encima del umbral de día/noche, la imagen de vídeo estará en color. Cuando el nivel de luz es inferior al umbral de día/noche, la cámara abrirá automáticamente el filtro de corte de infrarrojos y cambiará al modo monocromático. Si se han activado los iluminadores de infrarrojos, también se encenderán.
 - Marque la casilla **Restaurar automático después del tiempo de espera** para restaurar automáticamente el modo Día/Noche a **Automático** después de un determinado periodo de tiempo de espera. Al campo **Tiempo de espera** se puede asignar un valor entre 5 s y 3600 s para el periodo del tiempo de espera.
 - Use el control deslizante **Day/Night Threshold (Umbral de día/noche)** para establecer el umbral de día/noche. Mueva el control deslizante para seleccionar el nivel de luz cuando la cámara cambia entre el modo de día y el modo de noche. El control deslizante solo está disponible cuando el ajuste Day/Night Mode (Modo día/noche) está establecido en **Automatic (Automático)**.

El control deslizante puede mostrar uno de los siguientes valores:

 - **Day/Night Threshold (EV) (Umbral de día/noche (EV)):** el valor del control deslizante está en Valores de exposición (EV).

En el modo de día, el último nivel de luz conocido se muestra debajo del panel de imágenes y también se muestra como una barra azul en el control deslizante Day/Night Threshold (Umbral de día/noche).
 - **Umbral de día/noche (ganancia dB):** el valor del control deslizante se muestra en decibelios (dB).
 - Use la configuración **Hysteresis(Histéresis)** para refinar el desplazamiento del umbral.
 - Elija **Low (Bajo)** cuando la cámara debe pasar del día a la noche en escenas en las que la diferencia entre los niveles de luz y oscuridad son pequeñas.
 - Elija **High (Alto)** cuando la cámara debe cambiar los modos cuando la diferencia entre los niveles de luz y oscuridad son grandes.
 - El valor predeterminado es **Medium (Medio)**.

- **Color(Color):** la imagen de vídeo siempre será a color.
- **Monochrome (Monocromo):** la imagen de vídeo siempre será monocroma.
- **External (Externo):** la cámara abrirá el filtro de corte IR y cambiará al modo monocromo según el estado del circuito de entrada digital.

Nota: El estado predeterminado del circuito de la entrada digital se configura en la página Digital Inputs and Outputs (Entradas y salidas digitales). Para obtener más información, consulte *Entradas y salidas digitales* en la página 39

- **Day/Night Delay (seconds) (Retraso día/noche (segundos)):** establece el tiempo de retraso, en segundos, antes de que se realice el cambio del modo diurno al nocturno una vez que se alcance el umbral establecido.
- **Enable IR LED in Night Mode (Habilitar LED IR en modo nocturno):** Puede activar o desactivar manualmente los IR instalados en la cámara. Si no está marcada, los LEDs IR no se encenderán en modo Noche.
- **Enable Adaptive IR Compensation (Activar compensación adaptativa IR):** puede activar los ajustes de infrarrojos automáticos mediante la Compensación adaptativa IR. Esto permite que la cámara ajuste automáticamente la imagen de vídeo con respecto a la saturación causada por la iluminación de infrarrojos.
- **Mostrar ROI de contraste automático:** habilitar esta opción le permite ver y seleccionar la región de interés. El contraste se ajusta automáticamente en función de la región seleccionada.
- **Habilitar comprobación de visibilidad nocturna:** puede activar o desactivar manualmente la verificación de visibilidad nocturna en la cámara. La verificación de visibilidad nocturna, cuando está activada, realiza una prueba periódica de cambio entre el modo día/noche para verificar si hay suficiente nivel de luz para cambiar del modo nocturno al modo día. Cuando está desactivada, la cámara utilizará un método menos óptimo para determinar si el nivel de luz es suficiente para cambiar al modo diurno.

Nota: Deshabilitar la verificación de visibilidad nocturna podría retrasar la transición de la cámara entre los modos de noche y día, y hacer que el tiempo de transición sea menos óptimo. Por ejemplo, la cámara permanece en modo nocturno 30 minutos más de lo necesario.

- **Fast Night To Day Switch (Cambio rápido de noche a día):** habilite esta opción para acelerar el tiempo que tardan las cámaras en cambiar entre los modos de día y de noche. Cuando esta opción está habilitada, el cambio entre los modos de día y de noche tardará de 2 a 3 segundos. Actualmente esta opción solo está disponible con cámaras H5SL.

Nota: Esta opción está desactivada de forma predeterminada. Se recomienda NO habilitar esta opción en cámaras instaladas en lugares donde las fuentes de luz adicionales (como faros, reflectores y luces de la calle) pueden hacer que la cámara cambie frecuentemente entre el modo de día y el de noche.

8. Para ajustar la exposición de la imagen, ajuste Exposure Settings (Configuración de la exposición):

- **Flicker Control (Control de parpadeo):** si la imagen de vídeo parpadea debido a las luces fluorescentes que rodean la cámara, puede reducir los efectos de la luz al establecer Flicker Control (Control de parpadeo) en la misma frecuencia que las luces. En general, Europa es **50 Hz** y América del Norte es **60 Hz**.

Nota: Restablecer este control detendrá la transmisión de vídeo durante unos segundos.

- **Enable Wide Dynamic Range (Activar rango dinámico amplio):** puede activar los ajustes automáticos del color mediante el Rango dinámico amplio (WDR). Esto permite que la cámara ajuste la imagen de vídeo para adaptarse a las escenas en las que la luz brillante y la sombra oscura son claramente visibles.
- **Exposure (Exposición):** puede permitir que la cámara controle la exposición al seleccionar **Automatic (Automático)** o puede establecer una velocidad de exposición específica.

Nota: El aumento del tiempo de exposición manual puede afectar la velocidad de imagen.

- **Exposure Offset (Compensación de la exposición):** se trata de una configuración avanzada que le permite compensar condiciones de iluminación inusuales estableciendo un valor de compensación de exposición. Los valores negativos dan como resultado una imagen persistentemente más oscura, y los valores positivos dan como resultado una imagen persistentemente más brillante.
- **Maximum Exposure (Exposición máxima):** puede limitar el ajuste de exposición automática al seleccionar un nivel de exposición máxima. La lista desplegable Maximum Exposure (Exposición máxima) solo está disponible cuando el ajuste Exposure (Exposición) está establecido en Automatic (Automático).

Al establecer un nivel de exposición máxima para las situaciones con poca luz, puede controlar el tiempo de exposición de la cámara para permitir la máxima cantidad de luz sin crear imágenes borrosas.

- **Priority (Prioridad):** puede establecer **Velocidad máxima de imagen** o **Exposure (Exposición)** como prioridad.
 - Si se establece en **Velocidad máxima de imagen**, la cámara mantendrá la velocidad de imagen establecida como prioridad y no ajustará la exposición más allá de lo que se puede grabar para la velocidad de imagen establecida.
 - Si se establece en **Exposure (Exposición)**, la cámara mantendrá el ajuste de exposición como prioridad y anulará la velocidad de imagen establecida para conseguir la mejor imagen posible.
- **Maximum Iris (Diafragma máximo):** puede limitar la apertura de iris más grande que usará la lente configurando una apertura de iris máxima. Este valor es un número f. También se administra en EV en relación con la apertura más amplia posible de la lente. Este ajuste solo está disponible cuando el parámetro **Iris (Diafragma)** se ha establecido en **Automatic (Automático)**.

La apertura del iris también afecta a la cantidad de la escena enfocada. El número f más pequeño (0 EV) establece el iris en la apertura más amplia posible. Esto permite la mayor cantidad de luz en la cámara, pero enfoca menos la escena. Los números f más grandes (EV negativo) dan como resultado una apertura máxima más pequeña, enfocando más la escena. La cámara corregirá automáticamente la disminución de la luz utilizando una ganancia más alta o un tiempo de exposición más largo.

- **Preferred Iris (Diafragma preferido):** puede establecer una apertura de diafragma ideal para lograr una imagen con el contraste y enfoque correctos en las condiciones de iluminación más frecuentes. Este valor es un número f. También se administra en EV en relación con la apertura más amplia posible de la lente. Este ajuste solo está disponible cuando el parámetro **Iris (Diafragma)** se ha establecido en **Automatic (Automático)**.

Nota: El valor Preferred Iris (Diafragma preferido) debe ser menor o igual que el valor Maximum Iris (Diafragma máximo).

