AXIS Perimeter Defender

AXIS Perimeter Defender
AXIS Perimeter Defender PTZ Autotracking

Manual del usuario

Índice

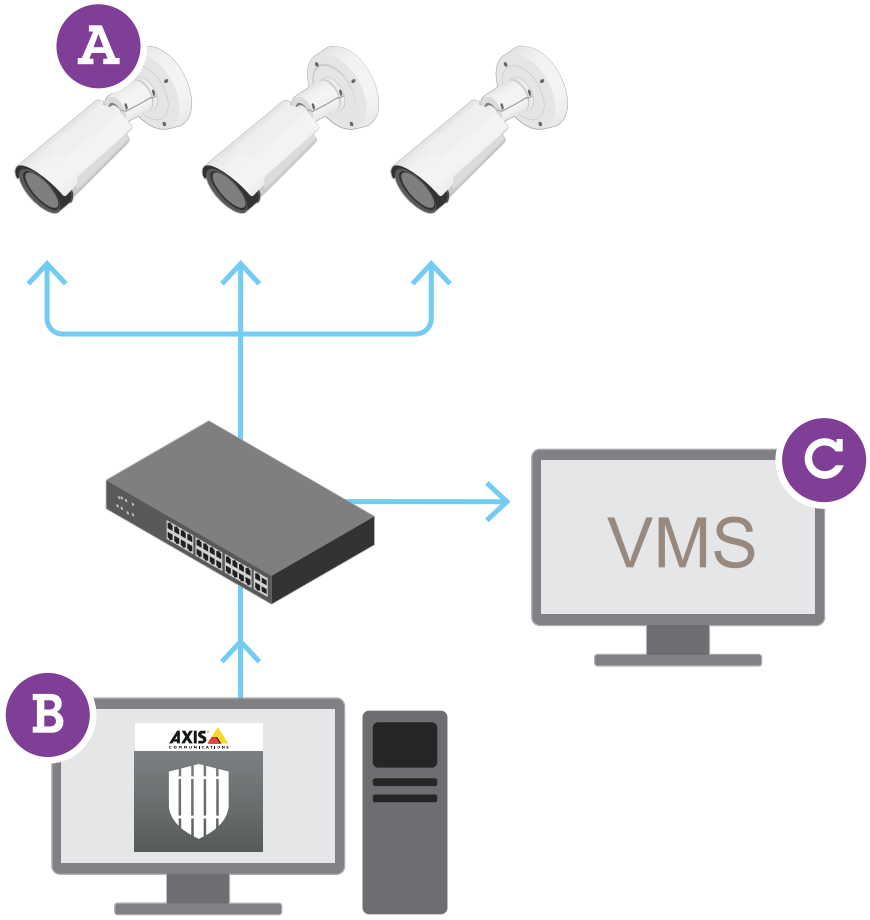
AXIS Perimeter Defender

AXIS Perimeter Defender es una aplicación para la vigilancia y la protección perimetral. Es ideal para la protección de un perímetro de alta seguridad en el que es necesario reforzar el sistema de control de acceso físico con una detección de intrusión fiable.

AXIS Perimeter Defender está diseñado principalmente para la denominada protección de zona estéril, por ejemplo a lo largo de una barrera que marca un límite. El término de zona estéril hace referencia a una zona en la no debería haber personas.

Utilice AXIS Perimeter Defender en un entorno exterior para:

- Detectar personas en movimiento.
- Detectar vehículos en movimiento, sin discriminar entre tipos de vehículos.



Esta cámara puede ejecutar la aplicación en modo de calibración, modo IA o ambos modos en combinación. Si decide ejecutarlo solo en modo IA, el montaje de la cámara es más flexible y no es necesario calibrar las cámaras.

AXIS Perimeter Defender consta de una interfaz de escritorio (B), desde la que se instala y configura la aplicación en las cámaras (A). A continuación, puede configurar el sistema para enviar alarmas al software de gestión de vídeo (C).

AXIS Perimeter Defender PTZ Autotracking es un complemento para la aplicación AXIS Perimeter Defender, mediante la misma interfaz de escritorio. Con el complemento se puede emparejar una cámara visual o térmica fija con una cámara PTZ de la línea de Q de AXIS. De este modo, puede mantener una cobertura de detección

continua de una escena con la cámara fija, mientras que la cámara PTZ realizará un seguimiento automático y le proporcionará vistas más cercanas de los objetos detectados.

Importante

AXIS Perimeter Defender PTZ Autotracking requiere calibración de las cámaras fijas y PTZ.

AXIS Perimeter Defender ofrece los siguientes tipos de escenarios de detección:

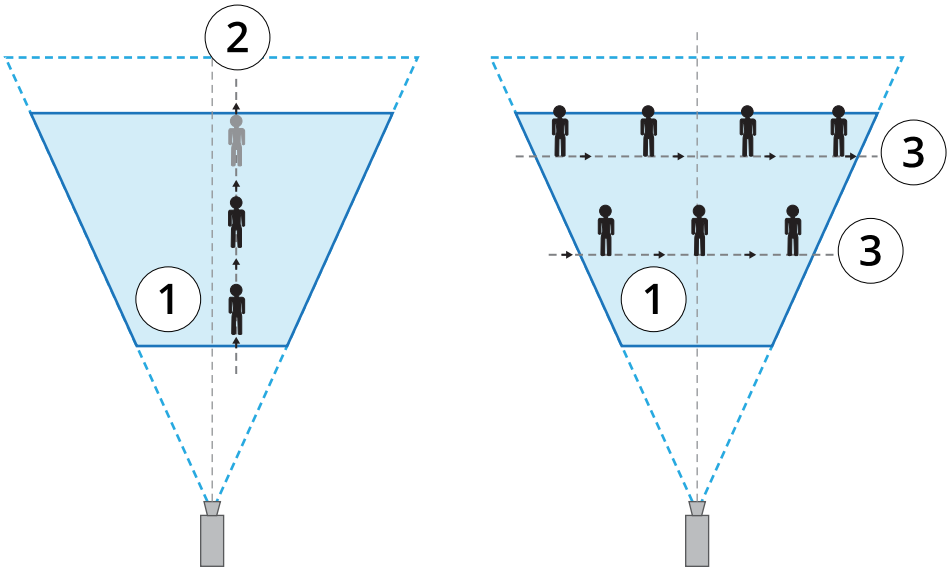
- **Intrusión**: activa una alarma cuando una persona o un vehículo entra en una zona definida en el suelo (desde cualquier dirección y con cualquier trayectoria).
- **Merodeo**: activa una alarma cuando una persona o un vehículo permanece en una zona definida en el suelo durante un tiempo superior a un número de segundos predefinido.
- **Traspaso de zonas**: activa una alarma cuando una persona o un vehículo atraviesan dos o más zonas definidas en el suelo en una secuencia determinada.
- **Condicional**: activa una alarma cuando una persona o un vehículo entra en una zona definida en el suelo sin pasar primero por otra zona o zonas definidas en el suelo.

¿Cómo funciona?

Detección de objetos

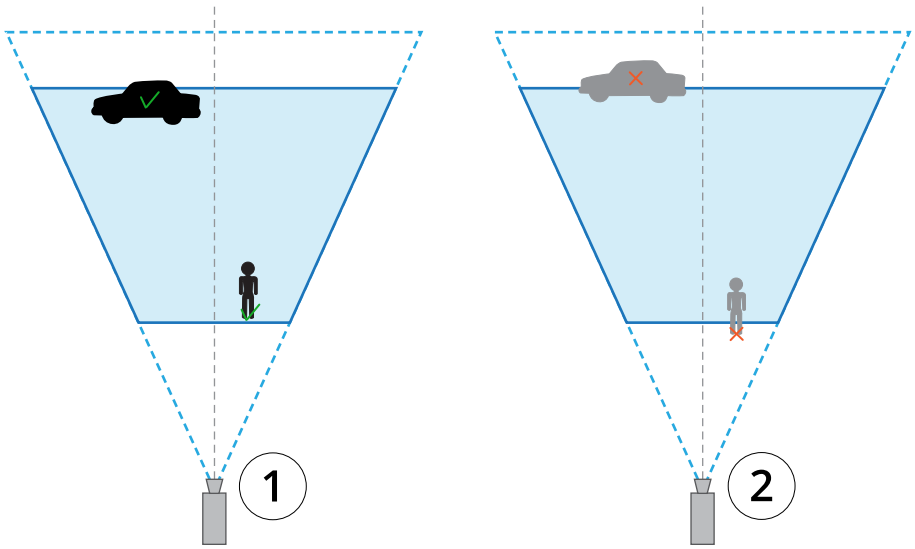
AXIS Perimeter Defender puede detectar personas o vehículos en movimiento. Para detectar:

- La persona o vehículo debe estar totalmente visible en la zona de detección durante al menos tres segundos.
- Un vehículo puede medir hasta 12 metros de largo (con el modo IA no hay longitud máxima).
- Las personas o vehículos deben moverse visiblemente en el campo de visión de la cámara. Esto significa que la tasa de detección de una persona que se acerca a la cámara en una línea recta es inferior en comparación con la de una persona que camina de forma perpendicular al campo de visión de la cámara.



1 Zona de detección
2 Persona alejándose caminando de la cámara
3 Personas caminando perpendicularmente hacia el campo de visión de la cámara

- El punto de detección debe estar dentro de la zona de detección. El punto de detección está ubicado a los pies de una persona o en el centro de un vehículo.



1 Punto de detección dentro de la zona de detección
2 Punto de detección fuera de la zona de detección

Una vez detectado, AXIS Perimeter Defender sigue realizando el seguimiento de la persona o vehículo, aunque se oculte parcialmente, por ejemplo cuando el cuerpo de una persona está oculto detrás de un automóvil pero la cabeza sigue visible.

Si una persona o un vehículo detectados dejan de moverse durante unos segundos, AXIS Perimeter Defender deja de realizar el seguimiento. Si empiezan a moverse de nuevo transcurridos menos de 15 segundos, la aplicación sigue continúa el seguimiento. Si la persona estaba en una zona de traspaso de zona, no hay ninguna garantía de que el escenario se active correctamente.

¿Cómo funciona Autotracking PTZ?

En AXIS Perimeter Defender PTZ Autotracking, una cámara fija y una cámara PTZ funcionan en conjunto. Cuando la cámara fija detecta personas o vehículos en movimiento, envía los datos de ubicación de los objetos a la cámara PTZ emparejada. Mientras los objetos permanezcan dentro del campo de visión de la cámara fija, la cámara PTZ puede seguirlos automáticamente y ajustar el nivel de zoom para mantenerlos visibles.

Condiciones en las que las detecciones se pueden retrasar o perder

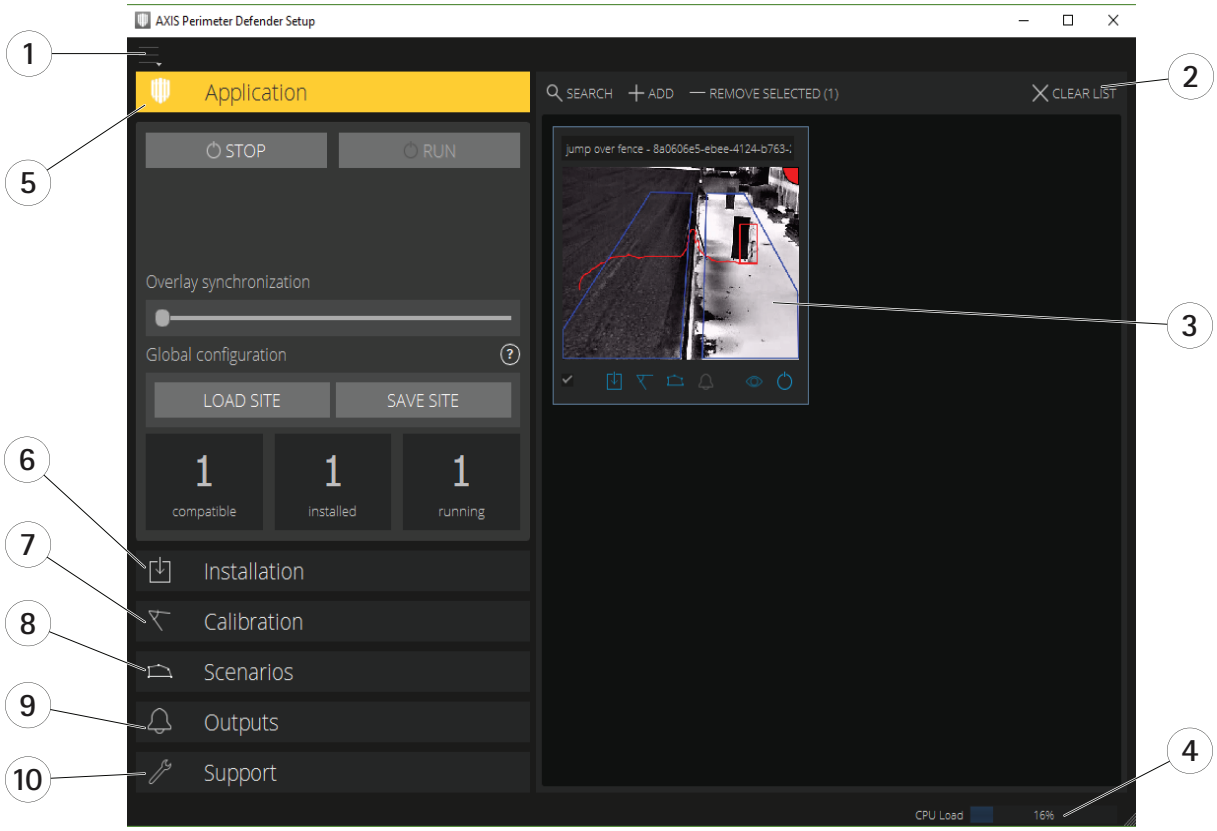
- Niebla
- Luz que incide directamente en la cámara
- Luz insuficiente
- Imagen con ruido excesivo

Situaciones que pueden activar falsas alarmas

- Personas o vehículos ocultos parcialmente. Por ejemplo, una furgoneta pequeña que aparece desde detrás de una pared puede parecer una persona, ya que la parte visible es alta y estrecha.
- Insectos en el objetivo de la cámara. Tenga en cuenta que las cámaras de día y noche con luces infrarrojas atraen a insectos y arañas.
- La combinación de faros de vehículos y lluvia intensa.
- Animales de tamaño humano, sobre todo si se han seleccionado tipos de acercamiento adicionales como agachado/cuclillas o reptar en la pestaña **Scenarios(Escenarios)**.
- Luz intensa que produce sombras.

La interfaz de usuario

La interfaz de AXIS Perimeter Defender le permite, por ejemplo, calibrar dispositivos, configurar escenarios y realizar acciones para varios dispositivos. La configuración remota permite la configuración desde cualquier lugar donde haya una conexión de red.



1 *Ajustes de la interfaz, on page 7*
2 *Maneje los dispositivos. Vea Agregar dispositivos, on page 17.*
3 *Vista en vivo, on page 8*
4 *Indicador de carga de CPU. Vea Carga de la CPU, on page 12.*
5 *Pestaña Aplicaciones, on page 9*
6 *Pestaña Instalación, on page 10*
7 *Pestaña de calibración, on page 10*
8 *Pestaña Escenarios, on page 10*
9 *Pestaña Salida, on page 11*
10 *Pestaña de soporte, on page 11*

Ajustes de la interfaz

El menú de ajustes de la interfaz contiene:

Configuración de carpeta –

Ruta de configuración del dispositivo: Seleccione dónde se almacenan archivos temporales y el vídeo de calibración.

Ruta de configuración de la instalación: Seleccione dónde se almacenan los archivos de configuración desde las rutas de carga.

Contraseñas de la cámara – Consulte las contraseñas que se están utilizando y añada nuevas contraseñas. Las contraseñas no se almacenan una vez que el usuario sale de la aplicación.

Administrar paquetes de clips de demostración – Importar o eliminar clips de demostración.

Activar el modo de velocidad de fotogramas completa – Cambiar la velocidad de fotogramas en la vista en directo. Vea *Carga de la CPU, on page 12*.

