

AXIS Camera Station Pro

Acerca de

AXIS Camera Station Pro es una solución de gestión de vídeo que ofrece supervisión, grabación y gestión integrales de transmisiones de vídeo de cámaras de red Axis. Ofrece funciones avanzadas para el control de acceso, gestión de múltiples sitios e integración de sistemas.

Es compatible con todas las versiones de AXIS OS que reciben soporte en las fases activas de Soporte a largo plazo (LTS) y Soporte específico del producto (PSS)*. Para obtener más información, consulte las notas de la versión de AXIS Camera Station Pro o el *AXIS OS Portal (Portal de AXIS OS)*. Para comprobar qué productos son compatibles con AXIS Camera Station Pro, consulte *Compatible products (Productos compatibles)*.

*Nuestro objetivo es fomentar la compatibilidad con versiones anteriores del AXIS OS siempre que sea comercialmente viable.

Opciones de acceso

AXIS Camera Station Pro servidor – gestiona toda la comunicación con las cámaras, los codificadores de vídeo y los dispositivos auxiliares de su sistema. Para obtener información sobre los requisitos del sistema y la planificación de capacidad, consulte las *Hardware guidelines (Pautas de hardware)* en la *Guía de instalación y migración de AXIS Camera Station Pro*.

AXIS Camera Station Pro cliente – Facilita el acceso a grabaciones, vídeos en directo, registros y configuración. Puede instalarlo en cualquier ordenador, habilitando la visualización remota y el control desde cualquier parte de Internet o la red corporativa.

Cliente web de AXIS Camera Station – proporciona acceso a grabaciones de AXIS Camera Station Pro y vídeo en directo en el navegador web. Consulte el *manual del usuario de cliente web de AXIS Camera Station* para obtener más información.

AXIS Camera Station Pro app para dispositivos móviles – facilita acceso a grabaciones y vídeos en directo en varios sistemas. Puede instalar la aplicación en dispositivos Android e iOS y habilitar la visualización remota desde otras ubicaciones.

Opciones de descarga

Encuentre la descarga o actualización adecuada para sus necesidades. Puede probar AXIS Camera Station Pro de forma gratuita, descargar la aplicación móvil o actualizar una instalación existente. Vaya a la *AXIS Camera Station Pro download page (página de descargas)* para comenzar.

- **Prueba gratuita de 90 días con todas las funciones:** Pruebe AXIS Camera Station Pro de forma gratuita durante 90 días. No requiere licencia para comenzar.
- **Actualice solo su cliente – Sin conexión:** Actualiza la parte del cliente de AXIS Camera Station Pro, que es la parte de la aplicación con la que interactúa directamente. Utilice esta opción si solo necesita actualizar el cliente y no el servidor.
- **Actualice su cliente y servidor – Sin conexión:** Un paquete de actualización comprimido tanto para el servidor como para el cliente. Tras la descarga, extraiga el archivo .ZIP para acceder a los archivos .msi y .cab, y luego ejecute el archivo .msi para iniciar la actualización.
- **Actualice su cliente y servidor – En línea:** Descarga, extrae e instala la actualización automáticamente. Ejecute el archivo .exe y siga los pasos indicados. Su ordenador debe permanecer conectado a Internet durante toda la instalación.
- **Mobile app for iOS (Aplicación móvil para iOS):** la aplicación móvil AXIS Camera Station Pro para iPhones e iPads. Descargas desde la App Store.
- **Aplicación móvil para Android:** La aplicación móvil AXIS Camera Station Pro para teléfonos y tabletas Android. Descargas desde Google Play.

Tutoriales en vídeo

Para obtener ejemplos más detallados sobre cómo utilizar el sistema, vaya a *Videos tutoriales de AXIS Camera Station Pro*.

Características del sistema

Para obtener más información sobre las características del sistema, vaya a la *guía de características de AXIS Camera Station Pro*.

Novedades

Para obtener más información acerca de las nuevas características de cada versión de AXIS Camera Station Pro, vaya a *Novedades de AXIS Camera Station Pro*.

Enlaces útiles para un administrador

A continuación se abordan algunos temas que podrían ser de su interés:

- *Conectar a un servidor, on page 9*
- *Configuración de dispositivos, on page 46*
- *Configurar almacenamiento, on page 75*
- *Configurar grabaciones y eventos, on page 80*
- *Configurar servicios conectados, on page 122*
- *Configurar servidor, on page 126*
- *Configurar la seguridad, on page 137*

Más manuales

- *Cliente web de AXIS Camera Station*
- *Guía de AXIS Camera Station Pro Integrator*
- *Aplicación móvil AXIS Camera Station*
- *Videos tutoriales de AXIS Camera Station Pro:*
- *Guía de solución de problemas de AXIS Camera Station Pro*
- *Guía de seguridad del sistema de AXIS Camera Station Pro*

Enlaces útiles para un operador

A continuación se abordan algunos temas que podrían ser de su interés:

- *AXIS Camera Station Pro guía de inicio para operadores*
- *Conectar a un servidor, on page 9*
- *Configurar cliente, on page 117*
- *Vista en vivo, on page 14*
- *Reproducción de grabaciones, on page 25*
- *Exportar grabaciones, on page 27*
- *Hoja de referencia de AXIS Camera Station Pro - revisión y exportación*

Inicio rápido

Este tutorial le guía por los pasos para que su sistema esté listo y en funcionamiento.

Antes de empezar:

- configurar la red en función de la instalación. Vea *Configuración de red*.
- Si es necesario, configure los puertos del servidor. Vea *Configuración del puerto del servidor*.
- Tenga en cuenta los aspectos de seguridad. Vea *Consideraciones de seguridad*.

Para los administradores:

1. *Inicie el sistema de gestión de vídeo*
2. *Agregar dispositivos*
3. *Configurar el método de grabación, on page 6*

Para los operadores:

1. *Ver vídeo en directo, on page 7*
2. *Visualización de grabaciones, on page 7*
3. *Exportar grabaciones, on page 7*
4. *Reproducir y verificar las grabaciones en AXIS File Player, on page 7*

Inicie el sistema de gestión de vídeo

Haga doble clic en el icono de cliente de AXIS Camera Station Pro para iniciar el cliente. Al iniciar al cliente por primera vez, intentará iniciar sesión en el servidor de AXIS Camera Station Pro instalado en el mismo equipo que el cliente.

Una vez que el cliente se abre, le permite activar la licencia del sistema. Haga clic en **Activar la licencia ahora** para ir a la página **Manage licences (Administrar licencias)**, donde puede registrar el servidor con una organización para iniciar el proceso de licencia. Consulte *Gestionar servicios conectados, on page 122* y *Gestionar licencias, on page 135* para obtener más información. Debe registrar y conectar el sistema a una organización para acceder a servicios conectados, como el cliente web de VMS, la supervisión del estado del sistema y las licencias en línea.

Puede conectarse a múltiples servidores de AXIS Camera Station Pro de varias maneras. Vea *Conectar a un servidor*.

Agregar dispositivos

La página **Add devices (Agregar dispositivos)** se abre la primera vez que inicia AXIS Camera Station Pro. AXIS Camera Station Pro busca dispositivos conectados en la red y muestra una lista de los dispositivos encontrados. Vea *Agregar dispositivos*.

1. Seleccione las cámaras que desea agregar de la lista. Si no puede encontrar la cámara, haga clic en **Manual search (Búsqueda manual)**.
2. Haga clic en **Añadir**.
3. Seleccione **Configuración rápida** o **Configuración del Espacio de diseño**. Haga clic en **Next (Siguiente)**. Vea *Importar proyectos del espacio de diseño, on page 49*.
4. Utilice los ajustes predeterminados y asegúrese de que el método de grabación está establecido en **None (Ninguno)**. Haga clic en **Instalar**.

Configurar el método de grabación

1. Vaya a **Configuración > Grabaciones y eventos > Método de grabación**.
2. Seleccione una cámara.

3. Active Motion detection (Detección de movimiento) o Continuous (Continuo) o ambos.
4. Haga clic en Aplicar.

Ver vídeo en directo

1. Abra una pestaña Live view (Visualización en directo).
2. Seleccione una cámara para ver el vídeo en directo.



Consulte *Vista en vivo*, on page 14 para obtener más información.

Visualización de grabaciones

1. Abra una pestaña Recordings (Grabaciones).
2. Seleccione la cámara desde la que desea ver las grabaciones.


Consulte *Grabaciones*, on page 25 para obtener más información.

Exportar grabaciones

1. Abra una pestaña Recordings (Grabaciones).
2. Seleccione la cámara desde la que desea exportar grabaciones.
3. Haga clic en  para mostrar los marcadores de selección.
4. Arrastre los marcadores para incluir las grabaciones que desea exportar.
5. Haga clic en  para abrir la pestaña Export (Exportar).
6. Haga clic en Export... (Exportar...).

Consulte *Exportar grabaciones*, on page 27 para obtener más información.

Reproducir y verificar las grabaciones en AXIS File Player

1. Vaya a la carpeta con las grabaciones exportadas.
2. Haga doble clic en la aplicación AXIS File Player.
3. Haga clic en  para mostrar las notas de la grabación.
4. Para verificar la firma digital:
 - 4.1. Vaya a **Herramientas > Verificar firma digital**.
 - 4.2. Seleccione **Validate with password (Validar con contraseña)** e introduzca la contraseña.
 - 4.3. Haga clic en **Verify (Verificar)**. Se muestra la página de resultados de verificación.

Nota

- La firma digital no es la misma que la de vídeo firmado. El vídeo firmado le permite rastrear el vídeo en la cámara de la que provenía, con lo que permite verificar que la grabación no se ha manipulado. Consulte *Vídeo firmado* y el manual de usuario de la cámara para obtener más información.
- Si los archivos guardados no tienen ninguna conexión con una base de datos de AXIS Camera Station (archivos no indexados), será preciso convertirlos para poder reproducirlos en AXIS File Player. Contacte con el equipo de asistencia técnica de Axis si necesita ayuda para convertir sus archivos.

Configuración de red

Configure los ajustes del proxy o cortafuegos antes de utilizar AXIS Camera Station Pro si el cliente de AXIS Camera Station Pro, el servidor de AXIS Camera Station Pro y los dispositivos de red conectados están en redes diferentes.

Configuración proxy del cliente

Si un servidor proxy se encuentra entre el cliente y el servidor, deberá configurar los ajustes del proxy en Windows en el ordenador cliente. Póngase en contacto con el soporte técnico de Axis para obtener más información.

Ajustes de proxy del servidor

Si el servidor proxy se encuentra entre el dispositivo de red y el servidor, deberá configurar los ajustes del proxy en Windows en el servidor. Póngase en contacto con el soporte técnico de Axis para obtener más información.

NAT y Firewall

Cuando un NAT, cortafuegos o similar separa el cliente y el servidor, configure el NAT o cortafuegos para asegurarse de que el HTTP port (Puerto HTTP), el puerto TCP y el puerto de transmisión especificados en el Control de servicio de AXIS Camera Station Pro puedan cruzar el cortafuegos o el NAT. Póngase en contacto con el administrador de la red para obtener instrucciones sobre cómo configurar el NAT o el cortafuegos.

Consulte *Lista de puertos para AXIS Camera Station Pro*, on page 214 y *Configurar el cortafuegos para permitir el acceso a AXIS Secure Remote Access* en la guía de solución de problemas de *AXIS Camera Station Pro* para obtener más información.

Configuración del puerto del servidor

El servidor de AXIS Camera Station Pro usa puertos, 29202 (TCP), 29204 (comunicación móvil) y 29205 (transmisión móvil) para la comunicación entre el servidor y el cliente. Puede cambiar los puertos en Control del Servicio de AXIS Camera Station Pro, si es necesario.

Nota

Cambie los puertos solamente si pretende utilizar AXIS Camera Station sin Axis Secure Remote Access v2 o cualquiera de nuestros otros servicios en la nube.

Para obtener más información, consulte *General* o *FAQ (Preguntas frecuentes)*.

Consideraciones de seguridad

Para evitar el acceso no autorizado a las cámaras y las grabaciones, se debe tener en cuenta lo siguiente:

- Utilice contraseñas seguras para todos los dispositivos de red (cámaras, codificadores de vídeo y dispositivos auxiliares).
- Instalar el servidor de AXIS Camera Station Pro, las cámaras, los codificadores de vídeo y los dispositivos auxiliares en una red segura independiente de la red de trabajo. Puede instalar el cliente de AXIS Camera Station Pro en un equipo de otra red, por ejemplo, una red con acceso a Internet.
- Asegúrese de que todos los usuarios tienen contraseñas seguras. Windows® Active Directory proporciona un alto nivel de seguridad.

Conectar a un servidor

Usando el cliente de AXIS Camera Station Pro puede conectar con varios servidores o con un único servidor instalado en el equipo local o en otra parte de la red. Puede conectarse a los servidores de AXIS Camera Station Pro de varias maneras:

Últimos servidores usados – Conéctese a los servidores usados en la sesión anterior.

Este equipo – Conéctese al servidor instalado en el mismo equipo que el cliente.

Servidor remoto – Vea *Conectar a un servidor remoto*, on page 9.

Axis Secure Remote Access – Vea *Iniciar sesión en AXIS Secure Remote Access*, on page 10.

Axis Secure Remote Access v2 – Vea *Iniciar sesión en AXIS Secure Remote Access v2*, on page 10.


Nota

Al intentar conectarse a un servidor por primera vez, el cliente comprueba el ID del certificado del servidor. Para asegurarse de que se está conectando al servidor correcto, coteje manualmente el ID del certificado con el que se muestra en AXIS Camera Station Pro Service Control. Vea *General*, on page 214.


Para permitir la conexión entre el cliente y el servidor, ambos deben tener la misma versión. Ante una incompatibilidad de las versiones al conectarse a un sistema local o a uno con asignación de puertos, lo que podría ocasionar problemas de compatibilidad, el cliente puede descargar la versión correcta para que coincida con el servidor. A continuación, el cliente cambia a la versión correspondiente.

En los sistemas conectados a través de un acceso remoto seguro, es preciso actualizar los clientes de forma manual. Para que un cliente pueda conectarse a varios servidores, cada servidor debe tener la misma versión. De forma predeterminada, el acceso directo del cliente utiliza la última versión.

Recomendamos que utilice **Kerberos** para autenticar a usuarios clientes de AXIS Camera Station Pro, consulte *Autenticar mediante Kerberos en la guía de seguridad del sistema de AXIS Camera Station Pro* para obtener más información.

Lista de servidores	Para conectarse a servidores de una lista de servidores, seleccione uno del menú desplegable de la Lista de servidores . Haga clic en  para crear o editar las listas de servidores. Vea <i>Listas de servidores</i> .
Importar la lista de servidores	Para importar un archivo de lista de servidores exportado desde AXIS Camera Station Pro, haga clic en Import server list (Importar lista de servidores) y examine hasta un archivo .msl. Vea <i>Listas de servidores</i> .
Eliminar contraseñas guardadas	Para eliminar los nombres de usuario y las contraseñas guardados de todos los servidores conectados, haga clic en Delete saved passwords (Eliminar contraseñas guardadas) .

Conectar a un servidor remoto

1. Seleccione **Servidor remoto**.
2. Seleccione un servidor de la lista desplegable **Remote server (Servidor remoto)** o introduzca la dirección IP o DNS. Si el servidor no aparece en la lista, haga clic en  para recargar todos los servidores remotos disponibles. Si el servidor está configurado para aceptar clientes en un puerto diferente del número de puerto predeterminado 29202, introduzca la dirección IP seguida del número de puerto, por ejemplo, 192.168.0.5:46001.
3. Puede hacer lo siguiente:

- Seleccione **Log in as current user (Iniciar sesión como usuario actual)** para iniciar sesión como el usuario actual de Windows®.
- Desmarque **Log in as current user (Iniciar sesión como usuario actual)** y haga clic en **Log in (Iniciar sesión)**. Seleccione **Other user (Otro usuario)** y facilite otro nombre de usuario y contraseña para iniciar sesión con credenciales diferentes.

Iniciar sesión en AXIS Secure Remote Access v2

1. Haga clic en el enlace **Iniciar sesión en AXIS Secure Remote Access v2**.
2. Introduzca las credenciales de la cuenta de My Axis.
3. Haga **Sign in (Iniciar sesión)**.
4. Seleccione una organización y haga clic en **OK (Aceptar)**.
5. Seleccione el servidor en el que desea iniciar sesión.
6. Inicie sesión con las credenciales del servidor.

Nota

Las credenciales del servidor son distintas de las credenciales de la cuenta de My Axis.

La barra de estado situada en la parte inferior del cliente AXIS Camera Station Pro muestra el uso de Axis Secure Remote Access v2. **Data used this month (Datos utilizados este mes)** muestra la cantidad total de datos retransmitidos que utiliza la organización durante el mes. El contador se restablece el primer día de cada mes a medianoche.

Consulte *Axis Secure Remote Access v2, on page 124* para obtener información sobre cómo habilitar Axis Secure Remote Access v2.

Axis Secure Remote Access v2 en dispositivos móviles

Para iniciar sesión en el servidor con Axis Secure Remote Access v2 en un dispositivo móvil (iOS y Android):

1. Con el dispositivo móvil, vaya a axis.com/products/axis-camera-station/overview y descargue la aplicación móvil de AXIS Camera Station.
2. Instale y abra la aplicación móvil.
3. Inicie sesión en Axis Secure Remote Access v2 con las credenciales de su cuenta My Axis.
4. Seleccione el servidor en el que desea iniciar sesión.
5. Inicie sesión con las credenciales del servidor.

Nota

- Las credenciales del servidor son distintas de las credenciales de la cuenta de My Axis.
- Para poder iniciar sesión con su cuenta de My Axis, tienen que invitarle a unirse a la organización como usuario.

La aplicación móvil muestra la cantidad total de datos retransmitidos que utiliza la organización durante el mes. Para obtener más información, lea el *manual del usuario de la aplicación móvil de AXIS Camera Station*.

Iniciar sesión en AXIS Secure Remote Access

Importante

Para mejorar la seguridad y la funcionalidad, estamos actualizando Axis Secure Remote Access (v1) a Axis Secure Remote Access v2. Suspendemos la versión actual el 1 de diciembre de 2025, por lo que le recomendamos firmemente actualizar a Axis Secure Remote Access v2 antes de esa fecha.

¿Qué supone esto para su sistema AXIS Camera Station Pro?

- Después del 1 de diciembre de 2025, ya no podrá acceder de forma remota a su sistema utilizando **Axis Secure Remote Access (v1)**.
- Para utilizar **Axis Secure Remote Access v2**, debe actualizar a la versión 6.8 de **AXIS Camera Station Pro**. Esta actualización es actualmente gratuita para todos los usuarios de **AXIS Camera Station 5** hasta el 1 de marzo de 2026.

Nota

- Al intentar conectarse a un servidor mediante **Axis Secure Remote Access**, el servidor no puede actualizar el cliente automáticamente.
 - Si el servidor proxy se encuentra entre el dispositivo de red y el servidor de **AXIS Camera Station Pro**, debe configurar los ajustes de proxy en **Windows** en el servidor de **AXIS Camera Station Pro** para acceder al servidor mediante **AXIS Secure Remote Access**.
1. Haga clic en el enlace **Iniciar sesión en AXIS Secure Remote Access**.
 2. Introduzca las credenciales de la cuenta de **My Axis**. Vea *Axis Secure Remote Access*.
 3. Haga **Sign in (Iniciar sesión)**.
 4. Haga clic en **Grant (Autorizar)**.














Configuración proxy del cliente

Si un servidor proxy se encuentra entre el cliente de **AXIS Camera Station Pro** y el servidor de **AXIS Camera Station Pro**, deberá configurar los ajustes del proxy en **Windows** en el ordenador cliente. Póngase en contacto con el soporte técnico de **Axis** para obtener más información.


AXIS Camera Station Pro cliente

La página Add devices (Agregar dispositivos) en la pestaña Configuration (Configuración) se abre cuando utiliza AXIS Camera Station Pro por primera vez. Vea *Agregar dispositivos*.

Pestañas




 Vista en vivo	Consulte el vídeo procedente de las cámaras conectadas en directo. Vea <i>Vista en vivo</i> .
 Grabaciones	Buscar, reproducir y exportar grabaciones. Vea <i>Grabaciones</i> .
 Búsqueda inteligente 1	Localice eventos importantes en el vídeo grabado mediante la búsqueda en movimiento. Vea <i>Búsqueda inteligente 1</i> .
 Búsqueda de datos	Busque datos procedentes de una fuente o sistema externo y realice un seguimiento de lo que ocurrió en el momento de cada evento. Vea <i>Búsqueda de datos, on page 43</i> .
 Configuración	administración y mantenimiento de dispositivos conectados, además de ajustes para el cliente y los servidores. Vea <i>Configuración</i> .
 Teclas de acceso rápido	una lista de teclas de acceso rápido para acciones. Vea <i>Teclas de acceso rápido</i> .
 Registros	Registros de alarmas, eventos y auditoría. Vea <i>Registros</i> .
 Gestión de acceso	Configure y gestione los titulares de tarjeta, grupos, puertas, zonas y reglas de acceso del sistema. Vea <i>Gestión de acceso, on page 183</i> .
 Búsqueda inteligente 2	Utilice filtros avanzados para encontrar vehículos y personas en función de sus características. Vea <i>Búsqueda inteligente 2, on page 37</i> .
 Supervisión del estado del sistema	Supervisar los datos de estado de uno o varios sistemas AXIS Camera Station Pro. Vea <i>Supervisión del estado del sistema ^{BETA}, on page 195</i> .
 Alertas de visualización en directo	ir automáticamente a la pestaña de alertas de visualización en directo de la cámara o ver cuando el activador de la acción de visualización en directo se activa. Vea <i>Crear acciones de visualización en directo</i> .
 Alertas de grabación	En la pestaña de Alarms (Alarmas) o Logs (Registros), seleccione una alarma y haga clic en  Go to recordings (Ir a grabaciones) para abrir la pestaña de alertas de grabaciones. Vea <i>Alarmas</i> y <i>Registros</i> .

Menú principal

	Abra el menú principal.
Servidores	Conéctese a un nuevo servidor de AXIS Camera Station Pro y vea las listas de servidores y el estado

	de conexión de todos los servidores. Vea <i>Configurar servidor</i> .
Acciones	Inicie o detenga manualmente una grabación y cambie el estado de los puertos de E/S. Vea <i>Grabar manualmente</i> y <i>Supervisar puertos de E/S</i> .
Ayuda	Abra las opciones relacionadas con la ayuda. Vaya a Help (Ayuda) > About (Acerca de) para ver la versión del cliente de AXIS Camera Station Pro que está utilizando.
Cerrar sesión	Desconecte del servidor y cierre sesión en el cliente de AXIS Camera Station Pro.
Salir	Salir y cerrar el cliente de AXIS Camera Station Pro.

Barra de título

 o F1	Abra la ayuda.
	Entre en el modo de pantalla completa.
 o ESC	Salga del modo de pantalla completa.

Barra de estado

La barra de estado puede incluir la siguiente información:

- un icono de advertencia cuando no exista una coincidencia entre la hora del cliente y del servidor. Asegúrese siempre de que la hora del cliente esté sincronizada con la hora del servidor para evitar problemas en la línea temporal.
- El estado de conexión del servidor muestra el número de servidores conectados. Vea *Estado de conexión*.
- El estado de licencia muestra el número de dispositivos sin licencias. Vea .
- El uso del acceso remoto seguro muestra cuántos datos quedan o cuál es el excedente que se ha utilizado este mes para la cantidad incluida en su nivel de servicio. Vea *Axis Secure Remote Access*.
- **AXIS Camera Station Pro** la actualización disponible aparece cuando hay una versión nueva si ha iniciado sesión como administrador. Vea *Actualizar AXIS Camera Station Pro, on page 129*.

Alarmas y tareas

Las pestañas Alarms (Alarmas) y Tasks (Tareas) muestran eventos y alarmas del sistema activadas. Vea *Alarmas y Tareas*.

Vista en vivo

La visualización en directo muestra las vistas, las cámaras y los vídeos en directo de las cámaras conectadas, así como todas las vistas y cámaras de los servidores conectados agrupadas por el nombre del servidor al conectarse a varios servidores AXIS Camera Station Pro.

Las vistas permiten acceder a todas las cámaras y dispositivos agregados a AXIS Camera Station Pro. Una vista puede incluir una o varias cámaras, una secuencia de elementos, un mapa o una página web. La visualización en directo actualiza las vistas automáticamente al agregar o eliminar dispositivos del sistema.

Gracias a la integración de AXIS Audio Manager Pro, también podrá configurar y añadir zonas de audio con interfaces de megafonía en la visualización en directo. Para obtener más información, consulte *Usar interfaces de megafonía en vistas divididas*, on page 21

Todos los usuarios pueden acceder a las vistas. Para obtener información sobre los derechos de acceso de usuarios, vea *Permisos de usuario*, on page 137.

Para obtener ayuda sobre cómo configurar la visualización en directo, consulte *Ajustes del cliente*.

Múltiples monitores

Para abrir una vista en otra pantalla:

1. Abra una pestaña Live view (Visualización en directo).
2. Seleccione una o más cámaras, vistas o secuencias.
3. Arrástrelos y colóquelos en la otra pantalla.





Para abrir una vista en un monitor conectado a un decodificador de vídeo de Axis:

1. Abra una pestaña Live view (Visualización en directo).
2. Seleccione una o más cámaras, vistas o secuencias.
3. Haga clic con el botón derecho en sus cámaras, vistas o secuencias y seleccione **Show on AXIS T8705 (Mostrar en AXIS T8705)** o **Show on AXIS D1110 (Mostrar en AXIS D1110)**, dependiendo del decodificador de vídeo que esté usando.

Nota

- AXIS T8705 solo admite cámaras Axis.
- AXIS D1110 admite hasta 9 secuencias en una vista dividida.

Gestionar vistas en la visualización en directo

	Agregue una nueva vista dividida, una secuencia, una vista de cámara, un mapa, una página web o una carpeta.
	Edite una vista o un nombre de cámara. Para obtener información sobre cómo editar los ajustes de la cámara, consulte <i>Editar ajustes de la cámara</i>
	Elimine una vista. Necesita permisos para editar la vista y todas las vistas secundarias para eliminarlas. Para obtener información sobre cómo eliminar cámaras de AXIS Camera Station Pro, consulte <i>Cámaras</i> , on page 53.
	Como administrador, puede bloquear la vista e impedir que los operadores o vistas se muevan o editen la vista.

Gestión de imagen en la visualización en directo

Navegar	Para ir a la vista de cámara, haga clic en una imagen en una vista dividida y seleccione Navigate (Navegar) .
Tomar instantánea	<p>Para tomar una instantánea, haga clic con el botón derecho en una imagen y seleccione Take snapshot (Tomar instantánea). El sistema guarda la instantánea en la carpeta de instantáneas que se especifica en Configuration (Configuración) > Client (Cliente) > Settings (Ajustes).</p> <p>Nota</p> <p>Axis Camera Station Pro normalmente utiliza el flujo de vídeo cuando se toman instantáneas, lo que significa que se obtiene una instantánea con la misma resolución que el flujo de vídeo. Sin embargo, en el caso de cámaras panorámicas y de ojo de pez, que requieren puntos de unión o corrección esférica, se toma la instantánea en el lado del cliente, directamente desde la pantalla. Este método puede dar como resultado imágenes de menor resolución, especialmente cuando se toman instantáneas en vistas con varias cámaras, en las que cada imagen aparece más pequeña en la pantalla.</p>
Añadir instantánea para exportar	Para añadir una instantánea a la lista de exportaciones de la pestaña Export (Exportar), haga clic con el botón derecho en una imagen y seleccione Add snapshot to Export (Añadir instantánea para exportar) .
Mostrar en	Para abrir una vista en otra pantalla, haga clic con el botón derecho en la imagen y seleccione Show on (Mostrar en) .
Emplee PTZ mecánico	Disponible para cámaras PTZ y cámaras con PTZ digital habilitado en la interfaz web de la cámara. Para utilizar PTZ mecánico, haga clic con el botón derecho en la imagen y seleccione Usar PTZ mecánico . Utilice el ratón para ampliar y para desplazarse horizontal y verticalmente
Zoom	utilice la rueda del ratón para ampliar y reducir la imagen. También puede pulsar CTRL + (+) para ampliar y CTRL + (-) para reducir.
Zoom de área	Para ampliar un área de la imagen, dibuje un rectángulo en el área que desee ampliar. Para reducir, utilice la rueda del ratón. Para ampliar un área situada cerca del centro de la imagen, utilice el botón derecho del ratón y arrastre para dibujar un rectángulo.
Movimiento vertical y horizontal	Haga clic en la imagen donde desee apuntar la cámara. Para aplicar un movimiento vertical y horizontal continuo en la imagen de la vista en vivo, sitúe el cursor en el centro de la imagen para mostrar la flecha de navegación. A continuación, mantenga

	pulsado para obtener una panorámica en la dirección de la flecha de navegación. Para aplicar un movimiento vertical y horizontal a una velocidad más alta, mantenga pulsado para alargar la flecha de navegación.
Ajustar enfoque	Para ajustar el enfoque de la cámara, haga clic con el botón derecho en la imagen y seleccione Set focus (Ajustar el enfoque) . Haga clic en EA para enfocar automáticamente la cámara. Para ajustar el enfoque manualmente, seleccione las barras en los lados Cercano y Alejado . Utilice Cercano para enfocar objetos situados cerca de la cámara. Utilice Alejado para enfocar objetos que se encuentran lejos.
Zona de recuerdo de enfoque	Para agregar o eliminar la zona de recuerdo de enfoque, haga clic con el botón derecho en la imagen y seleccione Focus recall zone (Zona de recuerdo de enfoque) .
Activar/Desactivar autotracking	Para activar o desactivar el autotracking de una cámara PTZ Axis con Autotracking PTZ de AXIS configurado, haga clic con el botón derecho en la imagen y seleccione Autotracking on/off (Autotracking activado/desactivado) .
Posiciones predefinidas	Para crear una posición predefinida, haga clic con el botón derecho en la imagen, seleccione Presets (Posiciones predefinidas) y, a continuación, seleccione una posición predefinida. Para crear posiciones predefinidas, vea <i>Posiciones predefinidas de PTZ</i> .
Agregar posición predefinida	Para agregar una posición predefinida, arrastre la vista de imagen hasta la posición deseada, haga clic con el botón derecho y seleccione Presets > Add preset (Posiciones predefinidas > Agregar posición predefinida) .
Movimiento PTZ absoluto	Disponible para dispositivos ONVIF compatibles con el posicionamiento PTZ absoluto. Utilice esta función para mover la cámara a coordenadas precisas y alcanzar un posicionamiento repetible. Para utilizar el movimiento PTZ absoluto, haga clic con el botón derecho del ratón en la visualización en directo de la cámara PTZ y seleccione Absolute PTZ Move (Movimiento PTZ absoluto) . Seleccione un sistema de coordenadas: Generic (Genérico) para coordenadas estándar o Spherical (Esférico) para coordenadas basadas en grados. Introduzca los valores de posición del movimiento horizontal/vertical y zoom, establezca la velocidad de movimiento y haga clic en OK o Send (Enviar) .
Perfil de flujo	Para establecer el perfil de flujo, haga clic con el botón derecho en una imagen y seleccione Stream profile (Perfil de flujo) . Vea <i>Perfiles de transmisión</i> .



Agregar posiciones digitales predefinidas









Control PTZ

Nota

Como administrador, puede desactivar el PTZ mecánico para los usuarios. Vea *Permisos de usuario*.

Grabación y reproducción instantánea en la visualización en directo

	Para ir a la pestaña Recordings (Grabaciones), seleccione una cámara o una vista dividida y haga clic en  .
	Indica una grabación en curso en la visualización en directo.
	Indica que se ha detectado movimiento.
	Para reproducir una grabación en curso, desplace el cursor sobre la imagen y haga clic en  Instant replay (Reproducción instantánea) . Se abre la pestaña Recordings (Grabaciones) y se reproducirán los últimos 5 segundos de la grabación.
REC	Para grabar manualmente desde la visualización en directo, desplace el cursor sobre la imagen y haga clic en el botón REC (GRABAR) . El botón se pone amarillo para indicar que la grabación está en curso. Para dejar de grabar, haga clic en REC (GRABAR) de nuevo.

Para configurar los ajustes de grabación manuales, como la resolución, la compresión y la velocidad de fotogramas, vea *Método de grabación*. Para obtener más información sobre la grabación y la reproducción, vea *Reproducción de grabaciones*.









Nota

Los administradores pueden desactivar la función de grabación manual para los usuarios. Vea *Permisos de usuario*.

Audio en vista en vivo

El audio está disponible si la cámara dispone de prestaciones de audio y si ha activado el audio en el perfil usado para la visualización en directo.

Vaya a **Configuration > Devices > Stream profiles (Configuración > Dispositivos > perfiles de flujo)** y configure el audio para la cámara. Vea *Perfiles de transmisión, on page 54*.

 Volume (Volumen)	Para cambiar el volumen de una vista, desplace el cursor sobre la imagen, desplace el cursor sobre el botón del altavoz y, a continuación, utilice el control deslizante para cambiar el volumen. Para silenciar o activar el audio, haga clic en  .
 Escuchar solo esta vista	Para silenciar otras vistas y escuchar solo esta vista, desplace el cursor sobre la imagen y haga clic en  .
 Hablar por el altavoz	Para hablar por el altavoz configurado en modo full-duplex, desplace el cursor sobre la imagen y haga clic en  .
 Pulsar para hablar	Para hablar por el altavoz configurado en los modos simplex y half-duplex, desplace el cursor sobre la imagen y mantenga pulsado  . Para mostrar el botón Push-to-talk (Pulsar para hablar) para todos los modos duplex, active Use push-to-talk for all duplex modes (Utilizar pulsar para hablar para todos los modos duplex) en Configuration > Client > Streaming > Audio (Configuración > Cliente > Transmisión > Audio) . Vea <i>Transmisión, on page 120</i> .



Nota

Como administrador, puede desactivar el audio para los usuarios. Vea *Permisos de usuario*.

Control en pantalla en la visualización en directo

Nota

El control en pantalla precisa firmware 7.40 o posterior.

	Para acceder a las características disponibles de la cámara, en la visualización en directo, haga clic en  .
---	---


Vista dividida

Una vista dividida muestra varias vistas en la misma ventana. Se pueden usar vistas de cámara, secuencias, páginas web, mapas y otras vistas divididas en la vista dividida.

Nota

Al conectarse a varios servidores AXIS Camera Station Pro, puede añadir a su vista dividida, cámara, dispositivo o zona de audio de otros servidores.

Para agregar una vista dividida:

1. En la pestaña Live view (Visualización en directo), haga clic en .
2. Seleccione Nueva vista dividida.

3. Introduzca un nombre para la vista dividida.
4. Seleccione la plantilla que desea utilizar en el menú desplegable **Template (Plantilla)**.
5. Arrastre y coloque una o varias vistas, zonas de audio o cámaras en la cuadrícula.
6. Haga clic en **Save view (Guardar vista)** para guardar la vista dividida en el servidor actual.

<p>Definir punto clave</p>	<p>Para definir un fotograma de punto clave, haga clic con el botón derecho en él y seleccione Set hotspot (Definir punto clave). Si hace clic en otro fotograma, se abre en el punto clave. Los puntos clave resultan útiles en las vistas divididas asimétricas con un fotograma grande y varios más pequeños. El fotograma mayor suele ser el punto clave.</p>
<p>Perfil de flujo</p>	<p>Para establecer el perfil de flujo para la cámara, haga clic con el botón derecho en la cámara en la vista de cuadrícula y seleccione Stream profile (Perfil de flujo). Consulte <i>Perfiles de transmisión</i>.</p>





Agregar una vista dividida

Panel de puerta en vista dividida.

Si ha configurado una puerta, puede ayudar a los titulares de tarjeta y supervisar el estado y las transacciones recientes de la puerta en una vista dividida.

1. Agregar una puerta. Vea *Agregar una puerta*, on page 149.
2. Agregue el panel de puerta a una vista. Consulte *Vista dividida*, on page 18.

<p>Panel</p>	<p>Para ver los detalles y el estado de la puerta y el estado de bloqueo, abra la pestaña Dashboard (Panel).</p> <p>En el panel se muestra la siguiente información:</p> <ul style="list-style-type: none"> • Evento de control de acceso con los datos del titular de tarjeta, incluida la fotografía, por ejemplo cuando el titular pasa la tarjeta. • Alarmas con información de activación de la alarma, por ejemplo cuando una puerta está abierta durante demasiado tiempo. • La última transacción.
	<p>Para marcar un evento y que esté disponible en la pestaña Transactions (Transacciones), haga clic en .</p>
<p>Acceso</p>	<p>Para conceder acceso de forma manual, haga clic en Access (Acceso). Así se desbloquea la puerta de la misma forma que si alguien presentara sus</p>

	credenciales, lo que normalmente quiere decir que se bloquea automáticamente una vez transcurrido un período de tiempo establecido.
Cerradura	Para bloquear la puerta manualmente, haga clic en Lock (Bloquear) .
Desbloquear	Para desbloquear la puerta manualmente, haga clic en Unlock (Desbloquear) . La puerta permanece desbloqueada hasta que vuelva a bloquearla manualmente.
Bloqueo	Para impedir el acceso a la puerta, haga clic en Lockdown (Bloqueo de emergencia) .
Transacciones	Para ver las transacciones recientes y las guardadas, abra la pestaña Transactions (Transacciones) .



Supervisión y asistencia en el panel de la puerta

AXIS Data Insights Dashboard en una vista dividida

AXIS Data Insights Dashboard presenta los datos de analíticas de sus dispositivos en gráficos y cuadros. Para agregar un panel a una vista dividida:

1. Configure un panel de control. Vea *Panel de información de datos de AXIS*, on page 180.
2. En la pestaña de visualización en directo, haga clic en **+**.
3. Seleccione **Nueva vista dividida**.
4. Expanda la carpeta **Dashboards (Paneles)**.
5. Arrastre y coloque un panel en la cuadrícula.
6. Haga clic en **Save view (Guardar vista)**.

Paneles	
Analítica de audio	Muestra datos de eventos de AXIS Audio Analytics.
Conteo de cruce de línea	Muestra los datos de recuento del escenario de recuento cruzado de AXIS Object Analytics.
Genérica	Muestra datos de todas las fuentes de datos admitidas.
Estado de la imagen	Muestra datos de eventos de AXIS Image Health Analytics.
Ocupación de un área	Muestra los datos de ocupación de AXIS Object Analytics en el escenario de área.
Recuento de entradas y salidas	Muestra datos del escenario de conteo de cruce de línea de AXIS Object Analytics, AXIS People Counter y AXIS P8815-2 3D Counter.

Paneles	
Supervisión de calidad del aire	Muestra datos de calidad del aire interior en tiempo real facilitados por AXIS Air Quality Sensors.
Supervisión detallada de calidad del aire	Muestra los datos añadidos de AXIS Air Quality Sensors.

Usar interfaces de megafonía en vistas divididas

Puede usar interfaces de megafonía para realizar anuncios en directo, llamadas o reproducir archivos de audio desde dispositivos de audio. Esto requiere la integración con AXIS Audio Manager Pro. Para obtener más información, consulte *Configure AXIS Audio Manager Pro, on page 175*.

Para usar interfaces de megafonía:

1. Edite o añada una nueva vista dividida.
2. Arrastre y suelte una o varias zonas de audio en la cuadrícula para convertirla en una interfaz de megafonía.

Nota

Las zonas de audio en AXIS Camera Station Pro son idénticas a las zonas configuradas en su servidor AXIS Audio Manager Pro.

3. Seleccione **Speak (Hablar)**, **Call (Llamar)** o **Play a file (Reproducir un archivo)**:
 - Seleccione **Speak (Hablar)** para la comunicación unidireccional, como anuncios en directo.
 - Seleccione **Call (Llamar)** para la comunicación bidireccional, por ejemplo, cuando desee hablar con alguien a través de un intercomunicador.
 - Seleccione **Play a file (Reproducir un archivo)** para reproducir un archivo desde el servidor AXIS Audio Pro a través del altavoz.


Secuencia

En las secuencias se cambia entre vistas.

Nota

Al conectarse a varios servidores AXIS Camera Station Pro, puede agregar a la secuencia cualquier vista, cámara o dispositivo de otros servidores.

Para agregar una secuencia:

1. En la pestaña Live view (Visualización en directo), haga clic en .
2. Seleccione **Nueva secuencia**.
3. Introduzca un nombre para la secuencia.
4. Arrastre y coloque vistas o cámaras en la vista de secuencia.
5. Organice las vistas en el orden en el que quiera la secuencia.
6. También puede establecer tiempos de permanencia para cada vista.
7. Para cámaras con capacidades PTZ, seleccione una posición predefinida de PTZ en la lista desplegable de **Posición predefinida de PTZ**. Vea *Posiciones predefinidas de PTZ*.
8. Haga clic en **Save view (Guardar vista)** para guardar la secuencia en el servidor actual.

Tiempo de permanencia	El tiempo de permanencia es el número de segundos que se muestra una vista antes de pasar a la siguiente. Se puede establecer para cada vista.
-----------------------	--



Para ver este vídeo, vaya a la versión web de este documento.

Agregar una secuencia

Vista de cámara

Una vista de cámara muestra vídeo en vivo de una cámara. Las vistas de la cámara se pueden utilizar en vistas divididas, secuencias y mapas.

Nota

Al conectarse con varios servidores de AXIS Camera Station Pro, la lista muestra todas las cámaras de todos los servidores conectados.

Para agregar una vista de cámara:

1. En la pestaña Live view (Visualización en directo) o Recordings (Grabaciones), haga clic en **+**.
2. Seleccione **Nueva vista de cámara**.
3. Seleccione la cámara en el menú desplegable y haga clic en **OK (Aceptar)**.

Mapa

Un mapa es una imagen importada en la que se pueden poner vistas de la cámara, vistas divididas, zonas de audio, secuencias, páginas web, otros mapas y puertas. El mapa ofrece una visión general y la forma de localizar dispositivos individuales y acceder a ellos. En el caso de instalaciones grandes, cree diversos mapas y dispóngalos en un mapa de vista general.

Los botones de acción también aparecen en la vista de mapa. Vea *Crear activadores de botones de acción*.

Nota

Al conectarse a varios servidores AXIS Camera Station Pro, puede agregar a su vista de mapas, cámara o dispositivo de otros servidores.





Para agregar un mapa:

1. En la pestaña Live view (Visualización en directo), haga clic en **+**.
2. Seleccione **Nuevo mapa**.
3. Introduzca un nombre para el mapa.
4. Haga clic en **Choose image (Elegir imagen)** y localice el archivo de mapa. El tamaño máximo del archivo es de 20 MB y se admiten los formatos BMP, JPG, PNG y GIF.
5. Arrastre vistas, cámaras, otros dispositivos y puertas al mapa.
6. Haga clic en un icono en el mapa para editar los ajustes.
7. Haga clic en **Add label (Agregar etiqueta)**, introduzca un nombre de etiqueta y defina tamaño, rotación, estilo y color de la etiqueta.

Nota

Algunos ajustes se pueden editar para múltiples iconos y etiquetas al mismo tiempo.

8. Haga clic en **Save view (Guardar vista)** para guardar el mapa en el servidor actual.

	El estado físico de la puerta cuando esta se configura con un monitor de puerta.
	El estado físico de la cerradura cuando la puerta se configura sin un monitor de puerta.
Icono	Seleccione el icono que desea utilizar. Esta opción solo está disponible para las cámaras y otros dispositivos.
Tamaño	Ajuste el control deslizante para cambiar el tamaño de los iconos.
Color	Haga clic en  para cambiar el color del icono.
Nombre	Active esta opción para mostrar el nombre del icono. Seleccione Inferior o Superior para cambiar la posición del nombre del icono.
Flecha de dirección	Muestra flechas orientadas a la dirección del campo de visión de cada cámara. Puede visualizar flechas con o sin áreas de cobertura.
Área de cobertura	Esta opción solo está disponible para las cámaras y otros dispositivos. Active esta opción para mostrar en el mapa el área de cobertura del dispositivo. Puede modificar Range (Rango) , Width (Ancho) , Direction (Dirección) y color del área de cobertura. Active Flash si quiere que el área de cobertura parpadee cuando la cámara esté grabando como consecuencia de la detección de movimiento o de otras reglas de acción. En la página de configuración del cliente, puede desactivar el parpadeo de todas las áreas de cobertura de todos los dispositivos. Consulte <i>Ajustes del cliente</i> , on page 117.
Eliminar	Haga clic en  para eliminar el icono del mapa.



Agregar un mapa



Activar audio desde un mapa

Página web

Una vista de página web muestra una página de Internet. Puede agregar una página web, por ejemplo, a una vista dividida o a una secuencia.

Para agregar una página web:

1. En la pestaña Live view (Visualización en directo), haga clic en **+**.
2. Seleccione **New webpage (Nueva página web)**.
3. Introduzca un nombre para la página web.
4. Introduzca la URL completa de la página web.
5. Haga clic en **OK**.



Carpetas

Utilice carpetas para categorizar objetos en una navegación con vista de árbol. Las carpetas pueden contener vistas divididas, secuencias, vistas de cámara, mapas, páginas web y otras carpetas.

Para agregar una carpeta:

1. En la pestaña Live view (Visualización en directo) o Recordings (Grabaciones), haga clic en **+**.
2. Seleccione **Nueva carpeta**.
3. Introduzca un nombre para la carpeta y haga clic en **Aceptar**.

Grabaciones

Desde la pestaña de grabaciones puede gestionar la búsqueda, reproducción y exportación de grabaciones. La pestaña consta de una vista de la grabación y dos paneles donde puede encontrar vistas, imágenes, herramientas de reproducción y cámaras de los servidores conectados agrupados por el nombre del servidor, consulte *Vista en vivo*.

Desde la vista principal de la grabación, puede gestionar la imagen de la misma forma que lo hace en la vista en vivo. Para más información, consulte *Gestión de imagen en la visualización en directo, on page 15*.

Para cambiar el método de grabación y los ajustes de grabación como resolución, compresión y velocidad de fotogramas, consulte *Método de grabación*.

Nota

No es posible eliminar grabaciones manualmente de AXIS Camera Station Pro. Debe cambiar el tiempo de conservación en **Configuration > Storage > Selection (Configuración > Almacenamiento > Selección)** para eliminar las grabaciones anteriores.

Reproducción de grabaciones






Es posible reproducir grabaciones de distintas cámaras al mismo tiempo si el marcador de reproducción se coloca sobre varias grabaciones de la línea temporal.

Puede mostrar vídeo en vivo y grabado al mismo tiempo cuando utiliza varios monitores.



Línea temporal de reproducción







Utilice la línea temporal para desplazarse en la reproducción y encontrar cuándo se realizó una grabación. Una línea roja en la línea temporal simboliza una grabación de detección de movimiento. Una línea azul en la línea temporal simboliza que una regla de acción ha activado la grabación. Desplace el cursor sobre una grabación en la línea temporal para mostrar el tipo de grabación y la hora. Para obtener una mejor vista y encontrar grabaciones, puede acercar, alejar y arrastrar la línea temporal. La reproducción se pausa temporalmente cuando arrastra la línea temporal y se reanuda cuando la libere. En una grabación, mueva la línea temporal (depuración) para obtener una descripción general del contenido y encontrar ocurrencias específicas.

Buscar grabaciones

	Haga clic para seleccionar una fecha y hora en la línea temporal.
	Utilice el filtro para configurar qué tipo de grabaciones mostrar en la línea temporal.
	Úselo para buscar marcadores guardados, consulte <i>Marcadores</i> .
	Haga clic para abrir una lista de grabaciones y marcadores creados con la cámara corporal de Axis. Aquí puede buscar la fecha y la hora, el método de activación de grabación y las categorías y notas que el usuario de la cámara ha agregado en AXIS Body Worn Assistant.
 Búsqueda inteligente 1	Utilice la búsqueda inteligente para buscar grabaciones, consulte <i>Búsqueda inteligente 1</i> .

Reproducción de grabaciones






	Reproduzca la grabación.
	Pause la grabación.

	Salte al inicio de la grabación o evento actual o anterior. Haga clic con el botón derecho para ir a grabaciones, eventos o ambos.
	Salte al inicio de la grabación o evento siguiente. Haga clic con el botón derecho para ir a grabaciones, eventos o ambos.
	Vaya al fotograma anterior de una grabación. Pausa la grabación para utilizar esta función. Haga clic con el botón derecho para establecer cuántos fotogramas omitir (hasta 20 fotogramas).
	Vaya al fotograma siguiente de una grabación. Pausa la grabación para utilizar esta función. Haga clic con el botón derecho para establecer cuántos fotogramas omitir (hasta 20 fotogramas).
	Cambie la velocidad de reproducción con los multiplicadores del menú desplegable.
	Silenciar audio. Sólo las grabaciones con audio tienen esta característica.
Control deslizante de audio	Deslice para cambiar el volumen del audio. Sólo las grabaciones con audio tienen esta característica.
Mostrar todos los metadatos del sistema corporal	Mostrar los metadatos de un sistema corporal completo y mostrar las notas y categorías de AXIS Body Worn Assistant.
Movimiento horizontal, vertical y zoom	Haga clic en la imagen y desplácese hacia arriba o hacia abajo para acercar y alejar la imagen y mover la vista para ver otras partes de la imagen. Para ampliar un área, sitúe el cursor en el área deseada y desplácese para acercar la imagen.


Marcadores

Nota

- No se puede eliminar una grabación bloqueada a menos que se desbloquee manualmente.
- El sistema elimina las grabaciones bloqueadas cuando retira la cámara de AXIS Camera Station Pro.

	Haga clic para mostrar todos los marcadores. Para filtrar los marcadores, haga clic en el icono.
	Añadir un nuevo marcador.
	Significa que es una grabación bloqueada. La grabación incluye al menos 2,5 minutos de vídeo antes y después del marcador.
	Edite el nombre y la descripción del marcador y desbloquee o bloquee la grabación.
	Elimine un marcador. Seleccione varios marcadores y mantenga presionada la tecla CTRL o MAYÚS para eliminar varios marcadores.
Impedir eliminar grabación	Seleccione o borre para bloquear o desbloquear la grabación.

Agregar marcadores

1. Ir a grabación.
2. En la línea temporal de la cámara, amplíe o reduzca la vista de la línea temporal y coloque el marcador en la posición deseada.
3. Haga clic en .
4. Introduzca un nombre y una descripción para el marcador. Utilice palabras clave en la descripción para que sea fácil encontrar y reconocer el marcador.
5. Seleccione **Impedir eliminar grabación** para bloquear la grabación.

Nota

No es posible eliminar una grabación bloqueada. Para desbloquear la grabación, anule la opción o elimine el marcador.

6. Haga clic en **OK (Aceptar)** para guardar el marcador.

Categorías de eventos

Asigne categorías a las grabaciones para facilitar la búsqueda de tipos específicos de eventos, como agresiones o controles de tráfico. Antes de comenzar, asegúrese de tener los permisos de usuario adecuados. Consulte *Privilegios de usuario o grupo, on page 139*.

Asignar categorías de eventos

1. En la pestaña **Recordings (Grabaciones)**, busque la grabación a la que desea asignar una categoría de evento.
2. Haga clic con el botón derecho del ratón en la grabación de la línea de tiempo y seleccione **Categorize event (Categorizar evento)**.
3. Añada una o varias categorías.
4. Haga clic en **OK**.

Al categorizar un evento, las categorías seleccionadas aparecen en la miniatura de la vista previa de la grabación. Si asigna un color a la categoría, la línea de tiempo mostrará ese color.

Eliminar categorías de eventos

1. En la pestaña **Recordings (Grabaciones)**, busque la grabación de la que desea eliminar las categorías.
2. Haga clic con el botón derecho del ratón en la grabación de la línea de tiempo y seleccione **Categorize event (Categorizar evento)**.
3. En la lista de categorías asignadas, seleccione la categoría que desea eliminar.
4. Haga clic en **Remove (Eliminar)**.
5. Repita los pasos 3 y 4 para cada categoría que desee eliminar.
6. Haga clic en **OK**.

Nota

Solo puede usar el botón Eliminar si tiene permiso para eliminar categorías o si selecciona una categoría no asignada de la lista.

Consulte *Configurar categorías de eventos, on page 89* para obtener más información.

Exportar grabaciones



En la pestaña **Export (Exportar)**, puede exportar grabaciones a un almacenamiento local o a una ubicación de red. Aquí también podrá encontrar información y una vista previa de la grabación. Es posible exportar varios archivos al mismo tiempo y puede seleccionar exportarlos a .asf, .mp4 y .mkv. Para reproducir sus grabaciones, utilice Windows Media Player (.asf) o AXIS File Player (.asf, .mp4, .mkv). AXIS File Player es un software gratuito de reproducción de vídeo y audio que no requiere instalación.

Nota

En AXIS File Player, puede cambiar la velocidad de reproducción de las grabaciones en los formatos .mp4 y .mkv, pero no en el formato .asf.

Antes de comenzar, asegúrese de tener permisos para exportar. Vea *Permisos de usuario para exportar*, on page 31.

Exportar grabaciones





1. En la pestaña **Recordings (Grabaciones)**, seleccione una cámara o una vista.
2. Añada las grabaciones a la lista de exportación. Las grabaciones en la línea de tiempo que no están incluidas en la exportación obtienen un color rayado.
 - 2.1. Haga clic en  para mostrar los marcadores de selección.
 - 2.2. Mueva los marcadores para incluir las grabaciones que desea exportar.
 - 2.3. Haga clic en  para abrir la pestaña **Export (Exportar)**.
3. Haga clic en **Export... (Exportar...)**.
4. Seleccione la carpeta a la que exporta las grabaciones.
5. Haga clic en **OK**. La tarea de exportar grabaciones aparece en la pestaña **Tasks (Tareas)**.







La carpeta de exportación incluye:

- Las grabaciones en formato seleccionado.
- Un archivo .txt con notas si selecciona **Include notes (Incluir notas)**.
- AXIS File Player, si selecciona **Include AXIS File Player (Incluir AXIS File Player)**.
- Un archivo .asx con una lista de reproducción si selecciona **Create playlist(.asx) (Crear lista de reproducción (.asx))**.



Exportar grabaciones


Pestaña Recordings (Grabaciones)	
	Para seleccionar varias grabaciones, haga clic en  y mueva los marcadores de selección al inicio y parada deseados.
	Para exportar grabaciones dentro de los marcadores de sección, haga clic en  .
Añadir grabaciones	Para exportar una sola grabación, haga clic derecho en una grabación y seleccione Export > Add recordings (Exportar > Agregar grabaciones) .
Agregar grabaciones de eventos	Para agregar todas las grabaciones que ocurrieron dentro del tiempo de un evento, haga clic con el botón derecho en una grabación y seleccione Export > Add event recordings (Exportar > Agregar grabaciones de eventos) .

Pestaña Recordings (Grabaciones)	
Eliminar grabaciones	Para eliminar una grabación de la lista de exportación, haga clic con el botón derecho en una grabación y seleccione Export > Remove recordings (Exportar > Eliminar grabaciones) .
Eliminar grabaciones	Haga clic con el botón derecho del ratón fuera de cualquier grabación y seleccione Export > Remove recordings (Exportar > Quitar grabaciones) para quitar de la lista de exportación todas las grabaciones incluidas en los marcadores de selección.
Pestaña Export (Exportar)	
Audio	Para excluir el audio de la grabación exportada, deselectione la casilla de la columna Audio . Para incluir siempre audio en las grabaciones exportadas, vaya a Configuration (Configuración > Server (Servidor) > Settings (Ajustes) > Export (Exportar) y seleccione Include audio when adding recordings to export (Incluir audio al agregar grabaciones para exportar) .
	Para editar una grabación, selecciónela y haga clic en  . Vea <i>Editar las grabaciones (redacciones) antes de exportar, on page 31</i> .
	Para editar las notas de la grabación, seleccione una grabación y haga clic en  .
	Para eliminar la grabación de la lista de exportación, seleccione una grabación y haga clic en  .
Cambiar para exportar	Para cambiar a la pestaña Export (Exportar) si la pestaña Incident report (Informe de incidencias) está abierta, haga clic en Switch to export (Cambiar a exportar) .
Perfil de flujo preferido	Seleccione el perfil de flujo en el campo Preferred stream profile (Perfil de flujo preferido) .
Previsualizar	Haga clic en una grabación en la lista exportada para previsualizarla y reproducirla. Solo puede obtener una vista previa de varias grabaciones si proceden de una misma cámara.
Guardar	Si quiere guardar la lista de exportación en un archivo, haga clic en Save (Guardar) .
Cargar	Si desea incluir una lista de exportación previamente guardada, haga clic en Load (Cargar) .
Nombre de la exportación	Puede introducir un nombre personalizado para la carpeta y los archivos exportados o dejarlo en blanco para usar la convención de nombres predeterminada en AXIS Camera Station Pro.

Pestaña Export (Exportar)	
Añadir el nombre de la cámara y la marca de tiempo	Seleccione esta opción para añadir el nombre de la cámara y la marca de tiempo al nombre de la carpeta y los archivos exportados.
Ajustar la hora de inicio y finalización	Para ajustar la hora de inicio y finalización de la grabación, vaya a la línea temporal en la vista previa y ajuste las horas de inicio y finalización. La línea temporal muestra hasta treinta minutos de grabaciones antes y después de la grabación seleccionada.
Añadir instantánea	Para agregar instantáneas, arrastre la línea temporal en la vista previa a una ubicación específica. Haga clic con el botón derecho en la vista previa y seleccione Add snapshot (Agregar instantánea) .

Configuración avanzada	
Incluir notas	Para incluir notas de las grabaciones, seleccione Incluir notas . Las notas están disponibles como archivo .txt en la carpeta exportada y como referencia a la grabación en AXIS File Player.
Incluir AXIS File Player	Para incluir AXIS File Player con las grabaciones exportadas, seleccione Incluir AXIS File Player .
Create playlist(.asx) (Crear lista de reproducción (.asx))	Para crear una lista de reproducción en formato .asx, utilizada por Windows Media Player, seleccione Crear lista de reproducción (.asx) . Las grabaciones se reproducirán en el orden en el que se grabaron.
Agregar firma digital	Para evitar la manipulación de la imagen, seleccione Add digital signature (Agregar firma digital) . Esta opción solo está disponible para las grabaciones con el formato .asf. Vea <i>Reproducir y comprobar las grabaciones exportadas, on page 32</i> .
Exportar a archivo Zip	Para exportar a un archivo Zip, seleccione Export to Zip file (Exportar a archivo Zip) ; y establezca una contraseña para el archivo Zip exportado.
Formato de exportación	En el menú desplegable Export format (Formato de exportación) , seleccione el formato con el que quiera exportar las grabaciones. Las grabaciones exportadas no incluyen audio en formato G.711 o G.726 si selecciona MP4.
Edited video encoding (Codificación de vídeo editada)	Si se ha editado algún vídeo, puede establecer el formato de codificación de vídeo en <i>Automatic</i> , <i>H. 264</i> o <i>M-JPEG</i> en Edited video encoding (Codificación de vídeo editado) . Seleccione <i>Automatic</i> para utilizar M-JPEG para el formato M-JPEG y H. 264 para otros formatos.


Permisos de usuario para exportar

Para exportar grabaciones o generar informes de incidentes es necesario tener permiso. Puede tener permiso para uno o ambos. Al hacer clic en  en la pestaña **Recordings (Grabaciones)**, se abrirá la pestaña **Export (Exportar)** conectada.

Para configurar los permisos, vaya a *Permisos de usuario*, on page 137.

Editar las grabaciones (redacciones) antes de exportar

Desenfocar un objeto en movimiento

1. En las pestañas **Export (Exportar)** o **Incident report (Informe de incidencias)**, seleccione una grabación y haga clic en .
2. Mueva la línea temporal a la primera aparición del objeto en movimiento que desea cubrir.
3. Haga clic en **Bounding boxes > Add (Cuadros delimitadores > Agregar)** para agregar un nuevo cuadro limitador.
4. Vaya a **Bounding box options > Size (Opciones de cuadro delimitador > Tamaño)** para ajustar el tamaño.
5. Mueva el cuadro limitador y colóquelo sobre el objeto.
6. Vaya a **Bounding box options > Fill (Opciones de cuadro delimitador > Rellenar)** y establézcalo en **Pixelated (Pixelado)** o **Black (Negro)**.
7. Cuando se reproduzca la grabación, haga clic con el botón derecho en el objeto y seleccione **Add key frame (Añadir fotograma clave)**.
8. Para agregar fotogramas clave continuos, mueva el cuadro limitador para cubrir el objeto mientras se reproduzca la grabación.
9. Mueva la línea temporal y asegúrese de que el cuadro limitador cubra el objeto durante toda la grabación.
10. Para establecer un final, haga clic con el botón derecho en la forma de diamante en el último fotograma clave y seleccione **Set end (Establecer fin)**. Esto elimina los fotogramas clave después del punto final.

Nota

Puede agregar varios cuadros delimitadores al vídeo. Si los cuadros limitadores se superponen, la parte superpuesta se llenará de color en este orden: negro, pixelado y transparente.

Quitar todo	Para eliminar todos los cuadros limitadores, haga clic en Bounding boxes > Remove all (Cuadros limitadores > Eliminar todo) .
Eliminar fotograma clave	Para eliminar un fotograma clave, haga clic con el botón derecho en el fotograma y seleccione Remove key frame (Eliminar fotograma clave) .


Mostrar un objeto en movimiento con el fondo desenfocado

1. Cree un cuadro limitador, consulte *Desenfocar un objeto en movimiento*, on page 31.
2. Vaya a **Bounding box options > Fill (Opciones de cuadro delimitador > Rellenar)** y establézcalo en **Clear (Transparente)**.
3. Vaya a **Video background (Fondo de vídeo)** y establézcalo en **Pixelated (Pixelado)** o **Black (Negro)**.

<p>Pixelar todo excepto esto</p>	<p>Seleccione varios cuadros limitadores en la lista. Haga clic con el botón derecho y seleccione Pixelate all but this (Pixelar todo excepto esto). Los cuadros limitadores seleccionados se vuelven Clear (Transparentes) y los no seleccionados Pixelated (Pixelados).</p>
----------------------------------	--

Generar cuadros delimitadores

Para generar cuadros limitadores a partir de los datos analíticos, active los datos analíticos de la cámara. Vea *Perfiles de transmisión, on page 54*.

1. En las pestañas **Export (Exportar)** o **Incident report (Informe de incidencias)**, haga clic en .
2. Haga clic en **Generate bounding boxes (Generar cuadros delimitadores)**.
3. Asegúrese de que los cuadros limitadores cubran el objeto en movimiento; ajústelos si es necesario.
4. Seleccione un relleno par los cuadros limitadores o el fondo del vídeo.

Mejorar la edición de vídeo con AXIS Video Content Stream


Para mejorar la edición de vídeo, instale la aplicación AXIS Video Content Stream 1.0 en cámaras con firmware 5.50 a 9.60. AXIS Camera Station Pro inicia la instalación automáticamente cuando añade una cámara al sistema. Vea *Instalar la aplicación de la cámara*.



Editar grabaciones antes de exportar

Reproducir y comprobar las grabaciones exportadas

Para evitar la manipulación de imágenes, puede agregar una firma digital a las grabaciones exportadas con o sin contraseña. Utilice AXIS File Player para verificar la firma digital y comprobar si hay cambios en la grabación.

1. Vaya a la carpeta con las grabaciones exportadas. Si el archivo Zip exportado está protegido con contraseña, introduzca su contraseña para abrir la carpeta.
2. Abra AXIS File Player, las grabaciones exportadas se reproducen automáticamente.
3. En AXIS File Player, haga clic en  para mostrar las notas en las grabaciones.
4. En AXIS File Player, compruebe la firma digital para las grabaciones con **Add digital signature (Añadir firma digital)**.
 - 4.1. Vaya a **Herramientas > Verificar firma digital**.
 - 4.2. Seleccione **Validate with password (Validar con contraseña)** e introduzca la contraseña si está protegida por contraseña.
 - 4.3. Para ver los resultados de la verificación, haga clic en **Verify (Verificar)**.

Exportar informes de incidencias

En la pestaña Informe de incidentes, puede exportar informes de incidentes a un almacenamiento local o a una ubicación de red. Aquí puede incluir grabaciones, instantáneas y notas en sus informes de incidentes.

Antes de comenzar, asegúrese de tener permisos para exportar. Vea *Permisos de usuario para exportar*, on page 31.









Informes de incidentes

Generar informes de incidencias

1. En la pestaña **Recordings (Grabaciones)**, seleccione una cámara o una vista.
2. Añada las grabaciones a la lista de exportación. Vea *Exportar grabaciones*, on page 27.
3. Haga clic en **Switch to incident report (Cambiar al informe de incidentes)** para ir a la pestaña de informe de incidentes.
4. Haga clic en **Create report (Crear informe)**.
5. Seleccione una carpeta para guardar el informe de incidente.
6. Haga clic en **OK**. La tarea de exportar informe de incidentes aparece en la pestaña **Tasks (Tareas)**.

La carpeta de exportación incluye:

- AXIS File Player.
- Las grabaciones en formato seleccionado.
- Un archivo .txt si selecciona **Include notes (Incluir notas)**.
- El informe de incidencias.
- La lista de reproducción, si se exportan varias grabaciones.

<p>Audio</p>	<p>Para excluir el audio de la grabación exportada, deseccione la casilla de la columna Audio. Para incluir siempre audio en las grabaciones exportadas, vaya a Configuration (Configuración > Server (Servidor) > Settings (Ajustes) > Export (Exportar) y seleccione Include audio when adding recordings to export (Incluir audio al agregar grabaciones para exportar).</p>
	<p>Para editar una grabación, selecciónela y haga clic en . Vea <i>Editar las grabaciones (redacciones) antes de exportar</i>, on page 31.</p>
	<p>Para editar las notas de la grabación, seleccione una grabación y haga clic en .</p>
	<p>Para eliminar la grabación de la lista de exportación, seleccione una grabación y haga clic en .</p>
<p>Cambiar a informe de incidentes</p>	<p>Para cambiar a la pestaña Incident report (Informe de incidencias) si la pestaña Export (Exportar) está abierta, haga clic en Switch to incident report (Cambiar a informe de incidencias).</p>


Perfil de flujo preferido	Seleccione el perfil de flujo en el campo desplegable Preferred stream profile (Perfil de flujo preferido) .
Previsualizar	Haga clic en una grabación en la lista exportada para previsualizarla y reproducirla. Solo puede obtener una vista previa de varias grabaciones si proceden de una misma cámara.
Guardar	Si quiere guardar el informe de incidentes en un archivo, haga clic en Save (Guardar) .
Cargar	Si desea incluir un informe de incidente previamente guardado, haga clic en Load (Cargar) .
Descripción	El campo Description (Descripción) se llena automáticamente con datos predefinidos de la plantilla Descripción. También puede agregar la información necesaria adicional que desee incluir en el informe de incidencias.
Categoría	Seleccione una categoría a la que pertenece el informe.
Reference ID (ID de referencia):	Se genera automáticamente una Reference ID (Identificación de referencia) y puede cambiarla manualmente si es necesario. La ID de referencia es única e identifica el informe de incidencias.
Incluir notas	Para incluir notas de las grabaciones y capturas de pantalla, seleccione Include notes (Incluir notas) . Las notas están disponibles como archivo .txt en la carpeta exportada y como referencia a la grabación en AXIS File Player.
Edited video encoding (Codificación de vídeo editada)	Si se ha editado algún vídeo, puede establecer el formato de codificación de vídeo en Automatic , H. 264 o M-JPEG en Edited video encoding (Codificación de vídeo editado) . Seleccione Automatic para utilizar M-JPEG para el formato M-JPEG y H. 264 para otros formatos.
Ajustar la hora de inicio y finalización	Para ajustar la hora de inicio y finalización de la grabación, vaya a la línea temporal en la vista previa y ajuste las horas de inicio y finalización. La línea temporal muestra hasta treinta minutos de grabaciones antes y después de la grabación seleccionada.
Añadir instantánea	Para agregar instantáneas, mueva la línea temporal en la vista previa a una ubicación específica. Haga clic con el botón derecho en la vista previa y seleccione Add snapshot (Agregar instantánea) .

Grabar manualmente

Nota

Cuando se conecta a varios servidores de AXIS Camera Station Pro, puede iniciar y detener manualmente una grabación en cualquier servidor conectado. Para hacer esto, seleccione el servidor en la lista desplegable **Selected server (Servidor seleccionado)**.

Para iniciar y detener manualmente una grabación desde el menú principal:

1. Vaya a  > **Actions (Acciones)** > **Record manually (Grabar manualmente)**.
2. Seleccione una o más cámaras.
3. Haga clic en **Start (Iniciar)** para empezar la grabación.
4. Haga clic en **Stop (Detener)** para detener la grabación.

Para iniciar y detener una grabación manual desde la pestaña **Live view (Visualización en directo)**:

1. Vaya a **Visualización en directo**.
2. Mueva el puntero del ratón al marco de visualización en directo de la cámara.
3. Haga clic en **REC (Grabar)** para iniciar la grabación. Aparece un indicador rojo en el marco de visualización durante la grabación.
4. Haga clic en **REC (DETENER)** para detener la grabación.

Búsqueda inteligente 1

Utilice la opción de búsqueda inteligente 1 para buscar las partes de una grabación con movimiento en un área de la imagen definida.

Para aumentar la velocidad de búsqueda, seleccione **Include analytics data (Incluir datos de analíticas)** en los perfiles de flujo. Vea *Perfiles de transmisión*.

Para usar la búsqueda inteligente 1:

1. Haga clic en **+** y abra una pestaña de **Smart search 1 (Búsqueda inteligente 1)**.
2. Elija la cámara en la que desea buscar.
3. Ajuste el área de interés. Puede agregar hasta 20 puntos a la forma. Para eliminar un punto, haga clic en él con el botón derecho.
4. Utilice el filtro **Short-lived objects (Objetos que permanecen poco en la escena)** y el filtro **Small objects (Objetos pequeños)** para que no se muestren los resultados no deseados.
5. Seleccione la hora y fecha de inicio y fin de la búsqueda. Utilice la tecla **MAYÚS** para seleccionar un intervalo de fechas.
6. Haga clic en **Buscar**.

Los resultados de la búsqueda aparecen en la pestaña **Results (Resultados)**. En ella puede hacer clic con el botón derecho en uno o varios resultados para exportar las grabaciones.

Short-lived objects filter (Filtro de objetos que permanecen poco en la escena)	Tiempo mínimo que un objeto debe estar en el área de interés para que se incluya en los resultados de la búsqueda.
Small objects filter (Filtro de objetos pequeños)	Tamaño mínimo que debe tener un objeto para que se incluya en los resultados de la búsqueda.



Búsqueda inteligente 1

Búsqueda inteligente 2

Utilice la búsqueda inteligente 2 para encontrar personas y vehículos en movimiento en las grabaciones.

Cuando activa la búsqueda inteligente 2 para una cámara Axis, AXIS Camera Station Pro. comienza a grabar metadatos de esa cámara. Búsqueda inteligente 2 utiliza metadatos para clasificar objetos en la escena y le permite usar filtros para encontrar cosas de interés.

Nota

La opción de búsqueda inteligente 2 requiere lo siguiente:

- La transmisión de metadatos de analíticas a través de RTSP.
- AXIS Video Content Stream en cámaras que tengan un AXIS OS anterior al 9.60. Consulte *Instalar la aplicación de la cámara, on page 69*.
- Sincronización de hora entre el servidor de AXIS Camera Station Pro y las cámaras.

