AXIS OS

Guía de seguridad

AXIS OS Lifecycle guide | *AXIS OS Forensics Guide* | *AXIS OS Vulnerability Scanner Guide* | *Security Advisories* | *AXIS OS Release Notes* | *AXIS OS Knowledge base* | *AXIS OS YouTube playlist*

Introducción

La guía de seguridad de sistemas de AXIS OS ofrece orientación práctica para reforzar la seguridad de los dispositivos Axis que ejecutan AXIS OS. Describe las opciones de configuración, las funciones y las prácticas operativas recomendadas que ayudan a reducir la superficie de ataque, proteger los datos y garantizar un funcionamiento fiable durante todo el ciclo de vida del dispositivo. La guía está dirigida a administradores de sistemas, integradores y profesionales de seguridad que desean implementar y mantener productos Axis de forma segura y resistente, de acuerdo con las mejores prácticas de la industria.

Configuración de interfaz web
La guía hace referencia a la configuración de los ajustes del dispositivo en la interfaz web del dispositivo Axis. La ruta de configuración difiere en función de la versión de AXIS OS instalada en el dispositivo:

Versión de AXIS OS	Ruta de configuración de interfaz web
< 7.10	Setup > System Options > Security > IEEE 802.1X (Configuración > Opciones del sistema > Seguridad > IEEE 802.1X X)
7.10	Settings (Configuración) > System (sistema) > Security (Seguridad)
≥ 10.9	System (Sistema) > Security (Seguridad)

Ámbito

Esta guía se aplica a todos los productos basados en OS de AXIS en los que se ejecuta AXIS OS (LTS o seguimiento activo), así como a los productos antiguos con las versiones de software 4.xx y 5.xx.

Los productos basados en AXIS OS están diseñados para el uso en sistemas de seguridad profesional o de inteligencia empresarial y para integrarse con otros productos, como sistemas de gestión de vídeo (VMS) y aplicaciones de gestión de dispositivos.

El producto puede utilizarse en entornos no profesionales por personal con formación técnica, pero no está diseñado ni dirigido al uso doméstico por particulares.

El producto adopta un enfoque de seguridad predeterminada, pero para alcanzar mayores niveles de seguridad, es importante seguir esta Guía de seguridad. Existen guías de diseño de sistemas seguros disponibles para algunos sistemas integrados que puede consultar en *help.axis.com*.

Niveles de protección CIS

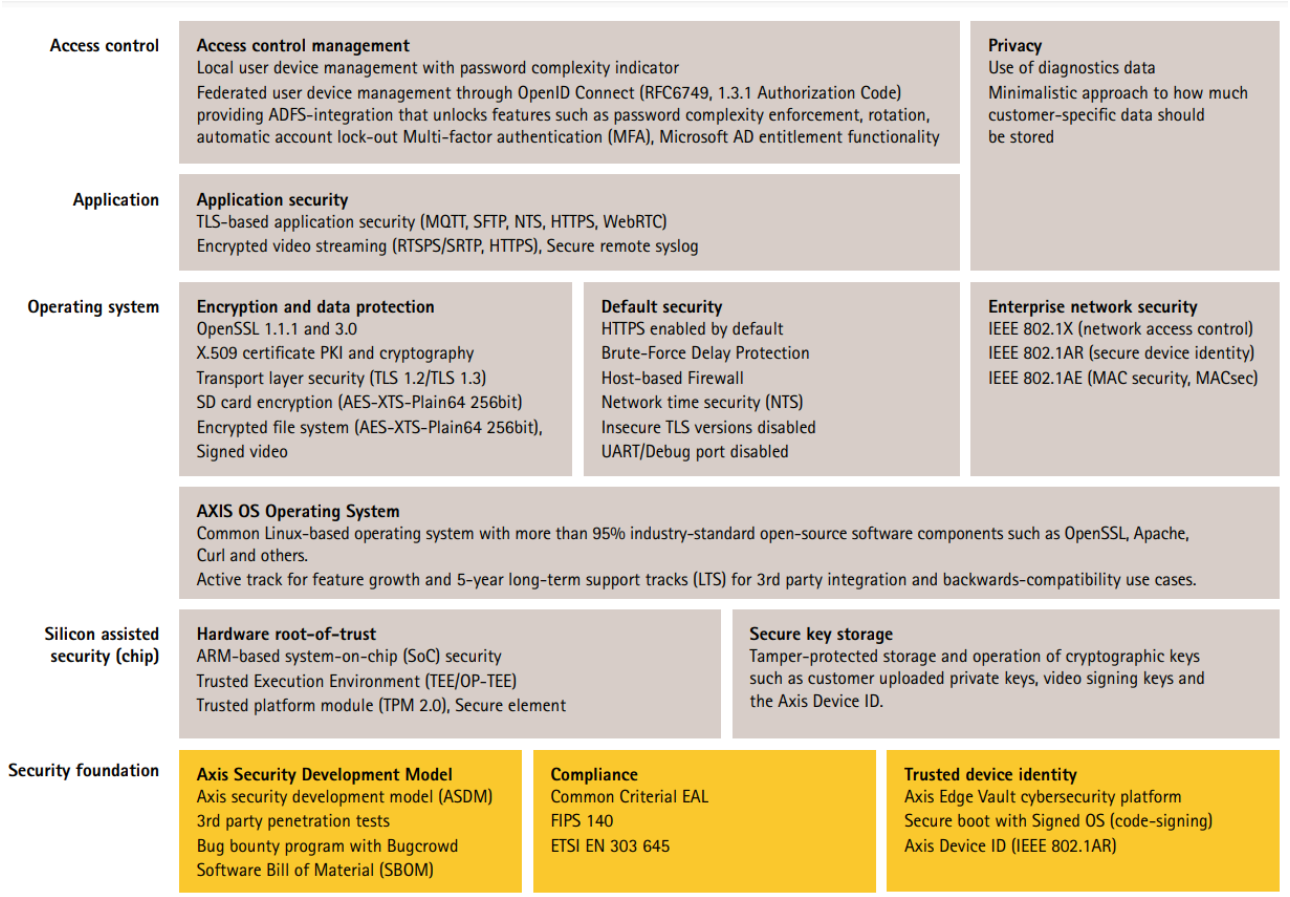
Seguimos los métodos descritos en el Center for Internet Safety (CIS) Controls Version 8 para estructurar nuestras recomendaciones sobre el marco de ciberseguridad. Los controles CIS, denominados SANS Top 20 Critical Security Controls, ofrecen 18 categorías de controles de seguridad críticos (DSC) centrados en hacer frente a las categorías de riesgo de ciberseguridad más habituales en una organización.

En esta guía se hace referencia a los controles de seguridad críticos agregando el número DSC (**N.º CSC**) para cada tema de protección. Para obtener más información sobre las categorías CSC, consulte los *18 controles de seguridad críticos de la CIS* en cisecurity.org.

Protección predeterminada

Los dispositivos Axis incluyen ajustes de protección predeterminados. Hay varios controles de seguridad que no es necesario configurar. Estos controles proporcionan un nivel básico de protección de los dispositivos y sirven de base para un mayor protección.

El diagrama de la arquitectura de seguridad de AXIS OS presenta las prestaciones de ciberseguridad de AXIS OS en diferentes capas. Ofrece un resumen completo de la estructura básica de seguridad, la seguridad asistida por silicio, el sistema operativo AXIS OS y la capa de control de acceso y aplicaciones.



Haga clic derecho y abra la imagen en una pestaña nueva para mejorar la visibilidad.

Autenticación

Desactivado de forma predeterminada

CSC n.º 4: Configuración segura de activos y software empresariales

El dispositivo Axis no funcionará hasta que se haya establecido la contraseña del administrador.

Después de configurar la contraseña del administrador, solo es posible acceder a las funciones de administrador o a las transmisiones de vídeo mediante la autenticación de credenciales de nombre de usuario y contraseña válidas. No recomendamos el uso de características que habiliten el acceso no autorizado, como la visualización anónima y el modo multicast siempre.

Para obtener información sobre cómo configurar el acceso a dispositivos, consulte *Acceso a dispositivos* en la base de conocimientos de AXIS OS.

Autenticación digest

CSC n.º 3: Protección de datos

Los clientes que accedan al dispositivo se autenticarán con una contraseña que debe cifrarse al enviarse a través de la red. Recomendamos habilitar HTTPS como se describe aquí. Si no fuera posible, le recomendamos utilizar únicamente la autentificación Digest en lugar de Basic o ambas, Basic y Digest. Esto reduce el riesgo de que los usuarios de la red se quejen de la contraseña.

Versión de AXIS OS	Ruta de configuración de interfaz web
< 7.10	Setup (Configuración) > System Options (Opciones del sistema) > Advanced (Avanzado) > Plain Config (Configuración sencilla) > Network (Red) > Network HTTP Authentication policy (Política de autenticación HTTP de red)
7.10	Settings (Configuración) > System (Sistema) > Plain config (Configuración sencilla) > Network (Red) > Network HTTP Authentication policy (Política de autenticación HTTP de red)
≥ 10.9	System (Sistema) > Plain config (Configuración sencilla) > Network (Red) > Network HTTP Authentication policy (Política de autenticación HTTP de red)

Protección contra ataques de reproducción ONVIF

CSC n.º 3: Protección de datos

La protección contra ataques por reproducción es una función de seguridad estándar activada de forma predeterminada en los dispositivos Axis. La finalidad es conseguir una autenticación de usuario basada en ONVIF lo suficientemente segura mediante la adición de un encabezado de seguridad adicional, que incluya el UsernameToken, la marca de tiempo válida, la nonce y el digest de contraseña. El digest de contraseña se calcula a partir de la contraseña (que ya está almacenada en el sistema), el valor nonce y la marca de hora. La finalidad del digest de la contraseña es validar al usuario y evitar ataques de reproducción, razón por la que los digests se almacenan en caché. Le recomendamos que mantenga activado este ajuste.

Versión de AXIS OS	Ruta de configuración de interfaz web
< 7.10	Setup (Configuración) > System Options (Opciones de sistema) > Advanced (Avanzado) > Plain Config (Configuración sencilla) > System (Sistema) > Enable Replay Attack Protection (Habilitar protección contra ataques por reproducción)
7.10	Settings (Configuración) > System (Sistema) > Plain config (Configuración sencilla) > WebService > Enable Replay Attack Protection (Habilitar protección contra ataques por reproducción)
≥ 10.9	System (Sistema) > Plain config (Configuración sencilla) > WebService > Enable Replay Attack Protection (Habilitar protección contra ataques por reproducción)

Evitar ataques de fuerza bruta

CSC n.º 4: Configuración segura de activos y software empresariales
CSC n.º 13: Supervisión y defensa de redes

Los dispositivos Axis cuentan con un mecanismo de prevención para identificar y bloquear ataques de fuerza bruta procedentes de la red, como la suposición de contraseñas. Esta característica, denominada protección contra retrasos por fuerza bruta, está disponible en AXIS OS 7.30 y posteriores.

La protección contra retrasos por fuerza bruta está activada de forma predeterminada a partir de AXIS OS 11.5. Para obtener ejemplos de configuración y recomendaciones detalladas, consulte *Protección contra retrasos por fuerza bruta* en la base de conocimientos de AXIS OS.

Versión de AXIS OS	Ruta de configuración de interfaz web
< 7.10	N/A
7.10	Settings (Configuración) > System (Sistema) > Plain config (Configuración sencilla) > System (Sistema) > PreventDosAttack
≥ 10.9	System (Sistema) > Security (Seguridad) > Prevent brute-force attacks (Evitar ataques de fuerza bruta)

Registro de auditoría

CSC n.º 1: Inventario y control de activos empresariales
CSC n.º 8: Gestión de registros de auditoría

Los registros de auditoría tienen fines relacionados con la ciberseguridad, como la gestión de incidentes y ayudar a establecer la supervisión a largo plazo de eventos y acciones relevantes. Recomendamos utilizar un servidor syslog remoto o alguna otra aplicación de supervisión de red para que el dispositivo Axis pueda enviar sus registros a un entorno de registro central. Esto simplifica el almacenamiento de los mensajes de registro y el tiempo de retención.

