AXIS OS Hardening Guide

AXIS OS Hardening Guide

Introducción

Introducción

Axis Communications mantiene una apuesta decidida por la aplicación de las prácticas de ciberseguridad recomendadas en el diseño, el desarrollo y las pruebas de los dispositivos, para minimizar el riesgo de fallos que puedan abrir la puerta a posibles ataques. Sin embargo, toda la cadena de suministro de proveedores y la organización del usuario final deben participar en la protección de una red, sus dispositivos y los servicios que admite. Un entorno seguro depende de sus usuarios, procesos y tecnología. El objetivo de esta guía es ayudarle a mantener la red, los dispositivos y los servicios protegidos.

Las amenazas más evidentes para un dispositivo Axis son la alteración física, el vandalismo y la manipulación. Para proteger un producto frente a estas amenazas, es importante seleccionar un modelo o carcasa resistente al vandalismo montarlo de la forma recomendada y proteger los cables.

Los dispositivos Axis son terminales de la red, como ordenadores y teléfonos móviles. Muchos de ellos disponen de una interfaz web que puede mostrar vulnerabilidades a los sistemas conectados. En esta guía le explicamos cómo puede reducir esos riesgos.

La guía proporciona asesoramiento técnico para todas aquellas personas implicadas en la implementación de soluciones de Axis. Incluye una configuración básica recomendada y una guía de protección que toma en cuenta la evolución en el panorama de amenazas. Es posible que tenga que consultar el manual de usuario del producto para aprender a configurar ajustes específicos. Tenga en cuenta que los dispositivos de Axis tienen una actualización de la interfaz web en AXIS OS 7.10 y 10.9 que cambió la ruta de configuración.

Configuración de la 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 del sistema operativo AXIS 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)

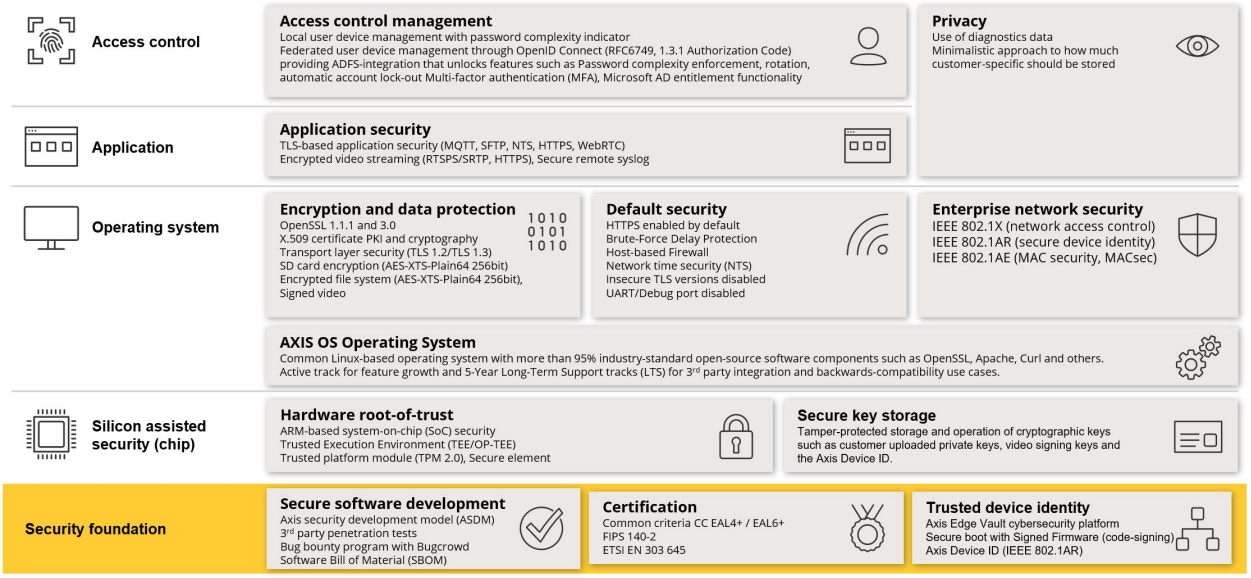
Ámbito

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 versiones 4.xx y 5.xx.

Introducción

Arquitectura de seguridad de AXIS OS

El diagrama de la arquitectura de seguridad de AXIS OS ilustra la capacidad de ciberseguridad de AXIS OS en varias capas y ofrece una visión integral de los cimientos de la 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.

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.

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.

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.

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

Acceso con credencial

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.

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. En esta tabla puede ver cuáles son.