El número f más pequeño (0 EV) establece el iris en la apertura más amplia posible. Esto permite la mayor cantidad de luz en la cámara, pero enfoca menos la escena. Los números f más grandes (EV negativo) dan como resultado aperturas más pequeñas, enfocando más la escena. La cámara corregirá automáticamente la disminución de la luz utilizando una ganancia más alta o un tiempo de exposición más largo.

- **Backlight Compensation (Compensación de contraluz):** si su escena tiene áreas de luz intensa que hacen que la imagen general sea demasiado oscura, puede habilitar Backlight Compensation (Compensación de contraluz) para lograr una imagen bien expuesta.
- **Iris (Diafragma):** puede permitir que la cámara controle el diafragma al seleccionar **Automatic (Automático)**, o puede establecerlo manualmente en **Open (Abrir)** o **Closed (Cerrado)**.
- **Maximum Gain (Ganancia máxima):** puede limitar el ajuste de ganancia automática al seleccionar un nivel de ganancia máxima.

Al establecer el nivel de ganancia máxima para situaciones de poca luz, puede potenciar al máximo los detalles de una imagen sin crear un ruido excesivo en las imágenes.

- **Ecualización:** esta configuración le permite ajustar la imagen de la cámara para igualar la diferencia de color entre los objetos cálidos y fríos. Un valor más bajo hará que los objetos cálidos sean más notables. Aumentar el valor dará como resultado una imagen de vídeo más equilibrada.

9. Haga clic en **Apply (Aplicar)** para guardar los cambios.

Adjustments (Ajustes)

En la página Adjustments (Ajustes), puede controlar la configuración de color, contraste y brillo de la imagen de vídeo.

La página Adjustments (Ajustes) también incluye un panel de imagen que muestra la transmisión de vídeo en directo de la cámara. Al hacer clic en **Apply (Aplicar)** para guardar los cambios, se actualiza la transmisión de vídeo.

Sugerencia: Las funciones y opciones no compatibles con la cámara están deshabilitadas.

1. En el panel de menú izquierdo, seleccione **Image and Display (Imagen y Visualización) > Adjustments (Ajustes)**.
2. Ajuste la imagen de vídeo según sea necesario.

Puede usar una configuración preestablecida o puede crear su propia configuración personalizada. Utilice la lista desplegable **Preset (Preselección)** para seleccionar la configuración que prefiera:

- a. **Avigilon:** esta preselección proporciona el balance de brillo y color recomendado para la videovigilancia.
- b. **Standard (Estándar):** esta preselección se configura para los cambios de día/noche generales en una escena interior o exterior.
- c. **Vivid (Intenso):** esta preselección ofrece un mayor color y brillo en una imagen más saturada.
- d. **Custom (Personalizado):** seleccione esta opción para configurar manualmente los ajustes de imagen siguientes:

Nota: Los parámetros Brightness (Brillo) y Contrast (Contraste) se deshabilitan si se habilita el rango dinámico amplio.

- **Saturation (Saturación):** puede ajustar la saturación de color del vídeo al introducir un porcentaje.
0 crea una imagen en blanco y negro, mientras que 100 crea imágenes en color intenso.
- **Sharpness (Nitidez):** puede ajustar la nitidez del vídeo al introducir un porcentaje.
0 aplica la menor cantidad de nitidez, mientras que 100 aplica la mayor nitidez para que los bordes de los objetos sean más visibles.

- **Brightness (Brillo):** puede ajustar el brillo del vídeo al introducir un porcentaje. 0 crea una imagen oscura, mientras que 100 crea una imagen llena de luz.
 - **Contrast (Contraste):** puede ajustar el contraste del vídeo al introducir un porcentaje. 0 aplica la cantidad mínima de contraste, mientras que 100 aplica el máximo contraste entre los objetos y la imagen.
3. Use la lista desplegable **White Balance (Balance de blancos)** para seleccionar cómo se controlan los ajustes del balance de blancos:
 - **Automatic (Automático):** la cámara controlará automáticamente el balance de blancos.
 - **Custom (Personalizado):** configure manualmente los niveles de **Red(Rojo)** y **Blue (Azul)**.

Dominant Color Compensation (Compensación de color dominante) (si está disponible): esta opción habilita un algoritmo de balance de blancos automático alternativo que debe usarse si un área grande del campo de visión contiene un color. Por ejemplo, una cámara que mira hacia un campo de hierba. Para este ejemplo, el modo de balance de blancos Dominant Color Compensation (Compensación de color dominante) mejorará el balance de blancos a un color más neutro.

4. Mueva el control deslizante **Temporal Filter Strength(Potencial de filtro temporal)** ligeramente hacia la izquierda o hacia la derecha para ajustar la cantidad de ruido frente al desenfoque en la escena. Un filtro temporal reduce el ruido de la imagen promediando el ruido en varios fotogramas.

Sugerencia: Empiece haciendo pequeños ajustes, ya que, si se aplican cambios excesivos, se puede degradar la calidad general de la imagen.

Si la imagen parece ruidosa, mueva el control deslizante hacia la derecha para reducir la cantidad de ruido en la escena y disminuir el ancho de banda utilizado.

Si la imagen parece borrosa, mueva el control deslizante hacia la izquierda para reducir la cantidad de desenfoque en la escena y aumentar el ancho de banda utilizado.

De forma predeterminada, el control deslizante se establece a la mitad, o 50.

5. Haga clic en **Apply (Aplicar)** para guardar los cambios.

Compresión y velocidad de imagen

En la página Compresión y velocidad de imagen, puede cambiar la configuración de la compresión y la calidad de imagen de la cámara para enviar vídeos a través de la red. Puede cambiar la configuración de la calidad de imagen y la compresión de la cámara por separado para los flujos primarios, secundarios y terciarios.

Nota: Si traslada o ajusta una cámara con análisis de vídeo o una detección de movimiento inusual, o cambia el nivel de zoom o de enfoque, restablezca el progreso de aprendizaje para obtener resultados más precisos. Si se actualiza la configuración de velocidad y compresión o de visualización de la cámara, puede que el progreso de aprendizaje se restablezca automáticamente.

Para habilitar un fácil acceso y un menor uso de ancho de banda, la interfaz web solo muestra vídeos en formato JPEG. La configuración de esta página solo afecta el vídeo transmitido al software de gestión de vídeos en red.

Las cámaras IP de alta definición de Avigilon tienen capacidad multidifusión. Si el formato de transmisión de la cámara está configurado en H.264 o H.265, la interfaz web de la cámara aún puede mostrar video en vivo en formato JPEG.

Nota: La cámara puede ajustar automáticamente la calidad de compresión para cumplir con el límite de ancho de banda especificado.

Importante: El ajuste de la configuración de la transmisión con HDSM habilitado y conectado a Avigilon Control Center (ACC) o Avigilon Unity Video (AUV) puede causar un comportamiento no deseado en el funcionamiento de la cámara y la falta de grabaciones. Los ajustes del flujo de cámara sólo deben configurarse en ACC o AUV.

Siga estos pasos para cada uno de los flujos primario, secundario y terciario para cambiar los ajustes de compresión y calidad de imagen de cada flujo.

1. En la lista desplegable **Format (Formato)**, seleccione el formato de transmisión preferido para ver el vídeo de la cámara en el software de gestión de vídeo en red.
Si utiliza la función Onboard Storage (Almacenamiento interno), seleccione **H.264(H.264)** o **H.265**. Para obtener más información, consulte *Habilitar el almacenamiento interno* en la página 36.
2. En el campo **Velocidad máxima de imagen**, introduzca cuántas imágenes por segundo desea que la cámara transmita por la red.

Nota: Ajustar la velocidad de imagen en un límite de 30 fps detendrá la transmisión de vídeo durante unos segundos.

Si la cámara funciona en modo High Framerate (Alta velocidad de fotogramas), la velocidad máxima de imagen aumenta. Para obtener más información sobre el modo High Framerate (Alta velocidad de fotogramas), consulte *General* en la página 6.

3. En la lista desplegable **Máxima calidad**, seleccione el nivel de calidad de la imagen exportada.
Un ajuste de calidad de imagen de 1 producirá el vídeo de calidad más alta y requerirá la mayoría ancho de banda.
4. En el campo **Max Bitrate (Velocidad de bits máxima)**, introduzca el ancho de banda máximo que la cámara puede usar.
5. En la lista desplegable **Resolution(Resolución) principal**, seleccione la resolución de imagen preferida.

