Control de seguridad con AXIS Device Manager

Versión 1.0

Índice

1. Introducción

La importancia de la ciberseguridad sigue creciendo en los sectores de la vigilancia y la seguridad. Para conseguir una ciberseguridad efectiva, debe garantizarse una profundidad de la defensa para proteger de forma adecuada la red IP en todos los niveles: desde los productos elegidos y los socios con los que colabore, hasta los requisitos que defina cualquiera de las partes.

1.1 Tres capas de protección para la ciberseguridad

Ofrecemos tres capas de protección para la ciberseguridad:

1. Gestión de la seguridad: exige aplicar los controles de seguridad necesarios para mitigar las amenazas a las que se enfrenta. Puede dividirse en dos partes: controles de seguridad y gestión rentable. Los controles de seguridad son protecciones o contramedidas que se implementan para evitar, detectar, combatir o minimizar los riesgos de seguridad para la propiedad física, la información, los sistemas informáticos y demás activos.

2. Gestión de vulnerabilidades: abarca todo lo que Axis hace para aplicar las mejores prácticas de ciberseguridad en el diseño, el desarrollo y la comprobación de nuestros productos, a fin de minimizar el riesgo de defectos que pudieran aprovecharse. Cuando se descubren vulnerabilidades, nos encargamos de gestionarlas. Corregimos con prontitud las vulnerabilidades críticas y emitimos recomendaciones de seguridad.

3. Aprendizaje y colaboración: pretende que Axis, usted mismo y los socios implicados en su red IP obtengan y compartan un concepto claro y común de las amenazas a las que se enfrenta, de sus posibles impactos y de cómo proteger su red.

1.2 Propósito de este documento

Esta guía de la aplicación describe cómo puede utilizarse AXIS Device Manager para proteger mejor su sistema y aumentar la seguridad. Se centra en aspectos clave y presenta una serie de recomendaciones.

1.3 Acerca de AXIS Device Manager

AXIS Device Manager es una herramienta in situ que pone a su disposición una forma sencilla, económica y segura de gestionar todas las tareas de instalación, seguridad, mantenimiento y gestión de dispositivos (consulte la siguiente tabla). Es adecuada para gestionar hasta un par de miles de dispositivos Axis en un mismo emplazamiento (o varios miles de dispositivos en varios emplazamientos). AXIS Device Manager permite implantar con eficacia controles de ciberseguridad con los que proteger sus dispositivos de red y alinearlos con una infraestructura de seguridad.

Funciones de gestión de dispositivos, AXIS Device Manager

Instalación	Mantenimiento
> Asignar dirección IP > Exportar lista de dispositivos y seguimiento de activos* > Gestión de usuarios y contraseñas* > Gestión de ACAP > Actualizar firmware* > Gestión de certificados HTTPS* > Distribución de certificados IEEE 802.1x* > Etiquetado de dispositivos	> Estado del dispositivo > Recopilar datos de dispositivo > Configurar dispositivos y copiar configuraciones en varios dispositivos > Conectar a varios servidores/sistemas > Restaurar puntos > Restaurar los ajustes predeterminados de fábrica > Sustituir dispositivos > Renovación y gestión de certificados* > Refuerzo de la ciberseguridad*