Protocol (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	UDP	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
Bonjour	5353	UDP	Utilizado por aplicaciones de terceros para detectar el dispositivo Axis a través del protocolo de detección mDNS (Bonjour)

Protección predeterminada

Protocol (Protocolo)	Puerto	Transporte	Comentarios
SSDP	1900	UDP	Utilizado por aplicaciones de terceros para detectar el dispositivo Axis a través de SSDP (UPnP)
WS-Discovery	3702	UDP	Utilizado por aplicaciones de terceros para detectar el dispositivo Axis a través del protocolo de detección WS-Discovery (ONVIF)

** Para obtener más información sobre la tecnología de extremo a extremo, consulte el informe técnico sobre 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.*

Le recomendamos que desactive 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 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 y, por lo tanto, están activadas de forma predeterminada.

Interfaz UART/de depuración

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

Todos los dispositivos Axis cuentan con la denominada interfaz UART (Transmisor receptor de asíncrono universal) física, que a veces se conoce como "puerto de depuración" o "consola serie". Solo es posible acceder físicamente a la interfaz desmantelando ampliamente 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.

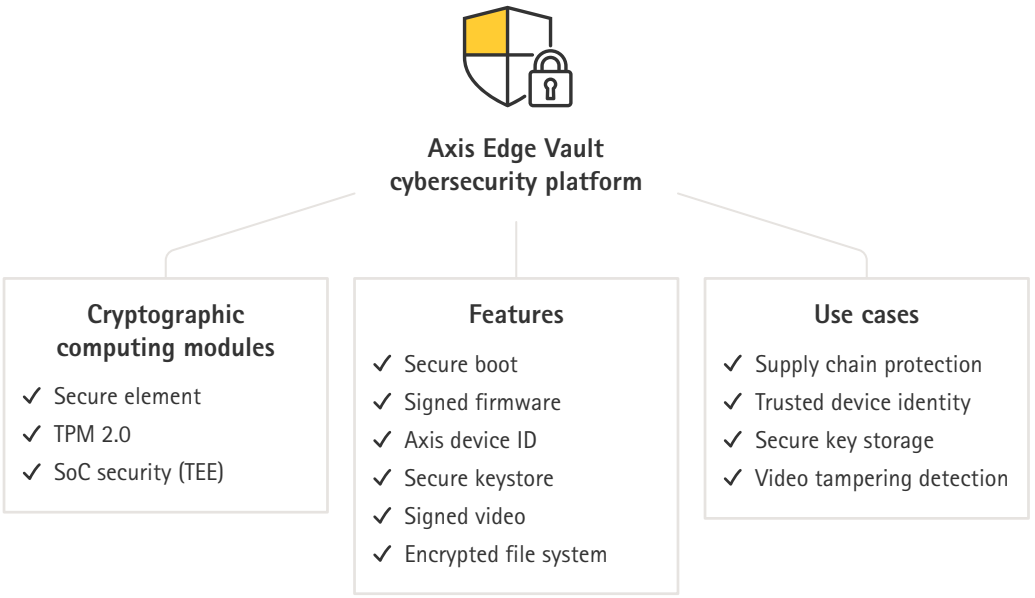
La interfaz UART/de depuración está activada de forma predeterminada en dispositivos Axis con AXIS OS 10.10 y versiones anteriores, pero requiere acceso autenticado y no expone ninguna información confidencial sin tener que autenticarse. A partir de AXIS OS 10.11, la interfaz UART/de depuración está 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. Se basa en una sólida base de módulos de computación criptográficos (elemento seguro y TPM) y seguridad SoC (TEE y arranque seguro), combinados con experiencia en seguridad de dispositivos locales. Axis Edge Vault se basa en una sólida root de confianza establecida mediante un arranque seguro y un firmware firmado. Estas características crean una cadena de software validado criptográficamente para la cadena de confianza de la que dependen todas las operaciones seguras.

Los dispositivos Axis con Axis Edge Vault minimizan la exposición de los clientes 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 dentro de la red del cliente.

