



# AXIS S3016 Recorder

**Manual del usuario**

## Sobre su dispositivo

AXIS S3016 Recorder es un grabador de vídeo en red con conmutador PoE integrado y discos duros de vigilancia. También incluye un puerto USB 3.0 para exportar fácilmente las secuencias de vídeo. La grabadora viene en tres modelos: 8 TB, 16 TB y 32 TB.

## Cómo funciona

### Acceda a su dispositivo

#### Localice el dispositivo en la red

Para localizar dispositivos de Axis en la red y asignarles direcciones IP en Windows®, utilice AXIS IP Utility o AXIS Device Manager Extend. Ambas aplicaciones son gratuitas y pueden descargarse desde [axis.com/support](http://axis.com/support).

Para obtener más información acerca de cómo encontrar y asignar direcciones IP, vaya a *How to assign an IP address and access your device* (*Cómo asignar una dirección IP y acceder al dispositivo*).

#### Compatibilidad con navegadores

Puede utilizar el dispositivo con los siguientes navegadores:

	Chrome™	Edge™	Firefox®	Safari®
Windows®	✓	✓	*	*
macOS®	✓	✓	*	*
Linux®	✓	✓	*	*
Otros sistemas operativos	*	*	*	*

✓: Recomendado

\*: Asistencia técnica con limitaciones

### Abrir la interfaz web del dispositivo

1. Abra un navegador y escriba la dirección IP o el nombre de host del dispositivo Axis. Si no conoce la dirección IP, use AXIS IP Utility o AXIS Device Manager Extend para localizar el dispositivo en la red.
2. Escriba el nombre de usuario y la contraseña. Si accede al dispositivo por primera vez, debe crear una cuenta de administrador. Vea .

Para obtener descripciones de todos los controles y opciones de la interfaz web del dispositivo, consulte .

### Crear una cuenta de administrador

La primera vez que inicie sesión en el dispositivo, debe crear una cuenta de administrador.

1. Introduzca un nombre de usuario.
2. Introduzca una contraseña. Vea .
3. Vuelva a escribir la contraseña.
4. Aceptar el acuerdo de licencia.
5. Haga clic en **Add account (agregar cuenta)**.

#### Importante

El dispositivo no tiene una cuenta predeterminada. Si pierde la contraseña de la cuenta de administrador, debe restablecer el dispositivo. Vea .

## Contraseñas seguras

### Importante

Utilice HTTPS (habilitado por defecto) para configurar su contraseña u otros ajustes confidenciales a través de la red. HTTPS ofrece conexiones de red seguras y cifradas para proteger datos confidenciales, como las contraseñas.

La contraseña del dispositivo es la principal protección para sus datos y servicios. Los dispositivos de Axis no imponen una política de contraseñas ya que pueden utilizarse en distintos tipos de instalaciones.

Para proteger sus datos le recomendamos encarecidamente que:

- Utilice una contraseña con al menos 8 caracteres, creada preferiblemente con un generador de contraseñas.
- No exponga la contraseña.
- Cambie la contraseña a intervalos periódicos y al menos una vez al año.

## Asegúrese de que nadie ha manipulado el software del dispositivo

Para asegurarse de que el dispositivo tiene el AXIS OS original o para volver a controlar el dispositivo tras un incidente de seguridad:

1. Restablezca la configuración predeterminada de fábrica. Vea .  
Después de un restablecimiento, el inicio seguro garantiza el estado del dispositivo.
2. Configure e instale el dispositivo.

## Información general de la interfaz web

Este vídeo le ofrece información general de la interfaz web del dispositivo.



*Interfaz web del dispositivo Axis*

## Cómo funciona

### Nota

El acceso a Internet es necesario durante la configuración del sistema.

- 1.
- 2.
- 3.
- 4.
- 5.

Cuando la instalación haya finalizado:

- Todos los dispositivos Axis del sistema tienen el SO de AXIS más reciente.
- Todos los dispositivos tienen una contraseña.
- La grabación con los ajustes predeterminados está activa.
- Puede utilizar el acceso remoto.

## Registrar una cuenta MyAxis

1. Registre una cuenta My Axis en [axis.com/my-axis/login](http://axis.com/my-axis/login).
2. Elija uno de los métodos de autenticación multifactor (MFA): **Authenticator App (TOTP)** o **Email (Correo electrónico)** y siga las instrucciones en pantalla. MFA es un sistema de seguridad que añade una etapa adicional de verificación para garantizar la identidad del usuario.

## Instalación del hardware

1. Instale el hardware de la cámara.
2. Conecte el grabador a la red a través del puerto LAN.
3. Conecte las cámaras al switch PoE integrado del grabador o a un switch PoE externo.
4. Conecte el ordenador a la misma red que el grabador.
5. Conecte la grabadora a la fuente de alimentación.

### Importante

En primer lugar, debe conectar el cable de alimentación al grabador y, a continuación, conectar el cable de alimentación a la toma de corriente.

6. Espere unos minutos hasta que el grabador y las cámaras se inicien antes de continuar.

### ⚠ PRECAUCIÓN

El grabador debe estar en un lugar bien ventilado y tener espacio suficiente alrededor para que no se caliente demasiado.

## Instale AXIS Camera Station Edge

1. Vaya a [axis.com/products/axis-camera-station-edge](http://axis.com/products/axis-camera-station-edge) y haga clic en **Download (Descargar)**.
2. Abra el archivo de configuración y siga las instrucciones del asistente de configuración.
3. Inicie sesión en su *cuenta MyAxis*.

## Crear una instalación

1. Iniciar AXIS Camera Station Edge.
2. Inicie sesión en su *cuenta MyAxis*.
3. Haga clic en **Create new site (Crear nueva instalación)** y asigne un nombre a la instalación.
4. Haga clic en **Next (Siguiente)**.
5. Seleccione los dispositivos que deseé añadir a la instalación.
6. Haga clic en **Next (Siguiente)**.
7. Seleccionar almacenamiento.
8. Haga clic en **Next (Siguiente)**.
9. Haga clic en **Install (Instalar)** y espere a que AXIS Camera Station Edge configure los dispositivos.  
La configuración puede tardar unos minutos.

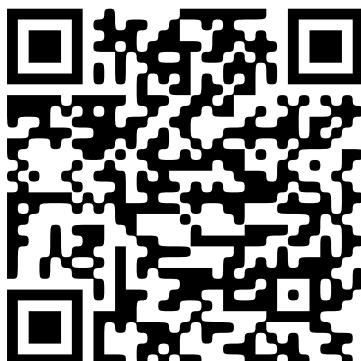
Cuando la instalación haya finalizado:

- Todos los dispositivos Axis del sistema tienen el SO de AXIS más reciente.
- Todos los dispositivos tienen una contraseña.
- La grabación con los ajustes predeterminados está activa.
- Puede utilizar el acceso remoto.

## Instalar la aplicación móvil

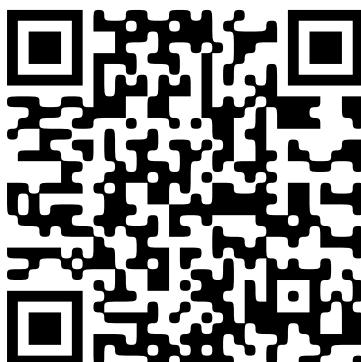
### Para Android

Haga clic en *Descargar* o escanee el siguiente código QR®.



### Para iOS

Haga clic en *Descargar* o escanee el siguiente código QR.



Abra la aplicación móvil AXIS Camera Station Edge e inicie sesión con sus credenciales de Axis.

Si no dispone de una cuenta MyAxis, se puede dirigir a [axis.com/my-axis](http://axis.com/my-axis) para registrar una nueva.

QR Code es una marca comercial registrada de DensoWave Incorporated en Japón y otros países.

## Empezar a utilizar AXIS Camera Station Pro

### Agregue su grabadora

#### Nota

AXIS Camera Station elimina grabaciones de cualquier sistema anterior cuando agrega el grabador a un nuevo sistema.

1. Vaya a **Configuración > Dispositivos > Agregar dispositivos**.
2. Seleccione el grabador en la lista y haga clic en **Add (Agregar)**. Si el grabador no aparece en la lista, utilice **Manual search (Búsqueda manual)** para encontrarlo manualmente.
3. Utilice la configuración predeterminada y haga clic en **Next (Siguiente)**.
4. Configure la contraseña para el cifrado de almacenamiento. Haga clic en **Next (Siguiente)**. Necesita esta contraseña para acceder al disco duro del grabador fuera del AXIS Camera Station o cuando se restablece la configuración predeterminada de fábrica desde la interfaz web del dispositivo.
5. Vaya a **Configuration > Devices > Other devices (Configuración > Dispositivos > Otros dispositivos)** y compruebe que se ha agregado el grabador.

6. Vaya a Configuration > Storage > Management (Configuración > Almacenamiento > Administración) y compruebe que se ha agregado el grabador a la lista de almacenamiento.

## Agregar dispositivos y seleccionar el grabador como almacenamiento de grabaciones

1. Vaya a Configuración > Dispositivos > Agregar dispositivos.
2. Seleccione sus dispositivos en la lista y haga clic en Add (Aregar). Si sus dispositivos no aparecen en la lista, utilice Manual search (Búsqueda manual) para buscarlos manualmente.
3. Utilice la configuración predeterminada y haga clic en Next (Siguiente).
4. Seleccione manualmente el grabador en la lista desplegable Recording storage (Almacenamiento de grabaciones) y haga clic en Install (Instalar).

### Nota

La grabadora no se seleccionará como almacenamiento de grabaciones si selecciona Automatic (Automático).

5. Vaya a Configuración > Almacenamiento > Selección. Haga clic en sus dispositivos y compruebe que el almacenamiento de grabaciones es el grabador.

## Configurar grabaciones

1. Vaya a Configuration > Storage > Selection (Configuración > Almacenamiento > Selección) y seleccione su dispositivo.
2. Configure Retention time (Tiempo de conservación).
  - Seleccione tiempo de conservación Unlimited (Ilimitado) para mantener las grabaciones hasta que se llene el almacenamiento.
  - Seleccione Limited (Limitado) y establezca el número máximo de días que guardar las grabaciones.
3. Haga clic en Aplicar.

### Nota

Fallback recording (Grabación remota) está activada de forma predeterminada para guardar las grabaciones en el grabador cuando se pierda la conexión entre AXIS Camera Station y el grabador. See *Grabación remota*.