**Indica una función de control de la ciberseguridad*

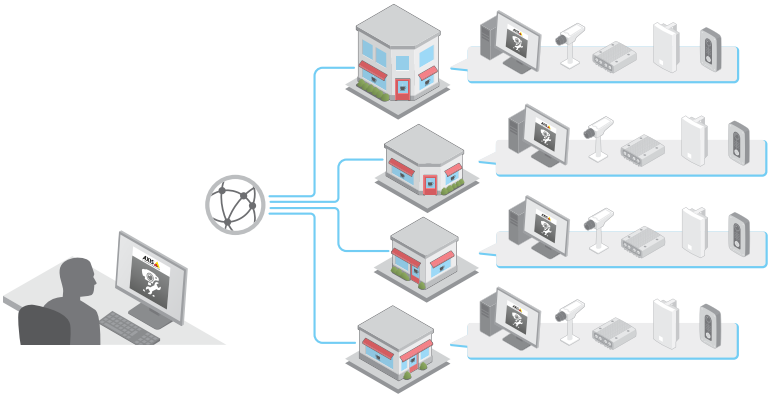


Figura 1. Gestión de varios sitios

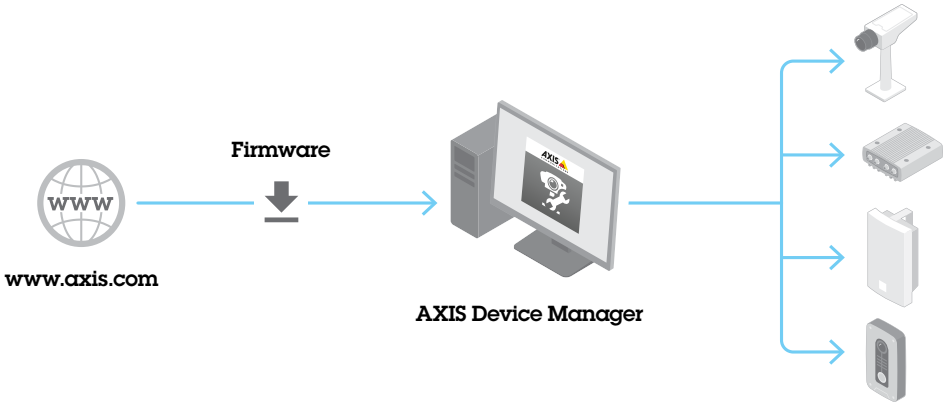


Figura 2. Actualización del firmware

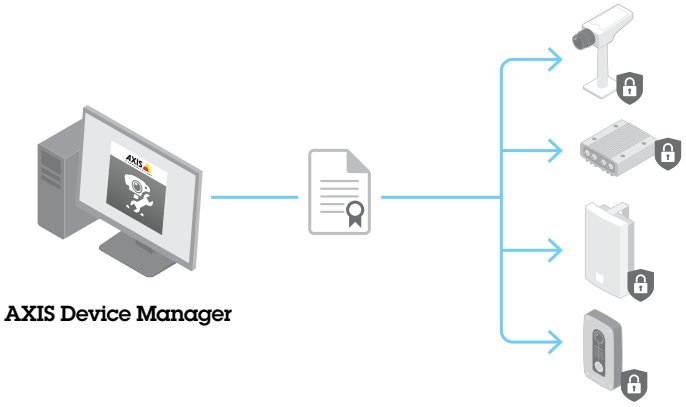


Figura 3. Gestión de certificados

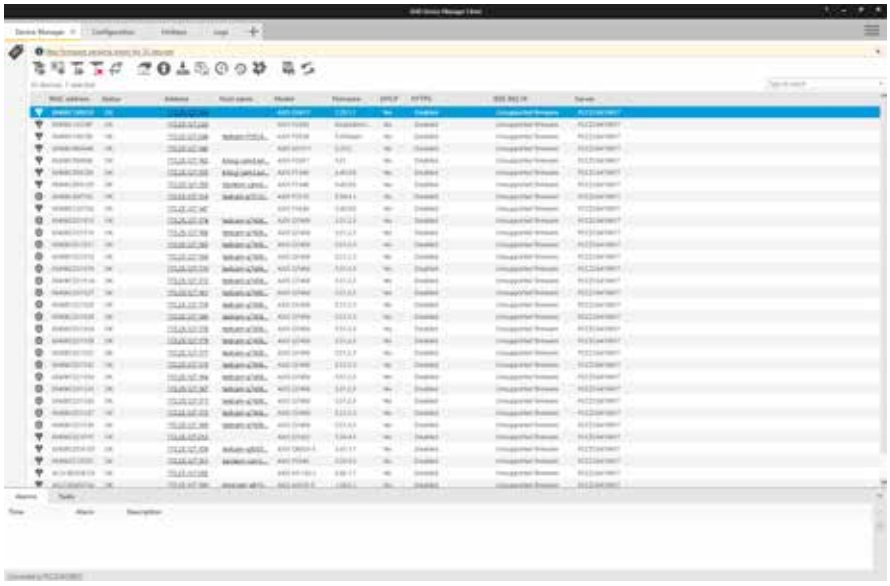
2. Inventario de dispositivos

Un aspecto fundamental a la hora de garantizar la seguridad de una red empresarial es mantener un inventario completo de los dispositivos que hay en ella. Al crear o revisar una política de seguridad global, es importante tener conocimientos y una documentación clara sobre cada dispositivo, no solo de los activos críticos. Esto es así, porque cada dispositivo que sea omitido puede ser un medio de acceso para los atacantes. No puede proteger los dispositivos que omita o de los que no tenga un conocimiento completo.

