DOCUMENTO TÉCNICO

Seguridad con la solución corporal de Axis

Febrero 2024

Resumen

Aunque se trata de una solución de plataforma abierta, el sistema de cámaras corporales Axis ofrece un excelente nivel de seguridad.

Para garantizar la seguridad en caso de pérdida de la cámara, la plataforma únicamente utiliza los componentes de software imprescindibles. En cambio, el controlador del sistema asume más funciones, ya que normalmente no está tan expuesto a amenazas físicas. Además, el almacenamiento interno de la máquina utiliza cifrado AES-256, para impedir el acceso no autorizado a los datos. Gracias a la comunicación basada en IPv6 y en certificados, la cámara solo descargará datos en el controlador del sistema o sistema específico del que forme parte.

Cuando se descargan datos de la cámara en el controlador del sistema se utiliza una conexión a la red con cifrado HTTPS. Los datos solo se almacenan temporalmente en la unidad de almacenamiento con cifrado AES-256 del controlador del sistema, ya que se transfieren inmediatamente al destino del contenido a través de otra conexión cifrada HTTPS.

La seguridad y la integridad del controlador del sistema se refuerzan todavía más con un TPM (módulo de plataforma de confianza) conforme con FIPS 140-2. Otras características, que el sistema corporal comparte con muchos dispositivos Axis, son el firmware firmado, el arranque seguro y el vídeo firmado.

Cuando se transmiten en directo imágenes a través de AXIS Body Worn Live, los datos se cifran en reposo, en tránsito y en el navegador web del usuario. También se cifran de extremo a extremo con el protocolo XChaCha20-Poly1305. Además, el administrador controla quién puede ver la secuencia en directo, en qué ordenador y navegador y con qué credenciales de usuario.

Índice

1 Acrónimos y terminología 4
2 Introducción 4
3 Seguridad en caso de pérdida de la cámara 4
4 Seguridad en la transferencia de datos 4
5 Otras tecnologías de seguridad 5
6 Seguridad con AXIS Body Worn Live 5

1 Acrónimos y terminología

BWC. Body worn camera (cámara corporal)

VMS. Video management system (sistema de gestión de vídeo)

EMS. Evidence management system (sistema de gestión de pruebas)

Destino del contenido. Ubicación en la que se almacenan las grabaciones y los datos de dispositivos como cámaras corporales. Algunos ejemplos de destinos de contenido pueden ser sistemas de gestión de vídeo, sistemas de gestión de pruebas y servidores de contenidos.

2 Introducción

El sistema corporal de Axis es de plataforma abierta, lo que facilita su integración con sistemas externos de gestión de vídeo y gestión de pruebas. Sin embargo, ofrece un excelente nivel de seguridad, ya que este aspecto ha sido siempre prioritario en todas las fases del despliegue del sistema.

Este documento técnico explica cómo funciona el intercambio de datos entre los componentes del sistema corporal Axis. Concretamente, presentamos las medidas adoptadas para proteger el sistema y sus datos, desde la grabación de una cámara corporal hasta el destino del contenido. También ponemos el foco en los diferentes soportes de almacenamiento y las consideraciones de seguridad asociadas.

3 Seguridad en caso de pérdida de la cámara

Durante su uso cotidiano, la cámara corporal está expuesta a las amenazas de posibles robos o actos vandálicos. Su diseño integra diferentes características para minimizar los efectos de estas amenazas y preservar la seguridad de los datos y el sistema incluso si desaparece una cámara.

La cámara corporal, por ejemplo, funciona con una plataforma de software reducida a la mínima expresión, en comparación con otras cámaras Axis, ya que prescinde de los componentes de software innecesarios. La cámara y el controlador del sistema no son compatibles con VAPIX ni con protocolos como FTP, SSH o SNMP. Además, la cámara tampoco puede funcionar como servidor. La integración con otros sistemas, como VMS y EMS, se gestiona a través del controlador del sistema, normalmente menos expuesto a amenazas físicas que las cámaras en sí.

