

AXIS Device Manager

Introducción

La importancia de la ciberseguridad sigue creciendo en los sectores de la vigilancia y la seguridad. Una ciberseguridad eficaz requiere garantizar una defensa lo suficientemente sólida como para proteger adecuadamente su red IP en todos los niveles, desde los productos y socios que elija hasta los requisitos que usted y ellos establezcan.

Esta guía describe cómo usar AXIS Device Manager para reforzar su sistema y mejorar la seguridad. Se centra en aspectos clave y presenta una serie de recomendaciones.

Gestión del ciclo de vida de los dispositivos

En Axis, conocemos la importancia de una sólida base de seguridad durante todo el ciclo de vida del dispositivo. Nuestro compromiso de ciberseguridad garantiza que nuestros productos y soluciones brinden una protección sólida contra posibles amenazas.

Implementación

Axis ofrece dispositivos seguros por diseño con funciones de seguridad integradas, como mecanismos de arranque seguro, un sistema operativo firmado y almacenamiento cifrado. Además, AXIS Device Manager ayuda a los instaladores y administradores de sistemas a configurar e implementar dispositivos de forma segura, garantizando una configuración estable desde el principio.

Servicio activo

Durante la fase operativa, Axis ofrece actualizaciones periódicas de software y parches de seguridad como protección frente a vulnerabilidades. AXIS Device Manager también permite la supervisión y mantenimiento remotos, fomentando una rápida resolución de problemas y un tiempo de inactividad mínimo. Además, nuestras guías de seguridad contienen recomendaciones para configurar dispositivos que satisfagan requisitos de seguridad específicos.

Desinstalación

A la hora de retirar o sustituir dispositivos, AXIS Device Manager facilita la desactivación segura borrando los datos confidenciales y restaurando los dispositivos a su configuración de fábrica. Esto garantiza la ausencia de información confidencial en el dispositivo, protegiendo los datos del usuario y evitando el acceso no autorizado.

AXIS Device Manager

AXIS Device Manager es una herramienta local que representa una forma sencilla, rentable y cibersegura de gestionar todas las tareas principales de instalación, seguridad y mantenimiento (consulte la siguiente tabla). La herramienta es adecuada para gestionar hasta dos mil dispositivos Axis en una sola ubicación, o varios miles de dispositivos repartidos entre varias ubicaciones. AXIS Device Manager permite implementar eficazmente controles de ciberseguridad para proteger sus dispositivos de red y adaptarlos a una infraestructura de seguridad.

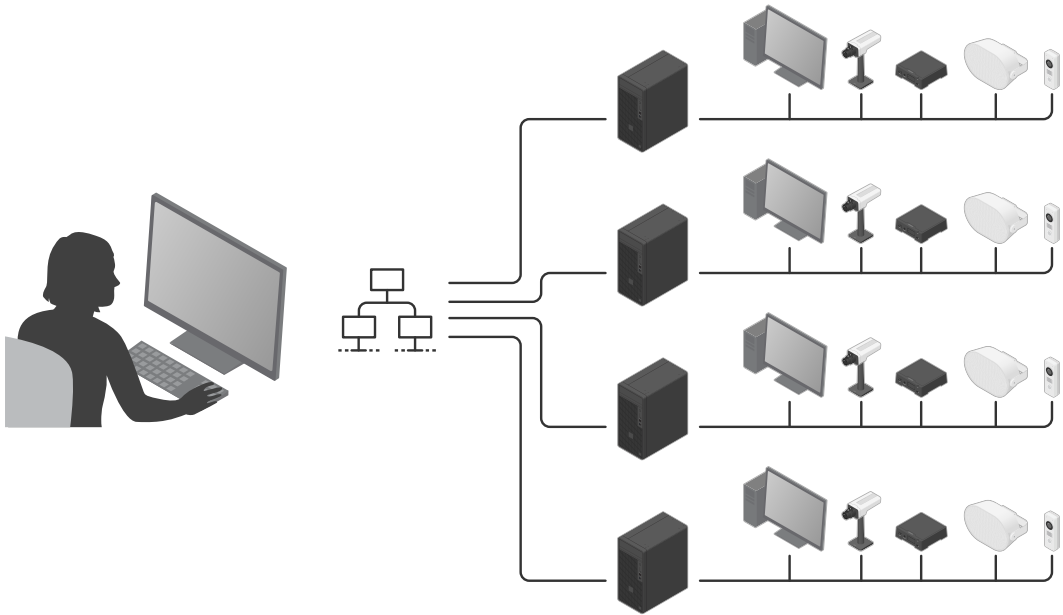
Funciones de gestión de dispositivos, AXIS Device Manager

Instalación	Mantenimiento
Asignación de una dirección IP	Estado de los dispositivos
Exportar lista de dispositivos y seguimiento de activos*	Recopilar datos de dispositivos
Gestión de usuarios y contraseñas*	Configurar dispositivos y copiar las configuraciones en varios dispositivos
Gestión de la plataforma de aplicaciones para cámaras AXIS	Conectarse a diversos servidores/sistemas
Actualizar el sistema operativo AXIS, basado en LTS o Active*	Restaurar puntos