El inventario de dispositivos constituye un paso fundamental para proteger una red empresarial. Para ayudarle a conseguirlo, AXIS Device Manager:

> Permite acceder fácilmente a un inventario actualizado y completo de los dispositivos de su red al trabajar con auditorías y servicios de respuesta frente a incidentes.
> Proporciona una lista completa de sus dispositivos, ordenados por número total, tipo, número de modelo, etc.
> Indica el estado de cada dispositivo presente en la red.

Recomendaciones
AXIS Device Manager ofrece una forma automatizada para acceder a inventario en tiempo real de los dispositivos de red Axis. Con él podrá identificar, enumerar y ordenar automáticamente sus dispositivos. Igual de importante es que permite utilizar etiquetas para agrupar y ordenar dispositivos en función de sus propios criterios, para conocer y documentar fácilmente todos los dispositivos Axis presentes en su red.



AXIS Device Manager ofrece una visión clara de su inventario de dispositivos.

3. Política de cuentas y contraseñas

El control de autenticación y privilegios es una parte importante a la hora de proteger los recursos de red. Implementar una política sirve para reducir el riesgo de uso incorrecto accidental o deliberado durante más tiempo. Una parte fundamental es reducir el riesgo de contraseñas cuya seguridad está comprometida. Es importante contar con contraseñas seguras; sin embargo, las contraseñas de dispositivos pueden difundirse dentro de una organización. Cuando esto sucede, pierde el control de las personas que pueden acceder a ellas. AXIS Device Manager ayuda a gestionar fácilmente varias cuentas y contraseñas para dispositivos Axis.

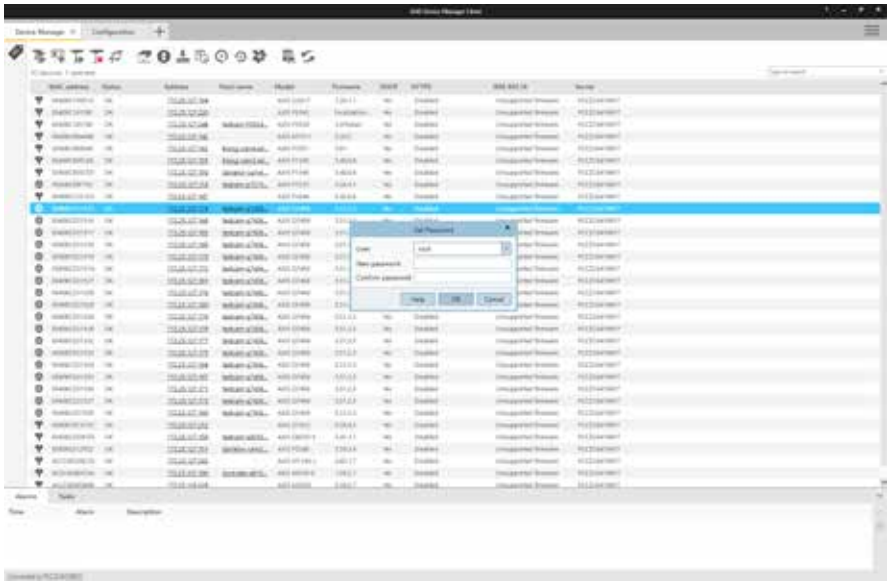
¿Por qué debería tener más de una cuenta de usuario en los dispositivos?
> Puede controlar los niveles de privilegio para diferentes tipos de usuario (máquinas y humanos).
> Puede reducir el riesgo de poner en peligro la contraseña root (maestra).
> Puede restablecer las credenciales para un tipo de usuario, sin afectar a los demás usuarios.

Trabajar con privilegios en AXIS Device Manager
En AXIS Device Manager, los dispositivos Axis pueden admitir varias cuentas y pertenecer a tres niveles de privilegio distintos: observador, operador y administrador. Aquí le mostramos cómo pueden gestionarse privilegios para cámaras de red Axis.