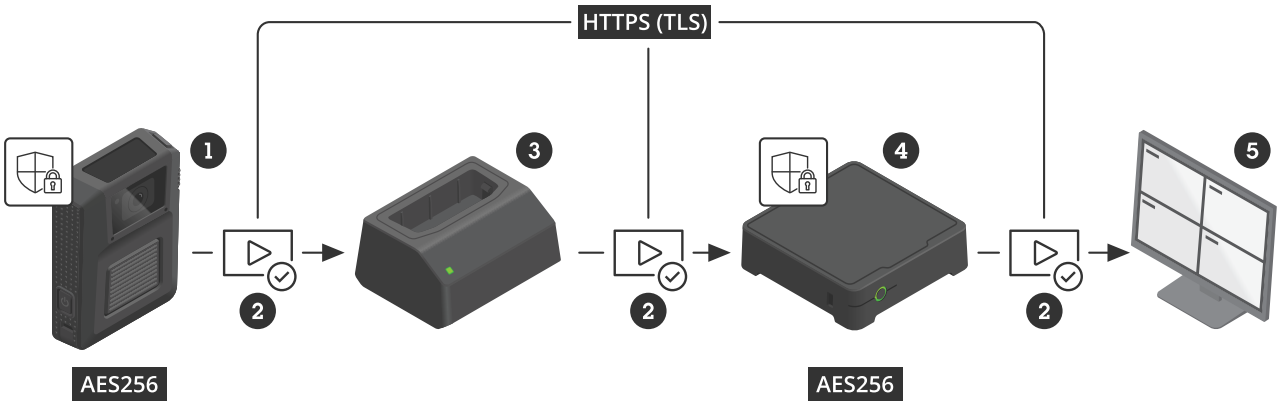
El almacenamiento interno de la cámara corporal utiliza cifrado AES-256 para impedir el acceso no autorizado a los datos en caso de pérdida de la cámara.

La cámara solo descargará datos en el controlador del sistema o sistema específico del que forme parte. Para garantizar que es así, la cámara corporal y el controlador del sistema se comunican mediante IPv6 y certificados. Cada vez que la cámara se conecta a su base, los certificados se renuevan automáticamente para que se correspondan con los más recientes del controlador del sistema.

Si una cámara se retira de la base y pasa más de cuatro semanas alejada del sistema, el controlador del sistema acepta de forma excepcional certificados más antiguos durante ocho semanas. Si pasa más tiempo, tendrá que aceptarse manualmente en el sistema de nuevo, utilizando la frase de contraseña maestra. De este modo se evita que una cámara perdida o alejada del sistema durante mucho tiempo pueda añadirse de nuevo accidentalmente, con los riesgos de seguridad que implicaría.

4 Seguridad en la transferencia de datos

En la mayoría de los casos, la cámara corporal, con vídeos y metadatos almacenados, se deja de nuevo en su base después de un turno. Todos los datos se descargan al controlador del sistema a través de la base, utilizando una conexión de red cifrada con HTTPS (HTTP con TLS). Los datos solo se almacenan temporalmente en el controlador del sistema, en una unidad de almacenamiento SSD con cifrado AES-256, y se transfieren inmediatamente al destino del contenido a través de HTTPS.



Transferencia y almacenamiento seguros de los datos entre la cámara corporal (1) y el destino del contenido (5).

1 *Cámara corporal con Axis Edge Vault*
2 *Vídeo firmado (función de ciberseguridad)*
3 *Base de conexión*
4 *Controlador del sistema con Axis Edge Vault*
5 *Destino del contenido*

También es posible usar una clave de cifrado del destino del contenido para cifrar los datos de la cámara corporal y el controlador del sistema, si el destino del contenido proporciona una clave de cifrado pública. En este caso se aplicará un nivel adicional de cifrado a los datos cuando se envíen al destino del contenido.

5 Otras tecnologías de seguridad

La seguridad y la integridad del controlador del sistema se refuerzan todavía más con un TPM (módulo de plataforma de confianza) conforme con FIPS 140-2.

Tanto las cámaras corporales como el controlador del sistema incorporan Axis Edge Vault, una plataforma de ciberseguridad basada en el hardware que protege todos los datos de los dispositivos y abre la puerta a varias funciones de seguridad. Por ejemplo, el sistema de archivos está cifrado y la clave está protegida con Axis Edge Vault. El *arranque seguro* significa que los dispositivos solo pueden arrancar con firmware autorizado. El *firmware firmado* les obliga a rechazar cualquier actualización de firmware si la integridad del firmware no está garantizada. El *vídeo firmado* aporta un nivel extra de protección, ya que añade una suma de verificación criptográfica a la transmisión de vídeo. De este modo es posible trazar el origen del vídeo hasta la cámara Axis concreta de la que se ha obtenido y verificar así que las imágenes no se han manipulado.

Consulte *www.axis.com/developer-community/signed-video* para obtener más información sobre el vídeo firmado o *www.axis.com/solutions/built-in-cybersecurity-features* para ver más detalles sobre las funciones de ciberseguridad de Axis.