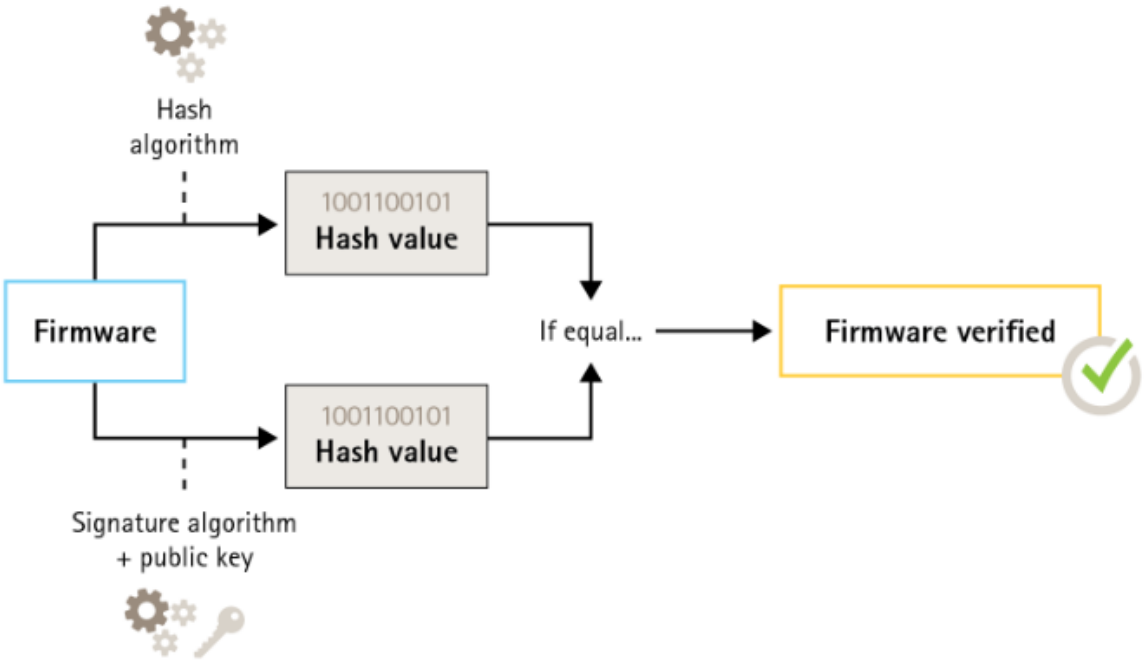
Protección predeterminada



Firmware firmado

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

El SO AXIS está firmado desde la versión 9.20.1. Siempre que actualice la versión de SO de AXIS en el dispositivo, el dispositivo comprobará la integridad de los archivos de actualización mediante la verificación de la firma criptográfica y rechazará los archivos manipulados. De esta forma, se evitará que los atacantes engañen a los usuarios para que instalen archivos comprometidos.



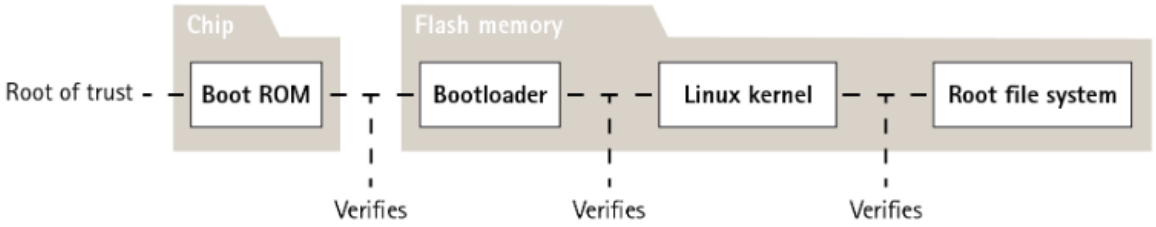
Protección predeterminada

Para obtener más información, consulte el informe 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.

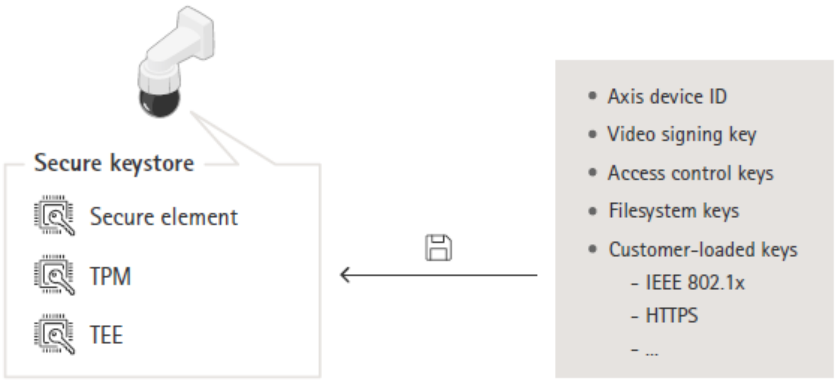


Para obtener más información, consulte el informe técnico *Axis Edge Vault*.

Almacenamiento de claves seguro

CSC N.º 6: Gestión del control de acceso

El almacén de claves seguro proporciona almacenamiento de información criptográfico basado en hardware y protegido contra 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 informe 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.

Protección predeterminada

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 informe técnico *Axis Edge Vault*.

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. 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)

Encabezados HTTP(s) predeterminados

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. A partir de AXIS OS 9.80, 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.

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. Por lo tanto, recomendamos que utilice únicamente la autenticación Digest en lugar de Basic o 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 predeterminada

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)

Prevent brute-force attacks (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 por retraso de fuerza bruta está activada de manera predeterminada a partir de AXIS OS 11.5. Para ver ejemplos y recomendaciones de configuración detallados, consulte *Protección contra retrasos de fuerza bruta* en la base de conocimientos de AXIS OS.