Los usuarios con privilegios de observador pueden acceder al vídeo y al control PTZ. Los usuarios con derechos de operador pueden optimizar los ajustes de la cámara y los perfiles de transmisión de video. Los administradores pueden administrar cuentas, modificar ajustes de red y controlar varios servicios del dispositivo. Cada tipo de usuario que acceda a la cámara debería tener su propia cuenta.

Pasos recomendados de procedimiento

> Antes de agregar cámaras al VMS, es recomendable agregarlas a AXIS Device Manager.
> En AXIS Device Manager, seleccione todas las cámaras y cree una nueva cuenta de usuario llamada "vms" o similar, y defina una contraseña segura. Los privilegios deben adaptarse a los requisitos del VMS, y pueden ser de operador o de administrador (consulte con el fabricante).
> Agregue los dispositivos al VMS con la cuenta "vms" y la contraseña que ha definido.
> Vuelva a AXIS Device Manager, seleccione de nuevo todas las cámaras y restablezca (cambie) la contraseña de la cuenta "root" con una contraseña nueva y segura. La contraseña de la cuenta "root" solo deben conocerla unas pocas personas (que utilicen AXIS Device Manager).
> Si alguien de la organización necesita utilizar un navegador web para acceder a un dispositivo por tareas de mantenimiento o localización de problemas, no le proporcione la contraseña root. Utilice AXIS Device Manager para crear una cuenta nueva (provisional) para los dispositivos seleccionados con privilegios de administrador u operador. Cuando terminen la tarea, utilice AXIS Device Manager para eliminar la cuenta provisional.
> AXIS Device Manager admite el uso de administradores locales, y de grupos y usuarios de dominio. Puede utilizar un administrador local si solamente se accederá al cliente AXIS Device Manager desde el equipo que aloja el servidor de AXIS Device Manager. Se recomienda utilizar usuarios de dominio si la persona que mantiene el sistema va a utilizar clientes remotos.



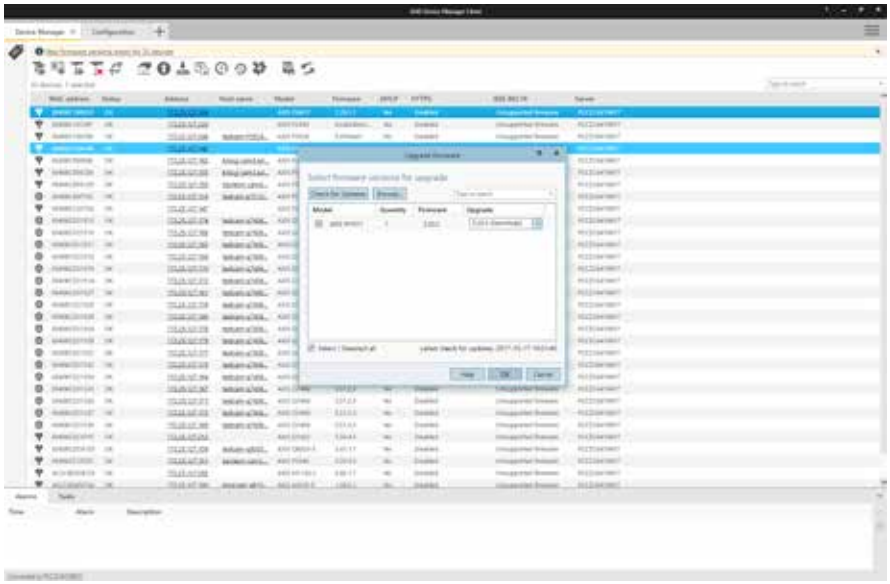
Cambio de funciones de usuario y contraseñas en AXIS Device Manager.

4. Actualizaciones de firmware

Las versiones de firmware más recientes incluyen parches para vulnerabilidades conocidas. Es fundamental utilizar siempre el software más reciente, porque los atacantes pueden tratar de aprovechar cualquier vulnerabilidad conocida. Igual de importante es que la implementación rápida del nuevo firmware potencia la capacidad de funcionamiento y acaba con los cuellos de botella relacionados con la implementación manual de las actualizaciones con nuevas versiones. AXIS Device Manager se conecta con www.axis.com y descarga las últimas versiones de servicio o de firmware aplicables. Si prefiere no hacer descargas directamente de Internet en su red, puede guardar las actualizaciones en un dispositivo USB y luego cargarlas en su cliente AXIS Device Manager. También muestra si hay nuevo firmware disponible y permite implantarlo rápidamente en dispositivos Axis.