## Configure su dispositivo

### Asignar energía

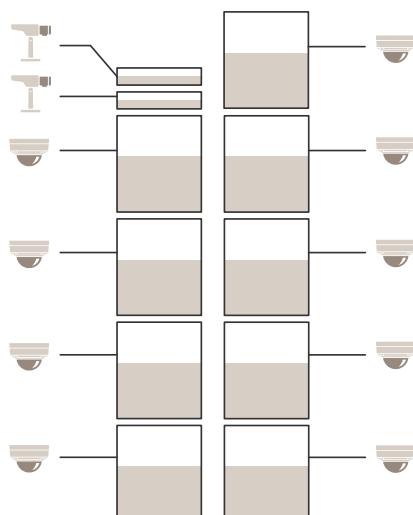
La grabadora reserva una cierta cantidad de potencia para cada puerto. La potencia total reservada no puede superar el presupuesto total de potencia. Un puerto no se encenderá si la grabadora intenta reservar más potencia de la disponible. Esto garantiza que todos los dispositivos conectados reciben alimentación.

#### Ejemplo:

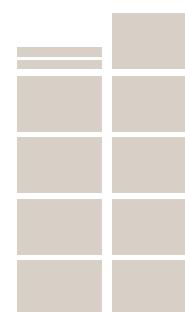
En este ejemplo:

- AXIS S3016 Recorder tiene una potencia total de 305 W.
- Dispositivo PoE clase 3. Solicita 15,5 W de potencia, pero en realidad consume 7,5 W de potencia.
- Dispositivo PoE clase 4. Solicita 30 W de potencia, pero en realidad consume 15 W de potencia.
- Potencia reservada.
- Consumo de potencia real.

Energía reservada



Consumo de potencia real



- Cada puerto reserva la cantidad de alimentación según la clase de PoE del dispositivo.
- La grabadora puede alimentar 9 dispositivos PoE clase 4 y 2 dispositivos PoE clase 3.
- La alimentación total reservada es  $(9 \times 30) + (2 \times 15.5) = 301$  W.
- La potencia real consumida es de  $(9 \times 15) + (2 \times 7.5) = 150$  W.

### Cambiar el nivel RAID

#### PRECAUCIÓN

Cambiar el nivel RAID reformatea el sistema de archivos y elimina todos los datos de sus discos.

1. En la interfaz web del dispositivo, vaya a **Sistema > Almacenamiento**.
2. Bajo **Herramientas**, seleccionar **Cambiar nivel RAID** y haga clic **usar herramienta**.
3. Seleccione un nivel RAID y haga clic en **Siguiente**.
4. Seleccionar **cifrar el disco** y escriba su contraseña. Haga clic en **Next (Siguiente)**.
5. Haga clic en **Yes (Sí)**.

- El mensaje de estado aparece en la esquina superior derecha. Espere hasta que finalice la operación y RAID configured se muestra antes de cerrar la página.

## Sustituir un disco duro

### Nota

Para evitar descargas electrostáticas, se recomienda utilizar una alfombrilla y una correa antiestáticas mientras se trabaja con los componentes interiores del sistema.

- Afloje los tornillos a la izquierda y a la derecha del bisel y retire el bisel.
- Localice el disco duro roto indicado por un LED rojo.  
Todos los LED están rojos en caso de una falla del RAID. Para identificar el disco duro roto, vaya a la interfaz web del dispositivo y vaya a **Sistema > Almacenamiento > Estado del disco duro**.
- Afloje el tornillo del sled del disco duro (T10).
- Saque el sled del disco duro del compartimiento para disco duro.
- Afloje los cuatro tornillos del disco duro (T8).
- Saque el disco duro del trineo del disco duro.
- Inserte un nuevo disco duro en el sled del disco duro.
- Apriete los cuatro tornillos del disco duro.
- Inserte y empuje el sled del disco duro hasta el fondo en el compartimiento para disco duro.
- Apriete el tornillo del trineo del disco duro. Espere hasta que el LED cambie a verde.
- Coloque el bisel y apriete los tornillos a la izquierda y a la derecha del bisel.

## Crear un nuevo RAID

### **⚠ PRECAUCIÓN**

Solo crea un nuevo RAID en caso de que falle el RAID. La creación de un nuevo RAID elimina todos los datos de sus discos duros.

- Reemplace los discos duros rotos. Vea .
- Configure el RAID. Consulte .
- Configure grabaciones en su sistema de gestión de vídeo. Vea y .

## Restablecer un grabador de manera forzada

### Importante

Desplace la grabadora con cuidado cuando esté encendida. Los movimientos repentinos o los golpes pueden dañar la unidad de disco duro.

### Nota

- Un restablecimiento forzado restablecerá todos los ajustes, incluida la dirección IP.
  - Un reinicio completo no eliminará las grabaciones.
- Apague el grabador:  
Pulse el botón de alimentación de la parte delantera del grabador durante 4-5 segundos hasta que oiga un sonido.
  - Espere a que el grabador se apague y gírelo para acceder al botón de control.
  - Mantenga pulsado el botón de control. Pulse y suelte el botón de encendido para encender el grabador. Suelte el botón de control tras 15-30 segundos cuando el indicador LED parpadee en ámbar.
  - Vuelva a colocar la grabadora en su sitio con cuidado.
  - El proceso finalizará cuando el indicador LED de estado se ilumine en color verde. El producto se ha restablecido a la configuración predeterminada de fábrica. Si no hay ningún servidor DHCP disponible en la red, la dirección IP del dispositivo adoptará de forma predeterminada una de las siguientes:

- **Dispositivos con AXIS OS 12.0 y posterior:** Obtenido de la subred de dirección de enlace local (169.254.0.0/16)
  - **Dispositivos con AXIS OS 11.11 y anterior:** 192.168.0.90/24
6. Si el disco duro está cifrado, debe montarse manualmente después de reiniciar el grabador:
- 6.1. Vaya a la interfaz web del dispositivo.
  - 6.2. Vaya a **System (Sistema) > Storage (Almacenamiento)** y haga clic en **Mount (Montar)**.
  - 6.3. Introduzca la contraseña de cifrado utilizada al cifrar el disco duro.

## Interfaz web

Para acceder a la interfaz web, escriba la dirección IP del dispositivo en un navegador web.

### Nota

La compatibilidad con las características y ajustes descrita en esta sección varía entre dispositivos. Este icono  indica que la función o ajuste solo está disponible en algunos dispositivos.

 Mostrar u ocultar el menú principal.

 Acceda a las notas de la versión.

 Acceder a la ayuda del producto.

 Cambiar el idioma.

 Definir un tema claro o un tema oscuro.

 El menú de usuario contiene:

- Información sobre el usuario que ha iniciado sesión.
-  **Cambiar cuenta:** Cierre sesión en la cuenta actual e inicie sesión en una cuenta nueva.
-  **Cerrar sesión:** Cierre sesión en la cuenta actual.
- ⋮
- El menú contextual contiene:
  - **Analytics data (Datos de analíticas):** Puede compartir datos no personales del navegador.
  - **Feedback (Comentarios):** Puede enviarnos comentarios para ayudarnos a mejorar su experiencia de usuario.
  - **Legal (Aviso legal):** Lea información sobre cookies y licencias.
  - **About (Acerca de):** Puede consultar la información del dispositivo, como la versión de AXIS OS y el número de serie.

## Estado

### Información sobre el dispositivo

Muestra información del dispositivo, como la versión del AXIS OS y el número de serie.

**Actualización de AXIS OS:** Actualizar el software en el dispositivo. Le lleva a la página de mantenimiento donde puede realizar la actualización.

### Estado de sincronización de hora

Muestra la información de sincronización de NTP, como si el dispositivo está sincronizado con un servidor NTP y el tiempo que queda hasta la siguiente sincronización.

**Configuración de NTP:** Ver y actualizar los ajustes de NTP. Le lleva a la página **Time and location (Hora y localización)**, donde puede cambiar los ajustes de NTP.

## Seguridad

Muestra qué tipo de acceso al dispositivo está activo y qué protocolos de cifrado están en uso y si se permite el uso de aplicaciones sin firmar. Las recomendaciones para los ajustes se basan en la guía de seguridad del sistema operativo AXIS.

**Hardening guide (Guía de seguridad):** Enlace a la *AXIS OS Hardening guide (guía de refuerzo del sistema operativo AXIS)*, donde encontrará más información sobre ciberseguridad en dispositivos Axis y prácticas recomendadas.

## Puertos de red

Muestra el estado de los puertos de red e información de energía, incluida la energía asignada y el consumo total de PoE.

**Configuración de los puertos de red:** Haga clic para ir a la página Puertos de red, donde podrá cambiar la configuración.

## Almacenamiento

Muestra el estado del almacenamiento e información, incluido el espacio libre y la temperatura del disco.

**Ajustes de almacenamiento:** Haz clic para ir a la página Almacenamiento a bordo, donde podrás cambiar la configuración.

## Clientes conectados

Muestra el número de conexiones y clientes conectados.

**View details (Ver detalles):** Consulte y actualice la lista de clientes conectados. La lista muestra la dirección IP, el protocolo, el puerto, el estado y PID/proceso de cada conexión.

## Grabaciones en curso

Muestra las grabaciones en curso y el espacio de almacenamiento designado.

**Grabaciones:** Consulte las grabaciones en curso y filtradas y la fuente. Para obtener más información, consulte



Muestra el espacio de almacenamiento en el que se guarda la grabación.

## Grabaciones

-  Reproduzca la grabación.
- Deje de reproducir la grabación.
-  Muestre u oculte información y opciones sobre la grabación.

**Definir intervalo de exportación:** si solo desea exportar parte de la grabación, introduzca un intervalo horario.

**Encrypt (Cifrar):** Seleccione esta opción para definir una contraseña para las grabaciones exportadas. No será posible abrir el archivo exportado sin la contraseña.

-  Haga clic para eliminar una grabación.

**Exportar:** Exporte toda o una parte de la grabación.

-  Haga clic para filtrar las grabaciones.

**Desde:** Mostrar grabaciones realizadas después de un determinado punto del tiempo.

**Hasta:** Mostrar grabaciones hasta un momento determinado.

**Fuente 

**Evento:** Mostrar grabaciones en función de eventos.**

**Almacenamiento:** Mostrar grabaciones según el tipo de almacenamiento.

## Aplicaciones



**Add app (Agregar aplicación):** Instale una nueva aplicación.

**Find more apps (Buscar más aplicaciones):** Encuentre más aplicaciones para instalar. Se le mostrará una página de información general de las aplicaciones de Axis.