Versión de AXIS OS	Ruta de configuración de interfaz web
< 7.10	N/D
≥ 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)

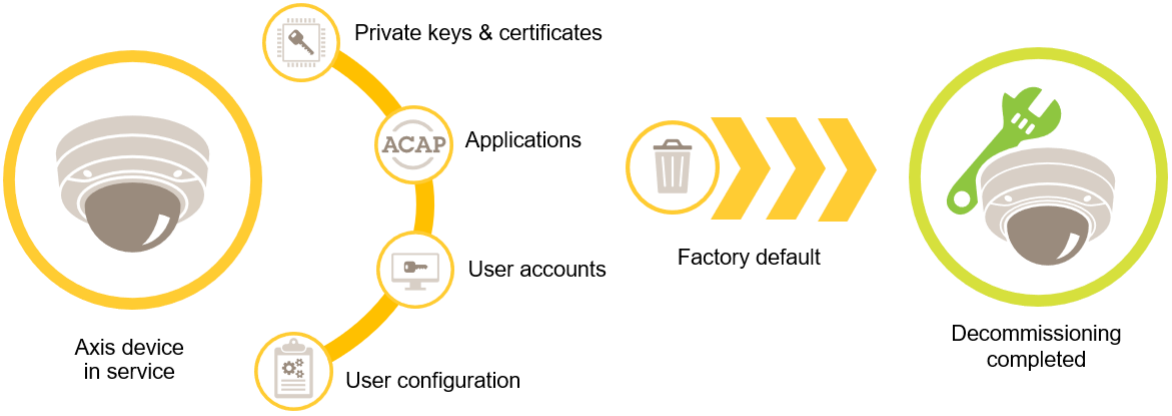
Desinstalación

CSC N.º 3: Protección de datos

Al desinstalar un dispositivo Axis, recomendamos restablecer el dispositivo a la configuración predeterminada de fábrica, que borrará los datos del dispositivo mediante sobrescritura/limpieza.

Los dispositivos Axis utilizan memoria tanto volátil como no volátil y, aunque la memoria volátil se borra siempre que desconecta el dispositivo de la fuente de alimentación, la información almacenada en la memoria no volátil permanece y vuelve a estar disponible al iniciarse. 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.

Protección predeterminada



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

Protección predeterminada

Gráficos y superposiciones cargados	Sí
Datos del reloj RTC	Sí

** El proceso de firmware firmado utiliza certificados personalizados que permiten a los usuarios cargar, entre otras cosas, el SO de AXIS.*
*** El usuario debe eliminar las grabaciones e imágenes almacenadas en el almacenamiento local (tarjeta SD, recurso compartido de red) por separado. Para obtener más información, consulte Formateo de tarjetas SD de Axis* en la base de conocimientos de AXIS OS.
**** Todas las configuraciones realizadas por el usuario, desde la creación de cuentas hasta la red, la O3C, los eventos, la imagen, las PTZ y las configuraciones del sistema.*
***** El dispositivo conserva todas las aplicaciones preinstaladas pero les elimina todas las configuraciones realizadas por el usuario.*
****** Los datos de producción (calibración, certificados de producción 802.1AR) y las estadísticas de vida útil incluyen información no sensible y no relacionada con el usuario.*

Protección básica

Protección básica

La protección básica es el nivel de protección mínimo recomendado para los dispositivos Axis. Los temas básicos de protección son "configurables en el extremo". 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.

Configuración predeterminada 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 en la página 9*.

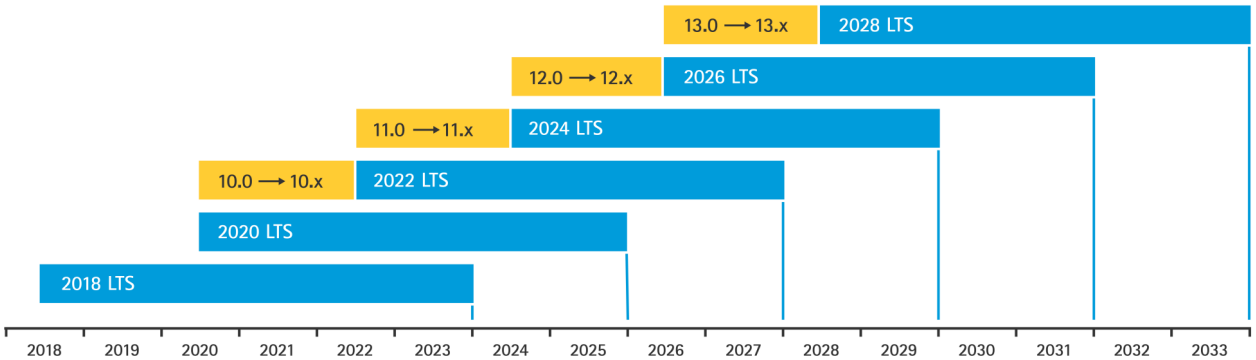
Versión de AXIS OS	Ruta de configuración de interfaz web
< 7.10	Setup (Configuración) > System Options (Opciones del sistema) > Default (Valor predeterminado)
≥ 7.10	Settings (Configuración) > System (Sistema) > Default (Valor predeterminado)
≥ 10.9	Maintenance (Mantenimiento) > Default (Valor predeterminado)