Para obtener más información, consulte *Audit Log (Registro de auditoría)* en la base de conocimientos de AXIS OS.

Versión de AXIS OS	**Ruta de configuración de interfaz web**
< 7.10	N/A
7.10	N/A
≥ 12.5	System (Sistema) > Logs (Registros)

Almacenamiento local

CSC n.º 4: Configuración segura de activos y software empresariales

CSC n.º 3: Protección de datos

A partir AXIS OS 12.0, se ha añadido la opción de montaje no ejecutable como opción opción predeterminada los recursos compartidos de red montados. Con esta acción impedirá cualquier ejecución directa de binarios desde el recurso compartido de red montado. Las tarjetas SD ya tenían esta opción incorporada en versiones anteriores de AXIS OS.

Además, los dispositivos Axis con AXIS OS 10.10 y versiones posteriores admiten la exportación cifrada de grabaciones de extremos. Le recomendamos que utilice esta función, ya que impide que personas no autorizadas puedan reproducir material de vídeo exportado.

Versión de AXIS OS	Ruta de configuración de interfaz web
< 7.10	N/A
7.10	N/A
≥ 10.9	Grabaciones

Seguridad de red

Protocolos de red

CSC n.º 4: Configuración segura de activos y software empresariales

De manera predeterminada, los dispositivos Axis tienen habilitados un número mínimo de protocolos y servicios de red, como se indica a continuación.

Protocolo	Puerto	Transporte	Comentarios
HTTP	80	TCP	El tráfico HTTP general, como el acceso a la interfaz web, la interfaz de la API VAPIX y ONVIF o la comunicación de extremo a extremo.*
HTTPS	443	TCP	El tráfico HTTPS general, como el acceso a la interfaz web, la interfaz de la API VAPIX y ONVIF o la comunicación de extremo a extremo.*
RTSP	554	TCP	Utilizado por el dispositivo Axis para la transmisión de vídeo/audio.
RTP	Rango de puertos efímero**	UDP	Utilizado por el dispositivo Axis para la transmisión de vídeo/audio.
UPnP	49152	TCP	Utilizado por aplicaciones de terceros para detectar el dispositivo Axis a través del protocolo de detección UPnP. **NOTA:** Deshabilitado de forma predeterminada a partir de AXIS OS 12.0.
Bonjour	5353	UDP	Utilizado por aplicaciones de terceros para detectar el dispositivo Axis a través del protocolo de detección mDNS (Bonjour).

Protocolo	Puerto	Transporte	Comentarios
SSDP	1900	UDP	Utilizado por aplicaciones de terceros para detectar el dispositivo Axis a través de SSDP (UPnP). **NOTA:** Deshabilitado de forma predeterminada a partir de AXIS OS 12.0.
WS-Discovery***	3702	UDP	Utilizado por aplicaciones de terceros para detectar el dispositivo Axis a través del protocolo de detección WS-Discovery (ONVIF).

* Consulte el documento técnico para obtener más información sobre la tecnología de extremo a extremo *Tecnología de extremo a extremo*.

**Asignado automáticamente dentro de un rango predefinido de números de puerto según RFC 6056. Para obtener más información, consulte el artículo de la Wikipedia sobre *Puerto efímero*.

*** El protocolo WebService Discovery (WS-Discovery) está deshabilitado de forma predeterminada en AXIS OS 12.1 y versiones posteriores.

Recomendamos desactivar los protocolos y servicios de red que no se utilicen siempre que sea posible. Para obtener una lista completa de los servicios que se utilizan de forma predeterminada o que se pueden activar en función de la configuración, consulte *Puertos de red utilizados habitualmente* en la base de conocimientos de AXIS OS.

Por ejemplo, debe habilitar manualmente la funcionalidad de entrada/salida de audio y micrófono en productos de videovigilancia de Axis como cámaras de red, mientras que en los altavoces de red y intercomunicadores Axis, la entrada/salida de audio y el micrófono son características clave activadas de forma predeterminada.

HTTPS activado

CSC n.º 3: Protección de datos

A partir de AXIS OS 7.20, HTTPS se ha habilitado de manera predeterminada con un certificado con firma propia que permite configurar la contraseña del dispositivo de una forma segura. En AXIS OS 10.10 y las versiones posteriores, el certificado con firma propia se ha sustituido por el certificado de ID de dispositivo seguro IEEE 802.1AR.

AXIS OS cuenta con los encabezados HTTP(s) relacionados con la seguridad más habituales activados de forma predeterminada para mejorar el nivel base de ciberseguridad en el estado predeterminado de fábrica. En AXIS OS 9.80 y las versiones posteriores, puede utilizar la API VAPIX de encabezado HTTP personalizada para configurar encabezados HTTP(s) adicionales.

Para obtener más información acerca de la API VAPIX del encabezado HTTP, consulte la *biblioteca VAPIX*.

Para obtener más información acerca de los encabezados HTTP(s) predeterminados, consulte *Encabezados HTTP (s) predeterminados* en la base de conocimientos de AXIS OS.

Versión de AXIS OS	Ruta de configuración de interfaz web
< 7.10	Setup (Configuración) > System Options (Opciones del sistema) > Security (Seguridad) > HTTPS
7.10	Settings (Configuración) > System (Sistema) > Security (Seguridad) > HTTP and HTTPS (HTTP y HTTPS)
≥ 10.9	System (Sistema) > Network (Red) > HTTP and HTTPS (HTTP y HTTPS)

Control de acceso a la red IEEE 802.1X

CSC n.º 6: Gestión del control de acceso
CSC n.º 13: Supervisión y defensa de redes

Los dispositivos Axis admiten el control de acceso a la red basado en puertos IEEE 802.1X mediante el método EAP-TLS. Para una protección óptima, recomendamos que utilice certificados de cliente firmados por una autoridad de certificación (CA) de confianza cuando autentique su dispositivo Axis.

Versión de AXIS OS	Ruta de configuración de interfaz web
< 7.10	Setup > System Options > Security > IEEE 802.1X (Configuración > Opciones del sistema > Seguridad > IEEE 802.1X X)
7.10	Settings (Configuración) > System (sistema) > Security (Seguridad) > IEEE 802.1X
≥ 10.9	System (Sistema) > Security (Seguridad) > IEEE 802.1X

En AXIS OS 12.6, hemos añadido la autentificación 802.1x a las grabadoras S3008 y S3008 MK II. Si conecta dispositivos con un ID de dispositivo Axis, pero sin compatibilidad con MACsec, vaya a **System (Sistema)> Network ports (Puertos de red)** y, en **Security (Seguridad)**, seleccione "Se requiere autentificación" para los puertos. Esto garantiza que solo se puedan conectar los dispositivos con un ID de dispositivo Axis.

IEEE 802.1AE MACsec

CSC n.º 3: Protección de datos
CSC n.º 6: Gestión del control de acceso

Los dispositivos Axis son compatibles con 802.1AE MACsec que es un protocolo de red bien definido que protege criptográficamente los enlaces Ethernet punto a punto en la capa de red 2, lo que garantiza la confidencialidad y la integridad de las transmisiones de datos entre dos hosts. Como MACsec funciona en la capa baja 2 de la pila de red, añade una capa de seguridad adicional a los protocolos de red que no ofrecen capacidades de cifrado nativa (ARP, NTP, DHCP, LLDP, NTP, ETC.), así como los que sí le ofrecen información sobre el protocolo de internet (HTTPS, TLS).

El estándar IEEE 802.1AE MACsec describe dos modos de funcionamiento: un modo CAK estático/de clave pre compartida (PSK) configurable manualmente y un modo CAK automático de sesión maestra/dinámico que utiliza sesiones IEEE 802.1X EAP-TLS. El dispositivo Axis admite los dos modos.

En AXIS OS 12.6, hemos añadido la compatibilidad con 802.1AE MACsec a las grabadoras S3008 y S3008 MK II. Si desea conectar dispositivos con un ID de Axis y compatibilidad con MACsec, vaya a **System (Sistema)> Network ports (Puertos de red)** y, en **Security (Seguridad)** , seleccione "Se requiere MACsec seguro". Esto se aplica tanto a la autentificación 802.1x como al cifrado MACsec.

Para obtener más información acerca de 802.1AE MACsec y cómo configurarlo en dispositivos con AXIS OS, consulte *IEEE 802.1AE* en la base de conocimientos de AXIS OS.

IEEE 802.1AR Identidad del dispositivo seguro

CSC n.º 1: Inventario y control de activos empresariales
CSC n.º 13: Supervisión y defensa de redes

Los dispositivos Axis con Axis Edge Vault son compatibles con el estándar de red IEEE 802.1AR, lo que permite la incorporación automatizada y segura de los dispositivos Axis a la red mediante el ID de dispositivo Axis, un certificado único instalado en el dispositivo durante la producción. Para ver un ejemplo de incorporación de dispositivos segura, consulte *Integración de dispositivos Axis segura en redes de Aruba*.

Para obtener más información, consulte el documento técnico *Axis Edge Vault*. Para descargar la cadena de certificados de ID de dispositivo de Axis, que se utiliza para validar la identidad del dispositivo de los dispositivos de Axis, consulte el *repositorio de infraestructura de clave pública* en axis.com.

Interfaz UART/de depuración

CSC n.º 4: Configuración segura de activos y software empresariales

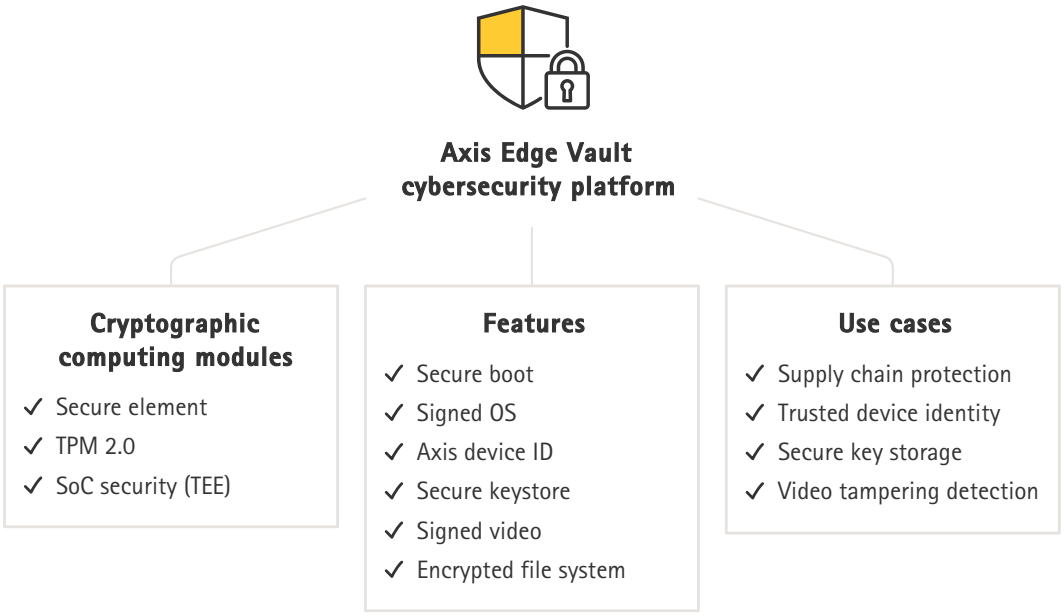
Todos los dispositivos Axis incluyen una interfaz física UART (Universal Asynchronous Receiver Transmitter), a veces denominada "puerto de depuración" o "consola serie". Sólo se puede acceder físicamente a la interfaz desmontando de forma exhaustiva el dispositivo Axis. La interfaz UART/de depuración se utiliza solo para el desarrollo y la depuración de productos durante proyectos internos de ingeniería de I+D dentro de Axis.