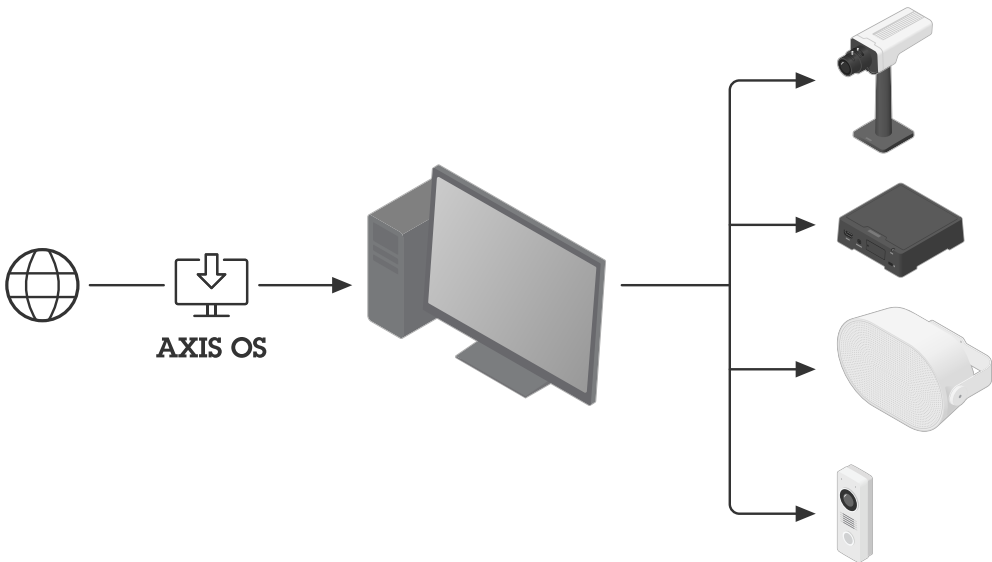
Gestión de certificados HTTPS*	Restauración de los ajustes predeterminados de fábrica
Administrar certificados IEEE 802.1*/**	Sustituir dispositivo(s)
Etiquetado de dispositivos	Renovación y gestión de certificados*
	Refuerzo de la ciberseguridad*

* Indica una función de control de la ciberseguridad.

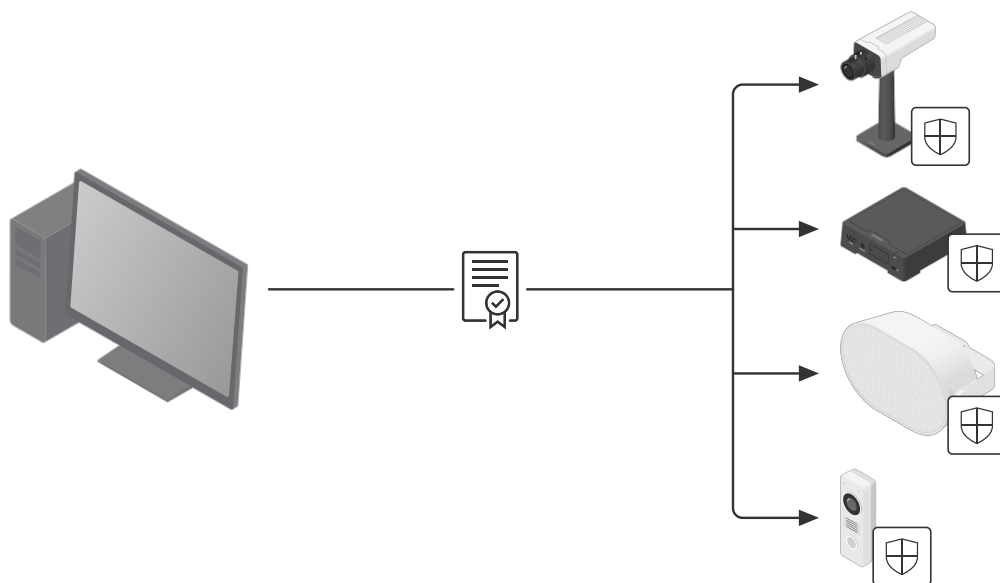
** Actualmente no compatibles con servicios de certificación de Active Directory. Validado para FreeRADIUS en Linux.



Gestión de varios sitios.



Actualización de AXIS OS.



Gestión de certificados.

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 residen en ella. Al crear o revisar una política de seguridad general, es importante tener conocimientos y una documentación clara de todos los dispositivos, no solo de los activos críticos. Esto se debe a que cualquier dispositivo omitido puede ser una vía de acceso para los atacantes. No puede proteger los dispositivos que omite o de los que no tenga un conocimiento completo.

