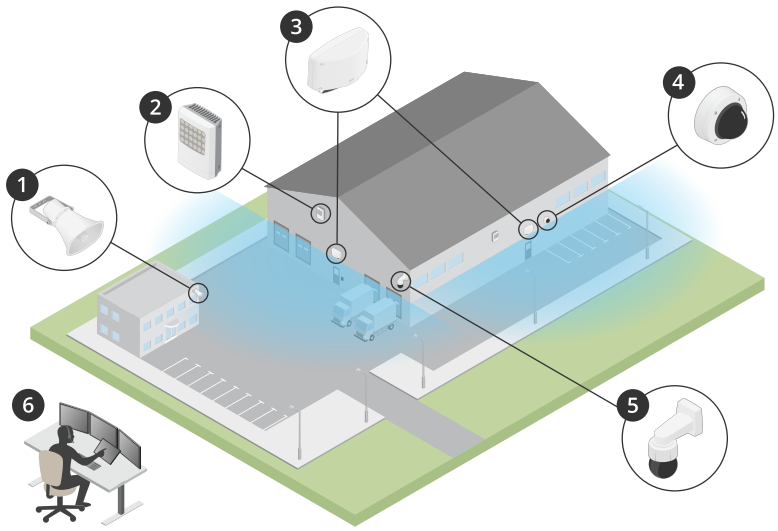
AXIS D2110-VE Security Radar

Manual del usuario

Índice

Presentación esquemática de la solución



1 *Altavoz exponencial C1310-E*
2 *Controlador de puerta*
3 *D2110–VE Security Radar*
4 *Cámara domo fija*
5 *Cámara PTZ*
6 *Centro de vigilancia*

Perfiles de radar

Nota

Para utilizar perfiles de radar, el dispositivo debe tener instalada la versión de firmware 10.11 o posterior. Visite para actualizar el firmware.

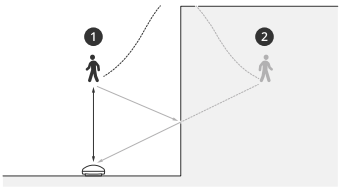
El manual del usuario puede ayudarle a utilizar el radar como le convenga. El AXIS D2110-VE Security Radar tiene dos perfiles:

- El **perfil de supervisión de área** se usa para detectar objetos grandes y pequeños en movimiento a velocidades de menos de 55 km/h.
- El **perfil de supervisión de carretera** se usa para detectar vehículos que se mueven a velocidades de hasta 105 km/h.

Toda la información de este manual que no corresponde al **perfil de supervisión de área** ni al **perfil de supervisión de carretera** es común a los dos perfiles y se puede consultar independientemente de cuál de los dos se use.

Dónde instalar el producto

- El radar se ha diseñado para supervisar áreas abiertas. Cualquier objeto sólido (como una pared, una valla, un árbol o un arbusto grande) en la zona de cobertura creará un punto ciego (sombra de radar) detrás de él.
- Instale el radar en un poste estable o en un punto en una pared donde no haya otros objetos o instalaciones. Los objetos situados a menos de 1 m a la izquierda y derecha del radar y que reflejan las ondas de radio afectan al rendimiento del radar.
- Los objetos metálicos dentro el campo de visión provocan reflejos que afectan a la capacidad del radar para realizar clasificaciones.



1 Detección real
2 Detección reflejada (seguimiento fantasma)

Para obtener información sobre cómo gestionar objetos reflectantes, consulte .

- Si quiere instalar más de dos radares en una zona de coexistencia, consulte .

Área de cobertura

El AXIS D2110–VE tiene una cobertura de área horizontal de 180°. El alcance de detección es de 5600 m^2para personas y de 11 300 m^2para vehículos.

Nota

La cobertura de área óptima se obtiene si el radar se monta a entre 3,5 y 4 m del altura. La altura de montaje influye en las dimensiones del ángulo muerto presente debajo del radar.

Perfil de supervisión de área

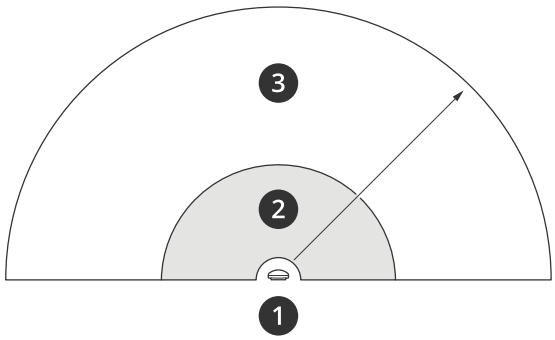
El **perfil de supervisión de área** está optimizado para objetos en movimiento de hasta 55 km/h. Permite determinar si un objeto es una persona, un vehículo o es desconocido. Se puede definir una regla que active una acción cuando se detecte un objeto en movimiento. Para realizar un seguimiento de los vehículos en movimiento a velocidades altas, utilice .

Instalar varios radares

Puede instalar varios radares para cubrir zonas como los alrededores de edificios o la zona exterior próxima a una valla.

Coexistencia

Si pone más de dos radares en una zona de coexistencia, las ondas de radio de los radares pueden provocar interferencias y afectar al rendimiento. El radio de una zona de coexistencia es de 350 m.



1 Radar
2 Área de detección
3 Zona de coexistencia

Nota

El rendimiento del radar en la zona de coexistencia también puede verse afectado por el entorno o la dirección del radar hacia vallas, edificios u otros radares cercanos.

Instalación de entre 2 y 3 radares en una zona de coexistencia

Si pone dos o tres radares en una zona de coexistencia, debe definir el número de radares próximos en la interfaz del dispositivo. De esta forma, mejora el rendimiento de los radares y se evitan interferencias.

1. Vaya a **Radar > Settings > Coexistence (Radar > Ajustes > Coexistencia)**.
2. Seleccione el número de radares próximos.

Consulte para ejemplos de instalaciones con varios radares.

Instalación de entre 4 y 6 radares en una zona de coexistencia

Nota

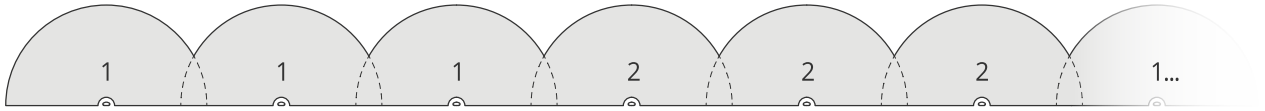
La versión 11.3 del firmware permite instalar hasta seis radares en una zona de coexistencia.

Si va a instalar entre cuatro y seis radares en una zona de coexistencia, primero debe definir el número de radares próximos y, a continuación, agregar cada uno de ellos a un grupo. Empiece por el radar más alejado, por ejemplo, el situado más a la izquierda. Agregue los radares en grupos de tres y agregue los más próximos entre sí al mismo grupo.

Los radares de un grupo se sincronizarán entre sí para optimizar el rendimiento y no interferir unos con otros.

1. Vaya a **Radar > Settings > Coexistence (Radar > Ajustes > Coexistencia)**.
2. Establezca el número de radares próximos en **3–5**.

3. Asigne el radar a un grupo.



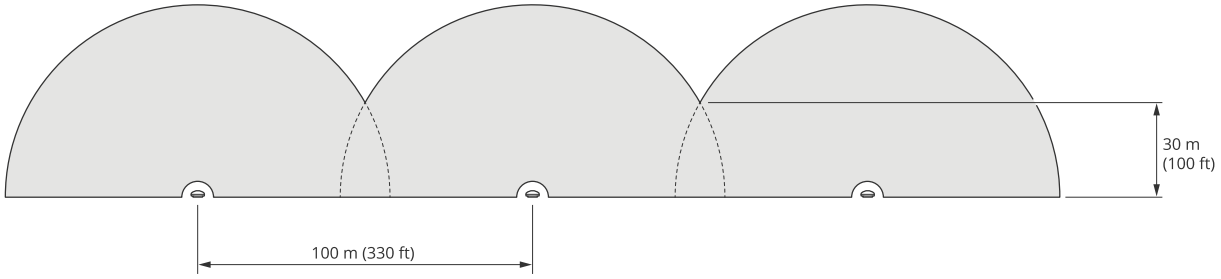
Este ejemplo ilustra como agrupar varios radares instalados uno al lado de otro en una zona de coexistencia.

Consulte otros ejemplos de instalaciones con varios radares en .

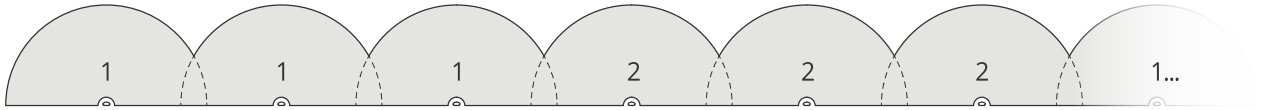
Ejemplos de zonas de instalación

Crear una valla virtual con varios radares

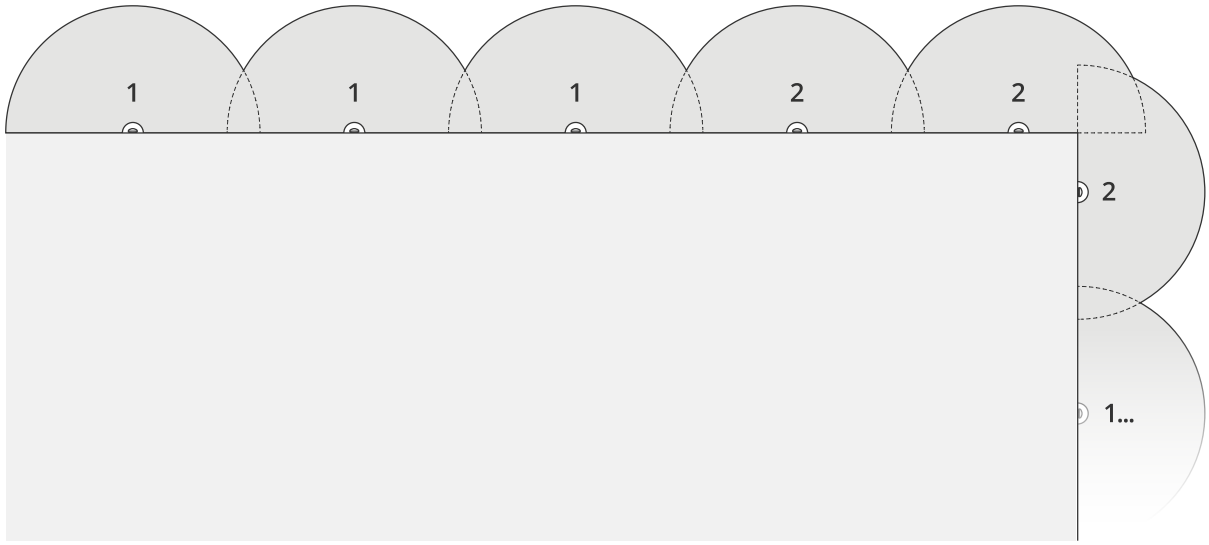
Para crear una valla virtual, por ejemplo, cerca de un edificio, puede poner varios radares uno al lado del otro. Le recomendamos colocarlos con una separación de 100 m.



Para evitar interferencias al colocar más de dos radares en una zona de coexistencia, defina el número de radares próximos en la interfaz del dispositivo. Por otra parte, si coloca más de tres radares, debe agregar cada radar a un grupo.



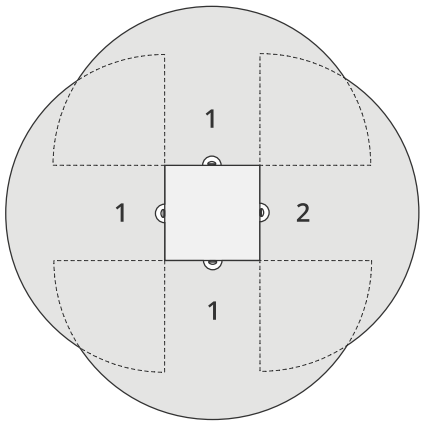
Puede ajustar la valla virtual de forma que también cubra las esquinas, como se muestra en este ejemplo.



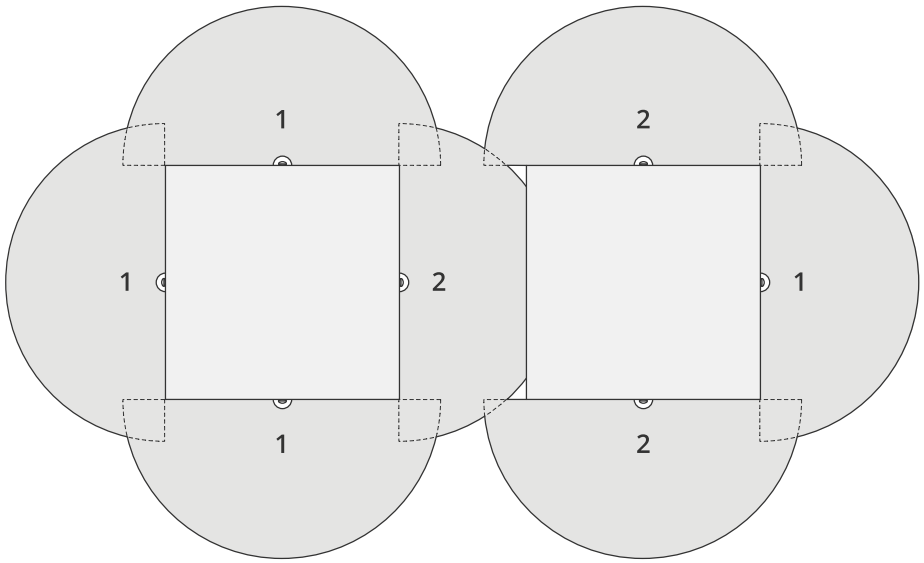
Consulte para obtener más información sobre radares próximos y grupos.

Cubrir una zona alrededor de un edificio

Para cubrir la zona alrededor de un edificio, coloque los radares en las paredes del edificio y orientados hacia afuera. Si va a colocar más de tres radares en una zona de coexistencia, defina el número de radares próximos en la interfaz del dispositivo y agregue cada radar a un grupo, como se indica en este ejemplo.



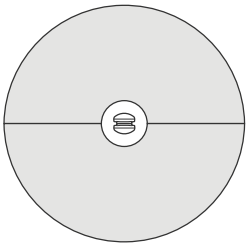
También puede cubrir la zona en torno a varios edificios.

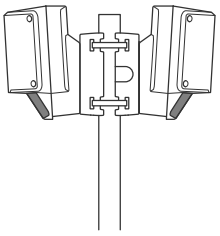


Consulte para obtener más información sobre radares próximos y grupos.

Cubrir una zona abierta

Para cubrir una zona abierta extensa, use dos montajes en poste para poner dos radares uno contra el otro.



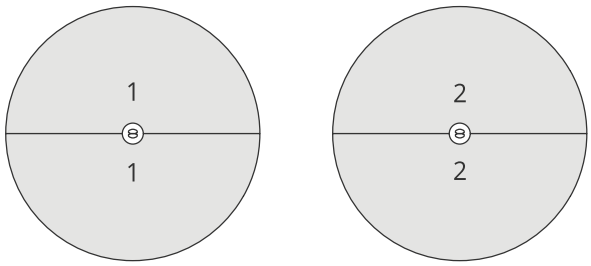


Puede usar la salida PoE de un radar para alimentar el segundo, pero no se puede conectar un tercer radar de esta manera.

Nota

La salida PoE en el radar se habilita cuando el radar se alimenta mediante un midspan de 60 W.

Si necesita varias instalaciones de radares uno contra el otro en una zona de coexistencia, defina el número de radares próximos en la interfaz del dispositivo y agregue cada radar a un grupo para evitar interferencias. En este ejemplo se indica cómo puede agrupar los radares en una instalación de uno contra otro.



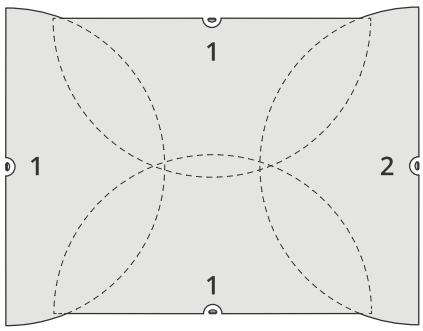
Consulte para obtener más información sobre radares próximos y grupos.

Instalación de varios radares frente a frente

En general, no es recomendable instalar más de tres radares frente a frente, ya que aumenta el riesgo de interferencias entre ellos. Sin embargo, en algunas zonas concretas puede ser necesario. Por ejemplo, si se quiere cubrir un campo de fútbol, los radares no se pueden poner en el centro.

Si instala más de tres radares frente a frente, la distancia mínima entre un radar y otro debe ser de 40 metros. También es muy importante definir el número de radares próximos en la interfaz del dispositivo y agregar cada radar a un grupo. De esta forma mejora el rendimiento de los radares.

Este ejemplo ilustra como agrupar cuatro radares para cubrir un campo.



Consulte para obtener más información sobre radares próximos y grupos.

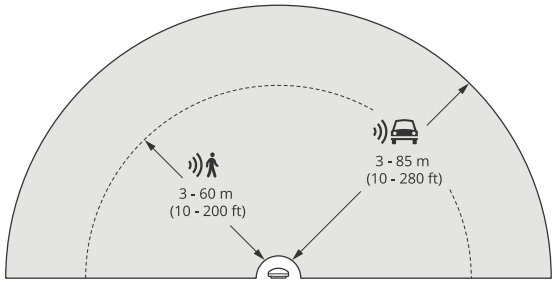
Alcance de la zona de detección

El alcance de detección es la distancia a la que puede hacerse el seguimiento de un objeto y activarse una alarma. Se mide desde un **límite de detección cercano** (la cercanía con la que puede hacerse una detección) hasta un **límite de detección lejano** (la distancia desde el dispositivo hasta la que puede hacerse una detección).

El **perfil de supervisión de área** está optimizado para detectar personas, pero también permite hacer el seguimiento de vehículos y otros objetos en movimiento que se mueven hasta una velocidad de 55 km/h, con una precisión de +/- 2 km/h.

Si se monta a la altura de instalación óptima, los alcances de detección son:

- **3–60 m** para detectar personas
- **3–85 m** para detectar vehículos



Nota

- Si instala el radar a una altura diferente, introduzca la altura real en la página web del producto al calibrar el radar.
- El rango de detección se ve afectado por la escena.
- El rango de detección se ve afectado por los radares cercanos.
- El rango de detección se ve afectado por el tipo de objeto.