**Permitir aplicaciones sin firma** : Active esta opción para permitir la instalación de aplicaciones sin firma.



Consulte las actualizaciones de seguridad en las aplicaciones AXIS OS y ACAP.

### Nota

El rendimiento del dispositivo puede empeorar si ejecuta varias aplicaciones al mismo tiempo.

Utilice el switch situado junto al nombre de la aplicación para iniciar o detener la aplicación.

**Abrir:** Acceda a los ajustes de la aplicación. que varían en función de la aplicación. Algunas aplicaciones no tienen ajustes.



El menú contextual puede contener una o más de las siguientes opciones:

- **Licencia de código abierto:** Consulte la información sobre las licencias de código abierto utilizadas en la aplicación.
- **App log (Registro de aplicación):** Consulte un registro de los eventos de la aplicación. El registro resulta útil si se debe contactar con el servicio de soporte técnico.
- **Activate license with a key (Activar licencia con una clave):** Si la aplicación requiere una licencia, tiene que activarla. Use esta opción si su dispositivo no tiene acceso a Internet. Si no dispone de clave de licencia, vaya a [axis.com/products/analytics](http://axis.com/products/analytics). Se necesita un código de licencia y el número de serie del producto de Axis para generar una clave de licencia.
- **Activate license automatically (Activar licencia automáticamente):** Si la aplicación requiere una licencia, tiene que activarla. Use esta opción si su dispositivo tiene acceso a Internet. Se necesita un código para activar la licencia.
- **Deactivate the license (Desactivar la licencia):** Desactive la licencia para sustituirla por otra, por ejemplo, al cambiar de licencia de prueba a licencia completa. Si desactiva la licencia, también la elimina del dispositivo.
- **Settings (Ajustes):** Configure los parámetros.
- **Eliminar:** Permite eliminar la aplicación del dispositivo permanentemente. Si primero no desactiva la licencia, permanecerá activa.

## Sistema

### Hora y ubicación

#### Fecha y hora

El formato de fecha y hora depende de la configuración de idioma del navegador web.

### Nota

Es aconsejable sincronizar la fecha y hora del dispositivo con un servidor NTP.

**Synchronization (Sincronización):** Seleccione una opción para la sincronización de la fecha y la hora del dispositivo.

- **Automatic date and time (Fecha y hora automáticas) (PTP):** sincronice utilizando el protocolo de tiempo de precisión.
- **Fecha y hora automáticas (servidores NTS KE manuales):** Sincronice con los servidores de establecimiento de claves NTP seguros conectados al servidor DHCP.
  - **Servidores NTS KE manuales:** Introduzca la dirección IP de un servidor NTP o de dos. Si usa dos servidores NTP, el dispositivo sincroniza y adapta la fecha y hora en función de la información de los dos.
  - **Trusted NTS KE CA certificates (Certificados CA NTS KE de confianza):** Seleccione los certificados CA de confianza que se emplearán para la sincronización horaria NTS KE segura o no seleccione ninguno.
  - **Tiempo máximo de encuesta NTP:** Seleccione la cantidad máxima de tiempo que debe esperar el dispositivo antes de que sondee el servidor NTP para obtener una hora actualizada.
  - **Tiempo mínimo de encuesta NTP:** Seleccione la cantidad mínima de tiempo que debe esperar el dispositivo antes de que sondee el servidor NTP para obtener una hora actualizada.
- **Fecha y hora automáticas (los servidores NTP utilizan DHCP):** Se sincroniza con los servidores NTP conectados al servidor DHCP.
  - **Servidores NTP alternativos:** Introduzca la dirección IP de un servidor alternativo o de dos.
  - **Tiempo máximo de encuesta NTP:** Seleccione la cantidad máxima de tiempo que debe esperar el dispositivo antes de que sondee el servidor NTP para obtener una hora actualizada.
  - **Tiempo mínimo de encuesta NTP:** Seleccione la cantidad mínima de tiempo que debe esperar el dispositivo antes de que sondee el servidor NTP para obtener una hora actualizada.
- **Fecha y hora automáticas (servidores NTP manuales):** Se sincroniza con los servidores NTP que seleccione.
  - **Servidores NTP manuales:** Introduzca la dirección IP de un servidor NTP o de dos. Si usa dos servidores NTP, el dispositivo sincroniza y adapta la fecha y hora en función de la información de los dos.
  - **Tiempo máximo de encuesta NTP:** Seleccione la cantidad máxima de tiempo que debe esperar el dispositivo antes de que sondee el servidor NTP para obtener una hora actualizada.
  - **Tiempo mínimo de encuesta NTP:** Seleccione la cantidad mínima de tiempo que debe esperar el dispositivo antes de que sondee el servidor NTP para obtener una hora actualizada.
- **Custom date and time (Personalizar fecha y hora):** Establezca manualmente la fecha y hora. Haga clic en **Get from system (Obtener del sistema)** para obtener una vez la configuración de fecha y hora desde su ordenador o dispositivo móvil.

**Time zone (Zona horaria):** Seleccione la zona horaria que desee utilizar. La hora se ajustará automáticamente para el horario de verano y el estándar.

- **DHCP:** Adopta la zona horaria del servidor DHCP. El dispositivo debe estar conectado a un servidor DHCP para poder seleccionar esta opción.
- **Manual:** Seleccione una zona horaria de la lista desplegable.

#### Nota

El sistema utiliza los ajustes de fecha y hora en todas las grabaciones, registros y ajustes del sistema.

## Red

### IPv4

**Asignar IPv4 automáticamente:** Seleccione IPv4 IP automática (DHCP) para permitir que la red asigne automáticamente su dirección IP, máscara de subred y router, sin configuración manual. Recomendamos utilizar la asignación automática de IP (DHCP) para la mayoría de las redes.

**IP address (Dirección IP):** Introduzca una dirección IP única para el dispositivo. Las direcciones IP estáticas se pueden asignar de manera aleatoria dentro de redes aisladas, siempre que cada dirección asignada sea única. Para evitar conflictos, le recomendamos ponerse en contacto con el administrador de la red antes de asignar una dirección IP estática.

**Subnet mask (Máscara de subred):** Introduzca la máscara de subred para definir qué direcciones se encuentran dentro de la red de área local. Cualquier dirección fuera de la red de área local pasa por el router.

**Router:** Introduzca la dirección IP del router predeterminado (puerta de enlace) utilizada para conectar dispositivos conectados a distintas redes y segmentos de red.

**Volver a la dirección IP estática si DHCP no está disponible:** Seleccione si desea agregar una dirección IP estática para utilizarla como alternativa si DHCP no está disponible y no puede asignar una dirección IP automáticamente.

#### Nota

Si DHCP no está disponible y el dispositivo utiliza una reserva de dirección estática, la dirección estática se configura con un ámbito limitado.

## IPv6

**Assign IPv6 automatically (Asignar IPv6 automáticamente):** Seleccione esta opción para activar IPv6 y permitir que el router de red asigne automáticamente una dirección IP al dispositivo.

## Nombre de host

**Asignar nombre de host automáticamente:** Seleccione esta opción para que el router de red asigne automáticamente un nombre de host al dispositivo.

**Hostname (Nombre de host):** Introduzca el nombre de host manualmente para usarlo como una forma alternativa de acceder al dispositivo. El informe del servidor y el registro del sistema utilizan el nombre de host. Los caracteres permitidos son A-Z, a-z, 0-9 y -.

**Active las actualizaciones de DNS dinámicas:** Permite que el dispositivo actualice automáticamente los registros de su servidor de nombres de dominio cada vez que cambie la dirección IP del mismo.

**Register DNS name (Registrar nombre de DNS):** Introduzca un nombre de dominio único que apunte a la dirección IP de su dispositivo. Los caracteres permitidos son A-Z, a-z, 0-9 y -.

**TTL:** El tiempo de vida (Time to Live, TTL) establece cuánto tiempo permanece válido un registro DNS antes de que sea necesario actualizarlo.

## Servidores DNS

**Asignar DNS automáticamente:** Seleccione esta opción para permitir que el servidor DHCP asigne dominios de búsqueda y direcciones de servidor DNS al dispositivo automáticamente. Recomendamos DNS automática (DHCP) para la mayoría de las redes.

**Search domains (Dominios de búsqueda):** Si utiliza un nombre de host que no esté completamente cualificado, haga clic en **Add search domain (Aregar dominio de búsqueda)** y escriba un dominio en el que se buscará el nombre de host que usa el dispositivo.

**DNS servers (Servidores DNS):** Haga clic en **Agregar servidor DNS** e introduzca la dirección IP del servidor DNS. Este servidor proporciona la traducción de nombres de host a las direcciones IP de su red.

**Nota**

Si DHCP está deshabilitado, las funciones que dependen de la configuración automática de la red, como el nombre de host, los servidores DNS, NTP y otras, podrían dejar de funcionar.

**Protocolos de detección de red**

**Bonjour®:** Active esta opción para permitir la detección automática en la red.

**Nombre de Bonjour:** Introduzca un nombre descriptivo; será el que se muestre en la red. El nombre predeterminado es el nombre del dispositivo seguido de la dirección MAC.

**UPnP®:** Active esta opción para permitir la detección automática en la red.

**Nombre de UPnP:** Introduzca un nombre descriptivo; será el que se muestre en la red. El nombre predeterminado es el nombre del dispositivo seguido de la dirección MAC.

**WS-Discovery:** Active esta opción para permitir la detección automática en la red.

**LLDP y CDP:** Active esta opción para permitir la detección automática en la red. Si se desactiva LLDP y CDP puede afectar a la negociación de alimentación PoE. Para solucionar cualquier problema con la negociación de alimentación PoE, configure el switch PoE solo para la negociación de alimentación PoE del hardware.

**Puertos de red**

**Power and ethernet (Alimentación e Ethernet):** Seleccione esta opción para activar la red para el puerto del switch.

**Power only (Solo alimentación):** Seleccione esta opción para desactivar la red para el puerto del switch. El puerto sigue proporcionando alimentación a través de Ethernet.

**Proxies globales**

**Http proxy (Proxy http):** Especifique un host proxy global o una dirección IP según el formato permitido.

**Https proxy (Proxy https):** Especifique un host proxy global o una dirección IP según el formato permitido.

Formatos permitidos para proxies http y https:

- `http(s)://host:puerto`
- `http(s)://usuario@host:puerto`
- `http(s)://user:pass@host:puerto`

**Nota**

Reinicie el dispositivo para aplicar los ajustes globales del proxy.