Elaborar el inventario de dispositivos es un paso esencial para proteger una red empresarial. AXIS Device Manager puede ayudarle en este aspecto, ya que:

- Le proporciona fácil acceso 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, que puede ordenarse por número total, tipo, número de modelo, etc.
- Indica del estado de cada dispositivo presente en su red.
- Ayuda a planificar con antelación, mostrando cuándo finalizará la asistencia técnica del software del dispositivo y enumerando qué productos más nuevos pueden utilizarse como sustitutos.

AXIS Device Manager Client
? - + X

Device Manager ×
 Configuration
Logs
Hotkeys
+

Manage devices

250 devices, 1 selected

	MAC address	Status	Address	Model	Firmware	DHCP	HTTPS	Server	Warranty expiration	End of software support	Device replacements
🔍	ACCC8BF37017	OK	10.21.66.4	AXIS Q9216-SLV	11.11.160	Yes	Enabled	ADM	2023-05-17 (3Y)	No information	No information
🔍	ACCC8EF34AD0	OK	10.21.66.228	AXIS Q1659	11.11.160	Yes	Enabled	ADM	2020-02-01 (3Y)	2029-12-31	AXIS Q1809-LE
🔍	ACCC8ECD1E9	OK	10.21.68.61	AXIS P8815-2	11.11.160	Yes	Enabled	ADM	Info unavailable	No information	No information
🔍	ACCC8ECD123	OK	10.21.68.60	AXIS P8815-2	11.11.160	Yes	Enabled	ADM	Info unavailable	No information	No information
🔍	ACCC8EEB2B4	OK	10.21.66.209	AXIS M1135	10.12.289	Yes	Enabled	ADM	2023-01-24 (3Y)	2027-12-31	AXIS M1135 Mk II
🔍	ACCC8EEBCBD4	OK	10.21.66.194	AXIS P3245-V	11.11.160	Yes	Enabled	ADM	1973-04-01 (3Y)	2029-12-31	AXIS P3265-V
🔍	ACCC8EEB910F	OK	10.21.66.210	AXIS M1137	10.12.289	Yes	Enabled	ADM	2023-01-24 (3Y)	2027-12-31	AXIS M1137 Mk II
🔍	ACCC8EA73EB	OK	10.21.66.134	AXIS M3075-V	10.12.289	Yes	Enabled	ADM	2023-03-13 (3Y)	2027-12-31	No information
🔍	ACCC8EE89BF7	OK	10.21.66.53	AXIS P1378	11.11.160	Yes	Disabled	ADM	2023-02-13 (3Y)	2029-12-31	AXIS P1388 AXIS P1388-B
🔍	ACCC8EE8935A	OK	10.21.66.52	AXIS P1377	11.11.160	Yes	Enabled	ADM	2023-02-13 (3Y)	2029-12-31	AXIS P1387 AXIS P1387-B
🔍	ACCC8EE80D84	OK	10.21.66.54	AXIS M3064-V	10.12.289	Yes	Enabled	ADM	2023-02-12 (3Y)	2027-12-31	AXIS M3085-V
🔍	ACCC8EE80849	OK	10.21.68.55	AXIS M3065-V	10.12.289	Yes	Enabled	ADM	2023-02-12 (3Y)	2027-12-31	AXIS M3085-V
🔍	ACCC8EE80816	OK	10.21.68.56	AXIS M3065-V	10.12.289	Yes	Enabled	ADM	2023-02-12 (3Y)	2027-12-31	AXIS M3085-V
🔍	ACCC8EE56609	OK	10.21.68.80	AXIS Q6055-E	8.40.78	Yes	Disabled	ADM	2023-02-06 (3Y)	2025-02-01	AXIS Q6075-E
🔍	ACCC8EE521A2	OK	10.21.66.5	AXIS P3925-R	12.5.68	Yes	Disabled	ADM	2026-03-13 (5Y)	2033-12-31	No information
🔍	ACCC8EE49D90	OK	10.21.66.211	AXIS M3205-LVE	10.12.289	Yes	Disabled	ADM	2023-01-07 (3Y)	2027-12-31	AXIS M3215-LVE
🔍	ACCC8EE2401B	OK	10.21.66.208	AXIS Q1798-LE	11.11.160	Yes	Enabled	ADM	2022-12-18 (3Y)	No information	No information
🔍	ACCC8EE1C43F	OK	10.21.66.207	AXIS P7304	12.5.68	Yes	Disabled	ADM	2022-12-04 (3Y)	2033-12-31	No information
🔍	ACCC8EE10192	OK	10.21.66.230	AXIS M1145-L	6.50.5.20	Yes	Enabled	ADM	2021-07-12 (3Y)	2026-11-30	AXIS M1325-LVE
🔍	ACCC8EE06247	OK	10.21.66.203	AXIS P3245-LVE	11.11.160	Yes	Enabled	ADM	2022-10-17 (3Y)	2029-12-31	AXIS P3265-LVE
🔍	ACCC8EDE17A8	OK	10.21.66.213	AXIS Q1700-LE	11.11.160	Yes	Enabled	ADM	2022-09-26 (3Y)	No information	No information
🔍	ACCC8EDC1601	OK	10.21.66.50	AXIS M3215-LVE	10.12.289	Yes	Disabled	ADM	2023-03-25 (3Y)	2030-11-30	AXIS M3215-LVE

Connected to ADM
⬆️ Alarms and Tasks

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

AXIS Device Manager representa 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. Además, e igualmente importante, le permite usar etiquetas para agrupar y ordenar dispositivos según sus propios criterios, lo que facilita obtener una visión general y documentar todos los dispositivos Axis en su red.