El rango de detección se midió en estas condiciones:

- El rango se midió a lo largo del suelo.
- El objeto era una persona de 170 cm de altura.
- La persona caminaba directamente delante del radar.
- Los valores se miden cuando la persona accede a la zona de detección.
- La sensibilidad del radar se estableció en **Medium (Medio)**.

Altura de montaje	0° en vertical	Inclinación de 10°	20° en vertical
2,5 m (8,2 ft)	3,0–60 m (9,8–197 ft)	No recomendadas	No recomendadas
3,5 m (11 ft)	3,0–60 m (9,8–197 ft)	No recomendadas	No recomendadas
4,5 m (15 ft)	4,0–60 m (13–197 ft)	No recomendadas	No recomendadas
5,5 m (18 ft)	7,5–60 m (25–197 ft)	No recomendadas	No recomendadas
6,5 m (21 ft)	7,5–60 m (25–197 ft)	5,5–60 m (18–197 ft)	No recomendadas
8 m (26 ft)	No recomendadas	9–60 m (30–197 ft)	7,5–30 m (25–98 ft)
10 m (33 ft)	No recomendadas	15–60 m (49–197 ft)	9–35 m (30–115 ft)
12 m (39 ft)	No recomendadas	23–60 m (75–197 ft)	13–38 m (43–125 ft)
14 m (36 ft)	No recomendadas	27–60 m (89–197 ft)	17–35 m (56–115 ft)
16 m (52 ft)	No recomendadas	No recomendadas	25–50 m (82–164 ft)

Casos de uso de supervisión de área

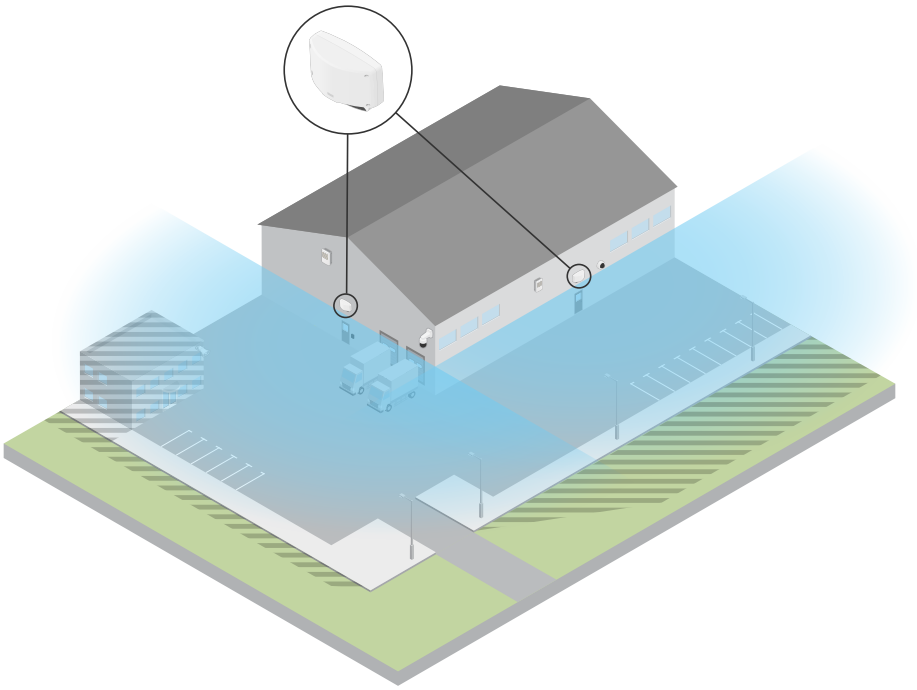
Cobertura de área en una piscina

En una piscina pública se habían producido varias intrusiones fuera del horario de funcionamiento. Como las instalaciones son privadas, los propietarios no pueden instalar videovigilancia, por lo que han instalado un radar y han configurarlo el **perfil de supervisión de área**. El radar está montado en el edificio y cubre toda la piscina y gran parte del entorno. Activa una advertencia desde un altavoz cuando se detecta una persona entre las horas de cierre y apertura, las 20:00 y las 06:00.

Cobertura de un campo en torno a un edificio

En una fábrica de productos químicos se ha agregado una capa de seguridad más al sistema utilizando radares para cubrir la zona en torno a un edificio importante. El sistema de seguridad ya cuenta con cámaras, cámaras

térmicas y controladores de puerta. Los radares pueden activar eventos para que las cámaras realicen el seguimiento de intrusos, amplíen el zoom y graben la actividad. Hay dispositivos intermitentes vinculados a las cámaras térmicas que parpadean para que los intrusos sepan que la zona está protegida y los controladores de puerta pueden restringir el acceso. Los radares permiten que el sistema de seguridad se active mucho antes de que un intruso haya llegado al edificio más importante.



Cobertura de una gran zona abierta

En un aparcamiento en el exterior de un pequeño centro comercial habían aumentado los robos en vehículos fuera del horario laboral. Siempre hay un guardia de seguridad de servicio, pero era necesario reforzar su seguridad por la noche sin incurrir en los costes de contratar más personal. Se han instalado dos radares de seguridad con el **perfil de supervisión de área**, montados contiguos para que cubran todo el aparcamiento. Los radares se han configurado para avisar al vigilante de servicio si se detecta algún comportamiento sospechoso y que pueda actuar en consecuencia. También se podría instalar un altavoz activado por los radares y que reproduzca un mensaje para disuadir a los intrusos.

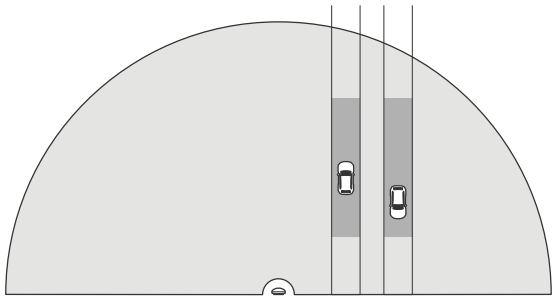
Perfil de supervisión de carretera

El **perfil de supervisión de carretera** resulta óptimo para controlar vehículos que circulan a una velocidad de hasta 105 km/h en zonas urbanas, zonas cerradas y en carreteras interurbanas. Este modo no debe usarse en la detección de personas u otros tipos de objetos. Para realizar un seguimiento de los objetos que no son vehículos, use el radar en .

Ejemplos de instalación en carretera

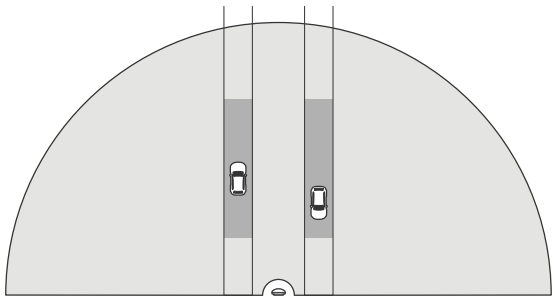
Montaje lateral

Para controlar los vehículos que circulan por una carretera, el radar se puede montar en un lateral. El radar proporciona una distancia de cobertura lateral de 10 m.



Montaje central

Para esta opción de montaje la posición debe ser estable. El radar se puede montar en un poste en medio de la carretera o en un puente que la atraviese. De esta forma, se obtiene una distancia de cobertura lateral de 10 m a los dos lados del radar. El radar cubre una distancia lateral mayor si se monta en el centro.



Nota

Es aconsejable montar el radar a una altura de entre 3 m y 8 m si se usa el **perfil de supervisión de carretera**.

Alcance de detección en carretera

El alcance de detección es la distancia a la que puede hacerse el seguimiento de un objeto y activarse una alarma. Se mide desde un **límite de detección cercano** (la cercanía con la que puede hacerse una detección) hasta un **límite de detección lejano** (la distancia desde el dispositivo hasta la que puede hacerse una detección).

Este perfil está optimizado para detectar vehículos y tiene una precisión de velocidad de +/- 2 km/h al supervisar a vehículos que circulan a 105 km/h como máximo.

Alcance de detección cuando el radar se monta a la altura de instalación óptima:

- **25–70 m** en el caso de vehículos que circulan a 60 km/h.
- **30–60 m** en el caso de vehículos que circulan a 105 km/h.

Casos de uso de supervisión de carreteras

Vehículos en zonas de velocidad baja

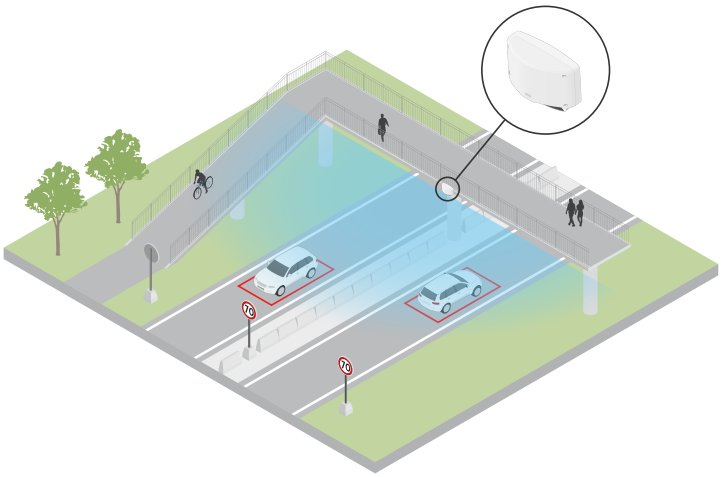
En un complejo industrial en el que hay una carretera larga entre dos almacenes se ha instalado un radar para tratar de imponer un límite de velocidad de 60 km/h. En el **perfil de supervisión de carretera**, el radar puede detectar sin un vehículo supera la velocidad límite en la zona de detección. A continuación, activa un evento que envía notificaciones por correo electrónico a los conductores y jefes. El aviso ayuda a aumentar el cumplimiento de las restricciones de velocidad.

Vehículos no deseados en una carretera cerrada

En una carretera cerrada que conduce a una vieja cantera seguían circulando vehículos y las autoridades han decidido instalar un radar de seguridad con el **perfil de supervisión de carretera**. El radar esta montado junto a la carretera y cubre toda su anchura. Cada vez que un vehículo entra en el escenario, se activa una señal intermitente que advierte a los conductores que deben salir de la carretera. También se envía un mensaje al equipo de seguridad para que vaya al lugar de los hechos si es necesario.

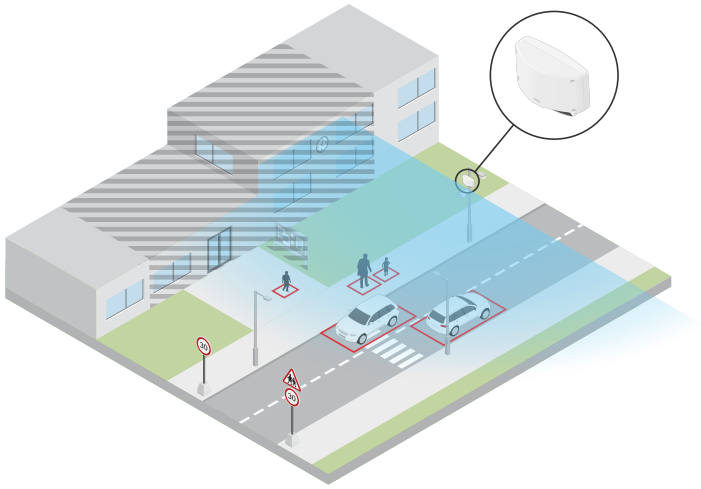
Control de velocidad en la carretera

En una carretera que atraviesa una ciudad pequeña se producían incidentes de exceso de velocidad. Para imponer un límite de velocidad de 70 km/h, las autoridades de tráfico han instalado un radar de seguridad con el **perfil de supervisión de carretera** en un puente sobre la calzada. Esto ha permitido detectar la velocidad a la que se desplazan los vehículos y determinar cuándo debe haber agentes en la carretera para controlar el tráfico.



Seguridad para personas y vehículos

El personal de una escuela ha identificado dos problemas de seguridad que hay que solucionar. Personas no autorizadas entran en las instalaciones durante horas lectivas y algunos vehículos superan la velocidad límite de 20 km/h en torno a la escuela. El radar se monta en un poste al lado del paso de peatones. Se decidió utilizar el para abordar los dos problemas porque permite que el radar detecte personas y vehículos que circulan a menos de 55 km/h. De este modo, el personal puede controlar que personas entran y salen en horario escolar, así como activar un altavoz que emite un aviso si un vehículo circula demasiado rápido.



Cómo funciona

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. Ambas aplicaciones son gratuitas y pueden descargarse desde *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™	Firefox®	Edge™	Safari®
Windows®	recomendado	✓	recomendado	
macOS®	recomendado	✓	recomendado	✓*
Linux®	recomendado	✓	recomendado	
Otros sistemas operativos	✓	✓	✓	✓

*No es totalmente compatible. Utilice otro navegador si experimenta problemas con la transmisión de vídeo.

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 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 en la red. HTTPS permite conexiones de red seguras y cifradas, protegiendo así datos confidenciales, como 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.

Información general de la interfaz web

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

Interfaz web del dispositivo Axis

Configure su dispositivo

Ajustar de la altura de montaje

Ajuste la altura de montaje del radar en la interfaz web. Esto ayuda al radar a detectar y medir correctamente la velocidad de los objetos que pasan.

Mida la altura desde el suelo hasta el radar con la mayor precisión posible. En el caso de escenas con superficies irregulares, establezca el valor que representa la altura media de la escena.

1. Vaya a **Radar > Settings > General (Radar > Ajustes > General)**.
2. Ajuste la altura en **Mounting height (Altura de montaje)**.

Calibrar mapa de referencia

Cargue un mapa de referencia para que sea más fácil ver por dónde se mueven los objetos detectados. Puede utilizar un plano o una foto aérea que muestre la zona cubierta por el radar. Calibre el mapa para que la cobertura del radar se ajuste a la posición, dirección y escala del mapa, y amplíe el mapa si está interesado en una parte específica de la cobertura del radar.

Puede utilizar un asistente de configuración que le guiará paso a paso por el proceso de calibración de los mapas o editar cada ajuste de forma individual.

Utilice el asistente de configuración:

1. Vaya a **Radar > Map calibration (Radar > Calibración del mapa)**.
2. Haga clic en **Setup assistant (Asistente de configuración)** y siga las instrucciones.

Para eliminar el mapa cargado y los ajustes que haya añadido, haga clic en **Reset calibration (Restablecer calibración)**.

Editar cada ajuste individualmente:
El mapa se calibrará gradualmente después de realizar cada ajuste.

1. Vaya a **Radar > Map calibration > Map** (Radar > Calibración del mapa > Mapa).
2. Seleccione la imagen que desea cargar o arrástrela y suéltela en el área designada.
   Para reutilizar una imagen de mapa con sus ajustes actuales de panorámica y zoom, haga clic en **Download map (Descargar mapa)**.
3. En **Rotate map (Girar mapa)**, utilice el control deslizante para girar el mapa hasta su posición.
4. Vaya a **Scale and distance on a map (Escala y distancia en un mapa)** y haga clic en dos puntos predeterminados del mapa.
5. En **Distance (Distancia)**, añada la distancia real entre los dos puntos que ha añadido al mapa.
6. Vaya a **Pan and zoom map (Mapa panorámico y zoom)** y utilice los botones para desplazarse por la imagen del mapa, o para acercar o alejar la imagen del mapa.

Nota

La función zoom no altera el área de cobertura del radar. Incluso si partes de la cobertura están fuera de la vista después de hacer zoom, el radar seguirá detectando objetos en movimiento en toda el área de cobertura. La única forma de excluir el movimiento detectado es añadir zonas de exclusión. Para obtener más información, vea .

7. Vaya a **Radar position (Posición del radar)** y utilice los botones para mover o girar la posición del radar en el mapa.

Para eliminar el mapa cargado y los ajustes que haya añadido, haga clic en **Reset calibration (Restablecer calibración)**.

El vídeo muestra un ejemplo de cómo calibrar un mapa de referencia en un radar Axis o en una cámara de fusión de radar y vídeo.

Establecer zonas de detección

Para determinar dónde detectar el movimiento, puede añadir una o varias zonas de detección. Utilice diferentes zonas para activar distintas acciones.

Existen dos tipos de zona:

- Un **scenario (escenario)** (anteriormente llamado zona de inclusión) es un área en la que los objetos en movimiento desencadenarán reglas. El escenario predeterminado es toda la zona que cubre el radar.
- Una **exclude zone (zona de exclusión)** es aquella en la que se ignorarán los objetos en movimiento. Utilice las zonas de exclusión si en un escenario hay áreas que desencadenan demasiadas alarmas no deseadas.

Agregar escenarios

Un escenario es una combinación de condiciones de activación y configuración de detección, que puede utilizar para crear reglas en el sistema de eventos. Agregue escenarios si desea crear reglas diferentes para distintas partes de la escena.

Agregar un escenario:

1. Vaya a **Radar > Scenarios (Radar > Escenarios)**.
2. Haga clic en **Add scenario (Agregar escenario)**.
3. Escriba el nombre del escenario.
4. Seleccione si quiere que se desencadene cuando haya objetos que se muevan por una zona o que crucen una o dos líneas.

Activador de objetos en movimiento en un área:

1. Seleccione **Movement in area (Movimiento en área)**.
2. Haga clic en **Next (Siguiente)**.
3. Seleccione el tipo de zona que se debe incluir en el escenario.
   Utilice el ratón para desplazar y cambiar la forma de la zona de manera que cubra la parte deseada de la imagen del radar o el mapa de referencia.
4. Haga clic en **Next (Siguiente)**.
5. Agregar ajustes de detección.

1. Agregue segundos hasta que se active después en **Ignore short-lived objects (Ignorar objetos que permanecen poco en la escena)**.
2. Seleccione el tipo de objeto que desea activar en **Trigger on object type (Desencadenar en tipo de objeto)**.
3. Agregue un rango para el límite de velocidad en **Speed limit (Límite de velocidad)**.

6. Haga clic en **Next (Siguiente)**.
7. Defina la duración mínima de la alarma en **Minimum trigger duration (Duración mínima del activador)**.
8. Haga clic en **Save (Guardar)**.