Actualización a la versión más reciente del sistema operativo AXIS

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

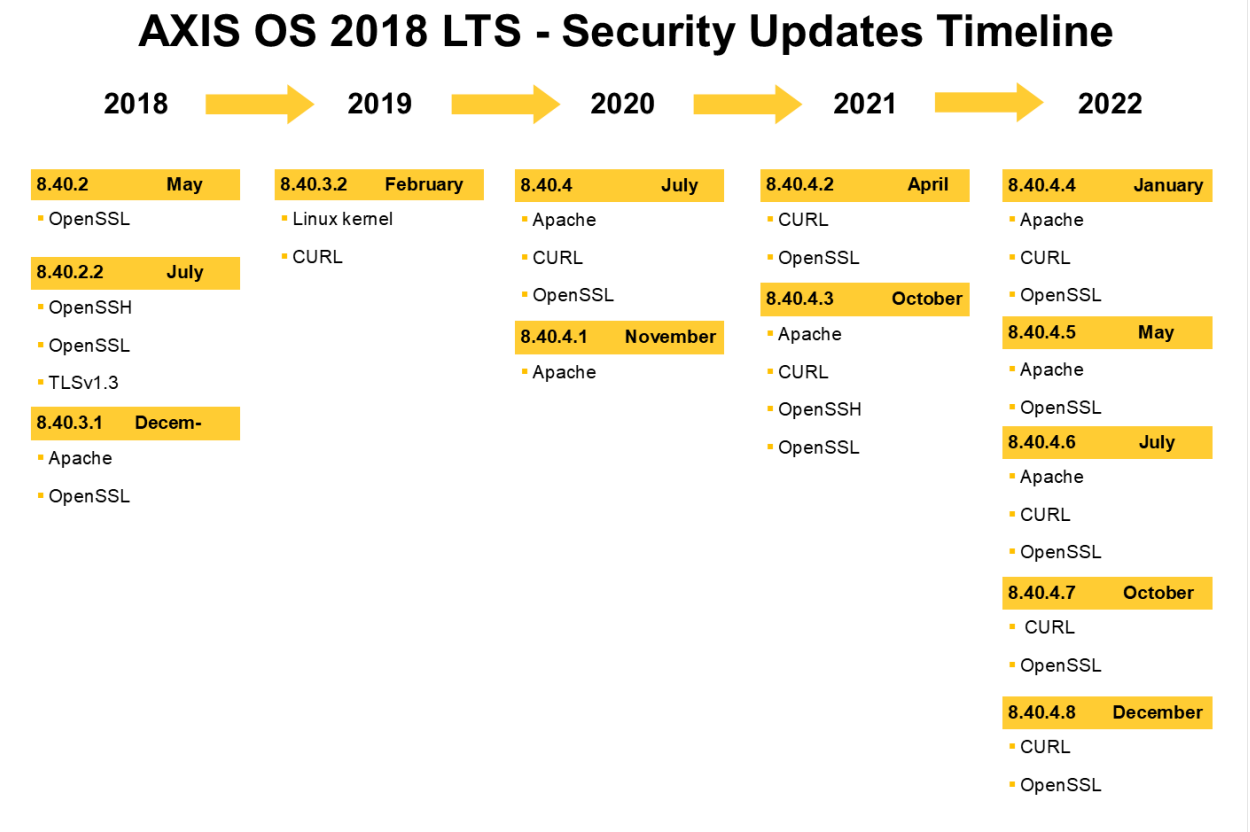
La aplicación de parches para el software es un aspecto importante de la ciberseguridad. A menudo, los atacantes tratan de aprovechar las vulnerabilidades conocidas y pueden tener éxito si obtienen acceso de red a un servicio no autorizado. Asegúrese de que utiliza siempre el sistema operativo AXIS más reciente, ya 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 mantiene dos tipos de seguimientos de SO AXIS: el seguimiento activo y el seguimiento de soporte a largo plazo (LTS). Aunque ambos tipos 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 *Firmware* en axis.com para descargar el SO de AXIS para su dispositivo.

Este gráfico ilustra la importancia de mantener actualizados los dispositivos Axis.



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	Maintenance (Mantenimiento) > Firmware upgrade (Actualización de firmware)

Establecer contraseña de root del dispositivo

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

La cuenta de root del dispositivo es la cuenta de administración principal del dispositivo. Antes de poder utilizar la cuenta de root, debe establecer una contraseña del dispositivo. Asegúrese de utilizar una contraseña segura y de limitar el uso de la cuenta de root solo a tareas de administración. No recomendamos el uso de la cuenta de root en la producción diaria.