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 con el tiempo. Imponer el uso de contraseñas sólidas es fundamental, pero también lo es reducir el riesgo de que se vean comprometidas. Las contraseñas de los dispositivos suelen propagarse dentro de una organización y, cuando esto sucede, se pierde el control sobre quién tiene acceso 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 otros.

Trabajar con privilegios en AXIS Device Manager

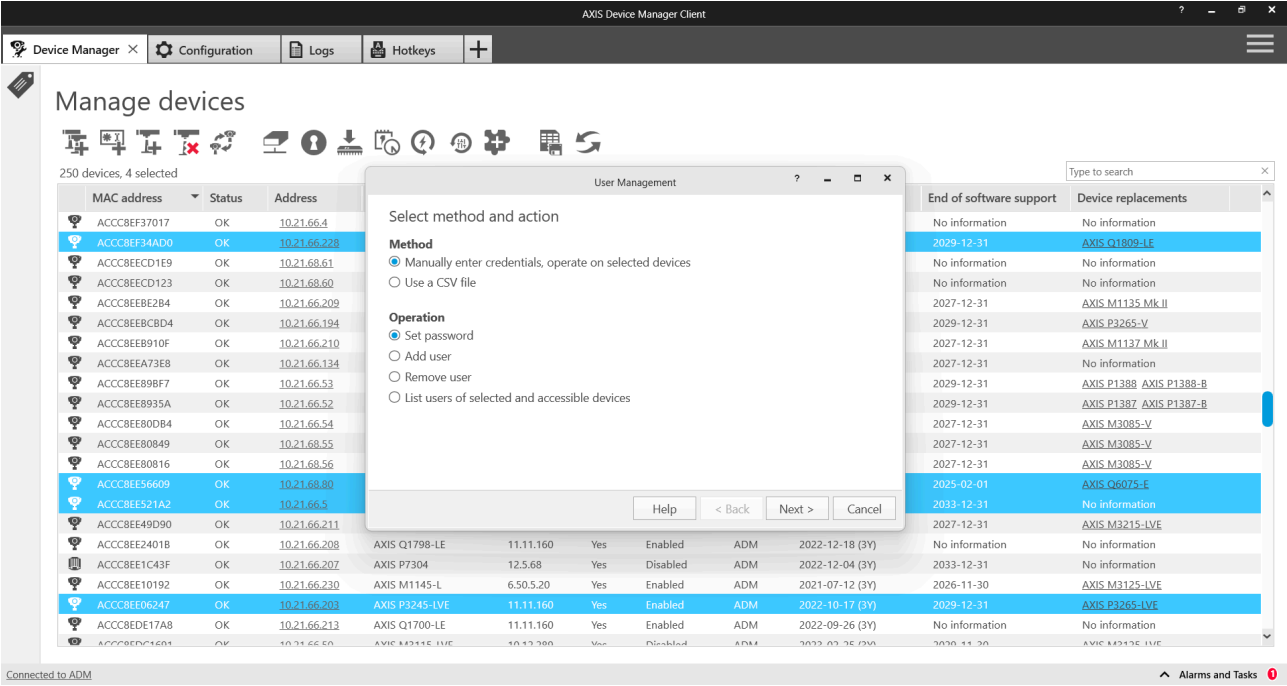
Los dispositivos Axis admiten varias cuentas, cada una con uno de tres niveles de privilegio distintos:

- **Viewers (Visualizadores):** Estos usuarios tienen acceso al control de vídeo y PTZ.
- **Operators (Operadores):** Usuarios con derechos de operador que pueden optimizar los ajustes de la cámara y los perfiles de transmisión de vídeo.
- **Administradores:** 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. Por ejemplo, podría configurar el rol "Personal de sala de control" con el nivel de privilegio "Operador", mientras que el rol "Personal de vigilancia" podría requerir solo el nivel de privilegio "Espectador".

Pasos recomendados

- Antes de incorporar cámaras al VMS, añádalas 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).
- Añada los dispositivos al VMS con la cuenta y la contraseña que creó.
- Regrese en 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" deben conocerla únicamente unas pocas personas (que utilicen AXIS Device Manager).
- Si alguien necesita utilizar un navegador web para acceder a un dispositivo por tareas de mantenimiento o localización de problemas, **no** le proporcione la contraseña root. En su lugar, utilice AXIS Device Manager para crear una cuenta nueva (provisional) para los dispositivos seleccionados con privilegios de administrador u operador. Cuando terminen su labor, 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. Recomendamos usar usuarios de dominio si la persona a cargo del mantenimiento del sistema utilizará clientes remotos.