La interfaz UART/de depuración está activada de forma predeterminada en dispositivos Axis con AXIS OS 10.10 y versiones anteriores, pero requiere acceso autenticado y no expone ninguna información confidencial sin tener que autenticarse. A partir de AXIS OS 10.11, la interfaz UART/de depuración está desactivada de forma predeterminada. La única manera de activar la interfaz es desbloqueándola mediante un certificado personalizado exclusivo para dispositivos proporcionado por Axis.

Axis Edge Vault

Por su parte, Axis Edge Vault proporciona una plataforma de ciberseguridad de hardware que protege los dispositivos Axis. Tiene dos sólidos pilares: los módulos de computación criptográfica (elemento seguro y TPM) y la seguridad del SoC (TEE y arranque seguro), combinados con una amplia experiencia en la seguridad de los dispositivos en el extremo. Axis Edge Vault se basa en una sólida root de confianza establecida mediante un arranque seguro y un SO firmado. Estas funciones permiten una cadena ininterrumpida de software validado criptográficamente para la cadena de confianza de la que dependen todas las operaciones seguras

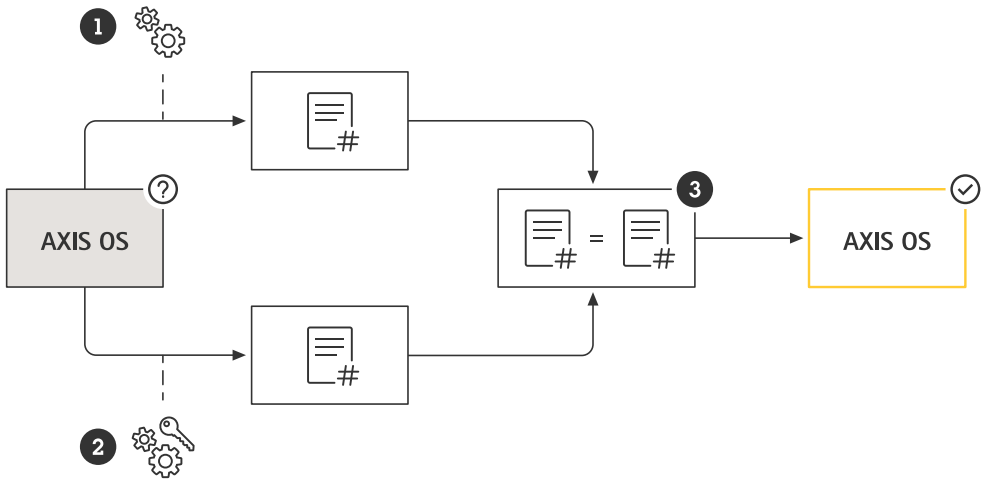
Los dispositivos con Axis Edge Vault minimizan la exposición a riesgos de ciberseguridad evitando escuchas ilegales y la eliminación maliciosa de información confidencial. Axis Edge Vault también garantiza que el dispositivo Axis es una unidad fiable y de confianza de la red.



SO firmado

CSC n.º 2: Inventario y control de activos de software

El AXIS OS está firmado a partir de la versión 9.20.1. Al actualizar la versión, el dispositivo comprobará la integridad de los archivos de actualización mediante la verificación de la firma criptográfica y rechazará cualquier archivo manipulado. De esta forma, se evitará que los atacantes engañen a los usuarios para que instalen archivos comprometidos.



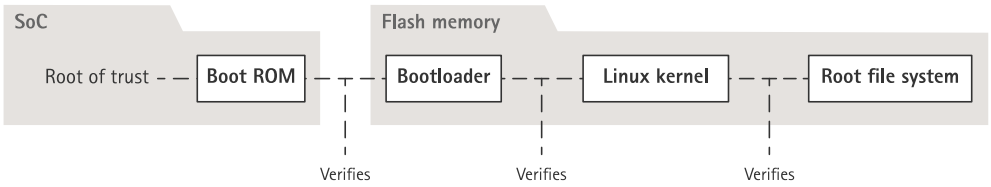
1) El dispositivo calcula el valor hash del AXIS OS. 2) El dispositivo utiliza la clave pública para descifrar la firma y obtener el valor hash. 3) Si los resultados coinciden, se verifica la firma del sistema operativo.

Para obtener más información, consulte el documento técnico *Axis Edge Vault*.

Arranque seguro

CSC n.º 2: Inventario y control de activos de software

Casi todos los dispositivos Axis disponen de una secuencia de arranque segura para proteger la integridad del dispositivo. El arranque seguro le impide implementar dispositivos Axis manipulados.

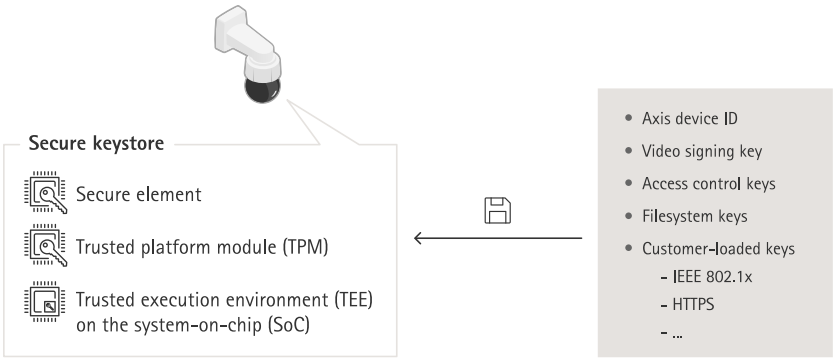


Para obtener más información, consulte el documento técnico *Axis Edge Vault*.

Almacén de claves seguro

CSC n.º 6: Gestión del control de acceso

el almacén de claves seguro es un espacio de almacenamiento para la información criptográfica que está integrado en el hardware y protegido frente a manipulaciones. Protege el ID del dispositivo Axis, así como la información criptográfica cargada por el cliente, al tiempo que evita el acceso no autorizado y las aplicaciones maliciosas en caso de una infracción de la seguridad. En función de los requisitos de seguridad, un dispositivo Axis puede tener uno o varios de estos módulos, como un TPM 2.0 (Módulo de plataforma de confianza) o un elemento seguro, o un entorno de ejecución de confianza (TEE).



Para obtener más información, consulte el documento técnico *Axis Edge Vault*.

Sistema de archivos cifrado

CSC n.º 3: Protección de datos

Un adversario malicioso podría tratar de extraer información del sistema de archivos desmontando la memoria flash y accediendo a ella a través de un dispositivo lector de memorias flash. Sin embargo, el dispositivo Axis puede proteger el sistema de archivos contra la exfiltración de datos maliciosa y la manipulación de la configuración en caso de que alguien obtenga acceso físico a él o lo robe. Cuando el dispositivo Axis está apagado, la información del sistema de archivos está cifrada en AES-XTS-Plain64 de 256 bits. Durante el proceso de arranque seguro, se descifra el sistema de archivos de lectura/escritura y el dispositivo Axis puede montarlo y utilizarlo.

Para obtener más información, consulte el documento técnico *Axis Edge Vault*.

Lista de materiales de software (SBOM)

CSC n.º 1: Inventario y control de activos empresariales

La lista de materiales de software (SBOM) para gestionar vulnerabilidades y mejorar la transparencia de la cadena de suministro es una herramienta vital para fomentar la confianza en los productos Axis. La SBOM se incluye con cada versión de software del dispositivo publicada en axis.com.

Desinstalación

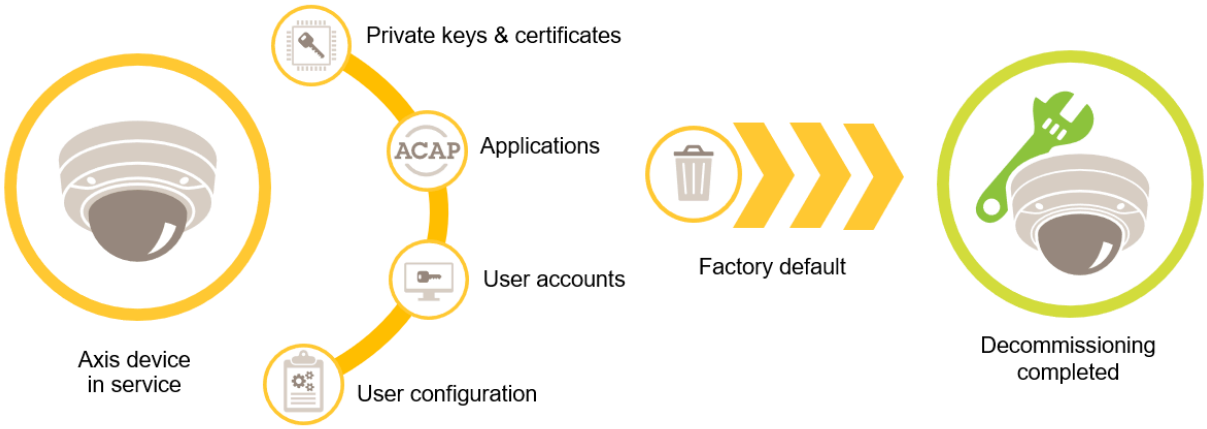
CSC n.º 3: Protección de datos

Los dispositivos Axis utilizan memoria volátil y no volátil. La memoria volátil se borra al desconectar el dispositivo de la fuente de alimentación, mientras que la información almacenada en la memoria no volátil se conserva y vuelve a estar disponible al iniciarlo. Evitamos la práctica habitual de eliminar simplemente los punteros de datos para que los datos almacenados sea invisibles para el sistema de archivos, por lo que es necesario restablecer los datos de fábrica. Para la memoria flash NAND, se utiliza la función UBI "Eliminar volumen". Se utiliza la función equivalente para la memoria flash eMMC, indicando que ya no se utilizan los bloques de almacenamiento. A continuación, el controlador de almacenamiento presentará dichos bloques de almacenamiento correspondientes.

Al desinstalar un dispositivo Axis, recomendamos restablecer el dispositivo a la configuración predeterminada de fábrica, que borrará los datos guardados en la memoria no volátil del dispositivo.

Tenga en cuenta que al aplicar un comando de restablecimiento a los ajustes predeterminados de fábrica no se borrarán inmediatamente los datos, sino que el dispositivo se reiniciará y el borrado de datos se producirá durante el arranque del sistema. Por lo tanto, no basta con generar el comando, sino que también se debe permitir que el dispositivo se reinicie y complete su arranque antes de apagarlo para garantizar que el borrado de datos se ha completado.

Este procedimiento de borrado de datos del cliente sigue la técnica de desinfección "Clear" descrita en NIST SP-800-88 Revisión 1.



Versión de AXIS OS	Ruta de configuración de interfaz web
< 7.10	Setup (Configuración) > System Options (Opciones del sistema) > Maintenance (Mantenimiento) > Default (Valor predeterminado)
7.10	Settings (Configuración) > System (Sistema) > Maintenance (Mantenimiento) > Default (Valor predeterminado)
≥ 10.9	Maintenance (Mantenimiento) > Default (Valor predeterminado)

Esta tabla contiene más información sobre los datos almacenados en la memoria no volátil.

Información y datos	**Se ha borrado después de los valores predeterminados de fábrica**
Nombres de usuario y contraseñas VAPIX y ONVIF	Sí
Certificados y claves privadas	Sí

Certificado con firma propia	Sí
Información almacenada en TPM y AXIS Edge Vault	Sí
Configuración de WLAN y usuarios/contraseñas	Sí
Certificados personalizados*	No
Clave de cifrado de tarjetas SD	Sí
Datos de tarjeta SD**	No
Configuración de recurso compartido de red y usuarios/contraseñas	Sí
Datos de recurso compartido de red**	No
Configuración del usuario***	Sí
Aplicaciones cargadas (ACAP)****	Sí
Datos de producción y estadísticas de vida útil****	No
Gráficos y superposiciones cargados	Sí
Datos del reloj RTC	Sí

* El proceso de SO firmado utiliza certificados personalizados que permiten a los usuarios cargar (entre otras cosas) AXIS OS.
** El usuario debe eliminar por separado las grabaciones e imágenes guardadas en el almacenamiento local (tarjeta SD, recurso compartido de red). El borrado de datos del cliente en la tarjeta SD se realiza de acuerdo con NIST SP-800-88 Revisión 1 Borrado criptográfico (CE) y para los datos en discos duros (grabador serie S30) es NIST SP-800-88 Revisión 1 Borrado. Para obtener más información, consulte en la base de conocimientos de AXIS OS.
*** Todas las configuraciones realizadas por el usuario, desde la creación de cuentas hasta las configuraciones de redes, O3C, eventos, imágenes, PTZ y sistemas.
**** El dispositivo conserva las aplicaciones preinstaladas, pero elimina todas las configuraciones que el usuario ha realizado en las mismas.
***** Los datos de producción (calibración, certificados de producción 802.1AR) y las estadísticas de ciclo de vida incluyen información no confidencial y no asociada al usuario.