Nota

Recomendaciones generales:

- Recomendamos utilizar grabación continua. Usar grabaciones activadas por detección de movimiento puede provocar detecciones sin grabación de vídeo.
- Recomendamos utilizar el formato H.264 si desea obtener una vista previa de las grabaciones en el resultado de la búsqueda.
- Asegúrese de que las condiciones de iluminación estén dentro de las especificaciones de la cámara para una clasificación de color óptima. Si es necesario, utilice iluminación adicional.

Flujo de trabajo


1. *Configurar la Búsqueda inteligente 2, on page 176*
2. Configure la sincronización de hora entre el servidor de AXIS Camera Station Pro y las cámaras. Vea *Sincronización de hora, on page 74*.
3. Cree un filtro o cargue un filtro ya existente. Vea *Búsqueda con filtros, on page 37*.
4. Gestionar los resultados de búsqueda. Vea *Resultados de búsqueda inteligente, on page 41*.










Búsqueda con filtros

1. Vaya a **Configuration > Smart search 2 > Settings (Configuración > Búsqueda inteligente 2 > Ajustes)** y seleccione las cámaras que desee utilizar en Búsqueda inteligente 2.
2. Haga clic en **+** y abra la pestaña **Smart search 2 (Búsqueda inteligente 2)**.
3. Defina sus criterios de búsqueda.
4. Haga clic en **Buscar**.

Si la búsqueda tarda más de lo esperado, pruebe uno o varios de los siguientes métodos para acelerarla:

- Active el procesamiento del servidor en segundo plano para las cámaras importantes o de uso frecuente.
- Aplique filtros de entrada a las cámaras para reducir las detecciones irrelevantes.
- Acorte el periodo de búsqueda.
- Reduzca el número de cámaras en la búsqueda.
- Defina el área, la dirección del objeto, el tamaño y la duración para reducir la cantidad de datos.

Cámaras	Para limitar la búsqueda por cámara, haga clic en Cameras (Cámaras= y seleccione las cámaras que desea incluir en la búsqueda.
Intervalo de búsqueda	Para limitar la búsqueda por tiempo, haga clic en Search interval (Intervalo de búsqueda) y seleccione un rango de tiempo, un intervalo específico de varios días o cree un intervalo personalizado.
Persona	Para detectar personas, haga clic en Object characteristics (Características del objeto) > Pre-classified (Preclasificado) y seleccione Person (Person) y los colores de la ropa. Puede seleccionar varios colores.
Vehículo	Para detectar vehículos, haga clic en Object characteristics (Características del objeto) > Pre-classified (Preclasificado) y seleccione los tipos y colores de vehículos. Puede seleccionar varios tipos y colores de vehículos.
Similitud visual	<p>Puede utilizar un resultado de búsqueda con una persona de la imagen para buscar personas visuales parecidas. Abra el menú contextual  en un elemento de resultados de búsqueda y seleccione Use as visual similarity reference (Usar como referencia de parecido visual). A continuación, haga clic en Search (Buscar).</p> <p>Nota</p> <p>La búsqueda por similitud crea representaciones abstractas a partir de imágenes recortadas de baja resolución de personas y las compara con otras representaciones. Cuando hay dos representaciones similares, se obtiene un resultado positivo en la búsqueda. La búsqueda por similitud no utiliza datos biométricos para identificar a una persona, pero puede, por ejemplo, reconocer la forma general y el color de la ropa de una persona en un momento dado.</p>
Búsqueda de texto libre	La búsqueda de texto libre le permite describir lo que busca en las grabaciones mediante lenguaje natural (solo en inglés). Vea <i>Búsqueda de texto libre, on page 39</i> .
de exclusión	Para filtrar por área, haga clic en Area (Área) , seleccione la cámara y active Filter by area on this camera (Filtrar por área en esta cámara) . Ajuste el área de interés en la imagen y agregue o elimine los puntos que necesite.
Traspaso de línea	Para filtrar por cruce de líneas, haga clic en Line crossing (Cruce de línea) , seleccione la cámara y active Filter by line crossing on this camera (Filtrar por cruce de línea en esta cámara) . Ajuste la línea en la imagen y agregue o elimine los puntos que necesite.
Tamaño y duración	Para filtrar por tamaño y duración, haga clic en Size and duration , seleccione la cámara y active Filter by

	<p>size and duration on this camera (Filtrar por tamaño y duración en esta cámara). Ajuste el ancho y la altura mínima como un porcentaje de la imagen total. Ajuste la duración mínima en segundos.</p>
Velocidad	<p>Para filtrar por velocidad, haga clic en Speed (Velocidad), seleccione la cámara y active Filter by speed on this camera (Filtrar por velocidad en esta cámara). Especifique el rango de velocidad que desea incluir en el filtro.</p> <p>Nota El filtro de velocidad está disponible para productos como radares y cámaras de fusión que pueden detectar la velocidad.</p>
Detecciones de objetos desconocidos	<p>Para incluir las detecciones que Búsqueda inteligente 2 clasifica como desconocidas, seleccione Object characteristics (Características del objeto) y luego Unknown object detections (Detecciones de objetos desconocidos).</p>
	<p>Para guardar un filtro, haga clic en , introduzca un nombre de filtro y haga clic en Save (Guardar).</p> <p>Seleccione Share with other users (Compartir con otros usuarios) para compartir el filtro con otros usuarios.</p> <p>Para sustituir un filtro existente, haga clic en , seleccione un filtro existente y haga clic en Replace (Sustituir).</p>
	<p>Para cargar una búsqueda reciente, haga clic en  > Recent searches (Búsquedas recientes) y seleccione una búsqueda.</p> <p>Para cargar un filtro guardado, haga clic en  > Saved filters (Filtros guardados) y seleccione un filtro.</p> <p>Para cargar un filtro compartido por otro usuario, haga clic en  > Shared filters (Filtros compartidos) y seleccione un filtro.</p>
	<p>Para restablecer un filtro, haga clic en  y haga clic en Reset (Restablecer).</p>

Búsqueda de texto libre

La búsqueda de texto libre le permite describir lo que busca en las grabaciones mediante su lenguaje natural.

Nota

- La búsqueda de texto libre requiere un mínimo de 16 GB de RAM.
- La búsqueda de texto libre requiere una conexión a internet.
 - La búsqueda de texto libre utiliza la conexión a internet para descargar el modelo de IA de axis.com cuando se configura por primera vez y cuando actualizamos el modelo.

- La búsqueda de texto libre se conecta una vez a la semana a los servicios en la nube de Axis para comprobar si los modelos de IA requieren alguna actualización para cumplir futuras normativas o requisitos. Si la conexión falla, no podrá utilizar la búsqueda de texto libre hasta que el sistema vuelva a conectarse.
- La búsqueda de texto libre realiza todo el procesamiento localmente en su servidor y no utiliza la conexión a internet para enviar ningún vídeo, imagen o texto de consulta.

Para activar la búsqueda de texto libre:

1. Abra una pestaña **Configuration (Configuración)**.
2. Vaya a **Smart Search 2 > Settings (Ajustes)**.
3. En la búsqueda de texto libre, seleccione **Use free text search (Usar búsqueda de texto libre)**. El sistema descarga los archivos necesarios de axis.com.

Para realizar una búsqueda de texto libre:

1. Abra una pestaña **Smart Search 2**.
2. Haga clic en **Object characteristics (Características del objeto)**.
3. Haga clic en **Free text (Texto libre)**.
4. Haga clic en **Show (Mostrar)** para leer información sobre el uso previsto, las limitaciones y el uso responsable.
5. Introduzca lo que quiere incluir y excluir en la búsqueda.
6. Haga clic en **Buscar**.

Directrices para la redacción de texto de consulta

Le recomendamos que utilice la siguiente estructura para sus textos de consulta:

{person, vehicle or other object} + {specific action or attributes of the person, vehicle, or object}

Describa bien el objeto utilizado unos pocos descriptores clave. Por ejemplo:

Texto de consulta	Comentario
Una señora con jersey rojo y un sombrero negro	Correcto
Señora de rojo	Demasiado impreciso
Una señora de 156 cm de estatura aproximadamente, con un cárdigan granate con detalles amarillos y un sombrero de ala grande negro inspirado en finales de los 80 con un ribete bronceado	Demasiados detalles

Describa la situación como si estuviera hablando con una persona, alguien que no fuera un experto en vigilancia. Por ejemplo:

Texto de consulta	Comentario
Una camioneta amarilla aparcada junto a un árbol	Correcto
Un vehículo sin conductor, matrícula: CHY67F, clase: camioneta, color: amarillo, posición: Junto a un álamo imponente.	Se parece demasiado a un informe policial

Buenos descriptores que la búsqueda de texto libre tiene muchas posibilidades de entender:

Descriptor	Ejemplo
Clase de objeto	Persona, Coche, Bicicleta, Animal
Color	Amarillo
Meteorología	Soleado
Marcas conocidas (marcas de coches, logotipos)	Camión de UPS

Descriptorios inadecuados:

Descriptor	Ejemplo
Texto	Un cartel en una tienda que dice «Prohibida la entrada a osos bailarines»
Señales emocionales	Un hombre que parece enfadado
Conteo	14 personas paseando por una plaza
Jerga regional	Una aspiradora roja

Moderación de las consultas de búsqueda





Las búsquedas con contenidos insultantes, irrespetuosos o tóxicos pueden bloquearse para mantener un entorno seguro y respetuoso. Nuestro sistema utiliza un modelo de procesamiento del lenguaje natural para evaluar cada consulta de búsqueda, así como una lista personalizada de categorías y palabras prohibidas para mejorar la aplicación de este principio.


Si no está de acuerdo con una palabra bloqueada o desea sugerir un término nuevo, puede hacernos llegar feedback anónimo a través de la interfaz de usuario de la búsqueda inteligente. Nuestro equipo se encargará de revisarlo.

Nota

- La búsqueda de texto libre solo está disponible en inglés.
- La búsqueda de texto libre comprende imágenes fijas. Puede ser difícil obtener buenos resultados utilizando la búsqueda de texto libre para acciones como caerse, correr o robar, porque requieren más contexto.
- La búsqueda de texto libre utiliza imágenes recortadas, por lo que podría no incluir el entorno circundante. Es posible que obtenga resultados menos precisos si utiliza descriptorios de escena como ciudad, urbano, parque, jardín, lago y playa.
- Para obtener información más detallada sobre la función de texto libre, también sobre sus limitaciones y las prácticas recomendadas, consulte nuestro documento técnico *Free text search in AXIS Camera Station Pro (Búsqueda con texto libre en AXIS Camera Station Pro)*.

Resultados de búsqueda inteligente

	Para agrupar detecciones que probablemente pertenezcan al mismo evento, puede agruparlas en intervalos de tiempo. Seleccione un intervalo en el menú desplegable  .
Últimos primero 	La búsqueda inteligente 2 muestra los resultados de la búsqueda en orden descendente con las últimas detecciones primero. Haga clic en  Oldest first

	(Más antiguos primero) para mostrar las detecciones más viejas primero.
Confidence level (Nivel de confianza)	Para filtrar aún más los resultados de la búsqueda, haga clic en Confidence level (Nivel de confianza) y defina el nivel de confianza. Una confianza elevada ignora las clasificaciones inciertas.
Columnas 	Para cambiar el tamaño de las imágenes en miniatura en el resultado de la búsqueda, haga clic en Columns (Columnas) y cambie el número de columnas.
Detection view (Vista de detección)	Para mostrar una vista recortada del objeto detectado como miniatura, seleccione Detection view (Vista de detección) .

Limitations (Limitaciones)

- Búsqueda inteligente 2 solo admite el área de visión primaria (no recortada).
- Búsqueda inteligente 2 solo admite modos de captura sin recorte.
- El uso de Búsqueda inteligente 2 con flujos de cámara reflejados y rotados para dispositivos con ARTPEC-7 o superior y versión de firmware inferior a 10.6 puede causar algunos problemas.
- Una latencia de red alta o muy variable puede provocar problemas de sincronización de la hora y afectar a la clasificación de las detecciones basada en metadatos de análisis.
- La clasificación de tipos de objetos y la precisión de la detección se ven afectadas negativamente por la baja calidad de imagen debido a un elevado nivel de compresión, por condiciones meteorológicas tales como lluvias fuertes o nieve y por cámaras de baja resolución, gran distorsión, gran campo de visión o con vibraciones excesivas.
- Es posible que la búsqueda inteligente 2 no detecte objetos pequeños y distantes.
- La clasificación del color no funciona en la oscuridad ni con iluminación de infrarrojos.
- Las cámaras corporales no son compatibles.
- El radar solo puede detectar personas y otros vehículos. No es posible habilitar la clasificación del servidor de fondo para el radar.
- La clasificación de objetos tiene un comportamiento desconocido en las cámaras térmicas.
- Búsqueda inteligente 2 no detectará objetos en movimiento cuando se cambia una posición predefinida PTZ y durante un periodo de recalibración corto después del cambio de posición.
- Los filtros de cruce de línea y área no siguen los cambios de posición de PTZ.




Búsqueda de datos

La búsqueda de datos le permite encontrar datos de una fuente externa. Una fuente es un sistema o dispositivo que genera datos que puede utilizar para saber más sobre lo que sucedió en un evento. Consulte *Fuentes de datos externos*, on page 73 para obtener más información. Aquí están algunos ejemplos:


- Un evento generado por un sistema de control de acceso.
- Una matrícula registrada por AXIS License Plate Verifier.
- Una velocidad capturada por AXIS Speed Monitor.

Para cambiar el tiempo que AXIS Camera Station Pro guarda los datos externos, vaya a **Configuration > Server > Settings > External data (Configuración > Servidor > Ajustes > Datos externos)**.

Para buscar datos:

1. Haga clic en  y seleccione **Data search (Búsqueda de datos)**.
2. Seleccione un intervalo de búsqueda .
3. Seleccione un tipo de origen de datos de la lista desplegable.
4. Haga clic en las opciones de búsqueda  y aplique los filtros adicionales. Los filtros pueden variar en función del tipo de origen de datos.
5. Introduzca cualquier palabra clave en el campo de búsqueda. Vea *Optimizar la búsqueda*, on page 44.
6. Haga clic en **Buscar**.

La búsqueda de datos marca los datos generados a partir de la fuente si la ha configurado con una vista. Haga clic en los datos de la lista para ir a la grabación asociada con el evento.

Intervalo de tiempo 	
En directo	Para buscar datos en tiempo real, seleccione Live (En vivo) como el intervalo de tiempo. La búsqueda de datos puede mostrar un máximo de 3000 eventos de datos en vivo. El modo en vivo no admite operadores de búsqueda.
Última hora – Últimos 30 días	Para buscar datos dentro un intervalo de tiempo preestablecido, seleccione una de las opciones disponibles: última hora, 4 horas, 12 horas, 24 horas, 48 horas, 7 días o 30 días.
Personalizar	Para buscar datos dentro de un rango de tiempo específico, seleccione Custom (Personalizado) y determine una fecha y hora de inicio y finalización.

Puede filtrar el resultado de la búsqueda en distintos tipos de orígenes:

Tipo de origen de datos	
Todos los datos	Esta opción incluye datos de orígenes externos y componentes.

Control de acceso	El control de acceso es un ejemplo de un componente que genera datos. Utilice esta opción si desea incluir los datos solo de este componente específico. El control de acceso le permite filtrar por puertas y zonas, titulares de tarjeta y tipos de eventos.
Tercero	Utilice esta opción si desea incluir datos de orígenes de terceros distintos a los componentes configurados.

Dependiendo de la fuente de datos, puede obtener diferentes elementos en el resultado de su búsqueda. Aquí están algunos ejemplos:

Resultados de búsqueda	
Servidor	El servidor al que se envían los datos del evento. Solo está disponible al conectarse con varios servidores.
Establecimiento	El nombre de la puerta y el nombre del controlador de puerta con dirección IP.
Introducir velocidad	La velocidad (kilómetros por hora o millas por hora) cuando el objeto entra en la zona de detección de movimiento por radar (RMD).
Clasificación	La clasificación del objeto. Por ejemplo: Vehículos.

Haga clic en **Download search result (Descargar resultados de búsqueda)** para exportar los resultados de la búsqueda a un archivo PDF o de texto. Puede reorganizar las columnas y ajustar el ancho de las mismas en el resultado de la búsqueda para mejorar el diseño de la tabla en el PDF generado. El PDF incluye hasta 10 columnas.


Optimizar la búsqueda

Puede utilizar los siguientes operadores de búsqueda para obtener resultados más precisos:

Utilice las comillas " " para encontrar coincidencias exactas de las palabras clave.	<ul style="list-style-type: none"> Una búsqueda con "door 1" muestra los resultados que contienen "door 1" (puerta 1). Una búsqueda con door 1 muestra los resultados que contienen "door" y "1" (puerta y 1).
Utilice AND para buscar las coincidencias que contienen todas las palabras clave.	<ul style="list-style-type: none"> Una búsqueda con door AND 1 muestra los resultados que contienen "door" y "1" (puerta y 1). Una búsqueda con "door 1" AND "door forced open" muestra los resultados que contienen "door 1" (puerta 1) y "door forced open" (apertura forzada de puerta).
Utilice OR o para buscar las coincidencias que contienen cualquier palabra clave.	<ul style="list-style-type: none"> Una búsqueda con "door 1" OR "door 2" muestra los resultados que contienen "door 1" o "door 2" (puerta 1 o puerta 2). Una búsqueda con door 1 OR door 2 muestra los resultados que contienen "door" o "1" o "2" (puerta o 1 o 2).
Utilice paréntesis () junto con AND o OR.	<ul style="list-style-type: none"> Una búsqueda con (door 1 OR door 2) AND "Door forced open" muestra los

	<p>resultados que contienen uno de los siguientes elementos:</p> <ul style="list-style-type: none"> - "puerta 1" y "apertura forzada de puerta" - "puerta 2" y "apertura forzada de puerta" • Una búsqueda con <code>door 1 AND (door (forced open OR open too long))</code> muestra los resultados que contienen uno de los siguientes elementos: <ul style="list-style-type: none"> - "puerta 1" y "apertura forzada de puerta" - "puerta 1" y "puerta abierta durante demasiado tiempo"
<p>Utilice <code>></code>, <code>>=</code>, <code><</code> o <code><=</code> para filtrar los números de una columna específica.</p>	<ul style="list-style-type: none"> • Una búsqueda con <code>[Max speed] > 28</code> muestra los resultados que contienen un número superior a 28 en la columna de velocidad máxima. • Una búsqueda con <code>[Average speed] <= 28</code> muestra los resultados que contienen un número inferior o igual a 28 en la columna de velocidad media.
<p>Utilice <code>CONTAINS</code> para buscar texto en una columna específica.</p>	<ul style="list-style-type: none"> • Una búsqueda para <code>[Cardholder] CONTAINS Oscar</code> muestra datos donde "Óscar" está en la columna de titular de tarjeta. • Una búsqueda con <code>[Door] CONTAINS "door 1"</code> muestra datos donde "door 1" (puerta 1) está en la columna de puerta.
<p>Use <code>=</code> para las coincidencias exactas de una columna específica</p>	<p>Una búsqueda con <code>[CardholderId] = ABC123</code> muestra las coincidencias de "ABC123" en la columna "Cardholder" (Titular de tarjeta).</p>

Configuración

En la pestaña Configuration (Configuración) puede gestionar y mantener los dispositivos conectados y contiene ajustes para el cliente y los servidores. Hacer clic en  y seleccione **Configuration (Configuración)** para abrir la pestaña Configuration (Configuración).

Configuración de dispositivos

En AXIS Camera Station Pro, un dispositivo es un producto de red con una dirección IP. Una cámara es una fuente de vídeo, como una cámara de red o a un puerto de vídeo (con una cámara analógica conectada) en un codificador de vídeo multipuerto. Por ejemplo, un codificador de vídeo de 4 puertos es un dispositivo con cuatro cámaras.

Nota

- AXIS Camera Station Pro solo admite dispositivos con direcciones IPv4.
- Algunos codificadores de vídeo tienen una dirección IP para cada puerto de vídeo. En este caso, AXIS Camera Station Pro trata cada puerto de vídeo como un dispositivo con una cámara.

En AXIS Camera Station Pro, un dispositivo puede ser:

- una cámara de red
- un codificador de vídeo con uno o más puertos de vídeo
- un dispositivo auxiliar que no sea una cámara, por ejemplo, un dispositivo de audio de E/S, un altavoz de red o un controlador de puerta
- un intercomunicador

Puede realizar las siguientes acciones en los dispositivos:

- Agregar cámaras y dispositivos sin capacidades de vídeo. *Vea Agregar dispositivos.*
- Editar las preferencias de las cámaras conectadas. *Vea Cámaras.*
- Editar las preferencias de dispositivos que no sean cámaras. *Vea Otros dispositivos.*
- Editar perfiles de flujo en cuanto a resolución, formato, etc. *Vea Perfiles de transmisión.*
- Modificar los ajustes de imagen en tiempo real. *Vea Configuración de imagen.*
- Agregar o eliminar posiciones predefinidas de PTZ. *Vea Posiciones predefinidas de PTZ.*
- Gestione y mantenga conectados los dispositivos. *Vea Gestión de dispositivos.*
- Gestione fuentes de datos externos. *Vea Fuentes de datos externos, on page 73.*

Agregar dispositivos

Nota

- El sistema considera las áreas de visión como cámaras individuales. Debe crear áreas de visión en la cámara antes de usarlas. *Vea Uso de áreas de visión.*
 - Al agregar un dispositivo, el dispositivo sincroniza su hora con el servidor de AXIS Camera Station Pro.
 - Le recomendamos que no utilice caracteres especiales como å, ä y ö en el nombre de host de un dispositivo.
1. Localice dispositivos, transmisiones de vídeo o vídeos pregrabados.
 - *Buscar dispositivos, on page 48*
 - *Encuentre sus transmisiones de vídeo, on page 48*
 - *Buscar vídeos pregrabados, on page 49*
 2. *Agregar dispositivos, transmisiones de vídeo o vídeos pregrabados, on page 49*

Debe resolver cualquier problema que se muestre en la columna de estado del dispositivo antes de poder agregar un dispositivo.

(vacío)	Si no hay ningún estado, puede agregar el dispositivo al AXIS Camera Station Pro.
Communicating (Comunicando)	AXIS Camera Station Pro servidor que intenta acceder al dispositivo.
Device certificate not trusted (El certificado del dispositivo no es de confianza)	AXIS Camera Station Pro no puede verificar que el certificado HTTPS del dispositivo está firmado por un emisor de confianza. Haga clic en el enlace para emitir un nuevo certificado HTTPS o indicar a AXIS Camera Station Pro que confíe en el existente.
La autoridad de certificación ha caducado	La autoridad de certificación que emitió el certificado del dispositivo ha dejado de ser válida. Haga clic en el enlace para emitir un nuevo certificado HTTPS o indicar a AXIS Camera Station Pro que confíe en el existente.
Discrepancia de dirección en el certificado del dispositivo	La dirección del dispositivo no coincide con la indicada en el certificado. Haga clic en el enlace para emitir un nuevo certificado HTTPS o indicar a AXIS Camera Station Pro que confíe en el existente.
Error de comunicación	AXIS Camera Station Pro no se puede contactar con el dispositivo.
Introducir contraseña	AXIS Camera Station Pro no sabe qué credenciales utilizar para acceder al dispositivo. Haga clic en el enlace para introducir un nombre de usuario y contraseña para una cuenta de administrador del dispositivo. De forma predeterminada, AXIS Camera Station Pro utilizará el nombre de usuario y la contraseña para todos los dispositivos en los que exista el usuario.
Configurar contraseña	La contraseña y la cuenta root no están configuradas o el dispositivo sigue utilizando la contraseña predeterminada. Haga clic en el enlace para definir la contraseña de usuario root. <ul style="list-style-type: none"> • Introduzca su contraseña o haga clic en Generate (Generar) para obtener una contraseña. Le recomendamos que muestre la contraseña generada y realice una copia. • Seleccione esta opción para utilizar esta contraseña en todos los dispositivos que tengan el estado <code>Set password</code>.
Modelo no admitido	AXIS Camera Station Pro no admite el modelo de dispositivo.
Firmware obsoleto	El firmware del dispositivo es antiguo y debe actualizarlo antes de poder agregar el dispositivo.
Dispositivo defectuoso	Los parámetros del dispositivo recuperados por AXIS Camera Station Pro están dañados.
Ajustar orientación de inclinación	Haga clic para seleccionar la orientación de inclinación Techo, Pared o Sobremesa, en función de cómo se ha montado la cámara. La orientación de

	inclinación es un ajuste necesario para algunos modelos de cámara.
Dispositivo ONVIF no compatible	AXIS Camera Station Pro no es compatible con este dispositivo de terceros.
Dispositivo no compatible	AXIS Camera Station Pro No es compatible con este tipo de dispositivo.

Nota

AXIS Camera Station Pro emite los nuevos certificados HTTPS, que se renuevan automáticamente.

Buscar dispositivos

Para buscar dispositivos que no se muestran en la lista:

1. Vaya a **Configuración > Dispositivos > Agregar dispositivos**.
2. Haga clic en **Cancelar** para detener la búsqueda de red activa.
3. Haga clic en **Manual search (Búsqueda manual)**.
4. Para encontrar varios dispositivos en uno o más rangos IP:
 - 4.1. Seleccione **Search one or more IP ranges (Buscar uno o varios rangos de direcciones IP)**.
 - 4.2. Introduzca el intervalo de IP. Por ejemplo: 192.168.10.*, 192.168.20-22.*, 192.168.30.0-50
 - Utilice un carácter comodín para todas las direcciones de un grupo.
 - Utilice un guion para un rango de direcciones.
 - Use una coma para separar varios rangos.
 - 4.1. Para cambiar el puerto predeterminado 80, introduzca el intervalo de puertos. Por ejemplo: 80, 1080-1090
 - Utilice un guion para un rango de puertos.
 - Use una coma para separar varios rangos.
 - 4.1. Haga clic en **Buscar**.
5. Para encontrar uno o varios dispositivos específicos:
 - 5.1. Seleccione **Enter one or more hostnames or IP addresses (Introducir uno o varios hostnames o direcciones IP)**.
 - 5.2. Introduzca los nombres de host o las direcciones IP separados por coma.
 - 5.3. Haga clic en **Buscar**.
6. Haga clic en **Aceptar**.

Encuentre sus transmisiones de vídeo

Puede agregar transmisiones de vídeo compatibles con lo siguiente:

- Protocolo: RTSP, HTTP, HTTPS
- Codificador de vídeo: M-JPEG para HTTP y HTTPS, H.264 for RTSP
- Codificación de audio: AAC y G.711 para RTSP

Esquemas URL de transmisión de vídeo compatibles:

- `rtsp://<address>:<port>/<path>`
 Por ejemplo: `rtsp://<address>:554/axis-media/media.amp`
- `http://<address>:80/<path>`
 Por ejemplo: `http://<address>:80/axis-cgi/mjpg/video.cgi?date=1&clock=1&resolution=1920x1080`

- `https://<address>:443/<path>`
Por ejemplo: `https://<address>:443/axis-cgi/mjpg/video.cgi?date=1&clock=1&resolution=1920x1080`
1. Vaya a **Configuración > Dispositivos > Agregar dispositivos**.
 2. Haga clic en **Enter stream URLs (Introducir URL de transmisión)** e introduzca una o varias URL separadas por comas.
 3. Haga clic en **Añadir**.

Buscar vídeos pregrabados

Puede agregar vídeos pregrabados en formato .mkv a AXIS Camera Station Pro.

Requisitos del archivo .mkv:

- Codificador de vídeo: M-JPEG, H.264, H.265
 - Codificación de audio: AAC
1. Cree una carpeta **PrerecordedVideos** en `C:\ProgramData\Axis Communications\AXIS Camera Station Server`.
 2. Agregue un archivo .mkv a la carpeta.
 3. Para la corrección esférica de vídeo pregrabado, agregue a la carpeta un archivo .dewarp con el mismo nombre que el archivo .mkv. Consulte *Configuración de imagen, on page 59* para obtener más información.
 4. Vaya a **Configuration > Devices > Add devices (Configuración > Dispositivos > Agregar dispositivos)** y active **Include pre-recorded video (Incluir vídeo pregrabado)**. Encontrará el vídeo pregrabado y varios vídeos pregrabados proporcionados por el sistema.

Agregar dispositivos, transmisiones de vídeo o vídeos pregrabados

1. En un sistema multiservidor, seleccione un servidor de la lista desplegable **Selected server (Servidor seleccionado)**.
2. Vaya a **Configuración > Dispositivos > Agregar dispositivos**.
3. Si quiere cambiar el nombre del dispositivo, haga clic en el nombre de la lista e introduzca un nuevo nombre.
4. Seleccione los dispositivos, transmisiones de vídeo o vídeos pregrabados. Haga clic en **Añadir**.
5. Elija si desea utilizar nombres de host en lugar de IP cuando sea posible para los dispositivos.
6. Elija **Quick configuration (Configuración rápida)** si solo desea configurar los ajustes básicos. Si está importando un proyecto de Site Designer, consulte *Importar proyectos del espacio de diseño*.
7. Elija sus preferencias en materia de **Retention time (Tiempo de conservación)**, **Recording storage (Almacenamiento de grabaciones)**, y **Recording method (Método de grabación)**.

Nota

Si elige la opción de almacenamiento de grabaciones **Automatic (Automático)**, a cada cámara se le asignará un almacenamiento con al menos 32 GB de capacidad en una unidad ajena al SO, siempre que sea posible. El sistema selecciona automáticamente los almacenamientos con al menos 15 GB de espacio disponible, seguidos de los almacenamientos con menos cámaras configuradas para grabar en ellos y de cualquier almacenamiento ya instalado en AXIS Camera Station Pro.

8. Haga clic en **Install (Instalar)**. AXIS Camera Station Pro activa automáticamente HTTPS en los dispositivos que lo admiten.

Importar proyectos del espacio de diseño

AXIS Site Designer es una herramienta de diseño online que le ayuda a configurar un sitio con productos y accesorios de Axis.

Si ha creado una instalación en AXIS Site Designer, puede importar los ajustes del proyecto a AXIS Camera Station Pro. Puede acceder al proyecto utilizando un código de acceso o un archivo de instalación de Site Designer descargado.

Para importar un proyecto de diseñador de instalación a AXIS Camera Station Pro:

1. Genere un código de acceso al proyecto del espacio de diseño o descargue un archivo de proyecto.
 - 1.1. Inicie sesión en <http://sitedesigner.axis.com> con su cuenta MyAxis.
 - 1.2. Seleccione un proyecto y vaya a la página correspondiente.
 - 1.3. Haga clic en **Share (Compartir)**.
 - 1.4. Haga clic en **Generate code (Generar código)** si el servidor de AXIS Camera Station Pro tiene conexión a Internet. También puede hacer clic en **Download settings file (Descargar archivo de ajustes)** si el servidor no tiene conexión a Internet.
2. En el cliente de AXIS Camera Station Pro, vaya a **Configuration > Devices > Add devices (Configuración > Dispositivos > Agregar dispositivos)**.
3. Seleccione las cámaras y haga clic en **Agregar**.
4. Seleccione **Configuración del Espacio de diseño** y haga clic en **Siguiente**.
5. Seleccione **Código de acceso** e introduzca el código de acceso. También puede seleccionar **Choose file (Seleccionar archivo)** y buscar el archivo de configuración de Site Designer que haya descargado.
6. Haga clic en **Importar**. En la importación, AXIS Camera Station Pro intenta hacer coincidir el proyecto de Site Designer con las cámaras seleccionadas por la dirección IP o el nombre del producto. Puede seleccionar la cámara correcta en el menú desplegable si no se produce la coincidencia.
7. Haga clic en **Instalar**.

AXIS Camera Station Pro importa las siguientes configuraciones del proyecto de Site Designer:

	Codificadores, codificadores de vídeo, controladores de puerta, detectores de radar y altavoces	Cámaras, intercomunicadores y la serie F/AF
Programaciones con nombre y franjas horarias	✓	✓
Mapas con nombre, color del icono, ubicación del icono y nombre del elemento	✓	✓
Nombre	✓	✓
Descripción	✓	✓
Grabación activada por movimiento: perfil de grabación y programación con velocidad de fotogramas, resolución, codificación de vídeo y compresión		✓
Grabación continua: perfil de grabación y programación con velocidad de fotogramas, resolución, codificación de vídeo y compresión		✓
Potencia de Zipstream		✓

	Codificadores, codificadores de vídeo, controladores de puerta, detectores de radar y altavoces	Cámaras, intercomunicadores y la serie F/AF
Ajustes de audio para vista en directo y grabaciones		✓
Tiempo de conservación de las grabaciones		✓

Nota

- Si ha definido solo uno de los perfiles de grabación o si hay dos perfiles de grabación idénticos en el proyecto de Site Designer, AXIS Camera Station Pro establece el perfil en medio.
- Si definió ambos perfiles de grabación en el proyecto de Site Designer, AXIS Camera Station Pro establece el perfil de grabación continua en medio y la grabación activada por movimiento en alto.
- AXIS Camera Station Pro optimiza la relación de aspecto, lo que significa que la resolución puede diferir entre la importación y el proyecto de Site Designer.
- AXIS Camera Station Pro puede definir los ajustes de audio si el dispositivo dispone de un micrófono integrado o altavoz. Para utilizar un dispositivo de audio externo, habilítelo manualmente después de instalarlo.
- AXIS Camera Station Pro no aplica la configuración de audio a los intercomunicadores incluso si la configuración en Site Designer es diferente. En los intercomunicadores, el audio siempre está activado solo en vista en vivo.



Agregar dispositivos de terceros

Es posible agregar dispositivos de terceros a AXIS Camera Station Pro del mismo modo que se agregan productos Axis. Vea *Agregar dispositivos*.

Nota

También puede agregar dispositivos de terceros como flujos de vídeo en AXIS Camera Station Pro. Vea *Encuentre sus transmisiones de vídeo, on page 48*.

Para obtener información sobre la compatibilidad de dispositivos de terceros, consulte la *documentación técnica más reciente*.

AXIS Camera Station Pro admite las siguientes funciones de dispositivos de terceros según las normas IEC62676-2-31 e IEC62676-2-32:

- Detección de cámaras
- Codificador de vídeo: M-JPEG, H.264
- Codificaciones de audio: G.711 (unidireccional, del dispositivo a AXIS Camera Station Pro)
- Un perfil de vídeo por cámara
- Vista en vivo
- Grabaciones manuales y continuas
- Reproducción
- Exportaciones de grabaciones

- Activadores de eventos del dispositivo
- PTZ

Uso de áreas de visión

Algunos modelos de cámara admiten áreas de visión. AXIS Camera Station Pro muestra las áreas de visión como cámaras individuales en la página **Add devices (Agregar dispositivos)**. Vea *Agregar dispositivos*.

Nota

- Todas las áreas de visión en una cámara de red se cuentan como una cámara en el número total de cámaras que permite la licencia de AXIS Camera Station Pro.
- La cantidad de cámaras que puede agregar depende de la licencia.
- Cada licencia de AXIS Camera Station Pro permite un número determinado de cámaras.


Para usar áreas de visión en AXIS Camera Station Pro, primero debe habilitarlas en la cámara:

1. Vaya a **Configuración > Dispositivos > Cámaras**.
2. Seleccione la cámara y haga clic en el enlace de la columna Dirección.
3. En la página de configuración de la cámara, introduzca el nombre de usuario y la contraseña para iniciar sesión.
4. Haga clic en **Help (Ayuda)** para obtener las instrucciones sobre dónde encontrar el ajuste, ya que difiere en función del modelo de cámara y del firmware.

Sustituir un dispositivo

Puede sustituir un dispositivo y mantener la configuración existente y las grabaciones. El número de transmisiones de vídeo configuradas en la nueva cámara debe ser el mismo que para la antigua.

Para sustituir un dispositivo:

1. Si el dispositivo que va a sustituir utiliza almacenamiento en la nube, vaya a **Cloud storage (Almacenamiento en la nube)** en My Systems y desactívelo en ese dispositivo en concreto.
2. Abra una pestaña **Configuration (Configuración)** y vaya a **Devices (Dispositivos) > Management (Gestión)**.
3. Seleccione el dispositivo que desee sustituir y haga clic en .
4. En el cuadro de diálogo **Replace device (Sustituir dispositivo)**, seleccione el dispositivo con el que desea sustituir el antiguo.
5. Haga clic en **Finish (Finalizar)**.
6. El cuadro de diálogo **Replaced device (Dispositivo sustituido)** aparece para confirmar que el dispositivo se ha sustituido correctamente. Haga clic en **OK**.
7. Si el dispositivo que ha sustituido utilizaba almacenamiento en la nube, reinicie el servicio en el servidor AXIS Camera Station Pro y active el almacenamiento en la nube en ese dispositivo en My Systems. Consulte *Activar el almacenamiento en la nube para cámaras individuales*.
8. Compruebe la configuración del nuevo dispositivo para asegurarse de que los ajustes sean correctos y de que el dispositivo funcione normalmente. Si procede:
 - 8.1. Reconfigure las posiciones predefinidas de PTZ en el dispositivo.
 - 8.2. Agregue cualquier puerto de E/S eliminado y actualice las reglas de acción relacionadas.
 - 8.3. Vuelva a configurar los ajustes de movimiento si la cámara antigua utilizaba la detección de movimiento en el vídeo integrada en lugar de la aplicación ACAP de detección de movimiento en el vídeo.

- 8.4. Inserte una tarjeta SD o desactive la opción **Failover recording (Grabación a prueba de fallos)** en los ajustes de selección de almacenamiento si la cámara antigua utilizaba la grabación a prueba de fallos.

Cámaras

Vaya a **Configuration > Devices > Cameras (Configuración > Dispositivos > Cámaras)** para ver la lista de todas las cámaras agregadas al sistema.

En esta página, podrá:

- Haga clic en la dirección de una cámara para abrir su interfaz web. Esto requiere que no haya NAT ni cortafuegos entre el cliente de AXIS Camera Station Pro y el dispositivo.
- Edite los ajustes de la cámara. Vea *Editar ajustes de la cámara*.
- Eliminar cámaras. De este modo, AXIS Camera Station Pro elimina todas las grabaciones, incluidas las bloqueadas, asociadas con las cámaras eliminadas.

Editar ajustes de la cámara

Para editar ajustes de la cámara:

1. Vaya a **Configuración > Dispositivos > Cámaras**.
2. Seleccione una cámara y haga clic en **Editar**.

<p>Habilitado</p>	<p>Para evitar la grabación y visualización de la transmisión de video, anule la selección de Enabled (Activado). Se pueden seguir configurando las grabaciones y la visualización en directo.</p>
<p>Canal</p>	<p>Si Channel (Canal) está disponible para codificadores de video multipuerto, seleccione el número de puerto.</p> <p>Si Channel (Canal) está disponible para las áreas de visión, seleccione el número correspondiente al área de visualización.</p>

Otros dispositivos

Vaya a **Configuration > Devices > Other devices (Configuración > Dispositivos > Otros dispositivos)** para ver una lista de dispositivos sin capacidades de video. La lista incluye controladores de puertas, dispositivos de audio y módulos de E/S.

Para obtener más información sobre los productos compatibles, vaya a www.axis.com y consulte *Usar audio desde otros dispositivos*.

En esta página, podrá:

- Haga clic en la dirección de un dispositivo para abrir su interfaz web. Esto requiere que no haya NAT ni cortafuegos entre el cliente de AXIS Camera Station Pro y el dispositivo.
- Edite los ajustes del dispositivo, como el nombre, la dirección y la contraseña.
- Eliminar dispositivos.

Editar otros ajustes del dispositivo

Para cambiar el nombre de un dispositivo que no sea una cámara:

1. Vaya a **Configuración > Dispositivos > Otros dispositivos**.
2. Seleccione un dispositivo y haga clic en **Editar**.

- introduzca el nuevo nombre del dispositivo.

Perfiles de transmisión

Un perfil de transmisión es un grupo de configuraciones que afectan la transmisión de vídeo, como la resolución, el formato de vídeo, la velocidad de fotogramas y la compresión. Vaya a **Configuration > Devices > Stream profiles** (Configuración > Dispositivos > perfiles de flujo) para abrir la página de perfiles de flujo. La página muestra una lista de todas las cámaras.

Están disponibles los siguientes perfiles en los ajustes de visualización en directo y grabaciones:

Alto – optimizado para la mayor calidad y resolución.

Medio – optimizado para equilibrar la calidad y el rendimiento.

Bajo – optimizado para el rendimiento.

Nota

El perfil de transmisión está configurado en **Automatic (Automático)** en Vista en vivo y grabaciones de forma predeterminada, lo que significa que el perfil de transmisión cambia automáticamente a **High (Alto)**, **Medium (Medio)** o **Low (Bajo)** dependiendo del tamaño disponible para la transmisión de vídeo.

Edit stream profiles (Editar perfiles de flujo)

- Vaya a **Configuration > Devices > Stream profiles** (Configuración > Dispositivos > Perfiles de transmisión) y seleccione las cámaras que desea configurar.
- En **Video profiles (Perfiles de vídeo)**, configure la resolución, el formato de vídeo, la velocidad de fotogramas y la compresión.
- En **Audio**, configure el micrófono y el altavoz.
- En **Advanced (Avanzado)**, configure datos analíticos, transmisión FFmpeg, indicadores de objetos de seguimiento automático PTZ y configuraciones de transmisión personalizadas. Estas configuraciones no están disponibles para todos los productos.
- Haga clic en **Aplicar**.

Perfiles de vídeo

<p>Codificador</p>	<ul style="list-style-type: none"> Las opciones disponibles dependen de las configuraciones del codificador de vídeo del dispositivo. Esta opción solo está disponible para dispositivos de terceros. Solo puede usar una configuración de codificador de vídeo para un perfil de vídeo. Si el dispositivo solo tiene una configuración de codificador, solo está disponible el perfil Medium (Medio).
<p>Resolución</p>	<p>Las opciones disponibles dependen del modelo de cámara. Una resolución superior proporciona una imagen con más detalles pero requiere más ancho de banda y espacio de almacenamiento.</p>
<p>Formatear</p>	<p>Las opciones disponibles dependen del modelo de cámara. La mayoría de las cámaras son compatibles con H.264 y M-JPEG. H.264 requiere menos ancho de banda y espacio de almacenamiento que M-JPEG. Algunas cámaras también son compatibles con H.265, que ofrece una compresión ligeramente mejor, pero requiere mayor potencia de procesamiento. Nuestras cámaras de última generación son</p>

	<p>compatibles con AV1, que ofrece una buena compresión y una serie de nuevas funciones, como superposiciones alternables.</p> <p>Obtenga más información al respecto en la <i>página de productos AV1</i>. Para comprobar si su cámara es compatible con AV1, consulte la <i>página de cámaras compatibles</i>.</p>
Velocidad de fotogramas	La velocidad de imágenes real depende del modelo de cámara, las condiciones de la red y la configuración del equipo.
Compresión	Las compresiones menores mejoran la calidad de la imagen pero requieren un ancho de banda y espacio de almacenamiento mayores.

Nota

- Solo las cámaras con el firmware 5 o superior aparecen en las listas desplegadas de audio.
- Si más de 5 cámaras usan la misma fuente de audio, la cámara fuente podría sobrecargarse y funcionar con menor eficiencia.

Zipstream

Potencia	La intensidad de Zipstream determina el nivel de reducción de la tasa de bits en una transmisión H.264 o H.265 en tiempo real. Esta opción solo está disponible en los dispositivos Axis compatibles con Zipstream.	Configuración predeterminada	Use el ajuste de Zipstream configurado en la página de la interfaz web del dispositivo.
		Apagado	Ninguno
		Bajo	Sin efectos visibles en la mayoría de las escenas
		Medio	Efectos visibles en algunas escenas: menos ruido y un nivel de detalle ligeramente más bajo en regiones de poco interés
		Alto	Efectos visibles en muchas escenas: menos ruido y un nivel de detalle más bajo en regiones de poco interés
		Más alto	Efectos visibles incluso en más escenas: menos ruido y un nivel de detalle más bajo en regiones de poco interés
		Extremo	Efectos visibles en la mayoría de las escenas: menos ruido y un nivel de detalle más bajo en regiones de poco interés

<p>Optimizar para almacenamiento</p>	<p>Zipstream optimiza la transmisión de video para el almacenamiento mediante el perfil Optimizar para almacenamiento. Optimizar para almacenamiento utiliza herramientas de compresión más avanzadas para ahorrar espacio de almacenamiento adicional en comparación con el ajuste de Zipstream predeterminado. Este perfil puede reducir aún más la velocidad de bits incluso para las escenas con mucho movimiento.</p> <ul style="list-style-type: none"> • El formato asf no es compatible con los fotogramas B que utiliza esta característica. • Esta característica no afecta a los vídeos grabados en grabadores de la serie AXIS S30. • Esta característica requiere AXIS OS 11.7.59 o posterior. 		
---	---	--	--

Audio

<p>Micrófono:</p>	<p>para asociar un micrófono a la cámara, seleccione Built-in microphone or line in (Micrófono integrado o entrada de línea), o el micrófono de otro dispositivo. Vea <i>Usar audio desde otros dispositivos</i>.</p>
<p>Altavoz:</p>	<p>Para asociar un altavoz a la cámara, seleccione Built-in speaker or line out (Altavoz integrado o salida de línea), o el altavoz de otro dispositivo. Utilice un micrófono conectado al ordenador para realizar anuncios. Vea <i>Usar audio desde otros dispositivos</i>.</p>
<p>Utilizar micrófono para:</p>	<p>permite habilitar el audio del micrófono para una o dos transmisiones. Es posible habilitar el audio para la visualización en directo y las grabaciones, solo la para visualización en directo, o solo para las grabaciones.</p>

Al conectarse a AXIS Audio Manager Pro, también puede seleccionar dispositivos de audio del servidor de AXIS Audio Manager Pro como dispositivo de audio asociado a una cámara. Para obtener más información, consulte *Configure AXIS Audio Manager Pro, on page 175*.

Avanzada

<p>Incluya datos de análisis</p>	<p>Para permitir la recopilación de datos que faciliten la búsqueda inteligente durante la transmisión de vídeo, seleccione Include analytics data (Incluir datos de analíticas). Esta opción solo está disponible en los dispositivos de Axis que admiten datos de analíticas. La recopilación de datos para <i>Búsqueda inteligente 1</i> puede traducirse en más latencia en la transmisión del vídeo en directo.</p>
<p>Utilizar FFmpeg</p>	<p>Para mejorar la compatibilidad con dispositivos de terceros, seleccione Use FFmpeg (Utilizar FFmpeg) a fin de habilitar la transmisión de FFmpeg. Esta opción solo está disponible para dispositivos de terceros.</p>
<p>Mostrar indicadores de objetos de autotracking PTZ</p>	<p>Para mostrar los indicadores de objeto detectados por una cámara PTZ durante la visualización en directo, seleccione Show PTZ autotracking object indicators (Mostrar indicadores PTZ de autotracking de objeto) y configure el búfer de transmisión de vídeo en 2000 milisegundos. Esta opción solo está disponible para una cámara PTZ Axis con AXIS PTZ Autotracking configurado. Para conseguir un flujo de datos adecuado que permita configurar AXIS PTZ Autotracking en AXIS Camera Station Pro, consulte <i>Configuración de AXIS PTZ Autotracking</i>.</p>
<p>Personalización de transmisión</p>	<p>Para personalizar la configuración de transmisión para un perfil específico, introduzca la configuración separada por & para el perfil. Por ejemplo, introduzca <code>overlays=off&color=0</code> para ocultar las superposiciones de esa cámara.</p> <p>Los ajustes personalizados anulan los existentes. No incluya información confidencial en los ajustes personalizados.</p>

Para personalizar los ajustes de perfil relativos a la resolución, la velocidad de fotogramas, la compresión, el formato de vídeo y el audio, seleccione la cámara que desee configurar. En el caso de las cámaras del mismo

modelo con las mismas opciones de configuración, es posible configurar varias cámaras simultáneamente. Vea *Ajustes de configuración*.

Para personalizar los ajustes de perfiles para las grabaciones, consulte *Método de grabación*.

Puede limitar la resolución y la velocidad de fotogramas de visualización en directo para reducir el consumo de ancho de banda, por ejemplo, si la conexión entre el cliente de AXIS Camera Station Pro y el servidor de AXIS Camera Station Pro es lenta. Vea Uso de ancho de banda en *Transmisión*.

Usar audio desde otros dispositivos

El audio de un dispositivo auxiliar, que no sea una cámara o de otro tipo puede usarse junto con el vídeo de una cámara de red o codificador de vídeo para el modo visualización en directo o grabación:

1. Agregar el dispositivo que no tiene cámara a AXIS Camera Station Pro. Vea *Agregar dispositivos*.
2. Configure la cámara para que utilice el audio del dispositivo. Vea *Perfiles de transmisión*.
3. Habilite el audio para Visualización en directo o Grabación. Vea *Perfiles de transmisión*.

Puede encontrar los siguientes ejemplos en los *tutoriales de vídeo de AXIS Camera Station Pro*:

- Configurar dispositivos de audio y realizar anuncios en directo
- Crear un botón de acción para reproducir audio manualmente cuando se detecta movimiento
- Reproducir audio automáticamente cuando se detecte movimiento
- Agregar un clip de audio al altavoz y AXIS Camera Station Pro

Configuración de imagen

Puede configurar los ajustes de imagen para las cámaras conectadas a AXIS Camera Station Pro.

Nota

Los cambios en la configuración de la imagen se aplican al instante.

Para configurar los ajustes de imagen:

1. Vaya a **Configuration > Devices > Image configuration (Configuración > Dispositivos > Configuración de imagen)** para ver una lista de todas las cámaras que se han agregado a AXIS Camera Station Pro.
2. Seleccione la cámara, y la transmisión de vídeo se mostrará bajo la lista en tiempo real. Utilice el campo **Introduzca criterio de búsqueda** para encontrar una cámara específica en la lista.
3. Configurar los ajustes de imagen.

Configuración de imagen

Brillo: Ajusta el brillo de la imagen. Los valores más altos proporcionan una imagen más brillante.

Nivel de color: Permite ajustar la saturación del color. Para reducir la saturación de color, seleccione un valor más bajo. El nivel de color 0 produce una imagen en blanco y negro. El valor máximo proporciona la máxima saturación de color.

Nitidez: Permite ajustar la cantidad de nitidez aplicada a la imagen. Si se aumenta la nitidez se podría incrementar el ruido de la imagen, especialmente en situaciones de poca luz. Una nitidez alta podría introducir también imágenes fantasma alrededor de áreas con alto contraste, por ejemplo, bordes pronunciados. Una nitidez inferior reduce el ruido de la imagen, pero proporciona una imagen menos nítida.

Contraste: Permite ajustar el contraste de la imagen.

Balance de blancos: Seleccione la opción de balance de blancos en la lista desplegable. El balance de blancos se utiliza para que los colores de la imagen parezcan iguales independientemente de la temperatura de color de la fuente de luz. Al seleccionar **Automático** o **Auto**, la cámara identifica la fuente de luz y compensa su color automáticamente. Si el resultado no es satisfactorio, seleccione una opción correspondiente al tipo de fuente de luz. Las opciones disponibles dependen del modelo de cámara.

Girar imagen: Permite definir los ángulos de rotación de la imagen.

Rotación de imagen automática: Active esta función para ajustar la rotación de la imagen automáticamente.

Mirror image (Imagen reflejada): Actívela para reflejar la imagen.

Backlight compensation (Compensación de contraluz): Actívela si un punto de luz brillante, por ejemplo una bombilla, provoca que otras zonas de la imagen aparezcan demasiado oscuras.

Dynamic contrast (wide dynamic range) (Contraste dinámico [amplio rango dinámico]): Active el amplio rango dinámico para mejorar la exposición cuando hay un contraste considerable entre las zonas claras y oscuras de una imagen. Utilice la barra deslizante para ajustar el contraste dinámico. En condiciones de retroiluminación intensa, habilite el contraste dinámico. En condiciones de poca luz, deshabilite el contraste dinámico.

Custom dewarp settings (Ajustes personalizados de corrección de aberración esférica): puede importar un archivo .dewarp que contenga los parámetros del objetivo, los centros ópticos y la orientación de inclinación de la cámara. Haga clic en **Reset (Restablecer)** para restablecer los parámetros a sus valores originales.

1. Cree un archivo .dewarp que incluya los siguientes parámetros:
 - **Obligatorio:** RadialDistortionX, RadialDistortionY, RadialDistortionZ y TiltOrientation. Los valores posibles para TiltOrientation son wall, desk y ceiling.
 - **Opcional:** OpticalCenterX y OpticalCenterY. Si desea configurar los centros ópticos, debe incluir los dos parámetros.
2. Haga clic en **Import (Importar)** y navegue hasta el archivo .dewarp.

Lo siguiente es un ejemplo de un archivo .dewarp:

```
RadialDistortionX=-43.970703 RadialDistortionY=29.148499 RadialDistortionZ=715.732193  
TiltOrientation=Desk OpticalCenterX=1296 OpticalCenterY=972
```

Posiciones predefinidas de PTZ

Movimiento horizontal/vertical y zoom (PTZ) es la capacidad de desplazarse horizontalmente (a izquierda y derecha), verticalmente (arriba y abajo) y ampliar y reducir.

Vaya a **Configuración > Dispositivos > Opciones predefinidas de PTZ** y se mostrará una lista de las cámaras que se pueden usar con PTZ. Haga clic en una cámara para ver todos sus ajustes predefinidos disponibles. Haga clic en **Refresh (Actualizar)** para actualizar la lista de valores predefinidos.

Puede usar PTZ con:

- cámaras PTZ, es decir, cámaras con PTZ mecánico incorporado.
- Cámaras fijas en las que se ha activado el PTZ digital
- Cámaras ONVIF compatibles con posiciones predefinidas de PTZ

El PTZ digital se habilita desde la página de configuración de la cámara. Para obtener más información, consulte el Manual de usuario de la cámara. Para abrir la página de configuración, vaya a la página de gestión del dispositivo, seleccione la cámara y haga clic en el enlace de la columna Address (Dirección).

Los preajustes de PTZ se pueden configurar en AXIS Camera Station Pro y en la página de configuración de la cámara. Le recomendamos que configure valores predefinidos de PTZ en AXIS Camera Station Pro.

- Cuando se configura un preajuste PTZ en la página de configuración de la cámara, solo se puede ver la transmisión dentro de la configuración predefinida. Los movimientos PTZ durante la visualización en directo se pueden ver y grabar.
- Cuando se configura un preajuste PTZ en AXIS Camera Station Pro, se puede ver la transmisión completa de la cámara. Los movimientos PTZ durante la visualización en directo no se pueden ver ni grabar.

Nota

PTZ no se puede utilizar si está habilitada la cola de control de la cámara. Para obtener más información acerca de la cola de control y cómo habilitarla y deshabilitarla, consulte el Manual de usuario de la cámara.

Para agregar una posición predefinida:

1. Vaya a **Configuración > Dispositivos > Opciones predefinidas de PTZ** y seleccione una cámara de la lista.
2. Para cámaras con PTZ mecánico, utilice los controles PTZ para desplazar la vista de la cámara a la posición deseada. Para cámaras con PTZ digital, utilice la rueda del ratón para acercar y arrastrar la vista de la cámara hasta la posición deseada.
3. Haga clic en **Agregar** e introduzca un nombre para la nueva opción predefinida.
4. Haga clic en **Aceptar**.

Para eliminar un valor predefinido, seleccione el valor predefinido y haga clic en **Quitar**. Esto eliminará el valor predefinido de AXIS Camera Station Pro y de la cámara.

Gestión de dispositivos

La gestión de dispositivos proporciona las herramientas necesarias para la administración y el mantenimiento de dispositivos conectados a AXIS Camera Station Pro.

Vaya a **Configuración > Dispositivos > Gestión** para abrir la página Gestión de dispositivos.

Si ha configurado la comprobación automática de versiones de firmware más recientes en *Ajustes de actualización del firmware*, on page 123, se muestra un enlace cuando hay nuevas versiones de firmware para los dispositivos. Haga clic en el enlace para actualizar las versiones del firmware. Vea *Actualizar firmware*.

Si ha configurado la comprobación automática de versiones de software más recientes en *Actualizar AXIS Camera Station Pro*, on page 129, se muestra un enlace cuando hay una nueva versión disponible de AXIS Camera Station Pro. Haga clic en el enlace para instalar una nueva versión de AXIS Camera Station Pro.

Aparecerá una lista de los dispositivos añadidos a AXIS Camera Station Pro. Utilice el campo **Introduzca criterio de búsqueda** para buscar dispositivos en la lista. Para ocultar o mostrar columnas, haga clic con el botón derecho en la fila del encabezado y seleccione qué columnas mostrar. Para mostrar las columnas en orden diferente, arrastre y suelte los encabezados.

La lista de dispositivos incluye la siguiente información:

- **Nombre:** El nombre del dispositivo o una serie de todos los nombres de cámaras asociadas si el dispositivo es un codificador de vídeo con varias cámaras conectadas, o una cámara de red con varias áreas de visión.
- **Dirección MAC:** La dirección MAC del dispositivo.
- **Estado:** El estado del dispositivo.
 - **OK (Aceptar):** el estado estándar para una conexión establecida con el dispositivo.
 - **Maintenance (Mantenimiento):** El dispositivo se encuentra en mantenimiento y no se puede acceder temporalmente.
 - **No se puede acceder:** no se puede establecer conexión con el dispositivo.
 - **Not accessible over set hostname (No se puede acceder a través del nombre de host establecido):** No se puede establecer conexión con el dispositivo a través del nombre de host.
 - **Servidor no accesible:** no se puede establecer conexión con el servidor al que está conectado el dispositivo.
 - **Introducir contraseña:** no se establece una conexión con el dispositivo hasta que se introduzcan unas credenciales válidas. Haga clic en el enlace para proporcionar unas credenciales de usuario válidas. Si el dispositivo es compatible con las conexiones cifradas, la contraseña se envía cifrada de forma predeterminada.
 - **Set password (Configurar contraseña):** La contraseña y la cuenta root no están configuradas o el dispositivo sigue utilizando la contraseña predeterminada. Haga clic en el enlace para definir la contraseña de usuario root.

- Escriba su contraseña o haga clic en **Generate (Generar)** para generar automáticamente una contraseña hasta la longitud máxima permitida por el dispositivo. Le recomendamos que muestre la contraseña generada automáticamente y realice una copia.
- Seleccione esta opción para utilizar esta contraseña en todos los dispositivos que tengan el estado `Set password`.
- Seleccione **Enable HTTPS (Habilitar HTTPS)** para habilitar HTTPS si el dispositivo lo admite.
- **Tipo de contraseña: sin cifrado:** no se establece conexión con el dispositivo, ya que el dispositivo se ha conectado anteriormente con una contraseña cifrada. Por motivos de seguridad, AXIS Camera Station Pro no permite el uso de contraseñas no cifradas para dispositivos en los que se hayan utilizado contraseñas cifradas anteriormente. Para dispositivos compatibles con el cifrado, el tipo de conexión se configura en las páginas web de configuración del dispositivo.
- **Certificate error (Error de certificado):** Se ha producido un error con el certificado en el dispositivo.
- **Certificado a punto de caducar:** El certificado en el dispositivo está a punto de caducar.
- **Certificate has expired (El certificado ha caducado):** El certificado en el dispositivo ha caducado.
- **HTTPS certificate not trusted (El certificado HTTPS no es de confianza):** El certificado HTTPS en el dispositivo no es de confianza por AXIS Camera Station Pro. Haga clic el enlace para emitir un nuevo HTTPS certificado.
- **HTTP failed (Fallo en HTTP):** no se puede establecer conexión HTTP con el dispositivo.
- **HTTPS failed (Error de HTTPS):** No se puede establecer conexión HTTPS con el dispositivo.
- **HTTP and HTTPS failed (ping or UDP OK) (Fallo de HTTP y HTTPS [ping o UDP OK]):** No se puede establecer conexión HTTP ni HTTPS con el dispositivo. El dispositivo responde a la comunicación mediante ping y a la comunicación UDP (protocolo de datagrama de usuario).
- **Dirección:** La dirección del dispositivo. Haga clic en el enlace para ir a la página de configuración del dispositivo. Muestra la dirección IP o nombre de host en función de cuál se utilizó al agregar el dispositivo. Vea *Pestaña de configuración del dispositivo, on page 73*.
- **Hostname (Nombre de host):** el nombre de host del dispositivo, si está disponible. Haga clic en el enlace para ir a la página de configuración del dispositivo. El nombre de host que se muestra es el nombre del dominio completo. Vea *Pestaña de configuración del dispositivo, on page 73*.
- **Fabricante:** el fabricante del dispositivo.
- **Modelo:** el modelo del dispositivo.
- **Firmware:** la versión del firmware que utiliza actualmente el dispositivo.
- **DHCP:** si el dispositivo está conectado al servidor mediante DHCP.
- **HTTPS:** El estado de HTTPS del dispositivo. Consulte el estado de HTTPS en *Seguridad, on page 70*.
- **IEEE 802.1X:** El estado de IEEE 802.1X del dispositivo. Consulte el estado de IEEE 802.1X en *Seguridad, on page 70*.
- **Servidor:** El servidor de AXIS Camera Station Pro al que está conectado el dispositivo.
- **Etiquetas:** (ocultas de manera predeterminada) las etiquetas agregadas al dispositivo.
- **Nombre descriptivo UPnP:** (oculto de manera predeterminada) el nombre UPnP. Se trata de un nombre descriptivo usado para facilitar la identificación del dispositivo.

Puede realizar las siguientes acciones en los dispositivos:

- Asignar dirección IP a los dispositivos. Vea *Asignación de una dirección IP*.
- Configurar contraseña para los dispositivos. Vea *Gestión de usuarios*.
- Actualizar el firmware de los dispositivos. Vea *Actualizar firmware*.

- Configurar la fecha y hora de los dispositivos. Vea *Configurar fecha y hora..*
- Reiniciar dispositivos.
- Restablecer la mayoría de los ajustes de los dispositivos, incluida la contraseña, a sus valores predeterminados de fábrica. Los siguientes ajustes no se restablecen: aplicaciones de la cámara cargadas, protocolo de arranque (DHCP o estático), dirección IP estática, router predeterminado, máscara de subred, hora del sistema.


Nota

- Para impedir el acceso no autorizado, recomendamos encarecidamente definir la contraseña después de restaurar un dispositivo.
- Si el dispositivo que va a restablecer utiliza almacenamiento en la nube, vaya a **Cloud storage (Almacenamiento en la nube)** en My Systems y desactívelo en ese dispositivo en concreto antes de restablecerlo. Una vez que se haya restablecido el dispositivo, reinicie el servicio en el AXIS Camera Station Pro servidor y active el almacenamiento en la nube en ese dispositivo en My Systems. Consulte *Activar el almacenamiento en la nube para cámaras individuales.*
- Instalar la aplicación de cámara en dispositivos. Vea *Instalar la aplicación de la cámara.*
- Recargar los dispositivos si se han cambiado los ajustes desde la página de configuración de los dispositivos.
- Configurar dispositivos. Vea *Configuración de dispositivos.*
- Gestión de usuarios. Vea *Gestión de usuarios.*
- Administrar certificados. Vea *Seguridad, on page 70.*
- Recopilar datos de dispositivo. Vea *Recopilar datos de dispositivos.*
- Seleccione esta opción para utilizar la dirección IP o el nombre de host. Vea *Conexión, on page 72.*
- Etiquetar dispositivos. Vea *Etiquetas.*
- Introducir credenciales de dispositivo. Haga clic derecho en un dispositivo y seleccione **Avanzado > Introducir credenciales de dispositivo** para introducir una contraseña para el dispositivo.
- Vaya a la pestaña de configuración del dispositivo y configúrelo. Vea *Pestaña de configuración del dispositivo, on page 73.*

Asignación de una dirección IP

AXIS Camera Station Pro puede asignar una dirección IP a varios dispositivos. Se pueden obtener nuevas direcciones IP automáticamente desde un servidor DHCP o asignarse desde un rango de direcciones IP.

Asignar direcciones IP

1. Vaya a **Configuración > Dispositivos > Gestión** y seleccione los dispositivos que configurar.
2. Haga clic en  o haga clic derecho y seleccione **Assign IP address (Asignar dirección IP)**.
3. Si no se puede configurar alguno de los dispositivos seleccionados, por ejemplo, si no se puede acceder a ellos, aparecerá el cuadro de diálogo de dispositivos no válidos. Haga clic en **Continue (Continuar)** para saltarse los dispositivos que no se puedan configurar.
4. Si selecciona un dispositivo al que asignar una dirección IP, haga clic en **Avanzado** para abrir la página Asignar dirección IP.
5. Seleccione **Obtener automáticamente direcciones IP (DHCP)** para obtener automáticamente las direcciones IP desde un servidor DHCP.
6. Seleccione **Asignar el siguiente rango de direcciones IP** y especifique el rango de IP, la máscara de subred y el router predeterminado.
Para especificar el rango de IP:
 - Usar comodines. Por ejemplo: 192.168.0.* o 10.*.1.*

- Escriba la primera y la última dirección IP separadas por un guión. Por ejemplo: 192.168.0.10-192.168.0.20 (este rango de direcciones se puede abreviar como 192.168.0.10-20) o 10.10-30.1.101
- Combinar comodines y rango. Por ejemplo: 10.10-30.1.*
- Use una coma para separar varios rangos. Por ejemplo: 192.168.0.*,192.168.1.10-192.168.1.20

Nota

Para asignar un rango de direcciones IP, los dispositivos deben estar conectados al mismo servidor de AXIS Camera Station Pro.

7. Haga clic en **Next** (Siguiente).
8. Revise las direcciones IP actuales y las nuevas direcciones IP. Para cambiar la dirección IP para un dispositivo, seleccione el dispositivo y haga clic en **Editar IP**.
 - En la sección Dirección IP actual se mostrarán la dirección IP actual, la máscara de subred y el router predeterminado.
 - Edite las opciones en la sección Nueva dirección IP y haga clic en **Aceptar**.
9. Haga clic en **Finalizar** cuando esté satisfecho con las nuevas direcciones IP.

Configuración de dispositivos

Puede configurar algunos ajustes en varios dispositivos a la vez copiando los ajustes de dispositivo de un equipo o mediante un archivo de configuración.

Nota

Para configurar todos los ajustes en un único dispositivo, vaya a la página de configuración del dispositivo. Vea *Pestaña de configuración del dispositivo, on page 73*.

- Para obtener más información sobre cómo configurar dispositivos, consulte *Métodos de configuración*.
- Para ver información sobre cómo crear un archivo de configuración, consulte *Crear archivo de configuración*.
- Para obtener más información sobre qué opciones se pueden copiar, consulte *Ajustes de configuración*.

Métodos de configuración

Hay distintos métodos de configurar los dispositivos. AXIS Device Management intentará configurar todos los dispositivos de acuerdo con los ajustes del método. Vea *Configuración de dispositivos*.

Utilizar la configuración del dispositivo seleccionado

Nota

Este método solo está disponible para configurar un único dispositivo reutilizando algunos o todos los ajustes existentes.

1. Vaya a **Configuración > Dispositivos > Gestión**.
2. Haga clic con el botón derecho en un dispositivo y seleccione **Configurar dispositivos > Configurar**.
3. Seleccione la configuración que debe aplicarse. Vea *Ajustes de configuración, on page 65*.
4. Haga clic en **Siguiente** para verificar los ajustes que se han de aplicar.
5. Haga clic en **Finalizar** para aplicar los ajustes especificados al dispositivo.

Copiar la configuración de otro dispositivo

1. Vaya a **Configuración > Dispositivos > Gestión**.
2. Haga clic con el botón derecho en los dispositivos y seleccione **Configurar dispositivos > Configurar**. Se pueden seleccionar dispositivos de diferentes modelos y firmware.
3. Haga clic en **Dispositivo** para mostrar dispositivos con configuraciones reutilizables.
4. Seleccione el dispositivo desde el que se copiará la configuración y haga clic en **Aceptar**.

5. Seleccione la configuración que debe aplicarse. Vea *Ajustes de configuración*, on page 65.
6. Haga clic en **Siguiente** para verificar los ajustes que se han de aplicar.
7. Haga clic en **Finalizar** para aplicar los ajustes especificados a los dispositivos.

Utilizar un archivo de configuración

Un archivo de configuración contiene los ajustes de un dispositivo. Se puede utilizar para configurar varios dispositivos a la vez y reconfigurar un dispositivo, por ejemplo si se restablecen los ajustes predeterminados de fábrica del dispositivo. Se puede aplicar un archivo de configuración desde un dispositivo a dispositivos de distinto modelo o con distinto firmware incluso si algunos de los ajustes no existen en todos los dispositivos.

Si algunos ajustes no existen o no se pueden aplicar, el estado de la tarea mostrará un Error en la pestaña Tareas de la parte inferior del cliente de AXIS Camera Station Pro. Haga clic con el botón derecho en la tarea y seleccione **Mostrar** para mostrar información sobre los ajustes que no se han podido aplicar.

Nota

Este método solo lo deberían utilizar usuarios experimentados.

1. Vaya a **Configuración > Dispositivos > Gestión**.
2. Haga clic con el botón derecho en los dispositivos y seleccione **Configurar dispositivos > Configurar**.
3. Haga clic en **Archivo de configuración** y vaya al archivo de configuración. Para obtener información sobre cómo crear un archivo de configuración, consulte *Crear archivo de configuración*, on page 65.
4. Desplácese al archivo .cfg y haga clic en **Abrir**.
5. Haga clic en **Siguiente** para verificar los ajustes que se han de aplicar.
6. Haga clic en **Finalizar** para aplicar los ajustes especificados a los dispositivos.

Crear archivo de configuración

Un archivo de configuración contiene los ajustes de un dispositivo. Estos ajustes se pueden aplicar posteriormente a otros dispositivos. Para ver información sobre cómo usar el archivo de configuración, consulte *Métodos de configuración*.

Los ajustes que se muestran son ajustes del dispositivo a los que se puede acceder mediante la gestión de dispositivos AXIS. Para buscar un ajuste concreto, utilice el campo **Introduzca criterio de búsqueda**.

Para crear un archivo de configuración:

1. Vaya a **Configuración > Dispositivos > Gestión**.
2. Seleccione el dispositivo desde el que crear el archivo de configuración.
3. Haga clic con el botón derecho y seleccione **Configurar dispositivos > Crear archivo de configuración**.
4. Seleccione los ajustes para incluir y cambiar los valores según sea necesario. Vea *Ajustes de configuración*.
5. Haga clic en **Siguiente** para verificar los ajustes.
6. Haga clic en **Finalizar** para crear el archivo de configuración.
7. Haga clic en **Guardar** para guardar los ajustes en un archivo .cfg.

Ajustes de configuración

Al configurar los dispositivos, puede configurar los parámetros, reglas de acción y ajustes adicionales de los dispositivos.

Parámetros

Son parámetros internos del dispositivo que se utilizan para controlar el comportamiento del dispositivo. Para obtener información general sobre los parámetros, consulte el manual del usuario del producto, disponible en www.axis.com

Nota

- Los parámetros solo deben modificarlos usuarios experimentados.
- No todos los parámetros de los dispositivos son accesibles desde AXIS Device Management.

Puede insertar variables en algunos campos de texto. Las variables serán sustituidas por texto antes de que se apliquen a un dispositivo. Para introducir una variable, haga clic derecho en el campo de texto y seleccione:

- **Insertar variable del número de serie del dispositivo:** esta variable se sustituirá con el número de serie del dispositivo al que se aplica el archivo de configuración.
- **Insertar variable de nombre del dispositivo:** esta variable se sustituirá con el nombre del dispositivo utilizado al aplicar el archivo de configuración. El nombre del dispositivo se puede encontrar en la columna Nombre en la página de gestión de dispositivos. Para cambiar el nombre de un dispositivo, vaya a la página Cámaras u Otros dispositivos.
- **Insertar variable de nombre del servidor:** esta variable se sustituirá con el nombre del servidor utilizado al aplicar el archivo de configuración. El nombre del servidor se puede encontrar en la columna Servidor en la página de gestión de dispositivos. Para cambiar el nombre de un servidor, vaya al control del servicio de AXIS Camera Station Pro.
- **Insertar variable de zona horaria del servidor:** esta variable se sustituirá con la zona horaria POSIX del servidor utilizado al aplicar el archivo de configuración. Esto se puede usar con el parámetro de zona horaria POSIX para configurar la zona horaria correcta en todos los dispositivos en una red con servidores en distintas zonas horarias.