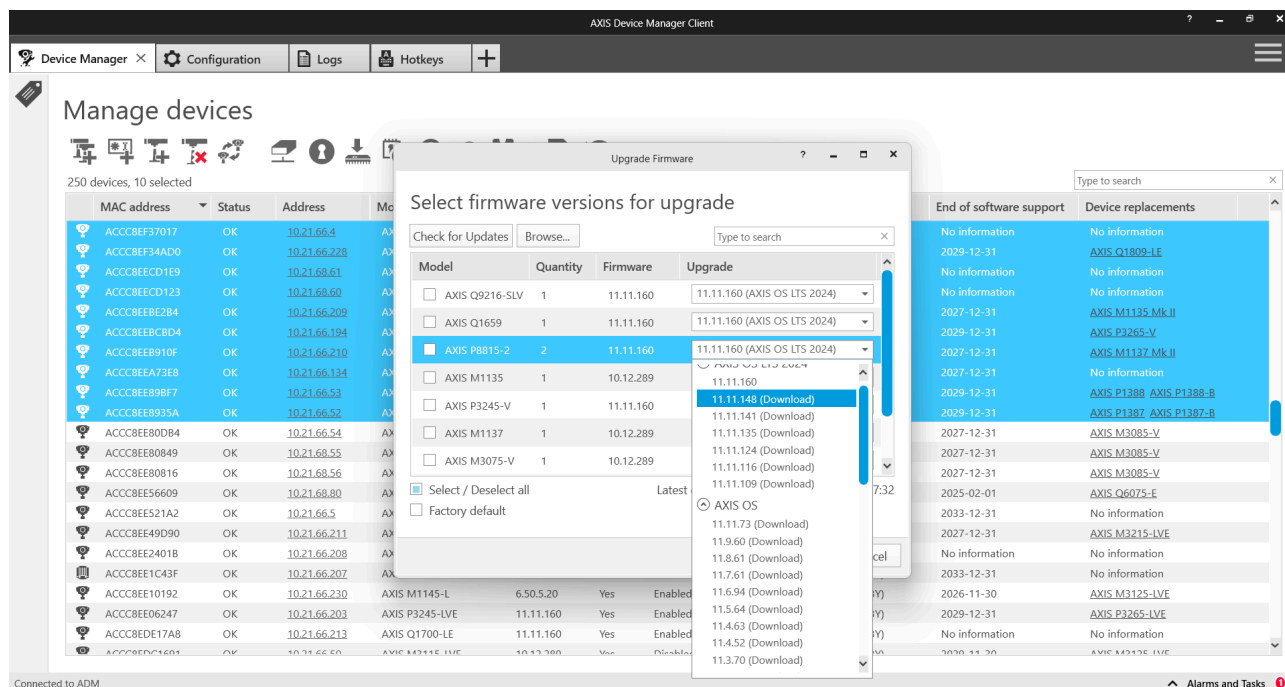
Cambio de funciones de usuario y contraseñas en AXIS Device Manager.

Actualizaciones de AXIS OS

Las versiones actualizadas del sistema operativo AXIS incluyen parches para vulnerabilidades conocidas. Es fundamental utilizar siempre el software más reciente, porque los atacantes pueden tratar de aprovechar las vulnerabilidades conocidas. Igualmente importante es que la rápida implementación de una nueva versión del sistema operativo AXIS mejora la capacidad operativa y elimina los cuellos de botella relacionados con la implementación manual de actualizaciones. AXIS Device Manager se conecta a www.axis.com y descarga las últimas versiones aplicables del sistema operativo AXIS o de los servicios. 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 nuevas versiones del sistema operativo AXIS disponibles y permite implantarlas rápidamente en dispositivos Axis.

Por qué debería ejecutar siempre las versiones del sistema operativo AXIS 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, así como con correcciones de errores y fallos.
- Puede acceder de forma inmediata a las últimas mejoras de funciones y prestaciones.



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

Protección adicional

Aplicar una buena política de usuario y contraseña, así como ejecutar versiones actualizadas del sistema operativo AXIS, mitigará los riesgos comunes para los dispositivos. La *AXIS Hardening Guide (Guía de protección de AXIS)* detalla medidas adicionales para reducir riesgos en organizaciones grandes y críticas. Esto incluye la desactivación de servicios que no se puedan utilizar y la activación de servicios que ayuden a detectar y supervisar indicios de un ataque o vulneración. AXIS Device Manager simplifica el proceso de implementación de algunas de estas políticas. Axis proporciona una plantilla de configuración para los ajustes básicos recomendados.

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

- Lea la *AXIS Hardening Guide (Guía de protección de AXIS)* y descargue el archivo de plantilla incluido al final del documento.
- Edite el archivo de configuración para seleccionar los elementos relevantes.
- Seleccione dispositivos en el inventario de AXIS Device Manager.
- Haga clic con el botón derecho y seleccione "Configurar dispositivos > Configurar..."
- Haga clic en "Archivo de configuración" y seleccione el archivo descargado.
- Ajuste los valores como corresponda.