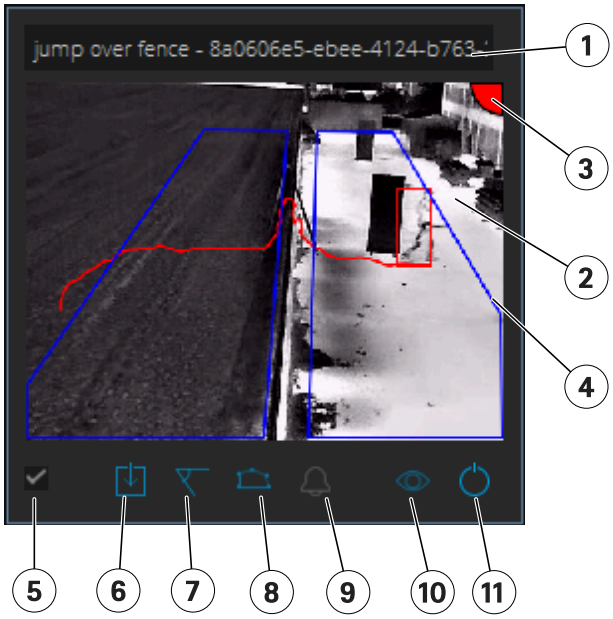
Mostrar en pies y pulgadas – Cambiar entre unidades métricas e imperiales.

Cambiar idioma – Cambiar el idioma de la aplicación.

Acerca de – Consulte la versión del programa de configuración de AXIS Perimeter Defender Setup.

Vista en vivo

Todos los dispositivos conectados reciben una vista en directo en la interfaz principal. La vista en directo proporciona el estado del dispositivo y un acceso rápido a las funciones principales.



1. Nombre del dispositivo – Haga clic para editar el nombre del dispositivo. Siempre incluye la dirección IP y el número MAC del dispositivo. Coloque el cursor sobre el nombre para mostrar la relación de aspecto utilizada para el análisis, que proporciona la cobertura máxima de campo de visión, y para ver si el dispositivo se encuentra en una conexión remota.

2. Imagen en directo – En el modo de vista general, la velocidad de fotograma es de 1 fps. Haga doble clic para maximizar la imagen y aumentar la velocidad de fotogramas a 8 fps.

3. Estado de la alarma – El estado de la alarma solo es visible si la superposición está activa y AXIS Perimeter Defender está instalado, configurado y en ejecución. Gris significa que la funcionalidad de alarma no está activa o que los ajustes de configuración se están cargando. Verde significa que la funcionalidad de alarma está activa. Rojo significa que se ha activado una alarma.

4. Zonas de detección – Las zonas de detección solo son visibles si la superposición está activa y AXIS Perimeter Defender está instalado, configurado y en ejecución.

5. Casilla de verificación de selección – Para seleccionar varios dispositivos, utilice esta casilla de verificación.

6. Estado de la instalación y botón de acceso rápido – Sitúe encima el puntero del ratón para mostrar la versión de AXIS Perimeter Defender instalada en el dispositivo. Si en lugar del icono aparece , significa que hay disponible una versión más reciente. Haga clic para abrir la pestaña Instalación del dispositivo. Gris significa que el dispositivo no está instalado. Naranja significa que el dispositivo está instalado, pero no tiene una licencia válida. Azul significa que el dispositivo está instalado con una licencia válida.

7. Estado de calibración y botón de acceso rápido – Haga clic para abrir la pestaña Calibración del dispositivo. Gris significa que el dispositivo no está calibrado. Azul significa que el dispositivo está calibrado.

8. Estado de los escenarios y botón de acceso rápido – Haga clic para abrir la pestaña Escenarios del dispositivo. Gris significa que no se ha definido ningún escenario. Azul significa que se ha definido al menos un escenario.

9. Estado de las salidas y botón de acceso rápido – Haga clic para abrir la pestaña Salida del dispositivo. Gris significa que no se han configurado salidas. Azul significa que se ha configurado al menos una salida.

10. Estado de la superposición y botón de activación/desactivación – Haga clic para activar y desactivar la superposición. Gris significa que la superposición está inactiva. Azul significa que la superposición está activa. La superposición se muestra como un cuadro delimitador alrededor de los objetos detectados, así como un recorrido que muestra la trayectoria de los objetos.

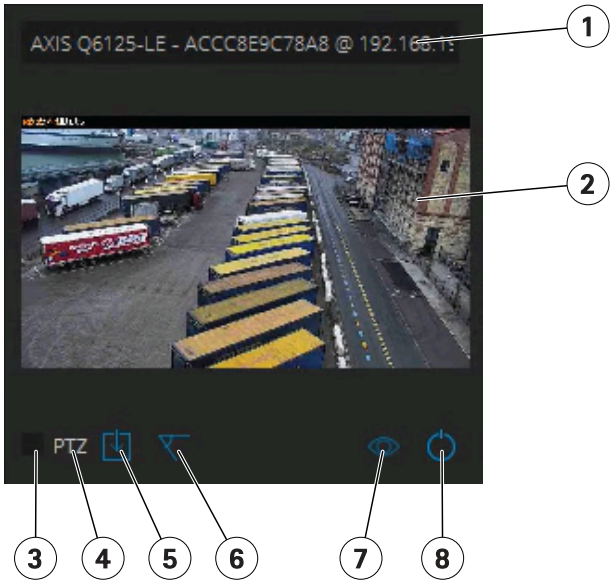
11. Estado de ejecución y botón de activación/desactivación – Haga clic para ejecutar/detener la aplicación en el dispositivo. Gris significa que la aplicación está detenida. Azul significa que se está ejecutando.

Nota

La superposición solo está disponible si hay disponible una conexión directa desde el dispositivo al equipo del usuario; es decir, si no hay firewalls o similares que impidan la conexión al puerto de superposición del dispositivo.

Visualización en directo: PTZ Autotracking

La visualización en directo para dispositivos que tienen instalado AXIS Perimeter Defender PTZ Autotracking difiere ligeramente de la visualización en directo normal.



1 *Nombre del dispositivo*
2 *Imagen en directo*
3 *Casilla de verificación de selección*
4 *Indica que el dispositivo utiliza AXIS Perimeter Defender PTZ Autotracking*
5 *Estado de instalación y botón de acceso rápido*
6 *Estado de calibración y botón de acceso rápido*
7 *Estado de superposición y botón de alternar*
8 *Estado de ejecución y botón de alternar*

Pestaña Aplicaciones

- **Run (Ejecutar)**: Inicia la analítica en los dispositivos seleccionados.
- **Stop (Detener)**: Detiene la analítica en los dispositivos seleccionados.
- **Load Site (Cargar sitio)**: Carga un sitio (instalación) guardado anteriormente, es decir, los dispositivos y sus respectivos archivos de configuración

- **Save Site (Guardar sitio)**: Guarda el sitio (instalación) actual, es decir, guarda toda la información de los dispositivos y sus respectivos archivos de configuración
- **Overlay synchronization (Sincronización de superposición)**: Controla la sincronización de la superposición de metadatos de AXIS Perimeter Defender. Este control deslizante controla el retraso entre la superposición de metadatos y las imágenes recibidas para compensar una transmisión de imágenes más lenta en comparación con los metadatos. El valor del control deslizante indica el retraso establecido para la cámara seleccionada actualmente. Si hay más de una cámara conectada, el valor indicado es el de la primera cámara seleccionada. Al cambiar el valor del control deslizante, se cambia el retraso para todas las cámaras seleccionadas.

También se puede ver el número de dispositivos compatibles agregados, el número total de dispositivos con AXIS Perimeter Defender instalado y el número de dispositivos en los que se ejecuta el análisis.

Pestaña Instalación

- **Application: Install (Aplicación: Instalar)**: Instala la aplicación en los dispositivos seleccionados.
- **Application: Uninstall (Aplicación: Desinstalar)**: Desinstala la aplicación en los dispositivos seleccionados.
- **Licence: Install (Licencia: Instalar)**: Instala la licencia en los dispositivos seleccionados.

Pestaña de calibración

- **Automatic (Automática)**: Realiza una calibración automática de los dispositivos seleccionados.
- **Manual**: Realiza una calibración manual de los dispositivos seleccionados.

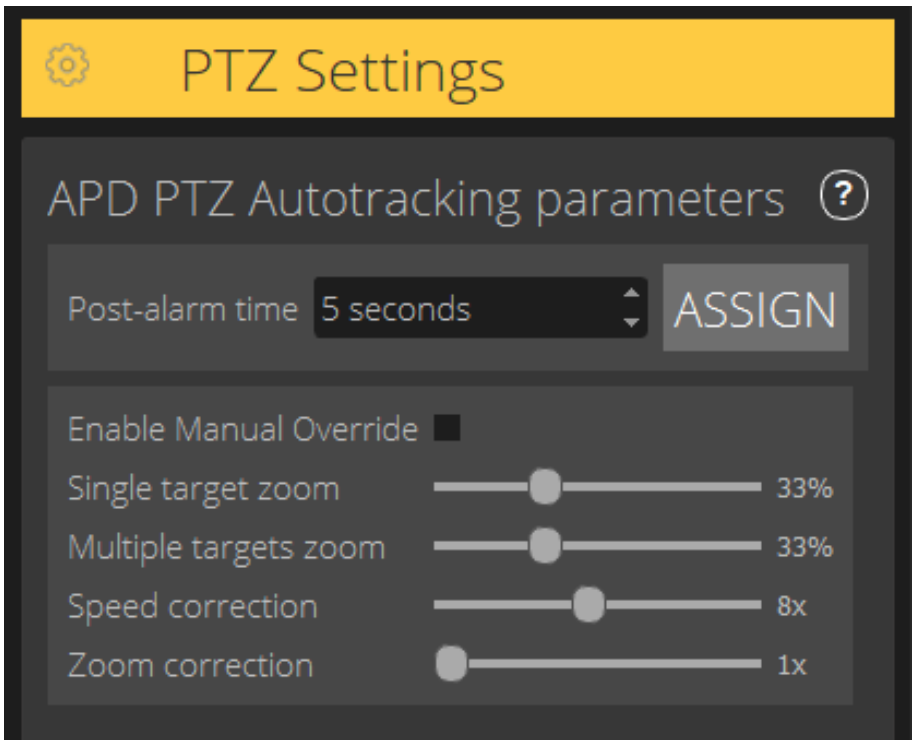
Pestaña Escenarios

- **Global parameters (Parámetros globales)**: Se aplican a todos los escenarios.
- **Advanced scenarios (Escenarios avanzados)**: Permite crear escenarios de intrusión, merodeo, traspaso de zona y condicionales.

Pestaña PTZ settings (Configuración PTZ)

Nota

Esta pestaña solo se muestra si dispone del complemento AXIS Perimeter Defender PTZ Autotracking.



- **Post-alarm time (Tiempo posterior a la alarma)**: Define el tiempo que debe transcurrir antes de que la cámara PTZ vuelva a su posición de inicio, una vez que el objeto para el que ha realizado el seguimiento ha desaparecido de la vista.
- **Enable manual override (Habilitar sustitución manual)**: Cuando se activa, el operador puede tomar el control de la cámara PTZ con un joystick, desde el VMS o en la página web de la cámara.
- **Single target zoom (Zoom en objetivo único)**: Ajusta el nivel de zoom para el seguimiento de un objetivo único. Un valor más alto proporciona mejores posibilidades para la identificación, pero también aumenta el riesgo de perder objetos en movimiento rápido.
- **Multiple targets zoom (Zoom en objetivos múltiples)**: Ajusta el nivel de zoom para el seguimiento de múltiples objetivos.
- **Speed correction (Corrección de velocidad)**: Ajusta la velocidad de seguimiento para mantener los objetos en movimiento rápidamente centrados en la imagen de la cámara PTZ. Tenga en cuenta que un valor alto puede dar lugar a inestabilidad en el seguimiento.
- **Zoom correction (Corrección de zoom)**: Un valor más alto aumenta el nivel de zoom para objetos cercanos al borde del campo de visión de la cámara PTZ.

Pestaña Salida

- **Configure (Configurar)**: Abre la página web del dispositivo para crear y configurar alarmas.
- **Test alarm (Probar alarma)**: Prueba la alarma configurada para el dispositivo.
- **Post-alarm time: Assign (Tiempo posterior a la alarma: Asignar)**: Ajusta el tiempo posterior a la alarma.

Pestaña de soporte

- **Load (Cargar)**: Carga la configuración de copia de seguridad para los dispositivos seleccionados. Esto es especialmente útil para una restauración rápida tras un error del dispositivo o una desinstalación accidental. La configuración incluye:

- Licencia
- Parámetros
- Calibración y escenarios

– Vídeo de calibración

- **Save (Guardar)**: Crea una copia de seguridad de la configuración de los dispositivos seleccionados.
- **Clear (Borrar)**: Borra la calibración y los escenarios de los dispositivos seleccionados. Esto es útil si las cámaras se han movido, puesto que las zonas de calibración y detección ya no son válidas.
- **View application log (Ver registro de la aplicación)**: Muestra el registro interno de AXIS Perimeter Defender.
- **Export support log (Exportar registro de soporte)**: Genera un archivo que contiene información detallada. Incluya siempre este archivo al realizar una solicitud de soporte técnico.

Carga de la CPU

El indicador de carga de la CPU indica la carga actual de la CPU del equipo en tiempo real. Una carga de la CPU excesiva podría provocar que un equipo o aplicación no respondiera. Asegúrese de cerrar otras aplicaciones cuando utilice la configuración de AXIS Perimeter Defender para sacar el máximo provecho a la asignación de CPU. Si la carga de la CPU es demasiado alta e intenta añadir un dispositivo, el sistema emite una advertencia.

Cada dispositivo añadido consume recursos de la CPU del ordenador host al descodificar y monitorizar la transmisión de vídeo. Para limitar el impacto en el equipo host, las secuencias de vídeo de dispositivos añadidos se muestran a una velocidad de fotograma reducida (aproximadamente 1 fps) de forma predeterminada. La velocidad de fotogramas normal (aproximadamente 8 fps) se restablece cuando se maximizan las secuencias o durante el proceso de calibración.

Importante

Enable full frame rate mode (Activar el modo de velocidad de fotogramas completa) puede provocar que la interfaz no responda si se conecta a un gran número de cámaras o cuando utiliza un ordenador de baja potencia.

Mostrar una demostración de AXIS Perimeter Defender

Para fines de demostración, AXIS Perimeter Defender y AXIS Perimeter Defender PTZ Autotracking vienen preinstalados con algunos clips de demostración que se pueden utilizar para demostrar el análisis sin necesidad de tener una cámara instalada activa. Los clips de demostración muestran el tipo de resultados de detección y seguimiento automático que se pueden esperar en diferentes entornos.

1. Vaya a **Application > Add > Demo Clips (Aplicación > Añadir > Clips de demostración)** y realice una o varias de las acciones siguientes:
   – Filtre los clips de demostración según su tipo.
   – Seleccione al menos un clip de demostración.
2. Para añadir los clips de demostración, haga clic en **Add Selected Demo Clips (Agregar clips de demostración seleccionados)**.

Una vez añadidos, los clips de demostración se muestran como secuencias de vídeo estándar en la interfaz. La calibración está disponible y el análisis ya está activado para que el usuario pueda ver inmediatamente los resultados de análisis y seguimiento automático en la secuencia de vídeo. Los análisis y el seguimiento automático se pueden detener o iniciar haciendo clic en el estado de ejecución en la vista en directo o en los botones **Run (Ejecutar)** o **Stop (Detener)** del panel izquierdo.

La calibración y el emparejamiento se pueden modificar y rehacer. De forma similar, se pueden agregar, eliminar y modificar los escenarios de detección.

La pestaña **Support (Soporte)** del panel izquierdo incluye un botón **Clear (Limpiar)** que le permite revertir la calibración y los escenarios a los valores originales. No es posible eliminar por completo la calibración.

Cómo funciona

El proceso de instalación de AXIS Perimeter Defender y AXIS Perimeter defender PTZ Autotracking difiere ligeramente.