Protección básica

Al utilizar dispositivos Axis, utilizar la misma contraseña simplifica la gestión, pero aumenta su vulnerabilidad ante filtraciones y fugas de datos. El uso de contraseñas únicas para cada dispositivo Axis proporciona alta seguridad, pero hace que la gestión de los dispositivos sea más compleja. Le recomendamos que cambie con regularidad la contraseña de sus dispositivos.

Recomendamos que implemente directrices que requieran que las contraseñas nuevas sean lo suficientemente largas y complejas, como las *recomendaciones de contraseña NIST*. Los dispositivos Axis admiten contraseñas de hasta 64 caracteres. Las contraseñas **con menos de 8 caracteres** se consideran débiles.

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)

Crear cuentas dedicadas

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

La cuenta raíz (root) predeterminada dispone de todos los privilegios y debe estar reservada a tareas administrativas. Recomendamos que cree una cuenta de usuario cliente con privilegios limitados para el funcionamiento diario. Esto reduce el riesgo de poner en peligro la contraseña del administrador del dispositivo.

Para obtener más información, consulte el informe técnico sobre *gestión de identidades y acceso en sistemas de videovigilancia*.

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)

Limitar acceso a la interfaz web

CSC n.º 5: Administración de cuentas

Los dispositivos Axis disponen de un servidor web que permite a los usuarios acceder al dispositivo a través de un navegador web estándar. La interfaz web se ha diseñado para la configuración, el mantenimiento y la solución de problemas. No está pensado para operaciones diarias, por ejemplo, como cliente para ver el vídeo.

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. Para obtener más información, vea *Inhabilitar acceso a la interfaz web en la página 14*.

Inhabilitar acceso a la interfaz web

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

A partir de 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/D
≥ 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)

Configurar los ajustes de red

CSC n.º 12: Gestión de infraestructuras de red

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. Recomendamos que revise la topología de red siempre que agregue nuevos tipos de componentes.

También recomendamos que utilice la configuración de direcciones IP estáticas en sus dispositivos Axis para garantizar la capacidad de alcance de la red y desenredar la dependencia de los servidores de la red (como los servidores DHCP) que podrían ser el objetivo de ataques.

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)

Configurar la fecha y hora

CSC n.º 8: Gestión de registros de auditoría

Desde una perspectiva de seguridad, es importante que defina la fecha y la hora correctas. Esto garantiza, por ejemplo, que los registros del sistema tengan una marca de hora correcta y que los certificados digitales se pueden validar y utilizar durante el tiempo de ejecución. Si no se sincroniza correctamente la hora, es posible que los servicios que utilicen certificados digitales como HTTPS, IEEE y 802.1x no funcionen correctamente.

Recomendamos que mantenga el reloj del dispositivo Axis sincronizado con servidores NTP (protocolo de tiempo de red, sin cifrar) o, preferiblemente, servidores de seguridad de hora de red (NTS, cifrado). Network Time Security (NTS), una variante cifrada y segura del Protocolo de tiempo de red (NTP), se agregó en AXIS OS 11.1. Recomendamos que configure varios servidores de hora para obtener una precisión de sincronización de hora superior, pero también para tener en cuenta un escenario de failover en el que uno de los servidores de hora configurados podría no estar disponible.

El uso de servidores NTP o NTS públicos puede ser una alternativa para organizaciones pequeñas y particulares que no pueden facilitar las propias instancias de servidores en hora local. 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 el extremo

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)

Exportar cifrado de grabación

CSC N.º 3: Protección de datos

A partir de AXIS OS 10.10, los dispositivos Axis admiten la exportación cifrada de grabaciones en el extremo. 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/D
≥ 7.10	N/D
≥ 10.9	Grabaciones

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

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.

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/D
≥ 7.10	N/D
≥ 11.2	System (Sistema) > Power over Ethernet (Alimentación a través de Internet)

Protección básica

Protocolos de detección de red

Los protocolos de detección, como Bonjour, UPnP, ZeroConf y WS-Discovery, 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/D
≥ 7.10	Setttings (Configuración) > System (Sistema) > 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)

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

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 es posible habilitarlas 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.

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	System (Sistema) > Plain config (Configuración sencilla) > HTTPS > Allow TLSv1.0 (Permitir TLSv1.0) *y/o* Allow TLSv1.1 (Permitir TLSv1.1)

Protección básica

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/D
≥ 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))

Encabezados de servidor HTTP

De forma predeterminada, los dispositivos Axis anuncian sus versiones Apache y OpenSSL actuales durante las conexiones HTTP(s) con clientes de la red. Esta información resulta útil cuando se utilizan escáneres de seguridad de red periódicamente, ya que proporciona un informe más detallado de las vulnerabilidades excepcionales en una versión de AXIS OS concreta.

Es posible desactivar los encabezados de servidor HTTP(s) para reducir la exposición de información durante las conexiones HTTP(s). Sin embargo, solo recomendamos desactivar los encabezados si utiliza su dispositivo de acuerdo con nuestras recomendaciones y lo mantiene actualizado en todo momento.