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, un servicio de certificado/directorio activo) emiten certificados para servicios de red privada/interna. En un sistema de gestión de vídeo, esto se aplica principalmente al cifrado de red HTTPS y al control de acceso a la red IEEE 802.1X. AXIS Device Manager incluye un servicio de CA para dispositivos Axis y puede funcionar como CA root privada o como CA intermedia privada, como parte de una infraestructura de clave pública (PKI) empresarial.

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 diferencia radica en que los certificados autofirmados no protegen contra la suplantación de red, en la que un equipo atacante intenta hacerse pasar por un servidor legítimo. Los certificados firmados por una CA añaden un aspecto de confianza para que los clientes autentiquen que están accediendo a un dispositivo fiable. 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

Conocido habitualmente como 802.1X, este estándar 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. Se pueden emplear varios métodos de autenticación: dirección MAC (filtrado MAC), usuario/contraseña o certificado de cliente. El propietario del sistema decide qué método emplear; la opción más adecuada depende de las amenazas, los riesgos 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.

The screenshot shows the AXIS Device Manager Client interface. The main window is titled 'Manage devices' and displays a list of 250 devices. A 'Secure communication' dialog box is open, showing options to enable or disable HTTPS and IEEE 802.1X. The dialog has three radio buttons: 'Enable or renew HTTPS', 'Enable or renew IEEE 802.1X', and 'Enable or renew HTTPS and IEEE 802.1X'. The third option is selected. Below the dialog, there is a table showing device details, including MAC address, status, address, and various configuration parameters.

MAC address	Status	Address
ACCC8EF37017	OK	10.21.66.4
ACCC8EF34AD0	OK	10.21.66.22
ACCC8EED1E9	OK	10.21.68.61
ACCC8EED123	OK	10.21.68.61
ACCC8EEB2B4	OK	10.21.66.21
ACCC8EEBCB04	OK	10.21.66.11
ACCC8EB910F	OK	10.21.66.21
ACCC8EEA73E8	OK	10.21.66.11
ACCC8EE89BF7	OK	10.21.66.21
ACCC8EE8935A	OK	10.21.66.52
ACCC8EE80DB4	OK	10.21.66.54
ACCC8EE80849	OK	10.21.68.55
ACCC8EE80816	OK	10.21.68.56
ACCC8EE56609	OK	10.21.68.80
ACCC8EE521A2	OK	10.21.66.5
ACCC8EE49D90	OK	10.21.66.21
ACCC8EE24018	OK	10.21.66.20
ACCC8EE1C43F	OK	10.21.66.20
ACCC8EE10192	OK	10.21.66.23
ACCC8EE06247	OK	10.21.66.203
ACCC8EE17A8	OK	10.21.66.213
ACCC8EE1601	OK	10.21.66.50

The 'Secure communication' dialog box has the following options:

- ☐ Enable or renew HTTPS
- ☐ Enable or renew IEEE 802.1X
- ☒ Enable or renew HTTPS and IEEE 802.1X

Below the dialog, there is a table showing device details, including MAC address, status, address, and various configuration parameters.

MAC address	Status	Address	Model	Firmware	Version	Enabled	ADM	2022-10-17 (3Y)	2022-09-26 (3Y)	2022-07-26 (3Y)	2022-07-26 (3Y)	2022-07-26 (3Y)
ACCC8EE8935A	OK	10.21.66.52	AXIS P3245-LVE	11.11.160	Yes	Enabled	ADM	2022-10-17 (3Y)				
ACCC8EE80DB4	OK	10.21.66.54	AXIS Q1700-LE	11.11.160	Yes	Enabled	ADM	2022-09-26 (3Y)				
ACCC8EE80849	OK	10.21.68.55	AXIS M3215-LVE	10.13.380	Yes	Disabled	ADM	2022-07-26 (3Y)				

Configuración de certificados en AXIS Device Manager.

Gestión de ciclo de vida de certificados

La gestión del ciclo de vida de los certificados permite gestionar de forma rentable todos los procesos y tareas relacionados con la emisión, instalación, inspección, reparación y renovación de certificados con el tiempo. AXIS Device Manager permite gestionar certificados de forma eficiente, permitiendo a los administradores:

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

Recomendaciones para CA root privadas e intermedias

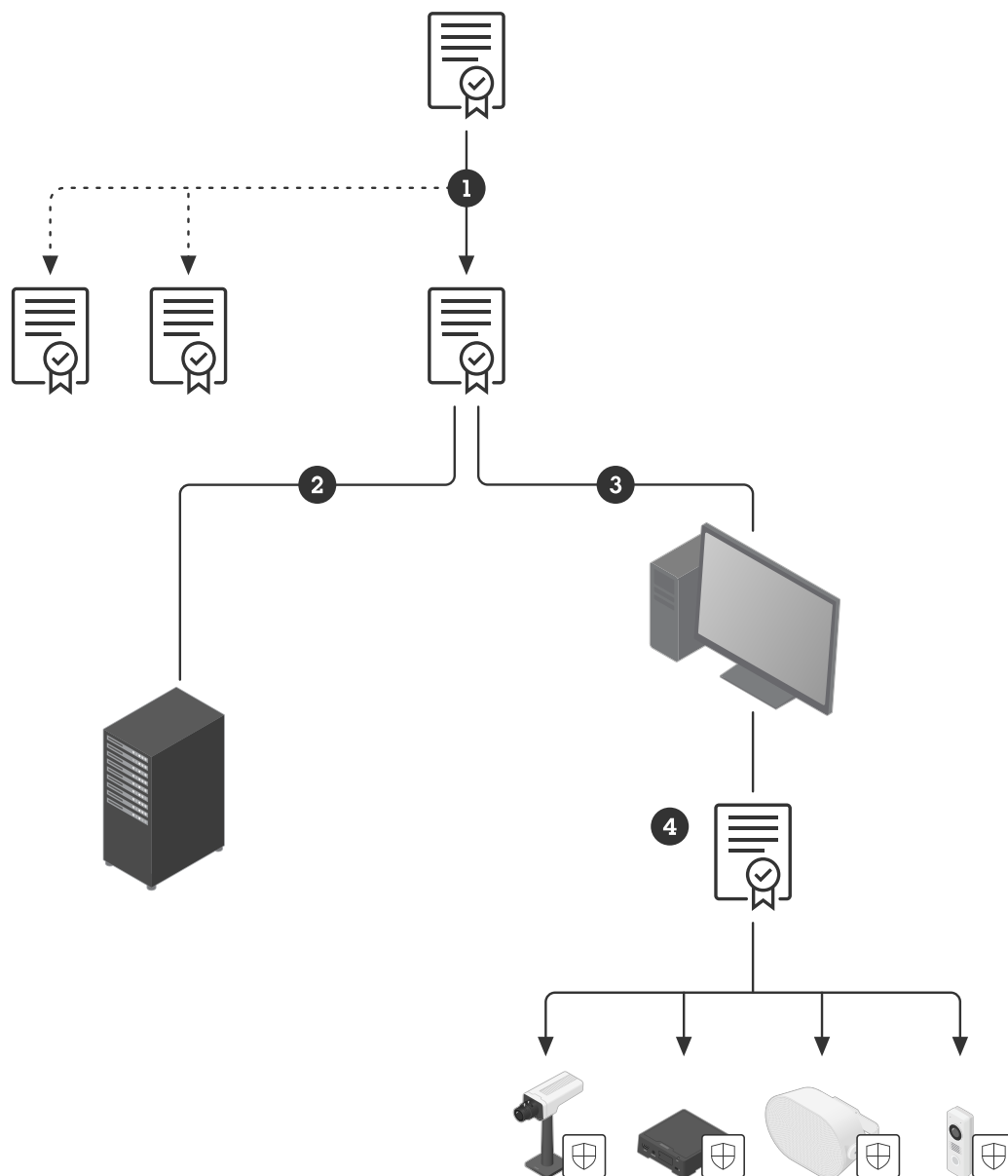
No se recomienda exponer dispositivos Axis como servidores públicos de cara al público. Por este motivo, utilizar una CA pública para recursos privados no constituye una solución rentable.

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

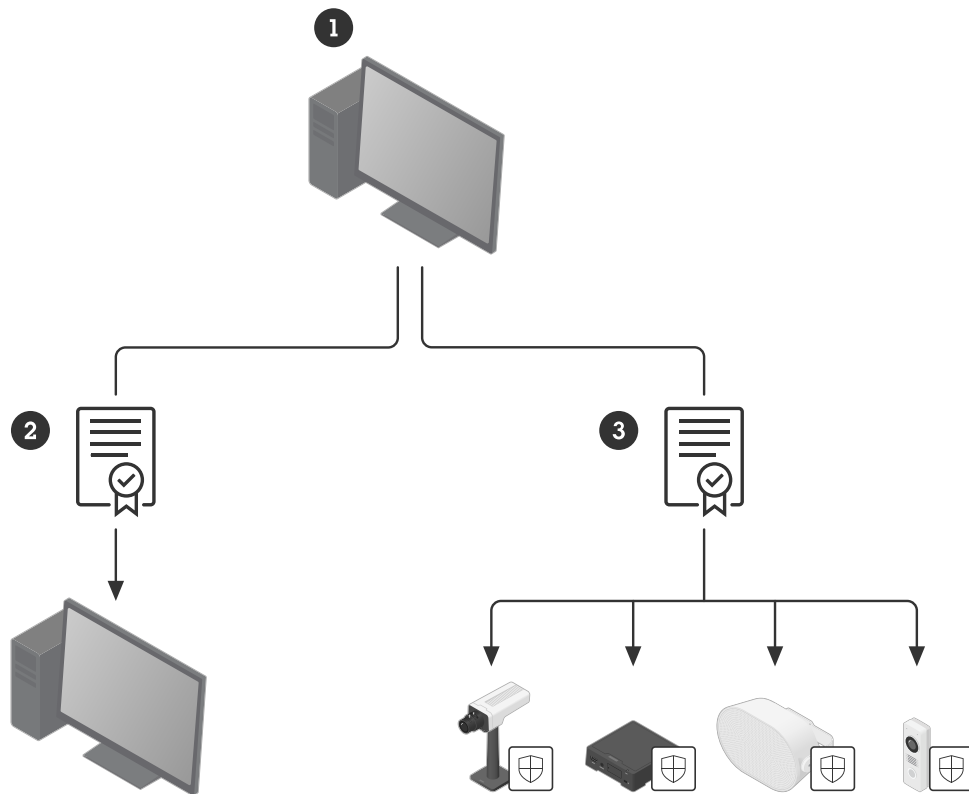
Utilizar AXIS Device Manager como CA privada es la solución más rentable. Después de generar un certificado de CA root, instale el certificado de AXIS Device Manager en el almacén de certificados del servidor VMS. Si otros clientes están accediendo a cámaras directamente (para el mantenimiento o la localización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