Introducción a AXIS Perimeter Defender

Debe seguir los siguientes pasos para poner en marcha su instalación con AXIS Perimeter Defender:

1. Monte la cámara. Vea *Montar la cámara, on page 13*.
2. Descargue e instale el software en su ordenador. Vea *Instalar el software en el ordenador, on page 16*.
3. Conéctese a sus dispositivos. Vea *Agregar dispositivos, on page 17*.
4. Instale AXIS Perimeter Defender en cada dispositivo. Vea *Instalar software en dispositivos, on page 18*.

Nota

No necesita calibrar solo los dispositivos que se ejecutan en modo IA. Para ejecutar dispositivos en modo de calibración y modo IA simultáneamente, es necesario calibrarlos.

5. Calibre los dispositivos. Vea *Calibrar - AXIS Perimeter Defender, on page 19*.
6. Añada escenarios para definir las reglas que deben activar alarmas. Vea *Definir escenarios, on page 26*.
7. Configure las alarmas que se enviarán. Vea *Definir salidas, on page 30*.

Primeros pasos con AXIS Perimeter Defender PTZ Autotracking

Debe seguir los siguientes pasos para poner en marcha su instalación con AXIS Perimeter Defender PTZ Autotracking:

1. Monte las cámaras. Vea *Montar la cámara, on page 13* y *Montar la cámara PTZ, on page 16*.
2. Descargue e instale el software en su ordenador. Vea *Instalar el software en el ordenador, on page 16*.
3. Conéctese a sus dispositivos. Vea *Agregar dispositivos, on page 17*.
4. Instale AXIS Perimeter Defender versión 2.5.0 o posterior en la cámara fija y AXIS Perimeter Defender PTZ Autotracking en la cámara PTZ. Vea *Instalar software en dispositivos, on page 18*.
5. Calibre los dispositivos y configure los escenarios. Vea *Calibrar: PTZ Autotracking, on page 26*.
6. Empareje los dispositivos. Vea *Emparejar las cámaras: PTZ Autotracking, on page 29*.
7. Configure las alarmas que se enviarán. Vea *Definir salidas, on page 30*.

Montar la cámara

Acerca de la herramienta de diseño

Para especificar la ubicación de la cámara, le recomendamos que utilice la herramienta de diseño para AXIS Perimeter Defender. Esta herramienta tiene en cuenta los requisitos de las cámaras Axis y de AXIS Perimeter Defender. Además, puede utilizarla cuando realice instalaciones duales, es decir, con dos cámaras combinadas. La herramienta le ayuda a decidir:

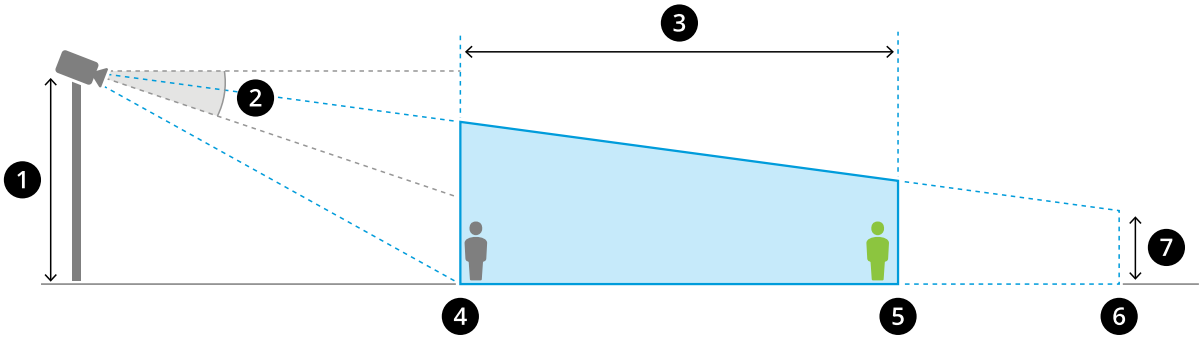
- Altura de montaje de la cámara
- Ángulo vertical
- Distancia mínima de detección
- Distancia máxima de detección

Para descargar la herramienta, vaya a *axis.com/products/axis-perimeter-defender*

Recomendaciones para montar la cámara

Nota

En el caso de cámaras que solo se ejecuten en modo IA, puede encontrar recomendaciones de montaje en la aplicación.



Una cámara adecuadamente montada.

1 *Altura de montaje*
2 *Movimiento vertical*
3 *Zona de detección*
4 *Distancia mínima de detección*
5 *Distancia máxima de detección*
6 *Distancia del campo de visión*
7 *Elevación del campo de visión*

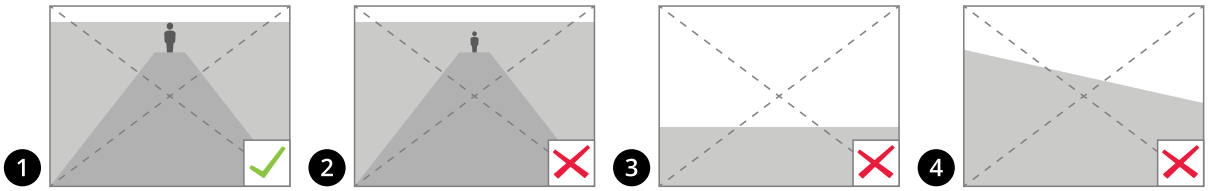
Altura del objeto a la distancia máxima de detección – Para que una persona de pie sea detectada a la distancia máxima de detección, la altura de píxel debe ser al menos el 5 % de la altura total de la imagen (3,5 % para las cámaras térmicas). Por ejemplo, si la altura de la imagen visualizada es de 576 píxeles, la altura de una persona que se encuentra al final de la zona de detección debe ser de al menos de 28 píxeles (20 píxeles para las cámaras térmicas).

Altura del objeto a la distancia mínima de detección – Para que una persona de pie se detecte a la distancia mínima de detección, la altura de píxel no puede ser superior al 60 % de la altura total de la imagen.

Altura del objeto en el modo IA – Cuando ejecuta la aplicación en el modo IA, los objetos deben tener el mismo tamaño o un tamaño superior que el avatar detectado.

Ángulo vertical – La cámara debe estar orientada hacia el suelo para que el centro de la imagen quede por debajo del horizonte. Monte la cámara de modo que la distancia mínima de detección sea mayor que la mitad de la altura de montaje de la cámara (distancia mínima de detección > altura de montaje de la cámara / 2).

Ángulo de giro – El ángulo de giro de la cámara debe ser prácticamente igual a cero.



1 *La altura del objeto, el ángulo de inclinación y el ángulo de giro son adecuados.*
2 *La altura del objeto a una distancia máxima de detección es inferior al 5 % de la altura de la imagen (3,5 % para las cámaras térmicas).*
3 *El centro de la imagen está por encima de la línea del horizonte.*
4 *El ángulo de giro de la cámara no debe ser casi igual a cero.*

La distancia máxima de detección depende de:

- Tipo y modelo de la cámara
- Objetivo de la cámara. Un rango focal más alto permite una distancia de detección más larga.

- El tamaño mínimo de píxel que un humano debe cubrir en la imagen que se va a detectar. La altura de píxel de una persona de pie debe ser al menos del 5 % de la altura de la imagen para las cámaras visuales y del 3,5 % para las cámaras térmicas.
- Meteorología
- Iluminación
- Carga de la cámara

Cuando monte la cámara, recuerde:

- La aplicación tolera pequeñas vibraciones de la cámara, pero se obtiene un mejor rendimiento cuando la cámara no está sujeta a vibraciones.
- El campo de visión de la cámara debe ser fijo.

Altura de montaje

Para alcanzar una determinada distancia de detección, además del tamaño mínimo de píxel, la cámara debe colocarse a una altura mínima. No hay una altura máxima de montaje mientras se cumplan los demás requisitos, sobre todo el ángulo vertical.

Distancia de detección requerida	Altura de montaje mínima de la cámara
20 m	2,5 m (altura mínima permitida)
100 m	3 m (10 ft)
200 m	4 m (13 pies)
300 m	5 m
500 m	6 m

Requisitos de la escena

Nota

En el caso de cámaras que solo se ejecuten en modo IA, puede encontrar los requisitos de escena en la aplicación.

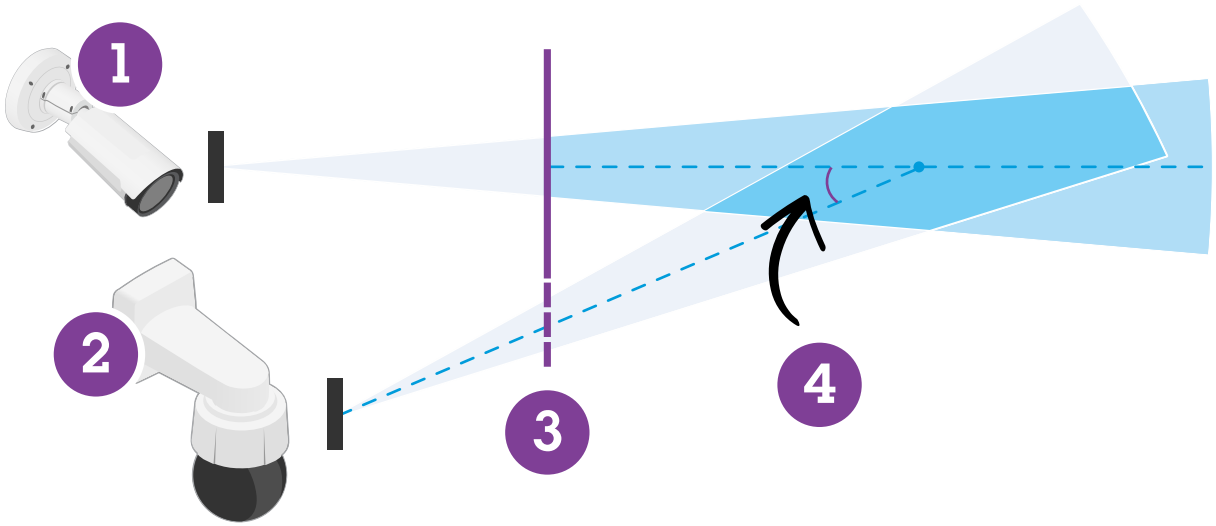
La zona de detección debe proporcionar las siguientes condiciones:

- Visión clara
- El suelo debe estar plano o solo con una pequeña pendiente.
- La iluminación no se activa por el movimiento
- Visión clara
- En el caso de las cámaras visuales, el nivel de iluminación y los ajustes de imagen deben ser suficientes para ofrecer un contraste suficiente entre humanos, vehículos y el fondo.
  - Si utiliza una cámara día-noche de Axis con iluminación artificial, recomendamos al menos 50 lux en toda la zona de detección.
  - Si utiliza puntos IR externos, recomendamos una distancia de detección máxima de 80 m y que el intervalo de los puntos de infrarrojos sea más del doble de la distancia de detección máxima.
  - Si utiliza la iluminación IR integrada, la distancia de detección máxima se limitará a 20 m como máximo, en función de la cámara y el entorno.
- En el caso de las cámaras térmicas, debe haber un contraste alto entre el fondo y el primer plano

Para optimizar el rendimiento de la detección, AXIS Perimeter Defender aprende automáticamente la diferencia entre el día y la noche y utiliza esta información para ajustar con precisión los algoritmos de detección. El ajuste preciso dura unas 24 horas, lo que significa que se consigue una detección óptima tanto de día como de noche después de ejecutar la aplicación durante ese tiempo.

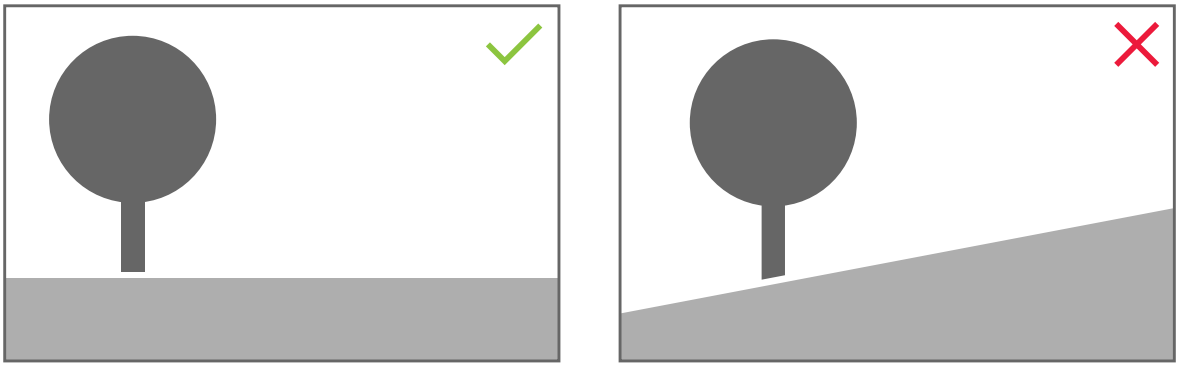
Montar la cámara PTZ

En este capítulo se describe cómo montar la cámara PTZ en relación con la cámara fija. Para obtener instrucciones sobre cómo montar la cámara fija, vea *Montar la cámara, on page 13*.



1 Cámara de red fija
2 Cámara de red PTZ
3 Distancia mínima de detección
4 Ángulo entre las cámaras

- La posición predefinida de inicio de la cámara PTZ debe abarcar más del 60 % de la zona de detección de la cámara fija.
- Para que la cámara PTZ pueda realizar el seguimiento, una persona de pie debe cubrir más del 4 % de la altura de la imagen de la cámara PTZ.
- La cámara PTZ debe colocarse antes de la distancia de detección mínima de la cámara fija (C).
- El ángulo entre la cámara fija y la cámara PTZ debe ser inferior a 30° (D).



- El suelo debe ser plano.

Instalar el software en el ordenador

Las cámaras que ejecutan AXIS Perimeter Defender deben ser accesibles a través de HTTP desde el equipo en el que se ejecuta la interfaz de configuración de AXIS Perimeter Defender.

La interfaz de configuración de AXIS Perimeter Defender (solo necesaria durante la fase de configuración) requiere:

- Procesador Intel® Core™ 2 Duo o superior

- Compatibilidad con Open GL
- Al menos 16 GB de RAM
- Windows® 10, Windows® 11 o Win Server 2022
- Resolución de pantalla mínima de 1024x768

Tenga en cuenta que el número de cámaras que puede manejar un solo ordenador es limitado. Por ejemplo, para una máquina con un procesador Intel® Core™ i5-1135G7 de 11.ª generación a 2,40 GHz se recomienda añadir un máximo de 10 cámaras y ejecutar una calibración automática simultánea en un máximo de 5 cámaras.

Nota

No es posible ejecutar la interfaz de configuración de AXIS Perimeter Defender en una máquina virtual.

1. Descargue el software AXIS Perimeter Defender desde *axis.com/products/axis-perimeter-defender*
2. Instale el software en el ordenador.

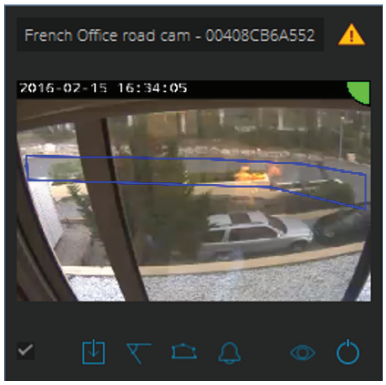
Agregar dispositivos

Puede añadir dispositivos a la aplicación AXIS Perimeter Defender de tres maneras diferentes:

- Automáticamente a través de un análisis de red. Vea *Añadir dispositivos automáticamente, on page 17*.
- Manualmente especificando la configuración de conexión. Vea *Añadir dispositivos manualmente, on page 18*.
- Automáticamente cargando una instalación previamente guardada. Vea *Cargar una configuración existente, on page 18*.

Al añadir un dispositivo, verá una lista de todas las demás aplicaciones instaladas en el dispositivo. Le recomendamos que detenga las aplicaciones no esenciales, ya que utilizan recursos de CPU de la cámara, lo que afecta al rendimiento de AXIS Perimeter Defender y puede impedir una correcta instalación.

Si un dispositivo no tiene suficientes recursos de CPU, ejemplo, porque se están ejecutando otras aplicaciones, AXIS Perimeter Defender reduce la velocidad de fotogramas. Si la velocidad de fotogramas es inferior a 5 fotogramas por segundo, se muestra un triángulo amarillo de advertencia junto al nombre del dispositivo en la vista en directo. Al pasar el cursor del ratón sobre el triángulo, se muestra la velocidad de fotogramas actual.