Protección básica

La protección básica es el nivel de protección mínimo recomendado para los dispositivos Axis. Los diferentes aspectos de la protección básica pueden configurarse en local. Esto significa que se pueden configurar directamente en el dispositivo Axis sin dependencias adicionales a la infraestructura de red, el vídeo o los sistemas de gestión de pruebas (VMS, EMS), equipos o aplicaciones de terceros.

Ajustes predeterminados de fábrica

CSC n.º 4: Configuración segura de activos y software empresariales

Antes de configurar el dispositivo, asegúrese de que se encuentra en el estado predeterminado de fábrica. También es importante restablecer la configuración predeterminada de fábrica del dispositivo cuando sea necesario borrarlo de los datos del usuario o retirarlo. Para obtener más información, vea *Desinstalación, on page 12*.

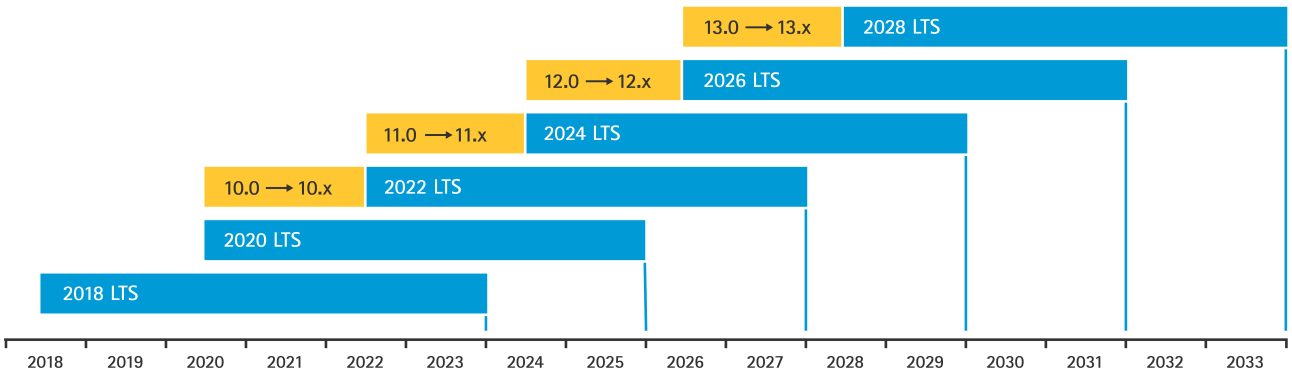
Versión de AXIS OS	Ruta de configuración de interfaz web
< 7.10	Setup (Configuración) > System Options (Opciones del sistema) > Maintenance (Mantenimiento) > Default (Valor predeterminado)
7.10	Settings (Configuración) > System (Sistema) > Maintenance (Mantenimiento) > Default (Valor predeterminado)
≥ 10.9	Mantenimiento > Ajustes predeterminados de fábrica

Actualización a la versión más reciente de AXIS OS

CSC n.º 2: Inventario y control de activos de software

La aplicación de parches para el software es un aspecto importante de la ciberseguridad. A menudo, los atacantes tratan de aprovechar las vulnerabilidades conocidas y pueden tener éxito si obtienen acceso de red a un servicio no autorizado. Asegúrese de utilizar siempre la última versión del AXIS OS, dado que puede incluir parches de seguridad para vulnerabilidades conocidas. Las notas de la versión de una versión específica pueden mencionar explícitamente una solución de seguridad crítica, pero no todas las correcciones generales.

Axis propone dos tipos de modelos para AXIS OS: seguimientos activos y seguimientos de soporte a largo plazo (LTS). Aunque ambos incluyen los parches más recientes para vulnerabilidades críticas, los seguimientos LTS no incluyen nuevas características, ya que el objetivo es minimizar el riesgo de problemas de compatibilidad. Para obtener más información, consulte *Ciclo de vida del sistema operativo AXIS* en la base de conocimientos de AXIS OS.



Axis ofrece una previsión de próximas versiones con información sobre nuevas características importantes, correcciones de errores y correcciones de seguridad. Para obtener más información, consulte *Próximas versiones* en la base de conocimientos de AXIS OS. Visite *Device software (Software del dispositivo)* en axis.com para descargar AXIS OS para su dispositivo.

Versión de AXIS OS	Ruta de configuración de interfaz web
< 7.10	Setup (Configuración) > System Options (Opciones de sistema) > Maintenance (Mantenimiento) > Upgrade Server (Actualizar servidor)
7.10	Settings (Configuración) > System (Sistema) > Maintenance (Mantenimiento) > Firmware upgrade (Actualización de firmware)
≥ 10.9	Mantenimiento > Actualización de AXIS OS

Crear cuentas dedicadas

CSC n.º 4: Configuración segura de activos y software empresariales
CSC n.º 5: Gestión de cuentas

Los dispositivos Axis pueden tener dos tipos de cuentas: una cuenta de administrador y una cuenta de usuario cliente. La cuenta de administrador es la cuenta principal para la gestión de su dispositivo y es esencial reservarla únicamente a tareas de administración. Al configurar su dispositivo, tendrá que crear un nombre de usuario y una contraseña para la cuenta de administrador.

Además de la cuenta de administrador, debe crear una cuenta de usuario cliente con privilegios limitados para las operaciones cotidianas. De este modo podrá gestionar su dispositivo de forma segura y evitará poner en riesgo la contraseña del administrador del dispositivo. Debe utilizar la cuenta de usuario cliente para tareas que no requieran privilegios de administración completos.

Al crear contraseñas para cualquiera de las dos cuentas, recomendamos que aplique directrices como las recomendaciones sobre contraseñas de NIST o de BSI, que exigen que las nuevas contraseñas sean suficientemente largas y complejas. Los dispositivos Axis admiten contraseñas de hasta 64 caracteres. Las contraseñas con menos de 8 caracteres se consideran débiles. Para obtener más información, consulte *Identity and access management (Identidad y gestión de acceso)* en la base de conocimientos AXIS OS.

Los dispositivos Axis que ejecutan AXIS OS 11.6 o superior son compatibles con OAuth 2.0, que permite la gestión centralizada de identidades y accesos (IAM) e identidades federadas para la autentificación en el dispositivo. Esto elimina la necesidad de administrar usuarios del dispositivo local. Para obtener más información, consulte *OAuth 2.0, on page 28*.

Versión de AXIS OS	Ruta de configuración de interfaz web
< 7.10	Setup (Configuración) > Basic Setup (Configuración básica) > Users (Usuarios)
7.10	Settings (Configuración) > System (Sistema) > Users (Usuarios)
≥ 10.9	System (Sistema) > Users (Usuarios)
= 11.6	System (Sistema) > Accounts (Cuentas)

Configurar los ajustes de red, fecha y hora

CSC n.º 4: CSC n.º 8: Gestión de registros de auditoría
CSC n.º 12: Gestión de infraestructuras de red

Es importante configurar correctamente los ajustes de red, fecha y hora del dispositivo para garantizar la funcionalidad y la seguridad del dispositivo Axis. Estos ajustes afectan a diferentes aspectos del comportamiento del dispositivo, como la comunicación de red, el registro y la validación de certificados.

La configuración de IP del dispositivo depende de la configuración de red, como IPv4/IPv6, la dirección de red estática o dinámica (DHCP), la máscara de subred y el router predeterminado. Revise la topología de su red cada

vez que añada nuevos componentes. Recomendamos que utilice una configuración de dirección IP estática para garantizar la accesibilidad a la red y minimizar las dependencias de servidores de red que puedan ser vulnerables a ataques, como servidores DHCP.

Versión de AXIS OS	Ruta de configuración de interfaz web
< 7.10	Setup (Configuración) > Basic Setup (Configuración básica) > TCP/IP
7.10	Settings (Configuración) > System (Sistema) > TCP/IP
≥ 10.9	System (Sistema) > Network (Red)

Es esencial una sincronización horaria precisa para mantener los registros del sistema, validar certificados digitales y habilitar servicios como HTTPS, IEEE y 802.1x. Recomendamos que sincronice el reloj de su dispositivo con servidores Network Time Protocol (NTP) o Network Time Security (NTS). Network Time Security (NTS), una variante cifrada y segura del Network Time Protocol (NTP), se incorporó en AXIS OS 11.1 Recomendamos que configure varios servidores de hora para conseguir una mayor precisión y para una mayor protección en caso de fallo. Si no puede alojar servidores de hora locales, valore la posibilidad de utilizar servidores NTP o NTS públicos. Para obtener más información sobre NTP/NTS en dispositivos Axis, consulte *NTP y NTS* en la base de conocimientos de AXIS OS.

Versión de AXIS OS	Ruta de configuración de interfaz web
< 7.10	Setup (Configuración) > Basic Setup (Configuración básica) > Date & Time (Fecha y hora)
7.10	Settings (Configuración) > System (Sistema) > Date and time (Fecha y hora)
≥ 10.9	System (Sistema) > Date and time (Fecha y hora)
= 11.6	System (Sistema) > Time and location (Hora y ubicación)

Cifrado de almacenamiento en local

CSC n.º 3: Protección de datos

Tarjeta SD
Si el dispositivo Axis admite y utiliza tarjetas Secure Digital (SD) para almacenar grabaciones de vídeo, recomendamos aplicar cifrado. Esto evitará que personas no autorizadas puedan reproducir el vídeo almacenado desde una tarjeta SD retiradas.

Para obtener más información sobre el cifrado de tarjetas SD en dispositivos Axis, consulte *compatibilidad con tarjetas SD* en la base de conocimientos de AXIS OS.

Versión de AXIS OS	Ruta de configuración de interfaz web
< 7.10	Setup (Configuración) > System Options (Opciones del sistema) > Storage (Almacenamiento)
7.10	Settings (Configuración) > System (Sistema) > Storage (Almacenamiento)
≥ 10.9	System (Sistema) > Storage (Almacenamiento)

Recurso compartido de red (NAS)
Si utiliza un almacenamiento en red tipo NAS como dispositivo de grabación, recomendamos mantenerlo en una zona cerrada con acceso limitado y activar el cifrado de disco duro en él. Los dispositivos Axis utilizan SMB

como protocolo de red para conectarse a un NAS para almacenar grabaciones de vídeo. Aunque las versiones anteriores de SMB (1.0 y 2.0) no proporcionan seguridad ni cifrado, las versiones posteriores (2.1 y posterior) sí, por lo que recomendamos usar versiones posteriores durante la producción.

Para obtener más información acerca de la configuración de SMB adecuada al conectar un dispositivo Axis a un recurso compartido de red, consulte *Recurso compartido de red* en la base de conocimientos de AXIS OS.

Versión de AXIS OS	Ruta de configuración de interfaz web
< 7.10	Setup (Configuración) > System Options (Opciones del sistema) > Storage (Almacenamiento)
7.10	Settings (Configuración) > System (Sistema) > Storage (Almacenamiento)
≥ 10.9	System (Sistema) > Storage (Almacenamiento)

Aplicaciones (ACAP)

CSC n.º 4: Configuración segura de activos y software empresariales

Puede cargar aplicaciones en el dispositivo Axis para ampliar su funcionalidad. Muchas de ellas cuentan con su propia interfaz de usuario para interactuar con una determinada función. Las aplicaciones pueden utilizar la funcionalidad de seguridad proporcionada por AXIS OS.