6. En el campo **Min Keyframe Interval (Intervalo mínimo de fotogramas clave)**, introduzca el número de fotogramas entre cada fotograma clave.
7. Haga clic en **Apply (Aplicar)** para guardar los cambios.

Activación de los ajustes de tecnología de HDSM SmartCodec™

La tecnología HDSM SmartCodec funciona mediante la separación de objetos de primer plano y las áreas de fondo, y reduce el ancho de banda mediante el aumento de la compresión de las áreas de fondo. De esta forma, se conserva la máxima calidad para los sujetos de interés, al tiempo que se reduce el ancho de banda para fondos sin cambios.

Una vez habilitada, la cámara cambiará automáticamente a la configuración del modo de escena inactiva cuando no se detecten eventos de movimiento. Un evento de movimiento se produce cuando la cámara detecta movimiento de píxeles en la escena. Para obtener más información, consulte *Motion Detection (Detección de movimiento)* en la página 30.

La cámara utiliza el movimiento de cambio de píxeles para detectar objetos en primer plano y, por lo tanto, utiliza la configuración de sensibilidad de detección de movimiento estándar de la cámara.

Nota: De forma adicional, los ajustes avanzados también se pueden actualizar en la página Ajustes avanzados de HDSM SmartCodec. Para obtener más información, consulte *Ajustes avanzados de tecnología HDSM SmartCodec* en la página siguiente.

1. Seleccione la casilla de verificación **Enable (Activar)** para activar las funciones de HDSM SmartCodec.
2. En el campo **Velocidad de imagen mínima**, introduzca cuántas imágenes por segundo desea que la cámara transmita cuando no haya movimiento en la escena.
3. En el campo **Intervalo de fotograma clave inactivo**, introduzca el número de fotogramas entre cada fotograma clave (entre 1 y 254) cuando no haya movimiento en la escena.
4. En la lista desplegable **Reducción del ancho de banda**, seleccione una de las opciones:
 - **Low (Bajo)**
 - **Medium (Medio)** (recomendado)
 - **High (Alto)**
 - **Custom (Personalizado)**
5. Haga clic en **Apply (Aplicar)** para guardar los cambios.

Visualización de la URI de transmisión RTSP

En la página Compression and Image Rate (Compresión y velocidad de imagen), también puede generar el protocolo de transmisión en tiempo real (RTSP) de la cámara. La URI de transmisión RTSP le permite ver la transmisión de vídeo en vivo de la cámara desde cualquier aplicación que admita la visualización de transmisiones RTSP, incluidos muchos reproductores de vídeo.

Nota: Solo puede generar la dirección de transmisión RTSP en la interfaz web de la cámara.

1. Si el botón **Generate RTSP Stream URI (Generar URI de transmisión RTSP)** no está disponible, el URI de transmisión RTSP se genera automáticamente.

En el área RTSP Stream URI (URI de transmisión RTSP), se muestran los URI generados automáticamente:

- **Unicast (Unidifusión):** seleccione esta opción si solo tiene previsto visualizar la transmisión de vídeo en un reproductor de vídeo a la vez.
- **Multicast (Multidifusión):** seleccione esta opción si tiene previsto visualizar el vídeo desde más de un reproductor de vídeo simultáneamente.

Para ver la transmisión RTSP:

- a. Copie y pegue la dirección generada en su reproductor de vídeo. NO abra la transmisión de vídeo en vivo todavía.
- b. Agregue su nombre de usuario y contraseña al comienzo de la dirección en este formato:

```
rtsp://<nombre de usuario>:<contraseña>@<RTSP Stream URI generado>/
```

Por ejemplo:

```
rtsp://admin:admin@192.168.1.79/defaultPrimary?streamType=u
```

- c. Abra la transmisión de vídeo en vivo.

2. Para ver la transmisión de vídeo en vivo de la cámara desde un reproductor de vídeo externo, haga clic en **Generate RTSP Stream URI (Generar URI de transmisión RTSP)**.

La dirección generada se muestra en la parte inferior del área RTSP Stream URI (URI de transmisión RTSP).

Acceso a la URI de imagen fija

En la página **Compression and Image Rate (Compresión y velocidad de imagen)**, puede acceder al último fotograma de imagen fija grabado por la cámara.

- Para acceder a la imagen fija, haga clic en el enlace de la URI en el área URI de imágenes fijas.

Se muestra el último fotograma de vídeo grabado de la transmisión secundaria de la cámara. Puede elegir guardar o imprimir la imagen directamente desde el navegador.

Ajustes avanzados de tecnología HDSM SmartCodec

En la página **Ajustes avanzados de tecnología HDSM SmartCodec**, puede seleccionar ajustes para escenas de movimiento y de inactividad. Otros ajustes de tecnología avanzada de HDSM SmartCodec pueden seleccionarse en **Ajustes de tecnología de HDSM SmartCodec** en la página **Compresión y velocidad de imagen**. Para obtener más información, consulte *Activación de los ajustes de tecnología de HDSM SmartCodec™* en la página anterior.

1. En el recuadro del menú de la izquierda, seleccione **Compression and Image Rate (Compresión y velocidad de imagen) > Avanzado**.
2. En el campo **Calidad de fondo** de la sección **En movimiento**, introduzca la calidad de compresión para el fondo (entre el valor predeterminado de 6 y la configuración más baja de 20).
3. En el campo **Demora tras movimiento** de la sección **En escenas de inactividad**, introduzca la demora (en segundos) una vez finalizado el movimiento antes de que la cámara accione la configuración de escena de inactividad (entre 5 y 60).
4. En el campo **Velocidad de imagen** de la sección **En escenas de inactividad**, introduzca la velocidad de fotogramas codificada (imágenes por segundo) cuando no haya movimiento en la escena.
5. En el campo **Calidad** de la sección **En escenas de inactividad**, introduzca la calidad de compresión cuando no haya movimiento en la escena (entre 6 y 20).
6. En el campo **Velocidad de bits máxima** de la sección **En escenas de inactividad**, introduzca el número máximo de kilobytes por segundo cuando no haya movimiento en la escena.
7. En el campo **Intervalo de fotograma clave** de la sección **En escenas de inactividad**, introduzca el número de fotogramas entre cada fotograma clave cuando no haya movimiento en la escena (entre 1 y 254 fotogramas).
8. Haga clic en **Apply (Aplicar)** para guardar los cambios.

Motion Detection (Detección de movimiento)

En la página Detección de movimiento, puede definir las áreas verdes de detección de movimiento en el campo de visión de la cámara. La detección de movimiento se ignora en las áreas no resaltadas en verde.

Para ayudarlo a definir la sensibilidad y el umbral de movimiento, el movimiento se resalta en rojo en el panel de imágenes.

Nota: Este ajuste de detección del movimiento configura la detección de cambio de píxeles en el campo de visión de la cámara. Si está configurando una cámara de análisis de vídeo Avigilon, deberá configurar la detección de movimiento de análisis detallado y otras funciones de análisis de vídeo a través del software Avigilon Control Center Client. Para obtener más información, consulte la *Guía del usuario de Avigilon Control Center Client*.

1. Defina el área de detección de movimiento.

Todo el campo de visión se resalta durante la detección de movimiento de forma predeterminada. Para definir el área de detección de movimiento, use cualquiera de las siguientes herramientas:

- Haga clic en **Clear All (Borrar todo)** para eliminar todas las áreas de detección de movimiento en la imagen de vídeo.
- Haga clic en **Set All (Establecer todo)** para configurar el área de detección de movimiento y abarcar toda la imagen de vídeo.

- Para establecer un área de detección de movimiento específica, haga clic en **Select Area (Seleccionar área)**, y a continuación, haga clic y arrastre en cualquier lugar de la imagen de vídeo.
 - Para borrar un área específica de detección de movimiento, haga clic en **Clear Area (Borrar área)** y, a continuación, haga clic y arrastre sobre cualquier área de detección de movimiento.
 - Use los botones **Zoom In (Acercar)** y **Zoom Out (Alejar)** para ubicar áreas específicas en la imagen de vídeo.
2. En el campo **Sensitivity (Sensibilidad)**, introduzca un porcentaje para definir cuánto debe cambiar cada píxel antes de que se considere en movimiento.
Cuanto mayor sea la sensibilidad, menor será la cantidad de cambio de píxel antes de que se detecte movimiento.
 3. En el campo **Threshold (Umbral)**, introduzca un porcentaje para definir cuántos píxeles deben cambiar antes de considerar que la imagen tiene movimiento.
Cuanto mayor sea el umbral, mayor será el número de píxeles que debe cambiar antes de que se considere que la imagen tiene movimiento.
 4. Si la cámara está conectada a un sistema de gestión de vídeo de otro fabricante (VMS), marque la casilla de verificación **Enable Onvif MotionAlarm Event (Activar evento de alarma de movimiento de Onvif)**.
Una vez habilitada, la cámara H.264 puede enviar información de alarma de movimiento al VMS de acuerdo con el protocolo ONVIF apropiado.
 5. Haga clic en **Apply (Aplicar)** para guardar los cambios.