Nota

Una velocidad de fotogramas inferior a 5 fps puede disminuir significativamente el rendimiento analítico de vídeo. Esto puede dar lugar a detecciones perdidas y falsas.

Para obtener más información, vea *Carga de la CPU, on page 12*.

Añadir dispositivos automáticamente

Importante

La funcionalidad de búsqueda no funciona entre diferentes redes; es decir, el programa de instalación de AXIS Perimeter solo puede encontrar dispositivos que estén conectados a la misma subred que el cliente que ejecuta el software. Para añadir dispositivos conectados a una subred diferente, añádalos manualmente. La

funcionalidad de búsqueda también puede fallar si los enrutadores o conmutadores de red están configurados para filtrar la multidifusión.

1. Para buscar dispositivos en la red circundante, vaya a **Application (Aplicación)** y haga clic en **Search (Buscar)**.
   Cuando realiza una búsqueda por primera vez y no hay contraseñas disponibles, se abre un cuadro de diálogo de contraseña. En caso contrario, se utiliza la contraseña disponible para conectarse a los dispositivos.
2. Seleccione los dispositivos y haga clic en **Add selected devices (Añadir los dispositivos seleccionados)**. Si la contraseña es correcta, aparece una imagen estática para guiar al usuario al seleccionar dispositivos.

Añadir dispositivos manualmente

1. Vaya a **Application (Añadir)** y haga clic en **Add (Añadir)**.
2. Introduzca la siguiente información:

- La dirección IP o nombre de host del dispositivo.
- La contraseña root del dispositivo, puesto que AXIS Perimeter Defender requiere acceso root.
- El puerto HTTP utilizado para conectarse. El puerto predeterminado es 80.
- Un nombre opcional para el dispositivo a fin de facilitar el reconocimiento.
- Si el dispositivo está en una red remota cuya conexión puede ser lenta, marque **Device on remote network (Dispositivo en red remota)**. Las conexiones lentas que no están configuradas como remotas pueden dar lugar a calibraciones no funcionales o incorrectas.

Nota

En las conexiones remotas, el usuario debe poder conectarse al dispositivo a través de HTTP. Configure correctamente el puerto HTTP. La configuración remota puede fallar cuando la conexión no tiene ancho de banda suficiente o no es estable.

3. Haga clic en **OK**.

Nota

Si añadir una cámara por su nombre de host no funciona, compruebe los ajustes de red y DNS o añada el dispositivo utilizando su dirección IP.

Cargar una configuración existente

Para cargar una configuración de instalación guardada anteriormente:

1. Vaya a **Application (Aplicación)** y haga clic en **Load site (Cargar instalación)**.
2. Desplácese para seleccionar el archivo de configuración de la instalación y haga clic en **Open (Abrir)**. La vista en directo se muestra automáticamente.

Instalar software en dispositivos

Debe instalar AXIS Perimeter Defender en cada dispositivo.

Si desea comprobar qué versión de AXIS Perimeter Defender está instalada en un dispositivo, puede situar el cursor del ratón sobre **Installation status (Estado de la instalación)** en la vista en directo.

Si un dispositivo no tiene instalado AXIS Perimeter Defender, todos los iconos de la vista en directo se muestran en gris.

Instalación del software en un dispositivo

1. Vaya a **Installation (Instalación)**.
2. Seleccione los dispositivos en los que desea instalar la aplicación.

3. Seleccione la última versión disponible de AXIS Perimeter Defender y haga clic en **Install (Instalar)**. AXIS Perimeter Defender está ahora instalado en los dispositivos seleccionados y se inicia automáticamente.
4. Seleccione una licencia y realice una de las siguientes acciones:

– Si realiza la instalación en un único dispositivo: seleccione el archivo de licencia para el dispositivo.

– Si realiza la instalación en varios dispositivos: seleccione la carpeta en la que se almacenan los archivos de licencia.

5. Haga clic en **Instalar**.

Calibrar - AXIS Perimeter Defender

Calibración

Nota

No necesita calibrar solo los dispositivos que se ejecutan en modo IA. Para ejecutar dispositivos en modo de calibración y modo IA simultáneamente, es necesario calibrarlos.

Para que AXIS Perimeter Defender interprete correctamente la escena, se deben calibrar todos los dispositivos. Durante la calibración, se introducen puntos de referencia que proporcionan información de profundidad y altura para el procesador. También puede definir la zona de interés.

La calibración consta de dos tareas:

1. Realizar una calibración:
   - automática: se recomienda en la mayoría de los casos. Vea *Realizar una calibración automática, on page 20*.
   - manual: se recomienda si se produce un error en la calibración automática de una cámara, para un ajuste preciso o cuando no es posible realizar un recorrido por la escena y en la escena hay objetos de altura conocida. Un ejemplo puede ser un perímetro remoto con una línea de cercado formada por un número de postes de cerca equidistantes y de la misma altura. Vea *Realizar una calibración manual, on page 24*.
2. Verifique los resultados de la calibración. Vea *Verificar la calidad de la calibración , on page 21*.

Para acelerar la configuración de una instalación de gran tamaño, puede calibrar varios dispositivos simultáneamente. Puede realizar la calibración automática o manualmente, igual que con una sola cámara. Antes de calibrar varios dispositivos a la vez, tenga en cuenta lo siguiente:

- El número máximo de dispositivos que puede instalar y configurar simultáneamente depende de la potencia de la CPU y de la memoria disponible en su ordenador. Un exceso de dispositivos en la configuración de AXIS Perimeter Defender pueden causar bloqueos. Cuando se muestre la advertencia de sobrecarga de la CPU, instale y configure un subconjunto de dispositivos mediante la función Save site (guardar instalación).
- La calibración automática de varios dispositivos requiere más recursos de CPU y RAM que para un único dispositivo. En los sistemas de especificaciones bajas, esto puede provocar que el ordenador no responda durante algún tiempo o que se bloquee la aplicación. En caso de fallo, los vídeos capturados siguen disponibles para su uso posterior en la calibración de una sola cámara.

Nota

- AXIS Perimeter Defender admite diferentes relaciones de aspecto de imagen según la resolución máxima proporcionada por la cámara. De este modo, es necesario volver a hacer todas las calibraciones anteriores si se cambia la resolución. Sin embargo, si se cambia la resolución de transmisión en la página web de la cámara, no es necesario volver a calibrar.
- Recomendamos utilizar la misma relación de aspecto de imagen en AXIS Perimeter Defender y en el VMS para asegurarse de que la información mostrada se ajusta al contenido de la imagen. Para conocer la relación de aspecto, sitúe el cursor del ratón sobre la cámara en la vista en directo.
- Si una cámara se mueve después de la calibración, es necesario volver a calibrarla para que los resultados de análisis sean correctos.

Realizar una calibración automática

Con la calibración automática, se puede calibrar una o varias cámaras dejando que una persona camine por la escena de vigilancia. La cámara recoge automáticamente la información necesaria para calibrarse por sí misma.

Para una calibración automática correcta:

- No calibrar cuando haya muchas personas en el campo de visión.
- No calibrar cuando haya muchos vehículos en circulación en el campo de visión.
- No calibrar cuando haya otros objetos en movimiento en el campo de visión. Por ejemplo, árboles o banderas que se mueven por el viento.
- No calibrar una cámara que no se haya instalado paralela al suelo.
- La persona que camina a través de la escena debe poder cubrir todo el campo de visión desde adelante hacia atrás. Si esto no fuera posible, es recomendable cambiar a la calibración manual.
- Si la cámara está en una red remota, pero no está conectada como remota, la persona que camina a través de la escena debe caminar durante unos 5 minutos para asegurar que se capturan suficientes imágenes. Esto se debe a que la velocidad de fotogramas es generalmente más baja para dispositivos en redes remotas.

1. Vaya a **Calibration (Calibración)**.
2. Seleccione los dispositivos que desea calibrar.
3. Haga clic en **Automatic (Automática)**.
4. Establezca el tiempo inicial de grabación. La captura debe comenzar al menos 10 segundos antes de que la persona que camina a través de la escena entre en el campo de visión.
5. Establezca la duración de la grabación. Considere que:
   - tiene que haber suficiente tiempo para que la persona camine de un lado a otro a través de toda la escena.
   - la duración del vídeo afecta al cálculo de la calibración.
6. Introduzca la altura (cm) de la persona que camina por la escena y haga clic en **Capture (Capturar)**. Para reutilizar un vídeo capturado anteriormente, haga clic en **Use previous capture (Usar captura anterior)**.
7. Haga que la persona camine a través de la escena de acuerdo con las siguientes instrucciones:
   - Caminar siguiendo un recorrido en zigzag que cubra tanto como sea posible la zona de detección de adelante hacia atrás de la escena. Recomendamos una ruta en forma de V por el campo de visión.
   - Permanecer casi siempre completamente visible de la cabeza a los pies en el campo de visión.
   - Caminar lentamente en líneas rectas.
   - Mantener una postura erguida todo el tiempo.
   - Hacer una pausa de 1-2 segundos antes de cambiar de dirección.

Un ejemplo de una secuencia de recorrido.

8. Compruebe que la calibración automática se ha realizado correctamente confirmando que la persona se detecta con precisión. Vea *Verificar la calidad de la calibración , on page 21*.
9. Para guardar la calibración, haga clic en **Accept (Aceptar)**.
   Para realizar una nueva calibración, haga clic en **New (Nueva)**.
   Para realizar una calibración manual, haga clic en **Manual**.

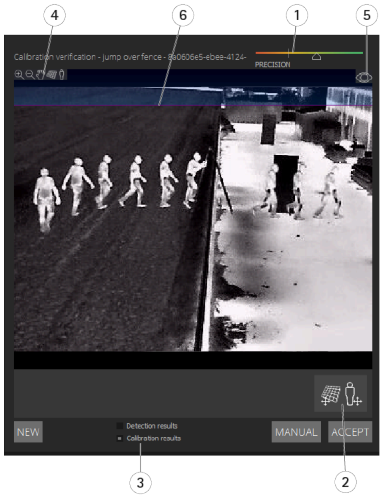
Una vez aceptada la calibración, los bordes azules indican la zona de detección máxima. La zona de detección máxima es el área más grande que se puede supervisar. Fuera de esta área, los intrusos pueden ser detectados, pero esto no se garantiza.

Verificar la calidad de la calibración

Después de una calibración, debe ver a la persona que ha caminado por la escena en distintos puntos diferentes. Si la persona no es visible en absoluto, la calibración automática ha fallado y necesita ser realizada de nuevo.

Hay varias maneras de verificar la calidad de la calibración:

- Compruebe el indicador de precisión de calibración. Refleja un nivel de precisión calculado automáticamente que mide hasta qué punto la persona cubrió la escena y lo bien que fue detectada. Si el indicador de precisión está en la zona roja, la calibración ha fallado y no se puede hacer clic en **Accept (Aceptar)**. Vea *Realizar una calibración manual, on page 24*.
- Puede utilizar la herramienta de cuadrícula. Vea *Utilizar la cuadrícula para verificar la calibración, on page 22*.
- Puede utilizar la herramienta de avatar. Vea *Utilice el avatar para verificar la calibración, on page 23*.
- Puede comprobar los resultados de la detección. Vea *Utilice los resultados de la detección para verificar la calibración, on page 23*.



1 *Indicador de precisión de calibración*
2 *Herramientas de cuadrícula y avatar*
3 *Vista dinámica o estática*
4 *Ver modificadores*
5 *Alternar entre la imagen de calibración y la vista en directo*
6 *Línea de horizonte*

La línea de horizonte representa el extremo visible del suelo en la escena. Al definir escenarios, no es posible colocar zonas de escenario en el área azul por encima de la línea del horizonte, ya que se situarían por encima del suelo y las zonas de escenario están por definición en el suelo.

Utilizar la cuadrícula para verificar la calibración

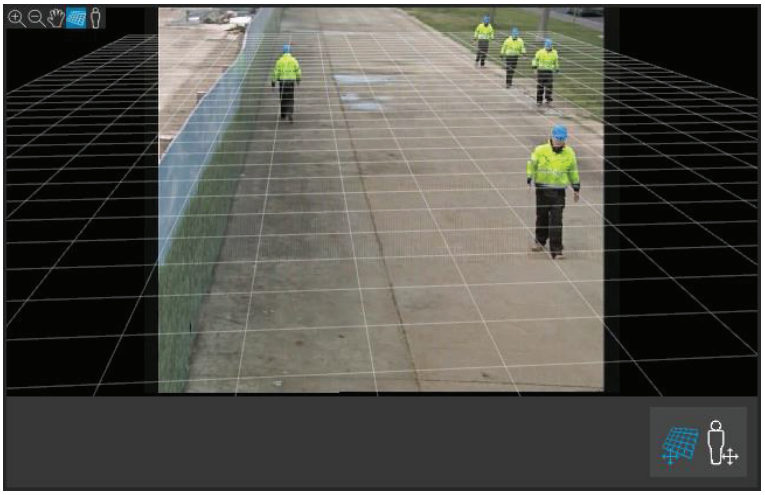
La cuadrícula debe corresponder a una cuadrícula cuadrada en el suelo. Puede alternar la visualización de la cuadrícula haciendo clic en el icono del modificador de vista de cuadrícula.

Importante

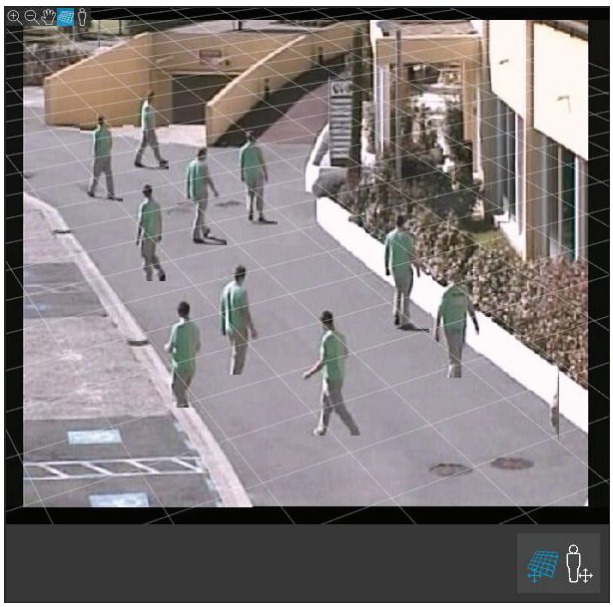
La cuadrícula no afecta a la calibración, es una herramienta para comprobar la correcta calibración.

Puede girar la cuadrícula arrastrándola en el panel de vista previa. Trate de alinearla con alguna estructura en la escena para comprobar si el resultado parece razonable.

Si la cuadrícula está paralela al suelo, no presenta pendientes extrañas, y, después de haber aplicado la rotación necesaria a la cuadrícula, es paralela a elementos artificiales que son paralelos en el mundo real, entonces la calibración es correcta.



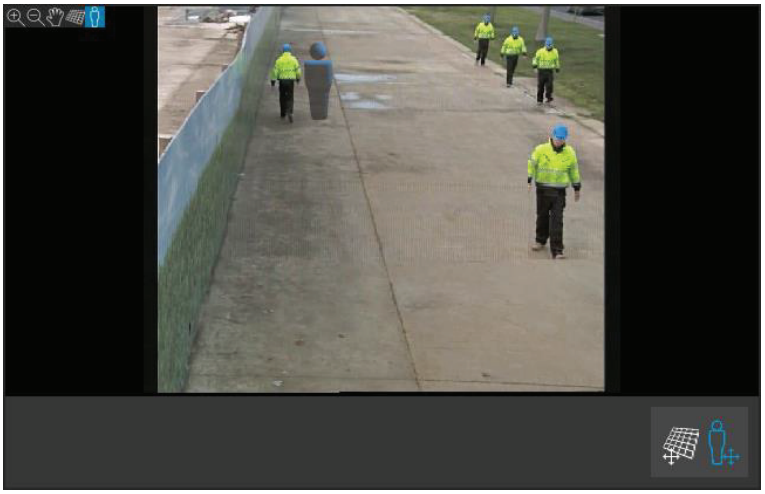
Un ejemplo en el que la cuadrícula está correctamente alineada con las líneas de la carretera.