Desencadene en objetos que cruzan una línea:

1. Seleccione **Line crossing (Línea de cruce)**.

2. Haga clic en **Next (Siguiente)**.
3. Coloque la línea en la escena.
   Utilice el ratón para mover y dar forma a la línea.
4. Para cambiar la dirección de detección, active **Change direction (Cambiar dirección)**.
5. Haga clic en **Next (Siguiente)**.
6. Agregar ajustes de detección.
   6.1. Agregue segundos hasta que se active después en **Ignore short-lived objects (Ignorar objetos que permanecen poco en la escena)**.
   6.2. Seleccione el tipo de objeto que desea activar en **Trigger on object type (Desencadenar en tipo de objeto)**.
   6.3. Agregue un rango para el límite de velocidad en **Speed limit (Límite de velocidad)**.
7. Haga clic en **Next (Siguiente)**.
8. Defina la duración mínima de la alarma en **Minimum trigger duration (Duración mínima del activador)**. El valor predeterminado se establece en 2 segundos. Si desea que el escenario se active cada vez que un objeto cruza la línea, reduzca la duración a 0 segundos.
9. Haga clic en **Save (Guardar)**.

Desencadene en objetos que cruzan dos líneas:

1. Seleccione **Line crossing (Línea de cruce)**.
2. Haga clic en **Next (Siguiente)**.
3. Para que el objeto cruce dos líneas para que se active la alarma, active **Require crossing of two lines (Requerir cruce de dos líneas)**.
4. Coloque las líneas en la escena.
   Utilice el ratón para mover y dar forma a la línea.
5. Para cambiar la dirección de detección, active **Change direction (Cambiar dirección)**.
6. Haga clic en **Next (Siguiente)**.
7. Agregar ajustes de detección.
   7.1. Defina el límite de tiempo entre cruzar la primera y la segunda línea en **Max time between crossings (Tiempo máximo entre cruces)**.
   7.2. Seleccione el tipo de objeto que desea activar en **Trigger on object type (Desencadenar en tipo de objeto)**.
   7.3. Agregue un rango para el límite de velocidad en **Speed limit (Límite de velocidad)**.
8. Haga clic en **Next (Siguiente)**.
9. Defina la duración mínima de la alarma en **Minimum trigger duration (Duración mínima del activador)**. El valor predeterminado se establece en 2 segundos. Si desea que el escenario se active cada vez que un objeto haya cruzado las dos líneas, reduzca la duración a 0 segundos.
10. Haga clic en **Save (Guardar)**.

Agregar zonas de exclusión

Las zonas de exclusión son áreas en las que se ignorarán los objetos en movimiento. Añada zonas de exclusión para ignorar, por ejemplo, el balanceo de hojas en el lateral de una carretera. También puede añadir zonas de exclusión para ignorar las huellas fantasma causadas por materiales reflectantes del radar, como una valla metálica.

Agregar una zona de exclusión:

1. Vaya a **Radar > Exclude zones (Radar > Zonas de exclusión)**.
2. Haga clic en **Add exclude zone (Agregar zona de exclusión)**.
   Utilice el ratón para desplazar y cambiar la forma de la zona de manera que cubra la parte deseada de la imagen del radar o el mapa de referencia.

Minimizar falsas alarmas

Si observa que recibe demasiadas falsas alarmas, puede filtrar determinados tipos de movimiento u objetos, cambiar la cobertura o ajustar la sensibilidad de detección. Consulte qué ajustes funcionan mejor para su entorno.

- Ajuste de la sensibilidad de detección del radar:
  Vaya a **Radar > Settings > Detection (Radar > Ajustes > Detección)** y seleccione una **Detection sensitivity (Sensibilidad de detección)** menor. Esto reduce el riesgo de falsas alarmas, pero también puede hacer que el radar no detecte algún movimiento.
  El ajuste de sensibilidad afecta a todas las zonas.
  - **Bajo**: Utilice esta sensibilidad cuando haya muchos objetos de metal o vehículos grandes en el área. El radar tardará más tiempo en rastrear y clasificar objetos. Esto puede reducir el rango de detección, especialmente para objetos en rápido movimiento.
  - **Medio**: Esta es la configuración predeterminada.
  - **Alto**: Utilice esta sensibilidad cuando tenga un campo abierto sin objetos metálicos delante del radar. Esto aumentará el rango de detección para personas.
- Modifique escenarios y zonas de exclusión:
  Si un escenario incluye superficies duras como un muro de metal, puede haber reflejos que originen varias detecciones del mismo objeto físico. Puede modificar la forma del escenario o agregar una zona de exclusión que ignore determinadas partes del escenario. Para obtener más información, consulte y .
- Desencadenar en objetos que cruzan dos líneas en lugar de una:
  Si un escenario de cruce de línea incluye objetos con balanceo o animales en movimiento, existe el riesgo de que un objeto cruce la línea y desencadene una falsa alarma. En este caso, puede configurar el escenario para que se desencadene solo cuando un objeto haya cruzado dos líneas. Para obtener más información, vea .
- Filtre por movimiento:
  - Vaya a **Radar > Settings > Detection (Radar > Ajustes > Detección)** y seleccione **Ignore swaying objects (Ignorar objetos con balanceo)**. Este ajuste reduce las falsas alarmas generadas por árboles, arbustos y banderas en la zona de cobertura.
  - Vaya a **Radar > Settings > Detection (Radar > Ajustes > Detección)** y seleccione **Ignore small objects (Ignorar objetos pequeños)**. Este ajuste está disponible en el perfil de supervisión de área y reduce las falsas alarmas de objetos pequeños en la zona de cobertura, como los gatos y los conejos.
- Filtre por tiempo:
  - Vaya a **Radar > Scenarios (Radar > Escenarios)**.
  - Seleccione un escenario y haga clic ⋮ para modificar sus ajustes.
  - Seleccione un valor más alto en **Seconds until trigger (Segundos hasta el activador)**. Este es el tiempo de retraso desde que el radar inicia el seguimiento de un objeto hasta que active una alarma. El temporizador se inicia cuando el radar detecta el objeto por primera vez, no cuando el objeto entra en la zona especificada en el escenario.
- Filtre por tipo de objeto:
  - Vaya a **Radar > Scenarios (Radar > Escenarios)**.
  - Seleccione un escenario y haga clic ⋮ para modificar sus ajustes.
  - Para impedir activaciones generadas por tipos de objetos concretos, anule la selección de los tipos de objetos que no deben desencadenar eventos en este escenario.

Ver y grabar vídeo

En esta sección se incluyen instrucciones sobre la configuración del dispositivo. Para obtener más información sobre cómo funcionan la retransmisión y el almacenamiento, vaya a .

Reducir el ancho de banda y el almacenamiento

Importante

La reducción del ancho de banda puede provocar la pérdida de detalles de la imagen.

1. Vaya a **Radar > Stream (Radar > Flujo)**.
2. Haga clic en visualización en directo.
3. Seleccione **Video format (Formato de vídeo) H.264**.
4. Vaya a **Radar > Stream > General (Radar > Flujo > General)** y aumente la **Compresión**.

Nota

Casi todos los navegadores web no admiten la descodificación H.265, por lo que el dispositivo no la admite en su interfaz web. En su lugar, puede utilizar un sistema o aplicación de gestión de vídeo que admita descodificación H.265.

Configurar el almacenamiento de red

Para almacenar las grabaciones en la red, es necesario configurar previamente el almacenamiento en red.

1. Vaya a **System > Storage (Sistema > Almacenamiento)**.
2. Haga clic en **Add network storage (Añadir almacenamiento en red)** en **Network storage (Almacenamiento en red)**.
3. Escriba la dirección IP del servidor anfitrión.
4. Escriba el nombre de la ubicación compartida del servidor anfitrión en **Network Share (Recurso compartido en red)**.
5. Escriba el nombre de usuario y la contraseña.
6. Seleccione la versión SMB o déjela en **Auto (Automática)**.
7. Seleccione **Agregar recurso compartido sin pruebas** si experimenta problemas de conexión temporales o si el recurso compartido aún no está configurado.
8. Haga clic en **Añadir**.

Grabar y ver vídeo

Grabar vídeo directamente desde el radar

1. Vaya a **Radar > Stream (Radar > Flujo)**.
2. Para empezar a grabar, haga clic en .

   Si no ha configurado ningún almacenamiento, haga clic en y . Para obtener instrucciones sobre cómo configurar el almacenamiento de red, consulte
3. Para dejar de grabar haga clic de nuevo.

Ver vídeo

1. Vaya a **Recordings (Grabaciones)**.
2. Haga clic para la grabación en la lista.

Controlar una cámara PTZ con el radar

Es posible utilizar la información sobre la posición de los objetos del radar para hacer que una cámara PTZ siga objetos. Hay dos maneras de hacerlo:

- . La opción integrada es adecuada cuando tienes una cámara PTZ y un radar montados muy cerca.

- . La aplicación de Windows es adecuada cuando desea utilizar varias cámaras PTZ y radares para rastrear objetos.

Nota

Utilice un servidor NTP para sincronizar la hora en las cámaras, los radares y el ordenador con Windows. Si los relojes no están sincronizados, puede experimentar retrasos en el seguimiento o seguimiento fantasma.

Controle una cámara PTZ con el servicio de autotracking por radar integrado

El autotracking del radar incorporado crea una solución de borde a borde donde el radar controla directamente la cámara PTZ. Es compatible con todas las cámaras PTZ de Axis.

Nota

Puede utilizar el servicio de autotracking de radar integrado para conectar un radar con una cámara PTZ. Para una configuración en la que desea utilizar más de un radar o cámara PTZ, utilice AXIS Radar Autotracking for PTZ. Para obtener más información, consulte .

Esta instrucción explica cómo emparejar el radar con una cámara PTZ, cómo calibrar los dispositivos y cómo configurar el seguimiento de objetos.

Antes de empezar:

- Defina el área de interés y evite alarmas no deseadas configurando zonas de exclusión en el radar. Asegúrese de excluir las zonas con materiales reflectantes de radar u objetos con balanceo, como el follaje, para evitar que la cámara PTZ realice un seguimiento de objetos irrelevantes. Para consultar las instrucciones, vea .

Empareje el radar con la cámara PTZ:

1. Vaya a **System > Edge-to-edge > PTZ pairing (Sistema > De extremo a extremo > Emparejamiento PTZ)**.
2. Introduzca la dirección IP, el nombre de usuario y la contraseña para la cámara PTZ.
3. Haga clic en **Connect (Conectar)**.
4. Haga clic en **Configure Radar autotracking (Configurar autotracking de radar)** o vaya a **Radar > Radar PTZ autotracking (Radar > Radar autotracking para PTZ)** para configurar el autotracking de radar.

Calibre el radar y la cámara PTZ:

5. Vaya a **Radar > Radar PTZ autotracking (Radar > Radar autotracking para PTZ)**.
6. Para configurar la altura de montaje de la cámara, vaya a **Camera mounting height (Altura de montaje de la cámara)**.
7. Para desplazar la cámara PTZ de modo que apunte en la misma dirección que el radar, vaya a **Alineación panorámica**.
8. Si necesita ajustar la inclinación para compensar un terreno inclinado, vaya a **Compensación de inclinación del terreno** y agregue una compensación en grados.

Configure el seguimiento PTZ:

9. Vaya a **Seguir** para seleccionar si desea seguir personas, vehículos y/u objetos desconocidos.
10. Para empezar a seguir objetos con la cámara PTZ, active **Tracking (Seguimiento)**.
    El seguimiento realiza un zoom automáticamente en un objeto, o un grupo de objetos, para mantenerlos en la vista de la cámara.
11. Activa **Cambio de objetos** si esperas que haya varios objetos que no quepan en la vista de la cámara. Con este ajuste, el radar da prioridad a los objetos a rastrear.
12. Para determinar cuántos segundos rastrear cada objeto, establezca **Tiempo de retención del objeto**.
13. Para que la cámara PTZ vuelva a su posición inicial cuando el radar ya no rastree ningún objeto, active **Return to home (Volver a inicio)**.
14. Para determinar cuánto tiempo debe permanecer la cámara PTZ en la última posición conocida de los objetos rastreados antes de volver a la posición inicial, configure **Tiempo de espera para volver a casa**.
15. Para ajustar con precisión el zoom de la cámara PTZ, ajuste el zoom en el control deslizante.

Controla una cámara PTZ con AXIS Radar Autotracking for PTZ

AXIS Radar Autotracking for PTZ es una solución basada en servidor que puede manejar diferentes configuraciones al rastrear objetos:

- Controlar varias cámaras PTZ con un radar.
- Controlar una cámara PTZ con varios radares.
- Controlar varias cámaras PTZ con varios radares.
- Controlar una cámara PTZ con un radar cuando esté montada en distintas posiciones que cubran la misma zona.

La aplicación es compatible con un conjunto específico de cámaras PTZ. Para más información, ver *axis.com/products/axis-radar-autotracking-for-ptz#compatible-products*.

Descargue la aplicación y consulte el manual del usuario para obtener información sobre cómo configurar la aplicación. Para más información, ver *axis.com/products/axis-radar-autotracking-for-ptz#compatible-products*.

Configurar reglas para eventos

Para obtener más información, consulte nuestra guía *Introducción a las reglas de eventos*.

Activar una acción

1. Vaya a **System > Events (Sistema > Eventos)** y agregue una regla. La regla determina cuándo debe realizar el dispositivo determinadas acciones. Puede configurar reglas como programadas, recurrentes o activadas manualmente.
2. Introduzca un **Name (Nombre)**.
3. Seleccione la **Condition (Condición)** que debe cumplirse para que se active la acción. Si especifica varias condiciones para la regla, deben cumplirse todas ellas para que se active la acción.
4. En **Action (Acción)**, seleccione qué acción debe realizar el dispositivo cuando se cumplan las condiciones.

Nota

Si realiza cambios a una regla activa, esta debe iniciarse de nuevo para que los cambios surtan efecto.

Activar una notificación al abrir la carcasa

Este ejemplo ilustra cómo configurar una notificación por correo electrónico al abrir la carcasa del dispositivo.

Añadir un destinatario de correo electrónico:

1. Vaya a **System > Events > Recipients (Sistema > Eventos > Destinatarios)** y haga clic en **Add recipient (Agregar destinatario)**.
2. Escriba un nombre para el destinatario.
3. Seleccione **Email (Correo electrónico)** como tipo de notificación.
4. Introduzca la dirección de correo electrónico del destinatario.
5. Introduzca la dirección de correo electrónico desde la que desea que la cámara envíe las notificaciones.
6. Facilite los datos de inicio de sesión de la cuenta de correo electrónico de envío, junto con el nombre de host SMTP y el número de puerto.
7. Haga clic en **Test (Prueba)** para probar la configuración del correo electrónico.
8. Haga clic en **Save (Guardar)**.

Crear una regla:

9. Vaya a **Settings > Events > Rules (Ajustes > Eventos > Reglas)** y haga clic en **Añadir una regla**.
10. Escriba un nombre para la regla.

11. En la lista de condiciones, seleccione **Casing open (Apertura de carcasa)**.
12. En la lista de acciones, seleccione **Send notification to email (Enviar notificación a correo electrónico)**.
13. Seleccione un destinatario de la lista.
14. Introduzca un asunto y un mensaje para el correo electrónico.
15. Haga clic en **Save (Guardar)**.

Grabar vídeo de una cámara cuando se detecte movimiento

En este ejemplo se explica cómo configurar el radar y una cámara de forma que esta empiece a grabar en la tarjeta SD cinco segundos antes de que el radar detecte movimiento y deje de grabar un minuto después.

Conecte los dispositivos:

1. Conecte un cable de una salida de E/S del radar a una entrada de E/S de la cámara.

Configure el puerto de E/S del radar:

2. Vaya a **System > Accessories > I/O ports (Sistema > Accesorios > Puertos de E/S)** y configure el puerto de E/S como salida y seleccione el estado normal.

Crear una regla en el radar:

3. Vaya a **System > Events (Sistema > Eventos)** y agregue una regla.
4. Escriba un nombre para la regla.
5. En la lista de condiciones, seleccione un escenario en **Radar motion (Movimiento de radar)**.
   Para configurar un escenario, consulte .
6. En la lista de acciones, seleccione **Toggle I/O while the rule is active (Alternar E/S mientras la regla esté activa)** y, a continuación, el puerto que esté conectado a la cámara.
7. Haga clic en **Save (Guardar)**.

Configure el puerto de E/S de la cámara:

8. Vaya a **System > Accessories > I/O ports (Sistema > Accesorios > Puertos de E/S)** y configure el puerto de E/S como una entrada y seleccione el estado normal.

Cree una regla en la cámara:

9. Vaya a **System > Events (Sistema > Eventos)** y agregue una regla.
10. Escriba un nombre para la regla.
11. En la lista de condiciones, seleccione **Digital Input is active (La entrada digital está activa)** y seleccione el puerto que debe activar la regla.
12. En la lista de acciones, seleccione **Record video (Grabar vídeo)**.
13. En la lista de opciones de almacenamiento, seleccione **SD card (Tarjeta SD)**.
14. Seleccione un perfil de flujo o cree uno nuevo
15. Defina el valor del activador previo en 5 segundos.
16. Establezca el búfer posterior en 1 minuto.
17. Haga clic en **Save (Guardar)**.

Encender una luz cuando se detecte movimiento

Encender una luz cuando in intruso entra en una zona de detección puede tener un efecto disuasorio. Además, mejorará la calidad de imagen de una cámara visual que grabe la intrusión.

En este ejemplo se explica cómo configurar el radar y un iluminador para que este último se encienda cuando se detecte movimiento y se apague un minuto después.

Conecte los dispositivos:

1. Conecte uno de los cables de iluminador a la fuente de alimentación a través del puerto de relé del radar. Conecte el otro cable directamente de la fuente de alimentación al iluminador.

Configure el puerto de relé del radar:

2. Vaya a **System > Accessories > I/O ports (Sistema > Accesorios > Puertos de E/S)** y seleccione **Open circuit (Circuito abierto)** como estado normal del puerto de relé.

Crear una regla en el radar:

3. Vaya a **System > Events (Sistema > Eventos)** y agregue una regla.
4. Escriba un nombre para la regla.
5. En la lista de condiciones, seleccione un escenario en **Radar motion (Movimiento de radar)**. Para configurar un escenario, consulte .
6. En la lista de acciones, seleccione **Toggle I/O once (Alternar E/S una vez)** y, a continuación, el puerto de relé.
7. Seleccione **Active (Activo)**.
8. Defina la **Duration (Duración)**.
9. Haga clic en **Save (Guardar)**.