Tamper Detection(Detección de manipulación)

En la página Tamper Detection(Detección de manipulación), puede establecer la sensibilidad de la cámara a la manipulación.

Para configurar las opciones de manipulación:

1. En el campo **Sensitivity (Sensibilidad)**, introduzca un número entre 1 y 10 para definir la sensibilidad de la cámara a un cambio repentino en la escena. Cuanto mayor sea el ajuste, más sensible es la cámara para detectar cambios de escena.

Nota: Un cambio repentino en la escena generalmente está causado por alguien que mueve la cámara de forma inesperada. Reduzca el ajuste si los pequeños cambios en la escena, como las sombras en movimiento, provocan eventos de manipulación. Si la cámara está instalada en el interior y es probable que la escena no cambie, puede aumentar este ajuste para capturar los eventos más inusuales.

2. En el campo **Trigger Delay(Retraso de desencadenador)**, introduzca la cantidad de segundos (hasta 30 segundos) que la condición de manipulación debe persistir en la escena antes de que se envíe el

evento de manipulación.

3. Haga clic en **Apply (Aplicar)** para guardar los cambios.

Configuración de análisis

En la página Análisis, puede configurar Análisis de autoaprendizaje.

1. Seleccione la casilla de verificación **Activar autoaprendizaje** para activar el análisis de autoaprendizaje.
2. Seleccione la casilla **Suspender autoaprendizaje** para desactivar temporalmente el análisis de autoaprendizaje.
3. Haga clic en el botón **Restablecer auto** aprendizaje para restablecer el autoaprendizaje.

Importante: Esta acción no puede deshacerse.

4. Haga clic en **Apply (Aplicar)** para guardar los cambios.

Configuración ampliada

En la página Configuración ampliada, puede configurar la configuración de ONVIF.

1. Seleccione la casilla **Activar documentos XML multipaquete** para activar los documentos XML multipaquete para reducir el tamaño de los metadatos. Sólo para sistemas de gestión de vídeo que admitan documentos XML multipaquete.
2. Seleccione la casilla **Activar solicitudes de opciones de análisis** para activar las Opciones para obtener el módulo de análisis y las Solicitudes para obtener las opciones de las reglas.
3. Seleccione la casilla **Activar metadatos XML** de análisis para enviar metadatos de análisis en el flujo de metadatos XML.
4. Seleccione la casilla **Activar codificación por longitud de ejecución de la máscara de movimiento** para activar la codificación por longitud de ejecución de la máscara de movimiento. Sólo para sistemas de gestión de vídeo que no requieran una máscara sin codificar.
5. Seleccione la casilla **Activar eventos suplementarios** para enviar eventos suplementarios no definidos por ONVIF que pueden ser útiles para algunos Sistemas de gestión de vídeo.
6. Seleccione la casilla **Activar eventos de análisis de instancia única** para enviar eventos de análisis de estancia única en lugar de eventos de propiedad.
7. Haga clic en **Apply (Aplicar)** para guardar los cambios.

Zonas de privacidad

En la página Privacy Zones (Zonas de privacidad), puede establecer zonas de privacidad en el campo de visión de la cámara para bloquear áreas que no desea ver o grabar. También puede crear zonas de privacidad extraíbles que sean borrosas en lugar de opacas. Las zonas de privacidad extraíbles solo se aplican a la transmisión de vídeo secundaria y terciaria. Esto permite que en ACC los ajustes de grupos y privilegios definan qué usuarios pueden ver la transmisión principal sin las zonas de privacidad extraíbles y qué usuarios solo pueden ver las transmisiones con las zonas de privacidad borrosas. Para obtener más información, consulte *Configurar una zona de privacidad extraíble para usuarios específicos* en la página siguiente.

La cámara admite hasta 64 zonas de privacidad. Hasta 16 de estas zonas pueden utilizarse como zonas de privacidad extraíbles.

Ajuste de una zona de privacidad

1. Para agregar una zona de privacidad, haga clic en **Add (Agregar)**. Se agrega un cuadro de zona de privacidad a la imagen de vídeo.
2. Para definir el área de la zona de privacidad, realice una de las siguientes acciones:
 - a. Arrastre cualquier lado o esquina del cuadro para cambiar el tamaño de la zona de privacidad. Las zonas de privacidad solo pueden ser de forma rectangular. Se pueden utilizar múltiples zonas de privacidad para ocultar otras formas.
 - b. Haga clic dentro del cuadro y arrastre para mover la zona de privacidad.
3. Para establecer la zona de privacidad como extraíble:
 - a. Haga clic en la casilla de verificación **Enable (Activar)** en los ajustes de **Removable Blur (Desenfoque eliminable)**.
 - b. Utilice la **Blurriness (Nivel de desenfoque)** para definir la cantidad de desenfoque en las zonas de privacidad. Todos los ajustes de Blurriness (Nivel de desenfoque) harán que el vídeo de esa zona quede completamente oscurecido.

Nota: Las zonas de privacidad extraíbles tienen líneas diagonales al configurarlas en la página Privacy Zones (Zonas de privacidad) para ayudar a distinguirlas de las zonas de privacidad normales. Cuando se vea en la página Live View (Imagen en vivo) o en un cliente ACC, la zona aparecerá como un rectángulo gris borroso.

4. Haga clic en **Apply (Aplicar)** para guardar la configuración de la zona de privacidad.

Eliminación de una zona de privacidad

Haga clic en **X(X)** en la esquina superior derecha del cuadro gris para eliminar la zona de privacidad. También puede seleccionar la zona de privacidad que desea eliminar de la lista y hacer clic en **Eliminar**.

Configurar una zona de privacidad extraíble para usuarios específicos

Esto solo se admite al conectar la cámara a un sistema ACC. Las zonas de privacidad extraíbles solo se aplican a la transmisión de vídeo secundaria y terciaria para que la configuración de ACC grupos y privilegios puedan utilizarse para definir qué usuarios pueden ver la transmisión principal sin las zonas de privacidad extraíbles y qué usuarios solo pueden ver las transmisiones con las zonas de privacidad borrosas.

Nota: Las zonas de privacidad extraíbles solo se aplican a la transmisión de vídeo secundaria y terciaria de cualquier VM a la que la cámara esté conectada. Otros sistemas VMS pueden tener

configuraciones de privilegios de usuario similares que pueden utilizarse como un método similar para definir qué transmisión pueden ver los usuarios. Consulte la documentación de su VMS para saber cómo configurar las transmisiones que los usuarios tienen acceso a ver.

El privilegio de grupo ACC Ver imágenes en alta resolución da a los usuarios de ese grupo acceso a la transmisión principal de alta resolución de las cámaras. Esta transmisión principal de alta resolución no tendrá las zonas de privacidad extraíbles aplicadas. Este privilegio solo debe concederse a administradores o usuarios similares que puedan tener la necesidad de ver las zonas privadas de la imagen. A los operadores generales y otros usuarios de ACC que no tengan el privilegio de Ver imágenes en alta resolución siempre se les aplicarán las zonas de privacidad extraíbles. Consulte la documentación de ACC para obtener más información sobre la configuración de privilegios de grupo.

Tenga en cuenta las siguientes limitaciones al utilizar las zonas de privacidad extraíbles:

- ACC High Definition Stream Management (HDSM)[™] mostrará las transmisiones principal, secundarias o terciarias según el nivel de zoom y el tamaño del portal de visualización cuando vea el vídeo en directo o grabado. Asegúrese de eliminar el privilegio de Ver imágenes en alta resolución de los usuarios de ACC que no necesitan ver el vídeo no borroso.
- A ciertos grupos de usuarios de ACC se les puede conceder la Anulación de Privilegios de Emergencia, que se puede utilizar para ver la transmisión de vídeo principal no borrosa. Esta función registra cada uso de la anulación de emergencia, incluyendo el nombre de usuario y la hora de acceso, en los registros de eventos de ACC.
- Cuando los operadores de ACC con acceso a la transmisión principal reproduzcan el vídeo grabado en un pequeño panel de vídeo, verán la zona de privacidad borrosa. La zona borrosa desaparecerá cuando el operador privilegiado haga una pausa o recorra el vídeo en la línea de tiempo. El operador privilegiado también puede cambiar a la vista de pantalla completa y/o ampliar el vídeo para que el HDSM muestre la transmisión principal no borrosa.