Un ejemplo en el que la cuadrícula no está correctamente alineada con las líneas de la carretera.

Utilice el avatar para verificar la calibración

El avatar le permite colocar un avatar de persona 3D de altura media en la escena. Puede alternar la visualización del avatar haciendo clic en el icono del modificador de vista de avatar.



Su tamaño en el panel de vista corresponde al tamaño de una persona promedio en esa posición según la calibración actual. Moviendo el avatar se asegurara de que su tamaño es razonable en relación con otros objetos o personas en la escena. Debe comprobar el avatar en diferentes posiciones, ya que el avatar podría estar correctamente dimensionado en una posición, pero no estarlo en otras partes de la imagen.

Utilice los resultados de la detección para verificar la calibración

Puede utilizar los resultados de detección para comprobar el rendimiento de AXIS Perimeter Defender con la calibración actual al recibir la grabación de vídeo de la persona caminando en una transmisión en directo.

1. Cambie de **Calibration results (Resultados de calibración)** a **Detection results (Resultados de detección)**.
2. Compruebe las detecciones de personas o vehículos que entran en la escena de vigilancia:
   - Si la calibración es correcta, las personas se marcan con rectángulos rojos y los vehículos con rectángulos azules.
   - Si las personas o vehículos con frecuencia no están marcados, lo más probable es que la calibración automática haya fallado.

– Una zona roja muestra la zona límite de detección según la calibración calculada, es decir, la zona donde no se respetan los requisitos previos sobre la altura humana en la imagen. En esta zona, la detección puede fallar debido al tamaño del objetivo.

Nota

- Si la calibración calculada es incorrecta, la zona roja también es incorrecta.
- Si la persona está demasiado lejos, es posible que no sea marcada. Se necesita un tamaño mínimo para que la detección funcione. Para obtener más información, vea *Montar la cámara, on page 13*.
- Es posible que la revisión de los resultados de detección no funcione en cámaras conectadas de forma remota, ya que la captura puede tener una velocidad de fotogramas demasiado baja. Esto no significa que la configuración haya fallado. En su lugar, utilice el avatar y la cuadrícula para verificar la calibración.

Realizar una calibración manual

Si no ha intentado una calibración automática, debe capturar un vídeo corto y crear una imagen compuesta antes de poder realizar una calibración manual. Siga los mismos pasos que para una calibración automática (*Realizar una calibración automática, on page 20*), pero seleccione **Manual** en lugar de **Automática** en la pestaña **Calibración**. Para crear la imagen compuesta después de haber capturado un vídeo:

- mueva el control deslizante para navegar por el clip de vídeo
- en posiciones clave, haga clic en el icono de la cámara para añadir imágenes a la imagen compuesta

Asegúrese de que la imagen compuesta refleje toda la sección transversal de la escena: la parte delantera, la parte trasera, derecha e izquierda.

Cuando tenga una imagen compuesta, creada manual o automáticamente, ya puede continuar con la calibración manual.

El motor de calibración se calibra calculando:

- el horizonte
- la forma en que las líneas verticales se extienden, o se dispersan, en la imagen
- la escala de la escena

Cuando realiza una calibración manual, debe proporcionar esta información al motor de calibración a través de elementos de calibración. Existen tres tipos de elementos de calibración:

- **Balizas de persona**, que se utilizan para marcar la altura conocida de una persona promedio en distintas posiciones de la escena. Si ya ha intentado una calibración automática, es muy probable que la imagen que se muestra en el panel del editor presente varias instancias de la misma persona. Coloque balizas de persona desde el nivel de suelo para marcar la altura y la dirección de la persona en una o varias posiciones. Una baliza de persona debe comenzar en el suelo y debe ser vertical en el mundo real. La longitud de una baliza de persona en el mundo real se debe corresponder con la altura indicada junto al botón **Person (Persona)** en el panel del editor. Las balizas de persona están marcadas con un símbolo de color azul claro semitransparente.
  Cuál es la mejor colocación para una baliza de persona

– Le recomendamos que coloque la baliza de persona con los pies juntos.

– Si coloca una baliza en una persona de pie sobre el suelo con los pies separados, coloque el punto inferior en el suelo en el centro entre los talones de la persona.

– Alinee la baliza con el torso de la persona. Sin embargo, si la persona se inclina en alguna dirección al caminar, por lo general hacia adelante, trate de compensar la inclinación colocando el palo más vertical. Utilice cualquier pista de la escena como guía, por ejemplo, árboles, cercas o postes de farolas.

– Para la escala de la escena, se necesita al menos una baliza de persona con la altura de la persona correspondiente. Si no hay ninguna persona visible en la escena, puede añadir una baliza de persona sobre otro objeto vertical de altura conocida; por ejemplo, un poste de cerca de 3 m, y establezca la altura de la persona a la altura del objeto.

- **Las líneas horizontales paralelas (líneas H)** se utilizan para marcar las líneas horizontales y paralelas conocidas en la escena. Estas líneas pueden estar en el suelo o en una pared o en ambas, pero todas

deben ser paralelas. Si añade líneas H, debe añadir al menos dos. Puede colocarlas en los lados o los márgenes de una carretera recta, en vías de ferrocarril rectas, en alguna estructura visible en una pared o en la parte superior e inferior de una fila de postes de cerca. Las líneas H están marcadas en color azul claro.

- **Las líneas verticales (líneas V)** se utilizan para marcar las líneas verticales conocidas en la escena. Una línea en V debe marcar alguna estructura vertical en el mundo real. Se puede tratar, por ejemplo, de un poste de cerca, la esquina de un edificio o una señal. No es necesario que una línea en V empiece en el suelo. Las líneas en V están marcadas en azul oscuro. Tenga en cuenta que las líneas V son muy sensibles, ya que un pequeño cambio de orientación puede cambiar drásticamente la calibración. Como regla general, las líneas V deben inclinarse a la derecha en el lado derecho de la imagen y a la izquierda en el lado izquierdo.

1 *Balizas de persona*
2 *Líneas verticales (líneas V)*
3 *Líneas horizontales paralelas (líneas H)*
4 *Herramientas de cuadrícula y avatar*

Número de elementos de calibración

Por lo general, cuantas más balizas de persona, líneas H y líneas V se añadan a la escena, mejor. El motor de calibración puede calibrar con muy pocas líneas, pero normalmente la calidad de calibración mejora con cuantas más líneas y balizas se aporten. Al añadir balizas de persona, recomendamos que las sitúe tanto cerca como lejos, a la derecha y a la izquierda.

Estructuras verticales en la imagen

De acuerdo con *Recomendaciones para montar la cámara, on page 14*, todas las cámaras deben apuntar ligeramente hacia abajo. Como resultado, todas las estructuras verticales en el mundo real parecen dispersarse como una cola de pavo real en la imagen. Esto significa que todas las balizas de persona y líneas V deben inclinarse hacia el borde de la imagen. Una baliza situada en la mitad derecha de la imagen debe inclinarse hacia la derecha y una baliza en la izquierda debe inclinarse hacia la izquierda. Al menos una de las balizas de persona o líneas V colocadas debe estar "correctamente inclinada" para que la calibración funcione.

El indicador de precisión proporciona información visual sobre el nivel y la calidad de detalle añadida a la escena. Para realizar calibraciones manuales correctas, las marcas deben cubrir la escena de delante hacia atrás y de izquierda a derecha. Esto se indica mediante un indicador de precisión verde.

Calidad de calibración

La calidad de la calibración se puede comprobar con la cuadrícula o los manipuladores de avatar. Vea *Verificar la calidad de la calibración , on page 21*. Como alternativa, haga clic en **Review (Revisar)**. Esto muestra el resultado de la ejecución de AXIS Perimeter Defender en el vídeo capturado mediante la calibración manual actual.

Calibrar: PTZ Autotracking

Importante

Para conseguir buenos resultados, la calibración debe ser de alta calidad. Siga cuidadosamente las directrices e instrucciones.

Nota

Puede calibrar ambas cámaras a la vez o una por una.

1. Seleccione la cámara fija y la cámara PTZ.
2. Vaya a **Calibration (Calibración)** y haga clic en **Setup PTZ position (Configurar posición PTZ)**. Se mostrará un elemento emergente con la vista de la cámara fija.
   La cámara PTZ cambiará el movimiento horizontal y vertical y el zoom durante un corto periodo de tiempo al inicio de la aplicación.
3. Compruebe que la vista de las dos cámaras están alineadas entre sí.
   Si no lo están, haga clic en la imagen de la vista en directo para ajustar la vista de la cámara PTZ hasta que coincidan con la vista de la cámara fija. Asegúrese de que no hay balanceos.
4. Haga clic en **Setup PTZ position (Configurar posición PTZ)**.
   Si el botón no es visible, mueva el elemento emergente con la vista de la cámara fija.
5. Haga clic en **Automatic (Automática)**.
6. Realice una calibración automática de acuerdo con las instrucciones que se indican en *Realizar una calibración automática, on page 20*.
7. Utilice el avatar para verificar la calidad de la calibración de la cámara fija. Vea *Utilice el avatar para verificar la calibración, on page 23*.
   Si la calidad es lo suficientemente buena, haga clic en **Accept (Aceptar)**.
   Si la calidad no es lo suficientemente buena, utilice el vídeo de la calibración automática para realizar una calibración manual. Haga clic en **Manual** y siga las instrucciones indicadas en *Realizar una calibración manual, on page 24*.
8. En **Scenarios (Escenarios)**, defina las reglas para las alarmas que se activarán. Vea *Definir escenarios, on page 26*.
9. En **Calibration (Calibración)**, haga clic en **Review (Revisar)** en la vista en directo de la cámara PTZ.
10. Utilice el avatar para verificar la calidad de la calibración de la cámara PTZ. Vea *Utilice el avatar para verificar la calibración, on page 23*.
    Si la calidad es lo suficientemente buena, haga clic en **Accept (Aceptar)**.
    Si la calidad no es lo suficientemente buena, utilice el vídeo de la calibración automática para realizar una calibración manual. Haga clic en **Manual** y siga las instrucciones indicadas en *Realizar una calibración manual, on page 24*.
11. Empareje las cámaras. Vea *Emparejar las cámaras: PTZ Autotracking, on page 29*.

Definir escenarios

Escenarios

AXIS Perimeter Defender incluye escenarios comunes de zona estéril que se pueden configurar para proteger y supervisar áreas sensibles. En la fase de calibración, se ha creado la zona de detección máxima para definir un escenario predeterminado del tipo de intrusión/merodeo. En este paso puede definir escenarios de detección más sofisticados de tres tipos diferentes:

Nota

Si es usuario de AXIS Perimeter Defender 4.0, ahora podrá configurar escenarios sin necesidad de la aplicación de escritorio. Los cambios se reflejarán en la aplicación de escritorio. Para obtener más información, vaya a la *Interfaz web, on page 39*.

- Intrusión/merodeo. Consulte *Configurar el escenario de intrusión/merodeo, on page 27*
- Traspaso de zona. Consulte *Configurar el escenario de traspaso de zona, on page 28*

- condicional. Vea *Configurar el escenario condicional, on page 28*

Si aparece el símbolo **!** en un nombre de escenario, indica que la configuración del escenario no está completa. El problema más común es que todavía no se ha definido la zona de detección.

Parámetros globales

Los parámetros globales que establezca en la interfaz de usuario se aplican a todos los escenarios.

Tipo de cámara – Para cámaras visuales, seleccione **Color – Day-Night (Color – Día-noche)**. Para cámaras térmicas, el tipo de cámara se establece automáticamente en térmica.

Nota

- Los tipos de enfoque adicionales pueden aumentar el riesgo de falsas alarmas, por ejemplo causadas por animales.
- Los tipos de acercamiento adicionales no son compatibles con dispositivos que solo se ejecutan en modo IA.

Tipos de acercamiento adicionales – Seleccione los que desea cubrir con su escenario de detección.

Mitigación avanzada – En el caso de dispositivos con modo IA, marque **IA** para activarla. Puede utilizar **Headlights/vehicles in scene (Faros/vehículos en la escena)** si la escena contiene vehículos, faros o efectos de faros como reflejos. Si utiliza este ajuste, el rendimiento en ocasiones se puede reducir en condiciones normales. De forma predeterminada, todos los escenarios pueden contener vehículos y, por lo tanto, faros. Puede utilizar **Insects/droplets on lens (Insectos/gotas en el objetivo)** para ignorar los activaciones por gotas de lluvia o insectos y reducir las falsas alarmas.

Sensibilidad – Para aumentar la sensibilidad del sistema, mueva el control deslizante hacia la derecha. Una mayor sensibilidad reduce el riesgo de detecciones perdidas, pero aumenta el riesgo de falsas alarmas.

Filtrado del tamaño del objetivo – En el caso de dispositivos con modo IA, puede filtrar objetos más pequeños que el tamaño objetivo.

Parámetro de duración

Para cada escenario que cree, puede establecer parámetros de duración.

Presencia mínima en la zona – Defina el tiempo que un objeto debe permanecer en una zona para que la zona se active.

Zona estrecha – Si la zona es estrecha y se puede cruzar en 1 o 2 segundos, existe el riesgo de que se pierdan alarmas. Puede mitigarlo con la función **Narrow zone (Zona estrecha)**. Tenga en cuenta que no se puede combinar con **Min presence in zone (Presencia mínima en la zona)**.

Configurar el escenario de intrusión/merodeo

El escenario de intrusión/merodeo está diseñado para activar una alarma cuando un objeto entra en una zona determinada y permanece en ella durante un tiempo superior al predefinido.

El escenario predeterminado creado en el paso de calibración es del tipo de intrusión/merodeo y utiliza la zona de detección máxima. Para usar este escenario en su estado actual, haga clic en **Accept (Aceptar)** en la pestaña **Scenarios (Escenarios)**.

Para cambiar el escenario predeterminado:

1. Vaya a **Scenarios > Advanced scenarios (Escenarios > Escenarios avanzados)**.
2. Cambie la zona de detección predeterminada:
   - Para mover los puntos existentes en la zona de detección, haga clic y arrástrelos con el ratón.
   - Para crear puntos adicionales, haga clic en cualquiera de los segmentos existentes y arrástrelos con el ratón.
3. En **Detect (Detectar)**, seleccione el tipo de objetos que desea detectar.

4. En **Duration parameters (Parámetros de duración)**, si no desea que un objeto active una alarma tan pronto entra en la zona establecida, ajuste el tiempo de merodeo en **Min presence in zone (Presencia mínima en la zona)**.
5. Si la zona es estrecha y se puede cruzar en 1-2 segundos, y todavía desea que se activen las alarmas, seleccione **Narrow zone (Zona estrecha)**. Esta configuración no se puede combinar con **Min presence in zone (Presencia mínima en la zona)**. Para obtener más información, vea *Parámetro de duración, on page 27*.
6. Para cargar los cambios en la cámara y volver a la vista principal, haga clic en **Accept (Aceptar)**.

Configurar el escenario de traspaso de zona

El escenario de traspaso de zona está diseñado para activar una alarma cuando un objeto pasa a través de dos zonas de detección en una secuencia determinada.

Importante

El escenario de traspaso de zona tiene la limitación siguiente: si el objeto que activa el escenario deja de moverse durante unos segundos en la zona de origen antes de pasar a la zona final, el escenario no se activa.

En **Duration parameters (Parámetros de duración)**, puede definir un tiempo de presencia mínimo para cada una de las zonas del escenario. Si T_A es el tiempo mínimo en la zona de origen y T_B en la zona final, solo se activará una alarma si el objeto permanece más tiempo del especificado en T_A en la zona de origen y luego más tiempo del definido en T_B en la zona final.