**No proxy (Sin proxy):** Utilice **No proxy (Sin proxy)** para evitar los proxies globales. Introduzca una de las opciones de la lista, o introduzca varias separadas por una coma:

- Dejar vacío
- Especifique una dirección IP
- Especifique una dirección IP en formato CIDR
- Especifique un nombre de dominio, por ejemplo: `www.<nombre de dominio>.com`
- Especifique todos los subdominios de un dominio concreto, por ejemplo `.<nombre de dominio>.com`

**Conexión a la nube con un clic**

La conexión One-Click Cloud (O3C), junto con un servicio O3C, ofrece acceso seguro y sencillo a Internet para acceder al vídeo en directo o grabado desde cualquier ubicación. Para obtener más información, consulte [axis.com/end-to-end-solutions/hosted-services](http://axis.com/end-to-end-solutions/hosted-services).

**Allow O3C (Permitir O3C):**

- **Un clic:** esta es la opción predeterminada. Presione el botón de control del dispositivo para conectarse a O3C. Según el modelo del dispositivo, mantenga pulsado o pulse y suelte el botón hasta que el LED de estado parpadee. Registre el dispositivo en el servicio O3C en un plazo de 24 horas para activar la opción **Siempre** y mantenerse conectado. Si no lo registra, el dispositivo se desconectará de O3C.
- **Siempre:** El dispositivo intenta conectarse continuamente a un servicio O3C a través de Internet. Una vez registrado el dispositivo, permanece conectado. Utilice esta opción si el botón de control está fuera de su alcance.
- **No:** desconecta el servicio O3C.

**Proxy settings (Configuración proxy):** Si es necesario, escriba los ajustes del proxy para conectarse al servidor proxy.

**Host:** Introduzca la dirección del servidor proxy.

**Puerto:** Introduzca el número de puerto utilizado para acceder.

**Inicio de sesión y Contraseña:** En caso necesario, escriba un nombre de usuario y la contraseña del servidor proxy.

**Authentication method (Método de autenticación):**

- **Básico:** Este método es el esquema de autenticación más compatible con HTTP. Es menos seguro que el método **Digest** porque envía el nombre de usuario y la contraseña sin cifrar al servidor.
- **Digest:** Este método de autenticación es más seguro porque siempre transfiere la contraseña cifrada a través de la red.
- **Automático:** Esta opción permite que el dispositivo seleccione el método de autenticación automáticamente en función de los métodos admitidos. Da prioridad al método **Digest** por delante del **Básico**.

**Owner authentication key (OAK) (Clave de autenticación de propietario [OAK]):** Haga clic en **Get key (Obtener clave)** para obtener la clave de autenticación del propietario. Esto solo es posible si el dispositivo está conectado a Internet sin un cortafuegos o proxy.

## SNMP

El protocolo de administración de red simple (SNMP) permite gestionar dispositivos de red de manera remota.

**SNMP:** Seleccione la versión de SNMP a usar.

- **v1 and v2c (v1 y v2c):**
  - **Read community (Comunidad de lectura):** Introduzca el nombre de la comunidad que tiene acceso de solo lectura a todos los objetos SNMP compatibles. El valor predeterminado es público.
  - **Write community (Comunidad de escritura):** Escriba el nombre de la comunidad que tiene acceso de lectura o escritura a todos los objetos SNMP compatibles (excepto los objetos de solo lectura). El valor predeterminado es escritura.
  - **Activate traps (Activar traps):** Active esta opción para activar el informe de trap. El dispositivo utiliza traps para enviar mensajes al sistema de gestión sobre eventos importantes o cambios de estado. En la interfaz web puede configurar traps para SNMP v1 y v2c. Las traps se desactivan automáticamente si cambia a SNMP v3 o desactiva SNMP. Si utiliza SNMP v3, puede configurar las traps a través de la aplicación de gestión de SNMP v3.
  - **Trap address (Dirección trap):** introduzca la dirección IP o el nombre de host del servidor de gestión.
  - **Trap community (Comunidad de trap):** Introduzca la comunidad que se utilizará cuando el dispositivo envía un mensaje trap al sistema de gestión.
  - **Traps:**
    - **Cold start (Arranque en frío):** Envía un mensaje trap cuando se inicia el dispositivo.
    - **Link up (Enlace hacia arriba):** Envía un mensaje trap cuando un enlace cambia de abajo a arriba.
    - **Link down (Enlace abajo):** Envía un mensaje trap cuando un enlace cambia de arriba a abajo.
    - **Authentication failed (Error de autenticación):** Envía un mensaje trap cuando se produce un error de intento de autenticación.

#### Nota

Todas las traps Axis Video MIB se habilitan cuando se activan las traps SNMP v1 y v2c. Para obtener más información, consulte *AXIS OS Portal > SNMP*.

- **v3:** SNMP v3 es una versión más segura que ofrece cifrado y contraseñas seguras. Para utilizar SNMP v3, recomendamos activar HTTPS, ya que la contraseña se envía a través de HTTPS. También evita que partes no autorizadas accedan a traps SNMP v1 y v2c sin cifrar. Si utiliza SNMP v3, puede configurar las traps a través de la aplicación de gestión de SNMP v3.
  - **Privacy (Privacidad):** Seleccione el cifrado que desea usar para proteger sus datos SNMP.
  - **Password for the account "initial" (contraseña para la cuenta "Inicial"):** Introduzca la contraseña de SNMP para la cuenta denominada "Initial". Aunque la contraseña se puede enviar sin activar HTTPS, no lo recomendamos. La contraseña de SNMP v3 solo puede establecerse una vez, y preferiblemente solo cuando esté activado HTTPS. Una vez establecida la contraseña, dejará de mostrarse el campo de contraseña. Para volver a establecer la contraseña, debe restablecer el dispositivo a su configuración predeterminada de fábrica.

## Seguridad

### Certificados

Los certificados se utilizan para autenticar los dispositivos de una red. Un dispositivo admite dos tipos de certificados:

- **Client/server certificates (Certificados de cliente/servidor)**

Un certificado de cliente/servidor valida la identidad del dispositivo de Axis y puede firmarlo el propio dispositivo o emitirlo una autoridad de certificación (CA). Un certificado firmado por el propio producto ofrece protección limitada y se puede utilizar antes de que se obtenga un certificado emitido por una autoridad de certificación.

- **Certificados CA**

Puede utilizar un certificado de la autoridad de certificación (AC) para autenticar un certificado entre iguales, por ejemplo, para validar la identidad de un servidor de autenticación cuando el dispositivo se conecta a una red protegida por IEEE 802.1X. El dispositivo incluye varios certificados de autoridad de certificación preinstalados.

Se admiten estos formatos:

- Formatos de certificado: .PEM, .CER y .PFX
- Formatos de clave privada: PKCS#1 y PKCS#12

**Importante**

Si restablece el dispositivo a los valores predeterminados de fábrica, se eliminarán todos los certificados. Los certificados CA preinstalados se vuelven a instalar.



**Agregar certificado:** Haga clic aquí para añadir un certificado. Se abre una guía paso a paso.

- **Más** : Mostrar más campos que rellenar o seleccionar.
- **Almacenamiento de claves seguro:** Seleccione esta opción para usar Trusted Execution Environment (SoC TEE), Secure element (Elemento seguro) o Trusted Platform Module 2.0 para almacenar la clave privada de forma segura. Para obtener más información sobre el almacén de claves seguro que desea seleccionar, vaya a [help.axis.com/axis-os#cryptographic-support](http://help.axis.com/axis-os#cryptographic-support).
- **Tipo de clave:** Seleccione la opción predeterminada o un algoritmo de cifrado diferente en la lista desplegable para proteger el certificado.



El menú contextual contiene:

- **Certificate information (Información del certificado):** Muestra las propiedades de un certificado instalado.
- **Delete certificate (Eliminar certificado):** Se elimina el certificado.
- **Create certificate signing request (Crear solicitud de firma de certificado):** Se crea una solicitud de firma de certificado que se envía a una autoridad de registro para solicitar un certificado de identidad digital.

**Almacenamiento de claves seguro**

- **Trusted Execution Environment (SoC TEE):** seleccione esta opción para utilizar SoC TEE para el almacenamiento seguro de claves.
- **Elemento seguro (CC EAL6+, FIPS 140-3 Level 3)** : Seleccione para utilizar un elemento seguro para un almacén de claves seguro.
- **Trusted Platform Module 2.0 (CC EAL4+, FIPS 140-2 nivel 2)** : Seleccione para usar TPM 2.0 para el almacén de claves seguro.

## Política criptográfica

La política criptográfica define cómo se utiliza el cifrado para proteger los datos.

**Activa:** Seleccione la política criptográfica que se aplicará al dispositivo:

- **Predeterminado – OpenSSL:** Seguridad y rendimiento equilibrados para uso general.
- **FIPS – Política para el cumplimiento de FIPS 140-2:** cifrado conforme con FIPS 140-2 para sectores regulados.

**Control y cifrado de acceso a la red**

## IEEE 802.1x

IEEE 802.1x es un estándar IEEE para el control de admisión de red basada en puertos que proporciona una autenticación segura de los dispositivos de red conectados e inalámbricos. IEEE 802.1x se basa en el protocolo de autenticación extensible, EAP.

Para acceder a una red protegida por IEEE 802.1x, los dispositivos de red deben autenticarse ellos mismos. Un servidor de autenticación lleva a cabo la autenticación, normalmente un servidor RADIUS (por ejemplo, FreeRADIUS y Microsoft Internet Authentication Server).

## IEEE 802.1AE MACsec

IEEE 802.1AE MACsec es un estándar IEEE para la seguridad del control de acceso a medios (MAC) que define la confidencialidad e integridad de los datos sin conexión para protocolos independientes de acceso a medios.

### Certificados

Si se configura sin un certificado de la autoridad de certificación, la validación de certificados del servidor se deshabilita y el dispositivo intentará autenticarse a sí mismo independientemente de la red a la que esté conectado.

Si se usa un certificado, en la implementación de Axis, el dispositivo y el servidor de autenticación se autentican ellos mismos con certificados digitales utilizando EAP-TLS (protocolo de autenticación extensible - seguridad de la capa de transporte).

Para permitir que el dispositivo acceda a una red protegida mediante certificados, debe instalar un certificado de cliente firmado en el dispositivo.