Enviar un correo electrónico si alguien cubre el radar con un objeto metálico

En este ejemplo se explica cómo crear una regla que envíe una notificación por correo electrónico cuando alguien manipula el radar cubriéndolo con un objeto metálico, como una lámina metálica o una placa metálica.

Nota

La opción para crear reglas para eventos de manipulación del radar está disponible en AXIS OS 11.11.

Añadir un destinatario de correo electrónico:

1. Vaya a **System > Events > Recipients (Sistema > Eventos > Destinatarios)** y haga clic en **Add recipient (Agregar destinatario)**.
2. Escriba un nombre para el destinatario.
3. Seleccione **Email (Correo electrónico)**.
4. Introduzca la dirección de correo electrónico a la que se debe enviar el correo.
5. La cámara no tiene un servidor de correo electrónico propio, por lo que deberá iniciar sesión en otro servidor de correo electrónico para enviar correos. Rellene el resto de la información según su proveedor de correo electrónico.
6. Para enviar un correo electrónico de prueba, haga clic en **Test (Probar)**.
7. Haga clic en **Save (Guardar)**.

Crear una regla:

8. Vaya a **System > Events (Sistema > Eventos)** y agregue una regla.
9. Escriba un nombre para la regla.
10. En la lista de condiciones, en **Device status (Estado del dispositivo)**, seleccione **Radar data failure (Fallo de datos del radar)**.
11. En **Reason (Razón)**, seleccione **Tampering (Manipulación)**.
12. En la lista de acciones, en **Notifications (Notificaciones)**, seleccione **Send notification to email (Enviar notificación a correo electrónico)**.
13. Seleccione el destinatario que ha creado.
14. Escriba un asunto y un mensaje para el correo electrónico.
15. Haga clic en **Save (Guardar)**.

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

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.

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.

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.

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.

Radar

Ajustes

General

Radar transmission (Transmisión de radar): Utilice esta opción para apagar completamente el módulo del radar.

Channel (Canal) : Si tiene problemas con varios dispositivos que se interfiera entre sí, seleccione el mismo canal para un máximo de cuatro dispositivos que estén cerca entre sí. En la mayoría de las instalaciones, seleccione **Auto (Automático)** para permitir que los dispositivos negocien automáticamente qué canal utilizar.

Mounting height (Altura de montaje): Introduzca la altura de montaje del producto.

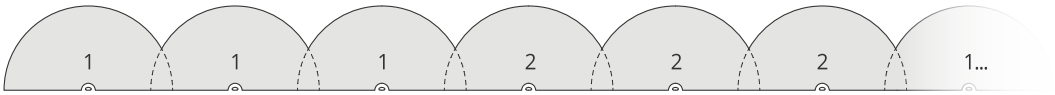
Nota

Sea tan específico como pueda cuando introduzca la altura de montaje. De este modo, el dispositivo puede visualizar la detección por radar en la posición correcta de la imagen.

Coexistencia

Number of neighboring radars (Número de radares cercanos): Seleccione el número de radares cercanos que se montan dentro de la misma zona de coexistencia. Esto ayudará a evitar interferencias. El radio de coexistencia es de 350 m.

- **0–1**: Seleccione esta opción si monta de uno a dos radares en la misma zona de coexistencia.
- **2**: Seleccione esta opción si monta tres radares en la misma zona de coexistencia.
- **3–5**: Seleccione esta opción si monta de cuatro a seis radares en la misma zona de coexistencia.
  - **Groups (Grupos)**: Seleccione un grupo (**Grupo 1** o **Grupo 2**) para el radar. Esto también ayudará a evitar interferencias. Recomendamos que agregue tres radares en cada grupo y que agregue los radares más cercanos entre sí en el mismo grupo.



Para obtener más información, vea .

Detección

Detection sensitivity (Sensibilidad de detección): Seleccione la sensibilidad que debe tener el radar. Cuanto mayor sea el valor, mayor será el alcance de detección, pero también mayor será el riesgo de falsas alarmas. Una sensibilidad más baja reduce el número de falsas alarmas, pero puede acortar el rango de detección.

Radar profile (Perfil de radar): Seleccione un perfil que se ajuste a su área de interés.

- **Supervisión de área**: Realice un seguimiento de objetos grandes y pequeños moviéndose a velocidades inferiores en áreas abiertas.
  - **Ignore stationary rotating objects (Ignorar objetos rotatorios estacionarios)** : Active esta función para minimizar las falsas alarmas de objetos estacionarios con movimientos rotatorios, como ventiladores o turbinas.
  - **Ignore small objects (Ignorar objetos pequeños)**: Active esta función para minimizar las falsas alarmas procedentes de objetos pequeños, tales como gatos o conejos.
  - **Ignore swaying objects (Ignorar objetos con balanceo)**: Active esta función para minimizar el número de falsas alarmas de objetos con balanceo, como árboles, arbustos o postes.
- **Supervisión de carreteras**: Realice un seguimiento de los vehículos que se mueven a mayor velocidad en zonas urbanas y carreteras suburbanas
  - **Ignore stationary rotating objects (Ignorar objetos rotatorios estacionarios)** : Active esta función para minimizar las falsas alarmas de objetos estacionarios con movimientos rotatorios, como ventiladores o turbinas.
  - **Ignore swaying objects (Ignorar objetos con balanceo)**: Active esta función para minimizar el número de falsas alarmas de objetos con balanceo, como árboles, arbustos o postes.

Ver

Information legend (Leyenda de información): Active esta función para que se muestre una leyenda con los tipos de objeto que el radar puede detectar y rastrear. Arrastre y coloque la leyenda de información para cambiarla de sitio.

Zone opacity (Opacidad de zona): Seleccione la opacidad o transparencia de la zona de cobertura.

Grid opacity (Opacidad de cuadrícula): Seleccione la opacidad o transparencia de la cuadrícula.

Color scheme (Esquema de colores): Seleccione un tema para la visualización de radar.

Rotation (Rotación) : Seleccione la orientación que prefiera para la imagen del radar.

Visualización de objetos

Trail lifetime (Vida útil de rastro): Seleccione el tiempo que está visible el rastro de un objeto de seguimiento en la vista de radar.

Icon style (Estilo de icono): Seleccione el estilo de icono de los objetos con seguimiento en la vista de radar. Para triángulos sencillos, seleccione **Triangle (Triángulo)**. Para símbolos representativos, seleccione **(Symbol) Símbolo**. Los iconos señalarán en la dirección del movimiento de los objetos con seguimiento, independientemente del estilo.

Show information with icon (Mostrar información con icono): Seleccione la información que se debe mostrar junto al icono del objeto de seguimiento:

- **Object type (Tipo de objeto)**: indica el tipo de objeto que detectado el radar.
- **Classification probability (Probabilidad de clasificación)**: indica el nivel de certeza del radar de que la clasificación de objetos es correcta.
- **Velocity (Velocidad)**: indica la velocidad a la que se mueve el objeto.

Flujo

General

Resolución: Seleccione la resolución de imagen apta para la escena de vigilancia. Una mayor resolución aumenta el ancho de banda y el almacenamiento.

Velocidad de imagen: Para evitar problemas de ancho de banda en la red o para reducir el tamaño de almacenamiento, puede limitar la velocidad de fotogramas a un número fijo. Si deja la velocidad de fotogramas en cero, la velocidad se mantendrá en el máximo nivel de velocidad posible según las condiciones actuales. Una velocidad de fotogramas más alta requiere más ancho de banda y capacidad de almacenamiento.

P-frames: Un fotograma P es una imagen pronosticada que solo muestra los cambios en la imagen con respecto al fotograma anterior. Introduzca el número deseado de fotogramas P. Cuanto mayor es el número, menos ancho de banda se necesita. Sin embargo, si hay congestión en la red, puede haber un declive notable en la calidad del vídeo.

Compression (Compresión): Utilice el control deslizante para ajustar la compresión de imagen. Cuanto mayor sea la compresión, menor será la velocidad de fotogramas y la calidad de imagen. Una compresión menor mejora la calidad de la imagen, pero requiere más ancho de banda y espacio de almacenamiento al grabar.

Vídeo firmado : Active esta opción para agregar la función de vídeo firmado a los vídeos. El vídeo firmado protege el vídeo contra manipulaciones mediante la adición de firmas criptográficas.

Control de velocidad de bits

- **Promedio**: Seleccione esta opción para ajustar automáticamente la velocidad de bits durante más tiempo y proporcionar la mejor calidad de imagen posible en función del almacenamiento disponible.
  -  Haga clic para calcular la velocidad de bits de destino en función del almacenamiento, el tiempo de retención y el límite de velocidad de bits disponibles.
  - **Velocidad de bits objetivo**: Introduzca la velocidad de bits de destino deseada.
  - **Tiempo de conservación**: Introduzca el número de días que guardar las grabaciones.
  - **Almacenamiento**: Muestra el almacenamiento estimado que se puede ser usado para el flujo.
  - **Velocidad de bits máxima**: Active esta función para establecer un límite de velocidad de bits.
  - **Bitrate limit (Límite de velocidad de bits)**: Introduzca un límite de velocidad de bits mayor que la velocidad de bits de destino.
- **Máximo**: Seleccione para establecer una velocidad de bits instantánea máxima del flujo en función del ancho de banda de la red.
  - **Máximo**: Introduzca la velocidad de bits máxima.
- **Variable**: Seleccione esta opción para permitir que la velocidad de bits varíe en función del nivel de actividad de la escena. Más actividad requiere más ancho de banda. Recomendamos esta opción para la mayoría de situaciones.

Calibración del mapa

Utilice la calibración del mapa para cargar y calibrar un mapa de referencia. El resultado de la calibración es un mapa de referencia que muestra la cobertura del radar en la escala adecuada, lo que facilita ver dónde se mueven los objetos.

Setup assistant (Asistente de configuración): Haga clic para abrir el asistente de configuración que le guiará paso a paso por el proceso de calibración.

Reset calibration (Restablecer calibración): Haga clic para eliminar la imagen actual del mapa y la posición del radar en el mapa.

Mapa

Cargar mapa: Seleccione o arrastre y suelte la imagen del mapa que desea cargar.

Download map (Descargar mapa): Haga clic para descargar el mapa.

Rotate map (Girar mapa): Utilice el control deslizante para girar la imagen de mapa.

Escala y distancia en el mapa

Distance (distancia): Añada la distancia entre los dos puntos que ha añadido al mapa.

Panorámica y zoom

Pan (Horizontal): Haga clic en los botones para realizar una panorámica de la imagen del mapa.

Zoom: Haga clic en los botones para acercar o alejar la imagen del mapa.

Reset pan and zoom (Restablecer panorámica y zoom): Haga clic para eliminar los ajustes de panorámica y zoom.

Posición del radar

Position (Posición): Haga clic en los botones para desplazar el radar por el mapa.

Rotation (Rotación): Haga clic en los botones para girar el radar por el mapa.

Zonas de exclusión

Una **exclude zone (zona de exclusión)** es aquella en la que se ignoran los objetos en movimiento. Utilice las zonas de exclusión si en un escenario hay áreas que desencadenan demasiadas alarmas no deseadas.

+ : Haga clic para crear una nueva zona de exclusión.

Para modificar una zona de exclusión, selecciónela en la lista.

Realizar un seguimiento de los objetos que pasan: Active esta opción para realizar un seguimiento de los objetos que atraviesan la zona de exclusión. Los objetos que pasan mantienen los ID de seguimiento y son visibles en toda la zona. No se realizará el seguimiento de los objetos que aparezcan dentro de la zona de exclusión.

Formas de zona predefinidas: Seleccione la forma inicial de la zona de exclusión.

- **Cubrir todo**: Seleccione esta opción para definir una zona de exclusión que cubra toda el área de cobertura del radar.
- **Restablecer en recuadro**: Seleccione esta opción para colocar una zona de exclusión rectangular en el centro del área de cobertura.

Para modificar la forma de la zona, arrastre y coloque cualquiera de los puntos de las líneas. Para eliminar un punto, haga clic en él con el botón derecho.

Escenarios

Un escenario es una combinación de condiciones de activación y de ajustes de escena y detección.


: Haga clic para crear un nuevo escenario. Puede crear hasta 20 escenarios.

Triggering conditions (Condiciones de activación): Seleccione la condición que activará las alarmas.

- **Movimiento en área**: Seleccione si quiere activar el escenario en objetos que se mueven por una zona.
- **Cruce de línea**: Seleccione si desea que el escenario se active cuando los objetos crucen una o dos líneas.

Scene (Escena): Defina el área o las líneas en el escenario en el que los objetos en movimiento activarán alarmas.

- Para **Movement in area (Movimiento en área)**, seleccione una de las posiciones predefinidas para modificar el área.
- Para **Line crossing (Cruce de línea)**, arrastre y coloque la línea en la escena. Para crear más puntos en una línea, haga clic en cualquier punto y arrastre. Para eliminar un punto, haga clic en él con el botón derecho.
  - **Requerir traspasar dos líneas**: Active esta opción si el objeto debe pasar dos líneas antes de que el escenario active una alarma.
  - **Change direction (Cambiar dirección):** Active esta opción si desea que el escenario active una alarma cuando los objetos crucen la línea en la otra dirección.

Detection settings (Ajustes de detección): Defina los criterios de activación del escenario.

- Para **Movement in area (Movimiento en área)**:
  - **Ignore short-lived objects (Ignorar los objetos que permanecen poco en la escena)**: Defina el retraso en segundos desde que el radar detecte el objeto hasta el momento en el que el escenario active una alarma. Esto puede ayudar a reducir las falsas alarmas.
  - **Trigger on object type (Activador por tipo de objeto)**: Seleccione el tipo de objetos (humano, vehículo, desconocido) con los que desea que se desencadene el escenario.
  - **Speed limit (Límite de velocidad)**: Se desencadena cuando los objetos se mueven a velocidades dentro de un rango específico.
    - **Invert (Invertir)**: Seleccione si desea activar velocidades por encima y por debajo del límite de velocidad establecido.
- Para **Line crossing (Cruce de línea)**:
  - **Ignore short-lived objects (Ignorar los objetos que permanecen poco en la escena)**: Defina el retraso en segundos desde que el radar detecte el objeto hasta el momento en el que el escenario active una acción. Esto puede ayudar a reducir las falsas alarmas. Esta opción no está disponible para los objetos que cruzan dos líneas.
  - **Tiempo máximo entre cruces**: Defina el tiempo máximo entre el cruce de la primera línea y la segunda. Esta opción solo está disponible para los objetos que cruzan dos líneas.
  - **Trigger on object type (Activador por tipo de objeto)**: Seleccione el tipo de objetos (humano, vehículo, desconocido) con los que desea que se desencadene el escenario.
  - **Speed limit (Límite de velocidad)**: Se desencadena cuando los objetos se mueven a velocidades dentro de un rango específico.
    - **Invert (Invertir)**: Seleccione si desea activar velocidades por encima y por debajo del límite de velocidad establecido.

Ajustes de la alarma: Defina los criterios de la alarma.

- **Duración mínima de la activación**: Defina la duración mínima de la alarma activada.

Superposiciones

: Haga clic para agregar una superposición. Seleccione el tipo de superposición de la lista desplegable:

- **Texto**: Seleccione esta opción para mostrar un texto integrado en la imagen de visualización en directo y visible en todas las vistas, grabaciones e instantáneas. Puede introducir su propio texto e incluir también modificadores preconfigurados para que se muestren automáticamente, por ejemplo, la hora, la fecha y la velocidad de fotogramas.
  - : Haga clic para añadir el modificador de fecha `%F` para mostrarla en formato aaaa-mm-dd.
  - : Haga clic para agregar el modificador de hora `%X` para mostrarla en formato hh:mm:ss (reloj de 24 horas).
  - **Modificadores**: Haga clic para seleccionar los modificadores de la lista para agregarlos al cuadro de texto. Por ejemplo, el modificador `%a` muestra el día de la semana.
  - **Size (Tamaño)**: Seleccione el tamaño de fuente deseado.
  - **Appearance (Aspecto)**: Seleccione el color del texto y del fondo; por ejemplo, texto blanco sobre fondo negro (valor predeterminado).
  - : Seleccione la posición de la superposición en la imagen o haga clic en la superposición y arrástrela para moverla en la visualización en directo.
- **Imagen**: Seleccione esta opción para mostrar una imagen estática superpuesta sobre el flujo de vídeo. Puede utilizar los archivos .bmp, .png, .jpeg o .svg.
  Para subir una imagen, haga clic en **Manage images (Gestión de imágenes)**. Antes de cargar una imagen, puede elegir:
  - **Escala con resolución**: Seleccione esta opción para escalar automáticamente la superposición de imagen de modo que se ajuste a la resolución de vídeo.
  - **Usar transparencia**: Seleccione e introduzca el valor hexadecimal RGB para ese color. Utilice el formato RRGGBB. Ejemplos de valores hexadecimales: FFFFFF para el blanco, 000000 para el negro, FF0000 para el rojo, 6633FF para el azul y 669900 para el verde. Solo para imágenes .bmp.
- **Scene annotation (Anotación de escena)** : Seleccione para mostrar una superposición de texto en la transmisión de vídeo que permanece en la misma posición, incluso cuando la cámara se desplaza o inclina en otra dirección. Puede optar por mostrar solo la superposición dentro de ciertos niveles de zoom.
  - : Haga clic para añadir el modificador de fecha `%F` para mostrarla en formato aaaa-mm-dd.
  - : Haga clic para agregar el modificador de hora `%X` para mostrarla en formato hh:mm:ss (reloj de 24 horas).
  - **Modificadores**: Haga clic para seleccionar los modificadores de la lista para agregarlos al cuadro de texto. Por ejemplo, el modificador `%a` muestra el día de la semana.
  - **Size (Tamaño)**: Seleccione el tamaño de fuente deseado.
  - **Appearance (Aspecto)**: Seleccione el color del texto y del fondo; por ejemplo, texto blanco sobre fondo negro (valor predeterminado).
  - : Seleccione la posición de la superposición en la imagen o haga clic en la superposición y arrástrela para moverla en la visualización en directo. La superposición se guarda y permanece en las coordenadas de giro e inclinación de esta posición.

- **Anotación entre niveles de zoom (%)**: Establezca los niveles de zoom en los que se mostrará la superposición.
- **Símbolo de anotación**: Seleccione un símbolo que aparezca en lugar de la superposición cuando la cámara no esté dentro de los niveles de zoom establecidos.