1. Vaya a **Scenarios > Advanced scenarios (Escenarios > Escenarios avanzados)**.
2. Haga clic en **New (Nuevo)** y seleccione **Zone-crossing (Traspaso de zona)**.
3. Cree dos zonas de detección separadas por al menos un metro:
   - Para crear una zona de detección, haga clic varias veces en la imagen.
   - Para finalizar la zona, haga clic con el botón derecho en la imagen.
4. Para especificar la dirección de traspaso prohibida, haga clic en **Select origin (Seleccionar origen)** y, a continuación, haga clic en una de las zonas.
5. En **Detect (Detectar)**, seleccione el tipo de objetos que desea detectar.
6. En **Duration parameters (Parámetros de duración)**, si no desea que una zona se active tan pronto como entre un objeto, establezca la **Min presence in (Presencia mínima en el interior)** para una o ambas zonas.
7. Si la zona es estrecha y se puede cruzar en 1-2 segundos, y todavía desea que se activen las alarmas, seleccione **Narrow zone (Zona estrecha)**. Esta configuración no se puede combinar con **Min presence in zone (Presencia mínima en la zona)**. Para obtener más información, vea *Parámetro de duración, on page 27*.
8. Para cargar los cambios en la cámara y volver a la vista principal, haga clic en **Accept (Aceptar)**.

Configurar el escenario condicional

El escenario condicional está diseñado para activar una alarma cuando un objeto entra en una zona determinada sin pasar primero a través de otras.

En **Duration parameters (Parámetros de duración)**, puede definir un tiempo de presencia mínimo para cada una de las zonas del escenario. Si T_A es el tiempo mínimo en la zona autorizada y T_B en la zona de intrusión, solo se activará una alarma si el objeto:

- permanece más tiempo del definido en T_B en la zona de intrusión sin haber entrado antes en la zona autorizada.
- permanece menos tiempo del definido en T_A en la zona autorizada, luego entra y permanece más tiempo del especificado en T_B en la zona de intrusión.

No se activa la alarma si el objeto:

- no entra o permanece menos tiempo del definido en T_B en la zona de intrusión.

- permanece más tiempo del especificado en T_A en la zona autorizada y, a continuación, entra en la zona de intrusión (independientemente de cuánto tiempo permanezca allí el objeto).

1. Vaya a **Scenarios > Advanced scenarios (Escenarios > Escenarios avanzados)**.
2. Haga clic en **New (Nuevo)** y seleccione **Conditional (Condicional)**.
3. Cree dos o más zonas de detección separadas por al menos un metro:
   - Para crear una zona de detección, haga clic varias veces en la imagen.
   - Para finalizar la zona, haga clic con el botón derecho en la imagen.
4. Para especificar la dirección de cruce, haga clic en **Select intrusion zone (Seleccionar zona de intrusión)** y, a continuación, haga clic en una de las zonas.
5. En **Detect (Detectar)**, seleccione el tipo de objetos que desea detectar.
6. En **Duration parameters (Parámetros de duración)**, si no desea que una zona se active tan pronto como entre un objeto, establezca la **Min presence in (Presencia mínima en el interior)** para una o ambas zonas.
7. Si la zona es estrecha y se puede cruzar en 1-2 segundos, y todavía desea que se activen las alarmas, seleccione **Narrow zone (Zona estrecha)**. Esta configuración no se puede combinar con **Min presence in zone (Presencia mínima en la zona)**. Para obtener más información, vea *Parámetro de duración, on page 27*.
8. Para cargar los cambios en la cámara y volver a la vista principal, haga clic en **Accept (Aceptar)**.

Emparejar las cámaras: PTZ Autotracking

Durante la configuración de AXIS Perimeter Defender PTZ Autotracking, se deben emparejar entre sí la cámara fija y la cámara PTZ para asegurarse de que la cámara PTZ realiza el seguimiento de un objeto en movimiento de una forma eficaz.

Si ha realizado una calibración automática, puede *Realizar un emparejamiento automático, on page 29* de las dos cámaras. De lo contrario, puede *Realizar un emparejamiento manual, on page 30*.

Realizar un emparejamiento automático

En el vídeo de emparejamiento, las líneas rojas representan a la persona y la caja de límite naranja representa la imagen ampliada de la cámara PTZ.

1. En **Calibration > PTZ Pairing review (Calibración > Revisar emparejamiento PTZ)**, compruebe los vídeos de emparejamiento de las dos cámaras:
   - compruebe que las líneas rojas de las dos imágenes están alineadas en todo el vídeo
   - compruebe que las líneas rojas siempre van de los pies a la cabeza de la persona
   - compruebe que la persona esté siempre centrada dentro de la caja de límite naranja en el vídeo de la cámara PTZ.
2. Si se cumplen las condiciones del paso 1, seleccione **Interactive pairing review (Revisar emparejamiento interactivo)**.
   Si no se cumplen las condiciones, haga clic en **Manual** y siga los pasos descritos en *Realizar un emparejamiento manual, on page 30*.
3. Mueva el control deslizante para navegar por el clip de vídeo. Compruebe lo siguiente:
   - Las líneas azules de las dos imágenes están alineadas durante todo el vídeo
   - La persona esté siempre centrada dentro de la caja de límite naranja en el vídeo de la cámara PTZ
4. Si hay escenas en las que falta la caja de límite naranja:
   4.1. Active el avatar en la imagen fija de la cámara.

4.2. Utilice el control deslizante para desplazarse hacia delante y hacia atrás en el vídeo. Coloque el avatar en la persona en la vista de la cámara fija y compruebe que el punto rojo se encuentra en el pie de la persona en la imagen de la cámara PTZ.

5. Si hay escenas en las que el emparejamiento automático no ha añadido líneas azules, haga clic en **Manual** y añada las líneas rojas manualmente a la persona. Vea *Realizar un emparejamiento manual, on page 30* para obtener instrucciones detalladas.
6. Haga clic en **Accept (Aceptar)** y en **Exit (Salir)**.

Realizar un emparejamiento manual

Al realizar un emparejamiento manual, se añaden líneas rojas verticales desde los pies hasta la cabeza de la persona que caminaba por la escena de vigilancia durante el paso de calibración. Es necesario añadir líneas en el vídeo para cubrir toda la escena.

Si ya ha realizado un emparejamiento automático, el vídeo ya contiene líneas azules.

Elimine las líneas azules y rojas que:
- no se inicien en los pies de la persona
- no lleguen hasta la cabeza de la persona
- no tengan una línea correspondiente en la imagen de la cámara PTZ

Para eliminar una línea, haga clic en ella y pulse Delete (Eliminar).

1. Mueva el control deslizante para navegar hasta una imagen del clip de vídeo en el que la persona es visible.
2. Añada una línea roja a la persona en la imagen fija de la cámara. Inicie la línea en los pies de la persona. Se asigna un número ID a la línea.
3. Añada una línea roja correspondiente en el mismo objeto de la imagen de la cámara PTZ. Compruebe que el número ID coincida con el de la imagen de la cámara fija.
4. Repita los pasos de 1 a 3 hasta que haya cubierto toda la escena.
   Cuando el clip de vídeo contiene un número suficiente de líneas para un emparejamiento válido:
   - el botón **Accept (Aceptar)** se muestra activo
   - se muestra una caja de límite naranja en la imagen de la cámara PTZ.
5. Compruebe que la persona esté siempre centrada dentro de la caja de límite naranja. Si hay escenas en las que no lo está, añada más líneas rojas.
6. Active el avatar en la imagen fija de la cámara.
7. Mueva el control deslizante para navegar por el clip de vídeo. Utilice el avatar para comprobar lo siguiente:
   - en la imagen fija de la cámara, el tamaño del avatar se debe corresponder con el tamaño de la persona en diferentes posiciones
   - en la imagen de la cámara PTZ, el punto rojo se encuentra en los pies de la persona
   - en la imagen de la cámara PTZ, la persona está siempre centrada dentro de la caja de límite naranja
8. Haga clic en **Accept (Aceptar)**. Si el botón está inactivo, debe añadir primero más líneas rojas.
9. Haga clic en **Exit (Salir)**.

Definir salidas

Para crear alarmas de salida de AXIS Perimeter Defender cuando se detecta una intrusión, se deben definir reglas. El sistema puede enviar alarmas, por ejemplo, a un VMS.

AXIS Perimeter Defender puede enviar alarmas a través de diferentes interfaces.

Desde la propia aplicación:

- Notificaciones de alarma XML o de texto sin formato a través de TCP/IP
- Flujos de metadatos XML a través de HTTP multiparte

Desde el dispositivo:

- Notificaciones básicas de texto libre para alarmas a través de TCP/IP
- Salidas eléctricas (contactos secos o mojados)
- Notificaciones por correo electrónico
- Carga FTP de imágenes de alarma

Se pueden activar varias interfaces al mismo tiempo.

Para obtener información más detallada, vea *Salidas, on page 32*.

Para definir las reglas para el envío de alarmas desde el dispositivo:

1. Vaya a **Outputs (Salidas)** y haga clic en **configure (Configurar)**. Se abrirá la página web del dispositivo en el navegador.
2. Permite crear una nueva regla de acción.
3. En la lista de activadores, seleccione **Applications (Aplicaciones)** y, a continuación, **AXISPerimeterDefender** y el escenario para activar la acción.

Nota

Para activar la misma acción en todos los escenarios definidos, seleccione **ALL_SCENARIOS**.

4. En la lista de acciones, seleccione la acción que se realizará cuando se cumpla la condición.
5. Haga clic en **OK**.

Para obtener información más detallada sobre cómo crear reglas de acción, consulte el manual de usuario del dispositivo.

Configuración avanzada

Salidas

Notificaciones de alarma en XML/texto

Esta interfaz permite que un destinatario TCP/IP reciba un mensaje XML o de texto más completo y descriptivo para cada alarma. Con respecto a la interfaz de texto libre, la interfaz XML/texto ofrece las siguientes ventajas:

- Se envía una notificación al principio de la alarma, al final de la alarma y cada 10 segundos durante la alarma.
- Marca temporal: las notificaciones de inicio de alarma y fin de alarma contienen una marca temporal que se sincroniza con el reloj de la cámara y proporciona la fecha y hora exactas de los eventos.
- Tipo de alarma: AXIS Perimeter Defender admite distintos tipos de alarma, vea *Definir escenarios, on page 26*. Las notificaciones de XML/texto contienen la información de qué tipo de alarma se ha activado. Atención: el escenario de "traspaso de zona" contiene el tipo "traspaso" y el escenario de merodeo contiene el tipo "presencia"
- Zonas involucradas en la generación de la alarma; donde cada escenario de AXIS Perimeter Defender está asociado a una o más zonas, las notificaciones de XML/texto incluyen qué zona está asociada a la alarma (p. ej., para una alarma de intrusión, la zona de intrusión en la que se ha detectado a una persona)

Con respecto a la interfaz de texto libre, la interfaz XML/texto presenta las siguientes limitaciones:

- El texto del mensaje es fijo y no hay campos de texto libre.
- Solo se admite un destinatario por cámara a la vez.

El destinatario de las notificaciones de XML/texto recibe cuatro tipos de mensajes:

- AXIS Perimeter Defender envía un mensaje CONNECTION_TEST cuando se configura la notificación XML para comprobar que la comunicación con el destinatario funciona según lo previsto.
- Cuando AXIS Perimeter Defender activa una alarma, envía un mensaje ALARM_START.
- Durante la duración de la alarma, AXIS Perimeter Defender envía varios mensajes de "alarma en curso", uno cada 10 segundos. Todos estos mensajes tienen la misma etiqueta GUID, idéntica a la del mensaje ALARM_START y los mensajes ALARM_STOP relacionados con la misma alarma
- Al final de la alarma, AXIS Perimeter Defender envía una alarma ALARM_STOP.

Para obtener una explicación del formato de estos mensajes, tanto en formato XML como en texto, vea *Ejemplos de formato XML y texto, on page 32*.

Ejemplos de formato XML y texto

El formato XML es el formato predeterminado para las notificaciones TCP/IP. Sin embargo, si el tamaño de la notificación es significativo, se puede utilizar un formato de texto, que genera mensajes más cortos. Para seleccionar el formato de texto, se debe seleccionar **Do not use XML for alarms parameter (No utilizar XML para parámetros de alarmas)** en la página de configuración de AXIS Perimeter Defender.

Ejemplo:
Un mensaje CONNECTION_TEST en formato XML tiene el siguiente aspecto:

```
<?xml version="1.0"?><KEENEO_MESSAGE xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"          xmlns:xsd="http://www.w3.org/2001/XMLSchema"          VERSION=
"5.0.0"         ID="1"          TYPE="CONNECTION_TEST"          SENDER_IP=
"192.168.1.40"          SENDER_PORT="0">  <REFERENTIAL>45</REFERENTIAL></KEENEO_MESSAGE>
```

- VERSION es la versión interna de la sintaxis y el protocolo XML.
- ID es la identidad numérica del mensaje. No se garantiza que los ID sean únicos ni progresivos.
- TYPE es el tipo de mensaje, en este caso "CONNECTION_TEST". El tipo de mensaje determina las subetiquetas del mensaje (ninguna para los mensajes de tipo "CONNECTION_TEST").

- SENDER_IP es la dirección IP de la cámara Axis que envía la notificación XML.
- SENDER_PORT siempre es cero; la cámara no puede recibir mensajes entrantes.
- REFERENTIAL es el ID numérico asociado a la cámara

Si se elige el formato de texto, los mensajes de notificación contienen 7 campos cada uno, separados por el carácter "|". Si un campo no puede especificarse (por ejemplo, porque no tiene sentido para ese tipo de mensaje), es sustituido por "-".

Los siete campos son, desde el primero hasta el último (entre paréntesis, el campo XML correspondiente cuando el formato es XML):

1. El ID numérico del mensaje ("ID" atributo del encabezado XML "KEENEO_MESSAGE").
2. La dirección IPv4 de la cámara ("SENDER_IP" atributo del encabezado XML "KEENEO_MESSAGE").
3. El número de referencia asociado a la instancia de AXIS Perimeter Defender (etiqueta "REFERENTIAL").
4. El tipo de mensaje ("TYPE" atributo del encabezado XML "KEENEO_MESSAGE").
5. El tipo de alarma (etiqueta "TYPE").
6. El nombre del escenario que ha activado la etiqueta de alarma (etiqueta "SCENARIO_NAME").
7. La marca de tiempo (etiqueta "TIMESTAMP"). El formato de marca de tiempo es el mismo que para el formato XML.

El mensaje anterior CONNECTION_TEST en formato TEXT es:

```
1|192.168.1.40|45|CONNECTION_TEST|-|-|-
```

Ejemplo:
Un mensaje ALARM_START en formato XML tiene el aspecto de este ejemplo:

```
<?xml version="1.0"?><KEENEO_MESSAGE xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"         xmlns:xsd="http://www.w3.org/2001/XMLSchema"         VERSION=
"5.0.0"         ID="9999"         TYPE="ALARM_START"         SENDER_IP=
"192.168.1.40"         SENDER_PORT="0">  <REFERENTIAL>0</REFERENTIAL>  <TYPE>INTRUSION</
TYPE>  <SCENARIO_NAME>Intrusion-0</SCENARIO_NAME>  <EXTRA_DATA>zone=testzone</EXTRA_
DATA>  <TIMESTAMP>2014-03-01T21:24:12.114</TIMESTAMP>  <GUID>77acddf9-e0d4-402e-a497-
231aeee22788</GUID></KEENEO_MESSAGE>
```

- El encabezado del mensaje es el mismo que el mensaje "CONNECTION_TEST".
- El tipo de mensaje es "ALARM_START" y tiene un conjunto de subetiquetas.

– REFERENTIAL es el ID numérico asociado a la cámara.

– TYPE es el tipo de alarma activada por AXIS Perimeter Defender, "INTRUSION" en este ejemplo. Otros tipos posibles son "PRESENCE", "PASSAGE" y "CONDITIONAL".

– SCENARIO_NAME es el nombre del escenario que activó la alarma, tal como se define en la interfaz de configuración. Vea *Configurar el escenario de intrusión/merodeo, on page 27*

– EXTRA_DATA lleva el nombre de zona (o la lista de nombres de zona) implicada en la alarma, como la zona de intrusión.