**Authentication method (Método de autenticación):** Seleccione un tipo de EAP utilizado para la autenticación.

**Client certificate (Certificado del cliente):** Seleccione un certificado de cliente para usar IEEE 802.1x. El servidor de autenticación utiliza el certificado para validar la identidad del cliente.

**CA Certificates (Certificados de la autoridad de certificación):** Seleccione certificados CA para validar la identidad del servidor de autenticación. Si no se selecciona ningún certificado, el dispositivo intentará autenticarse a sí mismo, independientemente de la red a la que esté conectado.

**EAP identity (Identidad EAP):** Introduzca la identidad del usuario asociada con el certificado de cliente.

**EAPOL version (Versión EAPOL):** Seleccione la versión EAPOL que se utiliza en el switch de red.

**Use IEEE 802.1x (Utilizar IEEE 802.1x):** Seleccione para utilizar el protocolo IEEE 802.1x.

Estos ajustes solo están disponibles si utiliza **IEEE 802.1x PEAP-MSCHAPv2** como método de autenticación:

- **Contraseña:** Escriba la contraseña para la identidad de su usuario.
- **Versión de Peap:** Seleccione la versión de Peap que se utiliza en el switch de red.
- **Label (Etiqueta):** Seleccione 1 para usar el cifrado EAP del cliente; seleccione 2 para usar el cifrado PEAP del cliente. Seleccione la etiqueta que utiliza el switch de red cuando utilice la versión 1 de Peap.

Estos ajustes solo están disponibles si utiliza **IEEE 802.1ae MACsec (CAK estática/clave precompartida)** como método de autenticación:

- **Nombre de clave de asociación de conectividad de acuerdo de claves:** Introduzca el nombre de la asociación de conectividad (CKN). Debe tener de 2 a 64 caracteres hexadecimales (divisibles por 2). La CKN debe configurarse manualmente en la asociación de conectividad y debe coincidir con los dos extremos del enlace para activar inicialmente MACsec.
- **Clave de asociación de conectividad de acuerdo de claves:** Introduzca la clave de la asociación de conectividad (CAK). Debe tener una longitud de 32 o 64 caracteres hexadecimales. La CAK debe configurarse manualmente en la asociación de conectividad y debe coincidir con los dos extremos del enlace para activar inicialmente MACsec.

**Firewall**

**Firewall:** Encender para activar el firewall.

**Política predeterminada:** Seleccione cómo desea que el firewall gestione las solicitudes de conexión no cubiertas por las reglas.

- **ACCEPT (Aceptar):** Permite todas las conexiones al dispositivo. Esta opción está establecida de forma predeterminada.
- **DROP (Soltar):** Bloquea todas las conexiones al dispositivo.

Para realizar excepciones a la política predeterminada, puede crear reglas que permitan o bloquen las conexiones al dispositivo desde direcciones, protocolos y puertos específicos.

+ **New rule (Nueva regla):** Haga clic para crear una regla.

**Rule type (Tipo de regla):**

- **FILTER (Filtro):** Seleccione esta opción para permitir o bloquear conexiones de dispositivos que coincidan con los criterios definidos en la regla.
  - **Policy (Directiva):** Seleccione Accept (Aceptar) o Drop (Soltar) para la regla del firewall.
  - **IP range (Intervalo IP):** Seleccione para especificar el rango de direcciones que deseé permitir o bloquear. Utilice IPv4/IPv6 en Start (Inicio) y End (Fin).
  - **IP address (Dirección IP):** Introduzca la dirección que deseé permitir o bloquear. Utilice el formato IPv4/IPv6 o CIDR.
  - **Protocol (Protocolo):** Seleccione el protocolo de red (TCP, UDP o Ambos) que deseé permitir o bloquear. Si selecciona un protocolo, también deberá especificar un puerto.
  - **MAC:** Introduzca la dirección MAC del dispositivo que deseé permitir o bloquear.
  - **Port range (Intervalo de puertos):** Seleccione esta opción para especificar el rango de puertos que deseé permitir o bloquear. Añádalos en Start (Inicio) y End (Fin).
  - **Puerto:** Introduzca el número de puerto que deseé permitir o bloquear. Los números de puerto deben situarse entre 1 y 65535.
  - **Traffic type (Tipo de tráfico):** Seleccione el tipo de tráfico que deseé permitir o bloquear.
    - **UNICAST:** Tráfico de un único emisor a un único destinatario.
    - **BROADCAST (Transmisión):** Tráfico de un único emisor a todos los dispositivos de la red.
    - **MULTICAST:** Tráfico de uno o varios emisores a uno o varios destinatarios.
- **LIMIT (Límites):** Seleccione esta opción para aceptar conexiones de dispositivos que coincidan con los criterios definidos en la regla, pero aplique límites para reducir el tráfico excesivo.
  - **IP range (Intervalo IP):** Seleccione para especificar el rango de direcciones que deseé permitir o bloquear. Utilice IPv4/IPv6 en Start (Inicio) y End (Fin).
  - **IP address (Dirección IP):** Introduzca la dirección que deseé permitir o bloquear. Utilice el formato IPv4/IPv6 o CIDR.
  - **Protocol (Protocolo):** Seleccione el protocolo de red (TCP, UDP o Ambos) que deseé permitir o bloquear. Si selecciona un protocolo, también deberá especificar un puerto.
  - **MAC:** Introduzca la dirección MAC del dispositivo que deseé permitir o bloquear.
  - **Port range (Intervalo de puertos):** Seleccione esta opción para especificar el rango de puertos que deseé permitir o bloquear. Añádalos en Start (Inicio) y End (Fin).
  - **Puerto:** Introduzca el número de puerto que deseé permitir o bloquear. Los números de puerto deben situarse entre 1 y 65535.
  - **Unit (Unidad):** Seleccione el tipo de conexiones que deseé permitir o bloquear.
  - **Period (Periodo):** Seleccione el periodo de tiempo relacionado con **Amount (Cantidad)**.
  - **Amount (Cantidad):** Determine el número máximo de veces que se permite que un dispositivo se conecte dentro del **Period (Periodo)**. La cantidad máxima es 65535.

- **Burst (Ráfaga):** Introduzca el número de conexiones que pueden superar la **Amount (Cantidad)** establecida una vez durante el **Period (Periodo)** establecido. Una vez alcanzado el número, solo se permitirá la cantidad determinada durante el periodo establecido.
- **Traffic type (Tipo de tráfico):** Seleccione el tipo de tráfico que desee permitir o bloquear.
  - **UNICAST:** Tráfico de un único emisor a un único destinatario.
  - **BROADCAST (Transmisión):** Tráfico de un único emisor a todos los dispositivos de la red.
  - **MULTICAST:** Tráfico de uno o varios emisores a uno o varios destinatarios.

**Test rules (Prueba de reglas):** Haga clic para probar las reglas que haya definido.

- **Test time in seconds (Tiempo de prueba en segundos):** Defina un límite de tiempo para probar las reglas.
- **Roll back (Restaurar):** Haga clic para restablecer el firewall a su estado anterior, antes de haber probado las reglas.
- **Apply rules (Aplicar reglas):** Haga clic para activar las reglas sin realizar pruebas. No le recomendamos esta opción.

## Certificado de AXIS OS con firma personalizada

Para instalar en el dispositivo software de prueba u otro software personalizado de Axis, necesita un certificado de AXIS OS firmado personalizado. El certificado verifica que el software ha sido aprobado por el propietario del dispositivo y por Axis. El software solo puede ejecutarse en un dispositivo concreto identificado por su número de serie único y el ID de su chip. Solo Axis puede crear los certificados de AXIS OS firmados personalizados, ya que Axis posee la clave para firmarlos.

**Install (Instalar):** Haga clic para instalar el certificado. El certificado se debe instalar antes que el software.

- ⋮ El menú contextual contiene:
  - **Delete certificate (Eliminar certificado):** Se elimina el certificado.

## Cuentas

### Cuentas



**Add account (Añadir cuenta):** Haga clic para agregar una nueva cuenta. Puede agregar hasta 100 cuentas.

**Cuenta:** introduzca un nombre de cuenta único.

**Nueva contraseña:** introduzca una contraseña para la cuenta. Las contraseñas deben tener entre 1 y 64 caracteres. La contraseña solo admite caracteres ASCII imprimibles (códigos de 32 a 126), por ejemplo, letras, números, signos de puntuación y algunos símbolos.

**Repetir contraseña:** Introduzca la misma contraseña de nuevo.

**Privilegios:**

- **Administrador:** Tiene acceso completo a todos los ajustes. Los administradores también pueden agregar, actualizar y eliminar otras cuentas.
  - **Operator (Operador):** Tiene acceso a todos los ajustes excepto:
    - Todos los ajustes del sistema.
  - **Viewer (Visualizador):** Puede:
    - Ver y tomar instantáneas de una transmisión de vídeo.
    - Ver y exportar grabaciones.
    - Movimiento horizontal, vertical y zoom; con acceso a la cuenta de PTZ.
- ⋮ El menú contextual contiene:

**Actualizar cuenta:** Editar las propiedades de la cuenta.

**Eliminar cuenta:** Elimine la cuenta. No puede eliminar la cuenta de root.

### Cuentas SSH



**Add SSH account (Agregar cuenta SSH):** Haga clic para agregar una nueva cuenta SSH.

- **Habilitar SSH:** Active el uso del servicio SSH.

**Cuenta:** introduzca un nombre de cuenta único.

**Nueva contraseña:** introduzca una contraseña para la cuenta. Las contraseñas deben tener entre 1 y 64 caracteres. La contraseña solo admite caracteres ASCII imprimibles (códigos de 32 a 126), por ejemplo, letras, números, signos de puntuación y algunos símbolos.

**Repetir contraseña:** Introduzca la misma contraseña de nuevo.

**Comentario:** Introduzca un comentario (opcional).



⋮ El menú contextual contiene:

**Actualizar cuenta SSH:** Editar las propiedades de la cuenta.

**Eliminar cuenta SSH:** Elimine la cuenta. No puede eliminar la cuenta de root.

### Host virtual



Add virtual host (Aregar host virtual): Haga clic para agregar un nuevo host virtual.

**Habilitada:** Seleccione esta opción para usar este host virtual.

**Server name (Nombre del servidor):** Introduzca el nombre del servidor. Utilice solo los números 0-9, las letras A-Z y el guión (-).

**Puerto:** Introduzca el puerto al que está conectado el servidor.

**Tipo:** Seleccione el tipo de autenticación que desea usar. Seleccione entre Basic, Digest y Open ID.



El menú contextual contiene:

- **Update (Actualizar):** Actualice el host virtual.
- **Eliminar:** Elimine el host virtual.