La opción para desactivar los encabezados de servidor HTTP(s) está disponible a partir de AXIS OS 10.6.

Versión de AXIS OS	Ruta de configuración de interfaz web
< 7.10	N/D
≥ 7.10	Settings (Configuración) > Plain config (Configuración sencilla > System (Sistema) > HTTP Server Header Comments (Comentarios de encabezado de servidor HTTP)
≥ 10.9	System (Sistema) > Plain config (Configuración sencilla > HTTP Server Header Comments (Comentarios de encabezado de servidor HTTP)

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)

Protección básica

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/D
≥ 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 FTP

FTP es un protocolo de comunicación inseguro que se utiliza únicamente para la localización de problemas y la 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 *Acceso SSH* en AXIS OS Portal. Para obtener más información acerca de las opciones de depuración mediante FTP, consulte *Acceso FTP* en AXIS OS Portal.

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 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. Le recomendamos que desactive 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)

Protección básica

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. Le recomendamos que desactive 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/D
≥ 7.10	N/D
≥ 10.9	N/D

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/D
≥ 10.9	N/D

IP address filter (Filtro de direcciones IP)

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

El filtrado de direcciones IP impide que clientes no autorizados accedan al dispositivo Axis. Recomendamos que configure el dispositivo para permitir las direcciones IP de los hosts de red autorizados o para denegar las direcciones IP de los hosts de red no autorizados.

Si decide permitir direcciones IP, asegúrese de añadir a su lista todos los clientes autorizados (servidor 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	Settings (Configuración) > Security (Seguridad) > IP address filter (Filtro de direcciones IP)

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. Aunque el acceso HTTP no es seguro y no tiene cifrado, HTTPS cifra el tráfico entre el cliente y el dispositivo Axis. Recomendamos que utilice HTTPS para todas las tareas administrativas del dispositivo Axis.

Protección básica

Para obtener instrucciones de configuración, consulte *Solo HTTPS en la página 22* y *Codificadores HTTPS en la página 22*.

Solo HTTPS

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 de Axis se incluyen con un certificado con firma propia. Aunque el diseño no garantiza la confianza de un certificado con firma propia, es adecuado acceder de forma segura al dispositivo de Axis durante la configuración inicial y cuando no hay ninguna infraestructura de clave pública (PKI) disponible. 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. Una vez que haya restablecido los ajustes predeterminados de fábrica del dispositivo Axis, es posible que la lista de cifrado se actualice automáticamente según la configuración de prácticas recomendadas más reciente disponible proporcionada por Axis.

Para obtener referencias y transparencia, utilice los paquetes de cifrado seguros y seguros enumerados en *TLS 1.2 e inferior en la página 22* y *TLS 1.3 en la página 22*.

TLS 1.2 e inferior

```
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:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384
```

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 básica

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)

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 AXIS A*

Protección ampliada

Las instrucciones de protección ampliada se basan en los temas de protección descritos en *Protección predeterminada en la página 4* y *Protección básica en la página 12*. 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

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 organizaciones pequeñas e individuos que no funcionan con un VMS o necesitan acceder a vídeo desde ubicaciones remotas, recomendamos utilizar AXIS Companion.

AXIS Companion utiliza software cliente Windows/iOS/Android, es gratuito y ofrece una manera sencilla de acceder al vídeo de forma segura sin necesidad de exponer el dispositivo Axis a Internet. Para obtener más información acerca de AXIS Companion, visite *axis.com/companion*.

Nota

Todas las organizaciones que utilizan un VMS deben consultar al proveedor del VMS para conocer las prácticas recomendadas sobre el acceso de vídeo remoto.

Limitar la exposición de la red

CSC n.º 12: Gestión de infraestructuras de red

Una manera común de reducir los riesgos de exposición a la red es aislar física y virtualmente los dispositivos de red, así como de infraestructuras y aplicaciones relacionadas. Entre estas infraestructuras y aplicaciones se incluyen software de gestión de vídeo (VMS), grabadoras de vídeo en red (NVR) y otros tipos de equipos de vigilancia.

Recomendamos que aísle sus dispositivos Axis y las infraestructuras y aplicaciones relacionadas en una red local que no esté conectada a su red de producción y empresarial.

Para aplicar protección básica, proteja la red local y su infraestructura (router, switches) frente a accesos no autorizados mediante la adición de varios mecanismos de seguridad de red. Estos mecanismos son, por ejemplo, la segmentación de VLAN, las capacidades de enrutamiento limitadas, la red privada virtual (VPN) para el acceso de sitio a sitio o WAN, el firewall de la capa de red 2/3 y las listas de control de acceso (ACL).

Para ampliar la protección básica, recomendamos que aplique técnicas de inspección de red más avanzadas, como una inspección más profunda de paquetes y detección de intrusiones. Esto añadirá una protección integral y coherente contra amenazas dentro de la red. La protección de red ampliada requiere equipos de hardware y/o software dedicados.