Los dispositivos Axis tienen instaladas varias aplicaciones desarrolladas por Axis según el *modelo de desarrollo de seguridad (ASDM) de Axis*. Para obtener más información sobre las aplicaciones axis, consulte *Analíticas* en axis.com.

En aplicaciones de terceros, recomendamos ponerse en contacto con el proveedor para obtener pruebas sobre la seguridad de la aplicación en términos de funcionamiento y pruebas, así como si se ha desarrollado según los modelos de desarrollo de seguridad recomendados habituales. Las vulnerabilidades detectadas en aplicaciones de terceros deben ser notificadas directamente a un proveedor externo.

Recomendamos que utilice solo aplicaciones de confianza y elimine aplicaciones que no se utilicen de los dispositivos Axis.

Versión de AXIS OS	Ruta de configuración de interfaz web
< 7.10	Setup (Configuración) > Applications (Aplicaciones)
7.10	Settings (Configuración) > Apps (Aplicaciones)
≥ 10.9	Aplicaciones

A partir de AXIS OS 12.0 (septiembre de 2024), la firma ACAP es obligatoria y está habilitada por defecto, con la opción de deshabilitarla. A partir de AXIS OS 13.0 (septiembre de 2026), la firma ACAP será obligatoria, sin opción de deshabilitarla. Los ACAP se firman en el portal ACAP mediante SHA-512 y una clave privada RSA de 4096 bits, almacenada de forma segura en un Thales Luna Network HSM 7 en el centro de datos de Axis en Lund, Suecia. Los dispositivos de red de Axis se suministran con la clave pública RSA de 4096 bits precargada para validar la firma ACAP antes de su instalación. La clave pública se almacena en el dispositivo de red de Axis, en el sistema de archivos Linux.

Desactivar servicios/funciones que no se utilizan

CSC n.º 4: Configuración segura de activos y software empresariales

Aunque los servicios y funciones que no se utilizan no suponen una amenaza inmediata para la seguridad, es buena práctica desactivarlos para reducir los riesgos innecesarios. Siga leyendo para obtener más información sobre los servicios y funciones que puede desactivar si no están en uso.

Acceso a la interfaz web

CSC n.º 4: Configuración segura de activos y software empresariales

CSC n.º 5: Gestión de cuentas

Los dispositivos Axis disponen de un servidor web que permite a los usuarios acceder al dispositivo a través de un navegador estándar. La interfaz web está destinada a la configuración, el mantenimiento y la resolución de problemas, no a las operaciones diarias como cliente para ver vídeos.

Los únicos clientes que deben permitirse interactuar con dispositivos Axis durante las operaciones diarias son los sistemas de gestión de vídeo (VMS) o herramientas de administración y gestión de dispositivos como AXIS Device Manager. Los usuarios del sistema nunca deben tener permiso para acceder directamente a dispositivos Axis.

A partir del AXIS OS 9.50, es posible desactivar la interfaz web de un dispositivo Axis. Una vez que implemente un dispositivo Axis en un sistema (o lo agregue a AXIS Device Manager), recomendamos que elimine la opción de que las personas de la organización accedan al dispositivo a través de un navegador web. Esto crea un nivel de seguridad adicional si la contraseña de la cuenta del dispositivo se comparte dentro de la organización. La opción más segura es configurar de forma exclusiva el acceso a dispositivos Axis a través de aplicaciones dedicadas que ofrecen arquitectura avanzada de gestión de acceso de identidad (ESO), más trazabilidad y garantías para evitar fugas de cuentas.

Versión de AXIS OS	Ruta de configuración de interfaz web
< 7.10	N/A
7.10	Settings (Configuración) > System (Sistema) > Plain config (Configuración sencilla)> System (Sistema) > Web Interface Disabled (Interfaz web desactivada)
≥ 10.9	System (Sistema) > Plain config (Configuración sencilla)> System (Sistema) > Web Interface Disabled (Interfaz web desactivada)

Puertos de red físicos sin utilizar

A partir de AXIS OS 11.2, los dispositivos con varios puertos de red, como AXIS S3008, tienen la opción de deshabilitar tanto el tráfico de PoE como de red de sus puertos de red. Dejar los puertos de red sin usar sin vigilancia y activos representa un riesgo de seguridad grave.

Versión de AXIS OS	Ruta de configuración de interfaz web
< 7.10	N/A
7.10	N/A
= 11.2	System (Sistema) > Power over Ethernet (Alimentación a través de Internet)

Protocolos de detección de red

Los protocolos de detección, como Bonjour, UPnP, ZeroConf y WS-Discovery y LLDP/CDP, son servicios de soporte que facilitan la búsqueda del dispositivo Axis y sus servicios en la red. Una vez que haya implementado el dispositivo y lo haya agregado al VMS, recomendamos que desactive el protocolo de detección para evitar que el dispositivo Axis anuncie su presencia en la red.

Versión de AXIS OS	Ruta de configuración de interfaz web
< 7.10	Setup (Configuración) > System Options (Opciones de sistema) > Advanced (Avanzado) > Plain Config (Configuración sencilla) > Network (Red) > Network Bonjour Enabled, Network UPnP Enabled, Network ZeroConf Enabled, Network UPnP NATTraversal Enabled* (Bonjour de red habilitado, UPnP de red habilitado, ZeroConf, de red habilitado, UPnP NATTraversal de red habilitado,*)
	N/A
7.10	Settings (Configuración) > System (Sistema) > Plain config (Configuración sencilla) > Network (Red) > Network Bonjour Enabled, Network UPnP Enabled, Network ZeroConf Enabled, Network UPnP NATTraversal Enabled* (Bonjour de red habilitado, UPnP de red habilitado, ZeroConf, de red habilitado, UPnP NATTraversal de red habilitado,*)
	Settings (Configuración) > System (Sistema) > Plain config (Configuración sencilla) > WebService > Discovery Mode (Modo de detección)
≥ 10.9	Settings (Configuración) > Plain config Configuración sencilla) > Network (Red) > Bonjour Enabled, UPnP Enabled, ZeroConf Enabled (Bonjour habilitado, UPnP habilitado, ZeroConf habilitado)
	System (Sistema) > Plain config (Configuración sencilla) > WebService > DiscoveryMode > Enable WS-Discovery discoverable mode (Habilitar modo de detección WS-Discovery)
≥ 11.11	System (Sistema) > Network (Red) > Network discovery protocols (Protocolos de detección de redes) > Bonjour, UPnP, WS-Discovery, LLDP y CDP**
	Settings (Configuración) > Plain config (Configuración sencilla) > Network (Red) > ZeroConf Enabled (ZeroConf habilitado)
≥12.1***	System (Sistema) > Network (Red) > Network discovery protocols (Protocolos de detección de redes) > Bonjour, LLDP y CDP**

* Esta funcionalidad se eliminó de AXIS OS 10.12 y no está disponible en versiones posteriores.

** Si se desactiva LLDP y CPD podría afectar a la negociación de alimentación PoE.
*** De forma predeterminada a partir de esta versión, ya no es preciso deshabilitar ZeroConf. Se utiliza una dirección de enlace local como alternativa cuando DHCP no está disponible y no se ha configurado ninguna dirección IP estática.

Divulgación de información

De manera predeterminada, los dispositivos Axis anuncian las versiones de software básicas de sus versiones actuales de software Apache, OpenSSL y AXIS OS durante las conexiones HTTP(S) con clientes en red o a través de la API de información básica del dispositivo VAPIX (*https://developer.axis.com/vapix/network-video/basic-device-information/*).

Esta información es fundamental para que los escáneres de seguridad de red o los sistemas de supervisión de red como Rapid7, Tenable Nessus y otros escaneen los dispositivos Axis en busca de vulnerabilidades destacadas. Sin esta información, es posible que estas aplicaciones no funcionen correctamente en dispositivos Axis. En general, Axis recomienda tener habilitada y funcional la divulgación de información, dado que ayuda a mantener las actualizaciones de software, el conocimiento de la situación, la supervisión y el funcionamiento seguro de los dispositivos Axis.

No obstante, algunos enfoques de ciberseguridad requieren mantener al mínimo, o desactivar por completo, la divulgación de información. Para cumplir este requisito, existen parámetros de configuración que permiten desactivar la divulgación de información. Sin embargo, solo recomendamos la desactivación si utiliza su dispositivo de acuerdo con nuestras recomendaciones y lo mantiene actualizado en todo momento.

Versiones de Apache/OpenSSL

La opción de desactivar los encabezados del servidor HTTP(S) para reducir la exposición de información durante las conexiones HTTP(S) está disponible a partir de AXIS OS 10.6.

Versión de AXIS OS	Ruta de configuración de interfaz web
< 7.10	N/A
7.10	Settings (Configuración) > System (Sistema) > Plain config (Configuración sencilla) > System (Sistema) > HTTP Server Header Comments (Comentarios de encabezado de servidor HTTP)

≥ 11.11	*https://IP_OR_HOSTNAME/config/web-ui/swagger-ui/?url=/config/discover/apis/basic-device-info/v2/openapi.json#/basic-device-info.v2beta/patch_basic_device_info_v2beta_allowAnonymous*
	
	{
	"datos": falso
	}

Audio

De forma predeterminada, los productos orientados a la videovigilancia de Axis, como las cámaras de red, la entrada/salida de audio y el micrófono, están desactivados. Si necesita capacidades de audio, debe habilitarlas antes de utilizarlas. En los productos Axis, en los que la funcionalidad de entrada/salida de audio y micrófono son características clave, como los intercomunicadores y los altavoces de red de Axis, las capacidades de audio están activadas de forma predeterminada.

Si no las utiliza, le recomendamos que desactive las capacidades de audio.

Versión de AXIS OS	Ruta de configuración de interfaz web
< 7.10	Setup (Configuración) > System Options (Opciones de sistema) > Advanced (Avanzado) > Plain Config (Configuración sencilla) > Audio > Audio A* > Enabled (Habilitado)
7.10	Settings (Configuración) > Audio > Allow audio (Permitir audio)
≥ 10.9	Audio > Device settings (Configuración de dispositivo)

Ranura(s) para tarjetas SD

Por lo general, los dispositivos Axis admiten al menos una tarjeta SD para el almacenamiento en el extremo local de grabaciones de vídeo. Si no se utilizan tarjetas SD, recomendamos desactivar completamente la ranura para tarjetas SD. La opción para desactivar la ranura para tarjetas SD está disponible en AXIS OS 9.80

Para obtener más información, consulte *Desactivación de la tarjeta SD* en la base de conocimientos de AXIS OS.

Versión de AXIS OS	Ruta de configuración de interfaz web
< 7.10	N/A
7.10	Settings (Configuración) > System (Sistema) > Plain config (Configuración sencilla) > Storage (Almacenamiento) > SD Disk Enabled (Disco SD habilitado)
≥ 10.9	System (Sistema) > Plain config (Configuración sencilla) > Storage (Almacenamiento) > SD Disk Enabled (Disco SD habilitado)

Acceso a SSH

SSH es un protocolo de comunicación seguro que se utiliza únicamente para la localización de problemas y la depuración. Es compatible con dispositivos Axis a partir de AXIS OS 5.50. Recomendamos desactivar el acceso SSH.

Para obtener más información acerca de las opciones de depuración mediante SSH, consulte *Acceso SSH* en la base de conocimientos de AXIS OS.

Versión de AXIS OS	Ruta de configuración de interfaz web
< 7.10	Setup (Configuración) > System Options (Opciones de sistema) > Plain Config (Configuración sencilla) > Network (Red) > SSH Enabled (SSH activado)
7.10	Settings (Configuración) > System (Sistema) > Plain config (Configuración sencilla) > Network (Red) > SSH Enabled (SSH activado)
≥ 10.9	System (Configuración) > Plain config (Configuración sencilla > Network (Red) > SSH Enabled (SSH activado)

USB

A partir de AXIS OS 12.1, el AXIS D1110 incluye la opción de desactivar el puerto USB. Dejar los puertos USB sin usar sin vigilancia y activos representa un riesgo de seguridad grave.