Almacenamiento

En la página Storage (Almacenamiento), puede habilitar la función de almacenamiento interno de la cámara y descargar el vídeo grabado directamente desde la cámara. El almacenamiento interno solo está disponible en cámaras equipadas con una tarjeta SD o ranura para tarjetas microSD.

Importante: Los errores de la tarjeta SD pueden hacer que la cámara se reinicie continuamente. Para evitarlo, la tarjeta SD se desactivará si se detectan errores persistentes. Para obtener más información, consulte *Errores de la tarjeta SD* en la página 39.

Si está utilizando una microtarjeta CryptR en la ranura para tarjetas SD de la cámara para el cifrado de nivel 3 de FIPS, no podrá usar el almacenamiento interno en la ranura para tarjetas SD. Para cámaras con 2 ranuras para tarjetas micro SD, solo puede usar las ranuras para almacenamiento o para microtarjetas CryptR, no se pueden usar las dos opciones al mismo tiempo.

Las cámaras que incluyen un TPM integrado no admiten la tarjeta micro CryptR y solo pueden utilizar las ranuras SD para el almacenamiento integrado.

Nota: Para cámaras con 2 ranuras para tarjetas microSD, la cámara grabará vídeo en tarjetas SD en ambas ranuras. La capacidad de almacenamiento total del sistema es la capacidad de almacenamiento combinada de cada una de las dos tarjetas individuales.

Habilitar el almacenamiento interno

Para usar la función de almacenamiento interno de la cámara, primero debe insertar una tarjeta SD en la cámara. Consulte el manual de instalación de la cámara para conocer la ubicación de la ranura para tarjetas SD.

Sugerencia: La tarjeta SD grabará a partir de la resolución más alta de la cámara, sin transmisión con inclinación. En la mayoría de los casos, ésta será la transmisión principal.

Nota: Para cámaras con 2 ranuras para tarjetas microSD, la cámara grabará vídeo en tarjetas SD en ambas ranuras. La capacidad de almacenamiento total del sistema es la capacidad de almacenamiento combinada de cada una de las dos tarjetas individuales.

1. En la página Storage (Almacenamiento), seleccione la casilla de verificación **Enable Onboard Storage (Activar almacenamiento interno)**.
2. De manera predeterminada, la cámara está configurada para grabar solo en la tarjeta SD cuando no puede comunicarse con el servidor de administración de vídeo en red. Si prefiere que la cámara grabe vídeo tanto en el servidor de administración de vídeo en red como en la tarjeta SD, desactive la casilla de verificación **Record only when server connection is interrupted (Grabar solo cuando la conexión del servidor se ha interrumpido)** para desactivar la configuración.
3. Seleccione uno de los siguientes modos de grabación:
 - **Continuous (Continuo):** la cámara nunca deja de grabar en la tarjeta SD.
 - **On Motion (En movimiento):** la cámara solo graba cuando hay movimiento en la escena.
Si está configurando una cámara de análisis de vídeo Avigilon, el ajuste On Motion (En movimiento) registrará ya sea cambio de los píxeles en los eventos de movimiento de escena o de análisis en función de cómo la cámara se configura en el software de Avigilon Control Center Client.

El vídeo grabado se dividirá en archivos de no más de cinco minutos de duración o 100 MB de tamaño.
4. En la Compression and Image Rate (Compresión y velocidad de imagen) página, asegúrese de que el formato esté configurado en **H.264(H.264)** o **H.265** para maximizar la capacidad de grabación y el rendimiento de la tarjeta SD.

ONVIF Profile G

ONVIF Profile G permite que los sistemas de gestión de vídeo recuperen el vídeo del almacenamiento interno de una cámara cuando hay un espacio en el vídeo de VMS debido a una interrupción de la red o un evento similar.

- Las cámaras con versiones de firmware 4.4.0.X o posteriores tendrán ONVIF Profile G habilitado.
- Las cámaras con firmware anterior que 4.4.0.X tendrán la opción de **Habilitar ONVIF Profile G** cuando actualicen su firmware.

Nota: Habilitar ONVIF Profile G requerirá volver a formatear la tarjeta SD. Perderá todo el material grabado en la tarjeta SD. Asegúrese de descargar los videoclips necesarios antes de habilitar Profile G.

ONVIF es una marca comercial de Onvif, Inc.

Descarga de vídeo grabado de la interfaz web

En la sección Recordings (Grabaciones) se indican todos los vídeos que se han grabado en la tarjeta SD.

Si está utilizando dos tarjetas SD, tendrá que seleccionar la tarjeta SD desde la que desea descargar el vídeo. Es posible que tenga que comprobar ambas tarjetas SD para la grabación que desea descargar. La cámara puede grabar vídeo en cualquiera de las dos tarjetas SD en función de la capacidad restante de las mismas.

Si está utilizando una microtarjeta CryptR en la ranura para tarjetas SD de la cámara para el cifrado de nivel 3 de FIPS, no podrá usar el almacenamiento interno en la ranura para tarjetas SD. Para cámaras con 2 ranuras para tarjetas micro SD, solo puede usar las ranuras para almacenamiento o para microtarjetas CryptR, no se pueden usar las dos opciones al mismo tiempo.

Le recomendamos que descargue el vídeo grabado desde la interfaz web. Sin embargo, si su ancho de banda es limitado, puede elegir descargar el vídeo grabado directamente desde la tarjeta SD. Para obtener más información, consulte *Descarga de vídeo grabado desde la tarjeta SD* en la página siguiente.

Para descargar vídeo grabado de la interfaz web, lleve a cabo las siguientes opciones:

Sugerencia: Si utiliza dos tarjetas SD, seleccione la tarjeta SD de la que desea descargar la grabación.

1. En la página Storage (Almacenamiento), seleccione la casilla de verificación junto a todos los vídeos que desea descargar.
Para ayudarle a encontrar el vídeo que desea, puede filtrar los vídeos por fecha y hora. Seleccione la casilla de verificación **Filter (Filtro)** y, a continuación, seleccione el intervalo de tiempo.
2. Haga clic en **Download(Descargar)**.

Los archivos de vídeo seleccionados se descargan automáticamente a la carpeta de descargas predeterminada de su navegador. Si el navegador lo solicita, permita que se realice la descarga.

Nota: No cierre la ventana de su navegador hasta que se complete la descarga o el archivo no se descargará correctamente. Esto es importante si está descargando múltiples archivos de vídeo porque los archivos se descargan uno por uno.

Descarga de vídeo grabado desde la tarjeta SD

Si no tiene suficiente ancho de banda para descargar el vídeo grabado directamente desde la interfaz web, puede optar por descargar el vídeo grabado directamente desde la tarjeta SD.

Para descargar vídeo grabado directamente desde la tarjeta SD, realice lo siguiente:

1. En el área Settings (Ajustes), deshabilite el almacenamiento interno desactivando la casilla de verificación **Enable Onboard Storage (Activar almacenamiento interno)** y, a continuación, haga clic en **Apply (Aplicar)**.
2. Extraiga la tarjeta SD de la cámara.
3. Inserte la tarjeta SD en un lector de tarjetas.
4. Cuando aparezca el cuadro de diálogo Reproducción automática de Windows, seleccione **Abrir carpeta para ver archivos**.
5. Abra la aplicación Avigilon Camera Footage (Metraje de cámara).

La ventana Avigilon Camera Footage (Metraje de cámara) indica todos los archivos de vídeo almacenados en la tarjeta SD.

- Para descargar todos los vídeos grabados, haga clic en **Download All (Descargar todo)**.
 - Para descargar un vídeo específico, seleccione los archivos de vídeo que desea descargar y haga clic en **Download Selected (Descargar seleccionados)**.
6. Cuando se le solicite, elija una ubicación para guardar los archivos de vídeo.
Los archivos comienzan a descargarse de la tarjeta SD y se guardan en la ubicación seleccionada.
 7. Cuando esté listo, expulse la tarjeta SD.
 8. Inserte la tarjeta SD nuevamente en la cámara y seleccione **Enable Onboard Storage (Activar almacenamiento interno)** para comenzar a grabar nuevamente en la tarjeta SD.