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, ya sea 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 *Guía del escáner de vulnerabilidades del sistema operativo AXIS*. Envíe el informe y las solicitudes adicionales en un ticket del servicio de soporte técnico 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 con firma de una autoridad de certificación (CA) con una cadena de certificación validada ayuda a eliminar las advertencias de certificados del navegador cuando se conecta a través de HTTPS. Un certificado con firma de CA también garantiza la autenticidad del dispositivo Axis cuando despliegue 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.

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

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.

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

Protección ampliada

Los dispositivos Axis con axis Edge Vault son compatibles con el estándar de red IEEE 802.1AR. Esto permite la integración automática y segura de dispositivos Axis en la red mediante el ID de dispositivo de 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.

Supervisión SNMP

CSC n.º 8: Gestión de registros de auditoría

Los dispositivos Axis admiten los siguientes protocolos SNMP:

- **SNMP v1**: admitido solo por motivos antiguos, no lo utilice.
- **SNMP v2c**: se puede utilizar en un segmento de red protegido.
- **SNMP v3**: recomendado para fines de supervisión.

Los dispositivos Axis también admiten la supervisión de MIB-II y AXIS Video MIB. Para descargar AXIS Video MIB, consulte *AXIS Video MIB* en la base de conocimientos de AXIS OS.

Para obtener más información sobre cómo configurar SNMP en el sistema operativo AXIS, consulte *SNMP (Protocolo de gestión de red simple)* 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) > Network (Red) > SNMP
≥ 7.10	Settings (Configuración) > System (Sistema) > SNMP
≥ 10.9	System (Sistema) > Network (Red) > SNMP

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 AXIS OS Portal
≥ 7.10	Settings (Configuración) > System (Sistema) > TCP/IP
≥ 10.9	System (Sistema) > Logs (Registros)

Transmisión de vídeo segura (SRTP/RTSPS)

CSC N.º 3: Protección de datos

Protección ampliada

A partir de AXIS OS 7.40, los dispositivos Axis admiten la transmisión segura de vídeo a través de RTP, lo que se conoce también como SRTP/RTSPS. SRTP/RTSPS utiliza un método seguro de transporte cifrado de extremo a extremo para asegurarse de que solo los clientes autorizados reciben la transmisión de vídeo desde el 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. Con el vídeo firmado, los dispositivos Axis pueden añadir una firma a su transmisión de vídeo para asegurarse de que el vídeo esté intacto y comprobar su origen realizando un seguimiento hasta el dispositivo que lo ha producido. 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 informe 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/D
≥ 7.10	N/D
≥ 10.9	System (Sistema) > Plain config (Configuración sencilla) > Image (Imagen) > SignedVideo (Vídeo firmado)

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 en la página 12*, sin embargo, no cubre los temas en *Protección ampliada en la página 24* 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

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 *Limitar la exposición a Internet en la página 24*.

Contraseña común
CSC N.º 4: Configuración segura de activos y software empresariales
CSC N.º 5: Administración 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 *Establecer contraseña de root del dispositivo en la página 13* y *Crear cuentas dedicadas en la página 14*.

Acceso anónimo
CSC N.º 4: Configuración segura de activos y software empresariales
CSC N.º 5: Administración 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, vea *Acceso con credencial en la página 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 en la página 8*. Para obtener recomendaciones de configuración, consulte *Autenticación digest en la página 8*.

Versión desfasada de AXIS OS
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 del sistema operativo AXIS en la página 12*.

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 en la página 12*. En esta tabla puede encontrar todos los ajustes básicos de configuración de seguridad independientemente de la versión del sistema operativo AXIS 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 del sistema operativo AXIS.

Guía de inicio rápido

Propósito	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` `https://ip-address/axis-cgi/param.cgi?action=update&HTTPS.AllowTLS11=no`

Guía de inicio rápido

Propósito	Llamada a la API de VAPIX
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:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384`

*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`
	`https://ip-address/axis-cgi/param.cgi?action=update&root.PTZ.BoaProtPTZOperator=password`

** Sustituya "X" por el número de puerto real en "port=X". Ejemplos: "port=1" will disable port 1 and "port=2" will disable port 2.*
*** Replace "1" with the actual port number in "eth1.1". Ejemplos: "eth1.1" will disable port 1 and "eth1.2" will disable port 2.*

**** After 20 failed login attempts within one second, the client IP address is blocked for 10 seconds. 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 en la página 12*. Utilice este *archivo de configuración*, que consta de los mismos ajustes de configuración enumerados en *Seguridad básica mediante API VAPIX en la página 28*.

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.

AXIS OS Hardening Guide
Ver. M43.2
Fecha: Septiembre 2023
N.º de pieza
© Axis Communications AB, 2022 - 2023