Reglas de actuación


Es posible copiar reglas de acción entre dispositivos. Solo usuarios experimentados deberían modificar las Reglas de acción. Para obtener información general sobre las reglas de acción, vea *Reglas de actuación*.

Configuración adicional

- **Perfiles de transmisión:** Un perfil de transmisión es un perfil de configuración de visualización en directo para los ajustes de codificación de vídeo, imagen y audio. Los perfiles de transmisión se pueden copiar entre dispositivos.
- **Ventanas de detección de movimiento:** Las ventanas de detección de movimiento se usan para definir áreas específicas en el campo de visión de la cámara. Normalmente, las alarmas se generan siempre que se genere (o detenga) un movimiento en las áreas especificadas. Es posible copiar ventanas de detección de movimiento entre dispositivos.

Gestión de usuarios

Vaya a **Configuración > Dispositivos > Gestión**; la página Gestión de dispositivos se abre para que pueda gestionar a los usuarios de los dispositivos.

Cuando configura una contraseña o elimina usuarios de varios dispositivos, los usuarios que no estén presentes en todos los dispositivos se indican con . Cada usuario aparece una única vez cuando el usuario está presente en diferentes dispositivos con diferentes funciones.

Nota

Las cuentas son específicas de los dispositivos y no están relacionadas con las cuentas de usuario de AXIS Camera Station Pro.

Configurar contraseña

Nota

- Los dispositivos con firmware 5.20 y posteriores admiten contraseñas de 64 caracteres. Los dispositivos


con versiones de firmware anteriores admiten contraseñas de 8 caracteres. Le recomendamos configurar contraseñas en dispositivos con firmware más antiguo por separado.

- Al configurar una contraseña en varios dispositivos que admiten diferentes longitudes de contraseña, la contraseña debe ajustarse a la longitud compatible más corta.
- Para impedir el acceso no autorizado y aumentar el nivel de seguridad, recomendamos encarecidamente que todos los dispositivos que se agregan a AXIS Camera Station Pro estén protegidos con contraseña.

En las contraseñas se pueden utilizar los siguientes caracteres válidos:

- letras A-Z, a-z
- números 0-9
- espacio, coma (,), punto (.), dos puntos (:), punto y coma (;)
- !, ", #, \$, %, &, ', (, +, *, -, /, <, >, =, ?, [, \, ^, -, ` , {, |, ~, @,], }

Para configurar la contraseña para los usuarios en los dispositivos:

1. Vaya a **Configuration > Devices > Management > Manage devices (Configuración > Dispositivos > Gestión > Gestionar dispositivos)**.
2. Seleccione los dispositivos y haga clic en . También puede hacer clic derecho en los dispositivos y seleccionar **User Management > Set password (Gestión de usuarios > Configurar contraseña)**.
3. Seleccione un usuario.
4. Escriba la contraseña o haga clic en **Generate (Generar)** para generar una contraseña segura.
5. Haga clic en **Aceptar**.

Agregar usuario

Para agregar usuarios locales o de Active Directory a AXIS Camera Station Pro:

1. Vaya a **Configuration > Devices > Management > Manage devices (Configuración > Dispositivos > Gestión > Gestionar dispositivos)**.
2. Haga clic derecho en los dispositivos y seleccione **User Management > Add user (Gestión de usuarios > Agregar usuario)**.
3. Introduzca un nombre de usuario y una contraseña y confirme la contraseña. Para obtener una lista de caracteres válidos, consulte la sección anterior Configurar contraseña.
4. Seleccione los derechos de acceso del usuario de la lista desplegable del campo **Función**:
 - **Administrador**: acceso ilimitado al dispositivo.
 - **Operador**: acceso a la transmisión de vídeo, a Eventos y a todos los ajustes, excepto a Opciones del sistema.
 - **Visor**: acceso a la transmisión de vídeo.
5. Seleccione **Activar control PTZ** para permitir que el usuario haga movimientos horizontales, verticales y zoom en Visualización en directo.
6. Haga clic en **Aceptar**.

Eliminar usuario

Para eliminar usuarios de los dispositivos:

1. Vaya a **Configuration > Devices > Management > Manage devices (Configuración > Dispositivos > Gestión > Gestionar dispositivos)**.
2. Haga clic derecho en los dispositivos y seleccione **User Management > Remove user (Gestión de usuarios > Eliminar usuario)**.
3. Seleccione el usuario que quiera eliminar de la lista desplegable del campo **Usuario**.
4. Haga clic en **Aceptar**.

Enumerar usuarios

Para mostrar en una lista todos los usuarios de los dispositivos y sus derechos de acceso:

1. Vaya a **Configuration > Devices > Management > Manage devices (Configuración > Dispositivos > Gestión > Gestionar dispositivos)**.
2. Haga clic derecho en los dispositivos y seleccione **User Management > List users (Gestión de usuarios > Enumerar usuarios)**.
3. Utilice el campo **Introduzca criterio de búsqueda** para buscar a los usuarios específicos en la lista.

Actualizar firmware




Firmware es el software que determina la funcionalidad del producto Axis. El uso del firmware más reciente garantiza que el dispositivo contará con la funcionalidad y las mejoras más recientes.

Se puede descargar nuevo firmware con AXIS Camera Station Pro o se puede importar desde un archivo en una unidad de disco duro o tarjeta de memoria. Las versiones de firmware que están disponibles para su descarga se muestran con el texto **(Descarga)** después de sus números de versión. Las versiones de firmware que están disponibles en el cliente local se muestran con el texto **(Archivo)** después de sus números de versión.

Al actualizar el firmware, puede seleccionar el tipo de actualización:

- **Estándar:** Actualice a la versión de firmware seleccionada y conserve los valores de configuración existentes.
- **Factory default (Predeterminado de fábrica):** Actualice a la versión de firmware seleccionada y restablezca todos los ajustes a los valores predeterminados de fábrica.

Para actualizar el firmware:

1. Vaya a **Configuración > Dispositivos > Gestión** y seleccione los dispositivos que configurar.
2. Haga clic en  o haga clic derecho y seleccione **Upgrade firmware (Actualizar firmware)**.
3. Si no se puede configurar alguno de los dispositivos seleccionados, por ejemplo, si no se puede acceder a ellos, aparecerá el cuadro de diálogo de dispositivos no válidos. Haga clic en **Continue (Continuar)** para saltarse los dispositivos que no se puedan configurar.
4. El dispositivo no es accesible durante el proceso de actualizar el firmware, haga clic en **Sí** para continuar. Si ya ha aceptado esta situación y no quiere que se vuelva a mostrar el mensaje, seleccione **No volver a mostrar este cuadro de diálogo** y haga clic en **Sí**.
5. El cuadro de diálogo Upgrade firmware (Actualizar firmware) muestra el modelo del dispositivo, el número de dispositivos de cada modelo, la versión de firmware existente, las versiones de firmware disponibles para actualizar y el tipo de actualización. De forma predeterminada, los dispositivos de la lista están preseleccionados cuando hay disponibles nuevas versiones del firmware para descargar, y la última versión del firmware está preseleccionada para cada dispositivo.
 - 5.1. Para actualizar la lista de versiones del firmware disponibles para descargar, haga clic en el botón **Comprobar actualizaciones**. Para explorar uno o varios archivos de firmware almacenados en el cliente local, haga clic en **Explorar**.
 - 5.2. Seleccione los dispositivos, las versiones del firmware que desea actualizar y el tipo de actualización.
 - 5.3. Haga clic en **OK (Aceptar)** para iniciar la actualización de los dispositivos de la lista.


Nota

De forma predeterminada, las actualizaciones de firmware se realizan para todos los dispositivos seleccionados al mismo tiempo. El orden de actualización se puede cambiar. Vea *Ajustes de actualización del firmware*.

Configurar fecha y hora.

La configuración de fecha y hora para sus dispositivos Axis puede sincronizarse con la hora del ordenador del servidor, con un servidor NTP o establecerse de forma manual.

Para configurar fecha y hora de los dispositivos:

1. Vaya a **Configuración > Dispositivos > Gestión**.
2. Seleccione el dispositivo y haga clic  o clic derecho sobre él y seleccione **Set date and time (Configurar fecha y hora)**.
3. La **hora del dispositivo** indica la fecha y hora actuales de su dispositivo Axis. Si selecciona varios dispositivos, no estará disponible la **hora del dispositivo**.
4. Seleccione la zona horaria.
 - Seleccione la zona horaria que desea utilizar con su producto Axis en la lista desplegable **Zona horaria**.
 - Seleccione **Ajustar automáticamente entre horario de verano e invierno** si su producto está situado en una zona que utilice el horario de verano.

Nota

Se puede establecer la zona horaria al seleccionar el modo horario **Sincronizar con servidor NTP** o **Configurar manualmente**.

5. En la sección **Modo horario**:
 - Seleccione **Synchronize with server computer time (Sincronizar con hora del ordenador del servidor)** para sincronizar la fecha y hora de su producto con el reloj del equipo del servidor, es decir, el equipo donde está instalado el servidor de AXIS Camera Station Pro.
 - Seleccione **Sincronizar con servidor NTP** para sincronizar la fecha y hora de su producto con un servidor NTP. Introduzca la dirección IP, DNS o nombre de host del servidor NTP en el campo proporcionado.
 - Seleccione **Configurar manualmente** para configurar manualmente la fecha y hora.
6. Haga clic en **Aceptar**.



Configurar fecha y hora.

Instalar la aplicación de la cámara

Una aplicación de la cámara es software que se puede cargar e instalar en productos de vídeo de red de Axis. Las aplicaciones agregan funcionalidad al dispositivo, por ejemplo, capacidades de detección, reconocimiento, seguimiento y recuento.

Algunas aplicaciones se pueden instalar directamente desde AXIS Camera Station Pro. Otras aplicaciones deben descargarse primero desde www.axis.com/global/en/products/analytics-and-other-applications o desde el sitio web del distribuidor de la aplicación.

Las aplicaciones pueden instalarse en dispositivos compatibles con la Plataforma de aplicaciones de cámaras AXIS. Algunas aplicaciones requieren también una versión de firmware o modelo de cámara específicos.

Si la aplicación requiere una licencia, el archivo de clave de licencia se puede instalar al mismo tiempo que la aplicación o posteriormente utilizando la página de configuración de los dispositivos.

Para obtener el archivo de la clave de licencia, es necesario registrar el código de licencia incluido con la aplicación en www.axis.com/se/sv/products/camera-applications/license-key-registration#/registration

Si una aplicación no se puede instalar, vaya a www.axis.com y compruebe si el modelo y la versión de firmware son compatibles con AXIS Camera Application Platform.

Aplicaciones de cámaras disponibles:


AXIS Video Motion Detection 4 – Una aplicación que detecta objetos en movimiento dentro de un área de interés. La aplicación no requiere licencia y se puede instalar en cámaras con firmware 6.50 y posterior. También puede consultar las notas de versión del firmware de su producto to para comprobar si es compatible con detección de movimiento por vídeo 4.

AXIS Video Motion Detection 2 – Una aplicación que detecta objetos en movimiento dentro de un área de interés. La aplicación no requiere licencia y se puede instalar en cámaras con firmware 5.60 y posterior.

AXIS Video Content Stream – Una aplicación que permite a las cámaras Axis enviar datos de seguimiento de objetos en movimiento a AXIS Camera Station Pro. Puede instalarse en cámaras con firmware entre 5.50 y 9.59. Solo se puede utilizar AXIS Video Content Stream en combinación con AXIS Camera Station Pro.

Otras aplicaciones – Cualquier aplicación que quiera instalar. Descargue la aplicación en su equipo local antes de iniciar la instalación.

Para instalar aplicaciones de cámara:

1. Vaya a **Configuración > Dispositivos > Gestión**.
2. Seleccione las cámaras para las que desee instalar las aplicaciones. Haga clic en  o clic derecho y seleccione **Install camera application (Instalar aplicación de cámara)**.
3. Seleccione la aplicación de la cámara que quiera instalar en las cámaras. Si quiere instalar otras aplicaciones, haga clic en **Examinar** y navegue hasta el archivo de la aplicación local. Haga clic en **Next (Siguiente)**.
4. Si tiene instalada la aplicación, puede seleccionar **Permitir sobrescritura de la aplicación** para reinstalar la aplicación, o **Permitir versión anterior de la aplicación** para instalar una versión anterior de la aplicación.

Nota

La instalación de una versión anterior o la sobrescritura de la aplicación restablece la configuración de la aplicación en los dispositivos.

5. Si la aplicación requiere una licencia, aparecerá el cuadro de diálogo **Instalar licencias**.
 - 5.1. Haga clic en **Sí** para iniciar la instalación de una licencia, y después haga clic en **Siguiente**.
 - 5.2. Haga clic en **Examinar** y navegue al archivo de licencia, y haga clic en **Siguiente**.

Nota

Para instalar **AXIS Video Motion Detection 2**, **AXIS Video Motion Detection 4** o **AXIS Video Content Stream** no se necesita licencia.

6. Repase la información y haga clic en **Finalizar**. El estado de la cámara cambia de **OK** a **Maintenance** y vuelve a **OK** cuando termina la instalación.

Seguridad

La autoridad de certificación (CA) de AXIS Camera Station Pro firma y distribuye automáticamente los certificados del cliente y del servidor a los dispositivos cuando habilita HTTPS o IEE 802.1X. La autoridad de

certificación ignora los certificados preinstalados. Para obtener más información sobre cómo configurar certificados, consulte *Certificados, on page 141*.

Administrar certificados HTTPS o IEEE 802.1X

Nota

Antes de habilitar IEEE 802.1X, asegúrese de que la hora de los dispositivos de Axis esté sincronizada en AXIS Camera Station Pro.

1. Vaya a **Configuración > Dispositivos > Gestión**.
2. Haga clic con el botón derecho del ratón en los dispositivos:
 - Seleccione **Security > HTTPS > Enable/Update (Seguridad > HTTPS > Habilitar/Actualizar)** para activar HTTPS o actualizar la configuración de HTTPS para los dispositivos.
 - Seleccione **Security > IEEE 802.1X > Enable/Update (Seguridad > IEEE 802.1X > Habilitar/Actualizar)** para activar IEEE 802.1X o actualizar la configuración de IEEE 802.1X para los dispositivos.
 - Seleccione **Security > HTTPS > Disable (Seguridad > HTTPS > Deshabilitar)** para deshabilitar HTTPS para los dispositivos.
 - Seleccione **Security > IEEE 802.1X > Disable (Seguridad > IEEE 802.1X > Deshabilitar)** para deshabilitar IEEE 802.1X para los dispositivos.
 - Seleccione **Certificates... (Certificados...)** para obtener información general, eliminar certificados u obtener información detallada sobre un certificado específico.

Nota

Si se instala el mismo certificado en varios dispositivos, este se mostrará como un único elemento. Al eliminar el certificado se eliminará de todos los dispositivos en los que está instalado.

Estado de HTTPS e IEEE 802.1X

En la página Gestión de dispositivos, se muestra el estado de HTTPS y IEEE 802.1X.

	Estado	Descripción
HTTPS	Encendido	AXIS Camera Station Pro utiliza HTTPS para conectarse al dispositivo.
	Apagado	AXIS Camera Station Pro utiliza HTTP para conectarse al dispositivo.
	Desconocido	No se puede acceder al dispositivo.
	Firmware no compatible	No se admite HTTPS porque el firmware del dispositivo es demasiado antiguo.
	Dispositivo no compatible	No se admite HTTPS en este modelo de dispositivo.
IEEE 802.1X	Habilitado	IEEE 802.1X está activo en el dispositivo.
	Deshabilitado	IEEE 802.1X no está activo, pero está listo para ser activado en el dispositivo.
	Firmware no compatible	No se admite IEEE 802.1X porque el firmware del dispositivo es demasiado antiguo.
	Dispositivo no compatible	IEEE 802.1X no es compatible con este modelo de dispositivo.

Recopilar datos de dispositivos

Esta opción se suele emplear para realizar una localización de problemas. Utilice esta opción para generar un archivo .zip con un informe de recopilación de datos para una ubicación específica en sus dispositivos.

Para recopilar datos del dispositivo:

1. Vaya a **Configuración > Dispositivos > Gestión**.
2. Haga clic con el botón derecho en los dispositivos y seleccione **Recopilar datos de dispositivo**.
3. En la sección Fuente de datos en dispositivos seleccionados:
 - haga clic en **Posiciones predefinidas** y seleccione en la lista desplegable uno de los comandos de uso habitual.

Nota

Algunas posiciones predefinidas no funcionan en todos los dispositivos. Por ejemplo, el estado PTZ no funciona en los dispositivos de audio.

- Haga clic en **Personalizado** y especifique la ruta URL a la fuente de recopilación de datos en los servidores seleccionados.
4. En la sección Guardar como, especifique el nombre del archivo y la ubicación de la carpeta para su archivo .zip de recopilación de datos.
 5. Seleccione **Abrir carpeta automáticamente cuando esté listo** para abrir la carpeta especificada cuando haya terminado la recopilación de datos.
 6. Haga clic en **Aceptar**.

Conexión

Para comunicarse con dispositivos mediante la dirección IP o el nombre de host:

1. Vaya a **Configuración > Dispositivos > Gestión**.
2. Seleccione los dispositivos, haga clic con el botón derecho y seleccione **Connection (Conexión)**.
 - Para conectarse a los dispositivos mediante la dirección IP, seleccione **Use IP (Utilizar IP)**.
 - Para conectarse a los dispositivos mediante el nombre de host, seleccione **Use hostname (Utilizar nombre de host)**.
 - Para cambiar las credenciales, o la dirección y los ajustes de puerto, seleccione **Editar**.

Etiquetas


Las etiquetas se usan para organizar dispositivos en la página Gestión de dispositivos. Un dispositivo puede tener varias etiquetas.

Los dispositivos pueden etiquetarse, por ejemplo, según el modelo o la ubicación. Por ejemplo, al etiquetar los dispositivos de acuerdo al modelo de cámara, se pueden encontrar y actualizar de manera rápida las cámaras de dicho modelo.

Para etiquetar dispositivos:



1. Vaya a **Configuración > Dispositivos > Gestión**.
2. Haga clic con el botón derecho en un dispositivo y seleccione **Etiquetar dispositivos**.
3. Seleccione **Usar etiqueta existente** y seleccione una etiqueta, o bien, seleccione **Crear nueva etiqueta** e introduzca un nombre para la etiqueta.
4. Haga clic en **Aceptar**.

Para eliminar una etiqueta de un dispositivo:

1. Vaya a **Configuration > Devices > Management (Configuración > Dispositivos > Gestión)** y haga clic en  en la esquina superior derecha.

2. En la carpeta Etiquetas, seleccione una etiqueta. Todos los dispositivos asociados con la etiqueta se muestran ahora.
3. Seleccione los dispositivos. Haga clic con el botón derecho y seleccione **Eliminar etiqueta de dispositivos**.
4. Haga clic en **Aceptar**.

Para gestionar una etiqueta:

1. Vaya a **Configuration > Devices > Management (Configuración > Dispositivos > Gestión)** y haga clic en  en la esquina superior derecha.
2. En la página Etiquetas del dispositivo:
 - Haga clic derecho en **Etiquetas** y seleccione **Nueva etiqueta** para crear una etiqueta.
 - Haga clic derecho en una etiqueta, seleccione **Cambiar nombre de etiqueta** e introduzca un nuevo nombre para la etiqueta.
 - Haga clic con el botón derecho en una etiqueta y seleccione **Eliminar** para eliminar una etiqueta.
 - Haga clic en  para anclar la página Device tags (Etiquetas del dispositivo).
 - Haga clic en una etiqueta para mostrar todos los dispositivos asociados con la etiqueta y haga clic en **All devices (Todos los dispositivos)** para mostrar todos los dispositivos conectados a AXIS Camera Station Pro.
 - Haga clic en **Advertencias/Errores** para mostrar los dispositivos que requieren atención, por ejemplo, los dispositivos a los que no se puede acceder.

Pestaña de configuración del dispositivo

Para configurar todos los ajustes en un único dispositivo:

1. Vaya a **Configuración > Dispositivos > Gestión**.
2. Haga clic en la dirección o en el nombre de host del dispositivo para ir a la pestaña de configuración del dispositivo.
3. Cambiar la configuración del servidor. Para obtener información sobre cómo configurar su dispositivo, consulte el Manual de usuario.
4. Cierre la pestaña y vuelva a cargar el dispositivo para asegurarse de que los cambios se implementan en AXIS Camera Station Pro.

Limitations (Limitaciones)

- No se admite la autenticación automática para dispositivos de terceros.
- No se puede garantizar la compatibilidad general con dispositivos de terceros.
- La pestaña de configuración del dispositivo con transmisiones de vídeo activas aumenta la carga y podría afectar al rendimiento del servidor.

Fuentes de datos externos

Una fuente de datos externa es un sistema o fuente que genera datos que se pueden utilizar para rastrear lo que ha sucedido en el momento de cada evento. Vea *Búsqueda de datos, on page 43*.

Vaya a **Configuration > Devices > External data sources (Configuración > Dispositivos > Fuentes de datos externos)** y se mostrará una lista de fuentes de datos externos. Haga clic en un encabezado de columna para ordenar por el contenido de la columna.

Elemento	Descripción
Nombre	El nombre del origen de datos externo.

Clave de fuente	Identificador único del origen de datos externo.
Ver	La vista a la que está vinculado el origen de datos externo.
Servidor	El servidor al que está conectada la fuente de datos. Solo está disponible al conectarse con varios servidores.

Se añade automáticamente una fuente de datos externa cuando

- se crea una puerta en **Configuration > Access control > Doors and zones (Configuración > Control de acceso > Puertas y zonas)**.
Para consultar un flujo de trabajo completo sobre cómo configurar una controladora de accesos en red de Axis en AXIS Camera Station Pro, consulte *Set up an Axis network door controller (Configurar una controladora de accesos en red de Axis)*.
- El primer evento lo recibe el dispositivo que está configurado con AXIS License Plate Verifier.
Para obtener un flujo de trabajo adecuado que permita configurar a AXIS License Plate Verifier en AXIS Camera Station Pro, consulte *Configurar AXIS License Plate Verifier*.

Si se configura una fuente de datos externa con una vista, los datos generados desde la fuente de datos se anotan automáticamente en la línea temporal de la vista emplazada en la pestaña Data search (Búsqueda de datos). Para conectar una fuente de datos a una vista:

1. vaya a **Configuration > Devices > External data sources (Configuración > Dispositivos > Fuentes de datos externos)**.
2. Seleccione una fuente de datos externa y haga clic en **Edit (Editar)**.
3. Seleccione una vista en la lista desplegable **View (Vista)**.
4. Haga clic en **OK**.

Sincronización de hora

Vaya a **Configuration > Devices > Time synchronization (Configuración > Dispositivos > Sincronización de tiempo)** para abrir la página sincronización de tiempo.

Aparecerá una lista de los dispositivos añadidos a AXIS Camera Station Pro. Haga clic con el botón derecho en la fila del encabezado y seleccione qué columnas mostrar. Para mostrar las columnas en orden diferente, arrastre y suelte los encabezados.

La lista de dispositivos incluye la siguiente información:

- **Nombre:** El nombre del dispositivo o una serie de todos los nombres de cámaras asociadas si el dispositivo es un codificador de vídeo con varias cámaras conectadas, o una cámara de red con varias áreas de visión.
- **Dirección:** La dirección del dispositivo. Haga clic en el enlace para ir a la página de configuración del dispositivo. Muestra la dirección IP o nombre de host en función de cuál se utilizó al agregar el dispositivo. Vea *Pestaña de configuración del dispositivo, on page 73*.
- **Dirección MAC:** La dirección MAC del dispositivo.
- **Modelo:** el modelo del dispositivo.
- **Habilitado:** Muestra si la sincronización de tiempo está activada.
- **Fuente de NTP:** La fuente NTP configurada para el dispositivo.
 - **Estática:** Los servidores NTP del dispositivo se especifican manualmente en **Servidor NTP principal** y **Servidor NTP secundario**.
 - **DHCP:** El dispositivo recibe el servidor NTP dinámicamente de la red. El **Servidor NTP principal** y el **Servidor NTP secundario** no están disponibles cuando se selecciona DHCP.

- **Servidor NTP principal:** El Servidor NTP principal está configurado para el dispositivo. Solo está disponible si se selecciona **Static (Estático)**.
- **Servidor NTP secundario:** El Servidor NTP secundario está configurado para el dispositivo. Solo disponible para dispositivos Axis compatibles con NTP secundario y cuando se selecciona **Static (Estático)**.
- **Desviación de hora del servidor:** Diferencia de hora entre el dispositivo y el servidor.
- **Hora UTC:** La hora universal coordinada del dispositivo.
- **Sincronizado:** Muestra si la configuración de sincronización de hora se ha aplicado realmente. Esto solo está disponible para dispositivos con firmware 9.1 o superior.
- **Tiempo hasta la próxima sincronización:** El tiempo restante para la siguiente sincronización.

El servicio Hora de Windows (W32Time) utiliza Network Time Protocol (NTP) para sincronizar la fecha y la hora del servidor de AXIS Camera Station Pro. Se muestra la siguiente información:

- **Servidor:** El servidor AXIS Camera Station Pro en el que se está ejecutando el servicio de hora de Windows.
- **Estado:** El estado del servicio Hora de Windows. O `Running` o `Stopped`.
- **Servidor NTP:** El servidor NTP está configurado para el servicio Hora de Windows.

Configure la sincronización de hora

1. Vaya a **Configuration > Devices > Time synchronization (Configuración > dispositivos > sincronización de hora)**.
2. Seleccione sus dispositivos y seleccione **Enable time synchronization (Activar sincronización de hora)**.
3. Seleccione la fuente NTP **Static (Estática)** o **DHCP**.
4. Si ha seleccionado **Static (Estática)**, configure el servidor NTP principal y secundario.
5. Haga clic en **Aplicar**.

Envíe una alarma cuando la diferencia de hora entre servidor y dispositivo sea mayor que 2 segundos	Seleccione esto para recibir una alarma si la diferencia de tiempo entre el servidor y el dispositivo es de más de 2 segundos.
Configure la zona horaria manualmente a través de la interfaz del dispositivo	Seleccione esta opción si no desea utilizar la zona horaria del servidor y utilizar otra en la ubicación dispositivo. Si elige esta opción, debe definir la zona horaria manualmente a través de la interfaz web del dispositivo.

Configurar almacenamiento

Vaya a **Configuración > Almacenamiento > Gestión** para abrir la página Gestión de almacenamiento. En la página Gestionar almacenamiento, podrá obtener información general del almacenamiento local y del almacenamiento de red que existe en AXIS Camera Station Pro.

Lista	
Establecimiento	La ruta y el nombre del almacenamiento.
Asignado	La cantidad máxima de almacenamiento asignado a las grabaciones.
Used (Utilizado)	La cantidad de espacio de almacenamiento utilizado actualmente para las grabaciones.

Lista	
Estado	<p>Estado del almacenamiento. Los valores posibles son:</p> <ul style="list-style-type: none"> • OK • Almacenamiento completo: El almacenamiento está lleno. El sistema invalida las grabaciones más antiguas desbloqueadas. • No disponible: La información del almacenamiento no está disponible actualmente. Por ejemplo, en el caso en que un almacenamiento de red se eliminase o desconectase. • Datos intrusos: Los datos de otras aplicaciones utilizan espacio de almacenamiento asignado para AXIS Camera Station Pro. También hay grabaciones sin conexión a la base de datos, denominadas grabaciones no indexadas, en el espacio de almacenamiento asignado para AXIS Camera Station Pro. • Sin permisos: El usuario no dispone de permiso de lectura o escritura para el almacenamiento. • Poco espacio: La unidad tiene menos de 15 GB de espacio libre, que AXIS Camera Station Pro considera demasiado poco. Para evitar errores o daños, AXIS Camera Station Pro realiza una limpieza forzada, independientemente de la posición del control deslizante de almacenamiento, para proteger la unidad. Durante la limpieza forzada, AXIS Camera Station Pro impide la grabación hasta que haya más de 15 GB de almacenamiento disponibles. • Capacidad insuficiente: El tamaño total del disco es inferior a 32 GB, que no es suficiente para AXIS Camera Station Pro. <p>Los grabadores AXIS OS compatibles con RAID también pueden tener los siguientes estados:</p> <ul style="list-style-type: none"> • Online (En línea): El sistema RAID funciona como debe. Existe una redundancia en caso de que uno de los discos físicos del sistema RAID se rompa. • Reducido: Uno de los discos físicos del sistema RAID no funciona. Aún es posible grabar y reproducir grabaciones desde el almacenamiento, pero no hay redundancia. Si se rompe otro disco físico, el estado de RAID cambiará a Failure (Error). Recomendamos sustituir el disco físico roto lo antes posible. Después de sustituir un disco roto, el estado de RAID cambia de Degradación a Sincronización. • Sincronización: Los discos RAID se sincronizan. Es posible grabar y reproducir grabaciones desde el almacenamiento, pero no existe redundancia si un disco físico se rompe. Una vez que los discos físicos se han sincronizado, hay redundancia en el sistema RAID y el estado de RAID cambia a Online (En línea). <p>Importante</p> <p>Nunca elimine un disco RAID mientras se sincroniza. Esto puede provocar un fallo en el disco.</p> <ul style="list-style-type: none"> • Failure (Error): Se han producido errores en varios discos físicos en el sistema RAID. Cuando esto sucede, todas las grabaciones del almacenamiento se pierden y solo es posible grabar una vez sustituya los discos físicos rotos.
Servidor	El servidor donde se encuentra el almacenamiento local o de red.

Descripción general	
Used (Utilizado)	Cantidad de espacio de almacenamiento actualmente utilizado por las grabaciones indexadas. Si hay un archivo en el directorio de grabaciones pero no está indexado en la base de datos, el archivo pertenece a la categoría Otros datos . Consulte Recopilar archivos no indexados en <i>Gestionar almacenamiento, on page 77</i> .
Gratis	Cantidad de espacio de almacenamiento que queda en la ubicación de almacenamiento. Es la misma cantidad que se muestra en "Space free" (Espacio libre) en las propiedades de Windows para la ubicación de almacenamiento.
Otros datos	Cantidad de espacio de almacenamiento que ocupan los archivos que no son grabaciones indexadas y, por lo tanto, son desconocidos para AXIS Camera Station Pro. Otros datos = Capacidad total - espacio utilizado - espacio libre
Capacidad total	Cantidad total de espacio de almacenamiento. Es la misma cantidad que se muestra en "Tamaño total" en las propiedades de Windows para la ubicación de almacenamiento.
Asignado	La cantidad de espacio de almacenamiento que AXIS Camera Station Pro puede utilizar para las grabaciones. Puede ajustar el control deslizante y hacer clic en Apply (Aplicar) para ajustar el espacio asignado.

Almacenamiento de red	
Ruta	La ruta al almacenamiento en red.
Nombre de usuario	El nombre de usuario utilizado para conectarse al almacenamiento de red.
Contraseña	La contraseña para el nombre de usuario utilizado para conectarse al almacenamiento de red.

Gestionar almacenamiento

Vaya a **Configuración > Almacenamiento > Gestión** para abrir la página Gestión de almacenamiento. En esta página, puede especificar la carpeta donde almacenar las grabaciones. Para evitar que el almacenamiento se llene, establezca un porcentaje máximo de la capacidad total que AXIS Camera Station Pro puede usar. Puede agregar unidades adicionales de almacenamiento local y en red por razones de seguridad y espacio.

Nota

- Cuando esté conectado a varios servidores de AXIS Camera Station Pro, seleccione el servidor del menú desplegable **Selected server (Servidor seleccionado)** para gestionar el almacenamiento.
- Cuando el servicio usa la cuenta de sistema para iniciar sesión, no puede agregar unidades de red vinculadas a carpetas compartidas en otros equipos. Vea *No se puede acceder al almacenamiento de red*.
- No puede eliminar el almacenamiento local o en red si las cámaras están configuradas para guardar grabaciones en ellas o si contienen grabaciones.

Añadir un dispositivo de almacenamiento local o una unidad de red compartida

1. Vaya a **Configuración > Almacenamiento > Gestión**.
2. Haga clic en **Añadir**.
3. Para agregar un dispositivo de almacenamiento local, seleccione **Local storage (Almacenamiento local)** y seleccione un dispositivo de almacenamiento del menú desplegable.

4. Para agregar una unidad de red compartida, seleccione **Unidad de red compartida** y escriba la ruta a una unidad de red compartida. Por ejemplo: \\ip_address\share.
5. Haga clic en **Aceptar** e introduzca el nombre de usuario y la contraseña para la unidad de red compartida.
6. Haga clic en **OK**.

Eliminar un dispositivo de almacenamiento local o una unidad de red compartida

Para eliminar una unidad de almacenamiento local o una unidad de red compartida, seleccione una unidad de almacenamiento local o una unidad de red compartida en la lista de almacenamiento y haga clic en **Remove (Eliminar)**.

Trasladar grabaciones a una nueva carpeta

1. Vaya a **Configuración > Almacenamiento > Gestión**.
2. Seleccione una unidad de almacenamiento local o de red compartida en la lista de almacenamiento.
3. En **Overview (Información general)**, introduzca un nombre de carpeta en **Move recordings to a new folder (Trasladar grabaciones a una nueva carpeta)** para cambiar la ubicación de almacenamiento de las grabaciones. Mediante esta acción también se trasladan las grabaciones existentes de la carpeta anterior a la nueva carpeta.
4. Haga clic en **Aplicar**.

Ajustar la capacidad de almacenamiento

1. Vaya a **Configuración > Almacenamiento > Gestión**.
2. Seleccione una unidad de almacenamiento local o de red compartida en la lista de almacenamiento.
3. En **Overview (Información general)**, mueva el control deslizante para establecer el espacio máximo que AXIS Camera Station Pro puede usar.
4. Haga clic en **Aplicar**.

Nota

- Recomendamos dejar libre al menos el 5% del espacio en disco para un rendimiento óptimo.
- El espacio mínimo de almacenamiento agregado a AXIS Camera Station Pro es de 32 GB con al menos 15 GB de espacio libre disponible.
- Si hay menos de 15 GB de espacio libre disponible, AXIS Camera Station Pro elimina automáticamente grabaciones antiguas para liberar espacio.

Recopilar archivos no indexados

Los archivos no indexados pueden constituir una parte sustancial de los **Otros datos** en el almacenamiento. Un archivo no indexado es cualquier dato en la carpeta de grabación que no forma parte de la base de datos actual. El archivo puede contener grabaciones de instalaciones previas o pérdida de datos cuando se utilizaba un punto de restauración.

El sistema no elimina los archivos recopilados, sino que se recopilan y se colocan en la carpeta **Non-indexed files (Archivos no indexados)** del almacenamiento de grabaciones. El almacenamiento puede encontrarse en el mismo equipo que el cliente o en un servidor remoto, en función de su configuración. Para acceder a la carpeta **Non-indexed files (Archivos no indexados)**, necesita acceso al servidor. AXIS Camera Station Pro coloca los datos en las carpetas después del orden en el que se encontraron, primero por servidor y después por dispositivos conectados a ese servidor en concreto.

Puede elegir entre buscar una grabación en concreto o un registro perdido o simplemente eliminar el contenido para liberar espacio.

Para recopilar los archivos no indexados para su revisión o eliminación:

1. Vaya a **Configuración > Almacenamiento > Gestión**.
2. Seleccione una unidad de almacenamiento local o de red compartida en la lista de almacenamiento.

3. En **Collect non-indexed files (Recopilar archivos no indexados)**, haga clic en **Collect (Recopilar)** para iniciar una tarea.
4. Cuando se haya terminado la tarea, vaya a **Alarms and Tasks > Tasks (Alarmas y tareas > Tareas)** y haga doble clic en la tarea para ver el resultado.

Seleccionar dispositivos de almacenamiento para conectar

Nota

Las grabaciones se guardan como archivos .acsm que deben convertirse antes de poder reproducirse. Contacte con el equipo de asistencia técnica de Axis si necesita ayuda para convertir sus archivos.

Vaya a **Configuración > Almacenamiento > Selección** para abrir la página **Seleccionar almacenamiento**. Esta página incluye una lista de todas las cámaras que hay en AXIS Camera Station Pro y puede especificar el número de días que se guardarán las grabaciones para cámaras específicas. Al realizar una selección, la información sobre el almacenamiento aparece bajo **Almacenamiento de grabaciones**. Puede configurar varias cámaras al mismo tiempo.

Nombre	El nombre del dispositivo o una serie de todos los nombres de cámaras asociadas si el dispositivo es un codificador de vídeo con varias cámaras conectadas, o una cámara de red con varias áreas de visión.
Dirección	La dirección del dispositivo. Haga clic en el enlace para ir a la página de configuración del dispositivo. Muestra la dirección IP o nombre de host en función de cuál se utilizó al agregar el dispositivo. Vea <i>Pestaña de configuración del dispositivo, on page 73</i> .
Dirección MAC	La dirección MAC del dispositivo.
Fabricante	el fabricante del dispositivo.
Modelo	el modelo del dispositivo.
Almacenamiento utilizado	La cantidad de espacio de almacenamiento utilizado actualmente para las grabaciones.
Establecimiento	La ruta y el nombre del almacenamiento.
Tiempo de conservación	El tiempo de conservación configurado para la cámara.
Grabación más antigua	La hora de la grabación más antigua que se guarda en el almacenamiento de la cámara.
Grabación failover	Muestra si la cámara utiliza la grabación a prueba de fallos.
Grabación alternativa	Muestra si la cámara utiliza la grabación de reserva.
Servidor	El servidor donde se encuentra el almacenamiento local o de red.

La solución de almacenamiento para cada cámara se configuró cuando se agregaron cámaras a AXIS Camera Station Pro. Para editar los ajustes de almacenamiento para una cámara:

1. Vaya a **Configuración > Almacenamiento > Selección**.
2. Seleccione la cámara para editar los ajustes de almacenamiento.
3. En **Recording storage (Almacenamiento de grabaciones)**, establezca la ubicación de almacenamiento y el tiempo de conservación.
4. Haga clic en **Aplicar**.

Almacenamiento de grabaciones	
Almacenar en	Seleccione el almacenamiento en el que guardar las grabaciones en el menú desplegable. Las opciones disponibles son las unidades de almacenamiento local y de almacenamiento de red que se hayan creado.
Grabación failover	<p>Seleccione esta opción para guardar las grabaciones en la tarjeta SD de la cámara cuando AXIS Camera Station Pro y la cámara pierden la conexión. Una vez que la conexión vuelve, las grabaciones a prueba de fallos se transfieren a AXIS Camera Station Pro.</p> <p>Nota Esta función solo está disponible para cámaras con tarjeta SD y firmware 5.20 o posterior.</p>
Ilimitada	Seleccione tiempo de conservación para mantener las grabaciones hasta que se llene el almacenamiento.
Limitada	<p>Seleccione para establecer el número máximo de días que guardar las grabaciones.</p> <p>Nota Si la cantidad de espacio reservado en el almacenamiento para AXIS Camera Station Pro se agota, el sistema borra las grabaciones antes del número de días designado.</p>
Número máximo de días para guardar grabaciones	Especifique el número de días que guardar las grabaciones.

Configurar grabaciones y eventos

Cuando agregamos cámaras a AXIS Camera Station Pro, configura automáticamente la grabación de movimiento o continua la grabación. Más adelante podrá cambiar el método de grabación para adaptarlo a sus necesidades, vaya a *Método de grabación*, on page 86.

Grabación de movimiento

Es posible usar detección de movimiento con todas las cámaras de red y codificadores de vídeo Axis. Al grabar únicamente cuando se detecta movimiento se ahorra una cantidad considerable de espacio de almacenamiento en comparación con la grabación continua. En **Recording method (Método de grabación)** puede activar y configurar **Motion detection (Detección de movimiento)**. Puede, por ejemplo, configurar los ajustes si la cámara detecta demasiados o pocos objetos en movimiento o si el tamaño de los archivos grabados es demasiado grande para el espacio de almacenamiento disponible.

Para configurar la grabación de movimiento:

1. Vaya a **Configuración > Grabaciones y eventos > Método de grabación**.
2. Seleccione una cámara.
3. Seleccione la casilla de verificación **Motion detection (Detección de movimiento)**.
4. Haga clic en **Motion settings (Ajustes de movimiento)** para configurar los ajustes de detección de movimiento, como el número de objetos detectables. Los ajustes disponibles son diferentes para cámaras diferentes, consulte *Editar detección de movimiento integrada* y *Editar AXIS Video Motion Detection 2 y 4*.
5. Seleccione un **Profile (Perfil)** en el menú desplegable. El perfil **High (Alto)** es el predeterminado.

6. Seleccione una programación o haga clic en **New schedule... (Nueva programación...)** para crear una nueva programación personalizada.
7. Determine los ajustes de tiempo para el búfer previo y posterior, así como el periodo de activación.
8. Haga clic en **Aplicar**.

Nota

Puede configurar la grabación de movimiento con Reglas de acción. Asegúrese de desactivar **Motion detection (Detección de movimiento)** en **Recording method (Método de grabación)** antes de utilizar reglas de acción.

Perfil	Utilice una resolución más baja para disminuir el tamaño de la grabación. Para editar los ajustes del perfil, consulte <i>Perfiles de transmisión</i> .
Horario	La programación de las grabaciones. Para reducir el impacto en su espacio de almacenamiento, grabe únicamente durante periodos de tiempo específicos.
Categorías de evento	Qué categoría de evento desea asignar a la grabación, si corresponde.
Búfer anterior	El número de segundos antes del movimiento detectado para incluirlo en una grabación.
Búfer posterior	El número de segundos después del movimiento detectado para incluirlo en una grabación.
Trigger period (Período de activación)	El intervalo de tiempo entre dos activadores sucesivos para reducir el número de grabaciones consecutivas. Si se produce una activación adicional dentro de este intervalo, la grabación continúa y se reinicia el período de activación.
Generar alarma	Activa una alarma cuando la cámara detecta movimiento.



Configuración de la detección de movimiento

DetECCIÓN DE OBJETOS

La grabación de detección de objetos captura vídeo cuando AXIS Object Analytics detecta y clasifica tipos de objetos como personas y vehículos. Recomendamos usarlo junto con la detección de movimiento o la grabación continua para garantizar que no se pierda ningún evento. AXIS Object Analytics admite hasta 10 escenarios por cámara.

Nota

Para poder usar esta función, la cámara necesita la versión de firmware 12.4.26 o posterior, un solo sensor y AXIS Object Analytics ACAP instalado.

Para utilizar la detección de objetos:

1. Vaya a **Configuración > Grabaciones y eventos > Método de grabación**.
2. Seleccione una cámara.

3. Seleccione la casilla de verificación **Object detection (Detección de objetos)**.
4. Configure sus ajustes. Para obtener más información, consulte la siguiente tabla.
5. Haga clic en **Aplicar**.
 - Los eventos de detección de objetos se muestran en rosa en la línea de tiempo.

Configuración de detección de objetos...	Haga clic para abrir la interfaz web de AXIS Object Analytics y configurar qué tipos de objetos (humanos, vehículos) activan grabaciones, establecer el tamaño mínimo de los objetos, definir áreas de detección y ajustar la configuración de tiempo en el área.
Perfil	Seleccione un Profile (Perfil) en el menú desplegable. El perfil High (Alto) es el predeterminado. Utilice una resolución más baja para reducir el tamaño de la grabación. Para editar los ajustes del perfil, consulte <i>Perfiles de transmisión</i> .
Horario	Configure la programación de las grabaciones. Para reducir el impacto en su espacio de almacenamiento, grabe únicamente durante períodos de tiempo específicos.
Categorías de evento	Seleccione qué categoría de evento desea asignar a la grabación, si corresponde. Para obtener más información, visite <i>Categorías de eventos, on page 27</i> .
Búfer anterior	Establezca el número de segundos antes del objeto detectado para incluirlo en una grabación.
Búfer posterior	Establezca el número de segundos después del objeto detectado para incluirlo en una grabación.
Trigger period (Período de activación)	Configure un intervalo de tiempo entre dos activadores sucesivos para reducir el número de grabaciones consecutivas. Si se produce una activación adicional dentro de este intervalo, la grabación continúa y se reinicia el período de activación.
Generar alarma	Seleccione esta opción para generar una alarma cuando AXIS Object Analytics detecte un objeto.

Grabación continua y programada

La grabación continua guarda imágenes continuamente y requiere más espacio de almacenamiento que otras opciones de grabación. Para reducir el tamaño del archivo, considere la posibilidad de grabar con detección de movimiento.

Para usar la grabación continua:

1. Vaya a **Configuración > Grabaciones y eventos > Método de grabación**.
2. Seleccione una cámara.
3. Seleccione la casilla **Continuous (Continua)** para utilizar la grabación continua.
4. Configure sus ajustes. Para obtener más información, consulte la siguiente tabla.
5. Haga clic en **Aplicar**.

Perfil	Seleccione un Profile (Perfil) en el menú desplegable. El perfil High (Alto) es el predeterminado. Utilice una resolución más baja para reducir el tamaño de la grabación. Para editar los ajustes del perfil, consulte <i>Perfiles de transmisión</i> .
Horario	Configure la programación de las grabaciones. Para reducir el impacto en su espacio de almacenamiento, grabe únicamente durante períodos de tiempo específicos.
Velocidad de bits media	Active y defina el almacenamiento máximo. EL sistema muestra la velocidad de bits media estimada en función del almacenamiento máximo especificado y el tiempo de conservación. La velocidad de bits media máxima es de 50 000 Kbit/s. Consulte <i>Configurar la velocidad de bits media, on page 86</i> .

Grabación manual

Para obtener más información sobre cómo realizar grabaciones manualmente, consulte *Grabar manualmente*.

Para configurar los parámetros de grabación manual:

1. Vaya a **Configuración > Grabaciones y eventos > Método de grabación**.
2. Seleccione una cámara.
3. Seleccione la casilla de verificación **Manual**.
4. Configure sus ajustes. Para obtener más información, consulte la siguiente tabla.
5. Haga clic en **Aplicar**.

Perfil	Seleccione un Profile (Perfil) en el menú desplegable. El perfil High (Alto) es el predeterminado. Utilice una resolución más baja para reducir el tamaño de la grabación. Para editar los ajustes del perfil, consulte <i>Perfiles de transmisión</i> .
Categorías de evento	Seleccione qué categoría de evento desea asignar a la grabación, si corresponde.
Búfer anterior	Establezca el número de segundos antes de presionar grabar para incluirlo en una grabación.
Búfer posterior	Establezca el número de segundos después de detener la grabación para incluirlo en una grabación.
Marcar durante la grabación	Seleccione esta opción para añadir detalles de marcadores cada vez que inicie una grabación manual. Los marcadores ayudan a encontrar e identificar grabaciones específicas más tarde. Este ajuste se aplica únicamente a operadores y administradores y está desactivado de forma predeterminada.
Duración máxima	Establezca la duración máxima de cada grabación, sin incluir los tiempos de búfer anterior ni posterior. Establézcalo en 0 para una duración ilimitada.

Grabación activada por regla

Una grabación activada por regla se inicia y detiene según una regla creada en Action rules (Reglas de acción). Puede utilizar reglas, por ejemplo, para generar grabaciones activadas por señales de puertos de E/S o eventos de dispositivo. Una regla puede tener varios desencadenadores.

Para crear una grabación activada por reglas, consulte *Reglas de actuación*.

Nota

Si utiliza una regla para configurar la grabación de movimiento, asegúrese de deshabilitar la grabación de movimiento para evitar grabaciones duplicadas.

Grabación failover

Utilice la grabación a prueba de fallos para garantizar que las grabaciones se guarden si se perdiera la conexión con AXIS Camera Station Pro. Una vez activada la grabación a prueba de fallos, la cámara guardaría las grabaciones en su tarjeta SD si la conexión se interrumpiera durante más de 20 segundos. La cámara debe tener una tarjeta SD instalada y la función activada. La grabación a prueba de fallos solo afectará a las grabaciones en H.264.

Para activar la grabación a prueba de fallos:

1. Vaya a **Configuración > Almacenamiento > Selección**.
2. Seleccione una cámara que admita grabación a prueba de fallos.
3. Seleccione **Grabación a prueba de fallos**.
4. Haga clic en **Aplicar**.

Nota

- Reiniciar el servidor de AXIS Camera Station Pro no activará grabaciones a prueba de fallos. Por ejemplo, cuando ejecute el mantenedor de base de datos, reinicie AXIS Camera Station Pro o reinicie el equipo donde está instalado el servidor.
- Activar la grabación a prueba de fallos sobrescribe cualquier configuración de respaldo existente para esa cámara en otros servidores.
- La grabación a prueba de fallos solo puede estar activa para un servidor AXIS Camera Station Pro a la vez por cada vista de cámara.

Al restablecer la conexión, AXIS Camera Station Pro importa automáticamente las grabaciones a prueba de fallos y las marca en gris oscuro en la línea de tiempo.

La cámara utiliza un búfer anterior y un búfer posterior de 20 segundos para minimizar las interrupciones en la grabación, pero aún pueden aparecer breves interrupciones de entre 1 y 4 segundos. Siempre se utiliza el perfil de transmisión de alta calidad para las grabaciones a prueba de fallos. El audio se incluye si está habilitado en la cámara y forma parte de la transmisión antes de activarse el modo a prueba de fallos.

Métodos de grabación	
Motion detection with prebuffer (Detección de movimiento con memoria intermedia anterior)	Si se pierde la conexión durante más de 20 segundos, la cámara graba continuamente en la tarjeta SD hasta que se restablece la conexión o la tarjeta SD se llena.
Motion detection without prebuffer (Detección de movimiento sin memoria intermedia anterior)	<ul style="list-style-type: none"> • Si se pierde la conexión durante más de 20 segundos cuando no hay grabación por detección de movimiento en curso, no se inicia la grabación a prueba de fallos. • Si se pierde la conexión durante más de 20 segundos mientras se está grabando movimiento, se inicia la grabación a prueba de fallos y continúa hasta que se restablece la conexión o la tarjeta SD se llena.
Grabación continua	Si se pierde la conexión durante más de 20 segundos, la cámara graba continuamente en la tarjeta SD hasta que se restablece la conexión o la tarjeta SD se llena.

Nota

Los dispositivos con una versión de AXIS OS anterior a la 11.11.42 emplean un método de grabación a prueba de fallos heredado. Las principales diferencias son:

- La cámara inicia la grabación a prueba de fallos después de 10 segundos de pérdida de conexión.
- La cámara utiliza un búfer de memoria interna de 10 segundos en lugar de un búfer anterior y posterior de 20 segundos.



Utilizar la tarjeta SD para la grabación a prueba de fallos

Grabación alternativa

Puede activar la grabación de reserva en un dispositivo que utilice AXIS S3008 Recorder como almacenamiento de grabaciones. Una vez activada la grabación remota, el dispositivo inicia automáticamente una grabación continua cuando se pierde la conexión entre AXIS Camera Station Pro y la grabadora. El dispositivo utiliza el perfil de flujo medio para las grabaciones en caso de error.

Nota

- Requiere AXIS Camera Station 5.36 o posterior, la versión de firmware 10.4 o superior para AXIS S3008 Recorder, la versión de firmware 5.50 o posterior del dispositivo Axis.
- Si se activa una grabación continua al iniciarse la grabación alternativa, se iniciará otra grabación continua. El sistema crea duplicados de la transmisión en la grabadora.

Para activar la grabación remota:

1. Asegúrese de haber agregado AXIS S3008 Recorder y los dispositivos y de haber seleccionado la grabadora como almacenamiento de grabación para el dispositivo. Consulte la *Set up AXIS OS Recorders (Configuración de AXIS OS Recorders)*.
2. Vaya a Configuración > Almacenamiento > Selección.

3. Seleccione el dispositivo y seleccione **Fallback recording (Grabación de reserva)**.
4. Haga clic en **Aplicar**.

Método de grabación

AXIS Camera Station Pro configura automáticamente la grabación de movimiento o continua al agregar dispositivos.

Una marca de verificación en la lista muestra qué método de grabación utiliza un dispositivo. Para personalizar los ajustes de vídeo y audio, consulte *Perfiles de transmisión*.

Para cambiar el método de grabación:

1. Vaya a **Configuración > Grabaciones y eventos > Método de grabación**.
2. Seleccione uno o varios dispositivos.
Para dispositivos del mismo modelo, puede configurar varios dispositivos al mismo tiempo.
3. En la pantalla **Recording method (Método de grabación)**, active o desactive un método de grabación.

Nota

Las áreas de visión no admiten detección de movimiento.

Configurar la velocidad de bits media

La velocidad de bits se ajusta automáticamente a lo largo de un periodo de tiempo prolongado. De esta forma, se puede conseguir el objetivo especificado y una buena calidad de vídeo basándose en el almacenamiento especificado.

Nota

- Esta opción solo está disponible para la grabación continua. Las cámaras deben admitir la velocidad de bits media y tener el firmware 9.40 o posterior.
 - Los ajustes de la velocidad de bits media influyen en la calidad del perfil de flujo seleccionado.
1. Vaya a **Configuration > Storage > Selection (Configuración > Almacenamiento > Selección)** y asegúrese de que ha definido un tiempo de conservación limitado para la cámara.
 2. Vaya a **Configuration > Devices > Stream profiles (Configuración > Dispositivos > Perfiles de flujo)** y asegúrese de que utiliza H.264 o H.265 como formato para el perfil de vídeo que se usará para grabaciones continuas.
 3. Vaya a **Configuración > Grabaciones y eventos > Método de grabación**.
 4. Seleccione la cámara y active **Continuous (Continua)**.
 5. En **Video settings (Ajustes de vídeo)**, seleccione el perfil de vídeo que ha configurado.
 6. Active **Average bitrate (Velocidad de bits media)** y defina el **Max storage (Almacenamiento máximo)**. EL sistema muestra la velocidad de bits media estimada en función del almacenamiento máximo especificado y el tiempo de conservación. La velocidad de bits media máxima es de 50 000 Kbit/s.

Nota

Max storage (almacenamiento máximo) indica el espacio máximo para las grabaciones durante el tiempo de conservación. Sólo garantiza que las grabaciones no excedan el espacio especificado, no garantiza que haya suficiente espacio para las grabaciones.

7. Haga clic en **Aplicar**.

Editar ajustes de movimiento

Si el dispositivo utiliza AXIS Object Analytics, puede editar los ajustes de la grabación de movimiento allí.

Nota

AXIS Object Analytics en AXIS Camera Station Pro requiere AXIS OS 12.4.

1. Abra una pestaña **Configuration (Configuración)**.

2. Vaya a **Recording and events (Grabación y eventos) > Recording method (Método de grabación)**.
3. Elija la cámara que desea configurar.
4. **Active Motion detection (Detección de movimiento)**.
5. Haga clic en **Motion Settings (Ajustes de movimiento)**.

Lea el *manual del usuario de AXIS Object Analytics* para obtener información sobre la configuración de AXIS Object Analytics en el dispositivo.

Editar AXIS Video Motion Detection 2 y 4

AXIS Video Motion Detection 2 y 4 son aplicaciones para cámaras que se pueden instalar en productos compatibles con AXIS Camera Application Platform. Cuando se instala AXIS Video Motion Detection 2 o 4 en la cámara, la detección de movimiento detecta objetos en movimiento dentro de un área de interés. Motion detection 2 requiere firmware 5.60 o posterior, y AXIS Video MotionDetection 4 requiere firmware 6.50 o posterior. También puede consultar las notas de versión del firmware de su producto to para comprobar si es compatible con detección de movimiento por vídeo 4.

Si se selecciona la detección de movimiento al agregar cámaras a AXIS Camera Station Pro, AXIS Video Motion Detection 2 y 4 se instalará en cámaras con el firmware necesario. Las cámaras sin el firmware requerido utilizan la detección de movimiento incorporada. Puede instalar la aplicación manualmente desde la página de gestión de dispositivos. Vea *Instalar la aplicación de la cámara*.

Con AXIS Video Motion Detection 2 y 4, podrá crear:

- **Área de interés:** Un área en una grabación donde la cámara detecta objetos en movimiento. La función ignora los objetos que quedan fuera del área de interés. El área se muestra encima de la imagen de vídeo en forma de polígono. El área puede tener de 3 a 20 puntas (esquinas).
- **Área de exclusión:** Un área dentro del área de interés en la que se ignoran los objetos en movimiento.
- **Filtros para ignorar:** Cree filtros para ignorar los objetos en movimiento que detecte la aplicación. Utilice los mínimos filtros posibles y configúrelos con cuidado para garantizar que no se ignore ningún objeto importante. Use y configure un filtro cada vez.
 - **Objetos que permanecen poco en la escena:** este filtro ignora los objetos que solo aparecen un breve periodo en la imagen. Por ejemplo, los haces de luz de un coche que pasa y las sombras que se mueven rápidamente. Establece el tiempo mínimo que deben aparecer los objetos en la imagen para activar una alarma. El tiempo se cuenta a partir del momento en el que la aplicación detecta el objeto. El filtro retrasa las alarmas y no las activa si el objeto desaparece de la imagen dentro del tiempo especificado.
 - **Objetos pequeños:** este filtro ignora los objetos que son pequeños, por ejemplo, los animales pequeños. Establece la anchura y la altura como un porcentaje de la imagen total. El filtro ignora los objetos más pequeños que la altura y la anchura especificadas y no activa ninguna alarma. El objeto debe ser más pequeño que los valores de ancho y alto para que el filtro lo ignore.
 - **Objetos con balanceo:** Este filtro ignora los objetos que solo se desplazan una distancia corta, por ejemplo, la vegetación o las banderas en movimiento y sus sombras. Establece la distancia como un porcentaje de la imagen total. El filtro ignora los objetos que se desplacen a una distancia inferior a la distancia que va desde el centro de la elipse hasta una de las puntas de flecha. La elipse es una medición del movimiento y se aplicará a todo el movimiento en la imagen.

Para configurar los ajustes de movimiento:

Nota

Los ajustes efectuados aquí cambiarán la configuración de la cámara.

1. Vaya a **Configuración > Grabaciones y eventos > Método de grabación**.
2. Seleccione una cámara con AXIS Video Motion Detection 2 o 4 y haga clic en **Configuración de movimiento**.
3. Editar el área de interés.

4. Editar el área de exclusión.
5. Crear filtros para ignorar.
6. Haga clic en **Aplicar**.

Añadir un nuevo punto	Para agregar un nuevo punto a su área de interés, haga clic en la línea entre dos puntos.
Quitar punto	Para eliminar un punto de su área de interés, haga clic en el punto y haga clic en Quitar punto .
Agregar área de exclusión	Para crear un área de exclusión, haga clic en Agregar área de exclusión y haga clic en la línea entre dos puntos.
Eliminar Excluir área	Para eliminar un área de exclusión, haga clic en Eliminar área de exclusión .
Filtro de objetos que permanecen poco en la escena	Para usar un filtro para objetos que permanecen poco en la escena, seleccione Filtro de objetos que permanecen poco en la escena y ajuste en el control deslizante de Tiempo el tiempo mínimo que deben aparecer los objetos para activar una alarma.
Small objects filter (Filtro de objetos pequeños)	Para usar un filtro para objetos pequeños, seleccione Filtro de objetos pequeños y ajuste en el control deslizante de Altura y Anchura el tamaño de los objetos que se han de ignorar.
Filtro de objetos con balanceo	Para usar un filtro para objetos con balanceo, seleccione Filtro de objetos con balanceo y ajuste en el control deslizante de Distancia el tamaño de la elipse.

Editar detección de movimiento integrada

Con la detección de movimiento incorporada, la cámara detecta movimiento dentro de una o más áreas incluidas e ignora todos los demás movimientos. Un área de inclusión es un área que detecta movimiento. Puede colocar un área de exclusión dentro de un área de inclusión para ignorar el movimiento. Se pueden usar varias áreas de inclusión y exclusión.

Para agregar y editar un área de inclusión:

Nota

Los ajustes efectuados aquí cambiarán la configuración de la cámara.

1. Vaya a **Configuración > Grabaciones y eventos > Método de grabación**.
2. Seleccione una cámara detección de movimiento integrada y haga clic en **Configuración de movimiento**.
3. Haga clic en **Add (Agregar)** en la sección **Window (Ventana)**.
4. Seleccione **Incluir**.
5. Para ver solo el área que edita, selecciona **Mostrar ventana seleccionada**.
6. Mueva y cambie el tamaño de la forma en la imagen del vídeo. Esta es el área de inclusión.
7. Ajuste **Tamaño del objeto**, **Historial** y **Sensibilidad** manualmente.
8. Para usar la configuración predefinida. Seleccione **Bajo**, **Moderado**, **Alto**, o **Muy alto**. **Bajo** detecta objetos de mayor tamaño con una historia más corta. **Muy alto** detecta objetos más pequeños con una historia más larga.

9. En la sección **Activity (Actividad)**, revise el movimiento detectado en el área de inclusión. Los picos rojos indican movimiento. Use el campo **Activity (Actividad)** al ajustar **Object size (Tamaño de objeto)**, **History (Historial)** y **Sensitivity (Sensibilidad)**.
10. Haga clic en **OK**.

Protección contra	Tamaño de objeto en relación al tamaño de la región. En un nivel alto, la cámara solo se detecta objetos muy grandes. En un nivel bajo, detecta incluso los objetos muy pequeños.
Historial	la longitud de memoria del objeto define cuánto tiempo debe permanecer un objeto en un área antes de considerarse sin movimiento. En un nivel alto, un objeto activará la detección de movimiento para un periodo de tiempo prolongado. En un nivel bajo un objeto desencadenará la detección de movimiento para un corto periodo de tiempo. Si no deben aparecer objetos en el área, seleccione un nivel de historia muy alto. Esto activa la detección de movimiento si el objeto está presente en el área.
Sensibilidad	diferencia de luminiscencia entre el fondo y el objeto. Con la alta sensibilidad, la cámara detecta objetos de color normal sobre fondos normales. Con una sensibilidad baja, sólo detecta objetos muy brillantes sobre un fondo oscuro. Para detectar únicamente una luz que parpadea, seleccione una sensibilidad baja. En el resto de casos, se recomienda un nivel de sensibilidad alto.

Para agregar y editar un área de exclusión:

1. En la pantalla **Editar detección de movimiento**, haga clic en **Agregar** en la sección **Ventana**.
2. Seleccione **Excluir**.
3. Mueva y cambie el tamaño de la forma sombreada en la imagen del vídeo.
4. Haga clic en **OK**.

Para eliminar un área de inclusión o exclusión:

1. En la pantalla **Editar detección de movimiento**, seleccione un área para eliminar.
2. Haga clic en **Remove (Eliminar)**.
3. Haga clic en **Aceptar**.

Configurar categorías de eventos

Las categorías de eventos facilitan la búsqueda de grabaciones de un determinado tipo, como agresiones o controles de tráfico. Para crear una categoría de evento:

1. Vaya a **Configuration (Configuración) > Recording and events (Grabación y eventos) > Event categories (Categorías de eventos)**.
2. Haga clic en **New (Nueva)**.
3. Introduzca un nombre para la categoría del evento.
4. De forma opcional, configure un color para la categoría de evento y un tiempo de retención personalizado para la categoría de evento.
5. Haga clic en **Aplicar**.

Nombre	Se recomienda utilizar un nombre para la categoría que represente un tipo de evento, como agresión o control de tráfico.
Tiempo de conservación	Puede establecer un tiempo de retención personalizado para cada categoría de evento que anule el tiempo de retención predeterminado de la cámara. El tiempo de retención de la categoría de evento personalizada solo se aplica si es mayor que el predeterminado.

Consulte *Categorías de eventos*, on page 27 para obtener más información.

Puertos de E/S

Muchas cámaras y codificadores de vídeo disponen de puertos de E/S para conexión de dispositivos externos. Algunos dispositivos auxiliares también pueden tener puertos de E/S.

Hay dos tipos de puertos de E/S:

Puerto de entrada – Se utiliza para la conexión de dispositivos que pueden conmutar entre un circuito abierto y cerrado. por ejemplo, contactos de puertas y ventanas, detectores de humo, detectores de rotura de cristal y PIR (detector pasivo por infrarrojos).

Puerto de salida – Se utiliza para conectarse a dispositivos como relés, puertas, cerraduras y alarmas. AXIS Camera Station Pro puede controlar dispositivos conectados a puertos de salida.

Nota

- Al conectarse a varios servidores de AXIS Camera Station Pro, puede seleccionar cualquier servidor conectado en el menú desplegable **Selected server (Servidor seleccionado)** para agregar y administrar los puertos de E/S.
- Los administradores pueden desactivar los puertos de E/S para los usuarios. Vea *Permisos de usuario*.

Las reglas de acción utilizan puertos de E/S como activadores o acciones. Los activadores utilizan señales de entrada, por ejemplo, cuando AXIS Camera Station Pro recibe una señal de un dispositivo conectado a un puerto de entrada, se llevarán a cabo acciones específicas. Las acciones usan puertos de salida, por ejemplo, cuando se activa una regla, AXIS Camera Station Pro puede activar o desactivar un dispositivo conectado a un puerto de salida. Vea *Reglas de actuación*.

Para obtener información acerca de cómo conectar dispositivos y cómo configurar puertos de E/S, consulte el manual de usuario o la guía de instalación de los productos Axis. Algunos productos tienen puertos que pueden actuar como entrada o salida.

Puede controlar los puertos de salida manualmente. Vea *Supervisar puertos de E/S*.

Agregar puertos de E/S

Para agregar puertos de E/S:

1. Vaya a **Configuración > Grabación y eventos > Puertos de E/S**.
2. Haga clic en **Add (Agregar)** para ver la lista de puertos de E/S que puede agregar.
3. Seleccione el puerto y haga clic en **OK (Aceptar)**.
4. Revise la información en **Type (Tipo)** y **Device (Dispositivo)**. Cambie la información si hace falta.
5. Introduzca un nombre en **Puerto**, **Estado activo** y **Estado inactivo**. Los nombres también se muestran en reglas de acción, Registros y supervisión de E/S.
6. Para los puertos de salida, puede configurar el estado inicial para cuando AXIS Camera Station Pro se conecte con el dispositivo. Seleccione **Al inicio definido** en y seleccione el estado inicial en el menú desplegable **Estado**.


Editar	Para editar un puerto, selecciónelo y haga clic en Editar . En el diálogo emergente, actualice la información del puerto y haga clic en Aceptar .
Eliminar	Para eliminar un puerto, selecciónelo y haga clic en Eliminar .
Recargar puertos de E/S	Si se han configurado puertos de E/S utilizando la página de ajustes del dispositivo, haga clic en Reload I/O Ports (Recargar puertos de E/S) para actualizar la lista.

Supervisar puertos de E/S

Nota

Al conectarse a varios servidores de AXIS Camera Station Pro, puede seleccionar cualquier servidor conectado en el menú desplegable **Selected server (Servidor seleccionado)** para supervisar puertos de E/S.

Para controlar los puertos de salida manualmente:

1. Vaya a  > **Actions (Acciones)** > **I/O Monitoring (Supervisión de E/S)**.
2. Seleccione un puerto de salida.
3. Haga clic en **Cambiar estado**.

Reglas de actuación

Utilice reglas de acción para responder automáticamente a los eventos. Por ejemplo, enviar un correo electrónico cuando una cámara detecta movimiento fuera del horario de oficina, interactuar con dispositivos conectados a los puertos de E/S y alertar a los operadores de eventos importantes.

Toda regla tiene activadores (eventos que activan la regla), acciones (lo que sucede cuando se activa) y una programación opcional. Al accionarse los activadores, la regla lleva a cabo todas las acciones.

Nota

- Cuando se conecta a múltiples servidores de AXIS Camera Station Pro, puede seleccionar cualquier servidor conectado en el menú desplegable **Selected Server (Servidor seleccionado)** para crear y gestionar reglas de acción.
- Para dispositivos de terceros, las acciones disponibles pueden diferir entre dispositivos. Muchas de estas acciones pueden requerir una configuración adicional en el dispositivo.

Permite crear una nueva regla de acción

1. Vaya a **Configuración** > **Grabaciones y eventos** > **Reglas de acción**.
2. Haga clic en **New... (Nueva...)**.
3. Introduzca un nombre para la regla en el campo **Nombre**.
4. En **Schedule (Programación)**, seleccione **Always (Siempre)** o **Custom schedule (Programación personalizada)** para seleccionar una programación del menú desplegable. También puede crear una nueva programación o editar una existente.
5. En **Triggers (Activadores)**, haga clic en **Add... (Añadir...)**, seleccione el tipo de activador, configúrelo y haga clic en **OK**. Consulte *Agregar activadores* para obtener más información.
6. En **Actions (Acciones)**, haga clic en **Add... (Añadir...)**, seleccione el tipo de acción, configúrelo y haga clic en **OK**. Consulte *Agregar acciones* para obtener más información.
7. Haga clic en **Aplicar**.
 - La regla se activa automáticamente al guardarla.

Editar	Para editar una regla existente, seleccione la regla y haga clic en Editar .
Copiar	Para copiar una regla existente, seleccione la regla y haga clic en Copy... (Copiar...) .
Eliminar	Para eliminar una regla, selecciónela y haga clic en Remove (Eliminar) .

Configure múltiples reglas de acción

Al seleccionar varias reglas, solo se muestran los activadores y las acciones que son iguales en todas las reglas seleccionadas. Cualquier cambio que realice se aplicará a todas las reglas seleccionadas.

- Vaya a **Configuración > Grabaciones y eventos > Reglas de acción**.
- Seleccionar varias reglas.
- Realice los cambios:
 - Añada activadores o acciones que se aplicarán a todas las reglas seleccionadas.
 - Elimine los activadores o acciones comunes a todas las reglas seleccionadas.
 - Modifique la programación de todas las reglas seleccionadas.
- Haga clic en **Aplicar**.

Nota

No es posible editar activadores o acciones individuales cuando se seleccionan varias reglas. Si sus cambios invalidaran alguna regla, no podrá aplicarlos.

Agregar activadores

Los activadores activan reglas y una regla puede tener varios activadores. La regla permanecerá activa siempre y cuando alguno de los activadores esté activo. Si quiere que la regla esté activa solo cuando todos los activadores estén activos, seleccione **All triggers must be active simultaneously to trigger the actions (Todos los activadores deben estar activos simultáneamente para activar las acciones)**. Aumente el periodo de activación si utiliza este ajuste en activadores de pulso. Los activadores de pulso son activadores que están activos temporalmente.

Están disponibles los desencadenadores siguientes:

Detección de movimiento – El movimiento registrado dentro de un área definida activa el activador de detección de movimiento. Vea *Crear activadores de detección de movimiento, on page 93*.

Siempre activo – Este activador está siempre activado. Por ejemplo, puede combinar este activador con una programación que siempre está activa y una acción de grabación con un perfil bajo para conseguir una segunda grabación continua adecuada para dispositivos con un rendimiento limitado.

Vista en vivo – El activador de visualización en directo se produce cuando un usuario abre el flujo de vídeo de una cámara específica. Puede utilizar esta opción, por ejemplo, para que las personas cercanas a una cámara sepan que alguien las está vigilando con los LED de la cámara. Consulte *Crear activadores de visualización en directo, on page 93*.

Evento del sistema y error – un activador de evento y error de sistema se activa cuando se producen errores de grabación, se llena un almacenamiento, no se puede conectar con un almacenamiento de red o se pierde la conexión con uno o más dispositivos. Vea *Crear activadores de eventos y errores de sistema, on page 94*.