- **Streaming indicator (Indicador de transmisión)** : Seleccione esta opción para mostrar una animación superpuesta sobre el flujo de vídeo. La animación indica que el flujo de vídeo se realiza en directo, aunque la escena no contiene ningún movimiento.
  - **Appearance (Aspecto)**: Seleccione el color de la animación y del fondo; por ejemplo, animación roja sobre un fondo transparente (valor predeterminado).
  - **Size (Tamaño)**: Seleccione el tamaño de fuente deseado.
  - : Seleccione la posición de la superposición en la imagen o haga clic en la superposición y arrástrela para moverla en la visualización en directo.

- **Widget: Linegraph (Gráfico lineal)** : Muestre un gráfico que muestre cómo cambia un valor medido con el tiempo.
  - **Title (Título)**: introduzca un nombre para el widget.
  - **Modificador de superposición**: Seleccione un modificador de superposición como fuente de datos. Si ha creado superposiciones MQTT, se ubicarán al final de la lista.
  - : Seleccione la posición de la superposición en la imagen o haga clic en la superposición y arrástrela para moverla en la visualización en directo.
  - **Size (Tamaño)**: Seleccione el tamaño de la superposición.
  - **Visible en todos los canales**: Desactívelo para mostrar solo el canal seleccionado en la actualidad. Actívelo para mostrar en todos los canales activos.
  - **Actualizar intervalo**: Elija el tiempo entre actualizaciones de datos.
  - **Transparency (Transparencia)**: Establezca la transparencia de toda la superposición.
  - **Transparencia de fondo**: Establezca la transparencia solo del fondo de la superposición.
  - **Puntos**: Actívelo para agregar un punto a la línea del gráfico cuando se actualicen los datos.
  - Eje X
    - **Label (Etiqueta)**: Introduzca la etiqueta de texto para el eje x.
    - **Ventana de tiempo**: Introduzca el tiempo que se visualizarán los datos.
    - **Unidad de tiempo**: Introduzca una unidad de tiempo para el eje x.
  - Eje Y
    - **Label (Etiqueta)**: Introduzca la etiqueta de texto para el eje y.
    - **Escala dinámica**: Actívelo para que la escala se adapte automáticamente a los valores de los datos. Desactívelo para introducir valores manualmente para una escala fija.
    - **Umbral mínimo de alarma** y **Umbral máximo de alarma**: Estos valores agregarán líneas de referencia horizontales al gráfico, lo que facilitará ver cuando el valor de los datos sube o baja demasiado.

- **Widget: Meter (Medidor)** : Muestra un gráfico de barras que muestra el valor de datos medido más recientemente.
  - **Title (Título)**: introduzca un nombre para el widget.
  - **Modificador de superposición**: Seleccione un modificador de superposición como fuente de datos. Si ha creado superposiciones MQTT, se ubicarán al final de la lista.

- : Seleccione la posición de la superposición en la imagen o haga clic en la superposición y arrástrela para moverla en la visualización en directo.
- **Size (Tamaño)**: Seleccione el tamaño de la superposición.
- **Visible en todos los canales**: Desactívelo para mostrar solo el canal seleccionado en la actualidad. Actívelo para mostrar en todos los canales activos.
- **Actualizar intervalo**: Elija el tiempo entre actualizaciones de datos.
- **Transparency (Transparencia)**: Establezca la transparencia de toda la superposición.
- **Transparencia de fondo**: Establezca la transparencia solo del fondo de la superposición.
- **Puntos**: Actívelo para agregar un punto a la línea del gráfico cuando se actualicen los datos.
- Eje Y
  - **Label (Etiqueta)**: Introduzca la etiqueta de texto para el eje y.
  - **Escala dinámica**: Actívelo para que la escala se adapte automáticamente a los valores de los datos. Desactívelo para introducir valores manualmente para una escala fija.
  - **Umbral mínimo de alarma** y **Umbral máximo de alarma**: Estos valores agregarán líneas de referencia horizontales al gráfico de barras, lo que facilitará ver cuando el valor de los datos sube o baja demasiado.

Radar autotracking para PTZ

Empareje el radar con una cámara PTZ para usar el autotracking por radar. Para establecer la conexión, vaya a **System > Edge-to-edge (Sistema > De extremo a extremo)**.

Configurar ajustes iniciales:

Camera mounting height (Altura de montaje de la cámara): La distancia desde el suelo hasta la altura de la cámara PTZ montada.

Alineación horizontal: Mueva horizontalmente la cámara PTZ de manera que señale en la misma dirección que el radar. Haga clic en la dirección IP de la cámara PTZ para acceder a ella.

Guardar desviación horizontal: Haga clic para guardar la alineación horizontal.

Desplazamiento de inclinación de suelo: Utilice el desplazamiento de inclinación de suelo para ajustar con precisión la inclinación de la cámara. Si el suelo está inclinado o la cámara no está montada horizontalmente, es posible que la cámara esté orientada demasiado hacia arriba o demasiado hacia abajo para realizar el seguimiento de un objeto.

Done (Listo): Haga clic para guardar los ajustes y continuar con la configuración.

Configuración de autotracking de PTZ:

Track (Rastrear): Seleccione esta opción si desea rastrear personas, vehículos u objetos desconocidos.

Tracking (Seguimiento): Active esta opción para empezar a seguir objetos con la cámara PTZ. El seguimiento realiza un zoom automáticamente en un objeto, o un grupo de objetos, para mantenerlos en la vista de la cámara.

Object switching (Cambio de objetos): Si el radar detecta varios objetos que no encajan en la vista de la cámara PTZ, esta cámara realiza un seguimiento del objeto al que el radar le da la prioridad más alta e ignora los demás.

Object hold time (Tiempo de espera del objeto): Determina durante cuántos segundos la cámara PTZ debe realizar un seguimiento de cada objeto.

Return to home (Volver a inicio): Active esta opción para que la cámara PTZ vuelva a su posición de inicio cuando el radar deje de realizar el seguimiento de un objeto.

Return to home timeout (Tiempo de espera para volver a inicio): Determina cuánto tiempo debe permanecer la cámara PTZ en la última posición conocida de los objetos rastreados antes de volver al inicio.

Zoom: Utilice el regulador PTZ para ajustar el zoom de la cámara PTZ.

Reconfigure installation (Volver a configurar la instalación): Haga clic para borrar todos los ajustes y volver a la configuración inicial.

Grabaciones

Ongoing recordings (Grabaciones en curso): Muestra todas las grabaciones en curso en la cámara.

- Inicia una grabación en el dispositivo.
- Elija en qué dispositivo de almacenamiento guardar la grabación.
- Detener una grabación en el dispositivo.

Las grabaciones activadas finalizarán cuando se detengan manualmente o cuando se apague el dispositivo.

Las **grabaciones continuas** seguirán hasta que se detengan manualmente. Aunque el aparato se apague, la grabación continuará cuando vuelva a encenderse.

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. Tenga en cuenta que si trabaja en una zona horaria distinta a la ubicación del dispositivo, el intervalo de tiempo se basa en la zona horaria del dispositivo.

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: Mostrar grabaciones según la fuente. La fuente hace referencia al sensor.

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*. 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.

- **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.
  - **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.

Localización de dispositivo

Especifique el lugar en el que se encuentra el dispositivo. El sistema de gestión de vídeo puede utilizar esta información para colocar el dispositivo en un mapa.

- **Format (Formato)**: Seleccione el formato que se utilizará al introducir la latitud y la longitud del dispositivo.
- **Latitude (Latitud)**: Los valores positivos son el norte del ecuador.
- **Longitude (Longitud)**: Los valores positivos son el este del meridiano principal.
- **Heading (Rumbo)**: Introduzca la dirección de la brújula a la que apunta el dispositivo. 0 es al norte.
- **Label (Etiqueta)**: Especifique un nombre descriptivo para el dispositivo.
- **Save (Guardar)**: Haga clic para guardar la localización del dispositivo.

Ajustes regionales

Establezca el sistema de medidas que se utilizará en todos los ajustes del sistema.

Metric (m, km/h) (Métrico (m, km/h)): seleccione la medición de la distancia en metros y la medición de la velocidad en kilómetros por hora.

U.S. customary (pies, mph) (Sistema estadounidense (pies, mph): seleccione la medición de la distancia en pies y la medición de la velocidad en millas por hora.

Red

IPv4

Asignar IPv4 automáticamente: Seleccione esta opción para que el router de red asigne automáticamente una dirección IP al dispositivo. Recomendamos IP automática (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 (Agregar 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.

HTTP y HTTPS

HTTPS es un protocolo que proporciona cifrado para las solicitudes de página de los usuarios y para las páginas devueltas por el servidor web. El intercambio de información cifrado se rige por el uso de un certificado HTTPS, que garantiza la autenticidad del servidor.

Para utilizar HTTPS en el dispositivo, debe instalar un certificado HTTPS. Vaya a **System > Security (Sistema > Seguridad)** para crear e instalar certificados.

Allow access through (Permitir acceso mediante): Seleccione si un usuario tiene permiso para conectarse al dispositivo a través de **HTTP**, **HTTPS** o ambos protocolos **HTTP and HTTPS (HTTP y HTTPS)**.

Nota

Si visualiza páginas web cifradas a través de HTTPS, es posible que experimente un descenso del rendimiento, especialmente si solicita una página por primera vez.

HTTP port (Puerto HTTP): Especifique el puerto HTTP que se utilizará. El dispositivo permite el puerto 80 o cualquier puerto en el rango 1024-65535. Si ha iniciado sesión como administrador, también puede introducir cualquier puerto en el rango 1-1023. Si utiliza un puerto en este rango, recibirá una advertencia.

HTTPS port (Puerto HTTPS): Especifique el puerto HTTPS que se utilizará. El dispositivo permite el puerto 443 o cualquier puerto en el rango 1024-65535. Si ha iniciado sesión como administrador, también puede introducir cualquier puerto en el rango 1-1023. Si utiliza un puerto en este rango, recibirá una advertencia.

Certificado: Seleccione un certificado para habilitar HTTPS para el dispositivo.

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 CPD 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.

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*.

Allow O3C (Permitir O3C):

- **Un clic**: Esta es la opción predeterminada. Para conectarse al O3C, pulse el botón de control del dispositivo. Según el modelo del dispositivo, mantenga pulsado o suelte el botón hasta que el LED de estado parpadee. Registre el dispositivo en el servicio O3C en un plazo de 24 horas para habilitar la opción **Siempre** y mantenerse conectado. Si no se 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.
  - **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*.
- **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+)**: 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.

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.

Evitar ataques de fuerza bruta

Blocking (Bloqueo): Active esta función para bloquear ataques de fuerza bruta. Un ataque de fuerza utiliza un sistema de ensayo y error para descubrir información de inicio de sesión o claves de cifrado.

Blocking period (Período de bloqueo): Introduzca el número de segundos para bloquear un ataque de fuerza bruta.

Blocking conditions (Condiciones de bloqueo): Introduzca el número de fallos de autenticación permitidos por segundo antes de que se inicie el bloqueo. Puede definir el número de fallos permitidos tanto a nivel de página como de dispositivo.

Firewall

Firewall: Encender para activar el firewall.

Política predeterminada: Seleccione cómo desea que el firewall gestione las solicitudes de conexión no contempladas en 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 hacer excepciones a la política predeterminada, puede crear reglas que permiten o bloquean 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 las conexiones de dispositivos que satisfagan 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 desea permitir o bloquear. Utilice IPv4/IPv6 en **Start (Inicio)** y **End (Fin)**.
  - **IP address (Dirección IP)**: Introduzca la dirección que desea permitir o bloquear. Utilice el formato IPv4/IPv6 o CIDR.
  - **Protocol (Protocolo)**: Seleccione un protocolo de red (TCP, UDP o ambos) para permitir o bloquear. Si selecciona un protocolo, también debe especificar un puerto.
  - **MAC**: Introduzca la dirección MAC de un dispositivo que desea permitir o bloquear.
  - **Port range (Intervalo de puertos)**: Seleccione para especificar el rango de puertos que desea permitir o bloquear. Añádalos en **Start (Inicio)** y **End (Fin)**.
  - **Puerto**: Introduzca un número de puerto que desea permitir o bloquear. Los números de puerto deben situarse entre 1 y 65535.
  - **Traffic type (Tipo de tráfico)**: Seleccione el tipo de tráfico que desea 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 (LIMITAR)**: Seleccione esta opción para aceptar conexiones de dispositivos que cumplan los criterios definidos en la regla, pero aplicando límites para reducir el tráfico excesivo.
  - **IP range (Intervalo IP)**: Seleccione para especificar el rango de direcciones que desea permitir o bloquear. Utilice IPv4/IPv6 en **Start (Inicio)** y **End (Fin)**.
  - **IP address (Dirección IP)**: Introduzca la dirección que desea permitir o bloquear. Utilice el formato IPv4/IPv6 o CIDR.
  - **Protocol (Protocolo)**: Seleccione un protocolo de red (TCP, UDP o ambos) para permitir o bloquear. Si selecciona un protocolo, también debe especificar un puerto.
  - **MAC**: Introduzca la dirección MAC de un dispositivo que desea permitir o bloquear.
  - **Port range (Intervalo de puertos)**: Seleccione para especificar el rango de puertos que desea permitir o bloquear. Añádalos en **Start (Inicio)** y **End (Fin)**.
  - **Puerto**: Introduzca un número de puerto que desea permitir o bloquear. Los números de puerto deben situarse entre 1 y 65535.
  - **Unit (Unidad)**: Seleccione el tipo de conexiones que desea permitir o bloquear.
  - **Period (Periodo)**: Seleccione el periodo de tiempo relacionado con la **Amount (Cantidad)**.
  - **Amount (Cantidad)**: Determine el número máximo de veces que un dispositivo puede conectarse dentro del **Period (Periodo)** establecido. El número máximo es 65535.

- **Burst (Ráfaga)**: Introduzca el número de conexiones que pueden superar la **Amount (Cantidad)** establecida una vez durante el **Period (Periodo)** determinado. Una vez alcanzado el número, solo se permite la cantidad establecida durante el período determinado.
- **Traffic type (Tipo de tráfico)**: Seleccione el tipo de tráfico que desea 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 (Reglas de prueba): Haga clic para probar las reglas definidas.

- **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 probar las reglas.
- **Apply rules (Aplicar reglas)**: Haga clic para activar las reglas sin realizar pruebas. No 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)**: No tiene acceso para cambiar ajustes.

El menú contextual contiene:

Actualizar cuenta: Editar las propiedades de la cuenta.

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

Acceso anónimo

Permitir la visualización anónima: Active esta opción para permitir que todos los usuarios accedan al dispositivo como visores sin tener que registrarse con una cuenta.

Allow anonymous PTZ operating (Permitir funcionamiento PTZ anónimo) : Active esta opción para permitir que los usuarios anónimos giren, inclinen y acerquen el zoom a la imagen.

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 (Agregar 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.

Configuración de OpenID

Importante

Si no puede utilizar OpenID para iniciar sesión, utilice las credenciales Digest o Basic que usó al configurar OpenID para iniciar sesión.

Client ID (ID de cliente): Introduzca el nombre de usuario de OpenID.

Outgoing Proxy (Proxy saliente): Introduzca la dirección de proxy de la conexión de OpenID para usar un servidor proxy.

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

Provider URL (URL de proveedor): Introduzca el enlace web para la autenticación de punto de acceso de API. El formato debe ser https://[insertar URL]/.well-known/openid-configuration

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.

Remote user (Usuario remoto): Introduzca un valor para identificar usuarios remotos. Esto ayudará a mostrar el usuario actual en la interfaz web del dispositivo.

Scopes (Ámbitos): Ámbitos opcionales que podrían formar parte del token.

Client secret (Secreto del cliente): Introduzca la contraseña de OpenID.

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

Enable OpenID (Habilitar OpenID): Active esta opción para cerrar la conexión actual y permitir la autenticación del dispositivo desde la URL del proveedor.

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.

MQTT

MQTT (Message Queuing Telemetry Transport) es un protocolo de mensajería estándar para Internet of things (IoT). Se diseñó para simplificar la integración del IoT y se utiliza en una amplia variedad de sectores para conectar dispositivos remotos con una huella de código pequeña y un ancho de banda de red mínimo. El cliente MQTT del software de dispositivos de Axis puede simplificar la integración de los datos y eventos producidos en el dispositivo con sistemas que no sean software de gestión de vídeo (VMS).

Configure el dispositivo como cliente MQTT. La comunicación MQTT se basa en dos entidades, los clientes y el intermediario. Los clientes pueden enviar y recibir mensajes. El intermediario es responsable de dirigir los mensajes entre los clientes.

Puede obtener más información sobre MQTT en la *base de conocimiento de AXIS OS*.

ALPN

ALPN es una extensión de TLS/SSL que permite seleccionar un protocolo de aplicación durante la fase de enlace de la conexión entre el cliente y el servidor. Se utiliza para habilitar el tráfico MQTT a través del mismo puerto que se utiliza para otros protocolos, como HTTP. En algunos casos, es posible que no haya un puerto dedicado abierto para la comunicación MQTT. Una solución en tales casos es utilizar ALPN para negociar el uso de MQTT como protocolo de aplicación en un puerto estándar, permitido por los cortafuegos.

Cliente MQTT

Conectar: Active o desactive el cliente MQTT.

Estado: Muestra el estado actual del cliente MQTT.

Broker

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

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

Puerto: Introduzca el número de puerto.

- 1883 es el valor predeterminado de **MQTT a través de TCP**
- 8883 es el valor predeterminado de **MQTT a través de SSL**
- 80 es el valor predeterminado de **MQTT a través de WebSocket**
- 443 es el valor predeterminado de **MQTT a través de WebSocket Secure**

Protocol ALPN: Introduzca el nombre del protocolo ALPN proporcionado por su proveedor de MQTT. Esto solo se aplica con MQTT a través de SSL y MQTT a través de WebSocket Secure.

Nombre de usuario: Introduzca el nombre de cliente que utilizará la cámara para acceder al servidor.

Contraseña: Introduzca una contraseña para el nombre de usuario.

Client ID (ID de cliente): Introduzca una ID de cliente. El identificador de cliente que se envía al servidor cuando el cliente se conecta a él.

Clean session (Limpiar sesión): Controla el comportamiento en el momento de la conexión y la desconexión. Si se selecciona, la información de estado se descarta al conectar y desconectar.

Proxy HTTP: Una URL con una longitud máxima de 255 bytes. Puede dejar el campo vacío si no desea utilizar un proxy HTTP.