Versión de AXIS OS	Ruta de configuración de interfaz web
< 7.10	N/A
7.10	N/A
≥ 12.1	System (Sistema) > > Accessories (Accesorios) > USB Configuration (Configuración USB)

Capacidades Wi-Fi

Algunos dispositivos Axis ofrecen capacidades Wi-Fi mediante un punto de acceso integrado a través de una llave USB Wi-Fi. El Wi-Fi solo se activa al pulsar el botón físico de configuración WLAN cuando no existe una conexión de red RJ45 física. Esto es así independientemente de si el dispositivo tiene la configuración predeterminada de fábrica o si está operativo. En AXIS M1075, el usuario puede conectarse al punto de acceso mediante el SSID y la contraseña SSID exclusiva del dispositivo, que se encuentran en la etiqueta del producto. En algunos productos Axis más recientes, solo se requiere el SSID (sin contraseña), lo que mejora la experiencia de instalación y no compromete la ciberseguridad.

Consulte el manual del usuario para configurar su dispositivo Axis y sus capacidades Wi-Fi. A continuación, se explica el funcionamiento de las capacidades integradas del punto de acceso en algunos productos Axis compatibles con Wi-Fi:

- El punto de acceso integrado solo se puede habilitar pulsando el botón físico de configuración WLAN, siempre que no se haya configurado ningún SSID/contraseña Wi-Fi ni exista una conexión de red RJ45 física. Esto es así independientemente de si el dispositivo tiene la configuración predeterminada de fábrica o si está operativo.
- El punto de acceso integrado se desactiva una vez que la cámara se conecta a un punto de acceso configurado por el usuario. Como alternativa, se desactiva automáticamente 15 minutos después de que el usuario presione el botón físico de configuración WLAN durante la instalación.

Si el dispositivo emplea un adaptador Wi-Fi conectado, se recomienda configurar correctamente las funciones Wi-Fi utilizando un SSID y una contraseña durante la configuración inicial del dispositivo, para ofrecer mayor seguridad.

Bluetooth

Algunos dispositivos Axis específicos brindan capacidad Bluetooth, que puede utilizar para disfrutar de una experiencia de usuario fluida al configurar el dispositivo en su estado inicial después de restablecer los valores predeterminados de fábrica, por ejemplo, para ajustar la imagen y las lentes.

Consulte el manual de usuario de su dispositivo para conocer su configuración y capacidades Bluetooth. Las siguientes descripciones explican las capacidades generales de Bluetooth de los productos Axis:

- Bluetooth se activa automáticamente en el estado predeterminado de fábrica siempre que no exista ningún usuario configurado y durante un máximo de 2 horas después de la puesta en funcionamiento inicial. Bluetooth se desactiva automáticamente al configurar un usuario o 2 horas después de la puesta en funcionamiento inicial, independientemente de si existe o no una conexión de red RJ45 física.
- Una vez desactivado el Bluetooth, el usuario no podrá activarlo manualmente. Solo podrá restablecer la funcionalidad de Bluetooth volviendo a restaurar el dispositivo a su estado predeterminado de fábrica.
- La conexión Bluetooth de su dispositivo al dispositivo Axis utiliza un túnel HTTPS que emplea el último cifrado TLS 1.2/1.3. Los productos de Axis utilizan el modo de seguridad Bluetooth 1, nivel 2 (cifrado con emparejamiento sin autentificación, Just Works).

Limitar el acceso a la red

CSC n.º 1: Inventario y control de activos empresariales
CSC n.º 4: Configuración segura de activos y software empresariales
CSC n.º 13: Supervisión y defensa de redes

Desde AXIS OS 11.9, se introdujo un firewall basado en host, una función de seguridad que permite crear reglas que regulan el tráfico entrante por dirección IP y/o números de puerto TCP/UDP. Esta prestación ayuda a evitar el acceso no autorizado al dispositivo o a sus servicios.

Si establece la política predeterminada en "Soltar", asegúrese de añadir a su lista todos los clientes (VMS y clientes administrativos) y/o puertos autorizados.

Versión de AXIS OS	Ruta de configuración de interfaz web
≥ 11.9	Sistema > Seguridad > Firewall

Filtrado de direcciones IP

Los dispositivos con AXIS OS 11.8 y versiones anteriores utilizan el filtrado de direcciones IP para evitar el acceso de clientes no autorizados. Recomendamos configurar su dispositivo para permitir direcciones IP de host de red autorizadas o denegar las no autorizadas.

Si decide permitir direcciones IP, asegúrese de añadir a su lista todos los clientes autorizados, como servidores VMS y clientes administrativos.

Versión de AXIS OS	Ruta de configuración de interfaz web
< 7.10	Setup (Configuración) > System Options (Opciones de sistema) > Security (Seguridad) > IP Address Filter (Filtro de direcciones IP)
7.10	Settings (Configuración) > System (Sistema) > TCP/IP > IP address filter (Filtro de direcciones IP)
10.9 — 11.8	Settings (Configuración) > Security (Seguridad) > IP address filter (Filtro de direcciones IP)

Nota

Puede configurar registros más detallados de los intentos de acceso a la red para ayudarle a identificar intentos de acceso no deseados desde otros hosts de red. Para ello, vaya a **System (Sistema)** > **Plain config (Configuración sencilla)** > **Network (Red)** y acceda al registro de filtros de red.

HTTPS

CSC n.º 3: Protección de datos

HTTP y HTTPS están activados de forma predeterminada en los dispositivos Axis a partir de AXIS OS 7.20. El acceso HTTP no es seguro y no incluye ningún tipo de cifrado, mientras que HTTPS cifra el tráfico entre el cliente y el dispositivo Axis. Recomendamos que utilice HTTPS para todas las tareas administrativas del dispositivo Axis.

Para obtener instrucciones de configuración, consulte *HTTPS only, on page 24* y *Codificadores HTTPS, on page 25*.

HTTPS only

Le recomendamos que configure el dispositivo de Axis para que utilice HTTPS solo (sin que sea posible acceder a HTTP). Esto activará automáticamente HSTS (HTTP Strict Transport Security), lo que mejorará aún más la seguridad del dispositivo.

A partir de AXIS OS 7.20, los dispositivos Axis incluyen un certificado autofirmado válido hasta el 19/01/2038. Si bien un certificado autofirmado no es fiable por diseño, sí es suficiente para acceder de forma segura al dispositivo Axis durante la configuración inicial y cuando no se dispone de una infraestructura de clave pública (PKI). Si se encuentra disponible, el certificado con firma propia debe eliminarse y sustituirse por los certificados de cliente firmados correctamente emitidos por una autoridad de PKI de elección. A partir de AXIS OS 10.10, el certificado con firma propia se ha sustituido por el certificado de ID de dispositivo seguro IEEE 802.1AR.

Versión de AXIS OS	Ruta de configuración de interfaz web
< 7.10	Setup (Configuración) > System Options (Opciones del sistema) > Security (Seguridad) > HTTPS
7.10	Settings (Configuración) > System (Sistema) > Security (Seguridad) > HTTP and HTTPS (HTTP y HTTPS)
≥ 10.9	System (Sistema) > Network (Red) > HTTP and HTTPS (HTTP y HTTPS)

Codificadores HTTPS

Los dispositivos Axis admiten y utilizan los conjuntos de cifrado TLS 1.2 y TLS 1.3 para cifrar de forma segura las conexiones HTTPS. La versión y el conjunto de cifrado TLS específicos utilizados dependen del cliente que se conecta al dispositivo de Axis y se negociará en consecuencia. A lo largo de actualizaciones periódicas de AXIS OS, la lista de codificadores disponibles del dispositivo Axis puede recibir actualizaciones sin que el sistema de cifrado configuración cambie. Un cambio de configuraciones de cifrado debe iniciarse por el usuario, ya sea realizando un restablecimiento de la configuración predeterminada de fábrica del dispositivo Axis o a través de una configuración manual del usuario. A partir de AXIS OS 10.8 y posterior, la lista de codificadores se actualiza automáticamente cuando el usuario realiza una actualización de AXIS OS.

TLS 1.2 e inferior

Al utilizar TLS 1.2 o inferior, puede especificar los codificadores HTTPS que el dispositivo Axis utilizará cuando se reinicie. No hay restricciones a los codificadores que puede elegir, pero le recomendamos que seleccione cualquiera de los siguientes cifrados fuertes o todos:

```
ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-
AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-
POLY1305:ECDHE-RSA-CHACHA20-POLY1305
```

Versión de AXIS OS	Ruta de configuración de interfaz web
< 7.10	Setup (Configuración)> System Options (Opciones de sistema) > Advanced (Avanzado) > Plain Config (Configuración sencilla) > HTTPS > Ciphers (Cifrados)
7.10	Settings (Configuración) > System (Sistema) > Plain config (Configuración sencilla) > HTTPS > Ciphers (Cifrados)
≥ 10.9	System (Sistema) > Plain config (Configuración sencilla) > HTTPS > Ciphers (Cifrados)

TLS 1.3

De forma predeterminada, solo están disponibles los conjuntos de cifrado fuertes según las especificaciones TLS 1.3:

```
TLS_AES_128_GCM_SHA256:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_256_GCM_
SHA384
```

El usuario no puede configurar estas suites.

Protección ampliada

Las instrucciones de protección ampliada se basan en los temas de protección descritos en *Protección predeterminada, on page 4* y *Protección básica, on page 15*. No obstante, aunque puede aplicar las instrucciones de protección predeterminadas y básicas directamente en su dispositivo Axis, el sistema de protección ampliado requiere la participación activa de toda la cadena de suministro del proveedor, la organización del usuario final y la infraestructura de TI y/o red existentes.

Limitar la exposición a internet y las redes

CSC n.º 12: Gestión de infraestructuras de red

Recomendamos que evite exponer cualquier dispositivo Axis como servidor web público o permitir cualquier otro tipo de acceso al dispositivo desde redes de clientes desconocidas. En el caso de pequeñas organizaciones y particulares que no utilizan software de gestión de vídeo (VMS) o que necesitan acceder a vídeo desde ubicaciones remotas, AXIS Camera Station Edge es una buena opción.

AXIS Camera Station Edge está disponible en Windows, iOS y Android, de forma gratuita, y ofrece una forma sencilla de acceder a vídeos de forma segura sin exponer el dispositivo a internet. Para obtener más información, consulte *axis.com/products/axis-camera-station-edge*.

Nota

Si su organización utiliza un VMS, consulte con el proveedor de su VMS para conocer las prácticas recomendadas en relación con el acceso remoto a vídeo.

Aislar los dispositivos de red y las infraestructuras y aplicaciones relacionadas reduce el riesgo de exposición a la red.

Recomendamos que aísle sus dispositivos Axis y las infraestructuras y aplicaciones relacionadas en una red local separada de su red de producción y empresarial.

Para aplicar protección básica, proteja la red local y su infraestructura (router, switches) frente a accesos no autorizados utilizando diferentes mecanismos de seguridad de red. Estos métodos pueden incluir segmentación de VLAN, restricciones de enrutamiento, VPN para acceso de sitio a sitio o WAN, cortafuegos de red de capas 2/3 y listas de control de acceso (ACL).

Para reforzar la protección básica, puede aplicar técnicas avanzadas de inspección de redes, como la inspección profunda de paquetes y la detección de intrusiones. De este modo mejorará la protección contra amenazas en la red. Tenga en cuenta que la protección de red ampliada de las redes suele requerir software y/o dispositivos de hardware especializados.

Barrido de vulnerabilidades de red

CSC n.º 1: Inventario y control de activos empresariales
CSC n.º 12: Gestión de infraestructuras de red

Puede utilizar escáneres de seguridad de red para realizar evaluaciones de vulnerabilidad de sus dispositivos de red. El propósito de una evaluación de la vulnerabilidad es proporcionar una revisión sistemática de las vulnerabilidades de seguridad potenciales y de las configuraciones incorrectas.