**Disabled (Deshabilitado):** El servidor está deshabilitado.

## Configuración de concesión de credenciales de cliente

**Admin claim (Reclamación de administrador):** Introduzca un valor para la función de administrador.

**Verification URL (URL de verificación):** Introduzca el enlace web para la autentificación de punto de acceso de API.

**Operator claim (Reclamación de operador):** Introduzca un valor para la función de operador.

**Require claim (Requerir solicitud):** Introduzca los datos que deberían estar en el token.

**Viewer claim (Reclamación de visor):** Introduzca el valor de la función de visor.

**Save (Guardar):** Haga clic para guardar los valores.

## Eventos

### Reglas

Una regla define las condiciones que desencadena el producto para realizar una acción. La lista muestra todas las reglas actualmente configuradas en el producto.

#### Nota

Puede crear hasta 256 reglas de acción.



Agregar una regla: Cree una regla.

**Name (Nombre):** Introduzca un nombre para la regla.

**Esperar entre acciones:** Introduzca el tiempo mínimo (hh:mm:ss) que debe pasar entre las activaciones de regla. Resulta útil si la regla se activa, por ejemplo, en condiciones del modo diurno/nocturno, para evitar que pequeños cambios de luz durante el amanecer y el atardecer activen la regla varias veces.

**Condition (Condición):** Seleccione una condición de la lista. Una condición se debe cumplir para que el dispositivo realice una acción. Si se definen varias condiciones, todas ellas deberán cumplirse para que se active la acción. Para obtener información sobre condiciones específicas, consulte *Introducción a las reglas para eventos*.

**Utilizar esta condición como activador:** Seleccione esta primera función de condición solo como activador inicial. Una vez que se activa la regla, permanecerá activa mientras se cumplen todas las demás condiciones, independientemente del estado de la primera condición. Si no selecciona esta opción, la regla estará activa siempre que se cumplan el resto de condiciones.

**Invert this condition (Invertir esta condición):** Seleccione si desea que la condición sea la opuesta a su selección.



Agregar una condición: Haga clic para agregar una condición adicional.

**Action (Acción):** Seleccione una acción de la lista e introduzca la información necesaria. Para obtener información sobre acciones específicas, consulte *Introducción a las reglas para eventos*.

## Destinatarios

Puede configurar el dispositivo para notificar a los destinatarios acerca de los eventos o enviar archivos.

### Nota

Si configura su dispositivo para utilizar FTP o SFTP, no cambie ni elimine el número de secuencia único que se añade a los nombres de archivo. Si lo hace, solo se podrá enviar una imagen por evento.

La lista muestra todos los destinatarios configurados actualmente en el producto, además de información sobre su configuración.

### Nota

Puede crear hasta 20 destinatarios.



**Agregar un destinatario:** Haga clic para agregar un destinatario.

**Name (Nombre):** Introduzca un nombre para el destinatario.

**Tipo:** Seleccione de la lista:

- **FTP**

- **Host:** Introduzca la dirección IP o el nombre de host del servidor. Si introduce un nombre de host, asegúrese de que se ha especificado un servidor DNS en **Sistema > Red > IPv4 e IPv6**.
- **Puerto:** Introduzca el número de puerto utilizado por el servidor FTP. El valor por defecto es 21.
- **Carpeta:** Introduzca la ruta al directorio en el que desea almacenar los archivos. Si el directorio aún no existe en el servidor FTP, obtendrá un mensaje de error al realizar la carga de archivos.
- **Nombre de usuario:** Introduzca el nombre de usuario para el inicio de sesión.
- **Contraseña:** Introduzca la contraseña para el inicio de sesión.
- **Utilice nombre de archivo temporal:** Seleccione esta opción para cargar archivos con nombres de archivo temporales generados automáticamente. Los archivos se renombran por los nombres deseados cuando se completa la carga. Si la carga se ha anulado o interrumpido, no obtendrá archivos dañados. Sin embargo, es probable que se sigan recibiendo los archivos temporales. De este modo, sabrá que todos los archivos que tienen el nombre deseado son correctos.
- **Usar FTP pasivo:** En circunstancias normales, el producto simplemente solicita al servidor FTP de destino que abra la conexión de datos. El dispositivo inicia activamente el control FTP y las conexiones de datos al servidor de destino. Normalmente esto es necesario si existe un cortafuegos entre el dispositivo y el servidor FTP de destino.

- **HTTP**

- **URL:** Introduzca la dirección de red al servidor HTTP y la secuencia de comandos que gestionará la solicitud. Por ejemplo, `http://192.168.254.10/cgi-bin/notify.cgi`.
- **Nombre de usuario:** Introduzca el nombre de usuario para el inicio de sesión.
- **Contraseña:** Introduzca la contraseña para el inicio de sesión.
- **Proxy:** Active e introduzca la información requerida si es necesario pasar un servidor proxy para conectarse al servidor HTTP.

- **HTTPS**

- **URL:** Introduzca la dirección de red al servidor HTTPS y la secuencia de comandos que gestionará la solicitud. Por ejemplo, `https://192.168.254.10/cgi-bin/notify.cgi`.
- **Validar certificado del servidor:** Seleccione para validar el certificado creado por el servidor HTTPS.
- **Nombre de usuario:** Introduzca el nombre de usuario para el inicio de sesión.
- **Contraseña:** Introduzca la contraseña para el inicio de sesión.
- **Proxy:** Active e introduzca la información requerida si es necesario pasar un servidor proxy para conectarse al servidor HTTPS.

- **Almacenamiento de red**

Puede agregar almacenamiento de red, como almacenamiento en red tipo NAS (almacenamiento en red) y usarlo como destinatario para almacenar archivos. Los archivos se almacenan en formato Matroska (MKV).

- **Host:** Introduzca la dirección IP o el nombre de host del almacenamiento de red.
- **Recurso compartido:** Escriba el nombre del recurso compartido en el host.

- **Carpeta:** Introduzca la ruta al directorio en el que desea almacenar los archivos.
  - **Nombre de usuario:** Introduzca el nombre de usuario para el inicio de sesión.
  - **Contraseña:** Introduzca la contraseña para el inicio de sesión.
- **SFTP** 
    - **Host:** Introduzca la dirección IP o el nombre de host del servidor. Si introduce un nombre de host, asegúrese de que se ha especificado un servidor DNS en **Sistema > Red > IPv4 e IPv6**.
    - **Puerto:** Introduzca el número de puerto utilizado por el servidor SFTP. El predeterminado es 22.
    - **Carpeta:** Introduzca la ruta al directorio en el que desea almacenar los archivos. Si el directorio aún no existe en el servidor SFTP, obtendrá un mensaje de error al realizar la carga de archivos.
    - **Nombre de usuario:** Introduzca el nombre de usuario para el inicio de sesión.
    - **Contraseña:** Introduzca la contraseña para el inicio de sesión.
    - **Tipo de clave pública del host SSH (MD5):** Introduzca la huella de la clave pública del host remoto (una cadena de 32 dígitos hexadecimales). El cliente de SFTP es compatible con servidores SFTP que emplean tipos de clave del host SSH-2 con RSA, DSA, ECDSA y ED25519. RSA es el método preferido durante la negociación, seguido de ECDSA, ED25519 y DSA. Asegúrese de introducir la clave de host MD5 correcta que utiliza el servidor SFTP. Si bien el dispositivo Axis admite claves hash MD5 y SHA-256, recomendamos usar SHA-256 debido a una seguridad más sólida que MD5. Para obtener más información sobre cómo configurar un servidor SFTP con un dispositivo Axis, vaya al *Portal de AXIS OS*.
    - **Tipo de clave pública del host SSH (SHA256):** Ingrese la huella digital de la clave pública del host remoto (una cadena codificada en Base64 de 43 dígitos). El cliente de SFTP es compatible con servidores SFTP que emplean tipos de clave del host SSH-2 con RSA, DSA, ECDSA y ED25519. RSA es el método preferido durante la negociación, seguido de ECDSA, ED25519 y DSA. Asegúrese de introducir la clave de host MD5 correcta que utiliza el servidor SFTP. Si bien el dispositivo Axis admite claves hash MD5 y SHA-256, recomendamos usar SHA-256 debido a una seguridad más sólida que MD5. Para obtener más información sobre cómo configurar un servidor SFTP con un dispositivo Axis, vaya al *Portal de AXIS OS*.
    - **Utilice nombre de archivo temporal:** Seleccione esta opción para cargar archivos con nombres de archivo temporales generados automáticamente. Los archivos se renombran por los nombres deseados cuando se completa la carga. Si la carga se ha anulado o interrumpido, no obtendrá archivos dañados. Sin embargo, es probable que se sigan recibiendo los archivos temporales. De este modo, sabrá que todos los archivos que tienen el nombre deseado son correctos.  - **SIP o VMS**  :
    - SIP:** Seleccione esta opción para realizar una llamada SIP.
    - VMS:** Seleccione esta opción para realizar una llamada de VMS.
    - **Desde cuenta SIP:** Seleccione de la lista.
    - **A dirección SIP:** Introduzca la dirección SIP.
    - **Prueba:** Haga clic para comprobar que los ajustes de la llamada funcionan.
  - **Correo electrónico**
    - **Enviar correo electrónico a:** Introduzca la dirección de correo electrónico a la que enviar correos electrónicos. Para especificar varias direcciones de correo electrónico, utilice comas para separarlas.
    - **Enviar correo desde:** Introduzca la dirección de correo electrónico del servidor emisor.
    - **Nombre de usuario:** Introduzca el nombre de usuario del servidor de correo. Deje este campo vacío si el servidor de correo no necesita autenticación.

- **Contraseña:** Introduzca la contraseña del servidor de correo. Deje este campo vacío si el servidor de correo no necesita autenticación.
- **Servidor de correo electrónico (SMTP):** Introduzca el nombre del servidor SMTP, por ejemplo, smtp.gmail.com, smtp.mail.yahoo.com.
- **Puerto:** Introduzca el número de puerto para el servidor SMTP, usando valores entre 0 y 65535. El valor por defecto es 587.
- **Cifrado:** Para usar el cifrado, seleccione SSL o TLS.
- **Validar certificado del servidor:** Si utiliza el cifrado, seleccione esta opción para validar la identidad del dispositivo. El certificado puede firmarlo el propio producto o emitirlo una autoridad de certificación (CA).
- **Autentificación POP:** Active para introducir el nombre del servidor POP, por ejemplo, pop.gmail.com.