Proxy HTTPS: Una URL con una longitud máxima de 255 bytes. Puede dejar el campo vacío si no desea utilizar un proxy HTTPS.

Keep alive interval (Intervalo de Keep Alive): Habilita al cliente para detectar si el servidor ya no está disponible sin tener que esperar a que se agote el tiempo de espera de TCP/IP.

Timeout (Tiempo de espera): El intervalo de tiempo está en segundos para permitir que se complete la conexión. Valor predeterminado: 60

Device topic prefix (Prefijo de tema del dispositivo): se utiliza en los valores por defecto del tema en el mensaje de conexión, en el mensaje LWT de la pestaña **MQTT client (Cliente MQTT)** y, en las condiciones de publicación de la pestaña **MQTT publication (Publicación MQTT)** ".

Reconnect automatically (Volver a conectar automáticamente): especifica si el cliente debe volver a conectarse automáticamente tras una desconexión.

Mensaje de conexión

Especifica si se debe enviar un mensaje cuando se establece una conexión.

Enviar mensaje: Active esta función para enviar mensajes.

Usar predeterminado: Desactive esta opción para introducir su propio mensaje predeterminado.

Topic (Tema): Introduzca el tema para el mensaje predeterminado.

Payload (Carga): Introduzca el contenido para el mensaje predeterminado.

Retain (Retener): Seleccione esta opción para mantener el estado del cliente en este **Tema**

QoS: Cambie la capa de QoS para el flujo de paquetes.

Mensaje de testamento y últimas voluntades

El testamento y últimas voluntades (LWT) permite a un cliente proporcionar un testimonio junto con sus credenciales al conectar con el intermediario. Si el cliente se desconecta de forma no voluntaria (quizá porque no dispone de fuente de alimentación), puede permitir que el intermediario entregue un mensaje a otros clientes. Este mensaje de LWT tiene el mismo formato que un mensaje normal y se enruta a través de la misma mecánica.

Enviar mensaje: Active esta función para enviar mensajes.

Usar predeterminado: Desactive esta opción para introducir su propio mensaje predeterminado.

Topic (Tema): Introduzca el tema para el mensaje predeterminado.

Payload (Carga): Introduzca el contenido para el mensaje predeterminado.

Retain (Retener): Seleccione esta opción para mantener el estado del cliente en este **Tema**

QoS: Cambie la capa de QoS para el flujo de paquetes.

Publicación MQTT

Usar prefijo de tema predeterminado: Seleccione esta opción para utilizar el prefijo de tema predeterminado, que se define en el prefijo de tema del dispositivo en la pestaña **Cliente MQTT**.

Incluir nombre de tema: Seleccione esta opción para incluir el tema que describe la condición en el tema de MQTT.

Incluir espacios de nombres de tema: Seleccione esta opción para incluir los espacios de nombres de los temas ONVIF en el tema MQTT.

Include serial number (Incluir número de serie): seleccione esta opción para incluir el número de serie del dispositivo en la carga útil de MQTT.

Add condition (Agregar condición): Haga clic para agregar una condición.

Retain (Retener): define qué mensajes MQTT se envían como retenidos.

- **None (Ninguno)**: envíe todos los mensajes como no retenidos.
- **Property (Propiedad)**: envíe únicamente mensajes de estado como retenidos.
- **Todo**: Envíe mensajes con estado y sin estado como retenidos.

QoS: Seleccione el nivel deseado para la publicación de MQTT.

Suscripciones MQTT

Add subscription (Agregar suscripción): Haga clic para agregar una nueva suscripción MQTT.

Filtro de suscripción: Introduzca el tema de MQTT al que desea suscribirse.

Usar prefijo de tema del dispositivo: Agregue el filtro de suscripción como prefijo al tema de MQTT.

Tipo de suscripción:

- **Sin estado**: Seleccione esta opción para convertir mensajes MQTT en mensajes sin estado.
- **Con estado**: Seleccione esta opción para convertir los mensajes MQTT en una condición. El contenido se utiliza como estado.

QoS: Seleccione el nivel deseado para la suscripción a MQTT.

Superposiciones MQTT

Nota

Conéctese a un intermediario de MQTT antes de agregar los modificadores de superposición de MQTT.

Add overlay modifier (Agregar modificador de superposición): Haga clic para agregar un nuevo modificador de superposición.

Topic filter (Filtro de tema): Agregue el tema de MQTT que contiene los datos que desea mostrar en la superposición.

Data field (Campo de datos): Especifique la clave para la carga del mensaje que desea mostrar en la superposición, siempre y cuando el mensaje esté en formato JSON.

Modifier (Modificador): Utilice el modificador resultante cuando cree la superposición.

- Los modificadores que empiezan con **#XMP** muestran todos los datos recibidos del tema.
- Los modificadores que empiezan con **#XMD** muestran los datos especificados en el campo de datos.

Almacenamiento

Almacenamiento de red

Ignorar: Active para ignorar el almacenamiento de red.

Agregar almacenamiento de red: Haga clic para agregar un recurso compartido de red en el que guardar grabaciones.

- **Dirección**: Introduzca la dirección IP el nombre de host del servidor host, que suele ser un dispositivo de almacenamiento conectado a la red (NAS). Le recomendamos que configure el host para utilizar una dirección IP fija (que no sea DHCP, ya que las direcciones IP dinámicas pueden cambiar) o que utilice DNS. No se admiten los nombres SMB/CIFS de Windows.
- **Recurso compartido de red**: Escriba el nombre de una ubicación de recurso compartido en el servidor host. Varios dispositivos de Axis pueden utilizar el mismo recurso compartido de red, porque cada uno tiene su propia carpeta.
- **Usuario**: Si el servidor requiere un inicio de sesión, escriba el nombre de usuario. Para iniciar sesión en un servidor de dominio concreto, escriba `DOMAIN\username`.
- **Contraseña**: Si el servidor requiere un inicio de sesión, escriba la contraseña.
- **Versión de SMB**: Seleccione la versión del protocolo de almacenamiento SMB para conectarse al NAS. Si selecciona **Auto**, el dispositivo intentará negociar una de las versiones seguras SMB: 3.02, 3.0 o 2.1. Seleccione 1.0 o 2.0 para conectarse a almacenamiento en red tipo NAS más antiguo que no admita versiones superiores. Puede leer más sobre la compatibilidad con SMB en dispositivos Axis *aquí*.
- **Agregar recurso compartido sin pruebas**: Seleccione esta opción para agregar el recurso compartido de red aunque se detecte un error durante la prueba de conexión. El error puede ser, por ejemplo, que no se ha introducido una contraseña y el servidor la requiere.

Remove network storage (Eliminar almacenamiento de red): Haga clic para desinstalar, desvincular y eliminar la conexión con el recurso compartido de red. Así se eliminan todos los ajustes del recurso compartido de red.

Desvincular: Haga clic para desvincular y desconectar el recurso compartido de red.
Bind (Vincular): Haga clic para vincular y conectar el recurso compartido de red.

Unmount (Desmontar): Haga clic para desmontar el recurso compartido de red.
Mount (Montar): Haga clic para montar el recurso compartido de red.

Write protect (Protección contra escritura): Active esta opción para dejar de escribir en el recurso compartido de red y evitar que se eliminen las grabaciones. El formato de un recurso compartido de red protegido contra escritura no se puede cambiar.

Tiempo de conservación: Seleccione el tiempo que desea guardar las grabaciones para limitar la cantidad de grabaciones antiguas o cumplir con la normativa sobre almacenamiento de datos. Si se llena el almacenamiento de red, las grabaciones antiguas se eliminarán antes de que transcurra el periodo de tiempo seleccionado.

Herramientas

- **Test connection (Probar conexión)**: Pruebe la conexión con el recurso compartido de red.
- **Format (Formato)**: Formatee el recurso compartido de red, por ejemplo, cuando tenga que borrar rápidamente todos los datos. CIFS es la opción del sistema de archivos disponible.

Usar herramienta: Haga clic para activar la herramienta seleccionada.

Almacenamiento integrado

Importante

Riesgo de pérdida de datos y grabaciones dañadas. No extraiga la tarjeta SD mientras el dispositivo esté en funcionamiento. Desmonte la tarjeta SD para extraerla.

Unmount (Desmontar): Haga clic en esta opción para eliminar la tarjeta SD de forma segura.

Write protect (Protección contra escritura): Active esta opción para dejar de escribir en la tarjeta SD y evitar que se eliminen las grabaciones. El formato de una tarjeta SD protegida contra escritura no se puede cambiar.

Formato automático: Active esta función para formatear automáticamente una tarjeta SD que se acaba de insertar. El formato del sistema de archivos se cambia a ext4.

Ignorar: Active esta función para dejar de almacenar las grabaciones en la tarjeta SD. Si ignora la tarjeta SD, el dispositivo deja de reconocerla. Este ajuste solo está disponible para los administradores.

Tiempo de conservación: Seleccione el tiempo que desea guardar las grabaciones para limitar la cantidad de grabaciones antiguas o cumplir con las normativas en materia de almacenamiento de datos. Cuando la tarjeta SD está llena, elimina las grabaciones antiguas antes de que transcurra su tiempo de retención.

Herramientas

- **Check (Comprobar)**: Con esta opción se comprueban errores en la tarjeta SD.
- **Repair (Reparar)**: Se reparan los errores del sistema de archivos.
- **Format (Formato)**: Formatea la tarjeta SD para cambiar el sistema de archivos y borrar todos los datos. Solo puede formatear la tarjeta SD en el sistema de archivos ext4. Se necesita contar con una aplicación o un controlador ext4 de terceros para acceder al sistema de archivos desde Windows®.
- **Encrypt (Cifrar)**: Use esta herramienta para formatear la tarjeta SD y habilitar el cifrado. Borra todos los datos de la tarjeta SD. Se cifrará cualquier dato nuevo que almacene en la tarjeta SD.
- **Descifrar**: Use esta herramienta para formatear la tarjeta SD sin cifrado. Borra todos los datos de la tarjeta SD. No se cifrará ningún dato nuevo que almacene en la tarjeta SD.
- **Change password (Modificar contraseña)**: Se cambia la contraseña necesaria para cifrar la tarjeta SD.

Usar herramienta: Haga clic para activar la herramienta seleccionada.

Activador de desgaste: Defina un valor para el nivel de desgaste de la tarjeta SD al que desee activar una acción. El nivel de desgaste oscila entre el 0 y el 200 %. Una nueva tarjeta SD que nunca se haya utilizado tiene un nivel de desgaste del 0 %. Un nivel de desgaste del 100 % indica que la tarjeta SD está cerca de su vida útil prevista. Cuando el nivel de desgaste llega al 200 % existe un riesgo alto de fallos de funcionamiento de la tarjeta SD. Recomendamos ajustar el activador del desgaste entre un 80 y un 90 %. Esto le da tiempo a descargar cualquier grabación y a sustituir la tarjeta SD a tiempo antes de que se desgaste. El activador de desgaste le permite configurar un evento y recibir una notificación cuando el nivel de desgaste alcance su valor establecido.

Perfiles de transmisión

Un perfil de flujo es un grupo de ajustes que afectan al flujo de vídeo. Puede utilizar perfiles de flujo en distintas situaciones, por ejemplo, al crear eventos y utilizar reglas para grabar.

Add stream profile (Agregar perfil de flujo): Haga clic para crear un perfil de flujo nuevo.

Preview (Vista previa): Una vista previa del flujo de vídeo con los ajustes del perfil de flujo que seleccione. La vista previa se actualiza cuando se modifican los ajustes de la página. Si el dispositivo tiene distintas áreas de visualización, puede cambiar el área de visualización en la lista desplegable de la esquina inferior izquierda de la imagen.

Name (Nombre): Agregue un nombre para su perfil.

Descripción: Agregue una descripción de su perfil.

Video codec (Códec de vídeo): Seleccione el códec de vídeo que debe aplicarse al perfil.

Resolución: Consulte para obtener una descripción de este ajuste.

Velocidad de imagen: Consulte para obtener una descripción de este ajuste.

Compression (Compresión): Consulte para obtener una descripción de este ajuste.

Zipstream (Flujo zip) : Consulte para obtener una descripción de este ajuste.

Optimize for storage (Optimizar para almacenamiento) : Consulte para obtener una descripción de este ajuste.

Dynamic FPS (FPS dinámico) : Consulte para obtener una descripción de este ajuste.

Dynamic GOP (GOP dinámico) : Consulte para obtener una descripción de este ajuste.

Mirror (Duplicar) : Consulte para obtener una descripción de este ajuste.

GOP length (Longitud de GOP) : Consulte para obtener una descripción de este ajuste.

Control de velocidad de bits: Consulte para obtener una descripción de este ajuste.

Include overlays (Incluir superposiciones) : Seleccione el tipo de superposiciones que desea incluir. Consulte para obtener información sobre cómo agregar superposiciones.

Include audio (Incluir audio) : Consulte para obtener una descripción de este ajuste.

ONVIF

Cuentas de ONVIF

ONVIF (Open Network Video Interface Forum) es un estándar de interfaz internacional que facilita que los usuarios finales, los integradores, los consultores y los fabricantes se beneficien de las distintas opciones que ofrece la tecnología de vídeo en red. ONVIF permite la interoperabilidad entre productos de distintos proveedores, proporciona mayor flexibilidad, costes reducidos y sistemas preparados para el futuro.

Al crear una cuenta ONVIF, se permite automáticamente la comunicación ONVIF. Utilice el nombre de cuenta y la contraseña para todas las comunicaciones ONVIF con el dispositivo. Para obtener más información, consulte la comunidad de desarrolladores de Axis en *axis.com*.

Agregar cuentas: Haga clic para agregar una nueva cuenta ONVIF.

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.

Función:

- **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**.
  - Agregar aplicaciones.
- **Cuenta de medios**: Permite acceder solo al flujo de vídeo.

El menú contextual contiene:

Actualizar cuenta: Editar las propiedades de la cuenta.

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

Perfiles multimedia de ONVIF

Un perfil de medios ONVIF está formado por un conjunto de configuraciones que puede utilizar para cambiar la configuración de flujo de medios. Puede crear nuevos perfiles con su propio conjunto de configuraciones o utilizar perfiles preconfigurados para una configuración rápida.

Añadir perfil de medios: Haga clic para agregar un nuevo perfil de medios ONVIF.

Nombre de perfil: Agregue un nombre para el perfil multimedia.

Fuente de vídeo: Seleccione la fuente de video para su configuración.

- **Seleccionar configuración**: Seleccione de la lista una configuración definida por el usuario. Las configuraciones en la lista desplegable corresponden a los canales de video del dispositivo, incluidas vistas múltiples, áreas de visualización y canales virtuales.

Video encoder (Codificador de vídeo): Seleccione el formato de codificación de video para su configuración.

- **Seleccionar configuración**: Seleccione una configuración definida por el usuario de la lista y ajuste la configuración de codificación. Las configuraciones en la lista desplegable actúan como identificadores/nombres de la configuración del codificador de video. Seleccione el usuario del 0 al 15 para aplicar sus propios ajustes, o seleccione uno de los usuarios predeterminados si desea utilizar configuraciones predefinidas para un formato de codificación específico.

Nota

Habilite el audio en el dispositivo para tener la opción de seleccionar una fuente de audio y una configuración del codificador de audio.

Fuente de audio : Seleccione la fuente de entrada de audio para su configuración.

- **Seleccionar configuración**: Seleccione una configuración definida por el usuario de la lista y ajuste la configuración de audio. Las configuraciones de la lista desplegable corresponden a las entradas de audio del dispositivo. Si el dispositivo tiene una entrada de audio, es usuario0. Si el dispositivo tiene varias entradas de audio, habrá usuarios adicionales en la lista.

Codificador de audio : Selecciona el formato de codificación de audio para tu configuración.

- **Seleccionar configuración**: Seleccione una configuración definida por el usuario de la lista y ajuste la configuración de codificación de audio. Las configuraciones de la lista desplegable actúan como identificadores/nombres de la configuración del codificador de audio.

Descodificador de audio : Seleccione el formato de descodificación de audio para su configuración.

- **Seleccionar configuración**: Seleccione una configuración definida por el usuario de la lista y ajuste la configuración. Las configuraciones de la lista desplegable actúan como identificadores/nombres de la configuración.

Salida de audio : Seleccione el formato de salida de audio para su configuración.

- **Seleccionar configuración**: Seleccione una configuración definida por el usuario de la lista y ajuste la configuración. Las configuraciones de la lista desplegable actúan como identificadores/nombres de la configuración.

Metadatos: Seleccione los metadatos para incluir en su configuración.

- **Seleccionar configuración**: Seleccione una configuración definida por el usuario de la lista y ajuste la configuración de los metadatos. Las configuraciones de la lista desplegable actúan como identificadores/nombres de la configuración de metadatos.

PTZ : Seleccione los ajustes de PTZ para su configuración.

- **Seleccionar configuración**: Seleccione una configuración definida por el usuario de la lista y ajuste la configuración PTZ. Las configuraciones en la lista desplegable corresponden a los canales de video del dispositivo con soporte PTZ.

Create (Crear): Haga clic para guardar los ajustes y crear el perfil.

Cancelar: Haga clic para cancelar la configuración y borrar todas los ajustes.

profile_x: Haga clic en el nombre del perfil para abrir y editar el perfil preconfigurado.

Detectores

Detección de impactos

Detector de golpes: Active para generar una alarma si un objeto golpea el dispositivo o si se manipula.

Nivel de sensibilidad: Mueva el control deslizante para ajustar el nivel de sensibilidad al que el dispositivo debe generar una alarma. Un valor bajo significa que el dispositivo solo genera una alarma si el golpe es potente. Un valor alto significa que el dispositivo genera una alarma incluso cuando la manipulación sea ligera.

Accesorios

Puertos de E/S

Use la entrada digital para conectar seguridad positiva que pueda alternar entre circuitos abiertos y cerrados, por ejemplo, sensores PIR, contactos de puertas o ventanas y detectores de cristales rotos.

Use la salida digital para establecer conexión con dispositivos externos, como relés y LED. Puede activar los dispositivos conectados a través de la interfaz de programación de aplicaciones VAPIX® o la interfaz web.

Puerto

Name (Nombre): Edite el texto para cambiar el nombre del puerto.

Direction (Dirección):  indica que el puerto es un puerto de entrada.  indica que el puerto es un puerto de salida. Si el puerto es configurable, puede hacer clic en los iconos para cambiar entre entrada y salida.