Entrada/salida – El activador de Entrada/Salida (E/S) se activa cuando el puerto de E/S de un dispositivo recibe una señal, por ejemplo, de una puerta conectada, un detector de humos o un conmutador. Vea *Crear activadores de entrada/salida, on page 94*. Le recomendamos que, si es posible, utilice activadores de eventos de dispositivos en lugar de activadores de entrada/salida.

Evento del dispositivo – Este activador utiliza eventos directamente desde la cámara o dispositivo auxiliar. Utilice esto si no hay ningún activador disponible en AXIS Camera Station Pro. Vea *Crear activadores de eventos de dispositivo, on page 95*.

Botón de acción – Utilice los botones de acción para iniciar y detener acciones desde la visualización en directo. Puede usar un botón en distintas reglas. Vea *Crear activadores de botones de acción, on page 100*.

Evento de AXIS Entry Manager – Este activador se activa cuando AXIS Camera Station Pro recibe señales de puertas configuradas en AXIS Entry Manager. Por ejemplo, puertas forzadas a abrirse, abiertas demasiado tiempo o acceso denegado. Vea *Crear activadores de eventos AXIS Entry Manager, on page 101*.

HTTPS externo – El activador HTTPS externo permite que aplicaciones externas activen eventos en AXIS Camera Station Pro mediante comunicación por HTTPS. Vea *Crear activadores de HTTPS externos, on page 102*.

Crear activadores de detección de movimiento

El activador de detección de movimiento se activa cuando la cámara detecta movimiento en un área definida. Dado que la cámara procesa la detección, no agrega ninguna carga de procesamiento a AXIS Camera Station Pro.

Nota

Si la grabación de movimiento está activada en la cámara, evite utilizar activadores de detección de movimiento para iniciar grabaciones. Desactive la grabación de movimiento antes de utilizar los activadores de detección de movimiento. Para deshabilitar la grabación movimiento, vaya a **Configuration > Recording and events > Recording method (Configuración > Grabación y eventos > Método de grabación)**.

Para crear un activador de detección de movimiento:

1. Vaya a **Configuración > Grabaciones y eventos > Reglas de acción**.
2. Haga clic en **New (Nueva)**.
3. Haga clic en **Agregar** y seleccione **Detección de movimiento**.
4. Haga clic en **OK**.
5. En la pantalla emergente:
 - 5.1. Seleccione la cámara que debería detectar movimiento.
 - 5.2. Configure un intervalo de tiempo entre dos activadores sucesivos para reducir el número de grabaciones consecutivas. Si se produce una activación adicional dentro de este intervalo, la grabación continúa y se reinicia el período de activación.
 - 5.3. Haga clic en **Configuración de movimiento** para configurar los ajustes de detección de movimiento. Los ajustes disponibles son diferentes para cámaras diferentes. Vea *Editar detección de movimiento integrada y Editar AXIS Video Motion Detection 2 y 4*.
6. Haga clic en **Aceptar**.

Crear activadores de visualización en directo

El activador de visualización en directo se produce cuando un usuario abre el flujo de vídeo de una cámara específica. Puede utilizar esta opción, por ejemplo, para que las personas cercanas a una cámara sepan que alguien las está vigilando con los LED de la cámara.

Para crear un activador de visualización en directo:

1. Vaya a **Configuración > Grabaciones y eventos > Reglas de acción**.
2. Haga clic en **New (Nueva)**.
3. Haga clic en **Agregar** y, a continuación, seleccione **Visualización en directo**.
4. Haga clic en **OK**.
5. Seleccione la cámara de activador.
6. Haga clic en **Aceptar**.

Crear activadores de eventos y errores de sistema

Seleccione uno o más eventos y errores del sistema para utilizar como activadores. Algunos de los eventos de sistema son los errores de grabación, almacenamiento completo, error de conexión con un almacenamiento de red y pérdida de conexión por parte de algún dispositivo.

Para crear un activador de eventos y errores de sistema:

1. Vaya a **Configuración > Grabaciones y eventos > Reglas de acción**.
2. Haga clic en **New (Nueva)**.
3. Haga clic en **Agregar** y, a continuación, seleccione **Evento y error del sistema**.
4. Haga clic en **OK**.
5. Seleccione un evento o error del sistema para crear el activador.
6. Haga clic en **OK**.

<p>Error de grabación</p>	<p>Seleccione Error de grabación para activar el activador si se produce un error durante la grabación, por ejemplo, si una cámara deja de transmitir.</p>
<p>En almacenamiento completo</p>	<p>Seleccione En almacenamiento lleno para activar el activador cuando un almacenamiento de grabaciones está lleno.</p>
<p>Si no se tiene contacto con el almacenamiento de red</p>	<p>Seleccione On no contact with network storage (Si no se tiene contacto con el almacenamiento de red) para activar el activador cuando existe un problema de acceso a un almacenamiento de red.</p>
<p>Si se pierde la conexión con la cámara</p>	<p>Seleccione On lost connection to camera (Si se pierde conexión con la cámara) para activar el activador cuando existe un problema de contacto con las cámaras.</p> <ul style="list-style-type: none"> • Seleccione All (Todas) para incluir todas las cámaras que se han agregado a AXIS Camera Station Pro. • Elija Selected (Seleccionado) y haga clic en Cameras (Cámaras) para que se muestre la lista de las cámaras agregadas a AXIS Camera Station Pro. Use Select all (Seleccionar todo) para seleccionar todas las cámaras o Deselect all (Deseleccionar todo) para deseleccionar todas las cámaras.

Crear activadores de entrada/salida

El activador de entrada/salida (E/S) se activa cuando el puerto de E/S de un dispositivo recibe una señal, por ejemplo, de una puerta conectada, un detector de humos o un conmutador.

Nota

- Agregue el puerto de E/S a AXIS Camera Station Pro antes de utilizar un activador de E/S. Vea *Puertos de E/S*.
- Si es posible, utilice activadores de eventos de dispositivos en lugar de activadores de entrada/salida. Los activadores de eventos de los dispositivos ofrecen una mejor experiencia de usuario general. Consulte *Crear activadores de eventos de dispositivo, on page 95* para obtener más información.

Para crear un activador de entrada/salida:

1. Vaya a **Configuración > Grabaciones y eventos > Reglas de acción**.

2. Haga clic en **New** (Nueva).
3. Haga clic en **Agregar** y, a continuación, seleccione **Entrada/Salida**.
4. Haga clic en **OK**.
5. En **Trigger port and state (Puerto y estado del activador)**, configure el puerto de E/S y los ajustes del activador.
6. Haga clic en **OK**.

Puerto y estado del activador	
Puerto de E/S	En I/O port (Puerto de E/S) , seleccione el puerto de entrada o salida.
Estado de activación	En Trigger state (Estado de activación) , seleccione el estado del puerto de E/S que debe activar el activador. Los estados disponibles dependen de la configuración del puerto.
Trigger period (Período de activación)	Configure un intervalo de tiempo entre dos activadores sucesivos en Trigger period (Periodo de activación) para reducir el número de grabaciones consecutivas. Si se produce una activación adicional dentro de este intervalo, la grabación continúa y se reinicia el período de activación.

Crear activadores de eventos de dispositivo

Este activador utiliza eventos directamente desde la cámara o dispositivo auxiliar. Utilice esto si no hay ningún activador disponible en AXIS Camera Station Pro. Los eventos son distintos en cada cámara y tienen uno o varios filtros que deben definirse. Los filtros son condiciones que deben cumplirse para que el activador de eventos del dispositivo se active. Para obtener información sobre eventos y filtros en productos Axis, consulte la documentación de VAPIX® en axis.com/partners y axis.com/vapix.

Para crear un activador de eventos de dispositivo:

1. Vaya a **Configuración > Grabaciones y eventos > Reglas de acción**.
2. Haga clic en **New** (Nueva).
3. Haga clic en **Agregar** y, a continuación, seleccione **Evento de dispositivo**.
4. Haga clic en **OK**.
5. En **Configure device event trigger (Configurar activador de evento de dispositivo)**, configure un activador de eventos.

Nota

Los eventos disponibles dependen del dispositivo seleccionado. Para dispositivos de terceros, muchos de estos eventos requieren una configuración adicional en el dispositivo.

6. En **Filters (Filtros)**, seleccione los filtros.
7. En **Activity (Actividad)**, compruebe el estado actual del activador de eventos del dispositivo como una función de tiempo. Un evento puede ser con estado o sin estado. La actividad de un evento con estado se representa mediante una función incremental. Una línea recta con pulsos desde cuando se activa el evento representa la actividad de un evento sin estado.
8. Haga clic en **OK**.

Configurar desencadenador de eventos de dispositivo	
Dispositivo	En Device (Dispositivo) , seleccione la cámara o el dispositivo auxiliar.
Evento	En Event (Evento) , seleccione el evento que se usará como activador.
Trigger period (Período de activación)	En el campo Trigger period (Periodo de activación) , configure un intervalo de tiempo entre dos activadores sucesivos para reducir el número de grabaciones consecutivas. Si se produce una activación adicional dentro de este intervalo, la grabación continúa y se reinicia el período de activación.

Ejemplos de eventos de dispositivo

Categoría	Evento del dispositivo
Amplificador	Sobrecarga del amplificador
Control de audio	Estado de la señal digital
Fuente de audio	Detección de audio
Autorización	Solicitud de acceso concedida
	Solicitud de acceso denegada
Llamar	Estado
	Cambio de estado
	Calidad de la red
	Estado de la cuenta SIP
	Vídeo entrante
Carcasa	Carcasa abierta
Dispositivo	Protección contra sobretensión con transformador de corriente
Sensores de dispositivos	Sistema preparado
	Sensor de PIR
Estado de los dispositivos	Sistema preparado
Puerta	Puerta forzada
	Se ha detectado la manipulación de la instalación de la puerta
	Puerta bloqueada
	Puerta abierta durante demasiado tiempo
	Posición de puerta
	Puerta desbloqueada
Búfer de eventos	Comienzo
Registro de eventos	Alarmas no registradas

	Eventos no registrados
	Alarma
Ventilador	Estado
Cambio de escena global	Servicio de imagen
Error de hardware	Error de almacenamiento
	Error del ventilador
Calefactor	Estado
Puertos de entrada	Entrada virtual
	Puerto de entrada digital
	Activador manual
	Puerto de entrada supervisada
	Puerto de salida digital
	Entrada interna
Luz	Estado
Estado de la luz modificado	Estado
Medios	Perfil cambiado
	Configuración cambiada
Supervisar	Latido
Detector de región del movimiento	Movimiento
Red	Pérdida de red
	Solo aplicable a los eventos utilizados por el dispositivo, no aplicable a los eventos utilizados por AXIS Camera Station Pro.
	Dirección agregada
	Dirección eliminada
Movimiento PTZ	Movimiento PTZ en el canal <nombre del canal>
Posiciones predefinidas de PTZ	Se ha alcanzado la posición predefinida de PTZ en el canal <nombre del canal>
Controlador PTZ	Auto-tracking (seguimiento automático)
	Cola de control PTZ
	Error PTZ
	PTZ lista
Configuración de la grabación	Crear grabación
	Eliminar grabación
	Seguimiento de configuración
	Configuración de grabación
	Configuración del trabajo de grabación

Cámara remota	Estado de Vapix
	Posición PTZ
Horario	Impulso
	Intervalo
	Evento programado
Estado	Activo
Almacenamiento	Interrupción del almacenamiento
	Grabación continua
Mensaje del sistema	Acción fallida
Manipulación	Inclinación detectada
	Impacto detectado
Sensores de temperatura	Por encima de la temperatura de funcionamiento
	Por debajo de la temperatura de funcionamiento
	Dentro de la temperatura de funcionamiento
	Por encima o por debajo de la temperatura de funcionamiento
Activador	Relés y salidas
	Entrada digital
Detección de movimiento por vídeo	VMD 4: perfil <nombre de perfil>
	VMD 4: cualquier perfil
Video Motion Detection 3	VMD 3
Fuente de vídeo	Alarma de movimiento
	Acceso a secuencias de vídeo en directo
	Visión día o noche
	Manipulación de la cámara
	Degradación de velocidad de bits media
	Fuente de vídeo conectada

Eventos de dispositivo de la controladora de accesos en red de Axis

Evento del dispositivo	Activar la regla de acción
Autorización	
Solicitud de acceso concedida	El sistema concedió acceso a un titular de tarjeta cuando se identificó con sus credenciales.
Coacción	Alguien usó el PIN de coacción. Puede utilizar esta opción, por ejemplo, para activar una alarma silenciosa.
Solicitud de acceso denegada	El sistema denegó el acceso a un titular de tarjeta cuando se identificó con sus credenciales.

Doble deslizamiento	Un titular de tarjeta pasa su tarjeta dos veces. El doble deslizamiento permite que un titular de tarjeta invalide el estado actual de una puerta. Por ejemplo, pueden usarla para desbloquear una puerta fuera de la programación normal.
Detección antipassback	Alguien usó una credencial perteneciente a un titular de tarjeta que entró en una zona antes que él.
Autorización con regla de dos personas	
Solicitud de acceso pendiente	El primero de cada dos titulares de tarjeta se ha identificado con las credenciales.
Solicitud de acceso concedida	El sistema concedió acceso al último titular de tarjeta cuando se identificó con las credenciales.
Carcasa	
Carcasa abierta	La carcasa del controlador de puerta en red se abre o retira. Puede utilizarse, por ejemplo, para enviar una notificación al administrador si se abre la carcasa para fines de mantenimiento o si alguien la ha manipulado.
Estado de los dispositivos	
Sistema preparado	El sistema está en el estado de preparado. Por ejemplo, el producto Axis detecta el estado del sistema y envía una notificación al administrador cuando se ha iniciado el sistema. Seleccione el botón de radio Sí para activar la regla de acción cuando el producto esté en estado preparado. Tenga en cuenta que la regla solo se puede activar cuando todos los servicios necesarios, como el sistema de eventos, se hayan iniciado.
Puerta	
Puerta forzada	Se ha forzado la apertura de la puerta.
Se ha detectado la manipulación de la instalación de la puerta	Cuando el sistema detecta lo siguiente: <ul style="list-style-type: none"> • La carcasa del dispositivo se abre o cierra • Movimiento del dispositivo • Extracción del lector conectado de la pared • Manipulación del monitor de puerta, lector o dispositivo REX conectado. Para usar este activador, asegúrese de activar la función de entradas supervisadas y de revisar la instalación de las resistencias de final de línea en los puertos de entrada del conector de la puerta correspondiente.
Puerta bloqueada	La cerradura de la puerta está bloqueada.
Puerta abierta durante demasiado tiempo	La puerta está abierta demasiado tiempo.
Posición de puerta	El monitor de puerta indica que la puerta está abierta o cerrada.
Puerta desbloqueada	La cerradura de la puerta permanece desbloqueada. Puede utilizar este estado, por ejemplo, para permitir la entrada de visitantes que no tienen que presentar sus credenciales.
Puertos de entrada	
Entrada virtual	Cambia el estado de una de las entradas virtuales. Puede usarlas un cliente, como un software de gestión, para iniciar diversas acciones.

	Seleccione el puerto de entrada que debe activar la regla de acción cuando se active.
Puerto de entrada digital	Cambia el estado de un puerto de entrada digital. Use este activador para iniciar varias acciones, por ejemplo, enviar notificaciones o hacer parpadear el LED de estado. Seleccione el puerto de entrada que debe activar la regla de acción cuando se active o seleccione Any (Cualquiera) para activar la regla de acción cuando se active uno de los puertos de entrada.
Activador manual	Desencadena el activador manual. Use este activador para iniciar o detener manualmente la regla de acción a través de la API VAPIX.
Entrada interna	La entrada de emergencia está activa o inactiva.
Red	
Pérdida de red	Pérdida de conexión de la red. Solo aplicable a los eventos utilizados por el dispositivo, no aplicable a los eventos utilizados por AXIS Camera Station Pro.
Dirección agregada	Se agrega una nueva dirección IP.
Dirección eliminada	Se elimina la dirección IP.
Horario	
Evento programado	Cambia el estado de una programación predefinida. Utilícelo para grabar vídeo en periodos de tiempo concretos, por ejemplo, en horario de oficina, los fines de semana, etc. Seleccione una programación en el menú desplegable Schedule (Programación) .
Mensaje del sistema	
Acción fallida	Una regla de acción genera un error y activa el mensaje de sistema de error en la acción.
Activador	
Entrada digital	Un puerto de entrada digital físico está activo o inactivo.

Crear activadores de botones de acción

Use los botones de acción para iniciar y detener acciones en **Live view (Visualización en directo)**. Los botones de acción se encuentran en la parte inferior de la visualización en directo o en un mapa. Puede usar un botón para varias cámaras y mapas. También puede haber varios botones de acción para una cámara o un mapa. Puede organizar los botones para una cámara al agregar o editar el botón de acción.

Existen dos tipos de botones de acción:

Botones de comando – Se usa para iniciar manualmente una acción. Utilice los botones de comando para acciones que no requieran botón de parada. Un botón de comando dispone de una etiqueta de botón y una sugerencia. La etiqueta para el botón de comando es el texto que aparece en el botón. Desplace el ratón sobre el botón para que se muestre la sugerencia.

Ejemplo: Cree un botón para activar una salida durante un tiempo predefinido, generar una alarma y enviar un correo electrónico.

Botones de conmutación – Se usa para iniciar y detener manualmente una acción. El botón tiene dos fases: activado y desactivado. Haga clic en el botón para cambiar entre los dos estados. De forma predeterminada, los botones de conmutación inician la acción cuando están en estado de activación, pero también se puede iniciar la acción en estado de desactivación.

Un botón de conmutación tiene una etiqueta de activación, una etiqueta de desactivación y una sugerencia. Los textos que se muestran en los botones en los estados activado y desactivado son las etiquetas de activación y desactivación. Desplace el ratón sobre el botón para que se muestre la sugerencia.

Ejemplo: Para crear un botón para abrir y cerrar puertas, use la acción de salida con el impulso definido como "siempre que algún activador esté activo".

Para crear un activador de botón de acción:

1. Vaya a **Configuración > Grabaciones y eventos > Reglas de acción**.
2. Haga clic en **New (Nueva)**.
3. Haga clic en **Agregar** y, a continuación, seleccione **Botón de acción**.
4. Haga clic en **OK**.
5. Seleccione **Crear nuevo botón** o **Usar botón existente**. Haga clic en **Next (Siguiente)**.
6. Si selecciona **Create new button (Crear nuevo botón)**:
 - 6.1. Seleccione **Botón de comando** o **Botón on/off**. Si quiere usar el botón de conmutación para iniciar la acción en el estado de desactivación, seleccione **Desencadenar en estado desactivado**.
 - 6.2. Haga clic en **Next (Siguiente)**.
 - 6.3. Agregar etiquetas y sugerencias para el botón.

Nota

La letra o el número después del primer subrayado en una etiqueta de un botón de acción pasa a ser la clave de acceso del botón de acción. Pulse ALT y la tecla de acceso para activar el botón de acción. Por ejemplo, al nombrar un botón de acción como A_BC, el nombre del botón de acción cambia a ABC en la visualización en directo. Pulse ALT + B y se activará el botón de acción.

7. Si selecciona **Use existing button (Usar botón existente)**:
 - 7.1. Busque el botón o haga clic en el botón que quiere utilizar.
 - 7.2. Si selecciona utilizar un botón de conmutación existente, debe seleccionar **Trigger on toggle (Desencadenar en estado activado)** o **Trigger on untoggle (Desencadenar en estado desactivado)**.
 - 7.3. Haga clic en **Next (Siguiente)**.
 - 7.4. Edite las etiquetas y sugerencias para el botón.
8. Seleccione la cámara o el mapa del menú desplegable.
9. Para agregar el botón a varias cámaras o mapas, haga clic en **Agregar a varias cámaras** o **Agregar a varios mapas**.
10. Si una cámara dispone de varios botones de acción, haga clic en **Arrange (Ordenar)** para modificar el orden de los botones. Haga clic en **OK**.
11. Haga clic en **Next (Siguiente)**.

Crear activadores de eventos AXIS Entry Manager

AXIS Camera Station Pro activa el desencadenador cuando recibe señales de puertas configuradas en AXIS Entry Manager. Por ejemplo, puertas forzadas a abrirse, puertas abiertas demasiado tiempo o acceso denegado.

Nota

El activador de eventos AXIS Entry Manager solo está disponible si se agrega AXIS A1001 Network Door Controller a AXIS Camera Station Pro.

1. Vaya a **Configuración > Grabaciones y eventos > Reglas de acción**.
2. Haga clic en **New (Nueva)**.
3. Haga clic en **Add (Agregar)** y seleccione **AXIS Entry Manager event (Evento de AXIS Entry Manager)**.
4. Haga clic en **OK**.

5. Seleccione un evento y una puerta para activar el activador.
6. Haga clic en **OK**.

Crear activadores de HTTPS externos

El activador HTTPS externo permite que aplicaciones externas activen eventos en AXIS Camera Station Pro mediante comunicación por HTTPS. Este activador solo admite la comunicación HTTPS y requiere que facilite el nombre de usuario de AXIS Camera Station Pro válido, incluidos el nombre de dominio y la contraseña en las solicitudes HTTPS.

Las siguientes solicitudes son compatibles con el método HTTP GET*. También puede utilizar POST con datos JSON que aparezcan en el cuerpo de la solicitud.

Nota

- Las solicitudes de activadores HTTPS externos solo se pueden probar en Google Chrome.
- El activador HTTPS externo utiliza el mismo puerto que la aplicación de visualización en móviles, vea Puerto de comunicación móvil y Puerto de transmisión móvil según se describen en *General*.
- Inicie el activador con el ID "trigger1": `https://[address]:29204/Acs/Api/TriggerFacade/ActivateTrigger?{"triggerName":"trigger1"}`
- Desactive el activador con el ID "trigger1": `https://[address]:29204/Acs/Api/TriggerFacade/DeactivateTrigger?{"triggerName":"trigger1"}`
- Inicie el activador con el ID "trigger1" y, a continuación, desactívelo automáticamente una vez transcurridos 30 segundos: `https://[address]:29204/Acs/Api/TriggerFacade/ActivateDeactivateTrigger?{"triggerName":"trigger1","deactivateAfterSeconds":"30"}`

Nota

El temporizador de la desactivación automática se cancela si se envía otro comando al mismo activador.

- Active y desactive inmediatamente el activador con el ID "trigger1": `https://[address]:29204/Acs/Api/TriggerFacade/PulseTrigger?{"triggerName":"trigger1"}`

Para crear un activador HTTPS externo:

1. Vaya a **Configuración > Grabaciones y eventos > Reglas de acción**.
2. Haga clic en **New (Nueva)**.
3. Haga clic en **Agregar** y seleccione **HTTPS externo**.
4. Haga clic en **OK**.
5. Introduzca un nombre de activador en **Trigger name (Nombre de activador)**.
6. Revise la URL de muestra que emplea la misma dirección del servidor que utilizó el cliente al iniciar sesión. Las URL solo funcionan una vez que se completan las reglas de acción.
7. Haga clic en **Aceptar**.

Acciones aptas para activadores HTTPS externos

- Las solicitudes para activar y desactivar el activador son aptas para acciones que inicien y detengan grabaciones.
- Las solicitudes para enviar pulsos al activador son aptas para acciones como **Raise Alarm (Generar alarma)** o **Send Email (Enviar correo electrónico)**.

Crear activadores de búsqueda inteligente 2

Para crear un activador de búsqueda inteligente 2:

1. Vaya a **Configuración > Grabaciones y eventos > Reglas de acción**.
2. Haga clic en **New (Nueva)**.

3. Haga clic en **Add (Añadir)** y seleccione **Smart search 2 (Búsqueda inteligente 2)**.
4. Haga clic en **OK**.
5. Seleccione y configure el activador:
 - Para crear un filtro de búsqueda inteligente que se pueda usar como activador, consulte *Desencadenadores, on page 177*.
 - Elija **High processing delay (Retardo de procesamiento alto)** para activar el activador cuando la búsqueda inteligente 2 tarde más de un minuto en procesar las detecciones.
6. Haga clic en **OK**.

Crear activadores de Audio Manager

Para crear un activador de Audio Manager:

1. Vaya a **Configuración > Grabaciones y eventos > Reglas de acción**.
2. Haga clic en **New (Nueva)**.
3. Haga clic en **Add (Añadir)** y seleccione **Audio Manager (Administrador de audio)**.
4. Haga clic en **OK**.
5. Seleccione y configure el activador.
6. Haga clic en **OK**.

Estado del dispositivo cambiado	Seleccione Device status changed (Estado del dispositivo cambiado) para activar el activador cuando cambie el estado del dispositivo, por ejemplo, al conectarse o desconectarse.
Estado de reproducción cambiado	Seleccione Playback status changed (Estado de reproducción cambiado) para activar el activador al iniciarse o detenerse la reproducción.
Destino habilitado o deshabilitado	Seleccione Target enabled or disabled (Destino habilitado o deshabilitado) para activar el activador al activarse o desactivarse el destino del activador.
Volumen del controlador de volumen cambiado	Seleccione Volume controller volume changed (Volumen del controlador de volumen cambiado) para activar el disparador cuando cambie la configuración del controlador de volumen.

Agregar acciones

Una regla puede tener varias acciones. Las acciones se inician cuando se activa la regla.

Están disponibles las acciones siguientes:

Grabar – esta acción inicia una grabación desde la cámara. Vea *Crear acciones de grabación*.

Generar alarma – Esta acción envía una alarma a todos los clientes AXIS Camera Station Pro. Vea *Crear acciones de generación de alarmas*.

Definir salida – Esta acción establece el estado de un puerto de salida. Úsela para controlar el dispositivo conectado al puerto de salida, por ejemplo, para encender una luz o bloquear una puerta. Vea *Crear acciones de salida*.

Enviar correos electrónicos – esta acción envía un mensaje de correo electrónico a uno o varios destinatarios. Vea *Crear acciones de envío de correos electrónicos*.

Vista en vivo – Esta acción abre la visualización en directo de una cámara, vista o posición predefinida específica en todos los clientes de AXIS Camera Station Pro. También puede usar la acción de visualización en directo para restaurar clientes de AXIS Camera Station Pro abiertos desde la barra de tareas o para situar clientes al frente de otras aplicaciones. Vea *Crear acciones de visualización en directo*.

Enviar notificación HTTP – esta acción envía una solicitud HTTP a una cámara, a un controlador de puerta o a un servidor web externo. Vea *Crear acciones de notificación HTTP*.

Sirena y luz – Esta acción activa una sirena y un patrón de luces en un dispositivo compatible conforme a un perfil preconfigurado. Vea *Crear acciones de sirena y luz, on page 110*.

E/S virtual – Esta acción activa un puerto de entrada virtual específico en un dispositivo. Vea *Crear acciones virtuales de E/S, on page 110*

AXIS Entry Manager – esta acción puede conceder acceso, bloquear o desbloquear una puerta conectada a un controlador de puerta configurado por AXIS Entry Manager. Vea *Crear acciones AXIS Entry Manager, on page 110*.

Enviar notificación de aplicación móvil – Esta acción envía un mensaje personalizado a la aplicación móvil de AXIS Camera Station. Vea *Crear acciones de notificación de envío de aplicación móvil, on page 111*.

La reglas se activan o desactiva. – Utilice esta acción para activar o desactivar otras reglas de acción. Vea *Crear una acción que activa o desactiva otras reglas de acción, on page 111*.

Enviar al decodificador de vídeo – Utilice esta acción si desea enviar una vista a un decodificador de vídeo para que se muestre en un monitor durante un periodo de tiempo determinado. Vea *Crear una acción que envíe una vista a un decodificador de vídeo, on page 112*

Control de acceso – esta acción incluye acciones de puerta y acciones de zona en AXIS Camera Station Secure Entry. Vea *Crear acciones de control de acceso, on page 112*.

Crear acciones de grabación

La acción de grabación empieza a grabar desde la cámara. Puede acceder a la grabación y reproducirla desde la pestaña Recordings (Grabaciones).

Para crear una acción de grabación:

1. Especifique una ubicación para guardar la grabación. Vaya a **Configuration > Storage > Selection (Configuración > Almacenamiento > Selección)**.
2. Vaya a **Configuración > Grabaciones y eventos > Reglas de acción**.
3. Haga clic en **New (Nueva)**.
4. Haga clic en **Agregar** y cree un activador. Haga clic en **Next (Siguiente)**. Vea *Agregar activadores*.
5. Haga clic en **Agregar** y seleccione **Grabar**.
6. Haga clic en **OK**.
7. En **Camera (Cámara)**, seleccione la cámara desde la que se va a grabar.
8. En **Video setting (Ajustes de vídeo)**, configure el perfil, búfer anterior y búfer posterior.
9. En **Event setting (Ajuste de evento)**, seleccione qué categoría de evento desea asignar a la grabación, si corresponde.
10. Haga clic en **Aceptar**.

Configuración de vídeo	
Perfil	Seleccione un perfil en el menú desplegable Profile (Perfil) . Para editar los ajustes del perfil, consulte <i>Perfiles de transmisión</i> .
Búfer anterior	Establezca el número de segundos antes del movimiento detectado para incluirlo en una grabación.
Búfer posterior	Determine el número de segundos que se deben incluir en la grabación cuando la acción deja de ejecutarse.

Crear acciones de generación de alarmas

La acción elevar alarma envía una alarma a todos los clientes de AXIS Camera Station Pro conectados. La alarma aparece en la pestaña **Alarms (Alarmas)** como una notificación de la barra de tareas. Se pueden incluir instrucciones en formato de archivo con los procedimientos de alarma junto con la alarma. El procedimiento de alarma está disponible en la pestaña **Alarmas** y en el espacio de trabajo **Registros**.

Para crear una acción de generación de alarma:

1. Vaya a **Configuración > Grabaciones y eventos > Reglas de acción**.
2. Haga clic en **New (Nueva)**.
3. Haga clic en **Agregar** y cree un activador. Haga clic en **Next (Siguiete)**. Vea *Agregar activadores*.
4. Haga clic en **Agregar** y, a continuación, seleccione **Generar alarma**.
5. Haga clic en **OK**.
6. En **Alarm message (Mensaje de alarma)**, configure el título, la descripción y la duración.
7. En **Alarm procedure (Procedimiento de alarma)**.
 - 7.1. Seleccione **En alarma, mostrar procedimiento de alarma**.
 - 7.2. Haga clic en **Upload (Cargar)** y busque el archivo deseado.
 - 7.3. Haga clic en **Previsualizar** para abrir el archivo cargado en una ventana de vista previa
 - 7.4. Haga clic en **OK**.

Mensaje de alarma	
Título	introduzca un título para la alarma. El título aparece en Alarms (Alarmas) en la pestaña Alarms (Alarmas) y en la notificación de la barra de tareas.
Descripción	Introduzca una descripción breve de la alarma. La descripción aparece en Alarms > Description (Alarmas > Descripción) en la pestaña Alarms (Alarmas) y en la notificación de la barra de tareas.
Duration (s) (Duración [s])	Ajuste el tiempo de duración entre 1 y 600 segundos para las alarmas emergentes.

Crear acciones de salida

La acción de salida establece el estado de un puerto de salida. Se utiliza para controlar el dispositivo conectado al puerto de salida, por ejemplo, para encender una luz o bloquear una puerta.

Nota

Agregue el puerto de salida a AXIS Camera Station Pro antes de utilizar una acción de salida. Vea *Puertos de E/S*.

Para crear una acción de salida:

1. Vaya a **Configuración > Grabaciones y eventos > Reglas de acción**.
2. Haga clic en **New (Nueva)**.
3. Haga clic en **Agregar** y cree un activador. Haga clic en **Next (Siguiente)**. Vea *Agregar activadores*.
4. Haga clic en **Agregar** y, a continuación, seleccione **Establecer salida**.
5. Haga clic en **OK**.
6. En **Output port (Puerto de salida)**, seleccione el puerto de salida.
7. En **State on action (Estado en acción)**, seleccione el estado con el que se va a definir el puerto. Las opciones disponibles dependen de la configuración del puerto.
8. Seleccione **Impulso** para definir cuánto tiempo debe permanecer el puerto de salida en el nuevo estado.

Nota

Para mantener el puerto en el nuevo estado después de la acción, desmarque **Impulso**.

9. Haga clic en **OK**.

Mientras un desencadenador esté activo	Para mantener el puerto en el nuevo estado mientras todos los desencadenadores de la regla estén activos, seleccione Mientras un desencadenador esté activo .
Mantener el estado durante un tiempo determinado	Para mantener el puerto en el nuevo estado durante un periodo de tiempo fijo, seleccione la opción de segundos y especifique el número de segundos.

Crear acciones de envío de correos electrónicos

La acción de correo electrónico envía un mensaje de correo electrónico a uno o varios destinatarios. Se pueden adjuntar instantáneas de las cámaras con el correo electrónico.

Nota

Para enviar correos electrónicos, primero hay que configurar un servidor SMTP. Vea *Configuración de puertos del servidor*.

Para crear una acción de envío de correos electrónicos:

1. Vaya a **Configuración > Grabaciones y eventos > Reglas de acción**.
2. Haga clic en **New (Nueva)**.
3. Haga clic en **Agregar** y cree un activador. Haga clic en **Next (Siguiente)**. Vea *Agregar activadores*.
4. Haga clic en **Agregar** y, a continuación, seleccione **Enviar correo electrónico**.
5. Haga clic en **OK**.
6. Agregue destinatarios en **Recipients (Destinatarios)**:
 - 6.1. Introduzca la dirección de correo electrónico en **New Recipient (Destinatario nuevo)** y seleccione **To (Para)**, **Cc (CC)** o **Bcc (CCO)**.
 - 6.2. Haga clic en **Add (Agregar)** para agregar la dirección de correo electrónico a **Recipients (Destinatarios)**.
7. En **Contents (Contenido)**, introduzca el asunto y el mensaje del correo electrónico.
8. En **Advanced (Configuración avanzada)**, configure adjuntos, número de correos electrónicos e intervalos.
9. Haga clic en **Aceptar**.

Avanzada	
Adjuntar instantáneas	Para adjuntar instantáneas en formato .jpg de las cámaras en la notificación por correo electrónico en forma de archivo adjunto, seleccione Attach snapshots (Adjuntar instantáneas) y haga clic en Cameras (Cámaras) . Aparece una lista de las cámaras agregadas a AXIS Camera Station Pro. Puede elegir Select all (Seleccionar todo) para seleccionar todas las cámaras o Deselect all (Deseleccionar todo) para deseleccionar todas las cámaras.
Enviar un correo electrónico por cada evento	Para evitar enviar múltiples correos electrónicos por el mismo evento, seleccione Enviar un correo electrónico por cada evento .
No enviar otro correo electrónico para	Para evitar enviar correos electrónicos demasiado cerca en el tiempo. Seleccione Don't send another email for (No enviar otro correo electrónico en) y establezca el tiempo mínimo entre correos electrónicos en el menú desplegable.

Crear acciones de visualización en directo

La acción en directo abre la pestaña **Live view (Visualización en directo)** con una cámara, vista o posición predefinida específica. La pestaña **Live view (Visualización en directo)** abre todos los clientes de AXIS Camera Station Pro conectados. Si la pestaña **Live view (Visualización en directo)** muestra una vista dividida con un punto clave, la cámara seleccionada en la acción de visualización en directo se carga en el punto clave. Para obtener más información sobre los puntos clave, consulte *Vista dividida*.

También puede usar la acción de visualización en directo para restaurar clientes de AXIS Camera Station Pro abiertos desde la barra de tareas o para situar clientes al frente de otras aplicaciones.

Para crear una acción de visualización en directo:

1. Vaya a **Configuración > Grabaciones y eventos > Reglas de acción**.
2. Haga clic en **New (Nueva)**.
3. Haga clic en **Agregar** y cree un activador. Haga clic en **Next (Siguiente)**. Vea *Agregar activadores*.
4. Haga clic en **Agregar** y, a continuación, seleccione **Visualización en directo**.
5. Haga clic en **OK**.
6. En **Live view actions (Acciones de visualización en directo)**, defina qué debe mostrarse cuando la acción esté activa.
7. En **Shown in (Se muestra en)**, configure cómo debe mostrarse la vista seleccionada.
8. En la sección **Bring to front (Llevar al frente)**, seleccione **On trigger bring application to front (En alarma mostrar la aplicación en primer plano)** para restaurar los clientes de AXIS Camera Station Pro abiertos desde la barra de tareas o llevar los clientes al frente de otras aplicaciones abiertas cuando se inicie la acción de visualización en directo.
9. Haga clic en **OK**.

Acciones en vivo	
Ver	Para abrir una visualización, seleccione View (Ver) y seleccione el área de visión deseada en el menú desplegable.
Cámara	Para abrir una visualización de cámara, seleccione Camera (Cámara) y seleccione la cámara en el menú desplegable. Si la cámara tiene una posición predefinida PTZ, seleccione Go to preset (Ir a posición predefinida) y seleccione un área del menú desplegable para abrir una posición predefinida.
Sin acción	Seleccione No action (Sin acción) para que no se abra ninguna vista.

Se muestra en	
Pestaña de alerta en vivo	Seleccione Live alert tab (Pestaña de alerta en directo) para abrir la vista seleccionada o la vista de cámara en la pestaña Live alert (Alerta en directo) .
Punto clave en vista	Seleccione Hotspot in view (Punto clave en la vista) y elija una vista con punto clave en el menú desplegable. Si el punto clave es visible en la visualización en directo cuando se activa la acción, la vista de cámara se muestra en el punto clave.

Ejemplo:

Para abrir una pestaña **Live view (Visualización en directo)**, vaya a la vista de punto clave y mostrar una vista de cámara en el punto clave, configure dos acciones de visualización en directo en una misma regla de acción:

1. Cree una acción de visualización en directo que muestre la vista de punto clave en la pestaña **Live alert (Alerta en directo)**.
 - 1.1. En **Live view actions (Acciones de visualización en directo)**, seleccione **View (Ver)**.
 - 1.2. Seleccione **Hotspot view (Vista de punto clave)**.
 - 1.3. En **Show in (Mostrar en)**, seleccione la pestaña **Live alert (Alerta en directo)**.
 - 1.4. Seleccione **On trigger bring application to front (En alarma mostrar la aplicación en primer plano)**.
2. Cree otra acción de visualización en directo para ir hasta la vista de punto clave y mostrar la vista de cámara en el punto clave.
 - 2.1. En **Live view actions (Acciones de visualización en directo)**, seleccione **Camera (Cámara)** y elija una vista de cámara.
 - 2.2. En **Show in (Mostrar en)**, seleccione **Hotspot in view (Punto clave en vista)**.
 - 2.3. Seleccione **Hotspot view (Vista de punto clave)**.

Crear acciones de notificación HTTP

La acción de notificación HTTP envía una solicitud de HTTP a un destinatario. El destinatario puede ser una cámara, un controlador de puerta, un servidor Web externo o cualquier servidor que pueda recibir solicitudes HTTP. Por ejemplo, las notificaciones HTTP se pueden utilizar para activar o desactivar una característica de la cámara, o bien, para abrir, cerrar, bloquear o desbloquear una puerta conectada a un controlador de puerta.

Los métodos GET, POST y PUT son compatibles.

Nota

Para enviar notificaciones HTTP a destinatarios fuera de la red local, puede ser necesario ajustar la configuración del servidor proxy de AXIS Camera Station Pro. Póngase en contacto con el soporte técnico de Axis para obtener más información.

Para crear una acción de notificación HTTP:

1. Vaya a **Configuración > Grabaciones y eventos > Reglas de acción**.
2. Haga clic en **New (Nueva)**.
3. Haga clic en **Agregar** y cree un activador. Haga clic en **Next (Siguiente)**. Vea *Agregar activadores*.
4. Haga clic en **Agregar** y, a continuación, seleccione **Enviar notificación HTTP**.
5. Haga clic en **OK**.
6. En **URL**, introduzca la dirección del destinatario y la secuencia de comandos que gestiona la solicitud. Por ejemplo: `https://192.168.254.10/cgi-bin/notify.cgi`.
7. Seleccione **Se requiere autenticación** si el destinatario requiere autenticación. Introduzca el nombre de usuario y la contraseña.
8. Seleccione un método de autenticación.
9. Haga clic en **Avanzada** para mostrar la configuración avanzada.
10. Haga clic en **OK**.

Método de autenticación	
Digest	Recomendamos utilizar esta opción, ya que proporciona la mejor protección contra escuchas ilegales.
Digest con Basic como reserva	Utilice esta opción si no está seguro del método de autenticación que utiliza el dispositivo.

Avanzada	
Método	Seleccione el método HTTP en el menú desplegable Method (Método) .
Tipo de contenido	Para solicitudes POST y PUT, seleccione el tipo de contenido en el menú desplegable Content type (Tipo de contenido) .
Cuerpo	Para solicitudes POST y PUT, introduzca el cuerpo de la solicitud en Body (Cuerpo) .
Trigger data (Activar datos)	También puede insertar datos de activación predefinidos desde el menú desplegable. Para obtener más información, consulte a continuación.

Trigger data (Activar datos)	
Tipo	El activador que activó esta regla de acción.
Source ID (ID de fuente)	El ID de fuente es el ID de la fuente que ha activado la regla de acción, que suele ser una cámara u otro tipo de dispositivo. No todas las fuentes tienen identificador de fuente.
Source Name (Nombre de fuente)	El nombre de fuente es el nombre de la fuente que ha activado la regla de acción, que suele ser una cámara

Trigger data (Activar datos)	
	u otro tipo de dispositivo. No todas las fuentes tienen nombre.
Hora (UTC)	Es la fecha y hora en la que se activó la regla de acción.
Hora (local)	La fecha y hora del servidor en la que se activó la regla de acción.

Crear acciones virtuales de E/S

Utilice acciones de E/S virtuales para activar un puerto de entrada virtual específico en un dispositivo. Puede utilizar cada puerto de un dispositivo para una acción.

1. Vaya a **Configuración > Grabaciones y eventos > Reglas de acción**.
2. Haga clic en **New (Nueva)**.
3. Haga clic en **Agregar** y cree un activador. Haga clic en **Next (Siguiendo)**. Vea *Agregar activadores*.
4. Haga clic en **Add (Agregar)** y seleccione **Virtual I/O (E/S virtual)**.
5. Haga clic en **OK**.
6. Seleccione el dispositivo y el puerto que desee activar.
7. Haga clic en **OK**.

Crear acciones de sirena y luz

La acción de sirena y luz activa un patrón de sirena y luz en AXIS D4100-E Network Strobe Siren según un perfil configurado.

Nota

Para utilizar esta acción, se debe configurar un perfil desde la página de configuración del dispositivo.

1. Vaya a **Configuración > Grabaciones y eventos > Reglas de acción**.
2. Haga clic en **New (Nueva)**.
3. Haga clic en **Agregar** y cree un activador. Haga clic en **Next (Siguiendo)**. Vea *Agregar activadores*.
4. Haga clic en **Add (Agregar)** y seleccione **Siren and light (Sirena y luz)**.
5. Haga clic en **OK**.
6. Seleccione un dispositivo en el menú desplegable **Device (Dispositivo)**.
7. Seleccione un perfil en el menú desplegable **Profile (Perfil)**.
8. Haga clic en **OK**.

Crear acciones AXIS Entry Manager

Una acción de AXIS Entry Manager puede conceder acceso y bloquear o desbloquear una puerta conectada a un controlador de puerta configurado por AXIS Entry Manager.

Nota

Una acción de AXIS Entry Manager solo se puede usar cuando AXIS A1001 Network Door Controller está disponible en AXIS Camera Station Pro.

1. Vaya a **Configuración > Grabaciones y eventos > Reglas de acción**.
2. Haga clic en **New (Nueva)**.
3. Haga clic en **Agregar** y cree un activador. Haga clic en **Next (Siguiendo)**. Vea *Agregar activadores*.
4. Haga clic en **Add (Agregar)** y seleccione **AXIS Entry Manager**.

5. Haga clic en **OK**.
6. Seleccione una acción y una puerta para realizar la acción.
7. Haga clic en **OK**.

Crear acciones de notificación de envío de aplicación móvil

La acción de notificación de aplicación móvil envía un mensaje personalizado a la aplicación móvil AXIS Camera Station. Puede hacer clic en la notificación recibida para ir a una vista de cámara específica. Consulte *el manual de usuario de la aplicación móvil AXIS Camera Station*.

Para crear una acción de envío de notificación de aplicación móvil:

1. Vaya a **Configuración > Grabaciones y eventos > Reglas de acción**.
2. Haga clic en **New (Nueva)**.
3. Haga clic en **Agregar** y cree un activador. Haga clic en **Next (Siguiete)**. Vea *Agregar activadores*.
4. Haga clic en **Add (Agregar)** y seleccione **Send mobile app notification (Enviar notificación de aplicación móvil)**.
5. Haga clic en **OK**.
6. En **Message (Mensaje)**, introduzca el mensaje que debe mostrarse en la aplicación móvil.
7. En **Click notification and go to (Hacer clic en la notificación e ir a)**, configure lo que debe mostrarse cuando haga clic en la notificación.
8. Haga clic en **Aceptar**.

Hacer clic en la notificación e ir a	
Cámara	Seleccione una vista de cámara en el menú desplegable Camera (Cámara) que debe mostrarse al hacer clic en la notificación en la aplicación móvil.
Configuración predeterminada	Seleccione Default (Predeterminado) para ir a la página de inicio de la aplicación móvil al hacer clic en la notificación en la aplicación móvil.

Crear una acción que activa o desactiva otras reglas de acción

Active o desactive las reglas, por ejemplo, si desea desactivar la detección de movimiento en una oficina cuando un empleado pase la tarjeta de acceso.

Para crear una acción de activación o desactivación de reglas:

1. Vaya a **Configuración > Grabaciones y eventos > Reglas de acción**.
2. Haga clic en **New (Nueva)**.
3. Haga clic en **Agregar** y cree un activador. Haga clic en **Next (Siguiete)**. Vea *Agregar activadores*.
4. Haga clic en **Add (Agregar)** y seleccione **Turn rules on or off (Activar o desactivar reglas)**.
5. Haga clic en **OK**.
6. Seleccione una o varias reglas de acción.
7. Elija si desea activar o desactivar las reglas de acción seleccionadas.
8. Introduzca un retraso si desea que transcurra tiempo entre el activador y el cambio de estado.
9. Seleccione **Return to the previous state when the trigger is no longer active (Volver al estado anterior cuando el activador ya no esté activo)** si no desea que la regla de acción seleccionada permanezca cambiada cuando el activador no esté activo. En el ejemplo anterior, la detección de movimiento vuelve a activarse cuando los empleados eliminan la tarjeta de acceso del lector.

10. Haga clic en **Aceptar**.

Crear una acción de marcador

Crear una acción de marcador:

1. Vaya a **Configuración > Grabaciones y eventos > Reglas de acción**.
2. Haga clic en **New (Nueva)**.
3. Haga clic en **Agregar** y cree un activador. Haga clic en **Next (Siguiente)**. Vea *Agregar activadores*.
4. Haga clic en **Add (Añadir)** y seleccione **Add bookmark (Añadir marcador)**.
5. Haga clic en **OK**.
6. Configure el marcador introduciendo un nombre y, de forma opcional, una descripción.
7. Haga clic en **OK**.

Crear una acción que envíe una vista a un decodificador de vídeo

Utilice esta acción si desea enviar una vista a un decodificador de vídeo para que se muestre en un monitor durante un periodo de tiempo determinado.

1. Vaya a **Configuración > Grabaciones y eventos > Reglas de acción**.
2. Haga clic en **New (Nueva)**.
3. Haga clic en **Agregar** y cree un activador. Haga clic en **Next (Siguiente)**. Vea *Agregar activadores*.
4. Haga clic en **Add (Agregar)** y seleccione **Send to video decoder (Enviar al decodificador de vídeo)**.
5. Haga clic en **OK**.
6. En **Decoder (Decodificador)**, seleccione el decodificador de vídeo al que desea enviar la vista.
7. En **View (Ver)**, seleccione la cámara o vista que desea enviar.
8. En **Duration (Duración)**, introduzca la cantidad de tiempo, en segundos, que desea que se muestre la vista.
9. Haga clic en **Aceptar**.

Crear acciones de control de acceso

La acción de control de acceso puede realizar las siguientes acciones en el sistema AXIS Camera Station Secure Entry:

- **Acciones de puertas:** conceder acceso, bloquear, desbloquear o bloquear las puertas seleccionadas.
- **Acciones de zonas:** bloquear, desbloquear o bloquear las puertas seleccionadas en las zonas indicadas.
- **Acciones de regla de acceso:** Active o desactive las reglas de acceso.

Nota

La acción de control de acceso solo está disponible para el sistema AXIS Camera Station Secure Entry.

Para crear una acción de control de acceso:

1. Vaya a **Configuración > Grabaciones y eventos > Reglas de acción**.
2. Haga clic en **New (Nueva)**.
3. Haga clic en **Agregar** y cree un activador. Haga clic en **Next (Siguiente)**. Vea *Agregar activadores*.
4. Seleccione **Add (Agregar)** y seleccione **Access control (Control de acceso)**.
5. Haga clic en **OK**.
6. Para realizar acciones de puerta:
 - 6.1. En **Access control (Control de acceso)**, seleccione **Door actions (Acciones de puerta)**.

- 6.2. En **Configure action (Configurar acción)**, seleccione las puertas y la acción.
- 7. Para realizar acciones de zona:
 - 7.1. en **Access control (Control de acceso)**, seleccione **Zone actions (Acciones de zona)**.
 - 7.2. En **Configure action (Configurar acción)**, seleccione las zonas, los tipos de puerta y la acción.
- 8. Para activar o desactivar las reglas de acceso:
 - 8.1. En **Access control (Control de acceso)**, seleccione **Action rule actions (Acciones de regla de acción)**.
 - 8.2. En **Configure action (Configurar acción)**, seleccione la regla de acceso que desee activar o desactivar.
 - 8.3. En **Action (Acción)** seleccione **Enable (Habilitar)** o **Disable (Deshabilitar)**.
- 9. Haga clic en **OK**.

Crear acciones de Audio Manager

Para crear una acción de Audio Manager

- 1. Vaya a **Configuración > Grabaciones y eventos > Reglas de acción**.
- 2. Haga clic en **New (Nueva)**.
- 3. Haga clic en **Agregar** y cree un activador. Haga clic en **Next (Siguiente)**. Vea *Agregar activadores*.
- 4. Haga clic en **Add (Añadir)** y seleccione **Audio Manager (Administrador de audio)**.
- 5. Haga clic en **OK**.
- 6. Seleccione y configure la acción que desea activar.
- 7. Haga clic en **OK**.

Acciones de Audio Manager	
Reproducir archivo de audio	Seleccione Play audio file (Reproducir archivo de audio) para reproducir un archivo seleccionado.
Detener archivo de audio	Seleccione Stop audio file (Detener archivo de audio) para interrumpir la reproducción de un archivo de audio iniciado anteriormente. El identificador de inicio debe coincidir con el empleado para la acción Reproducir archivo de audio .
Activar o desactivar destino	Seleccione Enable or disable target (Activar o desactivar destino) para activar o desactivar dispositivos
Silenciar volumen	Seleccione Mute volume (Silenciar volumen) para silenciar el controlador.
Establecer volumen	Seleccione Set volumen (Establecer volumen) para ajustar un nuevo volumen.
Volumen de compensación	Seleccione Offset volumen (Volumen de compensación) para aumentar o reducir el volumen respecto al nivel actual.

Horarios

La página **Schedules (Programaciones)** contiene todas las programaciones que puede aplicar a la grabación, reglas de acción y componentes como **AXIS Secure Entry**. **AXIS Site Designer** crea algunas programaciones durante la instalación.

Las programaciones permiten crear y editar horarios diarios y semanales personalizados, así como anular horarios preestablecidos. Las programaciones de anulación son siempre diarias, pero pueden aplicarse tanto a las programaciones diarias como a las semanales en fechas especiales, como días festivos.

La pestaña **Schedules (Programaciones)** es la vista principal para administrar todas sus programaciones diarias y semanales:

- **Name (Nombre):** El nombre del programa.
- **Tipo:** Indica si el programa es diario o semanal.
- **En uso:** Muestra si un componente, una regla de grabación o una regla de acción está utilizando la programación.
- **Override schedules (Programaciones de anulación):** Lista las programaciones de anulación aplicables a esta programación.

La pestaña **Override schedules (Programaciones de anulación)** es la vista principal para su gestión, donde puede consultar a qué programaciones diarias y semanales se han aplicado.

Nota

Si está conectado a varios servidores de AXIS Camera Station Pro, puede agregar y gestionar programaciones en cualquier servidor conectado. Seleccione el servidor en el menú desplegable **Selected server (Servidor seleccionado)** para gestionar las programaciones.

Gestión de programaciones diarias y semanales

Gestione las programaciones diarias y semanales en la pestaña **Schedules (Programaciones)**.

Para crear una nueva programación diaria o semanal, haga clic en **Nueva programación**.

Para eliminar una programación, selecciónela de la lista y haga clic en **Delete (Eliminar)**. Asegúrese de que la programación no está en uso antes de intentar borrarla.

Cree o seleccione una programación diaria o semanal para supervisar sus detalles.

- Si se trata de una programación diaria, haga clic en **Add dates (Añadir fechas)** para añadir un nuevo rango de fechas a la programación. Puede añadir varios rangos de fechas a la misma programación diaria.
- Para añadir una franja horaria, haga clic en **+** o doble clic en la fila.
- Para editar un rango de fechas o una franja horaria, haga clic con el botón izquierdo del ratón.
- Para añadir una programación de anulación, selecciónela en el menú desplegable y haga clic en **Add (Añadir)**. Para eliminar una programación de anulación, selecciónela de la lista y haga clic en **Remove (Eliminar)**.
- Haga clic en **Apply (Aplicar)** para guardar los cambios.

Gestión de programaciones de anulación

- Gestione las programaciones de anulación en la pestaña **Override schedules (Programaciones de anulación)**.
- Haga clic en **Add dates (Añadir fechas)** para añadir un nuevo rango de fechas a la programación. Puede añadir varios rangos de fechas a la misma programación de anulación.
- Para añadir una franja horaria, haga clic en **+** o doble clic en la fila.
- Para editar un rango de fechas o una franja horaria, haga clic con el botón izquierdo del ratón.
- Haga clic en **Apply (Aplicar)** para guardar los cambios.

Ejemplos de reglas de acción

Ejemplo: Apertura forzada de puerta

Apertura forzada de puerta

Un ejemplo de cómo configurar una regla de acción en AXIS Camera Station Pro para activar una grabación y una alarma cuando alguien fuerza la apertura de la puerta de entrada.

Antes de empezar, necesita:

- Instale una controladora de accesos en red de Axis. Vea *Agregar dispositivos*, on page 46.
- Configure el controlador de puerta. Consulte *Agregar una puerta*, on page 149.

Crear una regla de acción:

1. Vaya a **Configuración > Grabaciones y eventos > Reglas de acción**.
2. Haga clic en **New (Nueva)**.
3. Agregue el activador **Door forced event (Evento de puerta forzada)**.
 - 3.1. Haga clic en **Agregar** y, a continuación, seleccione **Evento de dispositivo**.
 - 3.2. Haga clic en **OK**.
 - 3.3. En **Configure device event trigger (Configurar activador de evento de dispositivo)**, configure los ajustes del activador.
 - 3.4. En **Filters (Filtros)**, configure los ajustes del filtro.
 - 3.5. En **Activity (Actividad)**, compruebe que el activador muestra actividad en la línea de señal.
 - 3.6. Haga clic en **OK**.
4. Haga clic en **Next (Siguiete)**.
5. Agregue una acción de grabación.
 - 5.1. Haga clic en **Agregar** y seleccione **Grabar**.
 - 5.2. Haga clic en **OK**.
 - 5.3. Seleccione una cámara en el menú desplegable **Camera (Cámara)**.
 - 5.4. En **Video setting (Ajustes de vídeo)**, configure el perfil, búfer anterior y búfer posterior.
 - 5.5. Haga clic en **OK**.
6. Agregue una acción para generar una alarma.
 - 6.1. Haga clic en **Agregar** y, a continuación, seleccione **Generar alarma**.
 - 6.2. Haga clic en **OK**.
 - 6.3. En **Alarm message (Mensaje de alarma)**, introduzca el título y la descripción de la alarma. Por ejemplo, *Se ha forzado la apertura de la puerta principal*.
 - 6.4. Haga clic en **OK**.
7. Haga clic en **Next (Siguiete)** y seleccione **Always (Siempre)** como programación.
8. Haga clic en **Finish (Finalizar)**.

Configurar desencadenador de eventos de dispositivo	
Dispositivo	Seleccione la controladora de accesos en red de Axis en el menú desplegable Device (Dispositivo) .
Evento	Seleccione Door > Door forced (Puerta > Puerta forzada) en el menú desplegable Event (Evento) .
Trigger period (Período de activación)	Defina 10 segundos como Trigger period (Período de activación) .

Filtros	
Nombre de puerta	Seleccione la puerta en el menú desplegable Door name (Nombre de puerta).
Estado de puerta	Seleccione Forced (Forzada) en el menú desplegable Door status (Estado de puerta).

Configuración de vídeo	
Perfil	Seleccione High (Alto) en el menú desplegable Profile (Perfil).
Búfer anterior	Defina 3 segundos como Prebuffer (Búfer anterior).
Búfer posterior	Defina 5 segundos como Postbuffer (Búfer posterior).

Ejemplo: Cuando entra una persona importante

Cuando entra una persona importante

Un ejemplo de cómo crear una regla de acción en AXIS Camera Station Pro que reproduce un mensaje de bienvenida y llama al ascensor cuando entra una persona importante.

Antes de empezar, tiene que:

- Instalar y configurar una controladora de accesos en red de Axis y añadir titulares de tarjetas. Vea *Configure el control de acceso, on page 146* y *Gestión de acceso, on page 183*.
- Instale un dispositivo de audio en red de Axis y asocie el dispositivo de audio con una cámara. Vea *Perfiles de transmisión, on page 54*.
- Instale AXIS A9188 Network I/O Relay Module, conecte la E/S al ascensor y agregue los puertos de E/S del módulo de relé de E/S de red a AXIS Camera Station Pro. Vea *Puertos de E/S, on page 90*.

Crear una regla de acción:

1. Vaya a **Configuración > Grabaciones y eventos > Reglas de acción**.
2. Haga clic en **New (Nueva)**.
3. Agregue el activador de eventos del dispositivo.
 - 3.1. Haga clic en **Agregar** y, a continuación, seleccione **Evento de dispositivo**.
 - 3.2. Haga clic en **OK**.
 - 3.3. En **Configure device event trigger (Configurar activador de evento de dispositivo)**, configure los ajustes del evento.
 - 3.4. En **Filters (Filtros)**, configure los ajustes del filtro.
 - 3.5. En **Activity (Actividad)**, compruebe que el activador muestra actividad en la línea de señal.
 - 3.6. Haga clic en **OK**.
4. Haga clic en **Next (Siguiete)**.
5. Agregue una acción de envío de notificación HTTP para reproducir un mensaje de bienvenida.
 - 5.1. Haga clic en **Add (Agregar)** y, a continuación, seleccione **Send HTTP notification (Enviar notificación HTTP)**.
 - 5.2. Haga clic en **OK**.
 - 5.3. En **URL**, introduzca la URL del clip de audio del mensaje de bienvenida.
 - 5.4. Seleccione **Authentication required (Se requiere autenticación)** e introduzca el nombre de usuario y la contraseña del dispositivo de audio.
 - 5.5. Haga clic en **OK**.

6. Agregar una acción Set output (Establecer salida)
 - 6.1. Haga clic en **Agregar** y, a continuación, seleccione **Establecer salida**.
 - 6.2. Haga clic en **OK**.
 - 6.3. En el menú desplegable **Output port (Puerto de salida)**, seleccione el puerto de salida del módulo de E/S que está conectado al ascensor.
 - 6.4. En el menú desplegable **State on action (Estado en acción)**, seleccione el estado del módulo de E/S para llamar al ascensor.
 - 6.5. Seleccione **Pulse (Pulsar)** y establezca 60 segundos para mantener el puerto en el estado.
 - 6.6. Haga clic en **OK**.
7. Haga clic en **Next (Siguiete)** y seleccione **Always (Siempre)** como programación.
8. Haga clic en **Finish (Finalizar)**.

Configurar desencadenador de eventos de dispositivo	
Dispositivo	Seleccione la controladora de accesos en red de Axis en el menú desplegable Device (Dispositivo) .
Evento	Seleccione Authorization > Access request granted (Autorización > Solicitud de acceso concedida) en el menú desplegable Event (Evento) .
Trigger period (Período de activación)	Defina 10 segundos como Trigger period (Período de activación) .

Filtros	
Nombre de puerta	Seleccione la puerta en el menú desplegable Door name (Nombre de puerta) .
Door side (Cara de puerta)	Seleccione el lado de la puerta en el menú desplegable Door side (Lado de puerta) .
Número de tarjeta	Seleccione Card number (Número de tarjeta) e introduzca el número de tarjeta de la persona importante.

Configurar cliente

Vaya a **Configuración > Cliente** para:



- Editar los ajustes específicos del cliente, como el tema y el idioma. Vea *Ajustes del cliente, on page 117*.
- Editar ajustes los específicos del usuario, como notificaciones y opciones de inicio. Vea *Configuración de usuarios, on page 118*.
- Puede editar ajustes específicos del rendimiento de la transmisión, como el escalado de vídeo y la decodificación de hardware. Vea *Transmisión, on page 120*.

Ajustes del cliente

Estos ajustes se aplican a todos los usuarios de AXIS Camera Station Pro del equipo. Vaya a **Configuration > Client > Settings (Configuración > Cliente > Ajustes)** para configurar los ajustes del cliente de AXIS Camera Station Pro.

Tema	
System, Light, Dark (Sistema, Claro, Oscuro)	<p>Seleccione el tema para el cliente. System (Sistema) es el tema predeterminado de las nuevas instalaciones.</p> <p>Si selecciona System (Sistema), este empleará el tema claro u oscuro según el tema del sistema Windows.</p>

General	
Ejecutar la aplicación cuando se inicie Windows	Active esta opción para que AXIS Camera Station Pro se ejecute automáticamente cada vez que se inicie Windows.

Vista en vivo	
Mostrar nombres de cámaras en visualización en directo	Se muestra el nombre de la cámara en la visualización en directo.
	Para indicar cualquier tipo de grabación, active Show recording indicators in live views and maps (Mostrar indicadores de grabación en visualizaciones en directo y mapas) .
	Para indicar grabaciones de detección de movimiento o grabaciones iniciadas por una regla de acción, active Show event indicators in live views and maps (Mostrar indicadores de eventos en visualizaciones en directo y mapas) .

Mapas	
Allow flashing coverage areas for all maps (Permitir áreas de cobertura intermitentes para todos los mapas)	Se utiliza para impedir o permitir el parpadeo de todas las áreas de cobertura mediante Flash. Este ajuste global no afecta a la configuración local en el nivel de mapa. Vea <i>Mapa</i> , on page 22.

Idioma	
Cambie el idioma del cliente de AXIS Camera Station Pro. El cambio se hace efectivo tras reiniciar el cliente.	

Feedback	
Los datos anónimos de uso del cliente se pueden compartir con Axis Communications para contribuir a mejorar la aplicación y la experiencia de usuario.	Compartir datos anónimos con Axis para mejorar la experiencia del usuario. Para cambiar esta opción del servidor, consulte <i>Configuración de puertos del servidor</i> , on page 126.

Configuración de usuarios

Estos ajustes se aplican al usuario de AXIS Camera Station Pro. Vaya a **Configuration > Client > User settings (Configuración > Cliente > Ajustes de usuarios)** para configurar los ajustes del usuario cliente de AXIS Camera Station Pro.

Sistema de navegación	
Navegación con vista en árbol para sistemas	Se activa de forma predeterminada para habilitar el panel de navegación con vista en árbol en las vistas y las cámaras.
Show in navigation (Mostrar en navegación)	Seleccione esta opción para mostrar vistas o cámaras, o las dos cosas, en el menú desplegable.
Mostrar la ruta de navegación al desplazarse por una vista	Active esta función para que la ruta de navegación se muestre en la parte superior de la vista en las vistas divididas.

Notificaciones	
Mostrar notificación en la barra de tareas para alarmas	Active esta opción para que se muestre una notificación en la barra de tareas de Windows cuando se inicie una alarma.
Mostrar notificación en la barra de tareas para tareas	Active esta función para que se muestre una notificación en la barra de tareas de Windows cuando un usuario agrega o finaliza una tarea.
Mostrar notificaciones en Gestión de dispositivos	Active esta función para que se muestren notificaciones cuando haya nuevo firmware disponible para su descarga.
Mostrar la ventana de notificación del intercomunicador	Active esta opción para que se muestre una ventana de notificación cuando un usuario pulse el botón de llamada en un sistema de intercomunicación conectado.

Instantánea	
Mostrar un mensaje cuando se tome una instantánea	Active esta función para que se muestre un mensaje cuando un usuario tome una instantánea.
Cuando se tome una instantánea, abra la carpeta de instantáneas	Active esta función para que se abra la carpeta de instantáneas cuando un usuario tome una instantánea.
Examinar	Haga clic en Browse (Examinar) para seleccionar la carpeta en la que guardar instantáneas.

Arranque	
Iniciar en pantalla completa	Active esta función para que AXIS Camera Station Pro se inicie en modo de pantalla completa.
Recordar últimas pestañas utilizadas	Active esta opción para que AXIS Camera Station Pro se inicie con las pestañas, vistas y vistas de cámara que estaban abiertas la última vez que AXIS Camera Station Pro se cerró.
Recordar últimos monitores utilizados	Active esta función para iniciar AXIS Camera Station Pro en el mismo monitor utilizado cuando AXIS Camera Station Pro se cerró la última vez.

Nota

- El sistema guarda las vistas y las vistas de cámara por pestaña. El sistema recuerda solo cuando el cliente se vuelve a conectar al mismo servidor.
- Se pueden recordar pestañas para recordar monitores, vistas y vistas de la cámara.
- El sistema no recuerda nunca las vistas dinámicas que arrastre y suelte en la visualización en directo.
- Si está conectado a varios servidores con distintos usuarios, el sistema no admite la opción **Remember last used tabs (Recordar últimas pestañas usadas)**.

Sonido en alarma	
Sin sonido	Seleccione esta opción si no quiere reproducir sonidos con una alarma.
Bip	Seleccione esta opción si quiere reproducir un sonido de alerta determinado con la alarma.
Sound file (Archivo de sonido)	Seleccione esta opción y haga clic en Browse (Explorar) para buscar un archivo de sonido si quiere un sonido personalizado para una alarma. Puede usar cualquier formato de archivo compatible con Windows Media Player.
Reproducir	Haga clic para probar el sonido.

Sonido de llamada entrante	
Sin sonido	Seleccione esta opción si no quiere reproducir sonidos con una llamada entrante.
Bip	Seleccione esta opción si quiere reproducir sonido determinado con una llamada entrante.
Sound file (Archivo de sonido)	Seleccione esta opción y haga clic en Browse (Explorar) para buscar un archivo de sonido si quiere un sonido personalizado para una llamada entrante. Puede usar cualquier formato de archivo compatible con Windows Media Player.
Reproducir	Haga clic para probar el sonido.

Prestaciones	
Mostrar búsqueda inteligente 1	De forma predeterminada, se muestra la búsqueda inteligente 1. Desactive esta opción para ocultarla.

Mostrar cuadros de diálogo de advertencia	
Advertencia de certificado no válido	Active esta opción para mostrar esta advertencia cuando corresponda.

Transmisión

Vaya a **Configuration > Client > Streaming (Configuración > Cliente > perfiles de flujo)** para configurar las opciones de transmisión del cliente de AXIS Camera Station Pro.

Ajuste de tamaño de vídeo	
Cambiar a ajuste perfecto	Seleccione esta opción para que el vídeo se muestre en todo el espacio disponible y que no se pierda la relación de aspecto ni se recorte la imagen.
Rellenar el área de vídeo (puede recortar partes del vídeo)	Seleccione esta opción para que el vídeo se ajuste al espacio disponible y conserve la relación de aspecto. Si el espacio disponible presenta una relación de aspecto diferente a la del vídeo, el sistema recorta el vídeo.

Descodificación de hardware	
Modo	<ul style="list-style-type: none"> • Automatic (Automático) Se usa la tarjeta gráfica, si la hay, para descodificar las transmisiones con una resolución superior a 3840 x 2160 p a 25 fps (lo que se conoce como 4K o UHD). • On (Activo) Se usa la tarjeta gráfica, si la hay, para descodificar las transmisiones con una resolución superior a 1920 x 1080 p a 25 fps (lo que se conoce como 1080p o HD). • Off (Desactivado) La descodificación por hardware está desactivada y AXIS Camera Station Pro utiliza la CPU para descodificar el vídeo.
Tarjeta gráfica	Seleccione una tarjeta gráfica en el menú desplegable.

Nota

- La descodificación de hardware utiliza la tarjeta gráfica para descodificar el vídeo. Si dispone de una tarjeta gráfica de alto rendimiento, la descodificación de hardware permite mejorar el rendimiento y reducir la utilización de la CPU, sobre todo durante al transmitir vídeo en alta resolución. La descodificación de hardware admite M-JPEG y H.264.
- Las cámaras con una resolución inferior a 1080p no pueden usar la descodificación de hardware, aunque la función esté **On (Activada)**.
- Si la tarjeta gráfica no admite la descodificación de 4K, la descodificación de hardware solo funciona en transmisiones de 1080p, aunque la función esté **On (Activada)**.

Uso de ancho de banda	
Utilizar siempre el perfil de flujo Bajo en este cliente	<p>Active esta opción para usar el perfil de flujo bajo para la visualización en directo. Vea <i>Perfiles de transmisión</i>.</p> <p>Este ajuste afecta al vídeo H.264 y M-JPEG y reduce el consumo de ancho de banda.</p>
Suspender transmisiones de vídeo de pestañas inactivas	Active esta función para que se suspendan las transmisiones de vídeo en las pestañas inactivas. Así se reduce el consumo de ancho de banda.

PTZ (Pan, Tilt, Zoom)	
Seleccionar vista con primer clic en vez de iniciando PTZ	Active esta función para activar la selección de vista cuando se hace clic por primera vez en la vista. Los demás clics que haga en la vista controlarán el PTZ.

Audio	
Push-to-talk release delay (ms) [Retardo de liberación de pulsar para hablar (ms)]	Determine el número de milisegundos que quiere que el audio se transmita desde el micrófono después de soltar el botón Push-to-talk (Pulsar para hablar).
Utilizar la función de pulsar para hablar para todos los modos de dúplex	Active esta opción para usar el modo de pulsar para hablar en los modos simplex, half-duplex y full-duplex.
Permitir siempre el audio para los intercomunicadores	Active esta opción para poder escuchar y hablar con los intercomunicadores, aunque no haya llamadas en curso desde ellos.

Reproducción instantánea	
Playback duration (s) [Duración de reproducción (s)]	Defina el tiempo de duración de la reproducción entre 1 y 600 segundos para volver a la línea temporal y reproducir la grabación.

Configurar servicios conectados

Gestionar servicios conectados

Los servicios conectados le ofrecen acceso a lo siguiente:

- Cliente web de AXIS Camera Station
- Gestión de dispositivos
- Gestión automática de licencias
- Supervisión del estado del sistema

Debe registrar el sistema y conectarlo a una organización para acceder a los servicios conectados. Consulte *Registre el sistema en una organización, on page 123* para obtener más información.

Estado	La tarjeta de estado muestra el estado de la conexión entre el servidor y los servicios conectados y el nombre de la organización que ha registrado o a la que está conectado.
Desconectar	Si desconecta un servidor conectado, todavía se registrará en la organización.