Recomendamos que realice evaluaciones periódicas de vulnerabilidad de sus dispositivos Axis y de su infraestructura relacionada. Antes de iniciar el barrido, asegúrese de que sus dispositivos Axis se han actualizado a la última versión disponible de AXIS OS, en LTS o en la ruta activa.

También recomendamos revisar el informe de barrido y filtrar falsos positivos conocidos para dispositivos Axis, que encontrará en la *AXIS OS Vulnerability Scanner Guide (Guía del escáner de vulnerabilidades de AXIS OS)*. Envíe el informe y las solicitudes adicionales en un ticket o al *Servicio de asistencia técnica de Axis* en axis.com.

Infraestructura de clave pública de confianza (PKI)

CSC n.º 3: Protección de datos
CSC n.º 12: Gestión de infraestructuras de red

Recomendamos que implemente certificados de cliente y servidor web en sus dispositivos Axis de confianza con firma de una autoridad de certificación pública o privada. Un certificado firmado por CA con una cadena de confianza validada ayuda a eliminar las advertencias de certificados del navegador cuando se conecta a través de HTTPS. Un certificado firmado por CA también garantiza la autenticidad del dispositivo Axis cuando implementa una solución de control de acceso a la red (NAC). Así se reduce el riesgo de ataques desde un ordenador que simula un dispositivo Axis.

Puede utilizar AXIS Device Manager, que viene con un servicio de autoridad de certificación integrado, para emitir certificados con firma para dispositivos Axis.

Syslog remoto

CSC n.º 8: Gestión de registros de auditoría

Puede configurar un dispositivo Axis para que envíe todos sus mensajes de registro cifrados a un servidor syslog central. Esto facilita las auditorías y evita que los mensajes de registro se eliminen en el dispositivo Axis, ya sea intencionada/maliciosamente o de forma no intencionada. En función de las políticas de la empresa, también puede ofrecer un tiempo de conservación ampliado de los registros de dispositivos.

Para obtener más información sobre cómo habilitar el servidor syslog remoto en distintas versiones del sistema operativo AXIS, consulte *Syslog* en la base de conocimientos de AXIS OS.

Versión de AXIS OS	Ruta de configuración de interfaz web
< 7.10	Para obtener instrucciones, consulte *Syslog* en la guía AXIS OS Lifecycle.
7.10	Settings (Configuración) > System (Sistema) > TCP/IP
≥ 10.9	System (Sistema) > Logs (Registros)

SNMP

CSC n.º 3: Protección de datos
CSC n.º 8: Gestión de registros de auditoría

Puede configurar un dispositivo Axis para que envíe datos cifrados de supervisión de estado del SNMP a un servidor SNMP central a través de SNMPv3. La supervisión de red basada en SNMP permite crear alertas y supervisar el dispositivo durante un largo tiempo. Recuerde que solo SNMPv3 ofrece cifrado y privacidad, por lo que recomendamos firmemente su uso en lugar de SNMPv1 y SNMPv2c.

Más información sobre *SNMP* en la base de conocimientos de AXIS OS.

Versión de AXIS OS	**Ruta de configuración de interfaz web**
< 7.10	Para obtener instrucciones, consulte *SNMP* en la base de conocimientos de AXIS OS.
7.10	Settings (Configuración) > System (Sistema) Network (Red) > SNMP
≥ 10.9	System (Sistema) > Network (Red) > SNMP

Transmisión de vídeo segura (SRTP/RTSPS)

CSC n.º 3: Protección de datos

A partir de AXIS OS 7.40, los dispositivos Axis son compatibles con la transmisión segura de vídeo a través de RTP, también denominada SRTP/RTSPS. SRTP/RTSPS utiliza un método de transporte cifrado seguro de extremo a extremo para garantizar que solo los clientes autorizados reciban la transmisión de vídeo del dispositivo Axis.

Recomendamos habilitar SRTP/RTSPS si su sistema de gestión de vídeo (VMS) lo admite. Si está disponible, utilice SRTP en lugar de transmisión de vídeo RTP sin cifrar.

Nota

SRTP/RTSPS solo cifra los datos de transmisión de vídeo. En el caso de tareas de configuración administrativa, recomendamos habilitar HTTPS solo para cifrar este tipo de comunicación.

Versión de AXIS OS	Ruta de configuración de interfaz web
< 7.10	Setup (Configuración) > System Options (Opciones de sistema) > Advanced (Avanzado) > Plain Config (Configuración sencilla) > Network (Red) > RTSPS
7.10	Settings (Configuración) > System (Sistema) > Plain config (Configuración sencilla) > Network (Red) > RTSPS
≥ 10.9	System (Sistema) > Plain config (Configuración sencilla) > Network (Red) > RTSPS

Vídeo firmado

CSC n.º 3: Protección de datos

A partir de AXIS OS 10.11, los dispositivos Axis con Axis Edge Vault admiten vídeo firmado, mediante el que los dispositivos Axis pueden añadir una firma a su transmisión de vídeo para garantizar que este permanezca intacto y poder verificar su origen, rastreándolo hasta el dispositivo que lo generó.

Axis proporciona la herramienta *Axis Signed media verifier*, que puede utilizar para verificar la autenticidad de los vídeos grabados desde un dispositivo Axis. Ofrecemos estos tres archivos de muestra que puede utilizar para explorar la herramienta.

- *Vídeo original, pero sin firmar*
- *Vídeo original y firmado*
- *Vídeo manipulado*

El sistema de gestión de vídeo (VMS) o el sistema de gestión de pruebas (EMS) también pueden verificar la autenticidad del vídeo proporcionado por un dispositivo Axis.

Para obtener más información, consulte el documento técnico *Axis Edge Vault*. Para buscar los certificados root de Axis que se utilizan para validar la autenticidad del vídeo firmado, consulte *Acceso al dispositivo* en la base de conocimientos de AXIS OS.

Versión de AXIS OS	Ruta de configuración de interfaz web
< 7.10	N/A
7.10	N/A
≥ 10.9	System (Sistema) > Plain config (Configuración sencilla) > Image (Imagen) > SignedVideo (Vídeo firmado)

OAuth 2.0

CSC n.º 4: Configuración segura de activos y software empresariales
CSC n.º 5: Gestión de cuentas

Con OAuth 2.0, puede incorporar dispositivos AXIS OS que ejecuten AXIS OS 11.6 o superior en una infraestructura de TI con un servicio de gestión de identidad y acceso (IAM) centralizado. Esto permite usar identidades federadas para autentificarse en el dispositivo Axis, eliminando la necesidad de administrar usuarios del dispositivo local.

OAuth mitiga los ataques CSRF por medio de un token exclusivo para garantizar la validez de cada solicitud.

Dependiendo de las características del proveedor de servicios, puede aplicar los siguientes mecanismos de seguridad para una autentificación mejorada basada en identidad en el dispositivo Axis:

- Autentificación multifactor (MFA)
- Aplicación de la complejidad de las contraseñas
- Rotación de contraseñas
- Autentificación por tiempo limitado
- Gestión centralizada de identidades (cuenta de usuario/servicio)

Para obtener más información sobre cómo habilitar y configurar OAuth 2.0 en dispositivos AXIS OS, consulte *OAuth 2.0 OpenID Connect* en la base de conocimientos de AXIS OS.

Versión de AXIS OS	**Ruta de configuración de interfaz web**
< 7.10	N/A
7.10	N/A
= 11.6	System (Sistema) > Accounts (Cuentas) > OpenID Configuration (Configuración de OpenID)

Accesorios antimanipulación física

CSC n.º 1: Inventario y control de activos empresariales
CSC n.º 12: Gestión de infraestructuras de red

Axis ofrece switches contra intrusión física y/o antimanipulación como accesorios opcionales para mejorar la protección física de los dispositivos Axis. Estos switches pueden activar una alarma que permite que los dispositivos Axis envíen una notificación o una alarma a clientes seleccionados.

Para obtener más información sobre los accesorios antimanipulación disponibles, consulte:

- *AXIS TA8501 Physical Tampering Switch*
- *AXIS Dome Intrusion Switch C*
- *Interruptor de puerta A de AXIS*

Protección de aspectos heredados

Esta sección incluye instrucciones de seguridad dirigidas a proteger las configuraciones de los parámetros que se encuentran en versiones o productos antiguos del AXIS OS. Estos parámetros no se encuentran en las rutas LTS más recientes o nuevas ni en la pista activa.

Entorno de editor de secuencias de comandos

Recomendamos deshabilitar el acceso al entorno del editor de secuencias de comandos. El editor de secuencias de comandos se utiliza únicamente para fines de localización de problemas y depuración.

El editor de secuencias de comandos se eliminó de AXIS OS 10.11 y no está disponible en versiones posteriores.

Versión de AXIS OS	Ruta de configuración de interfaz web
< 7.10	N/A
7.10	Settings (Configuración) > System (Sistema) > Plain config (Configuración sencilla) > System (Sistema) > Enable the script editor (editcgi) (Habilitar el editor de secuencias de comandos (editcgi))
≥ 10.9	Settings (Configuración) > Plain config (Configuración sencilla) > System (Sistema) > Enable the script editor (editcgi) (Habilitar el editor de secuencias de comandos (editcgi))

Acceso a FTP

FTP es un protocolo de comunicación no seguro que se utiliza únicamente con fines de solución de problemas y depuración. El acceso FTP se eliminó de AXIS OS 11.1 y no está disponible en versiones posteriores. Recomendamos que desactive el acceso FTP y utilice acceso SSH seguro para la localización de problemas.

Para obtener más información sobre SSH, consulte *SSH access (Acceso SSH)* en la guía AXIS OS Lifecycle. Para obtener más información acerca de las opciones de depuración mediante FTP, consulte *FTP access (Acceso FTP)* en la guía AXIS OS Lifecycle.

Versión de AXIS OS	Ruta de configuración de interfaz web
< 7.10	Setup (Configuración) > System Options (Opciones de sistema) > Plain Config (Configuración sencilla) > Network (Red) > FTP Enabled (FTP activado)
7.10	Settings (Configuración) > System (Sistema) > Plain config (Configuración sencilla) > Network (Red) > FTP Enabled (FTP activado)
≥ 10.9	System (Configuración) > Plain config (Configuración sencilla) > Network (Red) > FTP Enabled (FTP activado)

Acceso Telnet

Telnet es un protocolo de comunicación inseguro que se utiliza únicamente para fines de localización de problemas y depuración. Es compatible con dispositivos Axis con versiones anteriores a AXIS OS 5.50. Recomendamos desactivar el acceso Telnet.

Versión de AXIS OS	Ruta de configuración de interfaz web
< 5.50	Para obtener instrucciones, consulte *Acceso al dispositivo* en la base de conocimientos de AXIS OS.
< 7.10	N/A
7.10	N/A
≥ 10.9	N/A

ARP/Ping

ARP/Ping era un método para configurar la dirección IP del dispositivo AXIS usando herramientas como AXIS IP Utility. Esta funcionalidad se ha eliminado de AXIS OS 7.10 y no está disponible en versiones posteriores. Recomendamos desactivar la función en dispositivos Axis con AXIS OS 7.10 y versiones anteriores.

Versión de AXIS OS	Ruta de configuración de interfaz web
< 7.10	Setup (Configuración) > System Options (Opciones de sistema) > Advanced (Avanzado) > Plain Config (Configuración sencilla) > Network (Red) > ARP/Ping
7.10	N/A
≥ 10.9	N/A

Versiones de TLS desfasadas

Recomendamos desactivar las versiones de TLS antiguas, desfasadas e inseguras antes de poner en producción su dispositivo Axis. Las versiones de TLS desfasadas suelen estar desactivadas de forma predeterminada, pero todavía es posible activarlas en dispositivos Axis para ofrecer compatibilidad con versiones anteriores con aplicaciones de terceros que aún no han implementado TLS 1.2 y TLS 1.3.