¿Por qué debería ejecutar siempre las versiones de firmware más recientes?

> Su red y sus dispositivos están protegidos con los parches más recientes frente a vulnerabilidades conocidas, sobre todo las críticas.
> Sus dispositivos están actualizados, para incorporar las últimas mejoras de rendimiento y resolver cualquier fallo o defecto conocido.
> Puede acceder de forma inmediata a las últimas mejoras de funciones y prestaciones.



Con AXIS Device Manager, actualizar el firmware es más sencillo, gracias a las notificaciones en pantalla y al uso de cuadros de diálogo intuitivos.

5. Protección adicional

Una buena política de usuario/contraseña y el uso de las versiones de firmware actualizadas en los dispositivos servirán para mitigar los riesgos habituales para los dispositivos. La guía de protección de Axis detalla medidas adicionales para reducir riesgos en organizaciones grandes y críticas. Incluyen la desactivación de servicios que no se utilizan y la activación de servicios que pueden ayudar a detectar y monitorizar indicaciones de ataques o intrusiones.

Con AXIS Device Manager, el proceso para implementar algunas de estas políticas es más sencillo. Axis proporciona una plantilla de configuración para los ajustes básicos recomendados. Puede encontrar más información aquí:
www.axis.com/products/axis-device-manager/support-and-documentation.

Cómo reforzar la seguridad de los dispositivos según la guía de protección de Axis

> Descargue el archivo de configuración de la plantilla de protección en www.axis.com/products/axis-device-manager/support-and-documentation
> Edite el archivo de configuración para seleccionar los elementos relevantes
> Seleccione dispositivos
> Haga clic con el botón derecho y seleccione "Configurar dispositivos | Configurar..."
> Haga clic en "Archivo de configuración" y seleccione el archivo descargado
> Modifique los ajustes según sea necesario

6. Servicio de autoridad de certificación

Una autoridad de certificación (CA) es un servicio que emite certificados digitales para servidores, clientes o usuarios. Las CA pueden ser públicas o privadas. Las CA de confianza pública, como Comodo y Symantec (antes, Verisign) suelen utilizarse para servicios públicos, como correo electrónico y sitios web públicos.

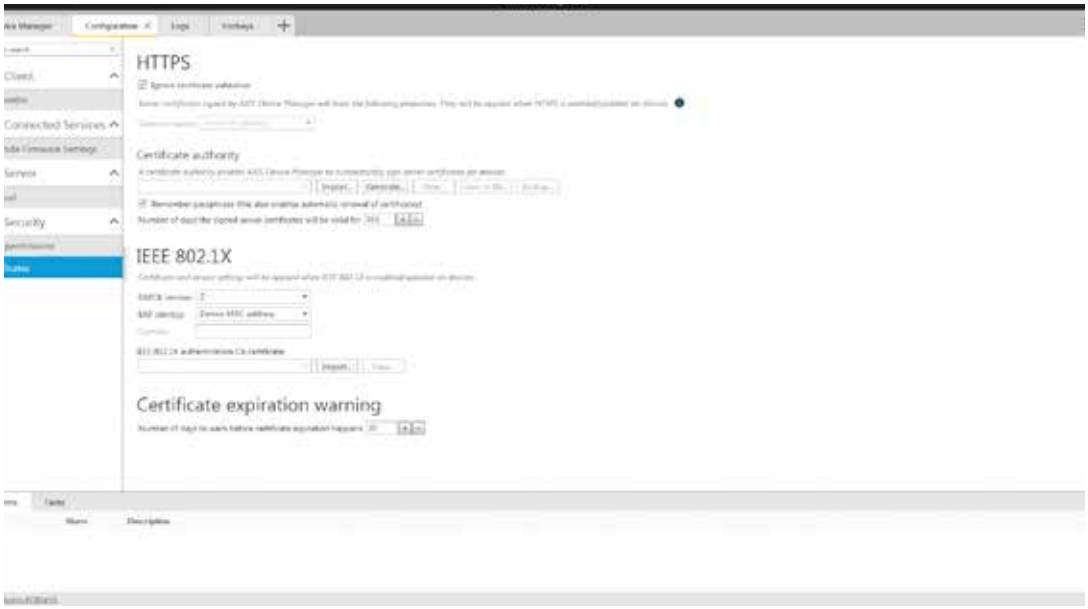
Las CA privadas (habitualmente, servicio de certificado/directorio activo) emiten certificados para servicios de red privada/interna. En un sistema de gestión de vídeo, suele ser para HTTPS (Hyper Text Transfer Protocol Secure) (cifrado de red) y IEEE 802.1x (control de acceso de red). AXIS Device Manager incluye un servicio de CA para dispositivos Axis y puede operar como CA root privada o CA intermedia privada; parte de una PKI (infraestructura de clave pública).