Gestión de licencias	Active la License management (Gestión de licencias) para sincronizar automáticamente las licencias. Esto significa que el sistema inserta los cambios que afectan al número de licencias en AXIS License Manager y recupera un nuevo estado de licencia. Desactive la License management (Gestión de licencias) para gestionar las licencias manualmente, por ejemplo, si el sistema no tiene conexión a Internet. Consulte <i>Gestionar licencias, on page 135</i> para obtener más información.
Sincronizar sistema	Active Synchronize system (Sincronizar sistema) para sincronizar automáticamente los dispositivos y vistas con el cliente web para AXIS Camera Station y AXIS Device Manager.

Registre el sistema en una organización

Para registrar el sistema:

1. Vaya a **Configuration (Configuración) > Connected services (Servicios conectados) > Management (Gestión)**.
2. Haga clic en **Register (Registrar)** y siga las instrucciones de la pantalla.

Para obtener más ayuda sobre los aspectos que se deben tener en cuenta al registrar su sistema, consulte la *guía de instalación y migración de AXIS Camera Station Pro*.

Ajustes de actualización del firmware

Nota

Al conectarse a varios servidores de AXIS Camera Station Pro, puede seleccionar cualquier servidor en el menú desplegable **Selected server (Servidor seleccionado)** para configurar los ajustes de actualización del firmware.

1. Vaya a **Configuración > Servicios conectados > Ajustes de actualización del firmware**.
2. En **Automatic check for updates (Comprobar actualizaciones automáticamente)**, configure la frecuencia y la forma de comprobar las actualizaciones de firmware.
3. En **Upgrade order (Orden de actualización)**, configure el orden para actualizar los dispositivos.

Comprobar actualizaciones automáticamente	
Check for updates (Comprobar actualizaciones)	Seleccione Every start-up (Cada puesta en marcha) en el menú desplegable para comprobar si hay versiones del firmware disponibles en el servidor en cada inicio. Por defecto, AXIS Camera Station Pro está fijado en Never (Nunca) .
Check now (Comprobar ahora)	Haga clic en esta opción para comprobar si hay versiones del firmware disponibles en el servidor.

Orden de actualización	
Paralela	Seleccione esta opción para actualizar todos los dispositivos al mismo tiempo. Esta opción es más rápida que Sequential (Secuencial) , pero todos los dispositivos quedan sin conexión a la vez.
Secuencial	Seleccione esta opción para actualizar los dispositivos de uno en uno. Esta opción tarda más, pero los dispositivos no quedan sin conexión al mismo tiempo. Seleccione Cancel remaining upgrades if one device fails (Cancelar las actualizaciones restantes si un dispositivo tiene un error) para detener la actualización secuencial.



Activar la comprobación automática del firmware

Axis Secure Remote Access v2

Axis Secure Remote Access v2 le permite conectarse a su servidor de AXIS Camera Station Pro a través de una conexión a Internet segura y cifrada.

Nota

Axis Secure Remote Access v2 está disponible para AXIS Camera Station Pro 6.8 o posterior.

Para habilitar Axis Secure Remote Access v2:

1. Registre el servidor en una organización. Vea *Registre el sistema en una organización, on page 123*.
2. Iniciar sesión para usar Axis Secure Remote Access v2. Consulte *Iniciar sesión en AXIS Secure Remote Access*.

Para limitar el acceso únicamente a los servidores AXIS Camera Station Pro:

1. Vaya a **Organization (Organización) > Users (Usuarios)** en My Systems.
2. Elija el usuario que desea configurar.
3. Haga clic en **Roles and access (Funciones y acceso)**.
4. Asigne la función "ACS Pro Secure Remote Access". Esta función solo permite acceder a los servidores AXIS Camera Station Pro sin permitirlo a otras funciones de Axis My Systems.

Una vez registrado, podrá gestionar aún más los permisos de acceso asignando funciones de usuario a la organización a través de Axis My Systems. Para obtener más información sobre los AXIS Camera Station Pro derechos de acceso de usuarios, consulte *Permisos de usuario, on page 137*.

Axis Secure Remote Access

Importante

Para mejorar la seguridad y la funcionalidad, estamos actualizando **Axis Secure Remote Access (v1)** a **Axis Secure Remote Access v2**. Suspendemos la versión actual el 1 de diciembre de 2025, por lo que le recomendamos firmemente actualizar a Axis Secure Remote Access v2 antes de esa fecha.

¿Qué supone esto para su sistema AXIS Camera Station Pro?

- Después del 1 de diciembre de 2025, ya no podrá acceder de forma remota a su sistema utilizando Axis Secure Remote Access (v1).
- Para utilizar Axis Secure Remote Access v2, debe actualizar a la versión 6.8 de AXIS Camera Station Pro. Esta actualización es actualmente gratuita para todos los usuarios de AXIS Camera Station 5 hasta el 1 de marzo de 2026.

Axis Secure Remote Access le permite conectarse a su servidor de AXIS Camera Station Pro a través de una conexión a Internet segura y cifrada. Axis Secure Remote Access no utiliza la redirección de puertos del router para acceder a la cámara.

Nota

- Axis Secure Remote Access solo está disponible para AXIS Camera Station 5.12 o superior.
- Cuando esté conectado a varios servidores de AXIS Camera Station Pro, seleccione uno en el menú desplegable **Selected server (Servidor seleccionado)** para configurar el acceso remoto seguro de Axis.

Habilitar Axis Secure Remote Access

Solo es posible acceder a Axis Secure Remote Access si se ha iniciado sesión en la cuenta MyAxis. Axis Secure Remote Access debe activarse manualmente. Esta función permite iniciar sesión en el servidor de forma remota. Consulte *Conectar a un servidor*.

1. Vaya a **Configuración > Servicios conectados > Axis Secure Remote Access**.
2. En la cuenta MyAxis, introduzca las credenciales correspondientes.
3. Haga clic en **Aplicar**.
4. En la sección Axis Secure Remote Access, haga clic en **Enable (Habilitar)** para activar el acceso remoto.

Axis Secure Remote Access en dispositivos móviles

Para iniciar sesión en el servidor con acceso remoto seguro en un dispositivo móvil (iOS y Android):

1. Con el dispositivo móvil, vaya a axis.com/products/axis-camera-station/overview y descargue la aplicación móvil de AXIS Camera Station.
2. Instale y abra la aplicación móvil.
3. Inicie sesión en Axis Secure Remote Access con la misma cuenta de My Axis utilizada para activar el acceso remoto.
4. Seleccione el servidor en el que desea iniciar sesión.
5. Inicie sesión con las credenciales del servidor.

Nota

Las credenciales del servidor son distintas de las credenciales de la cuenta de My Axis.

La aplicación móvil muestra la cantidad total de datos retransmitidos que utiliza la cuenta de My Axis durante el mes. Para obtener más información, lea el *manual del usuario de la aplicación móvil de AXIS Camera Station*.

Uso de Axis Secure Remote Access

El uso de Axis Secure Remote Access aparece en la barra de estado en la parte inferior del cliente de AXIS Camera Station Pro. Haga clic en el enlace para consultar información general de cómo usar la conexión remota segura.

Nivel de servicio	muestra el nivel de servicio de su suscripción a Axis Secure Remote Access.
Datos utilizados este mes	Muestra cuántos datos se han utilizado este mes. El contador se restablece el primer día de cada mes a medianoche.

Excedente	Muestra cuántos datos se han utilizado este mes por encima de la cantidad que incluye el nivel de servicio. Solo está disponible si hay excedente disponible en la suscripción.
Conexiones	Esta opción muestra los servidores conectados a través de Secure Remote Access.

Almacenamiento en la nube

AXIS Camera Station Cloud Storage es un servicio con licencia que permite almacenar grabaciones en la nube. Para obtener más información, consulte *AXIS Camera Station Cloud Storage – User manual*.

Antes de poder usar el servicio de almacenamiento en la nube, deberá registrar su sistema en los servicios conectados. Una vez registrado el sistema, podrá administrar el almacenamiento en la nube de sus cámaras en My Systems (Mis sistemas).

Configurar servidor

Configuración de puertos del servidor

Vaya a **Configuration > Server > Settings (Configuración > Servidor > Ajustes)** para configurar los ajustes generales del servidor de AXIS Camera Station Pro.

Nota

Cuando esté conectado a varios servidores de AXIS Camera Station Pro, seleccione uno en el menú desplegable **Selected server (Servidor seleccionado)** para configurar los ajustes del servidor.

Almacenamiento	
Al iniciarse el servidor, transfiera la propiedad de las carpetas de grabación a los administradores y restrinja el acceso a las carpetas de grabación a los administradores.	Cuando instala AXIS Camera Station Pro por primera vez, esta opción aparece seleccionada. Cuando actualice AXIS Camera Station Pro a una versión más reciente, la opción estará desactivada.

Exportar	
Incluir audio al agregar grabaciones para exportar	Seleccione esta opción para incluir audio al agregar la grabación a la lista de exportaciones.

Registros	
Especifique el número de días que se deben guardar alarmas, eventos y auditorías. Establezca un valor entre 7 y 1 000 días.	

Datos externos	
Especifique el número de días que se deben conservar los datos externos. Establezca un valor entre 1 y 1000 días.	

Servidores SMTP

Agregue servidores SMTP para enviar mensajes de correo electrónico cuando se produzcan alarmas del sistema o se active una regla de configuración de eventos.

Para agregar un servidor SMTP:

1. En **SMTP servers (Servidores SMTP)**, haga clic en **Add (Agregar)**.

2. En **Server (Servidor)**, configure la dirección del servidor, el puerto, la autenticación y el protocolo TLS.
3. En la sección **Sender (Remitente)**, introduzca la dirección de correo electrónico y el nombre que desea mostrar en el correo electrónico de remitente.

Servidor	
Dirección	Introduzca la dirección del servidor SMTP.
Puerto	Introduzca el puerto. 587 es el puerto predeterminado para las conexiones TLS SMTP.
Usar TLS	Seleccione esta opción si el servidor SMTP utiliza TLS. TLS es el protocolo predeterminado.
Usar autenticación	Seleccione esta opción si se requiere un nombre de usuario y una contraseña para este servidor. Introduzca el nombre de usuario y la contraseña para acceder al servidor.

Editar	Para editar un servidor SMTP, seleccione el servidor y haga clic en Editar .
Eliminar	Para eliminar un servidor SMTP, seleccione el servidor y haga clic en Quitar . En el diálogo emergente, haga clic en Sí para eliminar el servidor.
Test all... (Comprobar todo...)	Para comprobar un servidor SMTP, seleccione el servidor y haga clic en Test all... (Comprobar todo...) . En el cuadro de diálogo emergente, introduzca una dirección de correo electrónico en Recipient (Destinatario) y haga clic en OK (Aceptar) para enviar un correo electrónico de prueba. Las pruebas de servidor SMTP mostrarán una lista de resultados y acciones posibles para llevar a cabo.
Flechas	Seleccione un servidor y use las flechas para cambiar el orden de los servidores en la lista. El sistema usa los servidores en el orden en el que se muestran.

Resultados de la prueba de servidor	
OK	se ha establecido una conexión correcta con el servidor SMTP. Compruebe que los destinatarios recibieron el correo electrónico de prueba.
Error desconocido	se ha producido un error inesperado al intentar enviar el correo electrónico. Compruebe que el servidor SMTP funciona correctamente.
No hay contacto	AXIS Camera Station Pro no se puede acceder al servidor SMTP. Compruebe que el servidor SMTP funciona correctamente y que todos los routers y servidores proxy entre AXIS Camera Station Pro y el servidor SMTP admiten tráfico.
Error de configuración	Se solicitó TLS pero el servidor no es compatible con StartTLS, el servidor no admite autenticación o no hay un mecanismo de autenticación compatible.
Error de protocolo de enlace TLS/SSL	Error durante las negociaciones TLS/SSL, como un certificado de servidor no válido.

Resultados de la prueba de servidor	
Se requiere autenticación	El servidor requiere autenticación para enviar el correo electrónico.
Error de autenticación	Las credenciales son incorrectas.
Pérdida de conexión	Se estableció la conexión, pero después se perdió.

Alarma del sistema

Se produce una alarma del sistema si una cámara pierde la conexión, se niega el acceso al almacenamiento de grabación, se produce una desconexión imprevista del servidor o se produce un error de grabación. Se pueden enviar notificaciones por correo electrónico cuando se produce una alarma del sistema.

Nota

Para enviar correos electrónicos, primero hay que agregar un servidor SMTP.

Para enviar correos electrónicos por alarmas del sistema:

1. Seleccione **Enviar correo electrónico sobre alarma del sistema a los siguientes destinatarios** para activar los correos electrónicos por alarma en el sistema.
2. En **Recipients (Destinatarios)**:
 - 2.1. Seleccione si la dirección debe estar en los campos **To (Para)**, **Cc (CC)** o **Bcc (CCO)** del correo electrónico.
 - 2.2. Introduzca la dirección de correo electrónico.
 - 2.3. Haga clic en **Agregar** para agregar la dirección de correo electrónico en la casilla **Destinatarios**.

Conexión de dispositivo	
Seguir utilizando los nombres de host aunque dejen de estar disponibles	Use el nombre de host para conectarse. Para cambiar automáticamente al uso de la dirección IP para conectarse, desmarque la casilla de verificación. Puede seleccionar manualmente si desea utilizar el nombre de host o la dirección IP para conectarse a los dispositivos. Vea <i>Conexión</i> , on page 72.

Idioma	
Cambiar el idioma del servidor	Cambia el nombre del control del servicio de AXIS Camera Station Pro y de AXIS Camera Station Secure Entry. Por ejemplo: alarmas del sistema, mensajes del registro de auditoría y datos externos en la pestaña Data search (Búsqueda de datos) . El cambio se hace efectivo después de reiniciar.

Soluciones corporales	
Disco Carpeta	Seleccione la unidad y la carpeta donde desea recibir el contenido rechazado del sistema corporal. Consulte <i>Transferir grabaciones al almacenamiento de contenido rechazado en el manual de usuario de la solución corporal de Axis</i> para obtener más información.
Número de días para mantener el contenido rechazado del sistema corporal.	Este es el tiempo de retención del contenido rechazado.

Feedback	
Compartir datos de uso de servidor anónimos con Axis Communications	Seleccione esto para ayudarnos a mejorar la aplicación y la experiencia del usuario. Para cambiar las opciones del cliente, consulte <i>Ajustes del cliente, on page 117</i> .

Configuración avanzada

Solo debe cambiar la configuración cuando lo indique el servicio de asistencia técnica de Axis. Para cambiar un ajuste avanzado:

1. Introduzca el ajuste y su valor.
2. Haga clic en **Añadir**.

Para activar el registro de depuración para solucionar problemas, seleccione **Enable server side debug logging (Habilitar registro de depuración en el servidor)**. Este ajuste utiliza más espacio de disco y el archivo `log4net.config` del directorio `ProgramData` lo sobrescribe.

Consulte *Ajuste avanzado del servidor en la guía de solución de problemas de AXIS Camera Station Pro* para obtener más información.

Componentes

Los componentes son módulos de software que agregan más capacidades al sistema. La página de componentes le permite gestionar componentes y ver su estado.

Para ver la lista de componentes instalados:

1. Vaya a **Configuration > Server > Components (Configuración > Servidor > Componentes)**.
2. Active **Show components (Mostrar componentes)**.

Nota

Consideramos componentes con ajustes avanzados. Mostrar y gestionar componentes solo después de haber estado en contacto con el servicio de asistencia técnica de Axis.

Actualizar AXIS Camera Station Pro

Para obtener la versión más reciente de AXIS Camera Station Pro:

1. Vaya a **Configuration > Server > Update (Configuración > Servidor > Actualizar)**.
2. Haga clic en **Download and install... (Descargar e instalar...)**.

Nota

- Una vez que se inicia una actualización, ya sea manual o programada, no hay forma de cancelarla.
- Las actualizaciones programadas se inician automáticamente.
- En un sistema de múltiples servidores, actualice siempre el servidor local en último lugar.
- Cuando actualice el servidor local, se cerrarán temporalmente el cliente y el control de servicio. Durante la actualización, no observará la interfaz de usuario ni el indicador de progreso. Mantenga encendido el equipo servidor hasta que tanto el cliente como el servidor se hayan reiniciado.

Informe de incidentes

Si activa el permiso de informes de incidencias, puede generar los informes de incidencias, incluidas las grabaciones, las instantáneas y las notas sobre las incidencias. Vea *Exportar informes de incidencias, on page 32*.

Para configurar los ajustes para informes de incidencias:

1. Vaya a **Configuration > Server > Incident report (Configuración > Servidor > Informe de incidencias)**.

2. En **Location (Ubicación)**, seleccione dónde quiere almacenar los informes de incidencias.
3. En el menú desplegable **Export format (Formato de exportación)**, seleccione el formato con el que quiera exportar las grabaciones.
4. En **Categories (Categorías)**, agregue o elimine categorías para agrupar los informes de incidencias. Las categorías pueden ser el nombre de carpeta en la ubicación de exportación si configura la categoría como variable en la ruta de directorio del servidor.
 - 4.1. Introduzca en el cuadro el nombre de la categoría; por ejemplo, Accidente o Robo.
 - 4.2. Haga clic en **Añadir**.
 - 4.3. Para eliminar una categoría, selecciónela y haga clic en **Remove (Eliminar)**.
5. En **Description template (Descripción de plantilla)**, escriba la información que se mostrará en **Description (Descripción)** cuando se generen los informes de incidencias. Por ejemplo: Informe por: <Introduzca su nombre, correo electrónico y número de teléfono>.
6. Haga clic en **Aplicar**.

Establecimiento	
Server directory path (Ruta al directorio del servidor)	Seleccione y especifique la ruta de directorio para guardar los informes de incidencias en una carpeta del equipo. Puede usar como variables el nombre de servidor, la categoría o el nombre de usuario. Por ejemplo: C:\Reports\\$(Server Name)\\$(Category)\\$(User Name)\.
Network directory path (Ruta al directorio de red)	Seleccione esta opción para guardar los informes de incidencias en una carpeta de un almacenamiento de red. Introduzca la ruta del directorio o use las credenciales del almacenamiento de red. El recurso compartido debe ser accesible desde el servidor de AXIS Camera Station Pro. Consulte <i>Gestionar almacenamiento</i> para ver cómo agregar un almacenamiento para usarlo para grabaciones.

Formato de exportación	
ASF	Si se selecciona esta opción, se puede elegir Add digital signature (Agregar firma digital) para usar una firma digital y así impedir la manipulación de imágenes. Consulte la sección sobre la firma digital en <i>Exportar grabaciones</i> . También puede seleccionar Use password (Usar contraseña) para utilizar una contraseña para la firma digital.
MP4	Las grabaciones exportadas no incluyen audio en formato G.711 o G.726.

Exportación programada

Vaya a **Configuration > Server > Scheduled export (Configuración > servidor > Exportación programada)** para crear programaciones de exportación de grabaciones.

A la hora seleccionada, se exportarán todas las grabaciones a partir de la exportación anterior. Si la última exportación tiene más de una semana o si no hay una exportación anterior, la exportación solo cuenta las grabaciones de menos de una semana. Para exportar grabaciones más antiguas, vaya a la pestaña **Recordings (Grabaciones)** y expórtelas manualmente. Vea *Exportar grabaciones*.

Nota

Al conectarse a varios servidores de AXIS Camera Station Pro, puede seleccionar cualquier servidor del menú desplegable **Selected server (Servidor seleccionado)** para activar y gestionar las exportaciones programadas.

Exportación de grabaciones programadas

1. En **Scheduled export (Exportación programada)**, seleccione **Enable scheduled export (Habilitar exportación programada)** para usar la exportación programada.
2. En **Cameras (Cámaras)**, seleccione las cámaras cuyas grabaciones desea exportar. El sistema selecciona todas las cámaras de la lista de forma predeterminada. Desactive **Use all cameras (Usar todas las cámaras)** y seleccione cámaras concretas en la lista.
3. En **Export (Exportar)**, determine dónde guardar las grabaciones, el formato y la creación de una lista de reproducción.
4. En **Weekly schedule (Programación semanal)**, seleccione la hora y los días en los que se exportarán las grabaciones.
5. Haga clic en **Aplicar**.

Exportar	
Server directory path (Ruta al directorio del servidor)	Seleccione e introduzca la ruta del directorio para guardar las grabaciones en una carpeta del equipo.
Network directory path (Ruta al directorio de red)	Seleccione esta opción para guardar las grabaciones en una carpeta de un almacenamiento de red. Introduzca la ruta del directorio o use las credenciales del almacenamiento de red. El recurso compartido debe ser accesible desde el servidor de AXIS Camera Station Pro. Consulte <i>Gestionar almacenamiento</i> para ver cómo agregar un almacenamiento para usarlo para grabaciones.
Crear lista de reproducción (.asx)	Seleccione esta opción para crear una lista de reproducción en formato .asx que se usa en Windows Media Player. Las grabaciones se reproducen en el orden en el que se grabaron.
Formato de exportación	Permite seleccionar el formato en el que se deben exportar las grabaciones. ASF (ASF) – Select (Seleccione) Add digital signature (Agregar firma digital) para usar una firma digital e impedir la manipulación de la imagen. Consulte la sección sobre la firma digital en <i>Exportar grabaciones</i> . También puede seleccionar Use password (Usar contraseña) para utilizar una contraseña para la firma digital. MP4: las grabaciones exportadas no incluyen audio en formato G.711 o G.726.

Microsoft Windows 2008 Server

Para poder exportar grabaciones desde un servidor con Microsoft Windows 2008 Server, debe instalar la experiencia de escritorio:

1. Haga clic en **Inicio > Herramientas administrativas > Administrador de servidores** para abrir el Gestor del servidor.
2. En **Features summary (Resumen de características)**, haga clic en **Add features (Agregar características)**.

3. Seleccione **Desktop Experience (Experiencia de escritorio)** y haga clic en **Next (Siguiente)**.
4. Haga clic en **Instalar**.

Microsoft Windows 2012 Server

Para poder exportar grabaciones desde un servidor con Microsoft Windows 2012 Server, debe instalar la experiencia de escritorio:


1. Haga clic en **Inicio > Herramientas administrativas > Administrador de servidores** para abrir el Gestor del servidor.
2. Seleccione **Administrar > Agregar roles y características** para iniciar el Asistente para agregar roles y características.
3. En la sección **Features Summary (Resumen de características)**, seleccione **User Interfaces and Infrastructure (Infraestructura e interfaces de usuario)**.
4. Seleccione **Desktop Experience (Experiencia de escritorio)** y haga clic en **Next (Siguiente)**.
5. Haga clic en **Instalar**.

Ajustes de WebRTC


El cliente web para AXIS Camera Station usa WebRTC para comunicarse con el servidor.

Activar TURN	Esta opción habilita un servidor TURN local en el servidor de AXIS Camera Station Pro. Seleccione Enable TURN (Habilitar TURN) si desea que la comunicación WebRTC pueda utilizar un único puerto, lo que puede simplificar la configuración del cortafuegos.
Priorizar TURN	Seleccione esta opción si desea que WebRTC considere solo candidatos de relé.

Nueva conexión

Vaya a  > **Servers > New connection (Servidores > Nueva conexión)** para conectarse a un servidor de AXIS Camera Station Pro. Vea *Conectar a un servidor*.

Estado de conexión

Vaya a  > **Servers > Connection status (Servidores > Estado de conexión)** para que se muestre la lista de los estados de conexión para todos los servidores.

Use el control deslizante que hay junto al nombre del servidor para conectarse con el servidor o finalizar la conexión.

Códigos de estado	Descripción	Posibles soluciones
Conectando	El cliente trata de conectar con este servidor.	
Conectado	El cliente usa TCP mientras está conectado a este.	
Conectado (usando Secure Remote Access)	El cliente usa Secure Remote Access cuando está conectado a este servidor.	
Conectado (usando HTTP)	El cliente usa HTTP cuando está conectado a este servidor. Esta opción es menos eficaz que TCP y	

	más lenta en conexiones con varios servidores.	
Desconectando	El cliente se desconecta de este servidor.	
Desconectado	No existe conexión entre el cliente y este servidor.	
Conectando de nuevo	El cliente ha perdido la conexión con este servidor y trata de volver a conectarse.	
Fallo de reconexión	El cliente no puede volver a conectar con este servidor. Encuentra el servidor, pero los permisos o la contraseña del usuario pueden haber cambiado.	<ul style="list-style-type: none"> • Agregue al usuario en el cuadro de diálogo de permiso de usuario. • Verifique el nombre de usuario y la contraseña.
Inicio de sesión cancelado	El usuario ha cancelado el inicio de sesión.	
Nombre de usuario o contraseña incorrectos	Haga clic en el enlace de la columna Action (Acción) e introduzca las credenciales correctas.	
Usuario no autorizado en el servidor	El servidor no autoriza al usuario para que inicie sesión.	Agregue al usuario en el cuadro de diálogo de permiso de usuario.
Fallo de verificación de seguridad	Error de verificación de seguridad relacionado con WCF. Sincronice las horas UTC del equipo cliente y el servidor.	
Ningún contacto con el equipo servidor	No hubo respuesta del equipo servidor en la dirección usada.	<ul style="list-style-type: none"> • Compruebe que la red funciona correctamente. • Compruebe que el servidor se está ejecutando.
Ningún servidor en ejecución	El equipo que ejecuta el servidor es accesible, pero el servidor no se está ejecutando.	Inicie el servidor.
Fallo de comunicación	Error de conexión con el servidor. Asegúrese de que el equipo servidor es accesible.	<ul style="list-style-type: none"> • Compruebe que la red funciona correctamente. • Compruebe que el servidor se está ejecutando.
Nombre de host no válido	El DNS no puede convertir el nombre de host en una dirección IP.	<ul style="list-style-type: none"> • Compruebe que el nombre de host se ha escrito correctamente. • Compruebe que el DNS dispone de la información que necesita.
Ya conectado al mismo servidor	El cliente ya está conectado a este servidor.	Elimine la entrada del servidor duplicado.
No el servidor esperado	Ha respondido un servidor diferente al esperado en esta dirección.	Actualice la lista de servidores para conectar a este servidor.


La versión del cliente (x) no es compatible con la versión del servidor (y)	El cliente es demasiado antiguo o demasiado nuevo comparado con el servidor.	Compruebe que se ha instalado la misma versión de AXIS Camera Station Pro en el equipo cliente y en el equipo servidor.
Servidor demasiado ocupado	El servidor no ha podido responder debido a problemas de rendimiento.	Asegúrese de que el equipo servidor y la red no están sobrecargados.





Varios servidores

Listas de servidores

Los servidores de AXIS Camera Station Pro se pueden organizar en listas de servidores. Un servidor puede pertenecer a varias listas de servidores. Es posible importar, exportar y utilizar listas de servidores en otros clientes de AXIS Camera Station Pro.

Vaya a  > Servers > Server lists (Servidores > Listas de servidores) para abrir el cuadro de diálogo de listas de servidores.

Se muestra la lista predeterminada **Recent connections (Conexiones recientes)**, que contiene los servidores usados en la sesión anterior. Las **Recent connections (Conexiones recientes)** no se puede eliminar.

	Seleccione la lista de servidores y haga clic en  .
+ New server list (+ Nueva lista de servidores)	Haga clic en esta opción para agregar una nueva lista de servidores e introduzca un nombre para la lista.
Agregar	Para agregar un servidor a una lista de servidores, seleccione la lista y haga clic en Agregar . Introduzca la información necesaria.
Export lists (Exportar listas)	Haga clic en esta opción para exportar todas las listas de servidores en un archivo .msl. Puede importar la lista de servidores para iniciar sesión en los servidores. Vea <i>Conectar a un servidor</i> .
Editar	Para editar un servidor de una lista de servidores, seleccione el servidor y haga clic en Edit (Editar) . Solo puede editar un servidor cada vez.
Eliminar	Para eliminar servidores de una lista de servidores, seleccione los servidores y haga clic en Remove (Eliminar) .
Cambiar el nombre de un servidor	Haga doble clic en la lista e introduzca un nuevo nombre para la lista.



Organizar servidores en listas de servidores

Configurar switch

Si tiene un dispositivo de la serie AXIS Camera Station S22, puede configurarlo desde AXIS Camera Station Pro. Vaya a **Configuration > Switch > Management (Configuración > Switch > Gestión)** e introduzca sus credenciales para abrir la página de gestión del switch en el cliente de AXIS Camera Station Pro. Para obtener información cómo configurar el switch, consulte el manual de usuario de AXIS Camera Station serie S22 en *axis.com*.

Nota

AXIS Camera Station Pro solo puede conectarse a <https://192.168.0.1/> que es la dirección IP predeterminada del switch.

Gestionar licencias

La página Gestionar licencias muestra el estado actual de la licencia.

Prueba	Al instalar AXIS Camera Station Pro, dispone de un periodo de prueba de 90 días. Durante este periodo, el sistema es completamente funcional, lo que le permite configurarlo y probar todas las características antes de comprar cualquier licencia.
Comprobar las licencias	Si el periodo de licencia del sistema caduca sin la renovación automática, AXIS License Manager le ofrece otro periodo de gracia de 30 días.
Con licencia	El sistema dispone de licencia completa y está en funcionamiento hasta la fecha de caducidad más temprana.

<p>Los cambios realizados en el sistema requieren una sincronización de licencia</p>	<p>Al agregar dispositivos a un sistema con licencia, AXIS Camera Station Pro intenta sincronizar los cambios con AXIS License Manager para reevaluar el estado de la licencia del sistema. Si utiliza licencias automáticas, es posible que no observe que esto sucede. Sin embargo, si utiliza la licencia manual y no puede resincronizar los cambios del sistema con AXIS License Manager en un plazo de 60 días, el sistema dejará de tener licencia.</p>
<p>Sin licencia</p>	<p>El sistema funciona pero tiene una funcionalidad limitada. Las reglas de grabación y acción continúan funcionando y no perderá ninguna grabación. Las siguientes funciones no estarán operativas:</p> <ul style="list-style-type: none"> • Secuencias en directo • Reproducción de grabaciones • Reproducción instantánea • Toma de capturas • Exportar grabaciones

Puede elegir licenciar el sistema de dos maneras:

Licencias automáticas (sistemas en línea) – Con esta opción, el sistema inserta automáticamente los cambios que afectan al número de licencias en AXIS License Manager y recupera un nuevo estado de licencia. Esta opción requiere una conexión a Internet. Consulte *Autorizar un sistema en línea, on page 136* para obtener más información.

Licencias manuales (sistemas sin conexión) – Si utiliza esta opción, debe exportar manualmente el archivo del sistema, cargarlo en AXIS License Manager y, finalmente, importar la nueva licencia en el sistema. Cada vez que realice cambios en el sistema que afecten al número de licencias, debe repetir la licencia manual. Elija esta opción si prefiere gestionar las licencias manualmente o si el sistema no tiene conexión a Internet. Consulte *Autorizar un sistema fuera de línea, on page 136* para obtener más información.

Autorizar un sistema en línea

Para utilizar la licencia automática, debe registrar el sistema y conectarlo a una organización.

1. Vaya a Configuration (Configuración) > Licenses (Licencias) > Management (Gestión).
2. Asegúrese de que la Automatic licensing (Licencia automática) esté activada.
3. Haga clic en Register... (Registrar...).
4. Inicie sesión con la cuenta de My Axis y siga las instrucciones de la pantalla.
5. Haga clic en Go to AXIS License Manager (Ir a AXIS License Manager) para administrar las licencias allí. Lea el *manual del usuario de My Systems en help.axis.com* para obtener más información.

Autorizar un sistema fuera de línea

Para autorizar el sistema manualmente:

1. Vaya a Configuration (Configuración) > Licenses (Licencias) > Management (Gestión).
2. Desactive Automatic licensing (Licencia automática).
3. Haga clic en Export system file... (Exportar archivo de sistema...) y guarde el archivo en el equipo.

Nota

Debe conectarse a Internet para acceder a AXIS License Manager. Si el equipo del cliente no dispone de Internet, copie el archivo de sistema en un ordenador que lo haga.

4. Abra *AXIS License Manager*.
5. En *AXIS License Manager*:
 - 5.1. Seleccione la organización correcta o cree una si todavía no lo ha hecho. Lea el *manual del usuario de My Systems en help.axis.com* para obtener más información.
 - 5.2. Vaya a **System setup (Configuración del sistema)**.
 - 5.3. Haga clic en **Upload system file (Cargar archivo del sistema)**.
 - 5.4. Haga clic en **Upload system file (Cargar archivo del sistema)** y seleccione el archivo del sistema.
 - 5.5. Haga clic en **Upload system file (Cargar archivo del sistema)**.
 - 5.6. Haga clic en **Download license file (Descargar el archivo de licencia)**.
6. Volver al cliente *AXIS Camera Station Pro*.
7. Haga clic en **Import license file... (Importar archivo de licencia)** y seleccione el archivo de licencia.
8. Haga clic en **Go to AXIS License Manager (Ir a AXIS License Manager)** para administrar las licencias allí.

Configurar la seguridad

Permisos de usuario



Vaya a **Configuration > Security > User permissions (Configuración > Seguridad > Permisos de usuario)** para ver los usuarios y grupos que existen en *AXIS Camera Station Pro*.

Nota

Los administradores del equipo que ejecuta el servidor de *AXIS Camera Station Pro* reciben automáticamente privilegios de administrador de *AXIS Camera Station Pro*. No puede cambiar ni quitar los privilegios del grupo de administradores.

Para poder agregar un usuario o grupo, es necesario registrar el usuario o grupo en el equipo local o comprobar que tiene una cuenta de usuario de Windows® Active Directory. Para agregar usuarios o grupos, consulte *Agregar usuarios o grupos*.

Cuando un usuario forma parte de un grupo, el usuario disfruta del permiso de rol más alto asignado al individuo o grupo. El usuario también tiene el acceso que se le conceda individualmente y recibe los derechos derivados de ser parte de un grupo. Por ejemplo, supongamos que un usuario tiene acceso a la cámara X a nivel individual. El usuario es también miembro de un grupo que tiene acceso a las cámaras Y y Z. En consecuencia, el usuario tiene acceso a las cámaras X, Y y Z.

	Indica que la entrada es un usuario individual.
	Indica que la entrada es un grupo.
Nombre	El nombre de usuario que aparece en el equipo local o Active Directory.
Dominio	Es el dominio al que pertenece el usuario o grupo.
Función	El rol de acceso proporcionado al usuario o grupo. Valores posibles: Administrador, Operador y Visor.
Detalles	Información detallada sobre el usuario según aparece en el ordenador local o Active Directory.
Servidor	Es el servidor al que pertenece el usuario o grupo.

Agregar usuarios o grupos

Los usuarios y grupos de Microsoft Windows® y Active Directory pueden acceder a AXIS Camera Station Pro. Para agregar un usuario a AXIS Camera Station Pro, debe agregar usuarios o un grupo a Windows®.

Añadir un usuario en Windows® 10 y 11:

- Pulse la tecla de Windows + X y seleccione **Computer Management (Gestión de equipos)**.
- En la ventana **Computer Management (Gestión de equipos)**, vaya a **Local Users and Groups (Usuarios y grupos locales) > Users (Usuarios)**.
- Haga clic con el botón derecho en la carpeta **Users (Usuarios)** y seleccione **New user (Nuevo usuario)**.
- En el cuadro de diálogo emergente, introduzca los datos del nuevo usuario y desmarque **User must change password at next login (El usuario debe cambiar la contraseña en el próximo inicio de sesión)**.
- Haga clic en **Create (Crear)**.

Si utiliza un dominio de Active Directory, consulte con su administrador de red.

Agregar usuarios o grupos

1. Vaya a **Configuration > Security > User permissions (Configuración > Seguridad > Permisos de usuario)**.
2. Haga clic en **Añadir**.
Puede ver los usuarios y grupos disponibles en la lista.
3. En **Scope (Ámbito)**, seleccione dónde se deben buscar usuarios y grupos.
4. En **Show (Mostrar)**, seleccione esta opción para mostrar usuarios o grupos.
El resultado de la búsqueda no se muestra si hay demasiados usuarios o grupos. Use la función de filtrado.
5. Seleccione los usuarios o grupos y haga clic en **Agregar**.

Ámbito	
Servidor	Seleccione esta opción para buscar usuarios o grupos en el equipo local.
Dominio	Seleccione esta opción para buscar usuarios o grupos en Active Directory.
Servidor seleccionado	Si está conectado a varios servidores AXIS Camera Station Pro, seleccione un servidor en el menú desplegable Selected server (Servidor seleccionado) .

Configurar un usuario o grupo

1. Seleccione un usuario o grupo en la lista.
2. En **Role (Rol)**, seleccione **Administrator (Administrador)**, **Operator (Operador)** o **Viewer (Visor)**.
3. Si ha seleccionado **Operator (Operador)** o **Viewer (Visor)**, puede configurar los privilegios de usuario o grupo. Vea *Privilegios de usuario o grupo*.
4. Haga clic en **Save (Guardar)**.

Eliminar un usuario o grupo

1. Seleccione un usuario o un grupo.
2. Haga clic en **Remove (Eliminar)**.
3. En el diálogo emergente, haga clic en **Aceptar** para eliminar el usuario o el grupo.

Privilegios de usuario o grupo

Existen tres roles que se pueden dar a un usuario o grupo. Para ver cómo definir el rol de un usuario o un grupo, consulte *Agregar usuarios o grupos*.

Administrador – Acceso completo a todo el sistema, incluido acceso al vídeo en directo y grabado de todas las cámaras, a todos los puertos de E/S y a todas las vistas. Este rol es necesario para configurar cualquier aspecto del sistema.

Operador – Puede seleccionar cámaras, vistas y puertos de E/S para obtener acceso a vídeos en directo y grabados. Un operador tiene acceso completo a todas las funciones de AXIS Camera Station Pro excepto la configuración del sistema.

Visitante – Puede acceder al vídeo en directo de cámaras, puertos de E/S y vistas seleccionados. Un visor no tiene acceso a la configuración de vídeo grabado o del sistema.

Cámaras

Los siguientes privilegios de acceso están disponibles para grupos o usuarios con el rol **Operator (Operador)** o **Viewer (Visor)**.

Acceso	permite el acceso a la cámara y a todas las características de la cámara.
Vídeo	permite al usuario acceder a vídeo en directo desde la cámara.
Escuchar audio	Permite el acceso a la escucha desde la cámara.
Transmisión de audio	Permite el acceso para hablar con la cámara.
Grabación manual	permite iniciar y detener grabaciones de forma manual.
PTZ mecánica	permite el acceso a los controles PTZ mecánicos. Solo disponible para cámaras con PTZ mecánico.
Prioridad PTZ	Define la prioridad PTZ. Un número más bajo significa una mayor prioridad. Si no hay ninguna prioridad asignada, el valor es 0. Un administrador tiene la más alta prioridad. Cuando un rol con mayor prioridad opera una cámara PTZ, los demás no pueden operar la misma cámara durante 10 segundos de manera predeterminada. Solo está disponible para cámaras con PTZ mecánico y con Mechanical PTZ (PTZ mecánico) seleccionado.

Vistas

Los siguientes privilegios de acceso están disponibles para grupos o usuarios con el rol **Operator (Operador)** o **Viewer (Visor)**. Puede seleccionar varias vistas y configurar los privilegios de acceso.

Acceso	Permitir acceso a las vistas en AXIS Camera Station Pro.
Editar	Permitir editar las vistas en AXIS Camera Station Pro.

E/S

Los siguientes privilegios de acceso están disponibles para grupos o usuarios con el rol **Operator (Operador)** o **Viewer (Visor)**.

Acceso	permite acceso total al puerto de E/S.
Lectura	permite al usuario ver el estado del puerto de E/S. El usuario no puede cambiar el estado del puerto.
Escritura	permite cambiar el estado del puerto de E/S.

Sistema

Los privilegios de acceso en gris en la lista no se pueden configurar. La marca de verificación implica que el usuario o grupo tiene este privilegio de forma predeterminada.

Los siguientes privilegios de acceso están disponibles para usuarios o grupos con el rol **Operator (Operador)**. **Take snapshots (Tomar instantáneas)** también está disponible para el rol **Viewer (Visor)**.

Tomar instantáneas	Permite tomar instantáneas en el modos de visualización en directo y grabación.
Exportar grabaciones	Permite exportar grabaciones.
Generar informe de incidencias	Permite generar informes de incidencias.
Prevent access to recordings older than (Impedir el acceso a grabaciones anteriores a)	Impide acceder a grabaciones más antiguas que el número de minutos especificado. Los usuarios no encuentran estas grabaciones cuando realizan una búsqueda.
Acceder a alarmas, tareas y registros	Proporciona notificaciones de alarma y permite el acceso a la barra Alarms and tasks (Alarmas y tareas) y a la pestaña Logs (Registros) .
Access data search (Búsqueda de datos de acceso)	Permite buscar datos para realizar el seguimiento de lo que ocurrió en el momento del evento.
Añadir categorías a los eventos	Permitir añadir categorías de evento a la pestaña Recordings (Grabaciones) .
Eliminar categorías de evento	Permitir eliminar categorías de evento de la pestaña Recordings (Grabaciones) .

Control de acceso

Los siguientes privilegios de acceso están disponibles para usuarios o grupos con el rol **Operator (Operador)**. **Access Management (Gestión de acceso)** también está disponible para el rol **Viewer (Visor)**.

Configuración de control de acceso	Permite configurar puertas y zonas, perfiles de identificación, formatos de tarjeta y PIN, comunicación cifrada y servidor múltiple.
Gestión de acceso	Permite gestionar el acceso y acceder a los ajustes de Active Directory.

AXIS Audio Manager Pro

Los siguientes privilegios de acceso están disponibles para grupos o usuarios con el rol **Operator (Operador)** o **Viewer (Visor)**.

Acceda a la configuración de componentes de AXIS Audio Manager Pro	Solo para operadores. Permitir la configuración de AXIS Audio Manager Pro en AXIS Camera Station Pro y el acceso a la interfaz del servidor de AXIS Audio Manager Pro.
Acceso a la interfaz de AXIS Audio Manager Pro	Solo para visores. Permitir el acceso a la interfaz del servidor AXIS Audio Manager Pro.

Los siguientes privilegios de acceso están disponibles para usuarios o grupos con el rol **Viewer (Visor)**.

Supervisión del estado del sistema

Los siguientes privilegios de acceso están disponibles para usuarios o grupos con el rol **Operator (Operador)**. **Access to system health monitoring (Acceso a supervisión del estado del sistema)** también está disponible para el rol **Viewer (Visor)**.

Configuration of system health monitoring (Configuración de Supervisión del estado del sistema)	Permite configurar la supervisión del estado del sistema.
Access to system health monitoring (Acceder a supervisión del estado del sistema)	Permite acceder al sistema de supervisión del estado del sistema.

Certificados

Para gestionar los ajustes de los certificados entre el servidor de AXIS Camera Station Pro y los dispositivos, vaya a **Configuration > Security > Certificates (Configuración > Seguridad > Certificados)**.

Para obtener información sobre cómo activar, eliminar y ver certificados HTTPS y IEEE 802.1X, consulte *Seguridad, on page 70*.

AXIS Camera Station Pro se puede utilizar como:

- **Autoridad de certificación (CA) raíz:** Si usa AXIS Camera Station Pro como CA raíz significa que AXIS Camera Station Pro utiliza su propio certificado raíz para emitir certificados de servidor y no hay ninguna otra CA raíz implicada en el proceso.
- **Autoridad de certificación intermedia:** En este caso se necesita importar un certificado CA y su clave privada en AXIS Camera Station Pro para firmar y emitir certificados de servidor para los dispositivos de Axis. Este certificado CA puede ser un certificado root o un certificado CA intermedio.

Nota

Al desinstalar AXIS Camera Station Pro, elimina sus certificados CA de las Autoridades de Certificación Raíz de Confianza de Windows. Los certificados CA importados deben eliminarse manualmente.

Autoridad de certificación (CA)

Una CA permite activar HTTPS y IEEE 802.1X en dispositivos sin necesidad de instalar certificados de cliente y servidor. El certificado CA de AXIS Camera Station Pro puede automáticamente crear, iniciar sesión e instalar certificados de cliente/servidor en dispositivos al utilizar HTTPS o IEEE 802.1X. Puede utilizar AXIS Camera Station Pro como CA raíz o importar un certificado CA y dejar que AXIS Camera Station Pro actúe como CA intermedia. El sistema genera una CA raíz al instalar el servidor.

Importar	Haga clic en esta opción para importar un certificado CA existente y su clave privada. AXIS Camera Station Pro almacena su contraseña.
Generar	Haga clic para generar una nueva clave pública y privada y un certificado CA autofirmado válido durante 10 años. Si genera una nueva autoridad de certificación, se sustituyen todos los certificados de

	los componentes y se reinician todos los componentes.
Ver	Haga clic en esta opción para ver los detalles del certificado CA.
Exportar	Haga clic para exportar el CA a un archivo. Puede exportarlo de dos maneras: <ul style="list-style-type: none"> • Sin la clave privada: Guarda el certificado en formato .cer o .crt. Use esta opción si solo necesita instalar el certificado público en otros sistemas que deban confiar en certificados firmados por AXIS Camera Station Pro. • Con la clave privada: Guarda el CA en formato PKCS#12 (.pfx o .p12). Use esta opción si necesita importar el CA a otro servidor AXIS Camera Station Pro. <p>No puede volver a importar un certificado .cer o .crt a AXIS Camera Station Pro.</p>
Number of dates the signed client/server certificates will be valid for (Número de días durante los que serán válidos los certificados de servidor/cliente firmados)	Defina el número de días durante los que son válidos los certificados de servidor/cliente creados automáticamente. El número máximo es de 1095 días (tres años). La autoridad de certificación no firma certificados que sean válidos después de su propia fecha de caducidad.

Generar una CA root:

Cuando se inicia AXIS Camera Station Pro, busca una CA. Si falta, genera una CA raíz automáticamente. Incluye un certificado raíz firmado por el propio producto y una clave privada protegida con una contraseña. AXIS Camera Station Pro almacena la contraseña pero no la hace visible. Un certificado CA generado por AXIS Camera Station Pro es válido durante 10 años.

Para generar manualmente una nueva CA para sustituir la antigua, consulte *Sustituir una CA, on page 143*.

Si actualiza desde la versión 5.45 o anterior que use un certificado instalado manualmente en un dispositivo, AXIS Camera Station Pro usa automáticamente la CA root existente para instalar un nuevo certificado cuando caduque el instalado manualmente.

Nota

Cuando genera un certificado CA, se agrega a los certificados root de confianza de Windows.

Importar un CA:

Cuando instala un certificado CA de otra CA, puede utilizar AXIS Camera Station Pro como una CA intermedia. Importe una CA existente consistente en un certificado y una clave privada para permitir a AXIS Camera Station Pro firmar certificados en nombre de dicha CA. El archivo debe ser un archivo PKCS#12, el certificado debe tener una restricción básica (2.5.29.19) que indique que se trata de un certificado CA y debe utilizarse dentro del periodo de validez. Para importar una CA para sustituir la existente, consulte *Sustituir una CA, on page 143*.

Nota

- Si la autoridad de certificación importada no requiere contraseña, se muestra un cuadro de diálogo cada

vez que una acción requiera contraseña. Por ejemplo, al usar HTTPS o IEEE en un dispositivo o al agregar un dispositivo. Debe hacer clic en **OK (Aceptar)** para continuar.

- Cuando importa un certificado CA, se agrega a certificados raíz de confianza de Windows.
- Después de desinstalar AXIS Camera Station Pro, debe eliminar manualmente los certificados CA de las Autoridades de Certificación Raíz de Confianza de Windows.

Sustituir una CA

Para sustituir la autoridad de certificación que emite los certificados firmados usados en dispositivos con conexión HTTPS:

1. Vaya a **Configuration > Security > Certificates > HTTPS (Configuración > Seguridad > Certificados > HTTPS)**.
2. Desactive **Validate device certificate (Validar el certificado del dispositivo)**.
3. En **Certificate authority (Autoridad de certificación)**, haga clic en **Generate (Generar)** o **Import (Importar)**.
4. Introduzca su contraseña y haga clic en **OK (Aceptar)**.
5. Seleccione el número de días de validez de los certificados cliente/servidor firmados.
6. Vaya a **Configuración > Dispositivos > Gestión**.
7. Haga clic con el botón derecho del ratón en los dispositivos y seleccione **Seguridad > HTTPS > Habilitar/Actualizar**.
8. Vaya a **Configuration (Configuración) > Security (Seguridad) > Certificates (Certificados) > HTTPS** y active **Validate device certificate (Validar el certificado del dispositivo)**.

Emitir un certificado personalizado

Puede crear un certificado personalizado firmado por la autoridad de certificación de AXIS Camera Station Pro. Por ejemplo, puede utilizar estos certificados para extremos HTTPS externos. Debe renovar manualmente estos certificados cuando caduquen. Para emitir un certificado personalizado:

1. Vaya a **Configuration (Configuración) > Security (Seguridad) > Certificates (Certificados)**.
2. En **Issue custom certificate (Emitir certificado personalizado)**, haga clic en **Issue certificate... (Emitir certificado...)**.
3. Introduzca los detalles del certificado y haga clic en **OK (Aceptar)**.

Emitir certificado	
Nombre común (CN)	Identifica el titular del certificado. El CN suele ser el nombre de dominio completamente cualificado (FQDN) o la dirección IP en la que se instala el certificado.
Contraseña de clave privada	La contraseña que protege la clave privada.
Duración (días)	El número de días que es válido el certificado.
Autenticación de servidor	Seleccione esta opción si tiene previsto utilizar el certificado en un servidor como prueba de la identidad del servidor. Normalmente, los dispositivos u otros extremos con los que AXIS Camera Station Pro se conecta con HTTPS se consideran dispositivos de servidor y los certificados deben usar autenticación de servidor.
Autenticación de cliente	Seleccione esta opción si tiene previsto utilizar el certificado en un cliente como prueba de la identidad del cliente antes de permitir la conexión a un

Emitir certificado	
	servidor. Por ejemplo, los dispositivos que quieran acceder a una red controlada por acceso IEEE 802.1X deben utilizar este certificado antes de introducirlo.
Organización (O)	Organización del titular del certificado.
Código de países (C)	El código del país del titular del certificado.
DNS SAN	Nombres alternativos de asunto del servidor de nombres dinámicos. FQDN alternativas para contactar con el titular del certificado. Al emitir un certificado, el sistema agrega automáticamente el CN como un SAN de DNS. Puede introducir varias direcciones separadas por comas, por ejemplo, <code>dirección-1.com, dirección-2.com</code> .
IP SAN	Nombres alternativos del sujeto de la dirección IP. Direcciones IP alternativas para contactar con el titular del certificado. El sistema agrega automáticamente el CN como un SAN de IP si el CN es una dirección IP. Puede introducir varias direcciones separadas por comas, por ejemplo, <code>192.168.1.1,192.168.1.2</code> .

HTTPS

De forma predeterminada, AXIS Camera Station Pro valida la firma del certificado activo del servidor HTTPS en cada dispositivo conectado y no se conecta a ningún dispositivo que no tenga un certificado válido. El certificado del servidor debe estar firmado por la CA activa en AXIS Camera Station Pro o validado a través del Almacén de certificados de Windows. AXIS Camera Station Pro también valida si la dirección en el certificado HTTPS del dispositivo coincide con la dirección utilizada para comunicarse con el dispositivo si **Validate device address (Validar la dirección del dispositivo)** está activo.

Las cámaras con firmware 7.20 o posterior se suministran con un certificado con firma propia. Estos certificados no son de confianza. Debe generar o importar una CA para que AXIS Camera Station Pro pueda emitir nuevos certificados para los dispositivos al utilizar HTTPS.

Validar certificado	Active esta opción para permitir la conexión solo para dispositivos con un certificado válido. Sin validación de certificado, permite acceder a dispositivos con un certificado no válido.
Validar dirección de dispositivo	Desactive para un comportamiento estable en redes DHCP sin utilizar nombres de host. Active la función para exigir que las direcciones coincidan para aumentar la seguridad. Recomendamos que active este ajuste solo en redes en las que los dispositivos usan sobre todo el nombre de host para comunicarse o en dispositivos que tienen una dirección IP estática.

Nota

- Cuando no disponga de una conexión segura (HTTPS), podrá emitir un nuevo certificado HTTPS. Consulte *Agregar dispositivos, on page 46*
- Para utilizar HTTPS, se requiere una versión de firmware 5.70 o posterior para los dispositivos de vídeo y una versión de firmware 1.25 o posterior para los de control de acceso y de audio.

Limitations (Limitaciones)

- No se admiten los puertos no predeterminados (que no sean el 443).
- Todos los certificados de un lote de instalación deben tener la misma contraseña.
- Las operaciones de certificados a través de canales sin cifrar, como "Básica", no son compatibles. Defina los dispositivos en "Cifrado y sin cifrar" o "Solo cifrado" para permitir la comunicación "Digest".
- HTTPS no se puede activar en AXIS T85 PoE+ Network switch series.

IEEE 802.1X

Para la autenticación AXIS Camera Station Pro IEEE 802.1X, el solicitante es un dispositivo de red de Axis que desee conectarse a la LAN. El autenticador es un dispositivo de red, como un switch Ethernet o un punto de acceso inalámbrico. El servidor de autenticación suele ser un host con software compatible con los protocolos RADIUS y EAP.

Es necesario importar un certificado CA de autenticación IEEE 802.1X para activar IEEE 802.1X. El certificado CA de autenticación IEEE 802.1X y el certificado de cliente IEEE 802.1X se instalan al activar o actualizar IEEE 802.1X. Un certificado para la autenticación se puede obtener externamente, por ejemplo, desde el servidor de autenticación IEEE 802.1X o bien directamente desde AXIS Camera Station Pro. Este certificado se instala en cada dispositivo de Axis y verifica el servidor de autenticación.

Nota

Para utilizar certificados IEEE 802.1X, requiere la versión de firmware 5.50 o posterior para dispositivos de vídeo y la versión de firmware 1.25 o posterior para dispositivos de control de acceso y de audio.

Para configurar IEEE 802.1X:

1. Vaya a **Configuration > Security > Certificates (Configuración > Seguridad > Certificados)**.
2. En el menú desplegable **EAPOL Version (Versión EAPOL)**, seleccione la versión de protocolo de autenticación extensible (EAP) que desea utilizar.
3. En el menú desplegable **EAP identity (Identidad EAP)**, decida si se usará la dirección MAC del dispositivo, el nombre de host del dispositivo o un texto personalizado.
4. Si ha seleccionado **Custom (Personalizado)**, introduzca el texto que funciona como identidad EAP en **Custom (Personalizado)**.
5. Haga clic en **Import (Importar)** y seleccione el archivo de certificado CA de autenticación IEEE 802.1X.
6. En el menú desplegable **Common name (Nombre común)**, determine si se utilizará **Device IP address (Dirección IP del dispositivo)** o la **Device EAP identity (Identidad EAP del dispositivo)** como nombre común en los certificados individuales creados para cada dispositivo cuando AXIS Camera Station Pro actúa como autoridad certificadora.
7. Vaya a **Configuración > Dispositivos > Gestión**.
8. Haga clic con el botón derecho en los dispositivos y seleccione **Security > IEEE 802.1X > Enable/Update (Seguridad > IEEE 802.1X > Habilitar/Actualizar)**.

Limitations (Limitaciones)

- En el caso de dispositivos con varios adaptadores de red, como cámaras inalámbricas), solo puede habilitarse IEEE 802.1X para el primer adaptador, normalmente la conexión por cable.
- No se admiten los dispositivos sin el parámetro `Network.Interface.I0.dot1x.Enabled`. Por ejemplo: AXIS P39 Series, AXIS T85 Series y AXIS T87 Video Decoder.
- Las operaciones de certificados a través de canales sin cifrar, como "Básica", no son compatibles. Defina los dispositivos en "Cifrado y sin cifrar" o "Solo cifrado" para permitir la comunicación "Digest".

Advertencia de caducidad de certificado

Aparece una advertencia un certificado de cliente o servidor ha caducado o está a punto de caducar. La advertencia también desencadena una alarma del sistema para determinados certificados. Se aplica a todos los

certificados de cliente y servidor, certificados CA de dispositivo instalados por AXIS Camera Station Pro, el certificado CA de AXIS Camera Station Pro y el certificado IEEE 802.1X. La advertencia aparece como mensaje en **Status (Estado)** en la página **Device management (Gestión de dispositivos)** y como icono en la lista **Installed certificates (Certificados instalados)**.

En **Certificate expiration warning (Advertencia de caducidad de certificados)**, especifique cuántos días antes de la fecha de caducidad quiere que AXIS Camera Station Pro le notifique.

Renovación de certificados

Renovar el certificado entre el servidor y los dispositivos

Los certificados de cliente o servidor del dispositivo generados por AXIS Camera Station Pro se renuevan automáticamente 7 días antes de que aparezca la advertencia de caducidad. Para que sea así, debe haber activado HTTPS o IEEE 802.1X en el dispositivo. Si quiere renovar o actualizar un certificado manualmente, consulte *Seguridad, on page 70*.

Renovar el certificado entre el servidor y el cliente

Puede generar un nuevo certificado de servidor en la pestaña **Certificados** del control de servicio de AXIS Camera Station Pro. Para obtener instrucciones, consulte *Certificados, on page 232*.

Restablecer la contraseña

1. Vaya a **Configuration > Security > Certificates (Configuración > Seguridad > Certificados)**.
2. Desactive **Validate device certificate (Validar el certificado del dispositivo)** para asegurarse de que se puede acceder a los dispositivos que usan certificados CA.
3. En **Certificate authority (Autoridad de certificación)**, haga clic en **Generate (Generar)** e introduzca su contraseña.
4. En **Certificate authority (Autoridad de certificación)**, haga clic en **Export (Exportar)** para guardar el certificado CA localmente.
5. Vaya a **Configuración > Dispositivos > Gestión** y active HTTPS en los dispositivos seleccionados.
6. Active **Validate device certificate (Validar el certificado del dispositivo)**.

Configure el control de acceso

Si agrega una controladora de accesos en red al sistema, puede configurar el hardware de control de acceso en AXIS Camera Station versión 6.x o posterior.

Para obtener un flujo de trabajo adecuado que permita configurar una controladora de accesos en red de Axis en AXIS Camera Station Pro, consulte *Configurar una controladora de accesos en red de Axis*.

Nota

Antes de empezar, haga lo siguiente:

- Actualice la versión del AXIS OS del controlador en **Configuration (Configuración) > Devices (Dispositivos) > Management (Gestión)**.
- Fije la fecha y la hora para el controlador en **Configuration > Devices > Management (Configuración > Dispositivos > Administrar)**.
- Active HTTPS en el controlador en **Configuration > Devices > Management (Configuración > Dispositivos > Administrar)**.

Workflow to configure access control (Flujo de trabajo para configurar el control de acceso)

1. Para editar los perfiles de identificación predefinidos o crear un nuevo perfil de identificación, consulte *Perfiles de identificación, on page 164*.
2. Para utilizar una configuración personalizada para los formatos de tarjeta y la longitud del PIN, consulte *Formatos de tarjeta y PIN, on page 167*.

3. Agregue una puerta y aplique un perfil de identificación a la puerta. *Vea [Agregar una puerta](#), on page 149.*
4. Configure la puerta.
 - *[Agregar un monitor de puerta](#), on page 156*
 - *[Agregar entrada de emergencia](#), on page 158*
 - *[Agregar un lector](#), on page 158*
 - *[Agregar un dispositivo REX](#), on page 161*
5. Agregue una zona y agregue puertas a la zona. *Vea [Agregar una zona](#), on page 162.*

Compatibilidad de software de dispositivos para controladores de puerta

Importante

Tenga en cuenta lo siguiente cuando actualice el sistema operativo AXIS OS en su controlador de puerta:




- **Versiones de AXIS OS compatibles:** Las versiones de AXIS OS compatibles que se enumeran a continuación solo se aplican cuando se actualiza desde su versión original recomendada de AXIS Camera Station Pro y cuando el sistema tiene una puerta. Si el sistema no reúne estas condiciones, debe actualizarse a la versión de AXIS OS recomendada para la versión específica de AXIS Camera Station Pro.
- **Versión mínima compatible de AXIS OS:** La versión de AXIS OS más antigua instalada en el sistema determina la versión de AXIS OS mínima compatible, con un límite de dos versiones anteriores. Supongamos que está utilizando la versión 6.5 de AXIS Camera Station Pro y actualiza todos los dispositivos a la versión 12.0.86.2 de AXIS OS recomendada. Entonces, la versión 12.0.86.2 de AXIS OS se convierte en la versión mínima compatible para su sistema en adelante.
- **Actualizar más allá de la versión recomendada de AXIS OS:** Supongamos que actualiza a una versión de AXIS OS superior a la recomendada para una versión concreta de AXIS Camera Station Pro. Después, siempre puede regresar a la versión de AXIS OS recomendada sin ningún problema, siempre y cuando esté dentro de los límites de soporte técnico establecidos para la versión de AXIS Camera Station Pro.
- **Futuras recomendaciones de AXIS OS:** Siga siempre la versión de AXIS OS recomendada para la versión correspondiente de AXIS Camera Station Pro con el fin de garantizar la estabilidad del sistema y una compatibilidad total.

La siguiente tabla indica la versión mínima y recomendada del AXIS OS para cada versión de AXIS Camera Station Pro:

Versión de AXIS Camera Station	Versión mínima de AXIS OS	Versión recomendada de AXIS OS
Pro 6.15	12.5.68.1	12.8.55.1
Pro 6.14	12.5.68.1	12.8.55.1
Pro 6.13	12.5.68.1	12.6.102.1

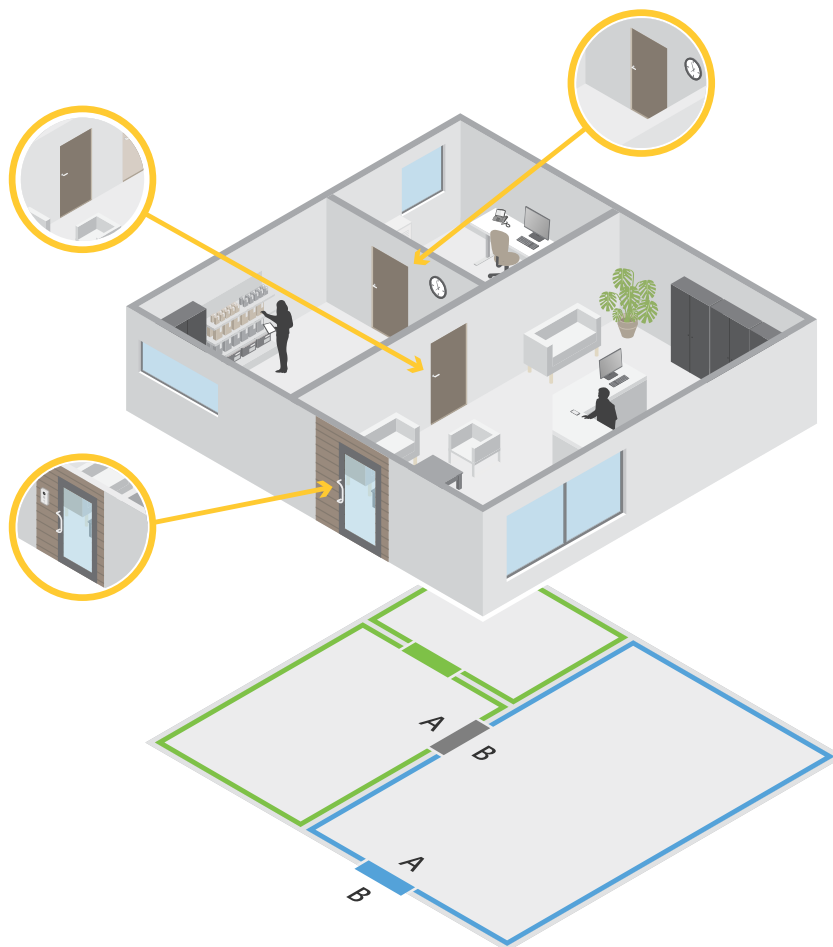
Puertas y zonas

Vaya a **Configuration > Access control > Doors and zones (Configuración > Control de acceso > Puertas y zonas)** para obtener una visión general y configurar puertas y zonas.

 Gráfico de PIN	Ver el gráfico de pines del controlador asociado a una puerta. Si desea imprimir el gráfico de pines, haga clic en Print (Imprimir) .
 Perfil de identificación	Cambie el perfil de identificación en las puertas.
 Canal seguro	Active o desactive OSDP Secure Channel para un lector específico.

Puertas	
Nombre	El nombre de la puerta.
Controlador de puerta	El controlador de puerta conectado a la puerta.
Lado A	La zona en la que está el lado A de la puerta.
Cara B	La zona en la que está el lado B de la puerta.
Perfil de identificación	Perfil de identificación aplicado a la puerta.
Formatos de tarjeta y PIN	Muestra el tipo de formatos de tarjeta o la longitud del PIN.
Estado	<p>Estado de la puerta.</p> <ul style="list-style-type: none"> • Online (En línea): La puerta está en línea y funciona correctamente. • Lector sin conexión: El lector de la configuración de puerta no tiene conexión. • Error del lector: El lector de la configuración de puerta no admite canal seguro o el canal seguro no está activado para el lector.
Zonas	
Nombre	Nombre de la zona.
Número de puertas	El número de puertas incluidas en la zona.

Ejemplo de puertas y zonas



- Hay dos zonas: zona verde y zona azul.
- Hay tres puertas: puerta verde, puerta azul y puerta marrón.
- La puerta verde es una puerta interna de la zona verde.
- La puerta azul es una puerta perimetral solo para la zona azul.
- La puerta azul es una puerta perimetral para la zona verde y la zona azul.

Agregar una puerta

Nota

- Puede configurar un controlador de puerta con una puerta que tenga dos cerraduras o dos puertas que tengan una cerradura cada una.
- Si un controlador de puerta no tiene puertas y está utilizando una nueva versión de AXIS Camera Station Pro con un firmware más antiguo en el controlador de la puerta, el sistema le impedirá añadir una puerta. Sin embargo, el sistema admite puertas nuevas en los controladores del sistema con firmware anterior si ya hay una puerta existente.

Cree una nueva configuración de puerta para agregar una puerta:

1. Vaya a **Configuration (Configuración) > Access control (Control de acceso) > Doors and zones (Puertas y zonas)**.
2. Haga clic en **+ Add door (Añadir una puerta)** y seleccione un tipo de puerta en la lista desplegable.

Tipos de puerta	
Puerta	Puerta estándar con monitor que admite bloqueos y lectores. Requiere un controlador de puerta.
Puerta inalámbrica	Puerta configurable con bloqueos inalámbricos y hubs de comunicación ASSA ABLOY Aperio®. Para obtener más información, consulte <i>Agregar un bloqueo inalámbrico, on page 154</i> .
Puerta de supervisión	Puerta que puede notificar si está abierta o cerrada. Para obtener más información, consulte <i>Agregar una puerta de supervisión, on page 156</i> .
Puerta aprovisionada	Puerta que se puede añadir como marcador de posición en el sistema sin necesidad de seleccionar el hardware.
Planta	Un tipo de puerta para el control de ascensores que autentifica el acceso a las plantas mediante lectores de tarjetas. Para obtener más información, consulte <i>Añadir una planta para el control de ascensores BETA, on page 157</i> .


3. Introduzca un nombre para la puerta y seleccione un controlador de puerta en el menú desplegable **Device (Dispositivo)** para asociarlo a esta. El controlador aparece en gris cuando no se puede agregar otra puerta, cuando está sin conexión o si HTTPS no está activo.
4. Haga clic en **Next (Siguiente)** para ir a la página de configuración de la puerta.
5. En el menú desplegable **Primary lock (Cerradura principal)**, seleccione un puerto de relé.
6. Para configurar dos cerraduras en la puerta, seleccione un puerto de relé del menú desplegable **Secondary lock (Cerradura secundaria)**.
7. Seleccione un perfil de identificación. Vea *Perfiles de identificación, on page 164*.
8. Configure los ajustes de puerta. Consulte *Ajustes de puerta, on page 151*.
9. *Agregar un monitor de puerta, on page 156*
10. *Agregar entrada de emergencia, on page 158*
11. *Agregar un lector, on page 158*
12. *Agregar un dispositivo REX, on page 161*
13. Configure el nivel de seguridad. Vea *Nivel de seguridad de puerta, on page 152*.
14. Haga clic en **Save (Guardar)**.

Copie una configuración de puerta existente para agregar una puerta:


1. Vaya a **Configuration (Configuración) > Access control (Control de acceso) > Doors and zones (Puertas y zonas)**.
2. Haga clic en **+ Add door (Agregar puerta)**.
3. Introduzca un nombre para la puerta y seleccione un controlador de puerta en el menú desplegable **Device (Dispositivo)** para asociarlo a esta.
4. Haga clic en **Next (Siguiente)**.
5. En el menú desplegable **Copy configuration (Copiar configuración)**, seleccione una configuración de puerta existente. Muestra las puertas conectadas y el controlador aparece en gris si se ha configurado con dos puertas o una puerta con dos cerraduras.
6. Cambie los ajustes si lo desea.

- Haga clic en **Save (Guardar)**.

Para editar una puerta:

- vaya a **Configuration > Access control > Doors and zones > Doors (Configuración > Control de acceso > Puertas y zonas > Puertas)**.
- Seleccione una puerta en la lista.
- Haga clic en  **Edit (Modificar)**.
- Cambie los ajustes y haga clic en **Save (Guardar)**.


Para eliminar una puerta:

- vaya a **Configuration > Access control > Doors and zones > Doors (Configuración > Control de acceso > Puertas y zonas > Puertas)**.
- Seleccione una puerta en la lista.
- Haga clic en  **Remove (Eliminar)**.
- Haga clic en **Yes (Sí)**.



Agregar y configurar puertas y zonas

Ajustes de puerta

- Vaya a **Configuration > Access control > Door and Zones (Configuración > Control de acceso > Puerta y zonas)**.
- Seleccione la puerta que desea editar.
- Haga clic en  **Edit (Modificar)**.

Tiempo de acceso (s)	Establece el número de segundos que la puerta permanece desbloqueada una vez se concedió permiso de acceso. La puerta permanece desbloqueada hasta que la puerta se abra o hasta que termine el tiempo establecido. La puerta se bloquea cuando se cierra aunque haya tiempo de acceso.
Open-too-long time (sec) [Tiempo de apertura demasiado largo (s)]	Solo es válido si ha configurado un monitor de puerta. Defina el número de segundos que permanece abierta la puerta. Si la puerta está abierta cuando termina el tiempo establecido, activa la alarma de puerta abierta durante demasiado tiempo. Configure una regla de acción para determinar qué acción activa el evento de puerta abierta durante demasiado tiempo.
Tiempo de acceso largo (seg)	Establece el número de segundos que la puerta permanece desbloqueada una vez se concedió permiso de acceso. El tiempo de acceso largo anula el tiempo de acceso para los titulares de tarjeta que tienen estos ajustes activados.

Long open-too-long time (sec) [Tiempo largo de apertura demasiado larga (s)]	Solo es válido si ha configurado un monitor de puerta. Defina el número de segundos que permanece abierta la puerta. Si la puerta está abierta cuando termina el tiempo establecido, activa el evento de puerta abierta durante demasiado tiempo. El tiempo de apertura demasiado largo sobrescribe el tiempo de apertura demasiado largo ya establecido para los titulares de tarjeta si activa los ajustes de Tiempo de acceso largo .
Tiempo antes de nuevo bloqueo (ms)	Defina el tiempo, en milisegundos, durante el que la puerta debe permanecer desbloqueada después de abrirse o cerrarse.
Volver a bloquear	<ul style="list-style-type: none"> • After opening (Después de abrirse): Solo es válido si ha agregado un monitor de puerta. • After closing (Después de cerrarse): Solo es válido si ha agregado un monitor de puerta.
Puerta forzada	Seleccione si desea que el sistema active una alarma cuando se fuerce una puerta.
Puerta abierta durante demasiado tiempo	Seleccione si desea que el sistema active una alarma cuando una puerta se mantenga abierta demasiado tiempo.