Las versiones obsoletas de TLS se eliminaron a partir de AXIS OS 12.0 y no están disponibles en versiones posteriores.

Versión de AXIS OS	Ruta de configuración de interfaz web
< 7.10	Setup (Configuración) > System Options (Opciones de sistema) > Advanced (Avanzado) > Plain Config (Configuración sencilla) > HTTPS > Allow TLSv1.0 (Permitir TLSv1.0) y/o Allow TLSv1.1 (Permitir TLSv1.1)
7.10	Settings (Configuración) > System (Sistema) > Plain config (Configuración sencilla) > HTTPS > Allow TLSv1.0 (Permitir TLSv1.0) y/o Allow TLSv1.1 (Permitir TLSv1.1)
≥ 10.9 – 11.11.X	System (Sistema) > Plain config (Configuración sencilla) > HTTPS > Allow TLSv1.0 (Permitir TLSv1.0) y/o Allow TLSv1.1 (Permitir TLSv1.1)

Registro de acceso

CSC n.º 1: Inventario y control de activos empresariales
CSC n.º 8: Gestión de registros de auditoría

El registro de acceso proporciona registros detallados de los usuarios que acceden al dispositivo Axis, lo que facilita tanto las auditorías como la gestión del control de acceso. Recomendamos habilitar esta característica y

combinarla con un servidor syslog remoto para que el dispositivo Axis pueda enviar sus registros a un entorno de registro central. Esto simplifica el almacenamiento de los mensajes de registro y el tiempo de retención.

Para obtener más información, consulte *Registro de accesos al dispositivo* en la base de conocimientos de AXIS OS.

Versión de AXIS OS	Ruta de configuración de interfaz web
< 7.10	Setup (Configuración) > System Options (Opciones de sistema) > Advanced (Avanzado) > Plain Config (Configuración sencilla) > System (Sistema) > Access log (Registro de acceso)
7.10	Settings (Configuración) > System (Sistema) > Plain config (Configuración sencilla) > System (Sistema) > Access log (Registro de acceso)
≥ 10.9	System (Sistema) > Plain config (Configuración sencilla) > System (Sistema) > Access log (Registro de acceso)

Guía de inicio rápido

La guía de inicio rápido ofrece una breve descripción general de los ajustes que debe configurar cuando proteja los dispositivos Axis con AXIS OS 5.51 y versiones posteriores. Cubre los temas de protección descritos en *Protección básica, on page 15*, sin embargo, no cubre los temas en *Protección ampliada, on page 26* ya que requieren una configuración amplia y específica del cliente caso a caso.

Recomendamos que utilice AXIS Device Manager para proteger varios dispositivos Axis de una forma rápida y económica. Si necesita utilizar otra aplicación para la configuración de dispositivos o solo necesita mejorar la seguridad de unos pocos dispositivos Axis, recomendamos el uso de la API de VAPIX.

Errores de configuración habituales

Nota

Los errores de configuración comunes indicados a continuación aumentan potencialmente la superficie de ataque del dispositivo Axis y reducen sus capas de defensa de ciberseguridad, lo que genera un mayor riesgo de explotación, mal uso o funcionamiento inseguro del dispositivo.

Dispositivos expuestos a Internet
CSC n.º 12: Gestión de infraestructuras de red

No recomendamos que exponga el dispositivo Axis como un servidor web público ni que, de otro modo, proporcione acceso a la red de clientes desconocidos al dispositivo. Para obtener más información, vea .

Contraseña común
CSC n.º 4: Configuración segura de activos y software empresariales
CSC n.º 5: Gestión de cuentas

Le recomendamos encarecidamente que utilice una contraseña única para cada dispositivo en lugar de una contraseña genérica para todos los dispositivos. Para obtener instrucciones, consulte *Identity and access management (Identidad y gestión de acceso)* en la base de conocimientos AXIS OS y *Crear cuentas dedicadas, on page 16*.

Acceso anónimo
CSC n.º 4: Configuración segura de activos y software empresariales
CSC n.º 5: Gestión de cuentas.

No recomendamos que permita que usuarios anónimos accedan a los ajustes de vídeo y configuración del dispositivo sin necesidad de proporcionar credenciales de inicio de sesión. Para obtener más información, consulte *Desactivado de forma predeterminada, on page 4*.

Comunicación segura desactivada
CSC n.º 3: Protección de datos

No recomendamos que utilice el dispositivo mediante métodos de acceso y comunicación no seguros, como HTTP o autenticación básica, en la que las contraseñas se transfieren sin cifrado. Para obtener más información, vea *HTTPS activado, on page 8*. Para obtener recomendaciones de configuración, consulte *Autenticación digest, on page 4*.

Versión de AXIS OS desfasada
CSC n.º 2: Inventario y control de activos de software

Le recomendamos encarecidamente que utilice el dispositivo Axis con la última versión disponible de AXIS OS, ya sea en LTS o en una ruta activa. Ambas pistas ofrecen las correcciones de errores y correcciones de seguridad más recientes. Para obtener más información, vea *Actualización a la versión más reciente de AXIS OS, on page 15*.

Seguridad básica mediante API VAPIX

Puede utilizar la API de VAPIX para mejorar la seguridad de sus dispositivos Axis en función de los temas tratados en *Protección básica, on page 15*. En esta tabla puede encontrar todos los ajustes básicos de configuración de seguridad independientemente de la versión de AXIS OS de su dispositivo Axis.

Es posible que algunos ajustes de configuración ya no estén disponibles en la versión de AXIS OS de su dispositivo puesto que algunas funciones se han eliminado con el tiempo para aumentar la seguridad. Si recibe un error al emitir la llamada a VAPIX, podría ser una indicación de que la funcionalidad ya no está disponible en la versión de AXIS OS.

Objetivo	Llamada a la API de VAPIX
*Inhabilitar POE en puertos de red sin utilizar**	`http://ip-address/axis-cgi/nvr/poe/setportmode.cgi?port=X&enabld=no`
*Inhabilitar el tráfico de red en puertos de red sin utilizar***	`http://ip-address/axis-cgi/network_settings.cgi { "apiVersion": "1.17", "method": "setDeviceConfiguration", "params": { "deviceName": "eth1.1", "staticState": "down" } }`
Deshabilitar el protocolo de detección Bonjour	`https://ip-address/axis-cgi/param.cgi?action=update&Network.Bonjour.Enabled=no`
Deshabilitar el protocolo de detección UPnP	`https://ip-address/axis-cgi/param.cgi?action=update&Network.UPnP.Enabled=no` `https://ip-address/axis-cgi/param.cgi?action=update&Network.UPnP.NATTraversal.Enabled=no`
Deshabilitar el protocolo de detección WebService	`https://ip-address/axis-cgi/param.cgi?action=update&WebService.DiscoveryMode.Discoverable=no`
Deshabilitar la conexión a la nube con un solo clic (O3C)	`https://ip-address/axis-cgi/param.cgi?action=update&RemoteService.Enabled=no`
Deshabilitar el acceso de mantenimiento SSH al dispositivo	`https://ip-address/axis-cgi/param.cgi?action=update&Network.SSH.Enabled=no`
Deshabilitar el acceso de mantenimiento FTP al dispositivo	`https://ip-address/axis-cgi/param.cgi?action=update&Network.FTP.Enabled=no`
Desactivar configuración de dirección IP ARP-Ping	`https://ip-address/axis-cgi/param.cgi?action=update&Network.ARPPingIPAddress.Enabled=no`
Deshabilitar la configuración de direcciones IP de Zero-Conf	`http://ip-address/axis-cgi/param.cgi?action=update&Network.ZeroConf.Enabled=no`
Habilitar HTTPS solo	`https://ip-address/axis-cgi/param.cgi?action=update&System.BoaGroupPolicy.admin=https` `https://ip-address/axis-cgi/param.cgi?action=update&System.BoaGroupPolicy.operator=https` `https://ip-address/axis-cgi/param.cgi?action=update&System.BoaGroupPolicy.viewer=https`
Habilitar solo TLS 1.2 y TLS 1.3	`https://ip-address/axis-cgi/param.cgi?action=update&HTTPS.AllowTLS1=no`

Objetivo	Llamada a la API de VAPIX
	`https://ip-address/axis-cgi/param.cgi?action=update&HTTPS.AllowTLS11=no`
Configuración de cifrado seguro TLS 1.2	`https://ip-address/axis-cgi/param.cgi?action=update&HTTPS.Ciphers=ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305`

*Activar la protección contra ataques de fuerza bruta****	`https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.ActivatePasswordThrottling=on`
	`https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSBlockingPeriod=10`
	`https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSPageCount=20`
	`https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSPageInterval=1`
	`https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSSiteCount=20`
	`https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSSiteInterval=1`

Deshabilitar el entorno del editor de secuencias de comandos	`https://ip-address/axis-cgi/param.cgi?action=update&System.EditCgi=no`
Habilitar el registro de acceso de usuarios mejorado	`https://ip-address/axis-cgi/param.cgi?action=update&System.AccessLog=On`
Activar la protección contra ataques de reproducción ONVIF	`https://ip-address/axis-cgi/param.cgi?action=update&WebService.UsernameToken.ReplayAttackProtection=yes`
Deshabilitar acceso a la interfaz web del dispositivo	`https://ip-address/axis-cgi/param.cgi?action=update&System.WebInterfaceDisabled=yes`
Desactivar encabezado de servidor HTTP/OpenSSL	`https://ip-address/axis-cgi/param.cgi?action=update&System.HTTPServerTokens=no`
Deshabilitar visor anónimo y acceso PTZ	`https://ip-address/axis-cgi/param.cgi?action=update&root.Network.RTSP.ProtViewer=password` `https://ip-address/axis-cgi/param.cgi?action=update&root.System.BoaProtViewer=password`

Objetivo	Llamada a la API de VAPIX
	`https://ip-address/axis-cgi/param.cgi?action=update&root.PTZ.BoaProtPTZOperator=password`
Evitar la instalación de aplicaciones ACAP que requieran privilegios de root	`http://ip-address/axis-cgi/applications/config.cgi?action=set&name=AllowRoot&value=false`
Impedir la instalación de aplicaciones ACAP sin firma	`http://ip-address/axis-cgi/applications/config.cgi?action=set&name=AllowUnsigned&value=false`

* Sustituya "X" por el número de puerto real en "port=X". Ejemplos: "port=1" desactivará el puerto 1 y "port=2" desactivará el puerto 2.
** Sustituya "1" por el número de puerto real en "eth1.1". Ejemplos: "eth1.1" desactivará el puerto 1 y "eth1.2" desactivará el puerto 2.
*** Después de 20 intentos fallidos de inicio de sesión en un segundo, la dirección IP del cliente se bloquea durante 10 segundos. Every following failed request within the 30 seconds page interval will result in the DoS blocking period being extended by another 10 seconds.

Seguridad básica mediante AXIS Device Manager (Extend)

Puede utilizar AXIS Device Manager y AXIS Device Manager Extend para aumentar la seguridad de sus dispositivos Axis en función de los temas tratados en *Protección básica, on page 15*. Utilice este *archivo de configuración*, que consta de los mismos ajustes de configuración enumerados en *Seguridad básica mediante API VAPIX, on page 33*.

Es posible que algunos ajustes de configuración ya no estén disponibles en la versión de AXIS OS de su dispositivo puesto que algunas funciones se han eliminado con el tiempo para aumentar la seguridad. AXIS Device Manager y AXIS Device Manager Extend eliminarán automáticamente estos ajustes de la configuración de seguridad.

Nota

Una vez cargado el archivo de configuración, el dispositivo Axis solo se configurará en HTTPS y la interfaz web se desactivará. Puede modificar el archivo de configuración según sus necesidades, por ejemplo, eliminando o añadiendo parámetros.

Notificaciones de seguridad

Le recomendamos que se suscriba al *servicio de notificación de seguridad de Axis* para recibir información sobre vulnerabilidades que se han descubierto recientemente en los productos, soluciones y servicios de Axis, así como cómo proteger sus dispositivos Axis.

T10177717_es

2026-03 (M64.2)