Eliminación del vídeo grabado

A medida que la tarjeta SD se llena, la cámara comienza a sobrescribir automáticamente el vídeo grabado más antiguo. También puede elegir eliminar manualmente el vídeo para aumentar el espacio destinado a nuevas grabaciones.

En la página Storage (Almacenamiento), puede optar por eliminar el vídeo de las siguientes maneras:

- Para eliminar archivos de vídeo individuales, seleccione todos los archivos que desea eliminar de la lista Recordings (Grabaciones) y haga clic en **Delete(Eliminar)**.
- Para eliminar todos los archivos de vídeo grabados, haga clic en **Format Card (Formatear tarjeta)** para formatear la tarjeta SD.

Errores de la tarjeta SD

Los errores de la tarjeta SD pueden hacer que la cámara se reinicie continuamente y comprometer la fiabilidad de la cámara. Para evitarlo, la tarjeta SD se desactivará si se detectan errores persistentes.

Una vez que se ha desactivado una tarjeta SD, la cámara y la interfaz web le notificarán el problema:

- El vídeo de la cámara superpondrá un texto de advertencia en la imagen de vídeo: `Grabación en tarjeta SD deshabilitada. Cambie la tarjeta para volver a habilitarla.`

Nota: El mensaje de superposición de vídeo puede desactivarse en la página de la cámara **Storage (Almacenamiento)** desmarcando la casilla de verificación **Habilitar superposición de alerta de vídeo con error grave de tarjeta SD**.

- La página de la cámara **Storage (Almacenamiento)** mostrará un mensaje de advertencia cuando seleccione la página: `Se ha deshabilitado la ranura de tarjeta SD debido a errores en la tarjeta, cambie la tarjeta.`

Para volver a activar la tarjeta SD, extráigala de la ranura para tarjetas SD de la cámara y sustitúyala por una tarjeta SD que funcione. Se ejecutará una prueba de velocidad en la nueva tarjeta cuando se inserte para determinar si funcionará sin problemas.

También puede forzar la reactivación de la tarjeta SD en la interfaz web haciendo clic en **Forzar habilitación de ranura de tarjeta SD** en la página **Storage (Almacenamiento)**.

Importante: No se recomienda forzar la reactivación de la tarjeta SD a menos que esté seguro de que no hay problemas con la tarjeta. Si la tarjeta continúa fallando, puede hacer que la cámara entre en un bucle de reinicio y, después de errores persistentes continuos, la tarjeta SD se desactivará de nuevo.

Entradas y salidas digitales

En la página Digital Inputs and Outputs (Entradas y salidas digitales), puede configurar los dispositivos externos de entrada y salida que estén conectados a la cámara. Esta opción no se muestra para las cámaras que no son compatibles con entradas y salidas digitales.

1. Para configurar una entrada digital:

- a. En el área Digital Inputs (Entradas digitales), introduzca un nombre para la entrada digital en el campo **Name (Nombre)**.
- b. Seleccione el estado apropiado de la lista desplegable **Circuit State (Estado del circuito)**. Las opciones son:
 - **Normally Open (Normalmente abierto)**
 - **Normally Closed (Normalmente cerrado)**

Nota: Algunas cámaras pueden detectar el estado del circuito de las entradas digitales automáticamente y la entrada se activará cuando se detecte un cambio de estado. Para estas cámaras, la configuración Circuit State (Estado del circuito) no tendrá efecto en la función de entrada digital.

- c. La lista desplegable **Type (Tipo)** se utiliza para las cámaras que pueden tener el modo día/noche activado por un detector de luz externo. Solo verá esta opción en las cámaras que admitan esta función. Si la entrada digital se utilizará para controlar los ajustes día/noche, seleccione **Force IRCF (Forzar IRCF)** en la lista desplegable Type (Tipo).

Para la conmutación día/noche controlada por una entrada digital externa, la opción **External (Externo)** debe seleccionarse como la **Day/Night Mode (Modo día/noche)**. Para obtener más información sobre cómo configurar el modo de día/noche, consulte *Imagen y Visualización* en la página 19.

- d. Haga clic en **Apply (Aplicar)** para guardar los cambios.

Una vez que la entrada digital esté conectada a la cámara, verá el estado de conexión en el área **Circuit Current State (Estado actual del circuito)**. Normalmente, el estado es *Open (Abrir)* o *Closed (Cerrado)*.

2. Para configurar una salida digital:

- a. En el área Digital Outputs (Salidas digitales), introduzca un nombre para la salida digital en el campo **Name (Nombre)**.
- b. Seleccione el estado apropiado de la lista desplegable **Circuit State (Estado del circuito)**.
- c. Marque la casilla **IRCF to Out (IRCF a salida)** para que el filtro de corte IR de la cámara controle la salida externa.

Esta característica se usa generalmente cuando la cámara está conectada a un iluminador IR externo. Una vez habilitado, el iluminador IR se enciende cuando el filtro de corte IR de la cámara está en modo monocromo.

- d. En el campo **Duration (Duración)**, introduzca cuánto tiempo estará activa la salida digital cuando se active. Puede introducir un número entre 100 y 86 400 000 milisegundos.
- e. Haga clic en **Trigger (Desencadenar)** para activar manualmente la salida digital desde la interfaz web.
- f. Haga clic en **Apply (Aplicar)** para guardar los cambios.

Arandela

En la página Washer (Lavado), puede activar la secuencia de limpiador y limpiaparabrisas para limpiar la ventana en las cámaras bullet con protección contra explosiones H5A. La función del lavador es compatible si estas cámaras tienen el lavado opcional instalado. Consulte la siguiente tabla para conocer los modelos de cámara y lavador que admiten la función de lavador.

Modelo	Número de pieza de la cámara	Número de pieza del lavador
H5A resistente PTZ	H5A-RGDPTZ-DP36	AVWASPT0V5L5M00 / AVWASPT0V23L11M00 / AVWASPT1V23L30M00 / AVWASPT3V23L30M00
H5A protegida contra explosiones PTZ	H5EXPTZ-x0-BO30	AVGEX-WASEX2T4AT / AVGEX-WASEX2T4IN / AVGEX-WASEX2T4KC / AVGEX-WASEX2T4GOR
Cámara HD Bullet con protección contra explosiones H5A	H5EX-xx-BO1	

Para activar la secuencia de lavado:

1. Haga clic en **Washer (Lavado)** en el panel de menú de la izquierda.
Seleccione la casilla de verificación **Enable Washer (Activar lavado)**.
2. Configure la **Wiper On Delay (Retraso de activación de escobilla)** para controlar la cantidad de tiempo entre el inicio del pulverizador del lavador y el inicio de la función del limpiaparabrisas.
3. Configure el tiempo que la lavadora rociará en el campo **Washer Period (Período de lavado)**.
4. Configure el tiempo que la función del limpiaparabrisas continuará en el campo **Wiper Off Delay (Retraso de desactivación de escobilla)**.
5. Haga clic en **Apply (Aplicar)** para guardar los ajustes.

Sugerencia: Recomendamos que la secuencia de lavado esté configurada para que Wiper On Delay (Retraso de activación de escobilla) sea de al menos 4 segundos para que el lavador tenga tiempo de pulverizar la ventana. El Wiper Off Delay (Retraso de desactivación de escobilla) debe durar al menos 8 segundos más que el Washer Period (Período de lavado) para dar al limpiaparabrisas tiempo para limpiar la ventana después de que el spray se haya detenido.

Audio

Utilice la configuración de la página Audio(Audio) para ajustar la calidad de audio de la cámara.

Para codificar la transmisión de audio, puede elegir entre el codificador de sonido Opus, que produce sonido de alta calidad, o el codificador de sonido de protocolo G.711. Utilice el codificador Opus si está utilizando la versión 6.10 o posterior del software ACC (o un sistema de gestión de vídeo de terceros que admita el protocolo Opus). De lo contrario, utilice el protocolo G.711, que cuenta con un amplio soporte.

1. En la sección Audio Settings(Configuración de audio):
 - a. En el campo **Encoding(Codificación)**, especifique el codificador de audio que se va a utilizar:
 - **Opus**: códec de audio de alta calidad predeterminado.
 - **G.711**: compatible con varias plataformas.
2. En la sección Device Speaker(Altavoz de dispositivo), utilice el control deslizante **Volume(Volumen)** para ajustar el volumen del altavoz (de 0 a 100).
3. En la sección Device Microphone(Micrófono de dispositivo):
 - a. Utilice el ajuste **Line in Gain (Línea en ganancia)** para ajustar la salida del micrófono integrado en la cámara.
4. Haga clic en **Apply (Aplicar)** para guardar los cambios.