Acciones manuales

Puede realizar las siguientes acciones manuales en puertas y zonas:

Reiniciar – Regresa a las reglas del sistema configuradas.

Autorizar acceso – Desbloquea una puerta o zona durante 7 segundos y vuelve a bloquearla.

Desbloquear – Mantiene la puerta desbloqueada hasta que el usuario la reinicia.

Cerradura – Mantiene la puerta bloqueada hasta que el sistema concede acceso a un titular de tarjeta.

Bloqueo – Nadie entra o sale hasta que el usuario reinicia o desbloquea.

Para realizar una acción manual:

1. Vaya a **Configuration (Configuración) > Access control (Control de acceso) > Doors and zones (Puertas y zonas)**.
2. Seleccione la puerta o zona en la que desea realizar una acción manual.
3. Haga clic en cualquiera de las acciones manuales.

Nivel de seguridad de puerta

Puede agregar las siguientes características de seguridad a la puerta:

Regla de dos personas – La regla de dos personas requiere que dos personas utilicen una credencial válida para acceder.

Doble deslizamiento – El doble deslizamiento permite que un titular de tarjeta invalide el estado actual de una puerta. Por ejemplo, pueden utilizarla para bloquear o desbloquear una puerta fuera de la programación habitual, lo que es más cómodo que entrar en el sistema para desbloquear la puerta. El barrido doble no afecta a una programación ya existente. Por ejemplo, si una puerta se va a bloquear a la hora de cierre y los empleados se van a un receso para el almuerzo, la puerta se seguirá bloqueando según la programación.


Puede configurar el nivel de seguridad mientras agrega una zona puerta o puede hacerlo en una puerta existente.

Para agregar una regla de dos personas a una puerta existente:

1. Vaya a **Configuration (Configuración) > Access control (Control de acceso) > Doors and zones (Puertas y zonas)**.
2. Seleccione la puerta para la que desea configurar un nivel de seguridad.
3. Haga clic en **Edit (Modificar)**.
4. Haga clic en **Security level (Nivel de seguridad)**.
5. Active la regla de dos personas.
6. Haga clic en **Aplicar**.

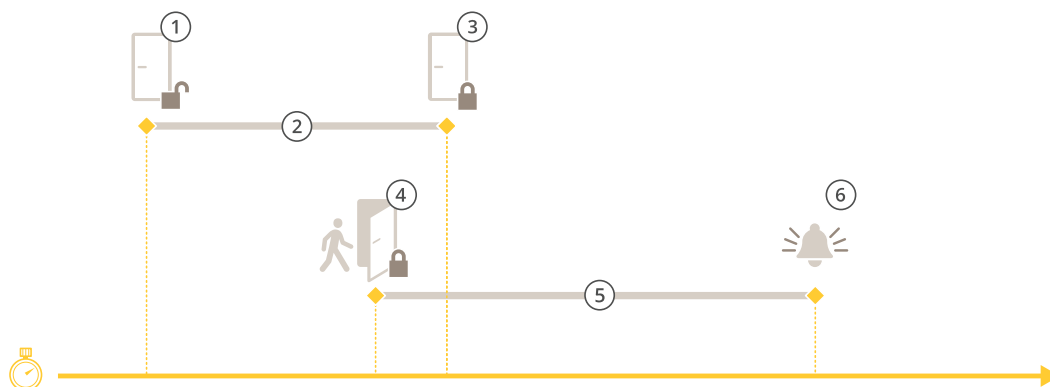
Regla de dos personas	
Lateral A y Lateral B	Seleccione los lados de la puerta en los que utilizar la regla.
Horarios	Seleccione cuándo está activa la regla.
Tiempo de espera (segundos)	El tiempo de espera es el tiempo máximo permitido entre los barridos de tarjeta u otro tipo de credencial válida.

Para añadir un doble deslizamiento a una puerta existente:

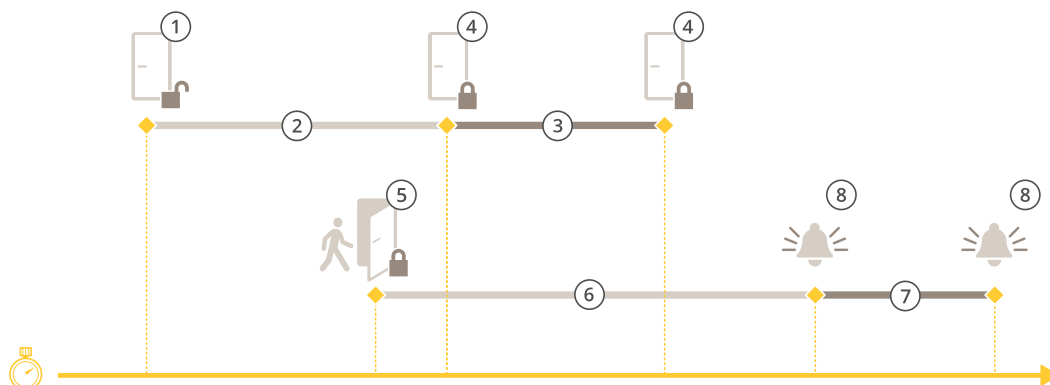
1. Vaya a **Configuration (Configuración) > Access control (Control de acceso) > Doors and zones (Puertas y zonas)**.
2. Seleccione la puerta para la que desea configurar un nivel de seguridad.
3. Haga clic en **Edit (Modificar)**.
4. Haga clic en **Security level (Nivel de seguridad)**.
5. Active el **barrido doble**.
6. Haga clic en **Aplicar**.
7. Aplique un **barrido doble** al titular de la tarjeta.
 - 7.1. Abra una pestaña **Gestión de accesos**.
 - 7.2. Haga clic  en el titular de tarjeta que desee editar y haga clic en **Edit (Editar)**.
 - 7.3. Haga clic en **Más**.
 - 7.4. Seleccione **Allow double-swipe (Permitir doble barrido)**.
 - 7.5. Haga clic en **Aplicar**.

Doble deslizamiento	
Tiempo de espera (segundos)	El tiempo de espera es el tiempo máximo permitido entre los barridos de tarjeta u otro tipo de credencial válida.

Opciones de hora



- 1 Acceso concedido: desbloquea las cerraduras
- 2 Tiempo de acceso
- 3 Ninguna acción realizada: bloquea las cerraduras
- 4 Acción realizada (puerta abierta): bloquea las cerraduras o las mantiene desbloqueadas hasta que se cierre la puerta
- 5 Tiempo de apertura demasiado largo
- 6 La alarma de tiempo de apertura demasiado largo se desactiva




- 1 Acceso concedido: desbloquea las cerraduras
- 2 Tiempo de acceso
- 3 2+3: Tiempo de acceso largo
- 4 Ninguna acción realizada: bloquea las cerraduras
- 5 Acción realizada (puerta abierta): bloquea las cerraduras o las mantiene desbloqueadas hasta que se cierre la puerta
- 6 Tiempo de apertura demasiado largo
- 7 6+7: Tiempo de apertura demasiado largo
- 8 La alarma de tiempo de apertura demasiado largo se desactiva

Agregar un bloqueo inalámbrico

AXIS Camera Station Pro admite los bloqueos inalámbricos de ASSA ABLOY Aperio® y los concentradores de comunicaciones. El bloqueo inalámbrico se conecta al sistema a través de un concentrador de comunicaciones Aperio conectado al conector RS485 del controlador de puerta. Puede conectar 16 bloqueos inalámbricos a un controlador de puerta.



Nota

- La configuración requiere que el controlador de puerta de Axis tenga AXIS OS versión 11.6.16.1 o posterior.
 - La configuración requiere una licencia de extensión de controlador de puerta AXIS válida.
 - La hora en el controlador de puerta Axis y el servidor de AXIS Camera Station Pro debe estar sincronizada.
 - Antes de comenzar, use la aplicación de Aperio compatible con ASSA ABLOY para emparejar los bloqueos Aperio con el concentrador de Aperio.
 - Los bloqueos inalámbricos no seguirán los horarios de desbloqueo cuando esté sin conexión.
1. Acceda al controlador de puerta.
 - 1.1. Vaya a **Configuración > Dispositivos > Otros dispositivos**.
 - 1.2. Abra la interface web del controlador de puerta conectado al concentrador de comunicaciones Aperio.
 2. Active AXIS Door Controller Extension (Extensión de controlador de puerta AXIS).
 - 2.1. En la interface web del controlador de puerta, vaya a **Apps (Aplicaciones)**.
 - 2.2. Abra el menú contextual de AXIS Door Controller Extension .
 - 2.3. Haga clic en **Activate license with a key (Activar licencia con una clave)** y seleccione su licencia.
 - 2.4. Active **AXIS Door Controller Extension (Extensión de controlador de puerta AXIS)**.
 3. Conecte el bloqueo inalámbrico al controlador de puerta a través del concentrador de comunicaciones.
 - 3.1. En la interfaz web del controlador de puerta, vaya a **Access control > Wireless locks (Control de acceso > Bloqueos inalámbricos)**.
 - 3.2. Haga clic en **Connect communication hub (Conectar concentrador de comunicaciones)**.
 - 3.3. Introduzca un nombre para el concentrador y haga clic en **Connect (Conectar)**.
 - 3.4. Haga clic en **Connect wireless lock (Conectar bloqueo inalámbrico)**.
 - 3.5. Seleccione la dirección de bloqueo y las capacidades del bloqueo que desea agregar y haga clic en **Save (Guardar)**.
 4. Agregue y configure la puerta con el bloqueo inalámbrico.
 - 4.1. En AXIS Camera Station Pro, vaya a **Configuration > Access control > Doors and zones (Configuración > Control de acceso > Puertas y zonas)**.
 - 4.2. Haga clic en **+ Add door (Agregar puerta)**.
 - 4.3. Seleccione el controlador de puerta conectado al concentrador de comunicaciones Aperio, seleccione **Wireless door (Puerta inalámbrica)** como **Door type (Tipo de puerta)**.
 - 4.4. Haga clic en **Next (Siguiendo)**.
 - 4.5. Seleccione su **Wireless lock (Bloqueo inalámbrico)**.
 - 4.6. Defina los lados de puerta A y B y agregue sensores. Para obtener más información, vea *Puertas y zonas, on page 147*.
 - 4.7. Haga clic en **Save (Guardar)**.

Una vez que haya conectado el bloqueo inalámbrico, podrá ver el nivel de batería y el estado en la descripción general de las puertas.

Nivel de batería	Acción
Bien	Ninguno
Bajo	El bloqueo funciona según lo esperado, pero debe sustituir la batería antes de que el nivel de batería sea crítico.
Crítico	Cambie la batería. Es posible que el bloqueo no funcione según lo esperado.

Estado de bloqueo	Acción
En línea	Ninguno
Atasco de bloqueo	Solucione cualquier problema mecánico con el bloqueo.

Agregar un monitor de puerta

Un monitor de puerta es un interruptor de posición de puerta que supervisa el estado físico de una puerta. Puede agregar un monitor de puerta a la puerta y configurar cómo conectar el monitor de puerta.

1. Vaya a la página de configuración de la puerta. Vea *Agregar una puerta*, on page 149.
2. En **Sensors (Sensores)**, haga clic en **Add (Agregar)**.
3. Seleccione el **Door monitor sensor (Sensor de monitor de puerta)**.
4. Seleccione el puerto de E/S al que desea conectar el monitor de puerta.
5. En **Door open if (Abrir puerta si)**, seleccione cómo están conectados los circuitos del monitor de puerta.
6. Para ignorar los cambios de estado antes de entrar en un nuevo estado estable, establezca un **Debounce time (Tiempo antirrebote)**.
7. Para activar un evento cuando se produce una interrupción en la conexión entre el controlador de puerta y el monitor de puerta, active **Supervised input (Entrada supervisada)**. Vea *Entradas con supervisión*, on page 163.

Puerta abierta si	
Circuito abierto	El circuito de monitor de puerta está normalmente cerrado. El monitor de puerta envía la señal de una puerta abierta cuando el circuito está abierto. El monitor de puerta envía la señal de una puerta cerrada cuando el circuito está cerrado.
Circuito cerrado	El circuito de monitor de puerta está normalmente abierto. El monitor de puerta envía la señal de una puerta abierta cuando el circuito está cerrado. El monitor de puerta envía la señal de una puerta cerrada cuando el circuito está abierto.

Agregar una puerta de supervisión

Una puerta de supervisión es un tipo de puerta que muestra si está abierto o cerrado. Por ejemplo, puede utilizar esta opción en una puerta de seguridad contra incendios que no requiere un bloqueo pero en la que debe saber si la puerta está abierta.

Una puerta de supervisión es distinta de una puerta regular con un monitor de puerta. Una puerta regular con un monitor de puerta admite bloqueos y lectores, pero requiere un controlador de puerta. Una puerta de supervisión admite un sensor de posición de puerta pero solo requiere un módulo de relé de E/S de red conectado a un controlador de puerta. Puede conectar hasta cinco sensores de posición de puerta a un módulo de relé de E/S de red.

Nota

Una puerta de supervisión requiere un AXIS A9210 Network I/O Relay Module con el firmware más reciente como la aplicación de la ACAP de la puerta de supervisión de AXIS.

Para configurar una puerta de supervisión:

1. Instale AXIS A9210 y actualícelo con la versión más reciente de AXIS OS.
2. Instale los sensores de posición de puerta.
3. En AXIS Camera Station Pro, vaya a **Configuration (Configuración) > Access control (Control de acceso) > Doors and zones (Puertas y zonas)**.
4. Haga clic en **Add door (Agregar puerta)**.
5. Introduzca un nombre.
6. En **Type (Tipo)**, seleccione **Monitoring door (Puerta de supervisión)**.
7. En **Device (Dispositivo)**, seleccione el módulo de relé de E/S de red.
8. Haga clic en **Next (Siguiente)**.
9. En **Sensors (Sensores)**, haga clic en **+ Add (+ Agregar)** y seleccione **Door position sensor (Sensor de posición de puerta)**.
10. Seleccione la E/S que está conectada al sensor de posición de puerta.
11. Haga clic en **Añadir**.

Añadir una planta para el control de ascensores ^{BETA}

Una planta es un tipo de puerta utilizada para controlar el acceso a las plantas del ascensor. Al añadir una planta, se crea un recurso de ascensor que agrupa todas las plantas de ese ascensor. Cada planta utiliza un lector de tarjetas dentro de la cabina del ascensor para autenticar a los usuarios antes de permitir el acceso a dicha planta.

Antes de empezar, necesita:

- Añadir un controlador de puerta de red compatible a su sistema, como *A1610*, *A1710-B* o *A1810-B*.
- Un *A9910 I/O Relay Expansion Module (Módulo de expansión de relés de E/S A9910)* para relés adicionales. Para obtener instrucciones sobre cómo añadir su módulo a un controlador, consulte .

Nota

Esta función está en fase beta y actualmente solo admite hasta 16 plantas y lectores de tarjetas.

Para configurar una planta:

1. Vaya a **Configuration (Configuración) > Access control (Control de acceso) > Doors and zones (Puertas y zonas)**.
2. Haga clic en **Add (Añadir)** y seleccione **Floor (Planta)** ^{BETA}.
3. Introduzca un nombre para la planta.
4. Seleccione su controlador.
5. En **Elevator (Ascensor)**, seleccione un ascensor existente o haga clic en **Create new elevator (Crear nuevo ascensor)** para añadir uno nuevo y, a continuación, introduzca un nombre.
6. En **Side A (Lado A)**, seleccione **Card reader (Lector de tarjetas)** y configure su lector. El **Side B (Lado B)** no se puede configurar por motivos de seguridad.

7. Haga clic en **Save and add new (Guardar y añadir nueva)** para añadir más plantas al mismo ascensor. La configuración del ascensor y del lector se mantiene para la siguiente planta. Tenga en cuenta que esta opción solo estará disponible si su controlador tiene relés disponibles.
8. Haga clic en **Save (Guardar)** una vez que añadida la planta. Las plantas aparecen conforme a la convención "Nombre del ascensor - Nombre de la planta". Por ejemplo: "Lado oeste - Planta 1".

Nota

- Los lectores empleados en varias plantas solo se pueden editar en la primera planta en la que se añadieron.
- Los ascensores se eliminan automáticamente al eliminar todas las plantas relacionadas.

Agregar entrada de emergencia

Puede agregar y configurar una entrada de emergencia para iniciar una acción que bloquee o desbloquee la puerta. También puede configurar cómo conectar el circuito.

1. Vaya a la página de configuración de la puerta. Vea *Agregar una puerta, on page 149*.
2. En **Sensors (Sensores)**, haga clic en **Add (Agregar)**.
3. Seleccione **Emergency input (Entrada de emergencia)**.
4. En **Emergency state (Estado de emergencia)**, seleccione la conexión del circuito.
5. Para ignorar los cambios de estado antes de entrar en un nuevo estado estable, establezca un **Debounce time (ms) [Tiempo antirrebote (ms)]**.
6. Seleccione la **Emergency action (Acción de emergencia)** que se activa cuando la puerta recibe señal de estado de emergencia.

Estado de emergencia	
Circuito abierto	El circuito de entrada de emergencia está normalmente cerrado. La entrada de emergencia envía una señal de estado de emergencia cuando el circuito está abierto.
Circuito cerrado	El circuito de entrada de emergencia está normalmente abierto. La entrada de emergencia envía una señal de estado de emergencia cuando el circuito está cerrado.

Acción de emergencia	
Abrir puerta	La puerta se desbloquea cuando recibe la señal de estado de emergencia.
Cerrar puerta	La puerta se bloquea cuando recibe la señal de estado de emergencia.

Agregar un lector

Puede configurar un controlador de puerta para que admita varios lectores cableados. Puede optar por añadir un lector a uno o a ambos lados de la puerta.

Si aplica una configuración personalizada de formatos de tarjeta o longitud de PIN a un lector, puede verlo en **Card formats (Formatos de tarjeta)** en **Configuration > Access control > Doors and zones (Configuración > Control de acceso > Puertas y zonas)**. Vea *Puertas y zonas, on page 147*.

Nota

- También puede añadir hasta 16 lectores Bluetooth a un controlador de puerta. Para obtener más información, consulte *Añadir un lector Bluetooth*, on page 160.
 - Si utiliza un intercomunicador de red Axis como lector de IP, el sistema utiliza la configuración de PIN establecida en la página web del dispositivo.
1. Vaya a la página de configuración de la puerta. Vea *Agregar una puerta*, on page 149.
 2. En un lado de la puerta, haga clic en **Add (Agregar)**.
 3. Seleccione **Card reader (Lector de tarjetas)**.
 4. Seleccione el **Reader type (Tipo de lector)**.
 5. Para utilizar una configuración de longitud de PIN personalizada para este lector.
 - 5.1. Haga clic en **Avanzado**.
 - 5.2. Active **Custom PIN length (Longitud de PIN personalizada)**.
 - 5.3. Establezca **Min PIN length (Longitud mínima de PIN)**, **Max PIN length (Longitud máxima de PIN)** y **End of PIN character (Carácter final de PIN)**.
 6. Para utilizar un formato de tarjeta personalizado para este lector.
 - 6.1. Haga clic en **Avanzado**.
 - 6.2. Active **Custom card formats (Formatos de tarjeta personalizados)**.
 - 6.3. Seleccione los formatos de tarjeta que desee utilizar para el lector. Si ya se está utilizando un formato de tarjeta con la misma longitud de bits, debe desactivarlo primero. Un icono de advertencia se muestra en el cliente cuando la configuración del formato de tarjeta es distinta de la configuración del sistema configurada.
 7. Haga clic en **Añadir**.
 8. Para agregar un lector al otro lado de la puerta, vuelva a realizar este procedimiento.

Para obtener información sobre cómo instalar un lector de códigos de barras AXIS, consulte *Instalar AXIS Barcode Reader*, on page 172.

Tipo de lector	
OSDP RS485 half-duplex	Para lectores RS485, seleccione OSDP RS485 half duplex (OSDP RS485 half-duplex) y un puerto de lector.
Wiegand	Para lectores que utilizan protocolos Wiegand, seleccione Wiegand (Wiegand) y un puerto de lector.
Lector de IP	En el caso de lectores de IP, seleccione IP reader (Lector de IP) y seleccione un dispositivo del menú desplegable. Para obtener información sobre los requisitos y los dispositivos compatibles, consulte .

Wiegand	
Control de LED	Seleccione Single wire (Cable simple) o Cable dual (R/G) . Los lectores con control de led dual utilizan diferentes cables para los LED rojo y verde.
Alerta de manipulación	Seleccione si la entrada de manipulación del lector está activa. <ul style="list-style-type: none"> • Open circuit (Circuito abierto): El lector envía la señal de manipulación de puerta cuando el circuito está abierto.

	<ul style="list-style-type: none"> • Circuito cerrado: El lector envía la señal de manipulación de puerta cuando el circuito está cerrado.
Tiempo de rebote de manipulación	Para ignorar los cambios de estado de la entrada de manipulación del lector antes de que entre en un nuevo estado estable, defina un Tamper debounce time (Tiempo antirrebote en manipulación) .
Entrada supervisada	Active para desencadenar un evento cuando se interrumpe la conexión entre el controlador de puerta y el lector. Vea <i>Entradas con supervisión, on page 163</i> .

Añadir un lector Bluetooth

Puede utilizar el AXIS A4612 Network Bluetooth Reader para ampliar los límites de puertas cableadas de los controladores de puertas Axis, que permiten asignar hasta 16 de estos lectores a su propia puerta. Cada lector puede gestionar la cerradura de la puerta, la solicitud de salida (REX) y el interruptor de posición de la puerta (DPS).

Añadir y utilizar estos lectores no requiere ninguna licencia adicional.

Para añadir un AXIS A4612 Network Bluetooth Reader a una puerta:

1. Asegúrese de haber emparejado el AXIS A4612 con el controlador de puerta. Consulte *Utilice la aplicación AXIS Mobile Credential como credencial Bluetooth, on page 160*.
2. Vaya a la página de configuración de la puerta. Consulte *Agregar una puerta, on page 149*.
3. En uno de los lados de la puerta, haga clic en **Add (Añadir)** y, a continuación, en **Card reader (Lector de tarjetas)**.
4. Seleccione **IP reader (Lector IP)** y elija el AXIS A4612 emparejado en el menú desplegable. Si desea utilizar este lector para emparejar credenciales, márkelo para emparejamiento. Haga clic en **Añadir**.
5. En la pestaña **Overview (Descripción general)**, modifique el perfil de identificación. Puede utilizar los perfiles **Tap in app (Tocar la aplicación)** o **Touch reader (Tocar el lector)** si solo tiene el AXIS A4612 conectado a un lado de la puerta y utiliza un REX en el otro.

Utilice la aplicación AXIS Mobile Credential como credencial Bluetooth

En este ejemplo se muestra cómo agregar un AXIS A4612 Bluetooth Reader a nuestro sistema para permitir que los titulares de tarjetas desbloqueen las puertas mediante la aplicación móvil de AXIS Mobile Credential.

1. Instale el lector de Bluetooth y conéctelo a una controlador de puerta.
2. Agregue el lector Bluetooth al controlador de puerta de la interfaz web.
 - 2.1. Acceda al controlador de puerta y vaya a **Peripherals (Periféricos) > Readers (Lectores)**.
 - 2.2. Haga clic en **Add reader (Agregar lector)**.
 - 2.3. Introduzca la información necesaria en el cuadro de diálogo **Add Bluetooth reader (Agregar lector de Bluetooth)**.
 - 2.4. Haga clic en **Añadir**.
3. Agregue el lector de Bluetooth a una puerta en AXIS Camera Station Pro.
 - 3.1. Vaya a **Configuration (Configuración) > Access control (Control de acceso) > Doors and zones (Puertas y zonas)**.
 - 3.2. Seleccione la puerta que desea agregar al lector de Bluetooth y haga clic en **Edit (Editar)**.
 - 3.3. Haga clic en **+ Add (+ Agregar)** en el lado de la puerta donde está ubicado el lector de Bluetooth.

- 3.4. Seleccione **Card reader (Lector de tarjetas)**.
- 3.5. En **Add IP reader (Agregar lector de IP)**, seleccione **IP reader (Lector de IP)**.
- 3.6. En **Select IP reader (Seleccionar lector de IP)**, seleccione el lector de Bluetooth.
- 3.7. Haga clic en **Añadir**.
4. Seleccione un lector de Bluetooth para el emparejamiento. Debe hacerlo para al menos un lector de Bluetooth en el sistema.
 - 4.1. Seleccione el lector de Bluetooth que acaba de agregar.
 - 4.2. Haga clic en **Edit (Modificar)**.
 - 4.3. En **Edit bluetooth reader (Editar lector de Bluetooth)**, seleccione **Use this reader for pairing (Usar este lector para emparejamiento)**.
 - 4.4. Haga clic en **Aplicar**.
5. Elija el perfil de identificación **Tap in app (Tocar la aplicación)** o **Touch reader (Tocar el lector)**. Consulte *Perfiles de identificación, on page 164* para obtener más información.
6. Agregue la credencial móvil al titular de la tarjeta. Vea *Agregar credenciales, on page 184*.
7. Empareje la credencial móvil con el lector de emparejamiento.
 - 7.1. Lleve el teléfono móvil del titular de la tarjeta al lector de Bluetooth habilitado emparejado.
 - 7.2. Siga las instrucciones proporcionadas en el correo electrónico enviado al titular de la tarjeta.

Agregar un dispositivo REX

Puede seleccionar agregar una solicitud al dispositivo de solicitud de salida (REX) en un lado o a ambos lados de la puerta. Un dispositivo REX puede ser un sensor PIR, un botón REX o una barra pulsadora.

1. Vaya a la página de configuración de la puerta. Vea *Agregar una puerta, on page 149*.
2. En un lado de la puerta, haga clic en **Add (Agregar)**.
3. Seleccione **dispositivo de solicitud de salida (REX)**.
4. Seleccione el puerto de E/S en el que desea conectar el dispositivo REX. Si solo hay un puerto disponible, se seleccionará automáticamente.
5. Seleccione qué **Action (Acción)** activar cuando la puerta recibe la señal REX.
6. En **REX active (REX activo)**, seleccione la conexión de circuito de monitor de puerta.
7. Para ignorar los cambios de estado antes de entrar en un nuevo estado estable, establezca un **Debounce time (ms) [Tiempo antirrebote (ms)]**.
8. Para activar un evento cuando se produce una interrupción en la conexión entre el controlador de puerta y el dispositivo de solicitud de salida (REX), active **Supervised input (Entrada supervisada)**. Vea *Entradas con supervisión, on page 163*.

Acción	
Abrir puerta	Seleccione para desbloquear la puerta cuando recibe la señal REX.
Ninguno	Seleccione si no desea activar ninguna acción cuando la puerta recibe la señal REX.

REX activo:	
Circuito abierto	Seleccione si el circuito REX está normalmente cerrado. El dispositivo de solicitud de salida (REX) envía la señal cuando el circuito esté abierto.
Circuito cerrado	Seleccione si el circuito REX está normalmente abierto. El dispositivo de solicitud de salida (REX) envía la señal cuando el circuito se cierra.


Agregar una zona

Una zona es un área física específica con un grupo de puertas. Puede crear zonas y agregar puertas a las zonas. Existen dos tipos de puertas:


- **Perimeter door (Puerta de perímetro):** Los titulares de tarjeta entran o salen de la zona por esta puerta.
- **Internal door (Puerta interna):** Una puerta interna dentro de la zona.

Nota


Una puerta perimetral puede pertenecer a dos zonas. Una puerta interna solo puede pertenecer a una zona.

1. vaya a **Configuration > Access control > Doors and zones > Zones (Configuración > Control de acceso > Puertas y zonas > Zonas)**.
2. Haga clic en  **Add zone (Agregar zona)**.
3. Escriba un nombre de zona.
4. Haga clic en **Add door (Agregar puerta)**.
5. Seleccione las puertas que desee agregar a la zona y haga clic en **Add (Agregar)**.
6. De forma predeterminada, la puerta se establece como puerta perimetral. Para cambiarlo, seleccione **Internal door (Puerta interna)** en el menú desplegable.
7. De forma predeterminada, una puerta perimetral utiliza el lado A de la puerta como entrada a la zona. Para cambiarlo, seleccione **Leave (Abandonar)** en el menú desplegable.
8. Para eliminar una puerta de la zona, selecciónela y haga clic en **Remove (Eliminar)**.
9. Haga clic en **Save (Guardar)**.

Para editar una zona:

1. vaya a **Configuration > Access control > Doors and zones > Zones (Configuración > Control de acceso > Puertas y zonas > Zonas)**.
2. Seleccione una zona en la lista.
3. Haga clic en  **Edit (Modificar)**.
4. Cambie los ajustes y haga clic en **Save (Guardar)**.

Para eliminar una zona:

1. vaya a **Configuration > Access control > Doors and zones > Zones (Configuración > Control de acceso > Puertas y zonas > Zonas)**.
2. Seleccione una zona en la lista.
3. Haga clic en  **Remove (Eliminar)**.
4. Haga clic en **Yes (Sí)**.

Nivel de seguridad de zona

Puede agregar la siguiente característica de seguridad a una zona:

Protección contra dobles entradas – Impide que los usuarios utilicen las mismas credenciales que otra persona que ha entrado en una zona antes. Es obligatorio que una persona salga de la zona antes de sus credenciales se puedan volver a usar.

Nota

- Con antipassback, recomendamos el uso de sensores de posición de puerta en todas las puertas de la zona para asegurarse de el sistema pueda registrar que un usuario la ha abierto tras haber pasado la tarjeta.
- Si un controlador de puerta no tiene conexión, anti passback funciona siempre que todas las puertas de la zona pertenezcan al mismo controlador de puerta. No obstante, si las puertas de la zona pertenecen a distintos controladores de puerta sin conexión, anti passback deja de funcionar.

Puede configurar el nivel de seguridad mientras agrega una zona nueva o puede hacerlo en una zona existente. Para agregar un nivel de seguridad a una zona existente:

1. Vaya a **Configuration (Configuración) > Access control (Control de acceso) > Doors and zones (Puertas y zonas)**.
2. Seleccione la zona para la que desea configurar el nivel de seguridad.
3. Haga clic en **Edit (Modificar)**.
4. Haga clic en **Security level (Nivel de seguridad)**.
5. Active las características de seguridad que desee agregar a la puerta.
6. Haga clic en **Aplicar**.

Protección contra dobles entradas	
Solo registro de infracciones (suave)	Utilice esta opción si desea permitir que una segunda persona entre por la puerta con las mismas credenciales que la primera persona. Esta opción solo genera una alarma del sistema.
Denegar acceso (exigente)	Utilice esta opción si desea evitar que el segundo usuario entre por la puerta si utiliza las mismas credenciales que la primera persona. Esta opción también genera una alarma del sistema.
Tiempo de espera (segundos)	El tiempo que se debe esperar hasta que el sistema permita la entrada de nuevo de un usuario. Introduzca 0 si no desea que se agote el tiempo de espera, lo que significa que la zona tiene antipassback hasta que el usuario sale de la zona. Utilice solo 0 tiempo de espera con Denegar acceso (exigente) si todas las puertas de la zona tienen lectores en ambos lados.

Entradas con supervisión

Las entradas supervisadas pueden activar un evento cuando se interrumpe la conexión con un controlador de puerta.

- Conexión entre el controlador de puerta y el monitor de puerta. Vea *Agregar un monitor de puerta, on page 156*.
- Conexión entre el controlador de puerta y el lector que utiliza protocolos Wiegand. Vea *Agregar un lector, on page 158*.
- Conexión entre el controlador de puerta y el dispositivo REX. Vea *Agregar un dispositivo REX, on page 161*.

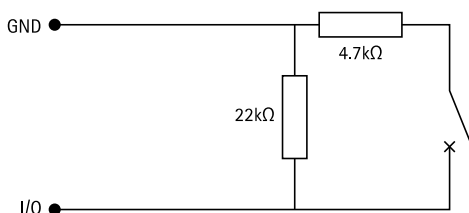
Para utilizar entradas supervisadas:

1. Instale las resistencias de final de línea lo más cerca posible del dispositivo periférico según el diagrama de conexión.
2. Vaya a la página de configuración de un lector, un monitor de puerta o un dispositivo de solicitud de salida (REX), active **Supervised input (Entrada supervisada)**.
3. Si ha seguido el diagrama de primera conexión en paralelo, seleccione **Parallel first connection with a 22 K Ω parallel resistor and a 4.7 K Ω serial resistor (Primera conexión en paralelo con una resistencia de 22 K Ω en paralelo y una resistencia de 4,7 K Ω en serie)**.
4. Si ha seguido el diagrama de primera conexión en serie, seleccione **Serial first connection (Primera conexión en serie)** y seleccione los valores de la resistencia en el menú desplegable **Resistor values (Valores de resistencia)**.

Diagramas de conexión

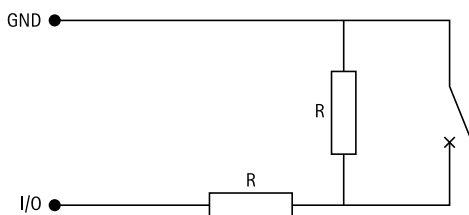
Parallel first connection (Primera conexión en paralelo)

Los valores de la resistencia deben ser de 4,7 K Ω y 22 K Ω .



Primera conexión en serie

Los valores de las resistencias deben ser iguales y situarse en el rango 1-10 K Ω .



Perfiles de identificación

Un perfil de identificación es una combinación de tipos de identificación y programaciones. Puede aplicar un perfil de identificación a una o más puertas para definir cómo y cuándo puede acceder un titular de tarjeta a una puerta.

Los tipos de identificación son portadores de la información de la credencial necesaria para acceder a una puerta. Los tipos de identificación comunes son tokens, números de identificación personal (PIN), huellas, mapas faciales y dispositivos de solicitud de salida (REX). Un tipo de identificación puede tener uno o más tipos de información.

Tipos de identificación compatibles: Tarjeta, PIN, REX, QR estático y QR dinámico.

Nota

Debe utilizar el QR dinámico y el PIN juntos.

Vaya a **Configuration > Access control > Identification profiles (Configuración > Control de acceso > Perfiles de identificación)** para crear, editar o eliminar perfiles de identificación.

Hay cinco perfiles de identificación predeterminados disponibles para su uso tal y como están o editar según sea necesario.

Tarjeta – Los titulares de tarjeta deben pasar la tarjeta para acceder a la puerta.

Tarjeta y PIN – Los titulares de tarjeta deben pasar la tarjeta e introducir el PIN para acceder a la puerta.

Número de identificación personal (PIN) – Los titulares de tarjeta deben introducir el PIN para acceder a la puerta.

Tarjeta o PIN – Los titulares de tarjeta deben pasar la tarjeta o introducir el PIN para acceder a la puerta.

QR – Los titulares de tarjeta deben mostrar el código QR® a la cámara para acceder a la puerta. Puede usar el perfil de identificación QR para el QR estático y para el QR dinámico.

Matrícula – Los titulares de tarjeta deben conducir hacia la cámara en un vehículo con una matrícula aprobada.

Tocar la aplicación – Los titulares de tarjeta deben tocar la credencial en la aplicación móvil de AXIS Camera Station mientras se encuentra en el rango del lector de Bluetooth.


Tocar el lector – Los titulares de tarjeta deben tocar el lector Bluetooth mientras llevan un teléfono móvil con una credencial móvil.

QR Code es una marca comercial registrada de DensoWave Incorporated en Japón y otros países.


Para crear perfil de identificación:

1. Vaya a **Configuration > Access control > Identification profiles (Configuración > Control de acceso > Perfiles de identificación)**.
2. Haga clic en **Create identification profile (Crear perfil de identificación)**.
3. Introduzca un nombre de perfil de identificación.
4. Seleccione **Include facility code for card validation (Incluir código de instalación para la validación de la tarjeta)** para usar el código de instalación como uno de los campos de validación de credenciales. Este campo solo está disponible si ha activado **Facility code (Código de instalación)** en **Access management > Settings (Gestión de acceso > Ajustes)**.
5. Configure el perfil de identificación para un lado de la puerta.
6. En el otro lado de la puerta, realice de nuevo los pasos anteriores.
7. Haga clic en **OK**.

Para editar un perfil de identificación:

1. Vaya a **Configuration > Access control > Identification profiles (Configuración > Control de acceso > Perfiles de identificación)**.
2. Seleccione un perfil de identificación y haga clic en .
3. Para cambiar el nombre del perfil de identificación, introduzca un nuevo nombre.
4. Realice los cambios en el lateral de la puerta.
5. Para editar el perfil de identificación en el otro lado de la puerta, realice de nuevo los pasos anteriores.
6. Haga clic en **OK**.

Para eliminar un perfil de identificación:

1. Vaya a **Configuration > Access control > Identification profiles (Configuración > Control de acceso > Perfiles de identificación)**.
2. Seleccione un perfil de identificación y haga clic en .
3. Si se ha usado el perfil de identificación en una puerta, seleccione otro perfil de identificación para la puerta.
4. Haga clic en **OK**.

Editar perfil de identificación	
×	Para eliminar un tipo de identificación y la correspondiente programación.

Tipo de identificación	Para cambiar un tipo de identificación, seleccione uno o varios tipos en el menú desplegable Identification type (Tipo de identificación) .
Horario	Para cambiar una programación, seleccione una o varias programaciones en el menú desplegable Schedule (Programación) .
+ Agregar	Agregue un tipo de identificación y la correspondiente programación, haga clic en Add (Agregar) y establezca los tipos de identificación y las programaciones.



Establecer perfiles de identificación

Crear un perfil de identificación


1. Vaya a **Configuration > Access control > Identification profiles (Configuración > Control de acceso > Perfiles de identificación)**.
2. Haga clic en **Create identification profile (Crear perfil de identificación)**.
3. Introduzca un nombre para el perfil de identificación.
4. Seleccione **Include facility code for card validation (Incluir código de instalación para la validación de la tarjeta)** para usar el código de instalación como uno de los campos de validación de credenciales. Este campo solo está disponible si ha activado **Facility code (Código de instalación)** en **Access management > Settings (Gestión de acceso > Ajustes)**.
5. Para el Lado A, haga clic en **+ Add (Añadir)**, seleccione un tipo de identificación y una programación.
 - Para exigir a los titulares de tarjetas que utilicen más de un tipo de identificación, seleccione varios tipos en la misma fila.
 - Para permitir que los titulares de tarjetas utilicen cualquiera de los dos tipos, vuelva a hacer clic en **+ Add (Añadir)** y añada otra fila.
6. Para el Lado B, haga clic en **+ Add (Añadir)**, seleccione un tipo de identificación y una programación.
7. Haga clic en **OK**.





Establecer perfiles de identificación


Editar un perfil de identificación

1. Vaya a **Configuration > Access control > Identification profiles (Configuración > Control de acceso > Perfiles de identificación)**.


2. Seleccione un perfil de identificación y haga clic en .
3. Para cambiar el nombre del perfil de identificación, introduzca un nuevo nombre.
4. Realice los cambios en el lateral de la puerta.
5. Para editar el perfil de identificación en el otro lado de la puerta, realice de nuevo los pasos anteriores.
6. Haga clic en OK.

Editar perfil de identificación	
	Para eliminar un tipo de identificación y la correspondiente programación.
Tipo de identificación	Para cambiar un tipo de identificación, seleccione uno o varios tipos en el menú desplegable Identification type (Tipo de identificación) .
Horario	Para cambiar una programación, seleccione una o varias programaciones en el menú desplegable Schedule (Programación) .
 Agregar	Agregue un tipo de identificación y la correspondiente programación, haga clic en Add (Agregar) y establezca los tipos de identificación y las programaciones.

Eliminar un perfil de identificación

1. Vaya a **Configuration > Access control > Identification profiles (Configuración > Control de acceso > Perfiles de identificación)**.
2. Seleccione un perfil de identificación y haga clic en .
3. Si se ha usado el perfil de identificación en una puerta, seleccione otro perfil de identificación para la puerta.
4. Haga clic en OK.

Restablecer un formato de tarjeta predefinido

1. Vaya a **Configuration > Access Control > Card formats and PIN (Configuración > Control de acceso > Formatos de tarjeta y PIN)**.
2. Haga clic en  para restablecer un formato de tarjeta al mapa de campos predeterminado.

Formatos de tarjeta y PIN

Un formato de tarjeta define cómo una tarjeta almacena datos. Es una tabla de traducción entre los datos entrantes y los datos validados en el sistema. Cada formato de tarjeta incluye un conjunto de reglas diferentes para cómo organizar la información almacenada. Al definir un formato de tarjeta, se indica al sistema cómo se debe interpretar la información que el controlador recibe del lector de tarjeta.

Hay formatos de tarjeta de uso común predefinidos disponibles para que los utilice tal como están o los edite según sea necesario. También se pueden crear formatos de tarjeta personalizados.

Vaya a **Configuration > Access Control > Card formats and PIN (Configuración > Control de acceso > Formatos de tarjeta y PIN)** para crear, editar o activar formatos de tarjeta. También puede configurar el PIN.

Los formatos de tarjeta personalizados pueden contener los siguientes campos de datos utilizados para la validación de credenciales.

Número de tarjeta – Un subconjunto de los datos binarios de credenciales codificados como números decimales o hexadecimales. Use el número de tarjeta para identificar una tarjeta o titular de tarjeta específico.

Código de instalación – Un subconjunto de los datos binarios de credenciales codificados como números decimales o hexadecimales. Use el código de instalación para identificar a un cliente final o instalación específicos.

Para crear un formato de tarjeta:


1. Vaya a **Configuration > Access Control > Card formats and PIN (Configuración > Control de acceso > Formatos de tarjeta y PIN)**.
2. Haga clic en **Add card format (Añadir formato de tarjeta)**.
3. Introduzca un nombre de formato de tarjeta.
4. En el campo de **Bit length (Longitud de bits)**, escriba una longitud de bits entre 1 y 256.
5. Seleccione **Invert bit order (Invertir orden de bits)** si desea invertir el orden de bits de los datos recibidos desde el lector de tarjetas.
6. Seleccione **Invert byte order (Invertir orden de bytes)** si desea invertir el orden de bytes de los datos recibidos del lector de tarjetas. Esta opción solo está disponible si se especifica una longitud de bits que pueda dividir por ocho.
7. Seleccione y configure los campos de datos para que se activen en el formato de tarjeta. El **Card number (Número de tarjeta)** o el **Facility code (Código de instalación)** deben estar activos en el formato de tarjeta.
8. Haga clic en **OK**.
9. Para activar el formato de tarjeta, seleccione la casilla delante del nombre del formato de tarjeta.

Nota


- No pueden estar activos simultáneamente dos formatos de tarjeta con la misma longitud de bits. Por ejemplo, si ha definido dos formatos de tarjeta de 32 bits, solo podrá activar uno de ellos. Desactive el formato de tarjeta para activar el otro.
- Solo se pueden activar y desactivar formatos de tarjeta si el controlador de puerta se ha configurado con al menos un lector.

i	Haga clic en i para ver un ejemplo de la salida después de invertir el orden de bits.
Gama	Defina el rango de bits de los datos para el campo de datos. El intervalo debe estar dentro de lo especificado para Bit length (Longitud de bits) .
Formato de salida	<p>Seleccione el formato de salida de los datos para el campo de datos.</p> <p>Decimal: También conocido como sistema numeral posicional base 10, consta de los números 0-9.</p> <p>Hexadecimal: también conocido como sistema numérico posicional de base 16, consta de 16 símbolos únicos: los números 0-9 y las letras a-f.</p>
Orden de bits del subrango	<p>Seleccione el orden de bits.</p> <p>Little endian: El primer bit es el más pequeño (el menos significativo).</p> <p>Big endian: El primer bit es el más grande (el más significativo).</p>


Para editar un formato de tarjeta:

1. Vaya a **Configuration > Access Control > Card formats and PIN** (Configuración > Control de acceso > Formatos de tarjeta y PIN).
2. Seleccione un formato de tarjeta y haga clic en .
3. Si edita un formato de tarjeta predefinido, solo puede editar **Invert bit order** (Invertir orden de bits) e **Invert byte order** (Invertir orden de bytes).
4. Haga clic en **OK**.


Solo puede eliminar los formatos de tarjeta personalizados. Para eliminar un formato de tarjeta personalizado:

1. Vaya a **Configuration > Access Control > Card formats and PIN** (Configuración > Control de acceso > Formatos de tarjeta y PIN).
2. Seleccione un formato de tarjeta personalizado, haga clic en  y en **Yes (Sí)**.

Para restablecer un formato de tarjeta predefinido:

1. Vaya a **Configuration > Access Control > Card formats and PIN** (Configuración > Control de acceso > Formatos de tarjeta y PIN).
2. Haga clic en  para restablecer un formato de tarjeta al mapa de campos predeterminado.


Para configurar la longitud de PIN:

1. Vaya a **Configuration > Access Control > Card formats and PIN** (Configuración > Control de acceso > Formatos de tarjeta y PIN).
2. En **PIN configuration** (Configuración de PIN), haga clic en .
3. Especifique **Min PIN length** (Longitud mínima de PIN), **Max PIN length** (Longitud máxima de PIN) y **End of PIN character** (Carácter final de PIN).
4. Haga clic en **OK**.



Configurar formatos de tarjeta

Configuración de PIN

1. Vaya a **Configuration > Access Control > Card formats and PIN** (Configuración > Control de acceso > Formatos de tarjeta y PIN).
2. En **PIN configuration** (Configuración de PIN), haga clic en .
3. Especifique **Min PIN length** (Longitud mínima de PIN), **Max PIN length** (Longitud máxima de PIN) y **End of PIN character** (Carácter final de PIN).
4. Haga clic en **OK**.

Crear un formato de tarjeta

1. Vaya a **Configuration > Access Control > Card formats and PIN** (Configuración > Control de acceso > Formatos de tarjeta y PIN).
2. Haga clic en **Add card format** (Añadir formato de tarjeta).

3. Introduzca un nombre de formato de tarjeta.
4. En el campo de **Bit length (Longitud de bits)**, escriba una longitud de bits entre 1 y 256.
5. Seleccione **Invert bit order (Invertir orden de bits)** si desea invertir el orden de bits de los datos recibidos desde el lector de tarjetas.
6. Seleccione **Invert byte order (Invertir orden de bytes)** si desea invertir el orden de bytes de los datos recibidos del lector de tarjetas. Esta opción solo está disponible si se especifica una longitud de bits que pueda dividir por ocho.
7. Seleccione y configure los campos de datos para que se activen en el formato de tarjeta. El **Card number (Número de tarjeta)** o el **Facility code (Código de instalación)** deben estar activos en el formato de tarjeta.
8. Haga clic en **OK**.
9. Para activar el formato de tarjeta, seleccione la casilla delante del nombre del formato de tarjeta.


Nota

- No pueden estar activos simultáneamente dos formatos de tarjeta con la misma longitud de bits. Por ejemplo, si ha definido dos formatos de tarjeta de 32 bits, solo podrá activar uno de ellos. Desactive el formato de tarjeta para activar el otro.
- Solo se pueden activar y desactivar formatos de tarjeta si el controlador de puerta se ha configurado con al menos un lector.
- Los formatos de tarjeta predefinidos se pueden editar, pero no eliminar. Para deshacer cualquier cambio realizado en un formato predefinido, haga clic en el icono de reinicio para restablecer su configuración predeterminada. Podrá eliminar los formatos de tarjeta que haya creado.


ⓘ	Haga clic en ⓘ para ver un ejemplo de la salida después de invertir el orden de bits.
Gama	Defina el rango de bits de los datos para el campo de datos. El intervalo debe estar dentro de lo especificado para Bit length (Longitud de bits) .
Formato de salida	<p>Seleccione el formato de salida de los datos para el campo de datos.</p> <p>Decimal: También conocido como sistema numeral posicional base 10, consta de los números 0-9.</p> <p>Hexadecimal: también conocido como sistema numérico posicional de base 16, consta de 16 símbolos únicos: los números 0-9 y las letras a-f.</p>
Orden de bits del subrango	<p>Seleccione el orden de bits.</p> <p>Little endian: El primer bit es el más pequeño (el menos significativo).</p> <p>Big endian: El primer bit es el más grande (el más significativo).</p>



Editar un formato de tarjeta

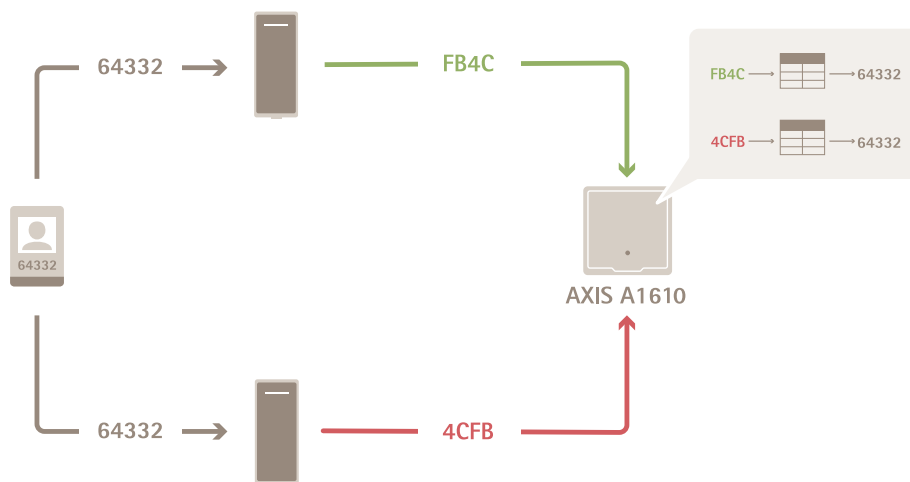
1. Vaya a Configuration > Access Control > Card formats and PIN (Configuración > Control de acceso > Formatos de tarjeta y PIN).
2. Seleccione un formato de tarjeta y haga clic en .
3. Si edita un formato de tarjeta predefinido, solo puede editar Invert bit order (Invertir orden de bits) e Invert byte order (Invertir orden de bytes).
4. Haga clic en OK.

Solo puede eliminar los formatos de tarjeta personalizados. Para eliminar un formato de tarjeta personalizado:

1. Vaya a Configuration > Access Control > Card formats and PIN (Configuración > Control de acceso > Formatos de tarjeta y PIN).
2. Seleccione un formato de tarjeta personalizado, haga clic en  y en Yes (Si).

Configuración del formato de tarjeta

Descripción general



- El número de tarjeta en decimal es 64332.
- Un lector transfiere el número de tarjeta al número hexadecimal FB4C. El otro lector lo transfiere al número hexadecimal 4CFB.
- AXIS A1610 Network Door Controller recibe FB4C y lo transfiere al número decimal 64332 de acuerdo con los ajustes de formato de tarjeta en el lector.
- AXIS A1610 Network Door Controller recibe 4CFB, lo convierte en FB4C invirtiendo el orden de bytes y lo transfiere al número decimal 64332 de acuerdo con los ajustes de formato de tarjeta en el lector.

Invertir orden de bits

Después de invertir el orden de bits, los datos de la tarjeta que recibe el lector se leen de derecha a izquierda, bit a bit.

$$64332 = 1111\ 1011\ 0100\ 1100 \longrightarrow 0011\ 0010\ 1101\ 1111 = 13023$$

→ Read from left
Read from right ←

Invertir orden de bytes

Un grupo de ocho bits es un byte. Después de invertir el orden de bytes, los datos de la tarjeta que recibe el lector se leen de derecha a izquierda, byte a byte.

$$64\ 332 = \begin{matrix} 1111 & 1011 & 0100 & 1100 \\ \text{F} & \text{B} & 4 & \text{C} \end{matrix} \longrightarrow \begin{matrix} 0100 & 1100 & 1111 & 1011 \\ 4 & \text{C} & \text{F} & \text{B} \end{matrix} = 19707$$

Formato de tarjeta Wiegand estándar de 26 bits



- 1 Paridad líder
- 2 Código de instalación
- 3 Número de tarjeta
- 4 Paridad de cola

Comunicación cifrada

Canal seguro OSDP

AXIS Camera Station Secure Entry admite el canal seguro OSDP (Protocolo abierto de dispositivos supervisados) para activar el cifrado de la línea entre el controlador y los lectores de Axis.

Para activar OSDP Secure Channel en todo un sistema:

1. Vaya a **Configuration > Access control > Encrypted communication (Configuración > Control de acceso > Comunicación cifrada)**.
2. Introduzca la clave de cifrado principal y haga clic en **OK (Aceptar)**.
3. Active **OSDP Secure Channel (Canal seguro OSDP)**. Esta opción solo está disponible una vez que haya introducido la clave de cifrado principal.
4. De forma predeterminada, la clave de cifrado principal genera una clave de canal seguro OSDP. Para configurar manualmente la clave de canal seguro OSDP:
 - 4.1. En **OSDP Secure Channel (Canal seguro OSDP)**, haga clic en .
 - 4.2. Elimine **Use main encryption key to generate OSDP Secure Channel key (Utilice la clave de cifrado principal para generar la clave de canal seguro OSDP)**.
 - 4.3. Introduzca la clave de canal seguro OSDP y haga clic en **OK (Aceptar)**.

Para encender o apagar el canal seguro OSDP para un lector específico, consulte *Doors and zones (Puertas y zonas)*.

AXIS Barcode Reader


AXIS Barcode Reader es una aplicación que se puede instalar en cámaras Axis. La controladora de acceso Axis utiliza la clave de autenticación de periféricos externos para otorgar acceso y autenticar el AXIS Barcode Reader y el AXIS License Plate Verifier.

Instalar AXIS Barcode Reader

1. Descargue el archivo de instalación de la aplicación de *axis.com*.
2. Vaya a la página web de su intercomunicador o cámara Axis.

3. Instale la aplicación.
4. Active la licencia.
5. Inicie la aplicación.
6. Recomendamos cambiar el siguiente ajuste de la cámara para obtener una precisión QR mejor.
 - 6.1. Vaya a los ajustes de la cámara.
 - 6.2. En **Image > Exposure (Imagen > Exposición)**, mueva el control **Blur-noise trade-off (Compensación de desenfoque-ruido)** hacia el centro.

Configurar AXIS Barcode Reader

1. Para cambiar el perfil de identificación QR, vaya a **Configuration (Configuración) > Access control (Control de acceso) > Identification profiles (Perfiles de identificación)** y haga clic en . Consulte *Perfiles de identificación*.
2. Agregar una puerta. Consulte *Agregar una puerta*.
3. Seleccione **QR** como perfil de identificación de esta puerta. Consulte *Ajustes de puerta*.
4. Agregue un lector de códigos de barras. Consulte *Agregar un lector*.
 - 4.1. Bajo un lado de la puerta, haga clic en **Add reader (Agregar lector)**.
 - 4.2. Seleccione **AXIS Barcode Reader (Lector de códigos de barras de AXIS)** en la lista desplegable **Reader type (Tipo de lector)**. Introduzca un nombre y haga clic en **OK (Aceptar)**.

Crear una conexión con un controlador de puerta

1. En AXIS Camera Station Pro:
 - 1.1. Vaya a **Configuration > Access control > Encrypted communication (Configuración > Control de acceso > Comunicación cifrada)**.
 - 1.2. En **External Peripheral Authentication Key (Clave de autenticación periférica externa)**, haga clic en **Show authentication key (Mostrar clave de autenticación)** y **Copy key (Copiar clave)**.
2. En la interfaz web del dispositivo en la que se ejecuta AXIS Barcode Reader:
 - 2.1. Abra la aplicación AXIS Barcode Reader.
 - 2.2. Si el certificado del servidor no se configuró en AXIS Camera Station Pro, encienda **Ignore server certificate validation (Ignorar la validación del certificado del servidor)**. Consulte *Certificados* para obtener más información.
 - 2.3. Active **AXIS Camera Station Secure Entry**.
 - 2.4. Haga clic en **Add (Agregar)**, introduzca la dirección IP del controlador de puerta y pegue la clave de autenticación.
 - 2.5. Seleccione el lector que lee códigos de barras del menú desplegable de la puerta.

BETA de varios servidores

Los servidores secundarios conectados pueden, con varios servidores, usar los titulares de tarjeta globales y grupos de titulares de tarjeta del servidor principal.

Nota

- Un sistema puede admitir hasta 64 subservidores.
- Requiere AXIS Camera Station 5.47 o posterior.
- Requiere que el servidor principal y los servidores secundarios estén en la misma red.
- En los servidores principales y servidores secundarios, asegúrese de configurar el Firewall de Windows para permitir las conexiones TCP entrantes en el puerto Secure Entry. El puerto predeterminado es

55767. Para obtener información sobre la configuración de puertos personalizada, consulte *General*, on page 214.

- Al conectar un servidor secundario a otro principal, se sustituye su clave de lector, lo que invalida cualquier credencial Bluetooth existente. Para evitarlo, establezca credenciales de Bluetooth en el servidor principal en lugar de en el secundario.

Flujo de trabajo

1. Configure un servidor como un servidor secundario y genere el archivo de configuración. Vea *Generar el archivo de configuración desde el servidor secundario*, on page 174.
2. Configure un servidor como servidor principal e importe el archivo de configuración de los servidores secundarios. Vea *Importar el archivo de configuración al servidor principal*, on page 174.
3. Configure los grupos de titulares de tarjeta y de titulares globales en el servidor principal. Vea *Agregar un titular de tarjeta*, on page 183 y *Agregar un grupo*, on page 189.
4. Consulte y supervise los titulares de tarjeta y los grupos de titulares de tarjeta globales desde el servidor secundario. Vea *Gestión de acceso*, on page 183.

Generar el archivo de configuración desde el servidor secundario

1. Desde el servidor secundario, vaya a **Configuration > Access control > Multi server (Configuración > control de acceso > multi servidor)**.
2. Haga clic en **Sub server (servidor secundario)**.
3. Haga clic en **Generate (generar)**. Se genera un archivo de configuración en formato .json.
4. Haga clic en **Download (Descargar)** y elija una ubicación para guardar el archivo.

Importar el archivo de configuración al servidor principal

1. Desde el servidor principal, vaya a **Configuration > Access control > Multi server (Configuración > control de acceso > multi servidor)**.
2. Haga clic en **Main server (Servidor principal)**.
3. Haga clic en **+ Add (Agregar)** y vaya al archivo de configuración generado del servidor secundario.
4. Introduzca el nombre del servidor, la dirección IP y el número de puerto del servidor secundario.
5. Haga clic en **Import (Importar)** para agregar el servidor secundario.
6. El estado del servidor secundario es **Connected**.

Revocar un servidor secundario

Solo puede revocar un servidor secundario antes de importar su archivo de configuración a un servidor principal.

1. Desde el servidor principal, vaya a **Configuration > Access control > Multi server (Configuración > control de acceso > multi servidor)**.
2. Haga clic en **Sub server (servidor secundario)** y haga clic en **Revoke server (Revocar servidor)**. Ahora puede configurar este servidor como servidor principal o servidor secundario.

Eliminar un servidor secundario

Después de importar el archivo de configuración de un servidor secundario, se conecta el servidor secundario al servidor principal.

Para eliminar un servidor secundario:

1. Desde el servidor principal:
 - 1.1. vaya a **Access management > Dashboard (Gestión de acceso > Panel)**.

- 1.2. Cambie los titulares de tarjeta y los grupos globales por los titulares de tarjeta y los grupos locales.
- 1.3. Vaya a **Configuration > Access control > Multi server (Configuración > Control de acceso > Multiservidor)**.
- 1.4. Haga clic en **Main server (Servidor principal)** para mostrar la lista de servidores secundarios.
- 1.5. Seleccione el servidor secundario y haga clic en **Delete (Eliminar)**.
2. Desde el servidor secundario:
 - Vaya a **Configuration > Access control > Multi server (Configuración > Control de acceso > Multiservidor)**.
 - Haga clic en **Sub server (Servidor secundario)** y **Revoke server (Revocar servidor)**.

Ajustes ^{BETA} de Active Directory

Nota

Las cuentas de usuario y los grupos de Microsoft Windows y Active Directory pueden acceder a AXIS Camera Station Pro. La forma de añadir usuarios en Windows varía en función de su versión. Para obtener más información, vaya a support.microsoft.com. Consulte el administrador de red si usa una red de dominio de Active Directory.

La primera vez que abra la página de configuración de Active Directory, podrá importar usuarios de Microsoft Active Directory a titulares de tarjetas en AXIS Camera Station Pro. Vea *Importar usuarios de Active Directory, on page 175*.

Después de la configuración inicial, se mostrarán las siguientes opciones en la página de ajustes de Active Directory.

- Cree y administre grupos de titulares de tarjetas basados en grupos en Active Directory.
- Configure la sincronización programada entre Active Directory y el sistema de gestión de acceso.
- Sincronice manualmente para actualizar todos los titulares de tarjetas importados desde Active Directory.
- Administre la asignación de datos entre los datos del usuario de Active Directory y las propiedades del titular de la tarjeta.

Importar usuarios de Active Directory

Para importar usuarios de Active Directory a titulares de tarjetas en AXIS Camera Station Pro:

1. Vaya a **Configuration (Configuración) > Access control (Control de acceso) > Active directory settings (Ajustes de Active Directory)^{BETA}**.
2. Haga clic en **Set up import (Configurar importación)**.
3. Siga las instrucciones que aparecen en pantalla para completar estos tres pasos principales:
 - 3.1. Seleccione un usuario de Active Directory para usarlo como plantilla para la asignación de datos.
 - 3.2. Asigne datos de usuario desde la base de datos de Active Directory a las propiedades del titular de la tarjeta.
 - 3.3. Cree un nuevo grupo de titulares de tarjetas en el sistema de gestión de acceso y seleccione qué grupos de Active Directory importar.

No puede cambiar ninguno de los datos de usuario importados, pero puede añadir credenciales a un titular de tarjeta importado (consulte *Agregar credenciales, on page 184*).

Configure AXIS Audio Manager Pro

Puede conectarse a un servidor AXIS Audio Manager Pro y usar sus dispositivos de audio conectados en AXIS Camera Station Pro.

Esta configuración requiere AXIS Camera Station Pro 6.12 o superior y AXIS Audio Manager Pro 5.0 o superior. Es preciso configurar previamente tanto el servidor AXIS Camera Station Pro como el servidor AXIS Audio Manager Pro, ya sea en el mismo servidor o en máquinas distintas de la misma red.

Importante

Si AXIS Camera Station Pro y AXIS Audio Manager Pro se ejecutan en el mismo servidor, ambos se configurarán para usar el puerto 443 de forma predeterminada. Para evitar problemas de conexión, configure uno de ellos para que utilice otro puerto.

Puede modificar la configuración del puerto en AXIS Camera Station Pro mediante *General, on page 214*. Para obtener información sobre cómo modificar la configuración del puerto en AXIS Audio Manager Pro, consulte *AXIS Audio Manager Pro – User manual (Manual de usuario de AXIS Audio Manager Pro)*.

Para comenzar a usar AXIS Audio Manager Pro en AXIS Camera Station Pro:

1. En AXIS Audio Manager Pro:
 - 1.1. Vaya a **System settings (Ajustes del sistema) > API access (Acceso a la API)**.
 - 1.2. Habilite la API e introduzca un nombre de usuario y una contraseña.
2. En AXIS Camera Station Pro:
 - 2.1. Vaya a **Configuration (Configuración) > AXIS Audio Manager Pro** y haga clic en **Connect (Conectar)** para establecer una conexión con su servidor AXIS Audio Manager Pro.
 - 2.2. En el cuadro de diálogo emergente, introduzca la **Server URL (URL del servidor)**, el **API username (nombre de usuario API)** y la **API password (contraseña API)** de su servidor AXIS Audio Manager Pro y haga clic en **Connect (Conectar)**.

Una vez establecida la conexión, podrá:

- Consultar el **Server status (Estado del servidor)** AXIS Audio Manager Pro y el **Device status (Estado del dispositivo)** de los dispositivos conectados a dicho servidor.
- Abra una nueva pestaña de AXIS Audio Manager Pro para acceder a la interfaz web del servidor.
- Use las nuevas funciones de audio en AXIS Camera Station Pro.

Para obtener más información, consulte *AXIS Audio Manager Pro, on page 205*.

Nota

Para evitar problemas con los certificados, recomendamos crear u obtener un certificado de una Autoridad de certificación (CA) de confianza, cargarlo en AXIS Audio Manager Pro y añadirlo a la lista de certificados de confianza del servidor de AXIS Camera Station Pro. Para obtener más información, consulte *AXIS Audio Manager Pro – User manual (Manual de usuario de AXIS Audio Manager Pro)*.


Configurar la Búsqueda inteligente 2



Con Búsqueda inteligente 2, puede configurar diversos filtros para encontrar fácilmente personas y vehículos de interés en las grabaciones generadas por las cámaras Axis.



Para obtener información sobre requisitos, limitaciones y cómo utilizar Búsqueda inteligente 2, consulte *Búsqueda inteligente 2, on page 37*.

1. Vaya a **Configuration > Smart search 2 (Configuración > Búsqueda inteligente 2) > Settings (Ajustes)**.
2. En **Cameras (Cámaras)**:

- 2.1. seleccione las cámaras a las que se deberían enviar metadatos a **Búsqueda inteligente 2**.
- 2.2. Para permitir una clasificación de servidor en segundo plano para una cámara, seleccione **Allow (Permitir)** en **Background server classification (Clasificación del servidor de fondo)**. Esto aumenta la carga del servidor pero mejora la experiencia del usuario.
- 2.3. Para limitar la cantidad de detecciones guardadas en el servidor, en **Filter (Filtro)**, haga clic en  y cree los filtros para **Area (Área)**, **Size and duration (tamaño y duración)** y **Swaying objects (Objetos con balanceo)**.
Puede usar estos filtros para excluir áreas, objetos pequeños o que solo aparecen un breve tiempo, u objetos con balanceo, como la vegetación.
Los filtros de búsqueda inteligente utilizan los filtros de ajustes de movimiento existentes como punto de partida.
3. En **(Storage) Almacenamiento**:
 - Seleccione la unidad y la carpeta para guardar las detecciones y haga clic en **Apply (Aplicar)**.
 - Defina el límite de tamaño de almacenamiento y haga clic en **Apply (Aplicar)**. Cuando el almacenamiento llega al límite, elimina las detecciones más antiguas.
4. Seleccione **Include periods with missing metadata (Incluir puntos cuando falten metadatos)** para mostrar los resultados que indican que no se grabaron metadatos durante un periodo determinado.
5. Seleccione **Let the server classify detections when you start a search (Permitir al servidor clasificar detecciones al iniciar una búsqueda)** para obtener resultados de búsqueda más detallados, incluidas las detecciones que la cámara no clasificó. Para obtener resultados de búsqueda más rápidos, mantenga esta opción desactivada.

Clasificación del servidor de fondo	
	Estado de clasificación del servidor de la última hora en la que la clasificación del servidor es lenta. Aparece cuando se clasifican detecciones menores al 95 %.
	Estado de clasificación del servidor de la última hora en la que la clasificación del servidor es lenta. Aparece cuando se clasifican detecciones menores al 50 %.

Desencadenadores

Puede configurar filtros de búsqueda inteligente para usarlos como activadores en las reglas de acción. Para crear un activador de búsqueda inteligente:

1. Vaya a **Configuration (Configuración) → Smart search 2 (Búsqueda inteligente 2) → Triggers (Activadores)**.
2. Haga clic en **Create (Crear)**.
3. Configure el filtro. Para obtener más información sobre los filtros de búsqueda inteligente, consulte *Búsqueda con filtros, on page 37*.
4. Haga clic en **Next (Siguiente)**.
5. Ajuste el nivel de **Confidence (Precisión)** de las detecciones. Una mayor precisión ignora las clasificaciones inciertas y reduce el número de detecciones.
6. Haga clic en **Next (Siguiente)**.
7. Introduzca un nombre para su activador y haga clic en **Save (Guardar)**.

Nota

- La búsqueda inteligente 2 suele necesitar unos segundos después de que un objeto salga del campo de visión de la cámara para analizar la grabación y verificar lo observado. Por ejemplo, si ha configurado una regla de acción para activarse al detectar un coche rojo, la acción se activará solo unos segundos

después de que salga del campo de visión de la cámara y la búsqueda inteligente determine que se trataba de un coche rojo.

- La **Visual similarity (Similitud visual)** no está disponible como opción para los activadores de la búsqueda inteligente 2.
- Crear un activador para una cámara permite que el servidor procese las detecciones de objetos incluso si la opción **Enable background processing (Habilitar procesamiento en segundo plano)** está desactivada para esa cámara.
- Los **Delayed detection periods (Periodos de detección retardada)** son periodos con una alta demora en el procesamiento que provocan que las reglas de acción se activen con retraso. Si esto sucede con frecuencia, puede reconfigurar el filtro de activadores para incluir menos cámaras y usar filtros de cámara como cruce de línea, área, tamaño y duración para mitigar el problema.

Para usar el activador de búsqueda inteligente 2 en una regla de acción, consulte *Crear activadores de búsqueda inteligente 2, on page 102*.

Configure la Supervisión del estado del sistema ^{BETA}

Nota

- Si está conectado a varios servidores de AXIS Camera Station Pro, puede configurar System Health Monitoring en cualquier servidor conectado. Para hacer esto, seleccione el servidor del menú desplegable **Selected server (Servidor seleccionado)**.
- Si administra sistemas en distintas redes, la supervisión del servidor en My Systems ofrece la misma funcionalidad que a través de la nube.

Ajustes

<p>Conexión a la nube</p>	<p>Si ha registrado su servidor en una organización, puede ver los datos de estado del sistema desde cualquier lugar. Si todavía no está conectado, haga clic en Manage (Gestionar) y siga las instrucciones que aparecen en pantalla.</p>
<p>Data retrieval frequency (Frecuencia de recuperación de datos)</p>	<p>Seleccione una frecuencia de datos inferior para solucionar cualquier advertencia sobre datos antiguos o problemas de rendimiento generales en el sistema. En una configuración multisistema, recomendamos utilizar la misma configuración o superior tanto para un subsistema como para su sistema principal.</p> <ul style="list-style-type: none"> • Low (Baja) - para sistemas con más de 100 dispositivos. • Medium (Medio) - Para sistemas con entre 25 y 100 dispositivos. • High (Alta) - para sistemas con menos de 25 dispositivos.

Notificaciones

Para enviar notificaciones por correo electrónico:

1. Configure un servidor SMTP y una dirección de correo electrónico para enviar las notificaciones. Vea *Configuración de puertos del servidor, on page 126*
2. Configure las direcciones de correo electrónico para recibir las notificaciones. Vea *Configurar destinatarios de correo electrónico, on page 179*.
3. Configurar las reglas de notificación. Vea *Configuración de las reglas de notificación., on page 179*.

Configurar destinatarios de correo electrónico

1. Vaya a Configuración > Supervisión del estado del sistema > Notificaciones.
2. En **Email recipients (destinatarios de correo electrónico)**, introduzca una dirección de correo electrónico y haga clic en **Save (guardar)**. Repetir para agregar varios destinatarios de correo electrónico.
3. Para probar el servidor SMTP, haga clic en **Send test email (enviar correo electrónico de prueba)**. Un mensaje muestra que se ha enviado el correo electrónico de prueba.

Configuración de las reglas de notificación.

Hay dos reglas de notificación activadas de forma predeterminada.

Sistema fuera de servicio – se envía una notificación cuando un sistema en configuración de sistema único o cualquier sistema en configuración multisistema está fuera de servicio más tiempo de lo normal.

Dispositivo fuera de servicio – Enviar una notificación cuando un dispositivo de la lista de Supervisión del estado del sistema está fuera de servicio durante más tiempo de lo normal.