– TIMESTAMP es la fecha y hora del inicio de la alarma, en el formato AAAA-MM-DDTHH:mm:ss.zzz, donde:
  – AAAA es el año en 4 dígitos, como 2014.
  – MM es el número de mes en 2 dígitos, como 01 para enero.
  – DD es el número de día en 2 dígitos, como 03 para el día 3.
  – "T" es una letra fija
  – HH es la hora en formato de 24 horas, de 00 a 23
  – mm son los minutos en 2 dígitos, de 00 a 59
  – ss son los segundos en 2 dígitos, de 00 a 59
  – zzz son los milisegundos en 3 dígitos, de 000 a 999.
  AXIS Perimeter Defender utiliza la fecha y hora internas de la cámara para generar la marca de tiempo de alarma, por lo que es importante sincronizar la cámara con algún tipo de reloj externo.

– GUID es un identificador único que es constante para todos los mensajes relacionados con la misma alarma (ALARM_START, ALARM_IN_PROGRESS y ALARM_STOP)

Este es el equivalente, en formato de texto, del mensaje ALARM_START:

```
9999|192.168.1.40|0|ALARM_START|INTRUSION|Intrusion-0|2014-03-01T21:24:12.114
```

Ejemplo:
Un mensaje ALARM_IN_PROGRESS en formato XML tiene el siguiente aspecto:

```
<?xml version="1.0"?><KEENEO_MESSAGE xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"         xmlns:xsd="http://www.w3.org/2001/XMLSchema"         VERSION=
"5.0.0"         ID="9999"         TYPE="ALARM_IN_PROGRESS"         SENDER_IP=
"192.168.1.40"         SENDER_PORT="0">   <REFERENTIAL>0</REFERENTIAL>   <TYPE>INTRUSION</
TYPE>   <SCENARIO_NAME>Intrusion-0</SCENARIO_NAME>   <GUID>77acddf9-e0d4-402e-a497-
231aeee22788</GUID></KEENEO_MESSAGE>
```

- El encabezado del mensaje es el mismo que el mensaje "CONNECTION_TEST" y "ALARM_START".
- El tipo de mensaje es "ALARM_IN_PROGRESS" y tiene un conjunto de subetiquetas.

– REFERENTIAL es el ID numérico asociado a la cámara.

– TYPE es el tipo de alarma activada por AXIS Perimeter Defender igual que el correspondiente ALARM_START.

– SCENARIO_NAME es el nombre del escenario que activó la alarma, el mismo de la ALARM_START correspondiente.

– El GUID es el mismo del correspondiente ALARM_START.

El mensaje ALARM_IN_PROGRESS correspondiente en formato TEXTO:

```
9999|192.168.1.40|0|ALARM_IN_PROGRESS|INTRUSION|Intrusion-0|-
```

Ejemplo:
Un mensaje ALARM_STOP en formato XML tiene el siguiente aspecto:

```
<?xml version="1.0"?><KEENEO_MESSAGE xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"         xmlns:xsd="http://www.w3.org/2001/XMLSchema"         VERSION=
"5.0.0"         ID="9999"         TYPE="ALARM_STOP"         SENDER_IP=
"192.168.1.40"         SENDER_PORT="0">   <REFERENTIAL>0</REFERENTIAL>   <TYPE>INTRUSION</
TYPE>   <SCENARIO_NAME>Intrusion-0</SCENARIO_NAME>   <EXTRA_DATA>zone=testzone</EXTRA_
DATA>   <TIMESTAMP>2014-03-01T21:24:26.304</TIMESTAMP>   <GUID>77acddf9-e0d4-402e-a497-
231aeee22788</GUID></KEENEO_MESSAGE>
```

- El encabezado del mensaje es el mismo que en los mensajes anteriores.
- El tipo de mensaje es "ALARM_STOP" y tiene el mismo conjunto de subtipos del mensaje ALARM_START.

El mensaje ALARM_IN_PROGRESS correspondiente en formato TEXTO:

```
9999|192.168.1.40|0|ALARM_STOP|INTRUSION|Intrusion-0|2014-03-01T21:24:26.304
```

La conexión TCP/IP siempre se cierra después de cada mensaje. Por lo tanto, el destinatario tiene que mantener el socket de escucha siempre abierto para poder recibir más notificaciones.

Errores de comunicación

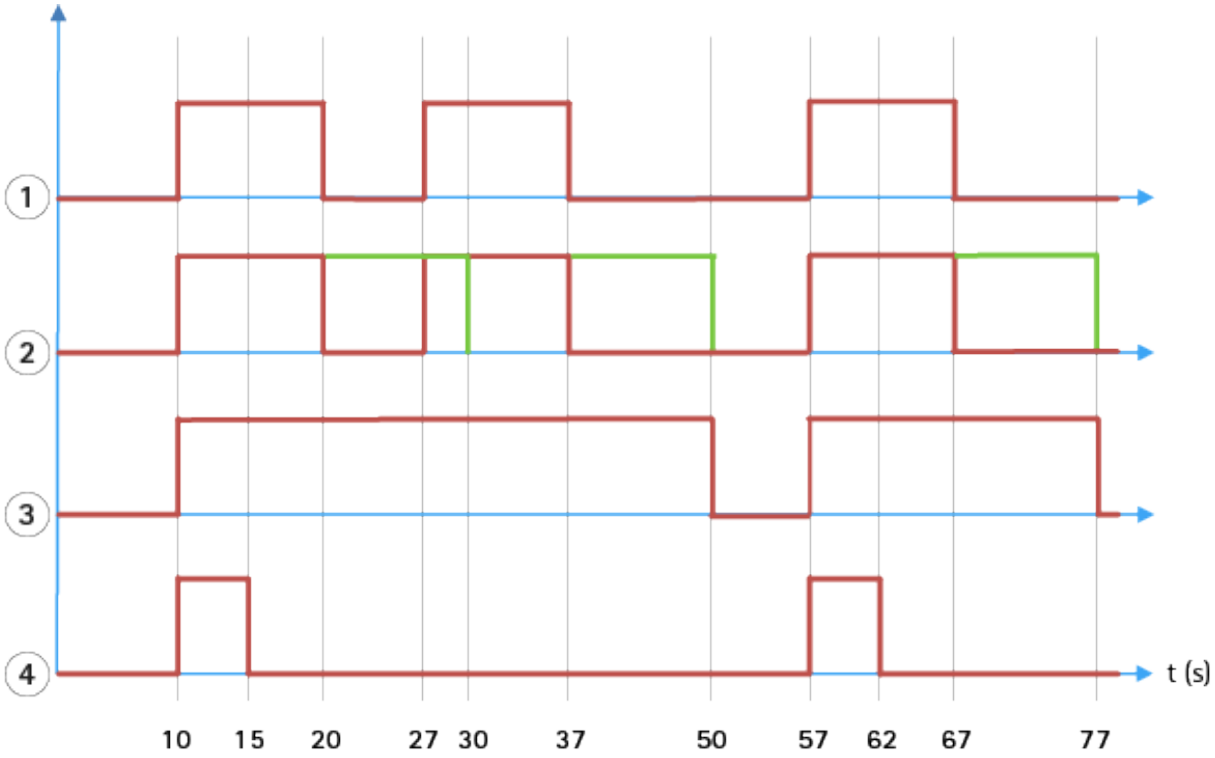
Si el destinatario remoto de las notificaciones XML no es accesible, por ejemplo debido a una desconexión de la red, AXIS Perimeter Defender comienza a almacenar en búfer las alarmas no entregadas internamente y periódicamente (al menos cada 10 segundos) intenta entregarlas de nuevo. Después de un número consecutivo de errores en la entrega de nuevos mensajes (los errores al entregar de nuevo un mensaje desde el búfer no se tienen en cuenta), AXIS Perimeter Defender declara al destinatario como "permanentemente sin conexión" y deja de enviar notificaciones XML al destinatario. El número de errores consecutivos se fija en 20, aproximadamente correspondiente a 4 o 5 alarmas de intrusión de una duración media de 40 segundos cada una. AXIS Perimeter Defender vuelve a enviar notificaciones al mismo destinatario si se produce uno de los siguientes eventos:

- AXIS Perimeter Defender se ha reiniciado.

- Se vuelve a guardar el mismo valor del parámetro "URL de streaming de alarma".

Tiempo posterior a la alarma:

AXIS Perimeter Defender implementa la noción de "tiempo posterior a la alarma". Se define como el intervalo de tiempo después de que se detiene una alarma, durante el cual, si se activa otra alarma, ambas alarmas se fusionan en una única.



1 Tres alarmas activadas por AXIS Perimeter Defender en los tiempos 10, 27 y 57. Cada alarma tiene una duración de 10 segundos, p. ej., un intruso ha tardado 10 segundos en traspasar la zona de intrusión.
2 Se añade un tiempo posterior a la alarma de 10 segundos.
3 Alarmas mediante notificaciones XML y metadatos XML.
4 Alarmas mediante notificaciones por correo electrónico, carga ftp de imágenes, contactos eléctricos y notificaciones básicas TCP/IP.

(2) Observe cómo un tiempo posterior a la alarma de 10 segundos (en verde) aumenta la duración de cada alarma, lo que conduce a la fusión de dos alarmas que están separadas por 10 segundos o menos.

(3) Puede ver el número de alarma resultante y la duración que ha generado AXIS Perimeter Defender a través de notificaciones XML y metadatos XML. El tiempo posterior a la alarma se puede utilizar para obtener menos alarmas más largas en lugar de un número mayor, más cortas y consecutivas.

(4) Para las notificaciones por correo electrónico, la carga de imágenes ftp, los contactos eléctricos y las notificaciones básicas de TCP/IP, el resultado del uso de un tiempo de 10 segundos después de la alarma es diferente. Estas notificaciones solo consideran el inicio de la alarma y no tienen en cuenta la detención de alarma. Por lo tanto, no hay noción de "duración de alarma" cuando se utilizan estas notificaciones y, como consecuencia, el tiempo posterior a la alarma no cambia la duración de la notificación en sí. Siempre se fija al valor elegido por el usuario al configurar la notificación. Por lo tanto, cuando alarmas consecutivas se fusionan en una sola debido al tiempo posterior a la alarma, solo se envía una notificación. Puede ver que AXIS Perimeter Defender fusiona las dos primeras alarmas, enviando de esta forma solo una notificación. Por lo tanto, las notificaciones por correo electrónico, la carga de imágenes ftp, los contactos eléctricos y las notificaciones básicas TCP/IP solo se notifican para dos de ellas. El gráfico muestra una duración fija de 5 segundos para estas notificaciones.

Cómo configurar el tiempo posterior a la alarma

1. Abra la configuración de AXIS Perimeter Defender.
2. Vaya a **Outputs (Salidas)**.
3. Cambie los ajustes de **Post-alarm time (Tiempo posterior a la alarma)**. El valor predeterminado es de 7 segundos.
4. Haga clic en **Asignar**.

Metadatos

Superposición de metadatos incrustados

La superposición de metadatos integrada es una característica que puede trazar detecciones de análisis para transmisiones en directo seleccionadas directamente en la cámara. Las detecciones son superposiciones gráficas en forma de cuadros delimitadores y líneas de trayectorias. Las transmisiones se seleccionan en función de su resolución y, si el dispositivo es compatible con áreas de visualización, en un área de visualización. Los metadatos integrados se muestran en la visualización en directo y durante la reproducción de material grabado.

Superposición de metadatos integrada en transmisiones seleccionadas

Por ejemplo, puede configurar la aplicación para que añada superposiciones en todas las transmisiones con resolución 640x480. En ese caso, solo las transmisiones con esta resolución tendrán la superposición y los demás no experimentarán cambios.

Superposición de metadatos integrados en áreas de visualización seleccionadas

Si se admite, también puede indicar un área de visualización junto con la resolución. Por ejemplo, puede optar por añadir superposiciones en las transmisiones recuperadas del área de visión número 3 a una resolución de 1280x720. En este caso, solo las transmisiones que coincidan con esta configuración tendrán las superposiciones, mientras que las demás no experimentarán cambios, tampoco las obtenidas del área de visión 3 pero a una resolución diferente ni las obtenidas a 1280x720 pero no del área de visión 3.

Añadir metadatos integrados a la transmisión de vídeo

Nota

Esta función solo está disponible en dispositivos con la versión del software 7.30 o superior.

Este ejemplo explica cómo activar las superposiciones de metadatos grabados en todas las transmisiones de vídeo con una resolución de 640x480. Las transmisiones de vídeo con cualquier otra resolución no se ven afectadas.

1. Seleccione la cámara en el panel con las vistas en directo.
2. Vaya a **Outputs > Burn-in Metadata superposición (Salidas > Superposición de metadatos integrada)**.
3. Seleccione **Habilitado**.
4. En la lista desplegable, seleccione la resolución 640x480.
5. Haga clic en **Aplicar**.
6. Compruebe que los metadatos aparecen en la visualización en directo para esa resolución.

Integración con VMS

AXIS Perimeter Defender se integra perfectamente con los siguientes sistemas de gestión de vídeo (VMS):

- Security Center de Genetec™
- XProtect® de Milestone

Para obtener información acerca de las versiones de VMS compatibles, consulte *axis.com/products/axis-perimeter-defender/support-and-documentation*

Las alarmas activadas por AXIS Perimeter Defender se convierten automáticamente en eventos en el VMS, que a su vez pueden activar un amplio conjunto de acciones y aprovechar toda la potencia del VMS. En paralelo, los metadatos en directo generados por AXIS Perimeter Defender se envían al VMS para su visualización y grabación

en directo. Por lo tanto, los metadatos también están disponibles al reproducir las secuencias de vídeo grabadas en el modo de reproducción.

Un sistema automatizado de detección de intrusiones está diseñado para activar alarmas y proporcionar información que ayuda a informar para la intervención de seguridad. Este aspecto puede incluir proporcionar un mensaje a un dispositivo móvil o mostrar el evento de alarma dentro de un VMS que puede incluir el asunto que creó el evento de alarma resaltado en pantalla.

Integración estándar de eventos

AXIS Perimeter Defender aprovecha las interfaces y funciones nativas de ACAP para el envío de alarmas e información complementaria a dispositivos externos o VMS. Los eventos emitidos por AXIS Perimeter Defender pueden convertirse en mensajes para el VMS, si tienen reglas de acción asociadas.

Están disponibles los siguientes canales de alarma desde la cámara hasta el VMS:

- Notificaciones básicas de texto libre para alarmas (TCP/IP)
- Salidas eléctricas (contactos secos o mojados)
- Notificaciones por correo electrónico
- Carga ftp de imágenes de alarma

Estas integraciones se pueden configurar en la cámara. Vea *Tiempo posterior a la alarma:, on page 35*.

Puentes VMS

Proporcionamos módulos de integración predesarrollados, denominados "puentes", para los siguientes sistemas de gestión de vídeo (VMS):

- Milestone XProtect® 2014 y 2016 Corporate/Expert/Enterprise/Professional/Express. Las ediciones Enterprise/Professional/Express no son compatibles con metadatos (no hay visualización de metadatos en directo o en reproducción)
- Genetec™ Service Center 5.3 y 5.4 Pro/Enterprise/SV32/SV16

Los puentes proporcionan dos integraciones:

- Creación de eventos de alarma personalizados en el VMS que coincidan con los eventos de salida de AXIS Perimeter Defender.
- Visualizar superposiciones de alarma, o cuadros delimitadores, encima del material de vídeo en directo y grabado desde estos (excepto para las ediciones Milestone XProtect® Enterprise/Professional/Express).

Debe descargar e instalar los puentes VMS como aplicaciones independientes. Para más información sobre cómo instalar y configurar estos puentes, vea el manual del usuario para el puente concreto.

Cree una regla en AXIS Camera Station.

En esta sección se explica cómo integrar AXIS Perimeter Defender con el sistema de eventos de AXIS Camera Station. Aprenderá a:

- Configurar una regla de AXIS Camera Station para que se active cuando se produzca una intrusión.
- Comprobar que la configuración se realice correctamente.

1. Configurar y calibrar AXIS Perimeter Defender en el software de configuración de AXIS Perimeter Defender. Para obtener ayuda con la instalación y calibración de AXIS Perimeter Defender, consulte el manual de usuario de AXIS Perimeter Defender o *la página del producto*.
2. Añada la cámara a AXIS Camera Station siguiendo el asistente **Agregar cámara**.
3. Configurar un activador Evento de dispositivo:
   3.1. Vaya a **Configuración** > **Grabación y eventos** y abra la pestaña **Reglas avanzadas**.
   3.2. Cree una nueva regla y seleccione el activador **Evento de dispositivo**.