Usuarios

En la página Users(Usuarios), puede agregar nuevos usuarios, editar usuarios existentes y cambiar contraseñas.

Añadir a un usuario

1. En la página Usuarios, haga clic en **Add... (Agregar...)**.
2. En la página Add User (Agregar usuario), introduzca un nombre de usuario y una contraseña para el nuevo usuario.
3. En la lista desplegable **Security Group (Grupo de seguridad)**, seleccione los permisos de acceso disponibles para este nuevo usuario.
 - **Administrator (Administrador)**: acceso completo a todas las funciones disponibles en la interfaz web de la cámara .
 - **Operator (Operador)**: tiene acceso a los controles de Vista en directo , pero acceso limitado a las funciones de configuración. El usuario puede acceder a la páginas General, Image and Display (Imagen y Visualización), Compression and Image Rate (Compresión y velocidad de imagen), Motion Detection (Detección de movimiento), Privacy Zones (Zonas de privacidad), Digital Inputs and Outputs (Entradas y salidas digitales), Microphone (Micrófono) y Speakers (Altavoces). El nuevo usuario también puede configurar los ajustes de almacenamiento interno, pero no puede eliminar las grabaciones de vídeo ni formatear la tarjeta SD.
 - **Usuario**: tiene acceso a los controles de Live View (Imagen en vivo), pero no puede acceder a ninguna de las páginas de configuración.
4. Haga clic en **Apply (Aplicar)** para añadir al usuario.

Edición de usuarios y contraseñas

1. En la página Users(Usuarios), seleccione un usuario de la lista User Name (Security Group) (Nombre de usuario [grupo de seguridad]) y haga clic en **Modify (Modificar)**.
2. Para cambiar la contraseña del usuario, introduzca una nueva contraseña para el usuario.
3. Para cambiar el grupo de seguridad del usuario, seleccione un grupo diferente en la lista desplegable **Security Group (Grupo de seguridad)**.

Nota: No puede cambiar el grupo de seguridad de la cuenta de administrador.

4. Haga clic en **Apply (Aplicar)** para guardar los cambios.

Eliminar un usuario

Nota: No puede eliminar el usuario predeterminado Administrator (Administrador) a menos que haya otro usuario con privilegios de administrador. La cámara siempre debe tener al menos un usuario administrador configurado.

1. En la página Users(Usuarios), seleccione un usuario en la lista Nombre de usuario (grupo de seguridad).
2. Haga clic en **Remove (Suprimir)**.

Cómo conservar nombres de usuario y contraseñas después de revertir el firmware

Para añadir un nivel de seguridad y proteger la cámara contra robos, tiene la opción de conservar los nombres de usuario y las contraseñas actuales de la cámara después de una reversión de firmware.



Si ha configurado su cámara para que utilice el cifrado FIPS 140-2 (FIPS 140-2), le recomendamos que no elija conservar los nombres de usuario y las contraseñas después de una reversión de firmware. La contraseña y el nombre de usuario no se almacenan de forma compatible con FIPS 140-2 y pueden afectar a su cumplimiento con el mismo.

Normalmente, al restaurar el firmware de la cámara a los ajustes predeterminados de fábrica, la cámara vuelve a utilizar el nombre de usuario y la contraseña predeterminados. Cuando activa esta función, la cámara continuará utilizando el nombre de usuario y las contraseñas que se han configurado, de modo que la cámara no se puede conectar a servidores nuevos sin las credenciales correspondientes.

Importante: Olvidar su propio nombre de usuario o contraseña después de habilitar esta configuración anula su garantía. El método principal para restauración del nombre de usuario y la contraseña predeterminados de fábrica se desactivará.

1. En la parte inferior de la página Users(Usuarios), seleccione la casilla de verificación **Do not clear usernames or passwords on firmware revert (No borre los nombres de usuarios ni las contraseñas durante la reversión del firmware)**.
2. Después de marcar la casilla de verificación, aparecerá el siguiente mensaje emergente:

Please store your administrator password in a safe place. Password recovery is not covered by warranty and loss of password may void your warranty.(Please store your administrator password in a safe place. (Almacene la contraseña del administrador en un sitio seguro). Password recovery is not covered by warranty and loss of password may void your warranty. (La recuperación de la contraseña no está cubierta por la garantía y su pérdida puede anular la garantía.)

3. Haga clic en **OK (Aceptar)** si acepta las limitaciones de la función.

Siempre conserve una copia de su contraseña en un lugar seguro para evitar perder acceso a su cámara.

Sistema

En la página System(Sistema), puede actualizar manualmente el firmware de la cámara, reiniciar la cámara y restaurar todos los ajustes predeterminados de fábrica de la cámara.

- Para actualizar el firmware de la cámara, consulte *Actualización del firmware de la cámara* en la página siguiente.
- Haga clic en **Download(Descargar)** para descargar el informe de errores.
- Haga clic en **Reboot (Reiniciar)** para reiniciar la cámara.
- Haga clic en **Restore (Restaurar)** para revertir el firmware de la cámara a los ajustes predeterminados de fábrica.
- Haga clic en **Restablecer software** para restablecer la cámara a la configuración predeterminada de fábrica, excepto para la configuración de red.

Sugerencia: Si ha habilitado la función que conserva su nombre de usuario y contraseña después de una reversión de firmware, asegúrese de tener una copia escrita de sus nombres de usuario y contraseñas actuales. Para obtener más información, consulte *Cómo conservar nombres de usuario y contraseñas después de revertir el firmware* en la página anterior.

- (Solo para cámaras H4SL-DO y H4SL-BO) Si el objetivo de la cámara deja de funcionar según lo previsto y no puede enfocar el objetivo a través de la página Image and Display (Imagen y Visualización), es posible que tenga que reiniciar el objetivo.

Haga clic en **Reinitialize (Reinicializar)** y, después, espere mientras la lente se reinicia. Se muestra un mensaje verde en la parte inferior de la página cuando se completa el proceso.

Actualización del firmware de la cámara

Para actualizar manualmente el firmware de la cámara:

1. Descargue la última versión del archivo .bin del firmware desde el sitio web de Avigilon ([avigilon.com/support](https://www.avigilon.com/support)) y complete los siguientes pasos:
2. En la página System(Sistema), haga clic en Seleccionar archivo y busque el archivo de firmware descargado.
3. Haga clic en **Upgrade (Actualizar)**. Espere hasta que finalice la actualización de la cámara.

Registro de dispositivos

La página Device Log(Registro de dispositivos) le permite ver los registros del sistema y los registros de acceso de la cámara.

El evento de registro más reciente siempre se muestra primero.

1. En la lista desplegable **Type (Tipo)**, seleccione una de las siguientes opciones:
 - **Access Logs (Registros de acceso)** — registros de usuarios que han iniciado sesión en la interfaz web.
 - **System Logs (Registros del sistema)** — registros de las operaciones de la cámara.
 - **Registros del kernel (depuración)**: registros de mensajes de depuración.
2. En la lista desplegable **Minimum Log Level (Nivel de registro mínimo)**, seleccione el nivel mínimo de mensajes de registro que desea ver:
 - **Error(Error)** — se envía cuando la cámara detecta un error grave. Estos son los mensajes de registro mayor nivel.
 - **Warning (Advertencia)** — se envía cuando la cámara encuentra un error leve, como un nombre de usuario o una contraseña no válidos.
 - **Info (Información)** — información de estado que envía la cámara. Estos son los mensajes de registro de menor nivel.
 - **Depuración**: información de solución de problemas enviada por la cámara para ayudar en el diagnóstico de problemas.
3. En la lista desplegable **Maximum Number of Logs (Número máximo de registros)**, seleccione el número de mensajes de registro que desea ver.
4. Haga clic en **Update(Actualizar)**.

Los registros se actualizan para mostrar la información filtrada.

Deshabilitar WebUI

En la página Deshabilitar WebUI, puede desactivar la interfaz web de la cámara, incluyendo cualquier llamada a la API que no sea ONVIF. Esto desactivará cualquier acceso a la cámara que no sea a través del ACC Client o de una VMS compatible con ONVIF.

Importante: Si desactiva la interfaz web y las API no ONVIF, solo podrá conectarse a la cámara con el ACC Client o con un VMS compatible con ONVIF.