1. Vaya a Configuración > Supervisión del estado del sistema > Notificaciones.
2. En **Notification rules (Reglas de notificación)**, active o desactive las reglas de notificación.
3. En **Applied rules (reglas aplicadas)**, puede ver una lista de los sistemas y dispositivos, incluidas las reglas de notificación aplicadas.

Multisistema



Con System Health Monitoring, puede supervisar los datos del estado de varios sistemas secundarios desde un sistema principal.

1. En un sistema secundario, genere la configuración del sistema. Vea *Generar configuración del sistema, on page 179*.
2. En el sistema principal, cargue la configuración del sistema. Vea *Recuperar datos de otros sistemas, on page 180*.
3. Repetir los pasos anteriores en los otros sistemas secundarios.
4. Supervise los datos de estado de varios sistemas desde el sistema principal. Vea *Supervisión del estado del sistema BETA, on page 195*.

Generar configuración del sistema

1. Vaya a Configuración > Supervisión del estado del sistema > Multisistema.
2. Haga clic en **Generate (generar)**.
3. Haga clic en **Copy (copiar)** para cargar la configuración en el sistema principal.
4. Para ver los detalles de la configuración del sistema, haga clic en **Show details (mostrar detalles)**.
5. Para eliminar la configuración del sistema, haga clic en **Delete (eliminar)** para eliminar en primer lugar la ya existente.

Después de carga la configuración del sistema en el sistema principal, la información del sistema principal aparece en **Systems with access (Sistemas con acceso)**.

Recuperar datos de otros sistemas

Una vez generada y copiada la configuración del sistema de un sistema secundario, puede cargarla en el sistema principal.

1. En el sistema principal, vaya a **Configuración > Supervisión del estado del sistema > Multisistema**).
2. Haga clic en **Paste (Pegar)** para rellenar la información que ha copiado del sistema secundario.
3. Compruebe la dirección IP del servidor y haga clic en **Add (agregar)**.
El sistema secundario aparece en **Available systems (Sistemas disponibles)**.

Configurar analíticas

Panel de información de datos de AXIS

AXIS Data Insights Dashboard presenta los datos de analíticas de sus dispositivos en gráficos y cuadros. La página de configuración de AXIS Data Insights Dashboard muestra todas las aplicaciones compatibles y los escenarios configurados en los dispositivos de su sistema. Vaya a **Analytics (Analíticas) > Data Insights Dashboard** para:

- Ver una lista de cámaras y fuentes de datos que ejecutan las aplicaciones compatibles.
- Ver una lista de aplicaciones y escenarios compatibles con cada dispositivo o fuente de datos. Las siguientes funciones son compatibles:
 - AXIS Object Analytics: Conteo de cruce de línea y ocupación de un área
 - AXIS Audio Analytics
 - AXIS Image Health Analytics
 - AXIS People Counter
 - AXIS P8815-2 3D Counter
 - AXIS Air Quality Sensors (supervisión de calidad del aire)

Nota

Puede almacenar un máximo de 100 MB de datos, lo que limita el tiempo de almacenamiento. Por ejemplo, un sensor de calidad del aire que supervisa los 12 tipos de datos genera un tiempo de retención aproximado de 430 días.

- Elija qué escenarios desea incluir en el panel.
- Etiquete escenarios para permitir el filtrado de datos en el panel, por ejemplo, para agrupar cámaras en la misma ubicación.

Nota

Para mostrar los datos de conteo de cruce de línea de AXIS Object Analytics en el panel **In and Out counting** (Recuento de entradas y salidas), indique la dirección seleccionando **In (Entrada)** u **Out (Salida)** en el campo **Direction (Dirección)**.

- Consulte el estado de los escenarios.

Incluir	Active el switch en la columna Include (Incluir) para mostrar los datos de un escenario en un panel.
Etiquetas	Seleccione etiquetas en el menú desplegable de la columna Tags (Etiquetas) para agregarlas a un escenario.

Para agregar una etiqueta nueva:

1. Abra la pestaña **Tags (Etiquetas)**.
2. Introduzca un nombre para la etiqueta.

3. Haga clic en la flecha.

Nota

- AXIS Data Insights Dashboard requiere protocolos de conexión cifrada TLS versión 1.2 y superior en su servidor de Windows.
- AXIS Data Insights Dashboard sobrescribe cualquier ajuste de MQTT existente de una cámara si:
 - La cámara no tiene un cliente MQTT configurado.
 - Puede habilitar manualmente un escenario para una cámara conectada a otro servidor de AXIS Camera Station Pro.
- Cuando está conectado a AXIS Data Insights Dashboard, el cliente MQTT de la cámara solo se dedica al panel de información de datos.
- Las cámaras y el servidor de AXIS Camera Station Pro deben estar en la misma red.
- Para un rendimiento óptimo, recomendamos un servidor con un mínimo de 16 GB de RAM para ejecutar AXIS Data Insights Dashboard en AXIS Camera Station Pro.
- Puede almacenar un máximo de 100 MB de datos, lo que se traduce en un tiempo de almacenamiento limitado. Por ejemplo:
 - La estimación de la ocupación en un aparcamiento provisto de cuatro cámaras, cada una de ellas configurada para detectar cinco subclases de vehículos como coches y bicicletas las 24 horas del día, los 7 días de la semana, da como resultado 260 días de tiempo de retención.
 - El conteo de personas en un entorno de establecimientos comerciales equipado con ocho cámaras en el que el flujo de personas es continuo durante 12 horas da como resultado unos 1270 días de tiempo de retención.
 - Un escenario de conteo cruzado de cámaras con seis clases y el flujo de conteo es constante durante 24 horas da como resultado unos 860 días de tiempo de retención.

Para obtener información acerca de cómo agregar un panel a una vista dividida, consulte *AXIS Data Insights Dashboard en una vista dividida, on page 20*.



Cómo habilitar AXIS Data Insights Dashboard

License Plate Verifier

Puede consultar el estado del AXIS License Plate Verifier ACAP en sus cámaras y agrupar estas para facilitar la gestión de la lista de matrículas en la página AXIS License Plate Verifier.

La pestaña **Cameras (Cámaras)** contiene una lista de todos los dispositivos conectados que cuentan con AXIS License Plate Verifier instalado:

- **Cámara:** El nombre de la cámara.
- **Version (Versión):** ¿Qué versión de AXIS License Plate Verifier está instalada en la cámara?
- **Estado:** El estado actual de AXIS License Plate Verifier.
- **Latest event (Evento más reciente):** Hora del último evento capturado por la cámara.
- **Allowed (Permitido):** La cantidad de matrículas incluidas en la lista "Permitidas" de la cámara.
- **Blocked (Bloqueado):** La cantidad de matrículas incluidas en la lista "Bloqueados" de la cámara.
- **Custom (Personalizado):** La cantidad de matrículas incluidas en la lista "Personalizado" de la cámara.
- **Grupo:** El grupo al que pertenece la cámara.

La pestaña **Groups (Grupos)** contiene una lista de todos sus grupos de cámaras y una sublista de las cámaras incluidas en cada grupo. En esta pestaña, podrá:

- Haga clic en **New... (Nuevo...)** para añadir un nuevo grupo
- Haga clic en **Delete (Eliminar)** para eliminar un grupo existente
- Renombre un grupo seleccionado en el campo **Group name (Nombre del grupo)**.
- Haga clic en **Add... (Añadir...)** para añadir una cámara a un grupo seleccionado.
- Haga clic en **Remove (Borrar)** para suprimir una cámara de un grupo.

Puede crear listas compartidas para cámaras en grupos. Para obtener más información, consulte *Gestión de matrículas, on page 204*.

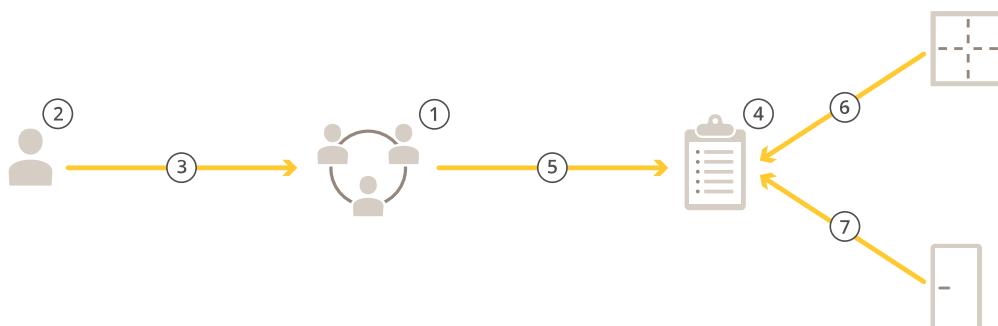
Gestión de acceso

La pestaña de gestión de acceso permite configurar y gestionar los titulares de tarjeta, grupos y reglas de acceso del sistema.

Para obtener un flujo de trabajo adecuado que permita configurar una controladora de accesos en red de Axis en AXIS Camera Station Pro, consulte *Configurar una controladora de accesos en red de Axis*.

Flujo de trabajo de gestión de acceso

La estructura de gestión de accesos es flexible, esto permite desarrollar un flujo de trabajo que se adapte a sus necesidades. El siguiente es un ejemplo de flujo de trabajo:




1. Agregar grupos. Vea *Agregar un grupo*, on page 189.
2. Agregar titulares de tarjeta. Vea *Agregar un titular de tarjeta*, on page 183.
3. Agregar titulares de tarjeta a grupos.
4. Agregar reglas de acceso. Vea *Agregar una regla de acceso*, on page 189.
5. Aplicar grupos a reglas de acceso.
6. Aplicar zonas a las reglas de acceso.
7. Aplicar puertas a reglas de acceso.

Agregar un titular de tarjeta

Un titular de tarjeta es una persona con un identificador único registrado en el sistema. Configure un titular de tarjeta con credenciales que identifica a la persona y cuándo y cómo conceder acceso a las puertas.

También puede elegir asignar usuarios de una base de datos de Active Directory como titulares de tarjeta, consulte *Ajustes BETA de Active Directory*, on page 175.

1. Abra una pestaña de  Access management (Gestión de acceso).
2. Vaya a **Cardholder management (Gestión de titulares de tarjeta) > Cardholders (Titulares de tarjeta)** y haga clic en **+ Add (Agregar)**.
3. Introduzca el nombre y apellidos del titular de tarjeta y haga clic en **Next (Siguiente)**.
4. Si lo desea, haga clic en **Advanced (Avanzado)** y seleccione las opciones que desee.
5. Agregar una credencial al titular de tarjeta. Vea *Agregar credenciales*, on page 184
6. Haga clic en **Save (Guardar)**.
7. Agregar el titular de tarjeta a un grupo.
 - 7.1. En **Groups (Grupos)**, seleccione el grupo al que desea agregar el titular de tarjeta y haga clic en **Edit (Editar)**.

- 7.2. Haga clic en **+ Add (Añadir)** y seleccione el titular de tarjeta que desea agregar al grupo. Puede seleccionar varios titulares de tarjeta.
- 7.3. Haga clic en **Añadir**.
- 7.4. Haga clic en **Save (Guardar)**.

Avanzada	
Tiempo de acceso largo	Seleccione esta opción para permitir que el titular de la tarjeta tenga un tiempo de acceso largo y un tiempo de apertura demasiado largo cuando haya un monitor de puerta instalado.
Suspender titular	Seleccione esta opción para suspender el titular de la tarjeta.
Allow double-swipe (Permitir doble barrido)	Seleccione esta opción para permitir que un titular de tarjeta anule el estado actual de una puerta. Por ejemplo, pueden usarla para desbloquear una puerta fuera de la programación normal.
Exento de bloqueo	Seleccione esta opción para permitir el acceso al titular de tarjeta durante el bloqueo.
Exento de antipassback	Seleccione para proporcionar a un titular de tarjeta una exención de una regla antipassback. La función antipassback impide que los usuarios utilicen las mismas credenciales que otra persona que ha entrado en una zona antes. Primero debe salir de la zona la primera persona antes de poder volver a utilizar las credenciales.
Titular de tarjeta global	Seleccione para poder ver y supervisar al titular de tarjeta en los servidores secundarios. Esta opción solo está disponible para los titulares de tarjeta creados en el servidor principal. Vea <i>BETA de varios servidores, on page 173</i> .



Agregar titulares de tarjeta y grupos

Agregar credenciales

Puede agregar los siguientes tipos de credenciales a un titular de tarjeta:

- código QR
- Número de identificación personal (PIN)
- Credencial móvil
- Tarjeta
- Matrícula

Para agregar una credencial de QR a un titular de tarjeta:

Nota

El uso de códigos QR como credenciales requiere que la hora del controlador del sistema y de la cámara con AXIS Barcode Reader esté sincronizada. Recomendamos utilizar la misma fuente de hora para ambos dispositivos para una sincronización perfecta de hora.

1. En **Credentials (Credenciales)**, haga clic en **+ Add (Agregar)** y seleccione **QR-code (Código QR)**.
2. Introduzca un nombre para la credencial.
3. **Dynamic QR (QR dinámico)** está activado de forma predeterminada. Debe utilizar el QR dinámico con credencial de PIN.
4. Establezca la fecha de inicio y fin para la credencial.
5. Para enviar un código QR por correo electrónico automáticamente después de guardar el titular de la tarjeta, seleccione **Enviar código QR al titular de tarjeta cuando se guarde la credencial**.
6. Haga clic en **Añadir**.

Para agregar una credencial de PIN a un titular de tarjeta:

1. En **Credentials (Credenciales)**, haga clic en **+ Add (Agregar)** y seleccione **PIN**.
2. Introduzca un PIN.
3. Para utilizar un PIN de coacción que active una alarma silenciosa, active **Duress PIN (PIN de coacción)** e introduzca un PIN de coacción.
4. Determine las fechas **Valid from (Válido desde)** y **Valid to (Válido hasta)** de la credencial.
5. Haga clic en **Añadir**.

También puede configurar un PIN de coacción que abre la puerta y activa una alarma silenciosa en el sistema.

Para agregar una credencial móvil a un titular de tarjeta:

Nota

El titular de la tarjeta debe tener una dirección de correo electrónico para recibir la credencial móvil.

1. En **Credentials (Credenciales)**, haga clic en **+ Add (Agregar)** y seleccione **Mobile credential (Credencial móvil)**.
2. Introduzca un nombre para la credencial.
3. Establezca la fecha de inicio y fin para la credencial.
4. Seleccione **Send the mobile credential to the cardholder after saving (Enviar la credencial móvil al titular de tarjeta después de guardar)**. El titular de la tarjeta recibe un correo electrónico con las instrucciones de emparejamiento.
5. Haga clic en **Añadir**.

Consulte el ejemplo en *Utilice la aplicación AXIS Mobile Credential como credencial Bluetooth, on page 160*.

Para agregar una credencial de tarjeta a un titular de tarjeta:

1. En **Credentials (Credenciales)**, haga clic en **+ Add (Agregar)** y seleccione **Card (Tarjeta)**.
2. Para introducir manualmente los datos de la tarjeta, introduzca el nombre de la tarjeta, el número de tarjeta y la longitud de bits.

Nota

La longitud de bits solo es configurable cuando se crea un formato de tarjeta con una longitud de bits específica que no está en el sistema.

3. Para obtener automáticamente los datos de la tarjeta de la última tarjeta que se ha pasado:
 - 3.1. Seleccione una puerta en el menú desplegable **Select reader (Seleccionar lector)**.
 - 3.2. Pase la tarjeta por el lector conectado a esa puerta.
 - 3.3. Haga clic en **Get last swiped card data from the selected reader (Obtener datos de la última tarjeta que se ha pasado desde los lectores de la puerta)**.

Nota

Puede utilizar el lector de tarjetas USB 2N para obtener los datos de la tarjeta. Para obtener más información, consulte *Configurar el lector de tarjetas USB 2N*.

4. Introduzca un código de instalación. Este campo solo está disponible si ha habilitado **Facility code (Código de instalación)** en **Access management > Settings (Gestión de acceso > Ajustes)**.
5. Establezca la fecha de inicio y fin para la credencial.
6. Haga clic en **Añadir**.

Para agregar una matrícula a un titular de tarjeta:

1. En **Credentials (Credenciales)**, haga clic en **+ Add (Agregar)** y seleccione **License plate (Matrícula)**.
2. Introduzca un nombre de credencial que describa el vehículo.
3. Introduzca el número de matrícula del vehículo.
4. Establezca la fecha de inicio y fin para la credencial.
5. Haga clic en **Añadir**.

Consulte el ejemplo en *Utilizar el número de matrícula como credencial, on page 188*.

Fecha de caducidad	
Válido desde	Establezca una fecha y hora para el momento en que la credencial debe ser válida.
Válido hasta	Seleccione una opción en el menú desplegable.

Válido hasta	
Sin fecha de finalización	La credencial nunca caduca.
Fecha	Establezca una fecha y hora en la que caduca la credencial.
Desde el primer uso	Seleccione cuándo caduca la credencial después del primer uso. Seleccione días, meses, años or número de veces después del primer uso.
Desde el último uso	Seleccione cuándo caduca la credencial después del último uso. Seleccione días, meses o años después del último uso.

Credencial con código QR

Nota

El uso de códigos QR como credenciales requiere que la hora del controlador del sistema y de la cámara con AXIS Barcode Reader esté sincronizada. Recomendamos utilizar la misma fuente de hora para ambos dispositivos para una sincronización perfecta de hora.

Para agregar una credencial con código QR a un titular de tarjeta:

1. En **Credentials (Credenciales)**, haga clic en **+ Add (Agregar)** y seleccione **QR-code (Código QR)**.
2. Introduzca un nombre para la credencial.
3. **Dynamic QR (QR dinámico)** está activado de forma predeterminada. Debe utilizar el QR dinámico con credencial de PIN.
4. Establezca la fecha de inicio y fin para la credencial.
5. Para enviar el código QR por correo electrónico automáticamente después de guardar el titular de la tarjeta, seleccione **Send QR-code to cardholder when credential is saved (Enviar código QR al titular de tarjeta cuando se guarde la credencial)**.

6. Haga clic en **Añadir**.

Credencial de PIN

Para agregar una credencial de PIN a un titular de tarjeta:

1. En **Credentials (Credenciales)**, haga clic en **+ Add (Agregar)** y seleccione **PIN**.
2. Introduzca un PIN.
3. De forma opcional, para activar una alarma silenciosa con un PIN independiente, active **Duress PIN (PIN de coacción)** e introduzca un PIN de coacción.
4. Determine las fechas **Valid from (Válido desde)** y **Valid to (Válido hasta)** de la credencial.
5. Haga clic en **Añadir**.

Credencial móvil

Nota

El titular de la tarjeta debe tener una dirección de correo electrónico para recibir la credencial móvil.

Para agregar una credencial móvil a un titular de tarjeta:

1. En **Credentials (Credenciales)**, haga clic en **+ Add (Agregar)** y seleccione **Mobile credential (Credencial móvil)**.
2. Introduzca un nombre para la credencial.
3. Establezca la fecha de inicio y fin para la credencial.
4. Seleccione **Send the mobile credential to the cardholder after saving (Enviar la credencial móvil al titular de tarjeta después de guardar)**. El titular de la tarjeta recibe un correo electrónico con las instrucciones de emparejamiento.
5. Haga clic en **Añadir**.

Consulte el ejemplo en *Utilice la aplicación AXIS Mobile Credential como credencial Bluetooth, on page 160*.

Credencial de tarjeta

Para agregar una credencial de tarjeta a un titular de tarjeta:

1. En **Credentials (Credenciales)**, haga clic en **+ Add (Agregar)** y seleccione **Card (Tarjeta)**.
2. Para introducir manualmente los datos de la tarjeta, introduzca el nombre de la tarjeta, el número de tarjeta y la longitud de bits.

Nota

La longitud de bits solo es configurable cuando se crea un formato de tarjeta con una longitud de bits específica que no está en el sistema.

3. Para obtener automáticamente los datos de la tarjeta de la última tarjeta que se ha pasado:
 - 3.1. Seleccione una puerta en el menú desplegable **Select reader (Seleccionar lector)**.
 - 3.2. Pase la tarjeta por el lector conectado a esa puerta.
 - 3.3. Haga clic en **Get last swiped card data from the selected reader (Obtener datos de la última tarjeta que se ha pasado desde los lectores de la puerta)**.

Nota

Puede utilizar el lector de tarjetas USB 2N para obtener los datos de la tarjeta. Para obtener más información, consulte *Configurar el lector de tarjetas USB 2N*.

4. Introduzca un código de instalación. Este campo solo está disponible si ha habilitado **Facility code (Código de instalación)** en **Access management > Settings (Gestión de acceso > Ajustes)**.
5. Establezca la fecha de inicio y fin para la credencial.
6. Haga clic en **Añadir**.

Credenciales de matrícula

Para agregar una matrícula a un titular de tarjeta:

1. En **Credentials (Credenciales)**, haga clic en **+ Add (Agregar)** y seleccione **License plate (Matrícula)**.
2. Introduzca un nombre de credencial que describa el vehículo.
3. Introduzca el número de matrícula del vehículo.
4. Establezca la fecha de inicio y fin para la credencial.
5. Haga clic en **Añadir**.

Utilizar el número de matrícula como credencial


En este ejemplo se muestra cómo usar un controlador de puerta, una cámara con AXIS License Plate Verifier y el número de matrícula de un vehículo como credenciales para conceder acceso.

1. Agregue el controlador de puerta y la cámara a AXIS Camera Station Pro. Vea *Agregar dispositivos, on page 6*
2. Defina la fecha y la hora para los nuevos dispositivos con **Synchronize with server computer time (Sincronizar con hora del equipo del servidor)**. Vea *Configurar fecha y hora., on page 69*.
3. Actualice el firmware de los dispositivos nuevos a la versión más reciente disponible. Vea *Actualizar firmware, on page 68*.
4. Agregue una puerta nueva conectada al controlador de puerta. Vea *Agregar una puerta, on page 149*.
 - 4.1. Agregue un lector en el **Lado A**. Consulte *Agregar un lector, on page 158*.
 - 4.2. En **Door settings (Ajustes de puerta)**, seleccione **AXIS License Plate Verifier** como **Reader type (Tipo de lector)** e introduzca un nombre para el lector.
 - 4.3. Si lo desea, puede agregar un lector o dispositivo de solicitud de salida (REX) al **Lado B**.
 - 4.4. Haga clic en **Ok (Aceptar)**.
5. Instale y active AXIS License Plate Verifier en la cámara. Consulte el manual del usuario de *AXIS License Plate Verifier*.
6. Iniciar AXIS License Plate Verifier.
7. Configurar AXIS License Plate Verifier.
 - 7.1. Vaya a **Configuration > Access control > Encrypted communication (Configuración > Control de acceso > Comunicación cifrada)**.
 - 7.2. En **External Peripheral Authentication Key (Clave de autenticación periférica externa)**, haga clic en **Show authentication key (Mostrar clave de autenticación)** y **Copy key (Copiar clave)**.
 - 7.3. Abra AXIS License Plate Verifier desde la interfaz web de la cámara.
 - 7.4. No realice la configuración.
 - 7.5. Vaya a **Settings (Ajustes)**.
 - 7.6. En **Access control (Control de acceso)**, seleccione **Secure Entry (Entrada segura)** como **Type (Tipo)**.
 - 7.7. En **IP address (Dirección IP)**, introduzca la dirección IP para el controlador de puerta.
 - 7.8. En **Authentication key (Clave de autenticación)**, pegue la clave de autenticación que copió anteriormente.
 - 7.9. Haga clic en **Connect (Conectar)**.
 - 7.10. En **Door controller name (Nombre del controlador de puerta)**, seleccione el controlador de puerta.
 - 7.11. En **Reader name (Nombre del lector)**, seleccione el lector que agregó anteriormente.
 - 7.12. Active la integración.
8. Agregue el titular de tarjeta al que desee acceder. Vea *Agregar un titular de tarjeta, on page 183*

9. Agregue las credenciales de la matrícula al nuevo titular de la tarjeta. Vea *Agregar credenciales*, on page 184
10. Agregar una regla de acceso. Vea *Agregar una regla de acceso*, on page 189.
 - 10.1. Agregue una programación.
 - 10.2. Agregue el titular de la tarjeta al que desee conceder acceso a la matrícula.
 - 10.3. Agregue la puerta con el lector AXIS License Plate Verifier.

Agregar un grupo

Los grupos le permiten gestionar de forma colectiva y eficiente los titulares de tarjeta y sus reglas de acceso.

1. Abra una pestaña de  Access management (Gestión de acceso).
2. Vaya a **Cardholder management (Gestión de titulares de tarjeta) > Groups (Grupos)** y haga clic en **+ Add (Agregar)**.
3. Introduzca un nombre y, si lo desea, las iniciales del grupo.
4. Seleccione **Global group (Grupo global)** para poder visualizar y supervisar en los servidores secundarios. Esta opción solo está disponible para los titulares de tarjeta creados en el servidor principal. Vea ^{BETA} *de varios servidores*, on page 173.
5. Agregar titulares de tarjeta al grupo:
 - 5.1. Haga clic en **+ Agregar**.
 - 5.2. Seleccione los titulares de tarjeta que desee añadir y haga clic en **Add (Agregar)**.
6. Haga clic en **Save (Guardar)**.

Agregar una regla de acceso

Una regla de acceso define las condiciones que deben cumplirse para conceder acceso.


Una regla de acceso consta de:

Titulares de tarjeta y grupos de titulares – a quién conceder acceso.

Puertas y zonas – dónde se aplica el acceso.

Horarios – cuándo conceder acceso.

Para agregar una regla de acceso:

1. Abra una pestaña de  Access management (Gestión de acceso).
2. Vaya a **Cardholder management (Gestión de titulares de tarjeta)**.
3. En **Access rules (Reglas de acceso)**, haga clic en **+ Add (Agregar)**.
4. Introduzca un nombre para la regla de acceso y haga clic en **Next (Siguiente)**.
5. Configure los titulares de tarjeta y los grupos:
 - 5.1. En **Cardholders (Titulares de tarjeta)** o **Groups (Grupos)**, haga clic en **+ Add (Agregar)**.
 - 5.2. Seleccione los titulares de tarjeta o grupos y haga clic en **Add (Agregar)**.
6. Configure las puertas y zonas:
 - 6.1. En **Doors (Puertas)** o **Zones (Zonas)**, haga clic en **+ Add (Agregar)**.
 - 6.2. Seleccione las puertas o zonas y haga clic en **Add (Agregar)**.
7. Configure las programaciones:
 - 7.1. En **Schedules (Programaciones)**, haga clic en **+ Add (Agregar)**.
 - 7.2. Seleccione una o más programaciones y haga clic en **Add (Agregar)**.


8. Haga clic en **Save (Guardar)**.

Una regla de acceso en la que le falten uno o más de los componentes descritos anteriormente está incompleta. Puede ver todas las reglas de acceso incompletas en la pestaña **Incomplete (Incompletas)**.



Exportar informes de configuración del sistema

Puede exportar informes que contengan diferentes tipos de información acerca del sistema. AXIS Camera Station Pro exporta el informe como un archivo de valores separados por comas (CSV) y lo guarda en la carpeta de descargas predeterminada. Para exportar un informe:

1. Abra una pestaña de  **Access management (Gestión de acceso)**.
2. Vaya a **Reports (Informes) > System configuration (Configuración del sistema)**.
3. Seleccione los informes que desea exportar y haga clic en **Download (Descargar)**.

Informe de detalles de titulares de tarjeta	Incluye información sobre los titulares de tarjetas, credenciales, validación de tarjetas y última operación.
Informe de acceso de titulares de tarjeta	Incluye información sobre titulares de tarjetas y sobre grupos de titulares de tarjetas, reglas de acceso, puertas y zonas con las que está relacionado el titular de tarjeta.
Informe de acceso de grupo de titulares de tarjeta	Incluye el nombre del grupo de titulares de tarjetas e información sobre titulares de tarjetas, reglas de acceso, puertas y zonas con las que está relacionado el grupo de titulares de tarjetas.
Informe de regla de acceso	Incluye el nombre de la regla de acceso e información sobre titulares de tarjetas, grupos de titulares de tarjetas, puertas y zonas con las que está relacionada la regla de acceso.
Informe de acceso de puerta	Incluye el nombre de la puerta e información sobre titulares de tarjetas, grupos de titulares de tarjetas, reglas de acceso y zonas con las que está relacionada la puerta.
Informe de acceso de zona	Incluye el nombre de la zona e información sobre titulares de tarjetas, grupos de titulares de tarjetas, reglas de acceso y puertas con las que está relacionada la zona.

Crear informes de actividad de titulares de tarjeta


En un informe de pase de lista se enumeran los titulares de tarjeta dentro de una zona específica, lo que ayuda a identificar quién está presente en un momento dado.

En un informe de agrupamiento se enumera a los titulares de tarjeta dentro de una zona específica, lo que ayuda a identificar quién está a salvo y quién ha desaparecido en una situación de emergencia. Ayuda a los gestores de edificios a localizar al personal y a los visitantes después de una evacuación. Un punto de

agrupamiento es un lector designado donde el personal se presenta durante las emergencias, y se genera un informe de personas dentro y fuera de las instalaciones. El sistema marca a los titulares de tarjeta como desaparecidos hasta que se registran en un punto de agrupamiento o hasta que alguien los marca manualmente como fuera de peligro.

Tanto los informes de pase de lista como los de agrupamiento requieren zonas para el seguimiento de los titulares de tarjeta.

Para crear y ejecutar un informe de pase de lista o agrupamiento:

1. Abra una pestaña de  Access management (Gestión de acceso).
2. Vaya a **Reports (Informes) > Cardholder activity (Actividad de los titulares de tarjeta)**.
3. Haga clic en **+ Add (Agregar)** y seleccione **Roll call / Mustering (Pase de lista / Agrupamiento)**.
4. Introduzca un nombre para el informe.
5. Seleccione las zonas que desee incluir en el informe.
6. Seleccione los grupos que desee incluir en el informe.
7. Si desea obtener un informe de agrupamiento, seleccione **Mustering point (Punto de agrupamiento)** y un lector para el punto de agrupamiento.
8. Seleccione un marco temporal para el informe.
9. Haga clic en **Save (Guardar)**.
10. Seleccione el informe y haga clic en **Run (Ejecutar)**.

Estado del informe de pase de lista	Descripción
Presente	El titular de tarjeta accedió a la zona especificada y no salió antes de que usted ejecutara el informe.
Ausente	El titular de tarjeta salió de la zona especificada y no volvió a entrar antes de que usted ejecutara el informe.

Estado del informe de agrupamiento	Descripción
A salvo	El titular de tarjeta pasó esta última en el punto de agrupamiento.
Ausente	El titular de tarjeta no pasó esta última en el punto de agrupamiento.

Importación y exportación

Importar titulares de tarjetas

Esta opción importa titulares de tarjeta, grupos de titulares de tarjetas, credenciales y fotografías de titulares de tarjeta desde un archivo CSV. Para importar las fotos del titular de la tarjeta, asegúrese de que el servidor dispone de acceso a las fotos.

Al importar titulares de tarjeta, el sistema de gestión de acceso guarda automáticamente la configuración del sistema, incluida toda la configuración de hardware y elimina cualquiera guardada anteriormente.

También puede elegir asignar usuarios de una base de datos de Active Directory como titulares de tarjeta, consulte *Ajustes BETA de Active Directory, on page 175*.

Importar opciones	
Nuevo	Esta opción elimina los titulares de las tarjetas existentes y añade nuevos titulares.
Actualizar	Esta opción actualiza los titulares de las tarjetas existentes y agrega nuevos titulares de tarjeta.
Agregar	Esta opción mantiene a los titulares de las tarjetas existentes y añade nuevos titulares. Los números de tarjeta y los identificadores de titular de tarjeta son exclusivos y solo pueden utilizarse una vez.

1. En la pestaña **Access management (Gestión de acceso)**, haga clic en **Import and export (Importar y exportar)**.
2. Haga clic en **Import cardholders (Importar titulares de tarjeta)**.
3. Seleccione **New (Nuevo)**, **Update (Actualizar)** o **Add (Agregar)**.
4. Haga clic en **Next (Siguiente)**.
5. Haga clic en **Choose a file (Seleccionar un archivo)** y vaya al archivo CSV. Haga clic en **Abrir**.
6. Introduzca un delimitador de columna, seleccione un identificador único y haga clic en **Next (Siguiente)**.
7. Asigne un encabezado a cada columna.
8. Haga clic en **Importar**.

Importar ajustes	
La primera fila es un encabezado	Seleccione si el archivo CSV contiene un encabezado de columna.
Delimitador de columnas	Introduzca un formato de delimitador de columnas para el archivo CSV.
Identificador único	El sistema utiliza un ID de titular de tarjeta para identificar a un titular de forma predeterminada. También puede utilizar el nombre y el apellido o la dirección de correo electrónico. El identificador único impide la importación de registros de personal duplicados.
Formato de número de tarjeta	Se ha seleccionado Allow both hexadecimal and number (Permitir hexadecimal y número) de forma predeterminada.

Exportar titulares de tarjetas

Esta opción exporta los datos de titulares de tarjeta del sistema a un archivo CSV.

1. En la pestaña **Access management (Gestión de acceso)**, haga clic en **Import and export (Importar y exportar)**.
2. Haga clic en **Export cardholders (Exportar titulares de tarjeta)**.
3. Elija una ubicación de descarga y haga clic en **Save (Guardar)**.

AXIS Camera Station Pro actualiza las fotos de los titulares de tarjetas en `C:\ProgramData\Axis Communications\AXIS Camera Station\Components\AXIS Secure Entry\Cardholder photos` cada vez que cambia la configuración.

Undo import (Deshacer importación)

El sistema guarda automáticamente su configuración al importar titulares de tarjeta. La opción **Undo import (Deshacer importación)** restablece los datos de titular de tarjeta y toda la configuración de hardware al estado en que se encontraron antes de la última importación de titulares de tarjeta.

1. En la pestaña **Access management (Gestión de acceso)**, haga clic en **Import and export (Importar y exportar)**.
2. Haga clic en **Undo import (Deshacer importación)**.
3. Haga clic en **Yes (Sí)**.

Configuración de gestión de acceso

Para personalizar los campos de titular de tarjeta utilizados en el panel de gestión de acceso:

1. En la pestaña **Access management (Gestión de acceso)**, haga clic en **Settings (Ajustes) > Custom cardholder fields (Campos personalizados del titular de tarjeta)**.
2. Haga clic en **+ Add (Agregar)** e introduzca un nombre. Puede añadir hasta 6 campos personalizados.
3. Haga clic en **Añadir**.

Para usar el código de la instalación para verificar el sistema de control de acceso:

1. En la pestaña **Access management (Gestión de acceso)**, haga clic en **Settings (Ajustes) > Facility code (Código de la instalación)**.
2. Seleccione **Facility code on (Código de instalación activado)**.

Nota

También debe seleccionar **Include facility code for card validation (Incluir código de instalación para validación de la tarjeta)** al configurar perfiles de identificación. Vea *Perfiles de identificación, on page 164*.

Para editar una plantilla de correo electrónico con el fin de enviar una credencial QR o móvil:

1. En la pestaña **Access management (Gestión de acceso)**, haga clic en **Settings (Ajustes) > Email templates (Plantillas de correo electrónico)**.
2. Edite su plantilla y haga clic en **Update (Actualizar)**.

Plantillas de insignias ^{BETA}

Puede personalizar las plantillas de insignias con información del titular, fotos, logotipos y marca personalizada. Para crear una nueva plantilla:

1. Vaya a **Access management (Gestión de acceso) > Settings (Ajustes) > Badge templates (Plantillas de insignias) ^{BETA}**.
2. Haga clic en **Create new template (Crear nueva plantilla)**.
3. Introduzca un nombre en el campo **Template name (Nombre de la plantilla)**.
4. Seleccione **Use as default template for printing (Usar como plantilla predeterminada para imprimir)** si desea que esta sea la plantilla empleada por defecto.
5. Personalice el diseño de la insignia:
 - Seleccione hasta cinco campos de texto para mostrar en la parte frontal, incluyendo cualquier campo personalizado que haya creado. Al imprimir, solo aparecen los campos completados en la insignia.
 - Seleccione la fuente y el color del texto.
 - Añada un color o una imagen de fondo.
 - Suba el logotipo de su organización.
 - Para el envés, añada un color o una imagen de fondo.

6. Haz clic en **Save (Guardar)** para guardar los cambios o en **Save as (Guardar como)** para guardarla como una nueva plantilla.

Nota

Una vez creada una plantilla, ya no se podrá editar, solo cambiarle el nombre.

Print badge (Imprimir insignia) ^{BETA}

Puede imprimir insignias de identificación para titulares de tarjetas con las plantillas de insignias configuradas. Recuerde que actualmente no se admite la codificación de tarjetas. Antes de empezar:

- Asegúrese de que el titular de la tarjeta posee al menos una credencial de tarjeta. No puede imprimir insignias para titulares de tarjetas sin credenciales.
- Necesita una impresora compatible con tarjetas de tamaño CR80 y un material de impresión adecuado, como cartulina gruesa.
- Configure los ajustes de impresión de su navegador:
 1. Determine el tamaño de página en CR80 o un tamaño personalizado que se ajuste a las dimensiones de su tarjeta.
 2. Establezca la orientación en vertical.
 3. Desactive los márgenes o configúrelos al mínimo.

Importante

Secure Entry funciona con impresoras con controladores de Windows. Se ha verificado el correcto funcionamiento de la serie de impresoras HID Fargo. Si necesita un controlador para su impresora, contacte con el proveedor de la misma.

Para imprimir insignias:

1. Vaya a **Access management (Gestión de acceso) > Cardholder management (Gestión de titulares de tarjetas) > Cardholders (Titulares de tarjetas)**.
2. Seleccione un o más titulares de tarjetas.
3. Haga clic en **Print badge (Imprimir insignia) ^{BETA}**.
4. Haga clic en **Select template (Seleccionar plantilla)** y, en el menú desplegable **Template (Plantilla)**, seleccione la opción que desea utilizar.
5. Si el titular de la tarjeta tiene varias credenciales, seleccione una en el menú desplegable **Card (Tarjeta)**.
6. Haga clic en **Print (Imprimir)**.




Nota

Si su impresora no admite la impresión doble, imprima primero todas las páginas frontales, luego dé la vuelta a la pila de tarjetas y vuelva a colocarlas en la bandeja para imprimir el envés.

Supervisión del estado del sistema ^{BETA}

La pestaña System Health Monitoring (Supervisión del estado del sistema) le permite supervisar los datos de estado desde un único sistema de AXIS Camera Station o desde varios sistemas AXIS Camera Station Pro en la misma red.

Si administra sistemas en distintas redes, la supervisión del servidor en My Systems ofrece la misma funcionalidad que a través de la nube.

	muestra un resumen de los dispositivos y de los sistemas a los que tiene acceso. Vea <i>Inventario</i> , on page 195.
	Muestra un resumen del almacenamiento y de los detalles de grabación de cada cámara de los sistemas supervisados. Vea <i>Almacenamiento</i> , on page 196.
	muestra los registros de System Health Monitoring desde los sistemas monitorizados. Vea <i>Notificaciones</i> , on page 197.

Limitations (Limitaciones)


- No es posible supervisar el espacio de almacenamiento para las grabaciones en AXIS S3008 Recorder.
- Los ajustes de notificación solo afectan al servidor local de supervisión del estado del sistema.
- El sistema indica las grabaciones excepto las continuas y las activadas por movimiento con **Ninguna** como tipo de grabación.

Flujo de trabajo

1. *Configure la Supervisión del estado del sistema ^{BETA}*, on page 178
 - 1.1. Configure las notificaciones. Vea *Notificaciones*, on page 178.
 - 1.2. Configure un sistema múltiple. Vea *Multisistema*, on page 179.
2. Supervise los datos de estado de los sistemas de AXIS Camera Station Pro.
 - 2.1. *Inventario*, on page 195
 - 2.2. *Almacenamiento*, on page 196
 - 2.3. *Notificaciones*, on page 197

Inventario


La página de inventario muestra un resumen de los dispositivos y sistemas a los que se tiene acceso.

1. En la pestaña **System Health Monitoring (Supervisión del estado del sistema) ^{BETA}**, haga clic en .
2. Para ver el resumen de un sistema, haga clic en **AXIS Camera Station**. El panel derecho muestra información como los detalles del servidor y del sistema.
3. Para ver el resumen de un dispositivo en un sistema, haga clic en el dispositivo de la lista. El panel derecho muestra información como los detalles del dispositivo y la información de almacenamiento si contiene un origen de vídeo.
4. Para descargar el informe del sistema, seleccione **AXIS Camera Station system report (Informe del sistema de AXIS Camera Station)** en el menú desplegable **Create report (Crear informe)**. Vea *Informe del sistema*, on page 209.
5. Para descargar un informe de supervisión del estado del sistema:

- 5.1. En el menú desplegable **Create report (Crear informe)**, seleccione **System Health Monitoring report (Informe de supervisión del estado del sistema)**.
- 5.2. Para incluir la base de datos en el informe, seleccione **Include all databases (Incluir todas las bases de datos)** y haga clic en **Download (Descargar)**.
- 5.3. Cuando el informe esté listo, haga clic para guardarlo.

Almacenamiento

La página de almacenamiento muestra el resumen de almacenamiento y los detalles de grabación de cada cámara de los sistemas supervisados. Haga clic en un encabezado de columna para ordenar por el contenido de la columna.

1. En la pestaña **System Health Monitoring (Supervisión del estado del sistema)** ^{BETA}, haga clic en .
2. Cuando supervise los datos de estado de varios sistemas, seleccione un sistema del menú desplegable.

Resumen	
Estado	Estado del almacenamiento. Vea <i>Configurar almacenamiento, on page 75</i> .
Establecimiento	La ruta y el nombre del almacenamiento.
Total	Cantidad total de espacio de almacenamiento. Es la misma cantidad que se muestra en "Tamaño total" en las propiedades de Windows para la ubicación de almacenamiento.
Asignado	La cantidad máxima de almacenamiento asignado a las grabaciones.
Used (Utilizado)	La cantidad de espacio de almacenamiento utilizado actualmente para las grabaciones.
Última actualización	Hora en la que se actualizó la información por última vez.

Cámara	
Estado	(empty) (vacío): Estado normal. Icono de advertencia: No se cumple con el periodo de conservación. Icono de información: La conservación no se cumple porque las grabaciones de la cámara son demasiado cortas
Nombre	Nombre de la cámara.
Tipo de grabación	Tipos de grabación empleados con la cámara.
Establecer conservación	Tiempo de conservación configurado para la cámara en Configuration > Storage > Selection (configuración > almacenamiento > selección) .
Conservación actual	El número de días que las grabaciones de la cámara han estado en el almacenamiento.
Grabación más antigua	La hora de la grabación más antigua que se guarda en el almacenamiento de la cámara.
Última grabación	La hora de la última grabación que se guarda en el almacenamiento de la cámara.
Establecimiento	La ubicación de almacenamiento utilizada por la cámara.
Almacenamiento utilizado	La cantidad de almacenamiento utilizada por la cámara para las grabaciones.
Última actualización	Hora en la que se actualizó la información por última vez.

Notificaciones

La página de notificaciones muestra los registros de System Health Monitoring de los sistemas supervisados. Haga clic en un encabezado de columna para ordenar por el contenido de la columna.

En la pestaña System Health Monitoring (Supervisión del estado del sistema) ^{BETA}, haga clic en  .

Historial	
Notificación enviada	Hora en la que se ha enviado la notificación.
Elemento	Muestra el nombre del dispositivo en las notificaciones activadas por <code>device down</code> o <code>system</code> en las notificaciones activadas por <code>system down</code> .
Sistema	Nombre del sistema en el que se produce el evento.
Regla	La regla que activó la notificación. <code>System down</code> o <code>Device down</code>
Detectado	La hora en la que se ha detectado el problema.
Resuelto	La hora en la que se ha resuelto el problema.

Teclas de acceso rápido

La pestaña de teclas de acceso rápido muestra las teclas de acceso rápido disponibles. El tipo de tecla de acceso rápido depende de su uso para controlar AXIS Camera Station Pro.

- Una combinación de teclado
- Una combinación de teclado numérico
- Un botón del joystick
- Un botón del mando de control secuencial

Cuando elimina una cámara o vista desde un servidor conectado, las teclas de acceso rápido asociadas también se eliminan.

El sistema agrupa las teclas de acceso rápido en las siguientes categorías:



- Cámara
- Gestión de dispositivos
- Ir a la cámara
- Ir a la vista
- Navegación
- Posiciones predefinidas de PTZ
- Grabaciones
- Secuencias
- Vista dividida
- Pestaña
- Otras

Debe asignar manualmente las acciones de navegar a las cámaras y desplazarse hasta las categorías de vistas.

Nota











- Cuando agregue o edite una tecla de acceso rápido y la tecla de acceso rápido ya esté en uso para otra acción, aparecerá un icono de advertencia. Desplace el ratón sobre el icono de advertencia para ver la acción en conflicto. Pulse ESC para cancelar. Pulse INTRO para utilizar la tecla de acceso rápido y eliminar automáticamente la tecla de acceso rápido en conflicto.
- Al conectarse a varios servidores, las categorías Navegar a las cámaras y Navegar a las vistas también muestran las cámaras y vistas en los servidores conectados.




<p>Asignar una tecla de acceso rápido</p>	<p>Si el valor en teclado de una acción está vacío, haga clic en el valor vacío para agregar la tecla de acceso rápido a esta acción.</p> <ul style="list-style-type: none"> • Para añadir una tecla de acceso rápido con el teclado, pulse Ctrl y al menos otra tecla o una tecla de función F2 - F12. • Para agregar una tecla de acceso rápido con un teclado, pulse una combinación de tecla numérica o pulse una de las teclas de función F1-F5. • Para agregar una tecla de acceso rápido con un joystick o mando de control secuencial, presione el botón en el dispositivo al que se vaya a asignar la acción.
<p>Editar una tecla de acceso rápido</p>	<p>Haga clic en el valor de teclado de una acción y edite el valor.</p>

Eliminar una tecla de acceso rápido	Haga clic en el valor de teclado de una acción y elimine el valor.
	Haga clic en para imprimir la tabla de teclas de acceso rápido.
	Haga clic en para restablecer todas las teclas de inicio rápido a los ajustes originales.

Teclado de control de vigilancia por vídeo

Asignación de teclas de acceso rápido - Joystick	Acción predeterminada	AXIS TU9002	AXIS T8311
Botón 1	Ir a posición predefinida 1	J1	J1
Botón 2	Ir a posición predefinida 2	J2	J2
Botón 3	Ir a posición predefinida 3	J3	J3
Botón 4	Ir a posición predefinida 4	J4	J4
Botón 5	Simular clic con el botón izquierdo del ratón	J5	L
Botón 6	Simular botón izquierdo derecho	J6	D
Botón 7	Seleccionar celda anterior en la vista dividida	Arriba a la izquierda	-
Botón 8	Seleccionar siguiente celda de la vista dividida	Arriba a la derecha	-
Botón 9	Saltar a la grabación anterior	⏮	-
Botón 10	Reproducir/pausa	▶	-
Botón 11	Saltar a la siguiente grabación	▶	-
Botón 12	Agregar marcador	🚩	-
Botón 13	Alternar la función de anillo de zoom entre zoom digital y velocidad de reproducción	M1	-
Botón 14	Alternar entre vista en directo/grabaciones	M2	-
Botón 15	Retroceder imagen	Arriba a la izquierda alternado	-
Botón 16	Avanzar imagen	Arriba a la derecha alternado	-

Asignación de teclas de acceso rápido - teclado	Acción predeterminada	AXIS TU9003	AXIS T8312
A	Abrir vistas		
B	Ir a la cámara o vista siguiente		
ALT+B	Ir a la cámara o vista anterior	Alt+ 	-
PESTAÑA	Ir a la pestaña siguiente		-
ALT+TAB	Ir a la pestaña anterior	Alt+ 	-
C	-	-	
D	-	-	
E	-	-	
MÁS	Enfocar más lejos	+	-
MENOS	Enfocar más cerca	-	-
F2	Abrir teclas de acceso directo	F2	F2
F4	Abrir registros	F4	F4
F5	Abrir configuración	F5	F5
F10	Enfoque automático	F10	-

Asignación de teclas de acceso rápido - Control secuencial	Acción predeterminada	AXIS T8313
Mando de control secuencial 1	Mostrar u ocultar marcador de exportación.	L
Mando de control secuencial 2	Agregar marcador	
Mando de control secuencial 3	Saltar a la grabación anterior	
Mando de control secuencial 4	Reproducir/Pausa	

Asignación de teclas de acceso rápido - Control secuencial	Acción predeterminada	AXIS T8313
Mando de control secuencial 5	Saltar a la siguiente grabación	▶
Mando de control secuencial 6	Alternar entre vista en directo/grabaciones	D

Nota

AXIS T8311 Video Surveillance Joystick no admite los botones 7 a 10 del joystick.

Registros

De forma predeterminada, la pestaña Registros muestra los registros activos, incluidos los registros de alarmas, eventos y auditoría activos. También puede buscar registros anteriores. Puede configurar el número de días que desea guardar los registros en **Configuration > Server > Settings (Configuración > Servidor > Ajustes)**.





Hora	Fecha y hora de la acción.
Tipo	El tipo de la acción: Alarma, Evento o Auditoría.
Categoría	La categoría de la acción.
Mensaje	Una descripción corta de la acción.
Usuario	AXIS Camera Station Pro usuario que realiza la acción.
Equipo	El equipo (nombre de dominio Windows) en el que está instalado AXIS Camera Station Pro.
Usuario de Windows	El usuario de Windows que administra AXIS Camera Station Pro.
Servidor	Solo está disponible al conectarse con varios servidores. El servidor en el que ocurre la acción.
Componente	El componente desde el que se genera el registro.





Búsqueda de registros

1. En la pestaña Logs (Registros), haga clic en **Search (Buscar)** en **Log search (Búsqueda de registros)**.
2. En el cuadro de filtro, escriba las palabras clave. AXIS Camera Station Pro busca en la lista de registros excepto en **Time (Hora)** y muestra los resultados de la búsqueda que contienen todas las palabras clave. Para los operadores de búsqueda compatibles, consulte *Optimizar la búsqueda, on page 44*.
3. Seleccione **Alarms (Alarmas)**, **Audits (Auditorías)** o **Events (Eventos)** en **Filter (Filtro)**.
4. Seleccione una fecha o un intervalo de fechas en el calendario.
5. Seleccione la **Start time (Hora de inicio)** y la **End time (Hora de finalización)** en los menús desplegables.
6. Haga clic en **Buscar**.


Registro de alarmas

El registro de alarmas muestra las alarmas del sistema y las alarmas generadas por reglas y detección de movimiento en una lista. Esta lista incluye la fecha y la hora de la alarma, la categoría de la alarma y un mensaje de alarma. Vea *Alarmas*.


	Haga clic en una alarma y  para abrir la pestaña Recordings (Grabaciones) e iniciar la reproducción cuando la alarma contiene una grabación.
	Haga clic en una alarma y  para abrir el procedimiento de alarma cuando la alarma contiene un procedimiento de alarma.

	Haga clic en una alarma y  para notificar a otros clientes que se han atendido las alarmas.
	Haga clic en una alarma y  para exportar el registro a un archivo de texto.

Registro de eventos

El registro de eventos muestra los eventos de la cámara y el servidor, por ejemplo, grabaciones, activadores, alarmas, errores y mensajes del sistema, en una lista. Esta lista incluye la fecha y la hora del evento, la categoría del evento y un mensaje de evento. Seleccione los eventos y haga clic en  en la barra de herramientas para exportar los eventos como archivo de texto.

Registro de auditoría

En el registro de auditoría puede ver todas las acciones del usuario, por ejemplo, grabaciones manuales, transmisión de vídeo iniciada o detenida, reglas de acción, puerta creada y titular de tarjeta creado. Seleccione las auditorías y haga clic en  en la barra de herramientas para exportar las auditorías como archivo de texto.

Gestión de matrículas

Para gestionar listas de matrículas en AXIS Camera Station Pro, abra la pestaña **License plate management (Gestión de matrículas)**.

En esta pestaña, puede editar tres listas de matrículas para cámaras individuales o grupos de cámaras:

1. Seleccione un grupo o una cámara de las listas **Groups (Grupos)** y **Cameras (Cámaras)**
2. Seleccione la lista que desea editar. De forma predeterminada, las tres listas que puede editar se denominan **Allow list (Lista de permitidos)**, **Block list (Lista de bloqueados)** o **Custom list (Lista personalizada)**.
3. Para editar el nombre de la lista, haga clic en **Edit list name (Editar nombre de la lista)**.
4. Introduzca las nuevas matrículas en la columna **Matrícula** y una descripción (si corresponde) en la columna **Descripción**. Haga clic en **Add (Añadir)** para guardarlas en la lista.
5. Haga clic en **Apply (Aplicar)** para guardar los cambios.

Para editar o eliminar una matrícula que haya añadido a una lista, selecciónela y haga clic en **Edit (Editar)** o **Remove (Eliminar)**.

AXIS Audio Manager Pro

La pestaña AXIS Audio Manager Pro permite acceder a la interfaz del servidor de AXIS Audio Manager Pro directamente desde AXIS Camera Station Pro. Para obtener más información sobre la interfaz del servidor, consulte el *AXIS Audio Manager Pro – User manual (Manual de usuario de AXIS Audio Manager Pro)*.

La pestaña solo aparecerá una vez que se haya conectado a un servidor de AXIS Audio Manager Pro en AXIS Camera Station Pro. Para obtener más información, consulte *Configure AXIS Audio Manager Pro, on page 175*.

Importante





No puede acceder a la interfaz del servidor de AXIS Audio Manager Pro con Secure Remote Access v2.

La integración también permite:






- *Crear activadores de Audio Manager, on page 103*
- *Crear acciones de Audio Manager, on page 113*
- Añadir zonas de audio a los mapas. Consulte *Mapa, on page 22*.
- *Usar interfaces de megafonía en vistas divididas, on page 21*
- Configurar privilegios de usuario relacionados con AXIS Audio Manager Pro en AXIS Camera Station Pro. Consulte *Privilegios de usuario o grupo, on page 139*.
- Seleccione los dispositivos de audio del servidor AXIS Audio Manager Pro como el dispositivo de audio asociado a una cámara. Consulte *Edit stream profiles (Editar perfiles de flujo), on page 54*.

Alarmas

La pestaña Alarmas está disponible en la parte inferior del cliente de AXIS Camera Station Pro y muestra los eventos activados y las alarmas del sistema. Para obtener información sobre cómo crear alarmas, consulte *Reglas de actuación*. Para obtener información acerca de la alarma "Mantenimiento de la base de datos requerido", consulte *Mantenimiento de la base de datos, on page 231*.

Hora	la hora en la que se produjo la alarma.
Categoría	la categoría de la alarma activada.
Descripción	una descripción breve de la alarma.
Servidor	Disponible cuando se conecta a varios servidores. El servidor AXIS Camera Station Pro que envía la alarma.
Componente	El componente que activa la alarma.
	Muestre un procedimiento de alarma, solo disponible cuando la alarma contiene un procedimiento de alarma.
	Vaya a grabaciones, solo disponible cuando la alarma contiene una grabación.
	Confirmar la alarma seleccionada
	Elimine la alarma. La alarma solo se elimina temporalmente si no confirma la alarma antes de eliminarla.

Para gestionar una alarma específica:

1. Haga clic en  **Alarms and Tasks (Alarmas y Tareas)** en la parte inferior del cliente de AXIS Camera Station Pro y abra la pestaña **Alarms (Alarmas)**.
2. Para alarmas con una grabación, seleccione la alarma y haga clic en  para ir a la grabación en la pestaña **Recording alerts (Alertas de grabaciones)**.
3. Para alarmas sin grabación, abra una pestaña con la visualización en directo y haga doble clic en la alarma para mostrar la grabación durante el tiempo de la alarma en la pestaña **Recording alerts (Alertas de grabación)**.
4. Para alarmas con un procedimiento de alarma, seleccione la alarma y haga clic en  para abrir el procedimiento de alarma.
5. Para notificar a otros clientes que las alarmas se han gestionado, seleccione las alarmas y haga clic en  .
6. Para eliminar alarmas de la lista, seleccione las alarmas y haga clic en  .

Tareas

La pestaña Tareas está disponible en la parte inferior del cliente de AXIS Camera Station Pro.

Las siguientes tareas son personales y solo las ven los administradores y usuarios que las han iniciado.

- Informe del sistema
- Crear informe de incidentes
- Exportar grabaciones


Los administrador pueden ver y gestionar todas las tareas iniciadas por cualquier usuario, incluidas las personales.





Los demás usuarios pueden:

- Ver todas las tareas iniciadas por ellos mismos y las tareas no personales iniciadas por otros usuarios.
- Cancelar o volver a intentar realizar las tareas iniciadas por ellos mismos. Solo pueden volver a intentar realizar el informe de incidencias y la exportación de grabaciones.
- Ver el resultado de todas las tareas de la lista.
- Eliminar de la lista todas las tareas finalizadas. Esta acción solo afecta al cliente local.

Nombre	El nombre de la tarea.
Start (Inicio)	Momento en que comenzó la tarea.
Mensaje	<p>Muestra el estado o la información sobre la tarea.</p> <p>Los estados posibles:</p> <ul style="list-style-type: none"> • Cancelando: depuración antes de cancelar la tarea. • Cancelado: la depuración ha finalizado y la tarea se ha cancelado. • Error: la tarea se ha completado con errores, es decir, la tarea falló en uno o más dispositivos. • Finalizado: Tarea completada. • Finalizado durante conexión perdida: se muestra si la tarea se completó mientras el servidor estaba desconectado. El estado de la tarea no se puede determinar. • Se perdió la conexión: se muestra si el cliente perdió la conexión con el servidor mientras se ejecutó la tarea. El estado de la tarea no se puede determinar. • Running (En ejecución): realizando la tarea. • Pendiente: a la espera de que finalice otra tarea.
Propietario	El usuario que inició la tarea.
Progreso	Muestra el progreso de la tarea.
Servidor	Disponible al conectarse a varios servidores. Muestra el servidor de AXIS Camera Station Pro que realiza la tarea.

Para gestionar una o varias tareas:

1. Haga clic en  **Alarms and Tasks (Alarmas y Tareas)** en la parte inferior del cliente de AXIS Camera Station Pro y haga clic en la pestaña **Tasks (Tareas)**.
2. Seleccione las tareas y haga clic en una de las acciones

	Haga clic para mostrar el cuadro de diálogo de resultado de la tarea.
	Haga clic para cancelar la tarea.
	Haga clic para eliminar las tareas de la lista.
	Si la tarea produce un error cuando exporte grabaciones o cree informes de incidentes, haga clic para volver a intentar realizar la tarea.

Resultado de la tarea

Si una tarea se realizó en varios dispositivos, el cuadro de diálogo muestra los resultados para cada dispositivo. Todas las operaciones con un fallo deben revisarse y configurarse manualmente.

En la mayoría de las tareas, aparecen los siguientes detalles. En el caso de tareas como exportar grabaciones y crear el informe del sistema, haga doble clic en la tarea para abrir la carpeta con los archivos guardados.

Dirección MAC	La dirección MAC del dispositivo actualizado.
Dirección	La dirección IP del dispositivo actualizado.
Mensaje	Información sobre la ejecución de la tarea: <ul style="list-style-type: none"> • Finalizado: la tarea se ha completado correctamente. • Error: la tarea no ha podido completarse en el dispositivo. • Cancelado: la tarea se canceló antes de que llegara a completarse.
Descripción	Información sobre la tarea.

En función del tipo de tarea realizada, se muestran los siguientes detalles:

Nueva dirección	La nueva dirección IP asignada al dispositivo actualizado.
Reglas de actuación	La versión del firmware y el nombre de producto del dispositivo.
Detalles	El número de serie y la dirección IP del dispositivo sustituido y el número de serie y la dirección IP del nuevo dispositivo.
Reference ID (ID de referencia):	El ID de referencia del informe de incidencias.

Generar informes

Página de configuración del cliente

La hoja de configuración del cliente es útil para solucionar problemas y ponerse en contacto con el soporte técnico.

Para ver un informe en formato HTML con una descripción general de la configuración del sistema del cliente:

1. Vaya a **Configuration (Configuración) > Server (Servidor) > Diagnostics (Diagnóstico)**.
2. Haga clic en **View client configuration sheet (Ver hoja de configuración del cliente)**.

Página de configuración del servidor

La página de configuración del servidor incluye información sobre la configuración general, los ajustes de cámara, incluidas las reglas de acción, programaciones, almacenamiento de grabaciones, dispositivos auxiliares y licencias. Esto resulta útil para solucionar problemas y al conectar con el servicio de asistencia.

Para ver un informe en formato HTML con una descripción general de la configuración del sistema del servidor:

1. Vaya a **Configuration (Configuración) > Server (Servidor) > Diagnostics (Diagnóstico)**.
2. Haga clic en **View server configuration sheet (Ver hoja de configuración del servidor)**.

Informe del sistema

El informe del servidor es un archivo .zip que contiene parámetros y archivos de registros que ayudarán al departamento de atención al cliente de Axis a analizar el sistema.

Al ponerse en contacto con el departamento de atención al cliente, incluya siempre un informe del sistema.

Para generar el informe del sistema:

1. Visite el menú de la esquina superior derecha.
2. Haga clic en **Help (Ayuda) > System report (Informe del sistema)**.
3. Edite el nombre del archivo si desea cambiar de nombre el archivo generado automáticamente.
4. Haga clic en **Explorar** para seleccionar dónde guardar el informe del sistema.
5. Seleccione sus ajustes preferidos:
 - **Automatically open folder when report is ready (Abrir carpeta automáticamente cuando el informe esté listo)** para consultarlo directamente.
 - **Include all databases (Incluir todas las bases de datos)** para añadir información detallada sobre grabaciones y datos del sistema.
 - **Include screenshots of all monitors (Incluir capturas de pantalla de todos los monitores)** para simplificar el análisis del informe del sistema.
6. Haga clic en **Aceptar**.



Para ver este vídeo, vaya a la versión web de este documento.

Generación de un informe del sistema

AXIS Installation Verifier

AXIS Installation Verifier inicia una prueba de rendimiento después de la instalación para verificar que todos los dispositivos del sistema estén plenamente operativos. La prueba dura unos 20 minutos.

Pruebas	
Condiciones normales	Compruebe el streaming de datos y el almacenamiento de datos utilizando los ajustes del sistema actual en AXIS Camera Station Pro. Salida: Aprobado o suspenso.
Condiciones con poca luz	Comprobación de la transmisión y del almacenamiento de datos utilizando los ajustes optimizados para unas condiciones de poca luz típicas, por ejemplo, los ajustes de ganancia. Salida: Aprobado o suspenso.
Prueba de estrés	Prueba que aumenta la transmisión y el almacenamiento de datos paso a paso, hasta que el sistema alcanza su límite máximo. Salida: Información acerca del rendimiento máximo del sistema.

Nota

- Solo puede probar dispositivos compatibles con AXIS Camera Application Platform 2 (ACAP 2) y posteriores.
- Durante la prueba, AXIS Camera Station Pro pasa al modo de mantenimiento y todas las actividades de vigilancia no están disponibles temporalmente.

Para empezar la prueba:


1. Vaya a **Configuration (Configuración) > Server (Servidor) > Diagnostics (Diagnóstico)**.
2. Haga clic en **Open AXIS installation verifier... (Abrir AXIS Installation Verifier...)**.
3. Haga clic en **Iniciar**.
4. Cuando termine la prueba, haga clic en **View report (Ver informe)** para ver el informe o haga clic en **Save report (Guardar informe)** para guardarlo.

Lista de activos

Puede exportar una lista de activos para el sistema de gestión de vídeo. La lista de activos incluye el nombre, tipo, modelo, estado y número de serie de lo siguiente:

- Todos los servidores conectados
- Todos los dispositivos conectados
- El terminal de cliente desde el que exportó la lista de activos al conectarse a varias terminales

Para exportar una lista de activos:

1. Vaya a  > **Other > Asset list (Otro > Lista de activos)**.
2. Haga clic en **Exportar**.
3. Seleccione la ubicación del archivo y haga clic en **Guardar**.
4. En **Última exportación**, aparece o se actualiza un enlace al archivo.
5. Haga clic en el enlace para ir a la ubicación del archivo.


Ajustes de cámara corporal

Para conectarse con un sistema corporal, debe crear un archivo de conexión. Consulte *Configuración de un sistema corporal de Axis*.

Nota

Antes de crear el archivo de conexión, renueve el certificado de servidor si la dirección IP del servidor ha cambiado o si AXIS Camera Station se actualizó desde una versión anterior a la 5.33. Para obtener información sobre cómo renovar el certificado, consulte *Certificados, on page 141*.

Para crear un archivo de conexión:

1. Vaya a  > Other > Body worn settings (Otro > Ajustes de sistemas corporales).
2. Para cambiar el nombre de instalación predeterminado mostrado en el sistema corporal, introduzca un nuevo nombre.
3. Haga clic en Exportar.
4. En Última exportación, aparece o se actualiza un enlace al archivo.
5. Haga clic en el enlace para ir a la ubicación del archivo.



Configuración de un sistema corporal de Axis



Reproducción y exportación de grabaciones de una cámara corporal de Axis

Estado de los servicios de Axis

Para consultar el estado de los servicios en línea de Axis:

1. Vaya a Configuration (Configuración) > Server (Servidor) > Diagnostics (Diagnóstico).
2. Haga clic en View status of Axis services (Ver el estado de los servicios de Axis).




AXIS Camera Station Pro control de servicio

El servidor usa control de servicio AXIS Camera Station Pro para iniciar y detener y para cambiar sus ajustes. Se inicia automáticamente una vez completada la instalación. Si se reinicia el equipo servidor, el control de servicio se reinicia automáticamente en aproximadamente 2 minutos. Un icono en el área de notificación de Windows muestra el estado del servicio.

Haga clic derecho en el icono y seleccione **Abrir control de servicio de AXIS Camera Station**, **Iniciar servicio**, **Detener servicio**, **Reiniciar servicio** o **Salir**.

Para abrir el control de servicio desde el menú de inicio:

Vaya al menú **Start (Inicio)** y seleccione **All Programs > Tools > Service Control** (Todos los programas > Herramientas > Control de servicio).

	<p>En ejecución</p>
	<p>Iniciando</p>
	<p>Detenida</p>

Modificar configuración	Seleccione para poder cambiar la configuración del servidor.
Configuración por defecto	Haga clic para restaurar todos los ajustes a la configuración predeterminada original.
Start (Inicio)	Haga clic para cambiar el estado del servidor.
Parada	
Reinicio	Haga clic para reiniciar el servidor.

General

En controles de servicio de AXIS Camera Station Pro, seleccione **Modify settings (Modificar ajustes)** y haga clic en **General** para cambiar la configuración general del servidor.

Configuración de puertos del servidor	
Nombre del servidor	El nombre del servidor. El nombre del servidor se muestra en el cliente de software. El nombre del servidor predeterminado es el nombre del equipo. El nombre no cambia si se modifica el nombre del ordenador.
Puerto cliente web	El cliente web para AXIS Camera Station utiliza este puerto.
Intervalo de puertos	Especifique el intervalo de puertos. El resto de los puertos cambia automáticamente.
Allow (permitir) AXIS Camera Station Pro para añadir excepciones al cortafuegos de Windows	Seleccione esta opción si desea permitir permitir que AXIS Camera Station Pro agregue automáticamente excepciones al cortafuegos de Windows cuando un usuario cambie el intervalo de puertos.

Nota

- Si entre el servidor y el cliente hay un NAT, cortafuegos o similar, configure el NAT o cortafuegos para permitir el paso de estos puertos.
- Los números de puerto deben estar dentro del intervalo 1024-65534.

Lista de puertos para AXIS Camera Station Pro

En las siguientes tablas se muestran qué puertos y protocolos usa AXIS Camera Station Pro. Es posible que tenga que permitir esto en el cortafuegos para un rendimiento y una usabilidad óptimos. Calculamos los números de puerto en función del puerto principal HTTP, 29200.

Servidor a dispositivos

Puerto	Número	Protocolo	Entrada/salida	Descripción
Puertos HTTP y HTTPS principales	80 y 443	TCP	Salida	Se utiliza para transmisiones de vídeo y datos de dispositivos.
Puerto bonjour predeterminado	5353	UDP	Multicast (entrada y salida)	Se utiliza para detectar dispositivos con

				<p>mDNS Discovery (Bonjour). Multicast 224.0.0.251.</p> <p>Si no se puede establecer el enlace con el puerto predeterminado, el motivo puede ser que otra aplicación lo utiliza y rechaza compartirlo. En ese caso, se utiliza un puerto aleatorio. Bonjour no detecta dispositivos con direcciones de enlace local cuando se utiliza un puerto aleatorio.</p>
Puerto SSDP predeterminado	1900	UDP	Multicast (entrada y salida)	<p>Se usa para detectar dispositivos con SSDP (UPNP).</p> <p>Multicast 239.255.255.250.</p>
Puerto WS-Discovery predeterminado	3702	UDP	Multicast (entrada y salida)	<p>La detección de servicios web WS-Discovery se usa para detectar dispositivos Onvif.</p> <p>Multicast 239.255.255.250.</p>

Ciente al servidor

Puerto	Número	Protocolo	Entrada/salida	Comunicación entre	Descripción
Puerto HTTP de transmisión	29200	TCP	Entrada	Servidor y cliente	Se usa para transmisiones de vídeo, audio y metadatos (cifrado AES).
Puerto TCP principal	29202	TCP	Entrada	Servidor y cliente	<p>Desplazamiento de más 2 desde el puerto HTTP de transmisión.</p> <p>Se usa para datos de aplicación (cifrado TLS 1.2).</p>

Puerto de servidor web API	29204	TCP	Entrada	Servidor y aplicación móvil	Desplazamiento de más 4 desde el puerto HTTP de transmisión. Se usa para datos de aplicación y transmisión de vídeo MP4 a través de HTTPS.
Puerto de medios de API	29205	TCP	Entrada	Servidor y aplicación móvil	Desplazamiento de más 5 desde el puerto HTTP de transmisión. Se usa para transmisión de vídeo a través de HTTP.