Se utilizan certificados con firma de CA para certificados IEEE 802.1x (cliente) y HTTPS (servidor).

HTTPS
HTTPS es la versión segura de HTTP, con la que se cifran las comunicaciones entre un cliente y un servidor. Los certificados con firma propia son suficientes para lograr una conexión cifrada. No existe ninguna diferencia en el nivel de cifrado entre certificados con firma de CA y con firma propia. La única diferencia es que los certificados con firma propia no protegen contra el spoofing de red, una forma de ataque en la que el ordenador atacante trata de hacerse pasar por un servidor legítimo. Los certificados con firma de CA agregan un punto de confianza para que los clientes autentiquen que están accediendo a un dispositivo de confianza. Tenga en cuenta que el cliente de vídeo (VMS) debe admitir la solicitud de vídeo a través de HTTPS (RTP a través de RTSP a través de HTTP) a fin de cifrar el vídeo.

IEEE 802.1X
Este estándar, denominado 802.1X, impide que dispositivos de red no autorizados accedan a la red local. Para acceder a la red (y a sus recursos), los dispositivos deben autenticarse a sí mismos. Puede utilizarse diferentes medios de autenticación, como: dirección MAC (filtro MAC), usuario/contraseña o certificado de cliente. El propietario del sistema decide qué método utilizar; la opción adecuada depende de las amenazas, el riesgo y los costes.

Operar una infraestructura 802.1X es una inversión. Requiere switches gestionables y servidores adicionales, habitualmente un RADIUS (Remote Authentication Dial-In User Service). Para utilizar certificados de cliente se requiere una CA (privada o pública) que pueda emitir certificados de cliente. En casi todos los casos, la infraestructura necesita personal para su mantenimiento y monitorización.



Configuración de certificados en AXIS Device Manager.

7. Gestión de ciclo de vida de certificados

La gestión de ciclo de vida de certificados es una forma de gestionar de forma económica todos los procesos y las tareas relacionadas con la emisión, la instalación, la inspección, la corrección y la renovación de certificados en un largo periodo de tiempo. AXIS Device Manager permite gestionar con eficiencia certificados, al permitir a los administradores hacer esto:

> Emitir certificados con firma de CA si no hay disponible otra CA.
> Distribuir fácilmente certificados IEEE 802.1X.
> Implantar fácilmente certificados HTTPS.
> Supervisar fechas de caducidad de certificados.
> Renovar certificados fácilmente antes de la caducidad.

Recomendaciones de CA intermedias y root privadas.
No se recomienda exponer dispositivos Axis como servidores públicos de cara al público. Por ello, utilizar una CA pública para recursos privados no es una solución rentable.

Para HTTPS, el servidor VMS es el único cliente que debe validar que está accediendo a una cámara de confianza. Los clientes de operador nunca accederán directamente a las cámaras, ya que el servidor VMS proporciona vídeo grabado y en vivo. En esta situación, incorporar certificados de servidor de cámara en una PKI empresarial existente tiene un valor limitado.

Utilizar AXIS Device Manager como CA privada es la solución más rentable. Después de generar un certificado de CA root, instale el certificado de AXIS Device Manager en el almacén de certificados del servidor VMS. Si otros clientes están accediendo a cámaras directamente (para el mantenimiento o la localización de problemas), instale el CA root de AXIS Device Manager también en esos clientes.