Normal state (Estado normal): Haga clic  para circuito abierto y  para circuito cerrado.

Current state (Estado actual): muestra el estado actual del puerto. La entrada o salida se activa cuando el estado actual difiere del estado normal. Una entrada del dispositivo tiene el circuito abierto cuando está desconectado o cuando hay una tensión superior a 1 V CC.

Nota

Durante el reinicio, se abre el circuito de salida. Cuando termina el reinicio, el circuito vuelve a la posición normal. Si modifica algún ajuste de esta página, los circuitos de salida recuperan las posiciones normales, con independencia de los activadores activos.

Supervisado  : Active esta opción para que sea posible detectar y activar acciones si alguien manipula la conexión con dispositivos de E/S digital. Además de detectar si una entrada está abierta o cerrada, también puede detectar si alguien la ha manipulado (mediante un corte o cortocircuito). La supervisión de la conexión requiere hardware adicional (resistencias de final de línea) en el bucle de E/S externa.

Edge-to-Edge

Emparejamiento

El emparejamiento le permite utilizar un dispositivo Axis compatible como si fuera parte del dispositivo principal.

Audio pairing (Emparejamiento de audio) permite emparejar el dispositivo con un altavoz o micrófono de la red. Una vez emparejado, el altavoz de red actúa como un dispositivo de salida de audio en el que se pueden reproducir clips de audio y transmitir sonido a través de la cámara. El micrófono de red tomará los sonidos de los entornos circundantes y los pondrá a disposición como dispositivo de entrada de audio, que se puede aprovechar en transmisiones multimedia y grabaciones.

Importante

Para que esta característica funcione con un software de gestión de vídeo (VMS), primero debe emparejar la cámara con el altavoz o micrófono y, a continuación, agregar la cámara al VMS.

Defina un límite de "Wait between actions (hh:mm:ss) (Espera entre acciones (hh:mm:ss)" en la regla de evento cuando utilice un dispositivo de audio emparejado por red en una regla de evento con "Audio detection (Detección de audio)" como condición y "Play audio clip (Reproducir clip de audio)" como acción. Esto le ayudará a evitar la detección de bucles si el micrófono de captura capta el audio del altavoz.

Add (Añadir): Añada un dispositivo para realizar el emparejamiento.

Discover devices (Detectar dispositivos): Haga clic para buscar dispositivos en la red. Una vez escaneada la red, se mostrará una lista de dispositivos disponibles.

Nota

La lista mostrará todos los dispositivos Axis encontrados, no solo los que se pueden emparejar.

Solo se pueden encontrar dispositivos con **Bonjour** habilitado. Para habilitar **Bonjour** en un dispositivo, abra la interfaz web del dispositivo y vaya a **System (Sistema) > Network (Red) > Network discovery protocols (Protocolos de detección de red)**.

Nota

Se muestra un icono de información para los dispositivos ya emparejados. Pase el cursor sobre el icono para obtener información sobre los emparejamientos activos.

Para emparejar un dispositivo de la lista, pulse .

Select pairing type (Seleccionar tipo de emparejamiento): Seleccione una opción en la lista desplegable.

Speaker pairing (Emparejamiento de altavoces): Seleccione para emparejar un altavoz de red.

Microphone pairing (Emparejamiento de micrófono) : Seleccione para emparejar un micrófono.

Dirección: Introduzca el nombre de host o la dirección IP del altavoz de red.

Nombre de usuario: Introduzca el nombre de usuario.

Contraseña: Introduzca una contraseña para el usuario.

Close (Cerrar): Haga clic para borrar todos los campos.

Conectar: Haga clic para establecer la conexión con el dispositivo que se emparejará.

PTZ pairing (Emparejamiento de PTZ) permite emparejar un radar con una cámara PTZ para usar el autotracking. El radar autotracking para PTZ hace que la cámara PTZ realice un seguimiento de objetos a partir de la información procedente del radar acerca de las posiciones de los objetos.

Add (Añadir): Añada un dispositivo para realizar el emparejamiento.

Discover devices (Detectar dispositivos): Haga clic para buscar dispositivos en la red. Una vez escaneada la red, se mostrará una lista de dispositivos disponibles.

Nota

La lista mostrará todos los dispositivos Axis encontrados, no solo los que se pueden emparejar.

Solo se pueden encontrar dispositivos con **Bonjour** habilitado. Para habilitar **Bonjour** en un dispositivo, abra la interfaz web del dispositivo y vaya a **System (Sistema) > Network (Red) > Network discovery protocols (Protocolos de detección de red)**.

Nota

Se muestra un icono de información para los dispositivos ya emparejados. Pase el cursor sobre el icono para obtener información sobre los emparejamientos activos.

Para emparejar un dispositivo de la lista, pulse .

Select pairing type (Seleccionar tipo de emparejamiento): Seleccione una opción en la lista desplegable.

Dirección: Introduzca el nombre de host o la dirección IP de la cámara PTZ.

Nombre de usuario: Introduzca el nombre de usuario de la cámara PTZ.

Contraseña: Introduzca la contraseña de la cámara PTZ.

Close (Cerrar): Haga clic para borrar todos los campos.

Conectar: Haga clic para establecer una conexión con la cámara PTZ.

Configure radar autotracking (Configurar autotracking de radar): Haga clic para abrir y configurar el autotracking. Puede ir también a **Radar > Radar PTZ autotracking (Radar > Radar autotracking para PTZ)** para configurarlo.

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.

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.

Configuración sencilla

La configuración sencilla está destinada a usuarios con experiencia en la configuración de dispositivos Axis. La mayoría de los parámetros se pueden definir y editar desde esta página.

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 dispositivo de Axis. Para obtener más información, consulte el documento técnico "Axis Edge Vault" en *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*.

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.
- **Autorollback (Restauración automática a versión anterior)**: 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**.

Validar la instalación

Validar la instalación del radar

Nota

Esta prueba le ayudará a validar la instalación en las condiciones actuales. Los cambios en la escena pueden afectar al funcionamiento diario de la instalación.

Aunque el radar está listo para su uso tan pronto como se instala, es recomendable llevar a cabo una validación antes de empezar a utilizarlo. Así puede aumentarse la precisión del radar porque es posible identificar problemas de instalación o gestionar objetos como árboles y superficies reflectantes en la escena.

Calibre el antes de intentar validarlo.

Es buena idea realizar la validación siempre que:

- Haya objetos en la escena que desee excluir, de modo que las zonas puedan contener determinados objetos, como vegetación o superficies metálicas.
- Empareje el radar con una cámara PTZ y desee configurar la función **Radar autotracking (Autotracking de radar)**.
- La altura del soporte de montaje del radar ha cambiado.

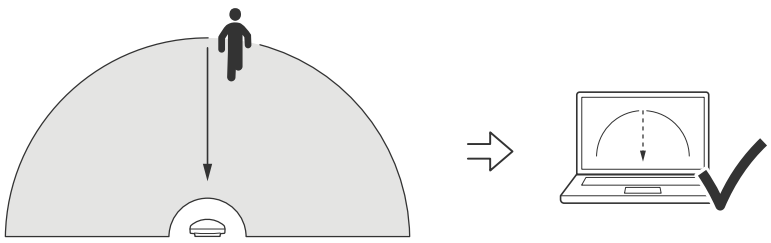
Validar el radar

Comprobar que no haya falsas detecciones

1. Compruebe que la zona de detección esté claramente despejada de la actividad humana.
2. Espere unos minutos para asegurarse de que el radar no está detectando ningún objeto estático en la zona de detección.
3. Si no hay detecciones no deseadas, puede omitir el paso 4.
4. Si hay detecciones no deseadas, obtenga información sobre cómo filtrar determinados tipos de movimiento u objetos, cambiar la cobertura o ajustar la sensibilidad de detección en .

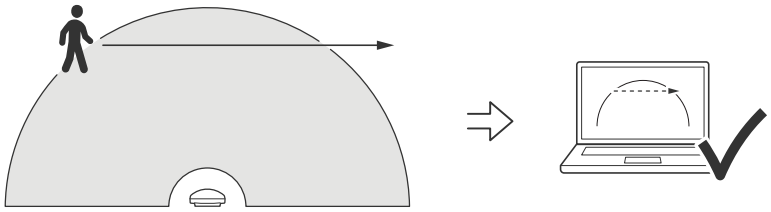
Comprobar el símbolo y la dirección de desplazamiento correctos al aproximarse al radar desde la parte frontal

1. Vaya a la interfaz web del radar y grabe la sesión. Para obtener ayuda al respecto, vaya a .
2. Empiece a 60 m delante del radar y camine directamente hacia el aparato.
3. Compruebe la sesión en la interfaz web del radar. El símbolo de clasificación como humano debe aparecer cuando se le detecte.
4. Compruebe que la interfaz web del radar muestra la dirección correcta de desplazamiento.



Comprobar el símbolo y la dirección de desplazamiento correctos al aproximarse al radar desde el lateral

1. Vaya a la interfaz web del radar y grabe la sesión. Para obtener ayuda al respecto, vaya a .
2. Empiece a 60 m del radar y atraviese directamente la zona de cobertura del radar.
3. Compruebe que la interfaz web del radar muestra el símbolo de clasificación como humano.
4. Compruebe que la interfaz web del radar muestra la dirección correcta de desplazamiento.



Cree una tabla parecida a la siguiente, que le ayudará a registrar los datos a partir de la validación.

Prueba	Correcto/Fallo	Comentario
1. Comprobar que no haya detecciones no deseadas cuando el área está despejada		
2a. Comprobar que el objeto se ha detectado con el símbolo correcto de "Humano" al aproximarse al radar desde la parte frontal		
2b. Comprobar que la dirección de desplazamiento es correcta al aproximarse al radar desde la parte frontal		
3a. Comprobar que el objeto se ha detectado con el símbolo correcto de "Humano" al aproximarse al radar desde el lateral		
3b. Comprobar que la dirección de desplazamiento es correcta al aproximarse al radar desde el lateral		

Completar la validación

Una vez haya llevado a cabo correctamente la primera parte de la validación, realice las siguientes pruebas para completar el proceso de validación.

1. Asegúrese de que ha configurado el radar y de que ha seguido las instrucciones.
2. Para realizar una validación adicional, agregue y calibre un mapa de referencia.
3. Ajuste el escenario del radar para desencadenar cuando se detecte un objeto adecuado. De forma predeterminada, **seconds until trigger (segundos hasta desencadenar)** se establece en dos segundos, pero puede cambiar esto en la interfaz web si es necesario.
4. Ajuste el radar para que grabe datos cuando se detecte un objeto adecuado.
   Consulte para obtener instrucciones.
5. Establezca la **trail lifetime (duración del rastro)** en una hora de manera que supere ampliamente el tiempo que tarda en abandonar el puesto, pasear por la zona de vigilancia y regresar al sitio. La **trail lifetime (duración del rastro)** mantendrá el seguimiento en la visualización en directo del radar durante el tiempo establecido y, una vez que haya finalizado la validación, se puede desactivar.
6. Camine a lo largo del borde del área de cobertura del radar y asegúrese de que el rastro del sistema coincida con la ruta que ha recorrido.
7. Si no está satisfecho con los resultados de la validación, vuelva a calibrar el mapa de referencia y repita la validación.

Descubrir más

Flujo y almacenamiento

Formatos de compresión de vídeo

Decida qué método de compresión de vídeo usar en función de los requisitos de visualización y de las propiedades de la red. Las opciones disponibles son:

Motion JPEG

Motion JPEG o MJPEG es una secuencia de vídeo digital compuesta por una serie de imágenes JPEG individuales. Dichas imágenes luego se muestran y se actualizan a una velocidad suficiente para crear una transmisión que muestre un movimiento constantemente actualizado. Para que el visor perciba movimiento, la velocidad debe ser de al menos 16 imágenes por segundo. La percepción de vídeo en completo movimiento se produce a 30 (NTSC) o 25 (PAL) imágenes por segundo.

La transmisión Motion JPEG utiliza cantidades considerables de ancho de banda, pero proporciona excelente calidad de la imagen y acceso a cada imagen de la transmisión.

H.264 o MPEG-4 Parte 10/AVC

Nota

H.264 es una tecnología sujeta a licencia. El producto de Axis incluye una licencia cliente de visualización H.264. Se prohíbe instalar otras copias del cliente sin licencia. Para adquirir más licencias, póngase en contacto con el distribuidor de Axis.

H.264 puede, sin comprometer la calidad de la imagen, reducir el tamaño de un archivo de vídeo digital en más de un 80 % respecto del formato Motion JPEG y en un 50 % respecto de los formatos MPEG antiguos. Esto significa que un mismo archivo de vídeo requiere menos ancho de banda de red y menos almacenamiento. O, dicho de otro modo, que se puede conseguir una calidad de vídeo más alta para una misma velocidad de bits.

H.265 o MPEG-H Parte 2/HEVC

H.265 puede, sin comprometer la calidad de la imagen, reducir el tamaño de un archivo de vídeo digital en más de un 25 % respecto de H.264.

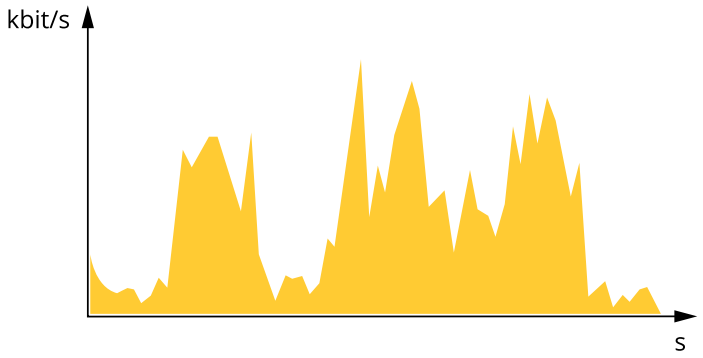
Nota

- H.265 es una tecnología sujeta a licencia. El producto de Axis incluye una licencia cliente de visualización H.265. Se prohíbe instalar otras copias del cliente sin licencia. Para adquirir más licencias, póngase en contacto con el distribuidor de Axis.
- Casi todos los navegadores web no admiten la descodificación H.265, por lo que la cámara no la admite en su interfaz web. En su lugar, puede utilizar un sistema o aplicación de gestión de vídeo que admita descodificación H.265.

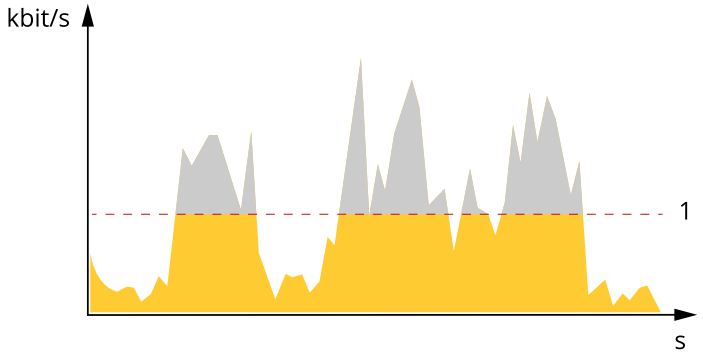
Control de velocidad de bits

El control de velocidad de bits permite gestionar el consumo de ancho de banda de un flujo de vídeo.

Velocidad de bits variable (VBR)
La velocidad de bits variable permite que el consumo de ancho de banda varíe en función del nivel de actividad de la escena. Cuanto mayor sea la actividad, más ancho de banda se necesitará. La velocidad de bits variable garantiza una calidad de imagen constante, pero es necesario asegurarse de que hay almacenamiento suficiente.



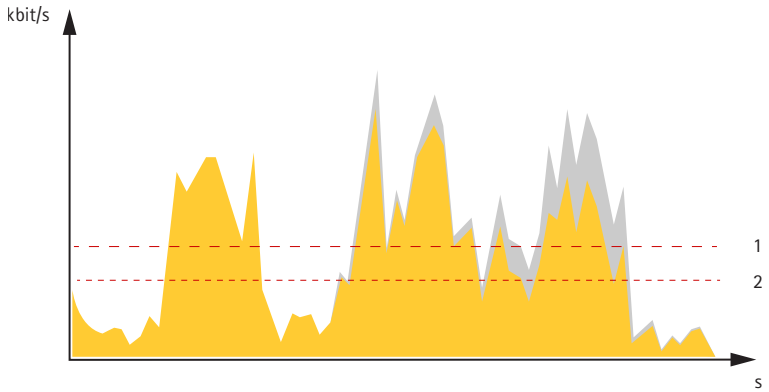
Velocidad de bits máxima (MBR)
La velocidad de bits máxima permite definir una velocidad objetivo para hacer frente a las limitaciones de velocidad de bits del sistema. La calidad de imagen o la velocidad de fotogramas puede empeorar si la velocidad de bits instantánea se mantiene por debajo de una velocidad objetivo especificada. Se puede dar prioridad a la calidad de imagen o a la velocidad de fotogramas. Es aconsejable que el valor de la velocidad de bits objetivo sea mayor que el de la prevista. Así se dispone de un margen en caso de que haya mucha actividad en la escena.



1 Velocidad de bits objetivo

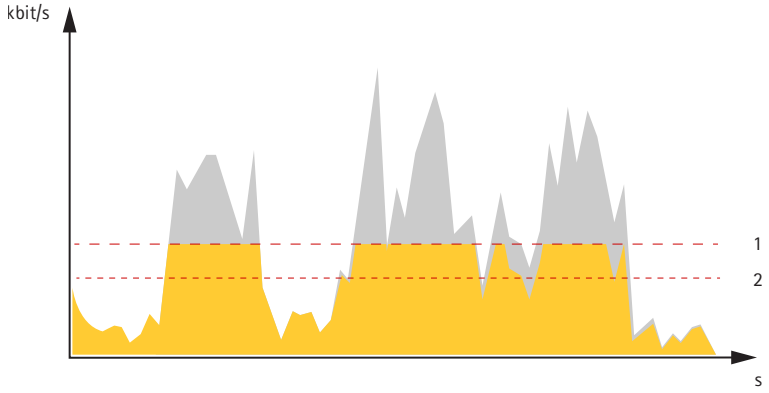
Velocidad de bits media (ABR)
Si se utiliza, la velocidad de bits se ajusta automáticamente a lo largo de un periodo de tiempo largo. De esta forma, se puede conseguir el objetivo especificado y la mejor calidad de vídeo posible con el almacenamiento disponible. La velocidad de bits es más alta en las escenas con mucha actividad que en las estáticas. Es más probable obtener una mejor calidad de imagen en escenas con mucha actividad si se utiliza la opción de velocidad de bits media. Si ajusta la calidad de imagen de forma que tenga la velocidad de bits objetivo especificada, puede definir el almacenamiento total necesario para guardar el flujo de vídeo durante un periodo especificado (periodo de retención). La velocidad de bits media se puede configurar de una de las siguientes maneras:

- Para calcular el almacenamiento necesario estimado, defina la velocidad de bits objetivo y el periodo de retención.
- Para calcular la velocidad de bits media en función del almacenamiento disponible y el periodo de retención necesario, utilice la calculadora de velocidad de bits objetivo.