Puerto HTTP de proxy local	29206	TCP	Entrada	Comunicación interna en el servidor	<p>Desplazamiento de más 6 desde el puerto HTTP de transmisión (ServerPortParser).</p> <p>Desplazamiento de más 2 desde el puerto del servidor web de la API (RemoteFacadeBinder).</p> <p>Solo se puede acceder internamente en AXIS Camera Station Pro el equipo servidor.</p> <p>Puerto para solucionar un problema desconocido. Las aplicaciones móviles hacen llamadas al módulo SRA, que recibe HTTPS, lo convierte en HTTP y lo vuelve a enviar al puerto HTTP de proxy local y al puerto de medios de la API.</p>
Puerto del extremo del proxy web	29207	TCP	Entrada	Servidor y componente	<p>Desplazamiento de más 7 desde el puerto HTTP de transmisión.</p> <p>Se usa para la comunicación segura entre el componente y los dispositivos.</p>

Dominios y puertos para el acceso remoto seguro v2

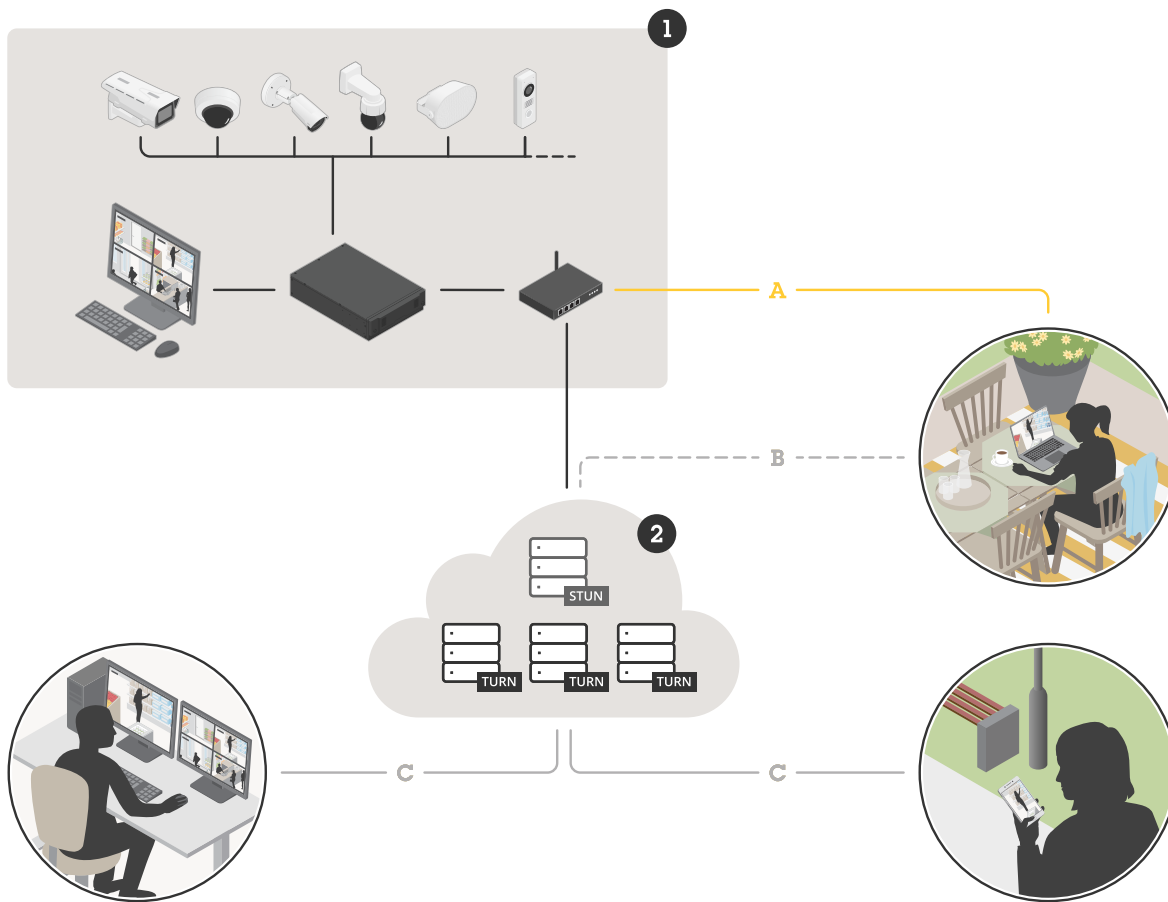


Imagen: Descripción general de la solución SRA v2 en AXIS Camera Station Pro

1. Instalación supervisada en red local con cliente de visualización local
 - A: conexión remota (entre iguales)
 - B: conexión temporal STUN/TURN a los servicios conectados a Axis Cloud

Nombre o tipo	Dirección	Número de puerto	Protocolo	Dirección
SRA v2: Inicio de sesión en MyAxis	https://eu.login.connect.axis.com	443	TCP	Comunicaciones entrantes y salientes
SRA v2: comunicación con el servicio en la nube	https://eu.cs.connect.axis.com	443	TCP	Comunicaciones entrantes y salientes
SRA v2: comunicación API con el servicio en la nube	https://api.vms.axis.cloud	443	TCP	Comunicaciones entrantes y salientes
Componente EdgeHost	75.2.119.140	443, 8443	-	Comunicaciones entrantes y salientes

Componente EdgeHost	99.83.133.42	443, 8443	-	Comunicaciones entrantes y salientes
Componente EdgeHost	cep.connect.axis.com	443, 8443	-	Comunicaciones entrantes y salientes

2. Servicios conectados a Axis Cloud

- C: conexión remota TURN a los servicios conectados a Axis Cloud

Nombre o tipo	Dirección	Número de puerto	Protocolo	Dirección
Comunicación con el proxy P2P y el componente WebRTC	wss://signaling.prod.webrtc.connect.axis.com	443	TCP	Comunicaciones entrantes y salientes
Comunicación con el proxy P2P y el componente WebRTC	https://*.turn.prod.webrtc.connect.axis.com	443, 3478, 5349, 49152-65535	TCP	Comunicaciones entrantes y salientes

Reservado para componentes

Componente	Escucha en la interfaz	Puerto	Número	Protocolo	Entrada/salida	Comunicación entre	Descripción
Entrada segura	localhost (127.0.0.1)	Puerto de servidor web	29214	HTTPS	Entrada	Cliente (pestaña de gestión de acceso) y componente	Desplazamiento de más 14 desde el puerto HTTP de transmisión. En las instalaciones más antiguas se utilizaba el puerto 8081.
Entrada segura	Todos (0.0.0.0/INADDR_ANY)	Puerto de servidor web	29215	HTTPS	Entrada	Servidor principal y servidores secundarios	Desplazamiento de más 15 desde el puerto HTTP de transmisión. Se utiliza para la comunicación entre el servidor principal y

Compo- nente	Escucha en la interfaz	Puerto	Número	Protocolo	Entrada/ salida	Comunica- ción entre	Descrip- ción
							los servidores secundarios en la configuración de varios servidores.
Supervisión del estado del sistema	Todos (0.0.0.0/INADDR_ANY)	Puerto de servidor web	29216	HTTPS	Entrada	Cliente (pestaña System Health Monitoring) y componente	Desplazamiento de más 16 desde el puerto HTTP de transmisión. Se usa para alojar páginas web de supervisión del estado del sistema y para compartir datos en una configuración multisistema.
Servicio en la nube de Supervisión del estado del sistema	localhost	Puerto de servidor web	29217	HTTPS	Entrada	AXIS Camera Station Pro (página web) y backend de CloudService (complemento)	Desplazamiento de más 17 desde el puerto HTTP de transmisión. Se utiliza para el servicio en la nube de supervisión del estado del sistema para habilitar la supervisión del estado del sistema.
Búsqueda inteligente 2	localhost	Puerto de servidor web	29218	HTTPS	Entrada	Cliente (pestaña de	Desplazamiento de más 18

Compo- nente	Escucha en la interfaz	Puerto	Número	Protocolo	Entrada/ salida	Comunica- ción entre	Descrip- ción
						búsqueda inteligente) y componen- te	desde el puerto HTTP de transmi- sión. Se usa para alojar la API de la búsqueda inteligente y proporci- onar la página web del cliente.
Núcleo de la API de VMS	127.0.0.1, ::1	API de GraphQL	29219	GraphQL	Entrada	Clientes de API de VMS y GraphQL	Desplaza- miento de más 19 desde el puerto HTTP de transmi- sión. Se utiliza para exponer ACS como una API de GraphQL a un cliente
			29222				Reservado para uso futuro.
Cliente web	localhost	Puerto de servidor web	29223	HTTPS	Entrada	WebClient a API de VMS/ Cliente incorpora- ble	Desplaza- miento de más 23 desde el puerto HTTP de transmi- sión. Como actúa como proxy delante de la API configura- ble de VMS.
Cliente incorpora- ble	localhost	Puerto de servidor web	29224	HTTPS	Entrada	Cliente incorpora- ble en el servidor de señales/ streamer API de	Desplaza- miento de más 24 desde el puerto HTTP de

Compo- nente	Escucha en la interfaz	Puerto	Número	Protocolo	Entrada/ salida	Comunica- ción entre	Descrip- ción
						VMS/ WebRTC	transmi- sión. Como actúa como proxy delante de la API de VMS.
Configura- ción del cliente web	localhost	Puerto de servidor web	29225	HTTPS	Entrada	AXIS Camera Station Pro cliente (página web)	Desplaza- miento de más 25 desde el puerto HTTP de transmi- sión. Se utiliza para alojar la página web de configura- ción del cliente web y backend.
Configura- ción de cliente incorpora- ble	localhost	Puerto de servidor web	29226	HTTPS	Entrada	AXIS Camera Station Pro cliente (página web)	Desplaza- miento de más 26 desde el puerto HTTP de transmi- sión. Se utiliza para alojar la página web de configura- ción del cliente incorpora- ble web y backend.
			29227				Reservado para uso futuro.
Generador de configura- ción ICE local	localhost	Puerto de servidor web	29228	HTTPS	Entrada	Servidor de señales al generador de configura- ción ICE	Desplaza- miento de más 28 desde el puerto HTTP de transmi- sión. Parte del

Compo- nente	Escucha en la interfaz	Puerto	Número	Protocolo	Entrada/ salida	Comunica- ción entre	Descrip- ción
							componen- te WebRTC en las instalacio- nes
Configura- ción de WebRTC local	localhost	Puerto de servidor web	29229	HTTPS	Entrada	AXIS Camera Station Pro cliente (página web)	Desplaza- miento de más 29 desde el puerto HTTP de transmi- sión. Se utiliza para alojar la página web de configura- ción de WebRTC y backend. Parte del componen- te WebRTC en las instalacio- nes
Servidor TURN local	localhost	puerto del servidor coturn	29230	UDP	Inbound/ Outbound (Entrada/ Salida)	Client/ WebClient incorpora- ble ↔ Servidor TURN	Desplaza- miento de más 30 desde el puerto HTTP de transmi- sión. Se utiliza para "WebRTC de puerto único" en ACS en las instalacio- nes
			29231				Reservado para uso futuro.
IAM local (IDP)	0.0.0.0	IDP_OIDC (público)	29232	HTTPS	Entrada	Proxy inverso e IAM local	Desplaza- miento de más 32 desde el puerto HTTP de transmi- sión.

Compo- nente	Escucha en la interfaz	Puerto	Número	Protocolo	Entrada/ salida	Comunica- ción entre	Descrip- ción
							Puerto público.
IAM local (IDP)	0.0.0.0	MTLS (adminis- trador)	29233	HTTPS	Entrada	Servicios de terceros	Desplaza- miento de más 33 desde el puerto HTTP de transmi- sión. Puerto de administra- dor.
IAM local (IDP)	127.0.0.1	TOKENIZER	29234	HTTPS	Entrada	Servicios de terceros	Desplaza- miento de más 34 desde el puerto HTTP de transmi- sión. Puerto tokenizer.
WebRTC	localhost	API de integración	29235	HTTPS	Entrada	Componen- te de la nube	Desplaza- miento de más 35 desde el puerto HTTP de transmi- sión. Lo utiliza la integración para configurar la conexión a la nube de webrtc. Parte del componen- te de WebRTC.
Telemetría abierta	127.0.0.1	Puerto gRPC	29236	gRPC	Entrada	Servicios de terceros	Desplaza- miento de más 36 desde el puerto HTTP de transmi- sión.
Telemetría abierta	127.0.0.1	Puerto HTTP	29237	HTTPS	Entrada	Servicios de terceros	Desplaza- miento de

Compo- nente	Escucha en la interfaz	Puerto	Número	Protocolo	Entrada/ salida	Comunica- ción entre	Descrip- ción
							más 37 desde el puerto HTTP de transmisión.
Audio Manager Pro		Puerto de servidor web	29238	HTTPS	Entrada	Servicios y componentes de integración de terceros	Desplazamiento de más 38 desde el puerto HTTP de transmisión.
			29239				Reservado para uso futuro.
			29240				Reservado para uso futuro.
Panel de información	localhost	2dpc/3dpc push Receptor	29241	HTTPS	Entrada (externo)	Receptor de mensajes Push (post) que contienen datos de recuento de 2dpc y 3dpc. Internamente: base de datos, broker Mosquitto	Desplazamiento de más 41 desde el puerto HTTP de transmisión.
Panel de información	0.0.0.0	Broker Mosquitto	29242	MQTT	Entrada (externo) Salida (externo)	Receptor de mensajes de eventos de la cámara. Posibilidad de puentear brokers MQTT si es necesario (de muchos a uno, por ejemplo, usando el tema.	Desplazamiento de más 42 desde el puerto HTTP de transmisión.

Compo- nente	Escucha en la interfaz	Puerto	Número	Protocolo	Entrada/ salida	Comunica- ción entre	Descrip- ción
						«Duplica- ción» de la base de datos y equilibrio de carga disponibles para los servicios profesiona- les al configurar una instalación) Interna- mente: Receptor	
			29243				Reservado para uso futuro.
Interme- diario de NATS	127.0.0.1	NATS	29244	NATS	Entrada	Entre AXIS Camera Station Pro y los componen- tes, y entre los propios componen- tes	Desplaza- miento de más 44 desde el puerto HTTP de transmi- sión.
Telemetría abierta	127.0.0.1	Puerto HTTP	29245	HTTP	Entrada	Extremo de supervisión para obtener métricas del recopilador de telemetría abierto	Desplaza- miento de más 45 desde el puerto HTTP de transmi- sión.

Compo- nente	Escucha en la interfaz	Puerto	Número	Protocolo	Entrada/ salida	Comunica- ción entre	Descrip- ción
Puerta de enlace API	Todos (0.0.0.0/ INADDR_ ANY)	Puerto alternativo de proxy inverso utilizado por el host en el extremo	29248	HTTPS	Entrada	Host en el extremo y proxy inverso	Desplaza- miento de más 48 desde el puerto HTTP de transmi- sión.
Puerta de enlace API	Todos (0.0.0.0/ INADDR_ ANY)	Puerto de respaldo alojado con certificados de servidor ACS, usado como comunica- ción de respaldo para el cliente Windows de ACS	29250	HTTPS	Entrada	Cliente ACS y puerta de enlace API	Desplaza- miento de más 50 desde el puerto HTTP de transmi- sión.

Otros puertos

Puerto	Número	Protocolo	Entrada/salida	Comunicación entre	Descripción
HTTPS de Internet	80 y 443	TCP	Salida	Cliente y servidor con Internet	Se usa para activar licencias, descargar firmware, para servicios conectados, etc.
Puerto de transmisión TCP del servidor	29198	TCP	Entrada	Servidor y dispositivo	Desplazamiento de menos 2 desde el puerto HTTP de transmisión.
Puerto UDP de estado de actualización	15156	UDP	Entrada y salida	Control de servidor y servicio	AXIS Camera Station Pro el control de servicio escucha en el puerto y el servidor transmite el estado de una actualización en curso.

Base de datos

Archivos de base de datos

Core database files (Archivos de base de datos del núcleo)

AXIS Camera Station Pro almacena los archivos de la base de datos principal en `C:\ProgramData\AXIS Communications\AXIS Camera Station Server`.

Para versiones anteriores a la 5.13 de AXIS Camera Station, hay un único archivo de base de datos: **ACS.FDB**.

Para la versión 5.13 o posterior de AXIS Camera Station, hay tres archivos de base de datos:

- **ACS.FDB**: Este archivo de base de datos principal contiene la configuración del sistema, como dispositivos, vistas, permisos, eventos y perfiles de flujo.
- **ACS_LOGS.FDB**: Este archivo de base de datos de registros contiene referencias a los registros.
- **ACS_RECORDINGS.FDB**: Este archivo de base de datos de grabaciones contiene los metadatos y referencias a las grabaciones almacenadas en la ubicación especificada en **Configuration > Storage (Configuración > Almacenamiento)**. AXIS Camera Station Pro requiere este archivo para mostrar las grabaciones en la línea de tiempo durante la reproducción.

Component database files (Archivos de base de datos de los componentes)

SecureEntry.db – El archivo de base de datos AXIS Secure Entry contiene todos los datos de control de acceso excepto las fotografías de los titulares de tarjetas. Se guarda en `C:\ProgramData\Axis Communications\AXIS Camera Station\Components\AXIS Secure Entry\INTERNAL\main_db`.

smartSearch.sqlite3 – El archivo de base de datos de búsqueda inteligente contiene la configuración de la cámara y filtros de búsqueda guardados. Se guarda en `C:\ProgramData\Axis Communications\AXIS Smart Search\data`.

Configuración de la base de datos

La base de datos crea una copia de seguridad cada noche y antes de la actualización de cada sistema. En control de servicio de AXIS Camera Station Pro, seleccione **Modify settings (Modificar ajustes)** y haga clic en **Database (Base de datos)** para cambiar los ajustes de copia de seguridad.

<p>Carpeta de copias de seguridad</p>	<p>Haga clic en Browse (Examinar) y seleccione dónde guardar las copias de seguridad de la base de datos. Reinicie el servidor de AXIS Camera Station Pro para aplicar el cambio.</p> <p>Si la ruta de la carpeta de copia de seguridad es incorrecta o AXIS Camera Station Pro no tiene acceso a la unidad de red, la copia de seguridad se guarda en <code>C:\ProgramData\Axis Communications\AXIS Camera Station Server\backup</code>.</p>
<p>Días para guardar las copias de seguridad</p>	<p>Especifique el número de días para guardar las copias de seguridad. Se puede utilizar cualquier número entre 1 y 30. El valor predeterminado es 14 días.</p>
<p>Progreso de la actualización</p>	<p>Haga clic View details (Ver detalles) para ver los detalles sobre la última actualización de la base de datos. Incluye eventos que se han producido desde la última vez que se reinició el control de servicio de AXIS Camera Station Pro.</p>

Base de datos de copia de seguridad

La base de datos contiene información acerca de grabaciones y otros metadatos necesarios para que el sistema funcione correctamente.

Importante

- La base de datos no almacena las grabaciones, sino que especifica una ubicación en **Configuration > Storage (Configuración > Almacenamiento)** para almacenarlas. Una copia de seguridad de las grabaciones de forma independiente.
- Los ajustes del servidor y la base de datos en el control de servicio de AXIS Camera Station Pro no se guardan.

Copia de seguridad del sistema

El sistema guarda automáticamente la copia de seguridad del sistema en la carpeta especificada en la pestaña **Database (Base de datos)**, consulte *Configuración de la base de datos, on page 228*. Una copia de seguridad del sistema incluye los archivos de la base de datos del núcleo y los archivos de la base de datos de los componentes, consulte *Archivos de base de datos, on page 228*.

Archivos de copia de seguridad	
System_YYYY-MM-DD-HH-mm-SSSS.zip	Una copia de seguridad activada por la noche.
PreUpgrade_YYYY-MM-DD-HH-mm-SSSS.zip	Una copia de seguridad activada antes de una actualización de la base de datos.
User_YYYY-MM-DD-HH-mm-SSSS.zip	Una copia de seguridad activada antes de eliminar un almacenamiento.

En el archivo .zip, puede encontrar los siguientes archivos:

ACS	Esta carpeta incluye los archivos de la base de datos principal ACS.FDB, ACS_LOGS.FDB y ACS_RECORDINGS.FDB.
Componentes	Esta carpeta solo está disponible si utiliza un componente. Por ejemplo, AXIS Camera Station Secure Entry o búsqueda inteligente. <ul style="list-style-type: none"> • webrtc: Esta carpeta contiene archivos de configuración WebRTC. • ACMSM: esta carpeta incluye el archivo de base de datos de AXIS Camera Station Secure Entry SecureEntry.db y las fotos de los titulares de tarjetas. • Búsqueda inteligente: Esta carpeta incluye el archivo de base de datos de búsqueda inteligente smartSearch-backup-yyyyMMddHHmssfff.sqlite3.
backup_summary.json	en estos archivos se incluye información más detallada sobre la copia de seguridad.
_cluster_yyyyMMddHHmssfff.dbcbackup	Este archivo contiene una copia de seguridad lógica del clúster de bases de datos PostgreSQL, que incluye datos de todo el clúster, como roles y espacios de tabla.

Copia de seguridad de mantenimiento

Especifique la carpeta de copia de seguridad para almacenar las copias de seguridad de mantenimiento en la pestaña **Database (Base de datos)**, consulte *Configuración de la base de datos, on page 228*. Una copia de seguridad de mantenimiento incluye los archivos de la base de datos principal, y cada archivo de la base de datos está en una carpeta aparte `PreMaintenance_YYYY-MM-DD-HH-mm-SSSS`.

Se puede activar de distintas maneras:

- Automáticamente al actualizar AXIS Camera Station Pro.
- Cuando ejecute manualmente el mantenedor de la base de datos manualmente desde el control de servicio de AXIS Camera Station Pro. Vea *Mantenimiento de la base de datos, on page 231*.
- Automáticamente mediante la tarea de mantenimiento de la base de datos programada configurada en el Programador de tareas de Windows. Vea *Herramientas, on page 233*.

Copia de seguridad manual

Nota

Una copia de seguridad manual solo puede realizar una copia de seguridad de los archivos de la base de datos del núcleo. No hace una copia de seguridad de los archivos de la base de datos de los componentes, por ejemplo, el archivo de base de datos de búsqueda inteligente.

Existen dos maneras de realizar una copia de seguridad manual:

- **Opción 1:** Vaya a `C:\ProgramData\AXIS Communications\AXIS Camera Station Server` y realice una copia de los archivos de la base de datos. A continuación, haga una copia de seguridad del clúster de bases de datos PostgreSQL:
 1. Abra un terminal como administrador en el directorio donde desee guardar la copia de seguridad.
 2. Ejecute `"C:\Program Files\Axis Communications\AXIS Camera Station\Core\DbConsole\DbConsole.exe" backup -cluster`
 3. La copia de seguridad se guarda en una carpeta llamada `yyyyMMddHHmmssfff` del directorio donde abrió el terminal.
- **Opción 2:** Genere un informe del sistema con todas las bases de datos incluidas y copie los archivos de copia de seguridad de la base de datos. Asegúrese de seleccionar **Incluir todas las bases de datos**. Vea *Informe del sistema, on page 209*.

Restaurar la base de datos

Si pierde la base de datos debido a un fallo de hardware u otros problemas, puede restaurar la base de datos a partir de las copias de seguridad guardadas. De forma predeterminada, el sistema mantiene los archivos de copia de seguridad durante 14 días. Para obtener más información sobre la copia de seguridad de la base de datos, consulte *Base de datos de copia de seguridad, on page 229*.

Nota

La base de datos no almacena las grabaciones, sino que especifica una ubicación en **Configuration > Storage (Configuración > Almacenamiento)** para almacenarlas. Una copia de seguridad de las grabaciones de forma independiente.

Para restaurar la base de datos:

1. Vaya al control de servicio de AXIS Camera Station Pro y haga clic en **Stop (Detener)** para detener el servicio.
2. Vaya a los archivos de copia de seguridad de la base de datos. Vea *Base de datos de copia de seguridad, on page 229*.
3. Extraiga los archivos.
4. Restaure el clúster de bases de datos PostgreSQL:

- 4.1. Abra un terminal como administrador en la carpeta extraída.
- 4.2. Ejecute "C:\Program Files\Axis Communications\AXIS Camera Station\Core\DbConsole\DbConsole.exe" restore -backup-file _cluster_YYYYMMddHHmssfff.dbcbbackup
- 4.3. Haga clic en **y** cuando se le solicite confirmar que confía en la fuente del archivo de copia de seguridad.
5. En la carpeta extraída, copie los siguientes archivos de la base de datos de ACS a C:\ProgramData\AXIS Communications\AXIS Camera Station Server\
 - ACS.FDB: Debe copiar este archivo para restaurar la base de datos.
 - ACS_LOGS.FDB: Copie este archivo si quiere restaurar registros.
 - ACS_RECORDINGS.FDB: Puede copiar este archivo si quiere restaurar grabaciones.
6. Si utiliza AXIS Camera Station Secure Entry, siga las instrucciones de RESTORE_INSTRUCTIONS.txt, que encontrará en C:\ProgramData\Axis Communications\AXIS Camera Station\Components\AXIS Secure Entry 2\INTERNAL\main_db.
7. Si utiliza la búsqueda inteligente, copie smartSearch-backup-YYYYMMddHHmssfff.sqlite3 de smartsearch a C:\ProgramData\Axis Communications\AXIS Camera Station\Components\AXIS Smart Search\data y cámbiele el nombre por smartSearch.sqlite3.
8. Si utiliza el cliente web del VMS, copie todos los archivos de webrtc a C:\ProgramData\Axis Communications\AXIS Camera Station\Components\WebRTC.
9. Vuelva al control de servicio de AXIS Camera Station Pro y haga clic en **Start (Iniciar)** para iniciar el servicio.

Mantenimiento de la base de datos

Realice el mantenimiento de la base de datos si aparece la alarma Database maintenance is required o si el sistema se apaga de manera imprevista, por ejemplo, tras un apagón.

Para iniciar el mantenimiento de la base de datos, consulte *Herramientas, on page 233*.

Nota

AXIS Camera Station Secure Entry utiliza DB Janitor para supervisar y comprimir el tamaño de los archivos de la base de datos si es necesario. El sistema de control de acceso deja de estar disponible temporalmente en los casos poco habituales de compresión forzada.

Recomendaciones para la base de datos

Para evitar problemas, tenga en cuenta lo siguiente:

Comprobar errores del disco – Los errores del disco pueden ocasionar daños en la base de datos. Utilice una herramienta como chkdsk (Comprobar disco, también conocido como Comprobación de errores) para buscar sectores dañados en el disco duro usado para la base de datos. Ejecute chkdsk con regularidad.

Software antivirus y copias de seguridad externas – No ejecute análisis de virus en la base de datos, ya que algún software de antivirus puede dañar la base de datos. Si utiliza un sistema de copia de seguridad externo, no realice una copia de seguridad de la base de datos activa y actual. En su lugar, cree una copia de seguridad a partir de los archivos de la carpeta de copia de seguridad.

Fallo de alimentación – Una desconexión imprevista, por ejemplo, debido a un apagón, puede dañar la base de datos. Utilice una SAI (fuente de alimentación ininterrumpida) para instalaciones críticas.

Falta de espacio – La base de datos podría resultar dañada si se agota el espacio del disco duro. Para evitarlo, instale el servidor de AXIS Camera Station Pro en un equipo dedicado con suficiente memoria. Para requisitos de hardware, consulte axis.com/products/axis-camera-station/hardware-guidelines.

Memoria RAM dañada – Ejecute la herramienta de diagnóstico de memoria de Windows periódicamente para buscar la existencia de errores en la memoria RAM.

Certificados

La pestaña **Certificates (Certificados)** permite gestionar los certificados de servidor para AXIS Camera Station Pro. Puede consultar información sobre el certificado de servidor actual, su fecha de caducidad, generar e importar nuevos certificados de servidor o exportar el actual. Los certificados de servidor se almacenan en **C:\ProgramData\Axis Communications\AXIS Camera Station Server\certs**.

Certificado de servidor

Generar	Crear un nuevo certificado de servidor autofirmado. Este sustituye al certificado anterior empleado por el servidor y requiere reiniciar el servidor para hacerse efectivo.
Importar...	Importar un certificado de servidor desde un archivo. Los formatos de archivo compatibles son PEM y PFX/PKCS12. La asistencia técnica también está limitada a RSA con claves de al menos 2048 bits.

Nota

Al importar un certificado con certificados intermedios en formato PEM, se espera que estos últimos se encuentren en el archivo .cer. Si crea sus propios certificados, consulte *Preparar certificados intermedios para importar*, on page 232.

Certificado actual

Recoge información sobre el certificado de servidor actual, empleado para verificar manualmente que el cliente se ha conectado al servidor correcto.

Ver	Consulte más información sobre el certificado de servidor.
Exportar...	Exporte el certificado de servidor como archivo PFX.

Generar un nuevo certificado de servidor

- Pulse la tecla de Windows + S para buscar y abrir el control de servicios de la AXIS Camera Station Pro.
- En la pestaña **Certificates (Certificados)**, haga clic en **Generate (Generar)** para componer un nuevo certificado de servidor.
- Reinicie el servidor para aplicar el nuevo certificado de servidor.

Preparar certificados intermedios para importar.

Para importar un certificado con certificados intermedios a la AXIS Camera Station Pro, combine el certificado de servidor y el certificado intermedio en un mismo archivo:

1. Abra uno de los certificados de servidor y el certificado intermedio en el bloc de notas. El contenido se estructurará del siguiente modo:


```
cert.cer
-----BEGIN CERTIFICATE-----
MIIFTDCCB....
-----END CERTIFICATE-----
```
2. Copie y pegue el contenido de un certificado en el otro y cambie la primera línea por **combined_cert.cer**:


```
combined_cert.cer
-----BEGIN CERTIFICATE-----
MIIFTDCCB....
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIE+zCCA+OgA.....
```

—END CERTIFICATE—

3. Guarde el archivo.

Herramientas

En control de servicio de AXIS Camera Station Pro, seleccione **Modify settings (Modificar ajustes)** y haga clic en **Tools (Herramientas)** para iniciar el mantenimiento de la base de datos y crear informes de sistema parciales.

Mantenedor de base de datos

- Abrir el control de servicio de AXIS Camera Station Pro.
- Haga clic en **Tools (Herramientas)**.
- En **Database maintainer (Mantenedor de base de datos)**, haga clic en **Run (Ejecutar)**.
- Se muestra el tiempo de inactividad estimado. Haga clic en **Sí** para continuar. Una vez iniciado el proceso no se puede cancelar.

Nota


- AXIS Camera Station Pro el servidor y todas las grabaciones en curso se detienen durante el mantenimiento. Después del mantenimiento, el servidor empieza automáticamente.
- No apague el equipo durante el mantenimiento.
- El mantenimiento de la base de datos requiere derechos de administrador en el equipo Windows.
- Si el mantenimiento de la base de datos no puede recuperar la base de datos, póngase en contacto con el servicio técnico de Axis.

Asegúrese de ejecutar el mantenimiento de la base de datos si aparece la alarma "Database maintenance is required" (Mantenimiento de la base de datos requerido) o si el sistema se apaga de manera imprevista, por ejemplo, tras un apagón.

El mantenimiento de la base de datos también se puede programar para ejecutarse automáticamente si habilita la "Tarea de mantenimiento de base de datos de AXIS Camera Station Pro" en el Programador de tareas de Windows. Puede editar el activador para personalizar cuándo y con qué frecuencia se ha de ejecutar el mantenedor de la base de datos.

Informe del sistema

El informe parcial del sistema es un archivo .zip que contiene parámetros y archivos de registros que ayudan al departamento de atención al cliente de Axis a analizar el sistema. Al ponerse en contacto con el departamento de atención al cliente, incluya siempre un informe del sistema. Para generar un informe de sistema completo,

vaya a  > **Help > System report (Ayuda > Informe del sistema)** en el cliente de AXIS Camera Station Pro.

Para generar un informe parcial del sistema:

1. Haga clic en **Ejecutar**.
2. Seleccione e introduzca la información solicitada en el cuadro de diálogo.
3. Haga clic en **Generar informe**.

Herramienta Informe del sistema	
Nombre de archivo	Introduzca un nombre de archivo para el informe del sistema.
Carpeta	Seleccione dónde guardar el informe del sistema.

Herramienta Informe del sistema	
Abrir carpeta automáticamente cuando el informe esté listo	Seleccione esta opción para abrir automáticamente la carpeta cuando el informe del sistema esté preparado.
Incluir la base de datos en el informe	Seleccione esta opción para incluir la base de datos en el informe del sistema. La base de datos de AXIS Camera Station Pro contiene información sobre las grabaciones y los datos necesarios para que el sistema funcione correctamente.

Registro de red

- Haga clic en el enlace para descargar una aplicación de análisis del protocolo de red.
- Tras instalarla, haga clic en **Start (Iniciar)** para iniciar la aplicación.

Restablecer la autoridad de certificación

- Haga clic en **Reset (Restablecer)** para generar una nueva autoridad de certificación y reiniciar el servicio.
- Una vez reiniciado el servicio, podrá iniciar sesión e importar una autoridad de certificación personalizada si fuera preciso.

Localización de problemas

Acerca de esta guía

Esta guía es una recopilación de problemas relacionados con AXIS Camera Station Pro y cómo solucionarlos. Hemos puesto los problemas en un tema relacionado para que resulte más fácil encontrar lo que se busca. Un tema puede ser, por ejemplo, audio o visualización en directo. En cada problema se describe una solución.

Descubrir más

Consulte axis.com/support para

- Preguntas frecuentes
- Requisitos de hardware
- Actualizaciones de software
- Tutoriales, material de formación y otra información útil

Reiniciar el servicio de servidor

Reiniciar el servicio del servidor de AXIS Camera Station Pro puede resolver algunos problemas generales.

Nota

- Reiniciar el servicio del servidor puede llevar un tiempo y no hay forma de cancelar el reinicio.
- El servidor no estará disponible mientras se reinicia el servicio del servidor.
- Todos los dispositivos conectados pierden la conexión con el servidor mientras se reinicia el servicio del servidor.

Para reiniciar el servicio del servidor:

1. Vaya a **Configuration (Configuración) > Server (Servidor) > Diagnostics (Diagnóstico)**.
2. Haga clic en **Restart AXIS Camera Station server service...** (Reiniciar el servicio del servidor de AXIS Camera Station...).

El servicio de AXIS Camera Station Pro

El servicio se reinicia a menudo

El servidor se puede sobrecargar, lo que genera una cola de tareas larga y puede que también dañe las bases de datos.

- En la gestión de recursos del sistema, compruebe si AXIS Camera Station Pro o cualquier otra aplicación utiliza un elevado número de recursos.
- Ejecute el mantenedor de la base de datos, vaya a *Database maintenance (Mantenimiento de la base de datos)* en el manual del usuario de AXIS Camera Station Pro.

Si nada de lo anterior ayuda, contacte con el servicio de soporte técnico de Axis. Vaya a *Proceso de escalada*, on page 251.

Dispositivos en el sistema de gestión de vídeo

Problemas habituales

No se puede contactar con la cámara	
El VMS no puede contactar con la cámara. Las cámaras mostradas no se agregaron.	<ol style="list-style-type: none"> 1. Asegúrese de que la cámara tenga conexión de red, de que haya alimentación y de que la cámara se ejecute. 2. Vaya a Configuration > Add devices (Configuración > Agregar dispositivos) e intente agregar la cámara de nuevo.
Se ha cancelado la instalación	
El usuario ha cancelado la instalación. Las cámaras mostradas no se agregaron.	Para agregar cámaras, vaya a Configuración > Agregar dispositivos .
Error al configurar la contraseña en la cámara	
No se puede definir la contraseña para las cámaras mostradas.	<ol style="list-style-type: none"> 1. Para definir la contraseña manualmente, vaya a Configuration > Devices > Management (Configuración > Dispositivos > Gestión). 2. Haga clic con el botón derecho en la cámara y seleccione User Management > Set password (Gestión de usuarios > Configurar contraseña).

No se puede agregar el dispositivo

Si el dispositivo se estaba utilizando en un sistema diferente antes de agregarlo a AXIS Camera Station Pro:

- Realice la configuración predeterminada de fábrica del dispositivo.

Si el dispositivo todavía no se puede agregar al sistema de gestión de vídeo, pruebe a agregar el dispositivo a AXIS Device Manager.

Puede agregar otro modelo de dispositivo que el que desea agregar:

- Si el dispositivo es un nuevo producto o tiene un firmware de reciente publicación, puede tratarse de un problema de compatibilidad. Asegúrese de utilizar la versión de software más reciente de AXIS Camera Station Pro.

Si no es posible agregar otro modelo de dispositivo:

- Solucione problemas de la cámara, vaya a axis.com/support/troubleshooting.

No es posible actualizar el firmware del dispositivo a través de AXIS Camera Station Pro

No es posible actualizar la cámara desde la interfaz web:

- Solucione problemas de la cámara, vaya a axis.com/support/troubleshooting.

No se puede actualizar el firmware para todos los dispositivos:

- Asegúrese de que haya una conexión de red.
- Si no se trata de un problema relacionado con la red, contacte con el servicio técnico de Axis. Vaya a *Proceso de escalada, on page 251*.

No se puede actualizar el firmware para algunos modelos específicos:

- Puede ser un problema de compatibilidad, póngase en contacto con el servicio de soporte técnico de Axis. Vaya a *Proceso de escalada*, on page 251.

No se han encontrado dispositivos

El sistema de gestión de vídeo busca automáticamente cámaras y codificadores de vídeo conectados en la red, pero no encuentra ninguna cámara.

- Asegúrese de que la cámara tiene conexión a la red y de que recibe alimentación.
- Si el cliente, servidor o las cámaras se encuentran en redes diferentes, configure ajustes de proxy y cortafuegos.
 - Cambie los ajustes del proxy del cliente si un servidor proxy separa el cliente y el servidor. Vaya a *Ajustes del proxy cliente* en el manual del usuario de AXIS Camera Station Pro.
 - Cambie el NAT o el sistema de seguridad si un NAT y o sistema de seguridad separa el cliente y el servidor. Asegúrese de permitir que el HTTP port (Puerto HTTP), el puerto TCP (Protocolo de control de transmisión) y el puerto de transmisión especificados en el control de servicio de AXIS Camera Station tienen permiso para pasar por el sistema de seguridad o NAT. Para ver la lista completa de puertos, consulte la *Lista de puertos para AXIS Camera Station Pro*, on page 214.
 - Cambie la configuración del proxy del servidor si un servidor de proxy separa el servidor y los dispositivos. Vaya a la sección Configuración del proxy en *Service control general (Servicio de control general)* en el manual del usuario de AXIS Camera Station Pro.
- Agregue cámaras manualmente; vaya a *Add devices (Agregar dispositivos)* en el manual del usuario de AXIS Camera Station Pro.

Mensaje "Reconectando a la cámara en 15 segundos" repetido

Problemas posibles:

- Una red sobrecargada.
- La cámara no es accesible. Asegúrese de que la cámara tiene conexión de red y de que recibe alimentación.
- Hay problemas con la tarjeta gráfica.

Soluciones posibles para problemas con la tarjeta gráfica:

- Instale el controlador más reciente de la tarjeta gráfica.
- Actualice a una tarjeta gráfica con más memoria de vídeo y mayor rendimiento.
- Utilice la CPU para la reproducción de vídeo.
- Cambie los ajustes de vídeo y audio. Por ejemplo, optimice los ajustes del perfil para un ancho de banda bajo.

Grabaciones

Consulte *Vista en vivo*, on page 240 para obtener más información sobre posibles problemas de rendimiento que influyan en las grabaciones y la reproducción.

Problemas habituales

La grabación continua no está habilitada

Las cámaras mostradas no tienen la grabación continua activada.

1. Para activar la grabación continua, vaya a **Configuration > Recording and events > Recording method (Configuración > Grabación y eventos > Método de grabación)**.
2. Seleccione la cámara y active **Continuous (Continua)**.


No se puede grabar en la unidad especificada

El sistema no puede configurar el almacenamiento de grabaciones.

1. Para utilizar un almacenamiento diferente, vaya a **Configuration > Storage > management (Configuración > Almacenamiento > Gestión)**.
2. Agregue el almacenamiento y configure los ajustes de almacenamiento para las cámaras.

Error al instalar la aplicación AXIS Video Content Stream

Este mensaje de error aparece si la aplicación no se puede instalar en una cámara compatible con AXIS Video Content Stream.

1. Para instalar la aplicación manualmente, vaya a **Configuration > Devices > Management (Configuración > Dispositivos > Gestión)**.
2. Seleccione una cámara y haga clic en .

La grabación no se inicia

Si las grabaciones no se inician o se detienen transcurridos unos segundos, indica que el disco está lleno o que hay un exceso de datos entrantes.

- En la página de configuración del servidor, en **Almacenamiento de grabaciones** compruebe si hay suficiente espacio y no hay datos entrantes.
- Aumente el límite de almacenamiento del sistema de gestión de vídeo.
- Asigne más almacenamiento al grupo de almacenamiento. Vaya a *Configure storage (Configurar almacenamiento)* en el manual del usuario de AXIS Camera Station Pro.

Huecos en la grabación durante la grabación continua

Junto con los huecos, las alarmas etiquetadas como **Errores de grabación**. Los huecos pueden darse por distintas razones, por ejemplo:

- Sobrecarga del servidor
- Problema de red
- Sobrecarga de la cámara
- Sobrecarga del disco

Controle si los huecos de grabación ocurren en todas las cámaras. Si no se producen en todas las cámaras, puede ser una sobrecarga de la cámara. Hágase estas preguntas para encontrar el motivo:

- ¿Con qué frecuencia se produce el hueco? ¿Cada hora o cada día?

- ¿Cuánto dura el hueco? ¿Unos segundos o varias horas?
- ¿A qué hora se produce el hueco?

Posibles soluciones:

- En el administrador de tareas del servidor, compruebe si el sistema utiliza uno de los recursos de hardware más de lo normal. Si el disco muestra signos de uso excesivo, agregue más discos y mueva varias cámaras para grabar en los discos nuevos.
- Reduzca la cantidad de datos escritos en el disco (ajustes de vídeo, flujo ZIP, imágenes por segundo, resolución). Tenga en cuenta la estimación de rendimiento de *AXIS Site Designer*, consulte axis.com/support/tools/axis-site-designer.

Para obtener más información, vea *Visualización en directo y rendimiento de la reproducción*, on page 240.

No se pueden reproducir grabaciones exportadas

Si Windows Media Player no reproduce las grabaciones exportadas, compruebe el formato de archivo. Para reproducir las grabaciones exportadas, utilice Windows Media Player (.asf) o AXIS File Player (.asf, .mp4, .mkv).

Para obtener más información, consulte *Reproducir y verificar grabaciones exportadas* en el manual del usuario de AXIS Camera Station Pro.

Nota

AXIS File Player abre automáticamente todas las grabaciones que están en la misma carpeta que el reproductor.

Las grabaciones desaparecen

El sistema solo guarda las grabaciones durante un número determinado de días. Para cambiar el número de días, vaya a **Configuración > Almacenamiento > Selección**.

Si se llena el almacenamiento, el sistema elimina las grabaciones antes del número de días especificado. Para evitar un almacenamiento completo, pruebe lo siguiente:

- Agregar más almacenamiento. Vaya a **Configuración > Almacenamiento > Gestión**.
- Cambie la cantidad de espacio de almacenamiento asignada a AXIS Camera Station Pro. Vaya a **Configuración > Almacenamiento > Gestión**.
- Reduzca el tamaño de los archivos grabados cambiando, por ejemplo, la resolución o la velocidad de fotogramas. Vaya a **Configuration > Devices > Stream profiles (Configuración > Dispositivos > Perfiles de flujo)**.
 - Utilice el formato de vídeo H.264 para grabar, el formato M-JPEG requiere mucho más espacio de almacenamiento.
 - Utilice Zipstream para reducir de forma adicional el tamaño de las grabaciones.

Problemas de grabación en caso de fallos

La grabación a prueba de fallos no graba en el servidor una vez restablecida la conexión.

Causa	Solución
El ancho de banda entre la cámara y el servidor no es suficiente para transferir la grabación.	Mejorar el ancho de banda
La cámara no grabó en la tarjeta SD durante la desconexión.	<ul style="list-style-type: none"> • Realice una comprobación del informe de servidor de la cámara. Consulte axis.com/support/troubleshooting. • Asegúrese de que la tarjeta SD funciona y de que hay grabaciones en ella.
La hora de la cámara ha cambiado desde la desconexión.	<ul style="list-style-type: none"> • Asegúrese de sincronizar el NTP para grabaciones futuras. • Sincronice la hora de la cámara con el servidor o configure el mismo servidor NTP en la cámara y el servidor.

La grabación a pruebas de fallos en AXIS Camera Station Pro no funciona en los siguientes escenarios:

- Apagados del servidor controlados.
- Interrupciones breves de la conexión de menos de 10 segundos.

Vista en vivo

Visualización en directo y rendimiento de la reproducción

En esta sección se describen posibles soluciones si experimenta pérdida de fotogramas o problemas gráficos en el cliente de AXIS Camera Station Pro.

Hardware de cliente

Verifique que la tarjeta gráfica o el controlador del adaptador de red están actualizados

1. Abra DirectX Diagnostic Tool (busque dxdiag en el equipo).
2. Vaya al sitio web del fabricante para asegurarse de que se está utilizando el controlador más reciente para este SO.
3. Compruebe que el cliente y el servidor se ejecuten en el mismo equipo.
4. Pruebe a ejecutar el cliente en un equipo dedicado.

Verificar el número de monitores

Si utiliza una tarjeta gráfica interna, no recomendamos más de dos monitores por tarjeta gráfica.

1. Abra DirectX Diagnostic Tool (busque dxdiag en el equipo)
2. Asegúrese de que AXIS Camera Station Pro es compatible con la tarjeta gráfica dedicada.

Nota

No se puede ejecutar el cliente en una máquina virtual.

Dispositivos conectados

Excesivos clientes conectados al mismo tiempo	En función del caso de uso habitual, asegúrese de que el sistema cumple los requisitos y siga las directrices de hardware. Consulte los <i>Requisitos del sistema en la guía de instalación y migración de AXIS Camera Station Pro</i> .
La cámara está conectada a otro sistema de gestión de vídeo que AXIS Camera Station Pro	Desconecte la cámara del otro cliente y desconéctela de forma predeterminada antes de conectarla a AXIS Camera Station Pro.
Una cámara utiliza muchas transmisiones diferentes, especialmente de alta resolución	<p>Puede ser un problema especialmente con algunas cámaras M-Line.</p> <ul style="list-style-type: none"> • Cambie el flujo al mismo perfil de flujo o a una resolución inferior. Consulte <i>Streaming profiles (perfiles de flujo)</i> en el manual del usuario de AXIS Camera Station Pro. • Cambie el flujo al mismo perfil de flujo o a una resolución inferior. Consulte <i>Streaming profiles (perfiles de flujo)</i> en el manual del usuario de AXIS Camera Station Pro.

Sobrecarga del servidor

Uso inusual de CPU/RAM a la misma hora que el problema	Asegúrese de que no hay otras aplicaciones que consuman CPU/RAM ejecutándose al mismo tiempo.
--	---

Problema de red

Uso inusual de ancho de banda a la misma hora que la incidencia	Asegúrese de que no hay otras aplicaciones que consuman ancho de banda ejecutándose al mismo tiempo.
Suficiente ancho de banda / Red remota o local	<ul style="list-style-type: none"> • Mire a través de la topología de red. • Realice una comprobación de estado de cualquier dispositivo de red, como switch, router o adaptador de red y cable, que se utilice entre cámaras, servidor y cliente.

No hay vídeo en la visualización en directo

La visualización en directo no muestra el vídeo de una cámara conocida.

- Apague la decodificación de hardware. La decodificación de hardware se activa de forma predeterminada, consulte Decodificación de hardware en *Streaming* en el manual del usuario de AXIS Camera Station Pro.

Otras soluciones posibles:

- Si no puede ver la visualización en directo a través de la interfaz web o si la interfaz web no funciona, solucione los problemas de la cámara. Vaya a axis.com/support/troubleshooting.
- Cree un informe del servidor de la cámara y vaya a axis.com/support/troubleshooting.
- Si hay un software antivirus instalado, es posible que se bloqueen las secuencias en directo.
- Permitir carpetas y procesos de AXIS Camera Station Pro, consulte *Preguntas frecuentes*.
- Asegúrese de que el cortafuegos no bloquee las conexiones de determinados puertos, consulte *Control general de servicios* en el manual del usuario de AXIS Camera Station Pro.
- Asegúrese de que la experiencia de escritorio se instaló para versiones de SO de servidor de Windows compatibles. Consulte *Exportación programada* en el manual del usuario de AXIS Camera Station Pro.
- Asegúrese de que el flujo de resolución inferior funciona.

Si ninguna de las sugerencias anteriores sirve de ayuda, contacte con la asistencia de Axis, vaya a *Proceso de escalada, on page 251*.

Almacenamiento

No se puede acceder al almacenamiento de red

Si utiliza la cuenta del sistema local para iniciar sesión en el control de servicio de AXIS Camera Station Pro, no puede añadir almacenamiento de red que enlace con carpetas compartidas de otros ordenadores.

Para cambiar la cuenta de conexión de servicio:

1. Abra el Panel de control de Windows.
2. Busque "Servicios".
3. Haga clic en **View local services (Ver servicios locales)**.
4. Haga clic con el botón derecho en **AXIS Camera Station Pro** y seleccione **Properties (Propiedades)**.
5. Vaya a la pestaña **Log on (Iniciar sesión)**.
6. Cambie de **Cuenta de sistema local a Esta cuenta**.
7. Seleccione un usuario con acceso a Windows Active Directory.

El almacenamiento de red no está disponible

Asegúrese de que el ordenador y el servidor que ejecutan el software de gestión de vídeo forman parte del mismo dominio que el almacenamiento de red.

No se puede volver a conectar a un almacenamiento de red con el nombre de usuario y la contraseña nuevos

Si el almacenamiento de red requiere autenticación, es importante que desconecte el almacenamiento de red de todas las conexiones en curso antes de cambiar el nombre de usuario y su contraseña.

Para cambiar el nombre de usuario y la contraseña de un almacenamiento de red y volver a conectarse:

1. Desconecte almacenamiento de red de todas las conexiones activas.
2. Cambie el nombre de usuario y la contraseña.
3. Vaya a **Configuration > Storage > Management (Configuración > Almacenamiento > Gestión)** y vuelva a conectar al almacenamiento de red con el nuevo nombre de usuario y contraseña.

Detección de movimiento

Problemas habituales

Error al instalar la aplicación AXIS Video Motion Detection

No se puede instalar AXIS Video Motion Detection 2 o 4. La cámara usa la detección de movimiento integrada para grabación de movimiento.

Para instalar la aplicación manualmente, vaya a *Instalar aplicación de la cámara* en el manual del usuario de AXIS Camera Station Pro.

Error al recuperar detección de movimiento actual

El sistema de gestión de vídeo no puede recuperar parámetros de detección de movimiento de la cámara. La cámara usa la detección de movimiento integrada para grabación de movimiento.

Para instalar la aplicación manualmente, vaya a *Instalar aplicación de la cámara* en el manual del usuario de AXIS Camera Station Pro.

Detección de movimiento no configurada

No puede configurar la detección de movimiento en las cámaras mostradas.

1. Para configurar la detección de movimiento manualmente, vaya a **Configuración > Grabaciones y eventos > Método de grabación**.
2. Seleccione la cámara y haga clic en **Motion Settings (Ajustes de movimiento)** para configurar la detección de movimiento.

La detección de movimiento no está habilitada

Las cámaras mostradas no tienen la grabación de movimiento activada.

1. Vaya a **Configuración > Grabaciones y eventos > Método de grabación**.
2. Seleccione la cámara y active **Motion detection (Detección de Movimiento)** para activar la grabación de detección de movimiento.

La detección de movimiento detecta demasiados objetos en movimiento u objetos insuficientes

En esta sección se describen posibles soluciones si tiene más o menos detecciones en las grabaciones relacionadas con detección de movimiento en el vídeo.

Ajustar configuración de movimiento

Puede seleccionar ajustes de movimiento para ajustar el área que detecta objetos en movimiento.

1. Vaya a **Configuración > Grabaciones y eventos > Método de grabación**.
2. Seleccione la cámara y haga clic en **Configuración de movimiento**.
3. Elija los ajustes en función del firmware de la cámara.

AXIS Video Motion Detection 2 y 4	Puede configurar el área de interés. Consulte <i>Editar AXIS Video Motion Detection 2 y 4</i> en el manual del usuario de AXIS Camera Station Pro.
Detección de movimiento integrada	Puede configurar las ventanas incluidas y excluidas. Consulte <i>Editar detección de movimiento integrada</i> en el manual del usuario de AXIS Camera Station Pro.

Ajustar período de activación

El periodo de activación es un intervalo de tiempo entre dos activadores sucesivos, use este ajuste para reducir el número de grabaciones consecutivas. La grabación continúa si se activa otro activador durante este intervalo. Si se activa otro desencadenador, el periodo de activación volverá a empezar a partir de ese punto.

Para cambiar el periodo de activación:

1. Vaya a **Configuración > Grabaciones y eventos > Método de grabación**.
2. Seleccione la cámara.
3. En **Advanced (Avanzada)** ajuste **Trigger period (Periodo de activación)** en segundos.

Reglas de actuación

Eventos inesperados de activación de E/S

Si recibe eventos inesperados de entrada/salida en torno a las 1:15 horas, sustituya los activadores de E/S existentes por activadores de eventos de dispositivo.

Audio

No hay audio en la visualización en directo

Si no hay audio en la visualización en directo, compruebe lo siguiente

- Asegúrese de que la cámara disponga de capacidad de audio.
- Asegúrese de que el equipo tenga una tarjeta de sonido y que la tarjeta esté en uso.
- Asegúrese de que el perfil en uso se configuró para el audio.
- Asegúrese de que el usuario tenga derechos de acceso al audio.

Configure perfiles para el uso de audio

1. Vaya a **Configuration > Devices > Stream profiles (Configuración > Dispositivos > Perfiles de flujo)**.
2. Seleccione la cámara.
3. Seleccione **MPEG-4** o **H.264** en **Format (Formato)** en los ajustes de perfil de vídeo.
4. En **Audio**, seleccione un micrófono en el menú desplegable **Micrófono**.
5. Seleccione cuándo desea utilizar audio en el menú desplegable **Use microphone for (Usar micrófono para)**.
6. Si procede, seleccione un altavoz en el menú desplegable **Speaker (Altavoz)**.
7. Haga clic en **OK**.

Compruebe y cambie derechos de acceso de usuario

Nota

Para seguir estos pasos, debe tener derechos de administrador para AXIS Camera Station Pro.

1. Vaya a **Configuration > Security > User permissions (Configuración > Seguridad > Permisos de usuario)**.
2. Seleccione un usuario o un grupo.
3. Seleccione **Audio listen (Escuchar audio)** o **Audio speak (Transmisión de audio)** para un dispositivo específico.
4. Haga clic en **Aplicar**.

No hay audio en las secuencias

Puede activar o desactivar el audio en los perfiles de flujo. Para obtener más información, consulte *perfiles de flujo* en el manual del usuario de AXIS Camera Station Pro.

No hay audio en la reproducción

El audio está disponible en la reproducción si habilita el audio en el perfil que se usó para la grabación.

Nota

No puede utilizar audio con vídeo M-JPEG. Seleccione otro formato de vídeo.

Para usar el audio en las grabaciones:

1. Vaya a **Configuration > Devices > Stream profiles (Configuración > Dispositivos > Perfiles de flujo)** para establecer el formato de vídeo para el perfil de vídeo que quiere usar.
2. Vaya a **Configuración > Grabaciones y eventos > Método de grabación.**
3. Seleccione la cámara.
4. Seleccione el perfil que ha configurado en el menú desplegable **Perfil.**
5. Haga clic en **Aplicar.**

Grabaciones activadas por regla

Para habilitar el audio en una regla existente:

1. Vaya a **Configuración > Grabaciones y eventos > Reglas de acción.**
2. Seleccione la regla y haga clic en **Editar.**
3. Haga clic en **Next (Siguiente)** para ir a **Actions (Acciones).**
4. Seleccione la acción **Record (Grabar)** y haga clic en **Edit (Editar).**
5. Seleccione un perfil que utilice audio.
6. Para guardar, haga clic en **Finalizar.**

Inicio de sesión

Imposible iniciar sesión o conectarse al servidor

Esta sección explica los problemas con el inicio de sesión y la conexión que pueden registrarse al conectarse a un único servidor. Al iniciar sesión en varios servidores, el cliente se inicia y puede ver el estado de conexión en la barra de estado. Para obtener más información sobre el estado de la conexión, consulte *Estado de la conexión* en el manual del usuario AXIS Camera Station Pro.

El nombre de usuario o la contraseña son incorrectos

La combinación de nombre de usuario y contraseña no es válida para iniciar sesión en el servidor especificado.

- Revise que los haya introducido correctamente o utilice otra cuenta.
- Asegúrese de que el usuario tenga derechos de acceso al servidor AXIS Camera Station Pro.
- Los relojes del servidor de AXIS Camera Station Pro y el cliente deben estar sincronizados. En el caso de usuarios del dominio, el reloj del servidor del dominio debe estar sincronizado con el servidor y el cliente.
- Un usuario que no se agregó al servidor, pero que es miembro del grupo de administradores locales del servidor, debe ejecutar el cliente como administrador.
- Para obtener información sobre derechos de acceso de usuarios, consulte *Configurar los permisos de usuario* en el manual del usuario de AXIS Camera Station Pro.

El usuario no está autorizado a conectarse al servidor	El usuario no puede usar AXIS Camera Station Pro en el servidor especificado.	Agregue al usuario en el cuadro de diálogo de permiso de usuario.
Imposible verificar la seguridad del mensaje	Se ha producido un error al establecer una conexión segura con el servidor,	Las horas UTC del servidor y el cliente deben estar bien sincronizadas. Ajuste la hora del cliente y la del

	seguramente porque las horas del cliente y del servidor no están sincronizadas.	servidor de modo que la diferencia entre ambos no sea superior a 3 horas.
Ningún contacto con el servidor	El cliente no puede establecer ningún tipo de conexión con el servidor.	<ul style="list-style-type: none"> • Asegúrese de que el equipo servidor pueda conectarse a la red. • Asegúrese de que el ordenador servidor esté en funcionamiento. • Asegúrese de que el cortafuegos se haya configurado bien. • Asegúrese de que ha escrito bien la dirección del servidor. • Compruebe los ajustes proxy del cliente.
No se recibe respuesta del servidor	El cliente puede establecer contacto con el equipo servidor, pero ningún servidor de AXIS Camera Station Pro se ejecuta.	Asegúrese de que se conecta al ordenador correcto y de que el servidor de AXIS Camera Station Pro se está ejecutando.
El cliente no se puede conectar al servidor	El cliente no se puede conectar al servidor y aparece un mensaje de error.	<p>Asegúrese de que la red se haya configurado bien:</p> <ul style="list-style-type: none"> • Compruebe que el SO es compatible. Para obtener una lista completa de los SO admitidos, vaya a <i>notas de versión</i> • Desde el control de servicio, compruebe que el servidor de AXIS Camera Station Pro esté en funcionamiento o inicie el servidor si es necesario. • Verifique que el cliente y el servidor están conectados a la misma red. <ul style="list-style-type: none"> – De no estarlo, el cliente debe utilizar la dirección IP externa del servidor. • Investigue si existe un servidor proxy entre el servidor y el cliente. <ul style="list-style-type: none"> – Configure el proxy del servidor en el control de servicio. – Configure los ajustes de proxy del cliente en la página de inicio de sesión y seleccione Change proxy settings (Cambiar ajustes de proxy). – Configure los ajustes de proxy del cliente en Opciones de Internet de Windows y seleccione la opción predeterminada en Change Proxy settings (Cambiar ajustes de proxy).
No se puede conectar con el servidor	Se ha producido un error desconocido al conectar con el servidor.	<ul style="list-style-type: none"> • Asegúrese de que la dirección y el puerto del servidor de AXIS Camera Station Pro sean correctos.

		<ul style="list-style-type: none"> • Asegúrese de que ningún NAT, cortafuegos o software antivirus bloqueen la conexión con el servidor. Consulte <i>Configurar el cortafuegos para permitir el acceso a AXIS Secure Remote Access</i> para obtener más información. • Use el control de servicio de AXIS Camera Station Pro para asegurarse de que el servidor esté en funcionamiento. <ul style="list-style-type: none"> – Abra el control de servicio de AXIS Camera Station Pro, consulte el <i>control de servicio de AXIS Camera Station</i> en el manual del usuario de AXIS Camera Station Pro. – Consulte el estado del servidor en la pestaña General. Si el estado es Stopped (Detenido), haga clic en Start (Iniciar) para iniciar el servidor.
Imposible encontrar el servidor	El cliente no puede resolver la dirección introducida a una dirección IP.	<ul style="list-style-type: none"> • Asegúrese de que el equipo servidor pueda conectarse a la red. • Asegúrese de que la dirección y el puerto del servidor de AXIS Camera Station Pro sean correctos. • Asegúrese de que ningún NAT, cortafuegos o software antivirus bloqueen la conexión con el servidor. Consulte <i>Configurar el cortafuegos para permitir el acceso a AXIS Secure Remote Access</i> para obtener más información.
La versión del servidor y del cliente son diferentes	El cliente ejecuta una versión más reciente del servidor de AXIS Camera Station Pro.	Actualice el servidor para que utilice la misma versión que el cliente.
	El servidor ejecuta una versión más reciente de AXIS Camera Station Pro que el cliente.	Actualice el cliente para que utilice la misma versión que el servidor.
Imposible conectar con el servidor. Servidor demasiado ocupado.	El servidor no puede responder debido a problemas de rendimiento.	Compruebe que el equipo servidor y la red no están sobrecargados.
El servidor local de AXIS Camera Station Pro no se ejecuta	Utilice This computer (este equipo) para conectarse, pero el servidor de AXIS Camera Station Pro instalado no se ejecuta.	Utilice el control de servicio para iniciar AXIS Camera Station Pro o seleccionar un servidor remoto en el que iniciar sesión.
Este ordenador no tiene el servidor de AXIS Camera Station Pro instalado	Puede usar Este equipo para conectarse, pero no hay ningún servidor instalado en este equipo.	Instale el servidor de AXIS Camera Station Pro o elija un servidor diferente.
La lista de servidores seleccionada está vacía	La lista de servidores seleccionada para iniciar sesión estaba vacía.	Para agregar servidores a la lista de servidores, haga clic en Edit (Editar) junto a la selección de la lista de servidores.

Licencias

Problemas con el registro de licencias

Si el registro automático genera un error, pruebe lo siguiente:

- Asegúrese de que el sistema esté registrado en una organización.
- Vaya a **Configuración** para asegurarse de que la **Licencia automática** está activada. Consulte *Gestionar licencias* en el manual del usuario de AXIS Camera Station Pro.
- Asegúrese de que la hora del servidor esté actualizada.

Para obtener más información, consulte *Instalación de AXIS Camera Station Pro y la guía de migración*.

Usuarios

No se encuentran los usuarios del dominio

Si la búsqueda de usuario de dominio no es correcta, cambie la cuenta de conexión de servicio:

1. Abra el **Panel de control** de Windows.
2. Busque "Servicios".
3. Haga clic en **View local services (Ver servicios locales)**.
4. Haga clic con el botón derecho en **AXIS Camera Station Pro** y seleccione **Properties (Propiedades)**.
5. Haga clic en la pestaña **Log on (Iniciar sesión)**.
6. Cambie de **Cuenta de sistema local** a **Esta cuenta**.
7. Seleccione un usuario con acceso a **Windows Active Directory**.

Errores de certificado

AXIS Camera Station Pro no puede comunicarse con el dispositivo hasta que solucione el error de certificado.

Posibles errores		
Certificado no encontrado	Si el certificado del dispositivo se eliminó.	Si conoce el motivo, haga clic en Reparar . Si sospecha de acceso no autorizado, investigue el problema antes de restaurar el certificado. Haga clic en Advanced (Avanzada) para ver los detalles del certificado. Motivos posibles para eliminar el certificado: <ul style="list-style-type: none"> • Se han restablecido los valores predeterminados de fábrica del dispositivo. • Se desactivó la comunicación HTTPS segura. • Una persona no autorizada accedió y modificó el dispositivo.
Certificado sin confianza	El certificado del dispositivo se ha modificado fuera de AXIS Camera Station Pro. Esto puede indicar que una persona no autorizada accedió y modificó el dispositivo.	Si conoce el motivo, haga clic en Trust This Device (Confiar en este dispositivo) . Si no, investigue el problema antes de confiar en el certificado. Haga clic en Advanced (Avanzada) para ver los detalles del certificado.

Falta la contraseña para la autoridad de certificación

Si tiene una autoridad de certificación en AXIS Camera Station Pro sin una contraseña almacenada, aparece la siguiente alarma.

Debe proporcionar una contraseña para el certificado de la autoridad de certificación. Lea el manual del usuario para obtener más información.

Puede resolver este problema de tres formas distintas:

- Activar HTTPS en un dispositivo
- Importar una autoridad de certificación existente
- Generar una nueva autoridad de certificación

Para activar HTTPS en un dispositivo:

1. Vaya a **Configuración > Dispositivos > Gestión**.
2. En la lista, haga clic con el botón derecho en un dispositivo y seleccione **Security (Seguridad) > HTTPS > Enable/Update (Habilitar/Actualizar)**.
3. Haga clic en **Sí** para confirmar.
4. Introduzca la contraseña de autoridad de certificación.
5. Haga clic en **OK**.

Para importar una autoridad de certificación existente:

1. Vaya a **Configuration (Configuración) > Security (Seguridad) > Certificates (Certificados) > Devices (Dispositivos)**.

2. En HTTPS, desactive **Validate device certificate (Validar el certificado del dispositivo)**.
3. En **Certificate authority (Autoridad de certificación)**, haga clic en **Import (Importar)**.
4. Introduzca su contraseña y haga clic en **OK (Aceptar)**.
5. Seleccione el número de días de validez de los certificados cliente/servidor firmados.
6. Vaya a **Configuración > Dispositivos > Gestión**.
7. Haga clic con el botón derecho del ratón en los dispositivos y seleccione **Seguridad > HTTPS > Habilitar/ Actualizar**.
8. Vaya a **Configuration (Configuración) > Security (Seguridad) > Certificates (Certificados) > Devices (Dispositivos)** y active **Validate device certificate (Validar el certificado del dispositivo)**.

Nota

AXIS Camera Station Pro pierde la conexión con los dispositivos y algunos componentes del sistema se reinician.

Para que AXIS Camera Station Pro genere una nueva autoridad de certificación:

1. Vaya a **Configuration (Configuración) > Security (Seguridad) > Certificates (Certificados) > Devices (Dispositivos)**.
2. En HTTPS, desactive **Validate device certificate (Validar el certificado del dispositivo)**.
3. En **Certificate authority (Autoridad de certificación)**, haga clic en **Generate (Generar)**.
4. Introduzca su contraseña y haga clic en **OK (Aceptar)**.
5. Seleccione el número de días de validez de los certificados cliente/servidor firmados.
6. Vaya a **Configuración > Dispositivos > Gestión**.
7. Haga clic con el botón derecho del ratón en los dispositivos y seleccione **Seguridad > HTTPS > Habilitar/ Actualizar**.
8. Vaya a **Configuration (Configuración) > Security (Seguridad) > Certificates (Certificados) > Devices (Dispositivos)** y active **Validate device certificate (Validar el certificado del dispositivo)**.

Nota

AXIS Camera Station Pro pierde la conexión con los dispositivos y algunos componentes del sistema se reinician.

Sincronización de hora

El servicio Hora de Windows no se está ejecutando

El servicio de Hora de Windows y el servidor NTP no están sincronizados. Esto puede deberse a que el servicio Hora de Windows no puede llegar al servidor NTP.

- Asegúrese de que el servidor NTP esté en línea.
- Asegúrese de que la configuración del cortafuegos sea correcta.
- Asegúrese de que el dispositivo está en una red que puede llegar al servidor NTP.

Si necesita ayuda, póngase en contacto con el administrador del sistema.

Diferencia horaria detectada en un dispositivo

El dispositivo no sincroniza con la hora del servidor. La grabación tiene marcas de tiempo con la hora en la que el servidor la recibió, en lugar de la hora en la que el dispositivo la registró.


1. Vaya a **Configuration > Devices > Time synchronization (Configuración > Dispositivos > Sincronización de tiempo)** y revise el desplazamiento de hora del servidor.
2. Si el desplazamiento de hora del servidor es superior a 2 segundos:
 - 2.1. Seleccione **Enable time synchronization (Habilitar sincronización de hora)**.

- 2.2. Asegúrese de que el dispositivo puede alcanzar el servidor NTP específico.
- 2.3. Vuelva a cargar el dispositivo en **Configuration > Devices > Management (Configuración > Dispositivos > Administración)** .
3. Si el desplazamiento de hora del servidor es inferior a 2 segundos, es posible que el dispositivo no envíe datos suficientes para la sincronización de hora.
 - 3.1. Borrar **Enviar alarma cuando la diferencia de tiempo entre el servidor y el dispositivo sea superior a 2 segundos** para desactivar las alarmas.

Para obtener asistencia, póngase en contacto con el servicio de asistencia técnica de Axis.

Asistencia técnica

La asistencia técnica es un servicio para los clientes que disponen de una versión con licencia de AXIS Camera

Station Pro. Para ponerse en contacto con el servicio de asistencia técnica, vaya a  > **Help > Online Support (Ayuda > Asistencia en línea)** o a axis.com/support

Le recomendamos que adjunte el informe del sistema y capturas de pantalla en el caso de soporte.

Vaya a  > **Help (Ayuda) > System report (Informe del sistema)** para crear un informe del sistema.

Proceso de escalada

Si tiene incidencias que no se pueden resolver con esta guía, escale el problema a soporte en línea de Axis, consulte *soporte en línea de Axis*. Para que nuestro servicio técnico entienda la incidencia y pueda resolverla, debe incluir la siguiente información:

- Una descripción clara sobre cómo reproducir la incidencia o en qué circunstancias se produce.
- La hora y el nombre de la cámara correspondiente o la dirección IP en la que se produce la incidencia.
- AXIS Camera Station Pro informe de sistema generado inmediatamente después de producirse la incidencia. El informe del sistema debe generarse desde el cliente o el servidor donde se reprodujo la incidencia.
- Capturas de pantalla o grabaciones opcionales de todos los monitores que muestran el problema. Active la función de superposición de depuración cuando tome las capturas de pantalla o realice la grabación.
- Si es necesario, incluya los archivos de la base de datos. Exclúyalas para que la carga vaya más rápido.

Algunos problemas requieren información adicional que el equipo de soporte solicita si es necesario.

Nota

Si el archivo es superior a 100 MB, por ejemplo, un rastreo de red o un archivo de la base de datos, use un archivo seguro mediante un servicio de uso compartido de archivos seguro en el que confíe para enviar el archivo.

Información adicional	
Registros de nivel de depuración	En ocasiones, usamos el registro de nivel de depuración para recopilar más información. Solo es así si lo solicita un ingeniero de soporte de Axis. Consulte las instrucciones en el servicio de <i>soporte en línea de Axis</i> .
Superposición de depuración de la visualización en directo	En ocasiones, es conveniente proporcionar capturas de pantalla de la información de superposición o un vídeo que muestre el cambio de valores en el tiempo que le interese. Para agregar información de superposición, haga lo siguiente:

Información adicional	
	<ul style="list-style-type: none"> • Pulse Ctrl + i una vez para mostrar información de superposición en la visualización en directo. • Pulse Ctrl + i dos veces para añadir información de depuración. • Pulsa Ctrl + i tres veces para ocultar la superposición.
Rastreo de red	<p>Si lo solicita el ingeniero de soporte, genere trazas de red al crear el informe del sistema. Tome las trazas de red al mismo tiempo que se produce el problema, cuando este es reproducible. Recursos utilizados:</p> <ul style="list-style-type: none"> • Un seguimiento de red de 60 segundos tomado en la cámara (aplicable solo para firmware 5.20 y posteriores) Utilice el siguiente comando VAPIX para cambiar el inicio de sesión, la dirección IP y la duración (en segundos) si es necesario: <code>http://root:pass@192.168.0.90/axis-cgi/debug/debug.tgz?cmd=pcapdump&duration=60</code> • Un seguimiento de red de 10-30 segundos tomado en el servidor que muestra la comunicación entre el servidor y la cámara.
Archivos de base de datos	<p>En casos en los que tenemos que examinar o reparar manualmente la base de datos. Seleccione la opción Include database in the report (Incluir base de datos en el informe) antes de generar el informe del sistema.</p>
Capturas de pantalla	<p>Utilice las capturas de pantalla cuando se trate de un problema de la visualización en directo relacionado con la interfaz de usuario. Por ejemplo, si desea mostrar una línea temporal para las grabaciones o cuando es difícil describirla.</p>
Grabaciones de pantalla	<p>Utilice grabaciones de pantalla cuando resulte difícil describir el problema con palabras, por ejemplo, cuando hay muchas interacciones en la interfaz de usuario involucradas para reproducir el problema.</p>

T10196821_es

2026-03 (M28.4)

© 2023 – 2026 Axis Communications AB