Para 802.1X, la cámara necesita un certificado de cliente a fin de autenticarse en un servidor RADIUS. Se recomienda hacer que el administrador para la CA/PKI empresarial genere un certificado de CA intermedia y que lo exporte como certificado PKCS#12 (P12) que puede instalarse en AXIS Device Manager.

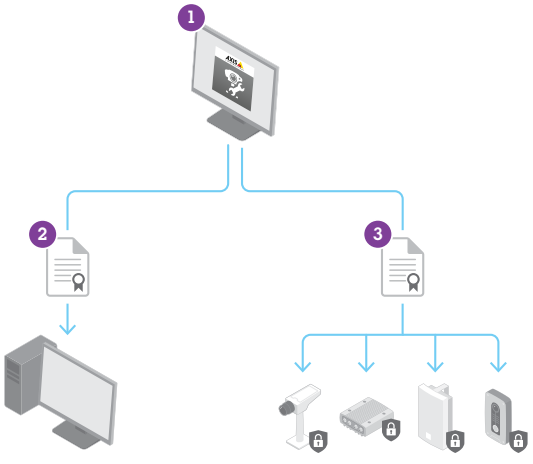


Figura 4, izquierda: La gestión de certificados HTTPS implica lo siguiente:
1) generar un certificado de CA root o intermedia en AXIS Device Manager; 2) exportar un certificado de CA al VMS; y 3) cargar certificados de servidor a los dispositivos.

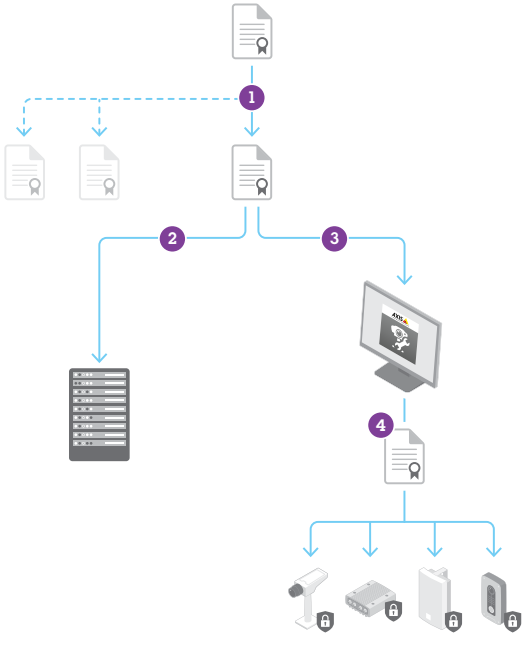


Figura 5, derecha: La distribución de certificados IEEE 802.1X implica lo siguiente: 1) generar un certificado de cliente y de CA intermedia; 2) instalar un certificado de CA en el servidor RADIUS; 3) importar un certificado de CA en AXIS Device Manager; y 4) cargar certificados de cliente y de CA a los dispositivos.

8. Conclusión

La gestión y el control de la seguridad son partes importantes a la hora de implementar una estrategia de ciberseguridad eficaz. Cada una de ellas es un proceso continuado para el que hay que mantener estados claros y seguir acciones adecuadas para mitigar posibles amenazas que puedan afectar a su red IP. AXIS Device Manager pone a su disposición una herramienta para gestionar sus dispositivos y aumentar la seguridad de su red. Contacte con su representante de Axis o visite www.axis.com para obtener más información o asistencia.

Acerca de Axis Communications

Axis ofrece soluciones de seguridad inteligentes que permiten crear un mundo más seguro e inteligente. Axis es la marca líder del mercado en vídeo en red y está impulsando el sector al lanzar permanentemente productos de red basados en una plataforma abierta, ofreciendo así gran valor a sus clientes a través de una red de socios global. Axis cuenta con relaciones duraderas con sus socios y les proporciona conocimientos y productos de red innovadores, tanto en mercados actuales como nuevos.

Axis tiene más de 2700 empleados dedicados en más de 50 países de todo el mundo, que cuentan con el respaldo de una red global integrada por más de 90 000 socios. Fundada en 1984, Axis es una compañía sueca que cotiza en la bolsa de Estocolmo NASDAQ con el nombre AXIS.

Para más información sobre Axis, visite nuestra web www.axis.com.