1 *Velocidad de bits objetivo*
2 *Velocidad de bits real*

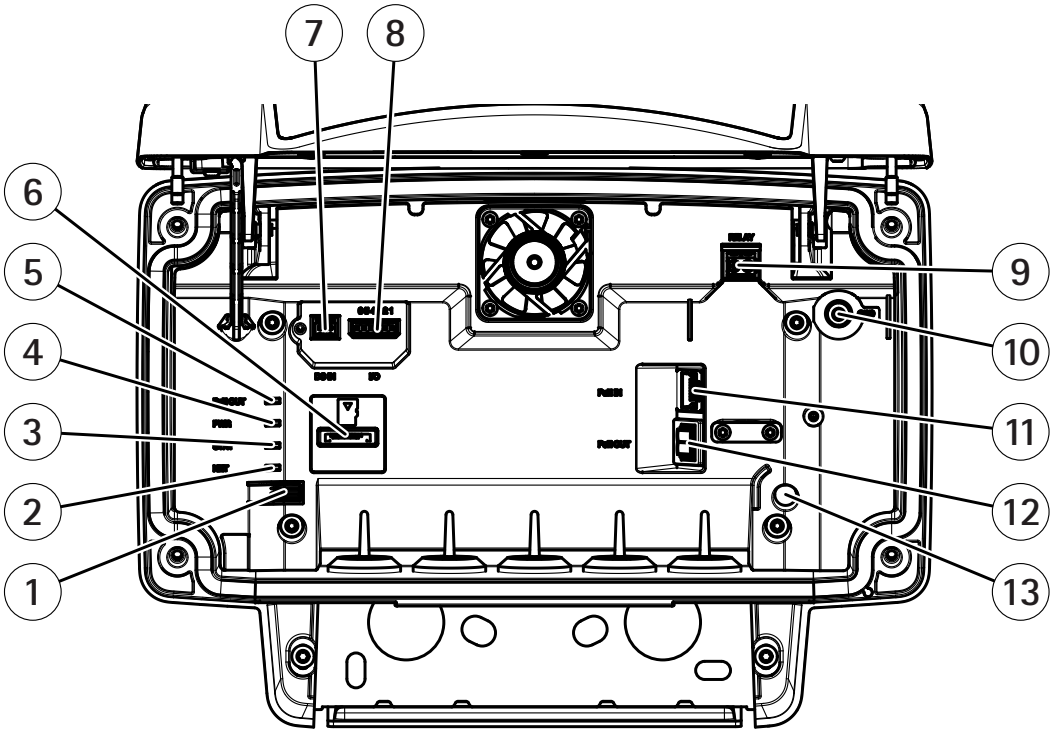
También puede activar la velocidad de bits máxima y especificar una objetivo con la opción de velocidad de bits media.



1 *Velocidad de bits objetivo*
2 *Velocidad de bits real*

Especificaciones

Guía de productos



1 *Botón de control*
2 *LED de red*
3 *LED de estado*
4 *LED de alimentación*
5 *Salida PoE LED*
6 *Ranura para tarjeta microSD*
7 *Conector de alimentación (CC)*
8 *Conector de E/S*
9 *Conector de relé*
10 *Tornillo de toma de tierra*
11 *Conector de red (entrada PoE)*
12 *Conector de red (salida PoE)*
13 *Sensor de alarma contra intrusiones*

Para conocer las especificaciones técnicas, vea .

Indicadores LED

LED de estado	Indicación
Verde	Fijo para indicar un funcionamiento normal.

LED de red	Indicación
Verde	Fijo para indicar la conexión a una red de 100 Mbit/s. Parpadea para indicar actividad en la red.
Ámbar	Fijo para indicar la conexión a una red de 10 Mbit/s. Parpadea para indicar actividad en la red.
Apagado	No hay conexión a la red.

LED de alimentación	Indicación
Verde	Funcionamiento normal.

Salida PoE LED	Indicación
Apagado	Salida PoE desactivada
Verde	Salida PoE activada

Ranura para tarjeta SD

Este dispositivo admite tarjetas microSD/microSDHC/microSDXC.

Para conocer las recomendaciones sobre tarjetas SD, consulte *axis.com*.

Los logotipos de microSD, microSDHC y microSDXC son marcas comerciales de SD-3C LLC. microSD, microSDHC, microSDXC son marcas comerciales o marcas comerciales registradas de SD-3C, LLC en Estados Unidos, en otros países o en ambos.

Botones

Botón de control

Para conocer la ubicación del botón de control, consulte .
El botón de control se utiliza para lo siguiente:

- Restablecer el producto a la configuración predeterminada de fábrica. Vea .
- Conexión a un servicio AVHS de vídeo alojado (AXIS Video Hosting System). Vea . Para conectarse, mantenga pulsado el botón durante 3 segundos hasta que el indicador de estado parpadee en color verde.

Conectores

Conector de red

Conector Ethernet RJ45 con alimentación a través de Ethernet Plus (PoE+).

⚠ PRECAUCIÓN

Riesgo de daños en el dispositivo. No alimente el dispositivo con PoE y CC.

Conector de red (salida PoE)

Alimentación a través de Ethernet IEEE 802.3at tipo 2, máx. 30 W

Use este conector para suministrar energía a otro dispositivo PoE, por ejemplo, una cámara, un altavoz exponencial o un segundo radar de Axis.

Nota

La salida PoE se habilita cuando el radar recibe alimentación a través de un midspan de 60 W (alimentación a través de Ethernet IEEE 802.3bt, tipo 3).

Nota

Si el radar recibe alimentación desde CC o midspan de 30 W, la salida de PoE se desactiva.

Nota

La longitud máxima del cable Ethernet es de 100 m en total para salida y entrada de PoE combinadas. Puede aumentarla con un PoE extender.

Nota

Si el dispositivo con PoE conectado requiere más de 30 W, puede agregar un midspan de 60 W entre el puerto de salida de PoE del radar y el dispositivo. El midspan alimenta el dispositivo y el radar de seguridad proporciona la conexión de Ethernet.

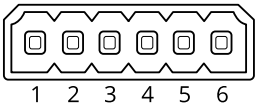
Conector de E/S

Utilizar el conector de E/S con dispositivos externos en combinación con activación de eventos y notificaciones de alarma, por ejemplo. Además del punto de referencia de 0 V CC y la alimentación (salida de CC), el conector de E/S ofrece una interfaz para:

Entrada digital – Conectar dispositivos que puedan alternar entre circuitos cerrados y abiertos, por ejemplo, sensores PIR, contactos de puertas y ventanas o detectores de cristales rotos.

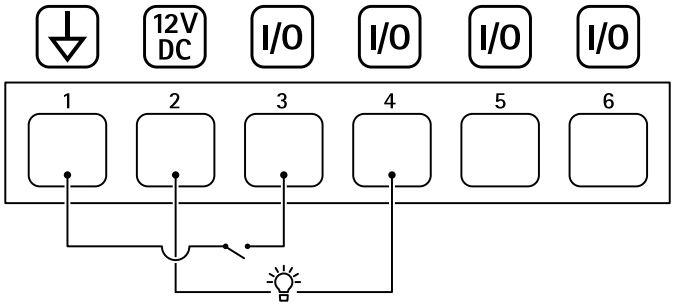
Salida digital – Conectar dispositivos externos como relés y LED. Los dispositivos conectados se pueden activar mediante la interfaz de programación de aplicaciones VAPIX®, mediante un evento o desde la interfaz web del dispositivo.

Bloque de terminales de 6 pines



Función	Pin	Notas	Especificaciones
Tierra CC	1		0 V CC
Salida de CC	2	⚠ Se puede utilizar para alimentar equipos auxiliares. Nota: Este pin solo se puede utilizar como salida de alimentación.	12 V CC Carga máx. = 50 mA
Configurable (entrada o salida)	3–6	Entrada digital: conéctela al pin 1 para activarla, o bien déjela suelta (sin conectar) para desactivarla.	0 a máx. 30 V CC
		Salida digital: conectada internamente a pin 1 (tierra CC) cuando está activa, y suelta (desconectada) cuando está inactiva. Si se utiliza con una carga inductiva, por ejemplo, un relé, conecte un diodo en paralelo a la carga como protección contra transitorios de tensión.	De 0 a un máximo de 30 V CC, colector abierto, 100 mA

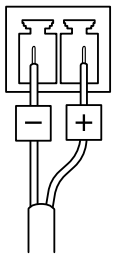
Ejemplo:



1 *Tierra CC*
2 *Salida de CC 12 V, 50 mA máx.*
3 *E/S configurada como entrada*
4 *E/S configurada como salida*
5 *E/S configurable*
6 *E/S configurable*

Conector de alimentación

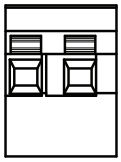
Bloque de terminales de 2 pines para la entrada de alimentación de CC. Use una fuente de alimentación limitada (LPS) que cumpla los requisitos de seguridad de baja tensión (SELV) con una potencia nominal de salida limitada a ≤100 W o una corriente nominal de salida limitada a ≤5 A.



⚠ PRECAUCIÓN

Riesgo de daños en el dispositivo. No alimente el dispositivo con PoE y CC.

Conector de relé



⚠ PRECAUCIÓN

Utilice cables de un solo núcleo para el conector de relé.

Función	Especificaciones
Tipo	Normalmente abierto
Clasificación	24 V CC/5 A
Aislamiento de otro circuito	2,5 kV

Limpie su dispositivo

Puede limpiar su dispositivo con agua tibia y jabón suave no abrasivo.

AVISO

- Los productos químicos agresivos pueden dañar el dispositivo. No utilice productos químicos como un limpiacristales o acetona para limpiar el dispositivo.
- No rocíe detergente directamente sobre el dispositivo. En su lugar, rocía detergente sobre un paño no abrasivo y úselo para limpiar el dispositivo.
- Evite limpiar en contacto directo con la luz o a temperaturas elevadas, ya que puede provocar manchas.

1. Utilice un aerosol de aire comprimido para quitar el polvo y la suciedad suelta del dispositivo.
2. Si es necesario, limpie el dispositivo con un paño de microfibra suave humedecido con agua tibia y jabón suave y no abrasivo.
3. Para evitar que queden manchas, seque el dispositivo con un paño limpio y no abrasivo.

Localización de problemas

Restablecimiento a la configuración predeterminada de fábrica

Importante

Es preciso tener cuidado si se va a restablecer la configuración predeterminada de fábrica. Todos los valores, incluida la dirección IP, se restablecerán a la configuración predeterminada de fábrica.

Para restablecer el producto a la configuración predeterminada de fábrica:

1. Desconecte la alimentación del producto.
2. Mantenga pulsado el botón de control mientras vuelve a conectar la alimentación. Vea .
3. Mantenga pulsado el botón de control durante 15-30 segundos hasta que el indicador LED de estado parpadee en color ámbar.
4. Suelte el botón de control. El proceso finalizará cuando el indicador LED de estado se ilumine en color verde. 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
5. Utilice las herramientas del software de instalación y gestión para asignar una dirección IP, configurar la contraseña y acceder al dispositivo.
   Las herramientas de software de instalación y gestión están disponibles en las páginas de servicio técnico en *axis.com/support*.

También puede restablecer los parámetros a la configuración predeterminada de fábrica a través de la interfaz web del dispositivo. Vaya a **Mantenimiento** > **Configuración predeterminada de fábrica** y haga clic en **Predeterminada**.

Comprobar la versión de AXIS OS

AXIS OS determina la funcionalidad de nuestros dispositivos. Cuando solucione un problema, le recomendamos que empiece comprobando la versión de AXIS OS actual. La versión más reciente podría contener una corrección que solucione su problema concreto.

Para comprobar la versión de AXIS OS:

1. Vaya a la interfaz web del dispositivo > **Status (estado)**.
2. Consulte la versión de AXIS OS en **Device info (información del dispositivo)**.

Actualización de AXIS OS

Importante

- Cuando actualice el software del dispositivo se guardan los ajustes preconfigurados y personalizados (siempre que dicha función esté disponible en el AXIS OS nuevo), si bien Axis Communications AB no puede garantizarlo.
- Asegúrese de que el dispositivo permanece conectado a la fuente de alimentación durante todo el proceso de actualización.

Nota

Al actualizar el dispositivo con el AXIS OS más reciente en la pista activa, el producto obtiene las últimas funciones disponibles. Lea siempre las instrucciones de actualización y las notas de versión disponibles en cada nueva versión antes de la actualización. Para encontrar el AXIS OS y las notas de versión más recientes, consulte *axis.com/support/device-software*.

1. Descargue en su ordenador el archivo de AXIS OS, disponible de forma gratuita en *axis.com/support/device-software*.

2. Inicie sesión en el dispositivo como administrador.
3. Vaya a **Maintenance > AXIS OS upgrade (mantenimiento > actualización de AXIS OS)** y haga clic en **Upgrade (actualizar)**.

Una vez que la actualización ha terminado, el producto se reinicia automáticamente.

Problemas técnicos, consejos y soluciones

Si no encuentra aquí lo que busca, pruebe a visitar la sección de solución de problemas en *axis.com/support*.

Problemas para actualizar AXIS OS

Fallo en la actualización de AXIS OS	Cuando se produce un error en la actualización, el dispositivo vuelve a cargar la versión anterior. La causa más frecuente es que se ha cargado el archivo de AXIS OS incorrecto. Asegúrese de que el nombre del archivo de AXIS OS corresponde a su dispositivo e inténtelo de nuevo.
Problemas tras la actualización de AXIS OS	Si tiene problemas después de actualizar, vuelva a la versión instalada anteriormente desde la página de **Mantenimiento**.

Problemas al configurar la dirección IP

El dispositivo se encuentra en una subred distinta	Si la dirección IP prevista para el dispositivo y la dirección IP del ordenador utilizado para acceder al dispositivo se encuentran en subredes distintas, no podrá configurar la dirección IP. Póngase en contacto con el administrador de red para obtener una dirección IP.
La dirección IP ya la utiliza otro dispositivo	Desconecte el dispositivo de Axis de la red. Ejecute el comando ping (en una ventana de comando/DOS, escriba `ping` y la dirección IP del dispositivo): • Si recibe `Reply from <IP address>: bytes=32; time=10...`, significa que la dirección IP podría estar en uso por otro dispositivo de la red. Solicite una nueva dirección IP al administrador de red y vuelva a instalar el dispositivo. • Si recibe: `Request timed out`, significa que la dirección IP está disponible para su uso con el dispositivo de Axis. Compruebe el cableado y vuelva a instalar el dispositivo.
Posible conflicto de dirección IP con otro dispositivo de la misma subred	Se utiliza la dirección IP estática del dispositivo de Axis antes de que el servidor DHCP configure una dirección dinámica. Esto significa que, si otro dispositivo utiliza la misma dirección IP estática predeterminada, podría haber problemas para acceder al dispositivo.

No se puede acceder al dispositivo desde un navegador

No se puede iniciar sesión	Cuando HTTPS esté activado, asegúrese de utilizar el protocolo correcto (HTTP o HTTPS) al intentar iniciar sesión. Puede que tenga que escribir manualmente `http` o `https` en el campo de dirección del navegador. Si se pierde la contraseña para la cuenta de root, habrá que restablecer el dispositivo a los ajustes predeterminados de fábrica. Vea .

El servidor DHCP ha cambiado la dirección IP	Las direcciones IP obtenidas de un servidor DHCP son dinámicas y pueden cambiar. Si la dirección IP ha cambiado, acceda a la utilidad AXIS IP Utility o AXIS Device Manager para localizar el dispositivo en la red. Identifique el dispositivo utilizando el modelo o el número de serie, o por el nombre de DNS (si se ha configurado el nombre). Si es necesario, se puede asignar una dirección IP estática manualmente. Para ver las instrucciones, vaya a *axis.com/support*.
Error de certificado cuando se utiliza IEEE 802.1X	Para que la autenticación funcione correctamente, los ajustes de fecha y hora del dispositivo de Axis se deben sincronizar con un servidor NTP. Vaya a **Sistema > Fecha y hora**.

Se puede acceder al dispositivo localmente pero no externamente

Para acceder al dispositivo externamente, le recomendamos que use una de las siguientes aplicaciones para Windows®:

- AXIS Camera Station Edge: gratuito, ideal para sistemas pequeños con necesidades de vigilancia básicas.
- AXIS Camera Station 5: versión de prueba de 30 días gratuita, ideal para sistemas de tamaño pequeño y medio.
- AXIS Camera Station Pro: versión de prueba de 90 días gratuita, ideal para sistemas de tamaño pequeño y medio.

Para obtener instrucciones y descargas, vaya a *axis.com/vms*.

No se puede conectar a través del puerto 8883 con MQTT a través de SSL

El cortafuegos bloquea el tráfico que utiliza el puerto 8883 por considerarse inseguro.	En algunos casos, el servidor/intermediario podría no proporcionar un puerto específico para la comunicación MQTT. Aun así, puede ser posible utilizar MQTT a través de un puerto utilizado normalmente para el tráfico HTTP/HTTPS. • Si el servidor/intermediario es compatible con WebSocket/WebSocket Secure (WS/WSS), normalmente en el puerto 443, utilice este protocolo en su lugar. Consulte con el proveedor del servidor/intermediario para comprobar si es compatible con WS/WSS y qué puerto y basepath usar. • Si el servidor/broker admite ALPN, el uso de MQTT puede negociarse a través de un puerto abierto, como 443. Consulte a su proveedor de servidores/brokers si admite ALPN y qué protocolo y puerto ALPN debe utilizar.

Consideraciones sobre el rendimiento

Al configurar el sistema, es importante tener en cuenta cómo los diferentes ajustes y situaciones afectan al ancho de banda necesario (la velocidad de bits).

Los siguientes factores son los más importantes que se deben considerar:

- Un uso denso de la red debido a una infraestructura deficiente afecta al ancho de banda.

T10145149_es

2025-06 (M31.2)