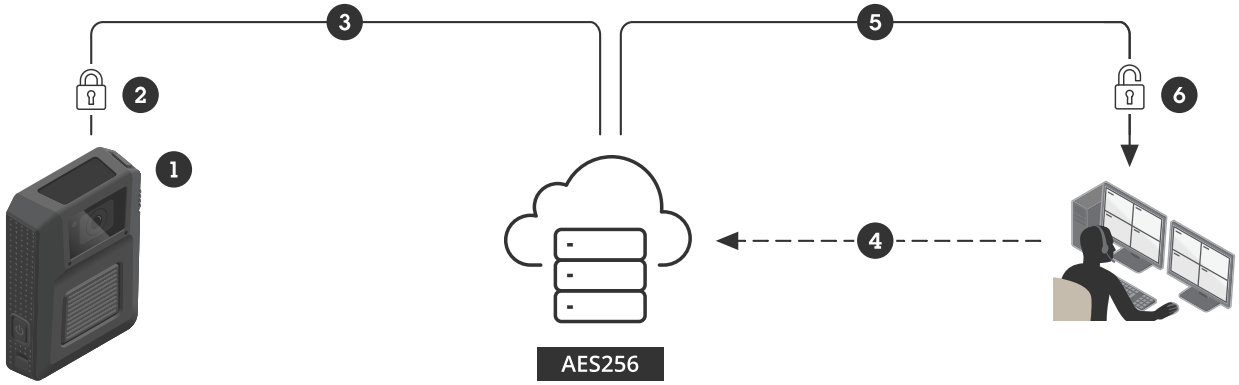
El usuario de la cámara solo puede ver el vídeo grabado sobre el terreno a través de la aplicación AXIS Body Worn Assistant. Si la aplicación está activada, la cámara corporal transmite el vídeo directamente a la aplicación, pero no se almacena ningún material para accesos posteriores en la caché ni en la memoria del dispositivo en el que se utiliza la aplicación. En la transmisión de vídeo se aplica también una superposición para disuadir el uso de dispositivos de grabación secundarios para capturar el vídeo. Y si ocurriera, es posible vincular el vídeo a la identidad del usuario de la cámara corporal gracias a la superposición. El conector compatible con USB-C de la cámara corporal no puede utilizarse en ningún caso para visualizar, eliminar o descargar el vídeo.

6 Seguridad con AXIS Body Worn Live

AXIS Body Worn Live es una aplicación que permite acceder a datos en tiempo real de cámaras corporales Axis. AXIS Body Worn Live pone a disposición de los usuarios una secuencia en directo de vídeo, audio y otros datos, como coordenadas de posición, y ofrece un resumen situacional único de un incidente. De entrada se ofrece como un servicio en la nube.

Con AXIS Body Worn Live, los datos no solo se cifran en reposo (durante su almacenamiento) y en tránsito, sino de extremo a extremo, entre la cámara y el navegador web de la persona que los ve.

Todos los datos y archivos alojados en AXIS Body Worn Live incluyen cifrado AES-256 en reposo. Todos los canales de comunicación están protegidos mediante HTTPS con TLS y empleando certificados firmados por organismos de confianza. AXIS Body Worn Live añade también otra capa de cifrado real de extremo a extremo con el protocolo XChaCha20-Poly1305.



Transmisión en directo segura con cifrado de extremo a extremo en AXIS Body Worn Live

1 *La cámara corporal captura el vídeo en directo y otros datos.*
2 *Los datos se cifran en la cámara corporal.*
3 *La cámara corporal transmite los datos a AXIS Body Worn Live.*
4 *El usuario solicita datos de AXIS Body Worn Live.*
5 *Se transmiten datos de AXIS Body Worn Live al usuario.*
6 *Los datos se desencriptan en el navegador web del usuario.*

El administrador del sistema de la cámara corporal tiene todo el control sobre quién puede ver la secuencia en directo. Los datos se cifran de forma que solo las personas autorizadas por el administrador pueden desencriptar y visualizar el vídeo. Además, el administrador puede revocar el acceso. El usuario necesitará el ordenador correcto, el navegador web correcto y las credenciales de usuario correctas. Nadie más, ni siquiera Axis, puede acceder a la secuencia en directo. Axis no tiene acceso a las claves de cifrado de extremo a extremo creadas por el usuario.

Acerca de Axis Communications

Axis contribuye a crear un mundo más inteligente y seguro mejorando la seguridad, la operatividad de las empresas y la inteligencia empresarial. Como líder del sector y empresa especializada en tecnología de redes, Axis ofrece videovigilancia, control de acceso, intercomunicadores y soluciones de audio. Su valor se multiplica gracias a las aplicaciones inteligentes de analítica y una formación de primer nivel.

Axis cuenta aproximadamente con 5.000 empleados especializados en más de 50 países y proporciona soluciones a sus clientes en colaboración con sus socios de tecnología e integración de sistemas. Axis fue fundada en 1984 y su sede central se encuentra en Lund (Suecia).aboutaxis_text2