La única forma de revertir esta configuración es haciendo una reversión física del firmware en la cámara. Para obtener más información, consulte la guía de instalación de la cámara.

Para desactivar la interfaz web y las API no ONVIF:

1. Seleccione la casilla de verificación **Deshabilitar API no ONVIF**.
2. Haga clic en **Apply (Aplicar)**.
3. Lea el mensaje de advertencia que aparece y haga clic en **OK (Aceptar)** si desea continuar con esta configuración.

About (Sobre)

En la página About (Sobre), puede encontrar información sobre su cámara, como la versión del firmware, el número de serie y la conformidad con ONVIF.

Comprobación de la fuente de alimentación de una cámara

Para cámaras con múltiples opciones de fuente de alimentación, puede ser útil comprobar la página About (Sobre) para confirmar qué fuente de alimentación está conectada actualmente.

Cámara ACC™ ES

Si va a configurar una cámara H4 Edge Solution (ES), verá la opción de la aplicación ACC ES(ACC ES) en el recuadro del menú izquierdo.

Las cámaras H4 ES cuentan con un componente de servidor que ejecuta el software Avigilon Control Center Server. Esto permite que cada cámara H4 ES también actúe como su propio sitio y servidor.

Desde las páginas de la aplicación ACC ES(ACC ES), se puede configurar los puertos de transmisión por secuencias y los ajustes de archivado para el software del servidor ACC.

Comprobación del estado de la cámara ACC ES(ACC ES)

En la primera página de la aplicación ACC ES(ACC ES), se puede comprobar el estado del software Avigilon Control Center.

- **Avigilon Control Center Information (Información de Avigilon Control Center)**
 - **ACC Site Name (Nombre del sitio de ACC):** el nombre del sitio del que forma parte la cámara.
 - **ACC Server Name (Nombre del servidor de ACC):** el nombre de la cámara.
 - **ACC Server Status (Estado de ACC Server):** el estado del software ACC Server.
 - **ACC Server Version (Versión de ACC Server):** la versión del software ACC Server.

Configuración de los ajustes de administración de la cámara ACC ES

En la página Setup (Configuración), puede configurar los parámetros de administración del sistema Avigilon Control Center como lo haría en la herramienta de administración ACC.

Reinicio del software ACC

Si el software ACC Server no funciona como se esperaba, puede intentar resolver el problema reiniciando el componente del servidor.

1. En la página Setup (Configuración), haga clic en **Disable ACC ES (Desactivar ACC ES)**.
2. Haga clic en **Apply (Aplicar)**.
La cámara apaga el software ACC Server.
3. Haga clic en **Enable ACC ES (Activar ACC ES)** para reiniciar el software de servidor ACC.

Formateo de la unidad de vídeo grabado

Las cámaras ACC ES HD incluyen una unidad de estado sólido que almacena el vídeo grabado directamente en la cámara. Si alguna vez necesita eliminar toda la configuración y los datos de vídeo grabados, puede reiniciar el almacenamiento.

1. Para formatear la SSD, haga clic en **Reinitialize Storage (Reiniciar el almacenamiento)**.
2. Cuando el navegador muestre el mensaje de error siguiente, haga clic en **Aceptar**:

This will require the ACC ES application to restart and will delete all ACC ES configuration settings and data. (Esta acción requiere que la aplicación ACC ES se reinicie y eliminará todos los ajustes y datos de configuración de ACC ES). Are you sure you want to continue? (¿Está seguro de que desea continuar?)

El software ACC Server de la cámara se reinicia. La cámara continuará transmitiendo vídeo pero no grabará nada hasta que el software ACC Server haya terminado de cargarse.

Cambiar los puertos de comunicación

ACC Server se comunica con el software ACC Client a través de un intervalo de puertos UDP y TCP. Solo es necesario cambiar los intervalos de puertos si el software ACC Client está intentando acceder a dos o más instancias del ACC Server que están detrás del mismo dispositivo NAT (por ejemplo, el enrutador) o si hay un conflicto de puertos.

1. En el área Service Ports (Puertos de servicio) y RTP Ports (Puertos RTP), puede cambiar el Base Port (Puerto de base) que se utiliza para acceder a ACC Server.
2. Haga clic en **Apply (Aplicar)**.
3. Cuando el navegador muestre el mensaje de error siguiente, haga clic en **Aceptar**:

The new service base port or login limits will only take effect once Control Center Server is restarted. (El nuevo puerto de base de servicios o los nuevos límites de inicio de sesión solo tendrán efecto al reiniciar el Control Center Server). Restart Control Center Server now? (¿Desea reiniciar el Control Center Server ahora?)

El software ACC Server de la cámara se reinicia. La cámara continuará transmitiendo vídeo pero no grabará nada hasta que el software ACC Server haya terminado de cargarse.

Anulación del límite de inicio de sesión

De manera predeterminada, solo 2 usuarios pueden iniciar sesión en el sitio al mismo tiempo. Si necesita un acceso adicional para usuarios que no vayan a supervisar el vídeo, puede anular el límite de inicios de sesión recomendado.

1. En la zona Login Limit (Límite de inicios de sesión), seleccione la casilla de verificación **Override ACC Client Login Limit (Anular el límite de inicios de sesión de ACC Client)**.
2. En el campo **Login Limit: (Límite de inicios de sesión)**, introduzca cuántos usuarios quiere que puedan iniciar sesión en el sitio de la cámara simultáneamente.
3. Haga clic en **Apply (Aplicar)**.

Se guarda la nueva configuración. Más de 2 usuarios ahora pueden iniciar sesión en el sitio de la cámara.

Nota: Tenga en cuenta que si más de 2 usuarios inician la sesión en el sitio simultáneamente, esto puede reducir el funcionamiento de la cámara, dependiendo de los ajustes de la cámara.

Habilitar Storage Management (Gestión de almacenamiento)

Se debe activar Storage Management (Gestión de almacenamiento) para poder archivar vídeos en el software ACC Client. La página Storage Management(Gestión del almacenamiento) le permite activar la función de archivado de vídeo y configurar la ubicación de red donde se guardarán los vídeos archivados.

1. Marque la casilla de verificación **Enable Storage Management(Activar gestión del almacenamiento)**.
2. En la lista desplegable **Protocolo de red**, seleccione una de las siguientes opciones:
 - **CIFS(CIFS)**: sistema de archivos de internet común. Por lo general, la ruta de red tiene este formato: //<nombre de host o IP> / <ruta>
 - **NFS(NFS)**: sistema de archivos de red. Por lo general, la ruta de red tiene este formato: <nombre de host o IP> : <ruta>
3. En el campo **Ruta de red**, introduzca la ruta a la ubicación de archivo de vídeo preferida.
4. Si la ubicación de la red requiere autenticación, marque la casilla de verificación **Authentication (Autenticación)** y, a continuación, introduzca las credenciales en los campos Username (Nombre de usuario) y Password(Contraseña).
5. Haga clic en **Apply (Aplicar)**.

Luego configure Programar archivado en el software ACC Client para permitir que el sistema archive automáticamente los vídeos grabados en la ubicación de red seleccionada. Para obtener más información, consulte la *Guía del usuario de Avigilon Control Center Client*.

Revisión de registros del software ACC

La página Logs (Registros) muestra los registros del sitio para los eventos del sistema Avigilon Control Center.

El evento de registro más reciente siempre se muestra primero.

1. En la lista desplegable **Type (Tipo)**, seleccione una de las siguientes opciones:
 - **Daemon Logs (Registros del daemon)** — registros de las operaciones de ACC Server. Esto incluye iniciar sesión en el sitio, crear eventos, etc.
 - **App Logs (Registros de aplicaciones)** — registros de las operaciones de la aplicación ACC ES dentro de la interfaz web.
2. En la lista desplegable **Minimum Log Level (Nivel de registro mínimo)**, seleccione una de las siguientes opciones:
 - **Error(Error)** — se envía cuando el sistema detecta un error grave. Estos son los mensajes de registro mayor nivel.
 - **Warning (Advertencia)** — se envía cuando el sistema detecta un error leve, como un nombre de usuario o contraseña no válidos. Se trata de la opción seleccionada de forma

predeterminada.

- **Info (Información)** — información de estado que envía el sistema. Estos son los mensajes de registro de menor nivel.

3. En la lista desplegable **Maximum Number of Logs (Número máximo de registros)**, seleccione el número de mensajes de registro que desea ver.

4. Haga clic en **Update(Actualizar)**.

Los registros se actualizan para mostrar la información filtrada.