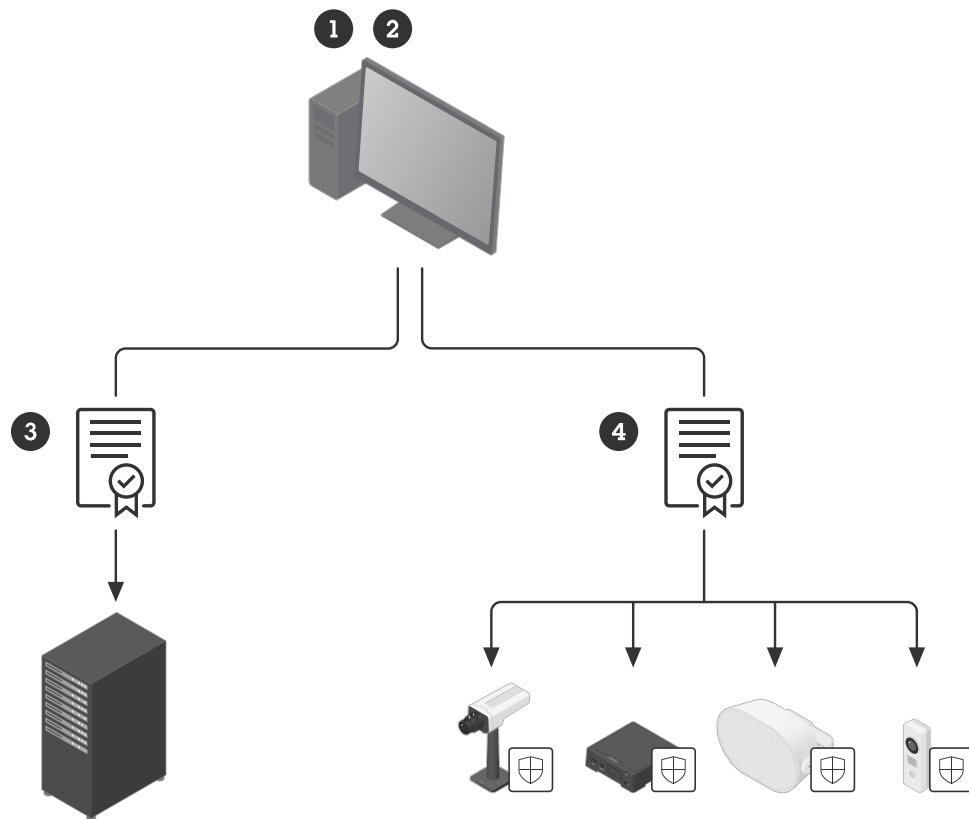
Para recibir ayuda con la configuración de un servidor FreeRADIUS, visite la sección de *documentos técnicos* de AXIS Device Manager.



La gestión de certificados HTTPS implica: 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.



Uso de una CA privada. La gestión de certificados IEEE 802.1X implica: 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.



Uso de AXIS Device Manager como CA. Para gestionar certificados IEEE 802.1X: 1) generar el certificado de CA root en AXIS Device Manager; 2) importar el certificado de CA de autenticación en AXIS Device Manager; 3) instalar el certificado de CA en el servidor Radius; 4) cargar los certificados de autenticación y de cliente de CA en los dispositivos.

Conclusión

La gestión y el control de la seguridad son partes importantes a la hora de implementar una estrategia de ciberseguridad eficaz. Cada proceso es continuo y exige claridad y adoptar las medidas adecuadas para mitigar toda amenaza potencial que pueda afectar a su red IP. AXIS Device Manager constituye una herramienta dirigida a administrar 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.

T10231485_es

2025-09 (M4.2)

© 2025 Axis Communications AB