#### Nota

Algunos proveedores de correo electrónico tienen filtros de seguridad que evitan que los usuarios reciban o vean grandes cantidades de adjuntos, que reciban mensajes de correo electrónico programados, etc. Compruebe la política de seguridad del proveedor de correo electrónico para evitar que su cuenta de correo quede bloqueada o que no reciba correos electrónicos esperados.

- **TCP**
  - **Host:** Introduzca la dirección IP o el nombre de host del servidor. Si introduce un nombre de host, asegúrese de que se ha especificado un servidor DNS en **Sistema > Red > IPv4 e IPv6**.
  - **Puerto:** Introduzca el número de puerto utilizado para acceder al servidor.

**Comprobación:** Haga clic en probar la configuración.



El menú contextual contiene:

**Ver destinatario:** Haga clic para ver todos los detalles del destinatario.

**Copiar destinatario:** Haga clic para copiar un destinatario. Cuando copia, puede realizar cambios en el nuevo destinatario.

**Eliminar destinatario:** Haga clic para eliminar el destinatario de forma permanente.

## Horarios

Se pueden usar programaciones y pulsos como condiciones en las reglas. La lista muestra todas las programaciones y pulsos configurados actualmente en el producto, además de información sobre su configuración.



**Agregar programación:** Haga clic para crear una programación o pulso.

## Activadores manuales

Puede usar el activador manual para desencadenar manualmente una regla. El activador manual se puede utilizar, por ejemplo, para validar acciones durante la instalación y configuración de productos.

## Almacenamiento

### Almacenamiento integrado

**RAID**

- **Libre:** Cantidad total de espacio libre en el disco.
- **Estado:** Si el disco está montado o no.
- **Sistema de archivos:** El sistema de archivos que utiliza el disco.
- **Cifrado:** Si el disco está cifrado o no.
- **Temperatura:** La temperatura actual del hardware.
- **Prueba de estado general:** El resultado después de comprobar el estado del disco.
- **Nivel RAID:** El nivel RAID utilizado para el almacenamiento. Los niveles RAID admitidos son 0, 1, 5, 6, 10.
- **Estado de RAID** El estado RAID del almacenamiento. Los valores posibles son **En Línea, Degradado, Sincronizando y Error**. El proceso de sincronización puede tardar varias horas.

**Herramientas****Nota**

Cuando ejecute las siguientes herramientas, asegúrese de esperar hasta que finalice la operación antes de cerrar la página.

- **Check (Comprobar):** Compruebe si hay errores en el dispositivo de almacenamiento e intenta repararlo automáticamente.
- **Repair (Reparar):** Reparar el dispositivo de almacenamiento. Las grabaciones activas se detendrán durante la reparación. La reparación de un dispositivo de almacenamiento puede provocar la pérdida de datos.
- **Format (Formato):** Borre todas las grabaciones y formatee el dispositivo de almacenamiento. Elija un sistema de archivos.
- **Encrypt (Cifrar):** Cifre los datos que se almacenan. Se borrarán todos los archivos del dispositivo de almacenamiento.
- **Descifrar:** Descifre los datos almacenados. Se borrarán todos los archivos del dispositivo de almacenamiento.
- **Change password (Modificar contraseña):** Cambie la contraseña del cifrado del disco. Modificar la contraseña no altera las grabaciones en curso.
- **Cambiar nivel RAID** Borre todas las grabaciones y cambie el nivel RAID del almacenamiento.
- **Usar herramienta:** Haga clic para ejecutar la herramienta seleccionada.

**Estado del disco duro** Haga clic para ver el estado, la capacidad y el número de serie del disco duro.

**Write protect (Protección contra escritura):** Active la protección contra escritura para evitar que se sobrescriba el dispositivo de almacenamiento.

**Registros****Informes y registros**

## Informes

- **Ver informe del servidor del dispositivo:** Consulte información acerca del estado del producto en una ventana emergente. El registro de acceso se incluye automáticamente en el informe del servidor.
- **Download the device server report (Descargar informe del servidor del dispositivo):** Se crea un archivo .zip que contiene un archivo de texto con el informe del servidor completo en formato UTF-8 y una instantánea de la imagen de visualización en directo actual. Incluya siempre el archivo.zip del informe del servidor si necesita contactar con el servicio de asistencia.
- **Download the crash report (Descargar informe de fallos):** Descargar un archivo con la información detallada acerca del estado del servidor. El informe de fallos incluye información ya presente en el informe del servidor, además de información detallada acerca de la corrección de fallos. Este informe puede incluir información confidencial, como trazas de red. Puede tardar varios minutos en generarse.

## Registros

- **View the system log (Ver registro del sistema):** Haga clic para consultar información acerca de eventos del sistema como inicio de dispositivos, advertencias y mensajes críticos.
- **View the access log (Ver registro de acceso):** Haga clic para ver todos los intentos incorrectos de acceso al dispositivo, por ejemplo, si se utiliza una contraseña de inicio de sesión incorrecta.
- **View the audit log (Ver registro de auditoría):** Haga clic para mostrar información sobre las actividades del usuario y del sistema, por ejemplo, autenticaciones y configuraciones correctas o fallidas.

## Registro de sistema remoto

Syslog es un estándar de registro de mensajes. Permite que el software que genera los mensajes, el sistema que los almacena y el software que los notifica y analiza sean independientes. Cada mensaje se etiqueta con un código de instalación, que indica el tipo de software que genera el mensaje y tiene un nivel de gravedad.



**Server (Servidor):** Haga clic para agregar un nuevo servidor.

**Host:** introduzca el nombre de host o la dirección IP del servidor.

**Format (Formato):** Seleccione el formato de mensaje de syslog que quiera utilizar.

- Axis
- RFC 3164
- RFC 5424

**Protocol (Protocolo):** Seleccione el protocolo que desee utilizar:

- UDP (el puerto predeterminado es 514).
- TCP (el puerto predeterminado es 601).
- TLS (el puerto predeterminado es 6514).

**Puerto:** Modifique el número de puerto para usar otro puerto.

**Severity (Gravedad):** Seleccione los mensajes que se enviarán cuando se activen.

**Tipo:** Seleccione el tipo de registros que desea enviar.

**Test server setup (Probar configuración del servidor):** Envíe un mensaje de prueba a todos los servidores antes de guardar la configuración.

**CA certificate set (Conjunto de certificados de CA):** Consulte los ajustes actuales o añada un certificado.

## Mantenimiento

### Mantenimiento

**Restart (Reiniciar):** Reiniciar el dispositivo. No afectará a la configuración actual. Las aplicaciones en ejecución se reinician automáticamente.

**Restore (Restaurar):** Casi todos los ajustes vuelven a los valores predeterminados de fábrica. Después deberás reconfigurar el dispositivo y las aplicaciones, reinstalar las que no vinieran preinstaladas y volver a crear los eventos y preajustes.

#### Importante

Los únicos ajustes que se guardan después de una restauración son:

- Protocolo de arranque (DHCP o estático)
- Dirección IP estática
- Router predeterminado
- Máscara de subred
- Configuración 802.1X
- Configuración de O3C
- Dirección IP del servidor DNS

**Factory default (Predeterminado de fábrica):** Todos los ajustes vuelven a los valores predeterminados de fábrica. Después, es necesario restablecer la dirección IP para poder acceder al dispositivo.

#### Nota

Todo el software de los dispositivos AXIS está firmado digitalmente para garantizar que solo se instala software verificado. Esto aumenta todavía más el nivel mínimo general de ciberseguridad de los dispositivos de Axis. Para obtener más información, consulte el documento técnico "Axis Edge Vault" en [axis.com](http://axis.com).

**Actualización de AXIS OS:** Se actualiza a una nueva versión de AXIS OS. Las nuevas versiones pueden contener mejoras de funciones, correcciones de errores y características totalmente nuevas. Le recomendamos que utilice siempre la versión de AXIS OS más reciente. Para descargar la última versión, vaya a [axis.com/support](http://axis.com/support).

Al actualizar, puede elegir entre tres opciones:

- **Standard upgrade (Actualización estándar):** Se actualice a la nueva versión de AXIS OS.
- **Factory default (Predeterminado de fábrica):** Se actualiza y todos los ajustes vuelven a los valores predeterminados de fábrica. Si elige esta opción, no podrá volver a la versión de AXIS OS anterior después de la actualización.
- **Automatic rollback (Restauración automática):** Se actualiza y debe confirmar la actualización en el plazo establecido. Si no confirma la actualización, el dispositivo vuelve a la versión de AXIS OS anterior.

**Restaurar AXIS OS:** Se vuelve a la versión anterior de AXIS OS instalado.

## solucionar problemas

**Reset PTR (Restablecer PTR)**  : Restablezca el ajuste PTR si, por alguna razón, los ajustes de Pan (Movimiento horizontal), Tilt (Movimiento vertical) o Roll (Giro) no funcionan de la forma prevista. Los motores PTR se calibran siempre en una cámara nueva. Sin embargo, la calibración se puede perder, por ejemplo, si la cámara pierde la alimentación o si los motores se mueven a mano. Al restablecer PTR, la cámara se vuelve a calibrar y vuelve a su posición predeterminada de fábrica.

**Calibration (Calibración)**  : Haga clic en Calibrate (Calibrar) para recalibrar los motores de movimiento horizontal, movimiento vertical y giro a sus posiciones predeterminadas.

**Ping:** Para comprobar si el dispositivo puede llegar a una dirección específica, introduzca el nombre de host o la dirección IP del host al que desea hacer ping y haga clic en Start (Iniciar).

**Port check (Comprobación del puerto):** Para verificar la conectividad del dispositivo con una dirección IP y un puerto TCP/UDP específicos, introduzca el nombre de host o la dirección IP y el número de puerto que desea comprobar; después, haga clic en Start (Iniciar).

### Rastreo de red

#### Importante

Un archivo de rastreo de red puede contener información confidencial, como certificados o contraseñas.

Un archivo de rastreo de red puede ayudar a solucionar problemas mediante la grabación de la actividad en la red.

**Trace time (Tiempo de rastreo):** Seleccione la duración del rastreo en segundos o minutos y haga clic en Descargar.

## Descubrir más

### Ciberseguridad

Para obtener información específica sobre ciberseguridad, consulte la ficha técnica del producto en [axis.com](http://axis.com).

Para obtener información detallada sobre ciberseguridad en AXIS OS, lea la *Guía de endurecimiento de AXIS OS*.

### SO firmado

El sistema operativo firmado lo implementa el proveedor del software que firma la imagen de AXIS OS con una clave privada. Cuando la firma se une al sistema operativo, el dispositivo validará el software antes de instalarlo. Si el dispositivo detecta que la integridad del software está comprometida, se rechazará la actualización de AXIS OS.

### Arranque seguro

El arranque seguro es un proceso de arranque que consta de una cadena ininterrumpida de software validado criptográficamente, comenzando por la memoria inmutable (ROM de arranque). Al estar basado en el uso del sistema operativo firmado, el arranque seguro garantiza que un dispositivo pueda iniciarse solo con un software autorizado.

### Axis Edge Vault

Axis Edge Vault es una plataforma de ciberseguridad basada en hardware que protege el dispositivo Axis. Ofrece características que garantizan la identidad e integridad del dispositivo y protegen su información confidencial frente a accesos no autorizados. Tiene dos sólidos pilares: los módulos de computación criptográfica (elemento seguro y TPM) y la seguridad del SoC (TEE y arranque seguro), combinados con una amplia experiencia en la seguridad de los dispositivos en el extremo.

### Módulo TPM

El módulo de plataforma segura (TPM) es un componente que proporciona funciones de cifrado para proteger la información contra accesos no autorizados. Está siempre activado y sus ajustes no se pueden cambiar.

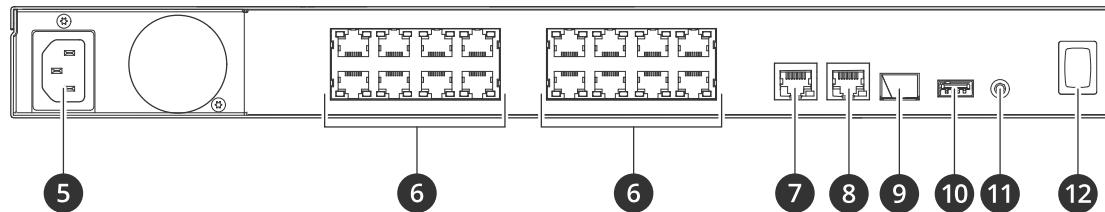
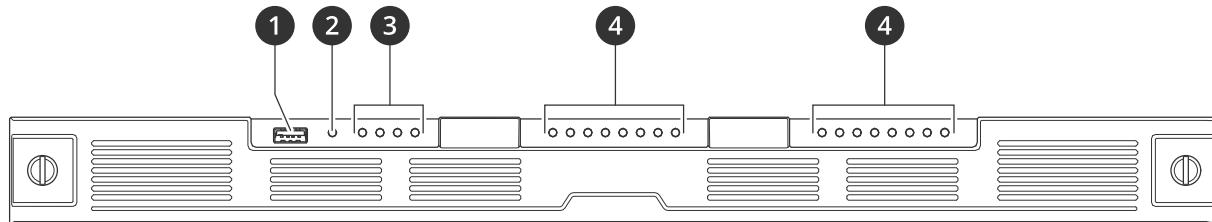
### ID de dispositivo de Axis

La posibilidad de verificar el origen del dispositivo es fundamental para poder confiar en su identidad. Durante la producción, se asigna a los dispositivos con Axis Edge Vault un certificado de ID de dispositivo de Axis único y conforme con el estándar IEEE 802.1AR en la propia fábrica. Es como una especie de pasaporte para demostrar el origen del dispositivo. El ID de dispositivo se guarda de forma segura y permanente en el almacén de claves seguro como certificado firmado por el certificado raíz de Axis. La infraestructura de TI del cliente puede utilizar el ID de dispositivo en la incorporación segura automatizada de dispositivos y en la identificación segura de dispositivos.

Para obtener más información sobre las características de ciberseguridad de los dispositivos Axis, vaya a [axis.com/learning/white-papers](http://axis.com/learning/white-papers) y busque ciberseguridad.

## Especificaciones

### Guía de productos



- 1 Puerto USB 3.0
- 2 LED de estado del producto
- 3 LED de estado de los discos duros
- 4 LED de estado PoE/rojo
- 5 Conector de alimentación
- 6 Puertos PoE
- 7 Puerto AUX RJ45
- 8 Puerto LAN RJ45
- 9 Puerto LAN SFP
- 10 Puerto USB 2.0
- 11 Botón de control
- 12 Botón de encendido

## Especificaciones

### LED frontales

LED	Color	Indicación
Estado del producto	Verde	El grabador está encendido y el estado es correcto.
	Ámbar	El grabador está arrancando o se está actualizando el software del dispositivo. Espere hasta que el LED cambie a verde.
	Rojo	Esto puede significar que se ha superado la capacidad de PoE. Si acabas de conectar un dispositivo a la grabadora, intenta quitarlo.

Estado del disco duro	Verde	La unidad está en línea.
	Parpadea en verde alternativamente.	El RAID se está sincronizando. Es posible grabar, pero aún no se ha logrado la redundancia.
	Ámbar	Esta unidad está en línea, pero otra unidad está averiada. Al RAID le falta redundancia.
	Rojo	La unidad está rota.
	todos son rojos	El RAID ha fallado. El sistema no está grabando.  Para identificar el disco duro roto en caso de una falla de RAID, vaya a la interfaz web del dispositivo y vaya a <b>Sistema &gt; Almacenamiento &gt; Estado del disco duro</b> .
	Apagado	Sin disco duro.
Estado de PoE	Verde	Se conecta un dispositivo.
	Ámbar	PoE está en uso pero no hay enlace de red.
	Rojo	El dispositivo conectado no puede iniciarse.  Se ha superado la capacidad de PoE.  Fallo PoE.
	Apagado	El puerto no está en uso o está deshabilitado.

**LED traseros**

LED	Color	Indicación
Puerto de red	Parpadea en verde	2.5 Gbit/s
	Parpadea en ámbar	1 Gbit/s
	Apagado	No hay red
Puerto PoE LED izquierdo	Verde	PoE está en uso.
	Rojo	Fallo PoE.  Se ha superado la capacidad de PoE.
	Apagado	El puerto no está en uso o está deshabilitado.
Puerto PoE LED derecho	Parpadea en verde	1 Gbit/s
	Parpadea en ámbar	100 Mbit/s

	Apagado	No hay red
--	---------	------------

## Botón de encendido

- Para apagar el grabador, pulse el botón de encendido hasta que el avisador acústico emita un sonido corto.
- Para silenciar al avisador acústico, presione brevemente el botón de encendido.

## Botón de control

El botón de control se utiliza para lo siguiente:

- Restablecer el producto a la configuración predeterminada de fábrica. Vea .
- Conectarse a un servicio de conexión a la nube (O3C) de un solo clic a través de Internet. Para conectarse, mantenga pulsado el botón durante 3 segundos hasta que el LED de estado parpadee en color verde.

## Localización de problemas

### Problemas técnicos, consejos y soluciones

Emitir	Solución
Mis grabaciones no están disponibles.	Vaya a .
No puedo conectarme a mis cámaras.	Vaya a .
Recibo la notificación de error: "No contact" (Sin contacto).	Vaya a .
Mis sitios no aparecen en la aplicación móvil.	Asegúrese de disponer de la última versión de la app móvil AXIS Camera Station Edge.

### Resolver problemas habituales

Antes de reiniciar, configure o reinicie sus dispositivos.

1. Compruebe que las cámaras y el grabador tienen alimentación eléctrica.
2. Compruebe que está conectado a Internet.
3. Compruebe que la red funciona.
4. Compruebe que las cámaras están conectadas a la misma red que el ordenador, salvo si las usa de forma remota.

Si todavía hay algo que no funciona:

5. Asegúrese de que sus cámaras, grabador y AXIS Camera Station Edge disponen de la última versión del software.  
Consulte .
6. Reinicie AXIS Camera Station Edge.
7. Reinicie las cámaras y el grabador.

Si todavía hay algo que no funciona:

8. Realice un restablecimiento forzado en las cámaras y el grabador para que vuelvan a tener todos los ajustes predeterminados de fábrica.  
Vea .
9. Vuelva a añadir las cámaras restablecidas a la instalación.

Si todavía hay algo que no funciona:

10. Actualice su tarjeta gráfica con los controladores más recientes.

Si todavía hay algo que no funciona:

11. Guarde un informe del sistema y póngase en contacto con el servicio técnico de Axis.  
Vea .

### Actualización de AXIS OS

Las nuevas actualizaciones de software del dispositivo ofrecen el conjunto de prestaciones, funciones y mejoras de seguridad más recientes y avanzadas.

1. Vaya a la interfaz web del dispositivo líder.
2. Vaya a Maintenance > AXIS OS upgrade (mantenimiento > actualización de AXIS OS) y haga clic en Upgrade (actualizar).
3. Siga las instrucciones de la pantalla.

## No puedo iniciar sesión en la interfaz web del producto

Si ha establecido una contraseña para el producto durante la configuración y, más adelante, agrega ese producto a una instalación, ya no podrá iniciar sesión en la interfaz web del producto con la contraseña establecida. El motivo es que AXIS Camera Station Edge cambia las contraseñas de todos los dispositivos de la instalación.

Para iniciar sesión en un dispositivo de la instalación, introduzca el nombre de usuario **root** y la contraseña de la instalación.

## Cómo borrar todas las grabaciones

1. En la interfaz web del dispositivo, vaya a **System (Sistema) > Storage (Almacenamiento)**.
2. Seleccione **Format (Formato)** y haga clic en **Use tool (Usar herramienta)**.

### Nota

Este procedimiento borra todas las grabaciones de la unidad de disco duro, pero la configuración del grabador y de la instalación no cambian.

## Guardar un informe del sistema



1. En AXIS Camera Station Edge, vaya a > **Save system report (Guardar informe del sistema)**.
2. En AXIS Camera Station Pro, vaya a > **Help (Ayuda) > System report (Informe del sistema)**.
3. Cuando registre un caso nuevo en el servicio de soporte de Axis, adjunte el informe del sistema.

## ¿Necesita más ayuda?

### Enlaces útiles

- *Manual de usuario de AXIS Camera Station Edge*
- *Manual de usuario de AXIS Camera Station Pro*

### Contactar con la asistencia técnica

Si necesita más ayuda, vaya a [axis.com/support](http://axis.com/support).



T10186767\_es

2025-12 (M9.2)

© 2022 – 2025 Axis Communications AB