3.3. Seleccione la cámara en la que esté instalado AXIS Perimeter Defender.

3.4. En la lista **Evento**, seleccione **AXISPerimeterDefender**.

3.5. En la lista **Función**, seleccione el nombre de la intrusión configurada (en este caso, "Intrusion-1"). Si quiere activar la regla para todos los escenarios configurados, seleccione **ALL_SCENARIOS**.

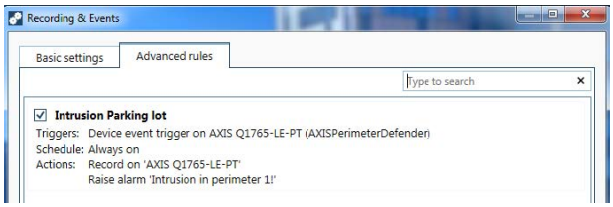
3.6. Seleccione **Sí** si se debe activar el activador cuando se produzca una intrusión. Cuando se detecta una intrusión, la ventana Actividad mostrará un cambio de estado que ayudará a comprobar si la configuración es correcta.

3.7. Haga clic en **Aceptar** y **Siguiente** para configurar las acciones.

3.8. En el cuadro de diálogo **Agregar acción**, puede agregar una o varias acciones para la regla.

En este ejemplo, añadimos una acción de grabación y una acción de alarma.

3.9. Haga clic en **Finish** (Finalizar).



En el ejemplo se muestra una regla que activa dos acciones cuando se produce una intrusión.

4. Compruebe que la configuración funciona como debe simulando una intrusión, por ejemplo accediendo físicamente al área supervisada.

Interfaz web

A partir de AXIS Perimeter Defender 4.0, ahora puede acceder a una interfaz web que permite configurar escenarios sin necesidad de tener instalada la aplicación de escritorio.

Para acceder a la interfaz web:

- Abra un navegador web.
- Introduzca la dirección IP del dispositivo
- Vaya a Apps (Aplicaciones)
- Vaya a **AXIS Perimeter Defender** en la lista y haga clic en **Open (Abrir)**.

Nota

La calibración aún no está disponible en la interfaz web. Para calibrar la cámara, utilice la aplicación de escritorio. Para obtener más información, vaya a *Calibrar - AXIS Perimeter Defender, on page 19*

Escenarios

Crear un escenario de intrusión

El escenario de intrusión está diseñado para activar una alarma cuando un objeto entra en una zona definida y permanece en ella durante un tiempo superior al establecido.

Para crear un escenario de intrusión:

1. Vaya a **Scenarios (Escenarios)** en la interfaz web.
2. Haga clic en **+ Create (Crear)**.
3. Seleccione **Intrusion (Intrusión)**.
4. Haga clic en **Select this template (Seleccionar esta plantilla)**.
5. Escoja un nombre descriptivo personalizado para el escenario
6. Seleccione qué tipo de objetos deben activar una alarma.
7. Para reformar la zona de detección predeterminada, arrastre los puntos de anclaje en cualquier dirección. Una vez movido un punto de anclaje, se crearán nuevos puntos para personalizar aún más la forma.
8. En **Intrusion zone (Zona de intrusión)**, si no desea que un objeto active una alarma tan pronto como entre en la zona establecida, ajuste la **Minimum presence in zone (Presencia mínima en la zona)**.
9. Si la zona es estrecha y se puede cruzar en 1-2 segundos, y todavía desea que se activen las alarmas, seleccione **Narrow zone (Zona estrecha)**. Para obtener más información, vea *Parámetro de duración, on page 27*.
10. Haga clic en **Save (Guardar)**.

Crear un escenario de cruce de zonas

El escenario de cruce de zonas está diseñado para activar una alarma cuando un objeto se mueve de una zona predefinida a otra restringida.

Para crear un escenario de cruce de zonas:

1. Vaya a **Scenarios (Escenarios)** en la interfaz web.
2. Haga clic en **+ Create (Crear)**.
3. Seleccione **Zone crossing (Cruce de zona)**.
4. Haga clic en **Select this template (Seleccionar esta plantilla)**.
5. Escoja un nombre descriptivo personalizado para el escenario

6. Seleccione qué tipo de objetos deben activar una alarma.
7. Para reformar las zonas predeterminadas, arrastre los puntos de anclaje en cualquier dirección. Una vez movido un punto de anclaje, se crearán nuevos puntos para personalizar aún más la forma.
8. En **Zone 1 (Zona 1)**, si no desea que un objeto active una alarma tan pronto como entre en la zona establecida, ajuste la **Minimum presence in zone (Presencia mínima en la zona)**.
9. Si la zona es estrecha y se puede cruzar en 1-2 segundos, y todavía desea que se activen las alarmas, seleccione **Narrow zone (Zona estrecha)**. Para obtener más información, vea *Parámetro de duración, on page 27*.
10. Para decidir qué zona debe restringirse, haga clic en la flecha direccional junto a **Restricted zone entry (Entrada a zona restringida)**. Por defecto, la **Zone 2 (Zona 2)** es la restringida.
11. Establezca los parámetros de la **Zone 2 (Zona 2)**.
12. Haga clic en **Save (Guardar)**.

Crear un escenario condicional

El escenario condicional le otorga la libertad de definir las condiciones de activación de alarmas en una escena.

Para crear un escenario condicional:

1. Vaya a **Scenarios (Escenarios)** en la interfaz web.
2. Haga clic en **+ Create (Crear)**.
3. Seleccione **Conditional (Condicional)**.
4. Haga clic en **Select this template (Seleccionar esta plantilla)**.
5. Escoja un nombre descriptivo personalizado para el escenario
6. Seleccione qué tipo de objetos deben activar una alarma.
7. Si necesita más zonas que las predeterminadas, haga clic en **+ Add zone (Añadir zona)**
8. Seleccione la zona de intrusión en el menú desplegable, bajo **Intrusion Zone (Zona de intrusión)**. Las flechas indican la relación de las distintas zonas con la zona de intrusión seleccionada.
9. Para reformar las zonas predeterminadas, arrastre los puntos de anclaje en cualquier dirección. Una vez movido un punto de anclaje, se crearán nuevos puntos para personalizar aún más la forma.
10. Si no desea que un objeto active una alarma tan pronto como entre en la zona establecida, ajuste la **Minimum presence in zone (Presencia mínima en la zona)**.
11. Si la zona es estrecha y se puede cruzar en 1-2 segundos, y todavía desea que se activen las alarmas, seleccione **Narrow zone (Zona estrecha)**. Para obtener más información, vea *Parámetro de duración, on page 27*.
12. Haga clic en **Save (Guardar)**.

Editar escenarios

Para editar un escenario que haya creado en la interfaz web o en la aplicación de escritorio:

1. Vaya a **Scenarios (Escenarios)** en la interfaz web.
2. Haga clic en **Edit (Editar)** en el escenario que desea modificar.
3. Haga clic en **Save (Guardar)** cuando haya terminado.

Renombrar escenarios

Para cambiar el nombre de varios escenarios a la vez:

1. Seleccione los escenarios que desea renombrar
2. Haga clic en **Rename (Renombrar)**, ahora disponible en el menú.
3. Cambie los nombres a su gusto.

4. Haga clic en **Save (Guardar)**.

Eliminar escenarios

Para eliminar varios escenarios a la vez:

1. Seleccione los escenarios que desea eliminar
2. Haga clic en **Delete (Eliminar)**, ahora disponible en el menú.
3. Para confirmar, haga clic en **Delete (Eliminar)**.

Ajustes

La interfaz web cuenta con un panel de ayuda integrado con información sobre las distintas configuraciones de cada página. Haga clic en el icono de ayuda (?) para acceder al panel.

Localización de problemas

Para que todas las funcionalidades funcionen según lo esperado, es obligatorio configurar los siguientes parámetros de Axis:

- Red / TCP-IP / Básica / Router predeterminado
- Red / TCP-IP / Avanzada / Nombre de dominio
- Red / TCP-IP / Servidor DNS primario
- Red / TCP-IP / Servidor DNS secundario
- Red / TCP-IP / Dirección del servidor NTP
- Red / TCP-IP / SMTP (email)
- Opciones del sistema / Fecha y hora / Zona horaria
- Opciones del sistema / Fecha y hora / Sincronizar con servidor NTP

Actualizar a la última versión

Para disfrutar de las últimas mejoras sin tener que volver a calibrar y redefinir escenarios, le recomendamos que actualice a la versión más reciente de AXIS Perimeter Defender.

1. Descargue e instale la versión más reciente de AXIS Perimeter Defender.
2. Haga clic en **Instalar**. El programa de instalación de AXIS Perimeter Defender realiza automáticamente los pasos necesarios para completar la instalación:

– Copia de seguridad de la calibración, los escenarios, los parámetros y la licencia existentes.

– Instalación de la nueva versión.

– Restauración de la licencia.

– Restauración de la calibración y los escenarios.

– Restauración de parámetros.

– Si una aplicación estaba en ejecución, se reiniciará.

Actualizar el software de la cámara

Nota

Antes de actualizar el software de la cámara, guarde todos los ajustes de AXIS Perimeter Defender. La actualización del software elimina la aplicación y su configuración de la cámara. Si se guardan los ajustes, se pueden restaurar mediante el programa de instalación de AXIS Perimeter Defender.

1. Utilice el programa de instalación de AXIS Perimeter Defender para guardar la configuración de la instalación.
2. Actualice el software de la cámara. Para obtener instrucciones, consulte el Manual de usuario de la cámara.
3. Inicie el programa de instalación de AXIS Perimeter Defender.
4. Utilice la opción de carga de instalación para cargar automáticamente la configuración guardada de la instalación para cada cámara actualizada.

Resolución de problemas de instalación

Problema	Posible razón	Solución
Se muestra un mensaje de Windows® que indica que no es posible instalar el software.	El sistema operativo del ordenador portátil o PC no es compatible.	Compruebe que el sistema operativo Windows® coincide con las especificaciones de requisitos.
Se muestra un mensaje de Windows® que indica que la instalación ha sido incorrecta.	Windows® Compatibility Assistant ha detectado un posible problema con la instalación.	Confirme que la instalación es correcta de todos modos y continúe.
La instalación presenta un error durante la instalación de XVID.	La instalación de XVID presenta un error debido a una antigua instalación parcial de XVID presente en el ordenador.	Elimine la carpeta XVID en C:\Program Files (x86) y pruebe a repetir la instalación.
El paquete del instalador se bloquea repentinamente después de la visualización del EULA. Se muestra un mensaje de error de Windows® que la aplicación se ha cerrado de manera inusual. Es imposible cerrar el instalador.	Un problema conocido en los instaladores conduce a un bloqueo de la aplicación en algunas circunstancias.	Abra el administrador de tareas y finalice todos los procesos "msiexec.exe". A continuación, finalice el proceso del instalador y reinicie el instalador.

Resolución de problemas de configuración

Problema	Posible razón	Solución
Problemas para abrir AXIS Perimeter Defender.	No dispone de suficientes derechos de usuario de Windows®.	Asegúrese de que tiene derechos de administrador.
La funcionalidad de búsqueda no encuentra mis cámaras.	Firewall	En ocasiones, los firewalls y el software antivirus pueden bloquear la detección de cámaras. Si es necesario, configure el firewall para permitir el tráfico de red hacia y desde AXIS Perimeter Defender. Si esto no resolviese el problema, configure el firewall para abrir los siguientes puertos: UDP, puerto 5353 y TCP, puerto 80.
	Problemas de dirección IP	Cualquier dispositivo perteneciente a una red debe contar con una dirección IP exclusiva para poder comunicarse con otros dispositivos. Cuando se utiliza AXIS Perimeter Defender, se recomienda utilizar direcciones IP fijas para las cámaras. Asegúrese que cada dispositivo IP en la red tiene su propia dirección IP y no reutiliza una dirección IP ya en uso.
	La cámara no está disponible desde el ordenador del usuario.	En un navegador, vaya a la dirección IP de la cámara para confirmar si está disponible o no. Si no puede acceder a ella, la cámara no se ha instalado

Problema	Posible razón	Solución
		correctamente en la red o el ordenador no tiene acceso a la cámara.
No es posible añadir una cámara.	Los parámetros de conexión de la cámara, por ejemplo la dirección IP, la contraseña o el puerto HTTP, son incorrectos.	Compruebe que los parámetros introducidos son correctos y repita el proceso.
	La cámara no se puede ver desde el ordenador del usuario.	En un navegador, vaya a la dirección IP de la cámara para confirmar si está disponible o no. Si no puede localizarla, entonces la cámara no se ha instalado correctamente en la red o el ordenador no tiene acceso a la red en la que está encendida la cámara.
Pérdida de secuencias de vídeo en la instalación de AXIS Perimeter Defender.	La fuente de vídeo ya no está disponible.	La fuente de vídeo se ha interrumpido y no se ha actualizado en la pantalla.
	Utilice un navegador para comprobar si la cámara está disponible.	Haga clic en la ventana donde debería mostrarse la transmisión y cambie el tamaño de la interfaz; la transmisión debería reaparecer.
La calibración automática no funciona o produce malos resultados.	No se cumplen los requisitos previos.	Asegúrese de que se cumplen los requisitos de montaje. Vea *Montar la cámara, on page 13*.
	La cámara se tambalea.	No es posible calibrar una cámara que se tambalea.
	Conexión lenta a una cámara no configurada como remota.	Conecte la cámara como dispositivo remoto para reducir los requisitos de ancho de banda.
	Hay otros objetos en movimiento en la escena utilizada para la calibración automática, como vehículos, árboles u otras personas.	Repita la calibración automática o calibre el dispositivo manualmente.
	El campo de visión está abarrotado, haciendo que la persona que camina frente a la cámara quede oculta parcialmente la mayor parte del tiempo.	Calibre el dispositivo manualmente.
	El campo de visión es pequeño, como las entradas.	Calibre el dispositivo manualmente.
	El vídeo de captura no se grabó correctamente debido a un espacio en disco insuficiente.	Compruebe que hay suficiente espacio de disco y que la aplicación tiene permisos para guardar la grabación de vídeo en el ordenador donde se ejecuta la interfaz de AXIS Perimeter defender.

Resolución de problemas de operación

Problema	Posible razón	Solución
La aplicación no se ejecuta aunque la configuración es correcta.	El software de la cámara no está actualizado.	Asegúrese de que tiene el software más reciente para la cámara.
La superposición no se muestra en el programa de instalación de AXIS Perimeter Defender, pero se está ejecutando el análisis.	La aplicación se bloquea después de una operación de inicio o de parada o tras una actualización del paquete de AXIS Perimeter Defender.	Reinicie la cámara.
	Un firewall está bloqueando la conexión al puerto de escucha de metadatos de la cámara.	Configure el firewall para permitir que la interfaz de configuración conecte con el puerto de escucha de metadatos en la cámara.
	Un programa antivirus está bloqueando la recepción de la superposición.	Configure el antivirus para permitir que se reciba la superposición.
No se activan alarmas en la instalación de AXIS Perimeter Defender en el equipo de configuración, aunque el análisis se está ejecutando y la superposición es visible.	Aunque el objetivo está en la escena, no coincide con un escenario condicional, por ejemplo, no se mueve de una zona a otra en el escenario de traspaso de zona.	Asegúrese de que el escenario se ha especificado correctamente, incluidas las condiciones.
	Detección deficiente.	Asegúrese de que se cumplen los requisitos de montaje. Vea *Montar la cámara, on page 13*. Asegúrese también de que la calibración es lo suficientemente precisa y de que la sensibilidad es lo suficientemente alta.

Revolución de problemas de rendimiento

Problema	Posible razón	Solución
La imagen en pantalla y los análisis se conectan y desconectan continuamente.	La carga de la CPU de la cámara es demasiado alta.	Posibles soluciones: • No visualice transmisiones de la cámara innecesariamente: cada una aumenta la carga de la CPU. • Si está activada la grabación en caso de detección de movimiento, pruebe a reducir la calidad de la grabación para no sobrecargar la CPU. • Desactive la grabación en caso de detección de movimiento y compruebe que la detección de movimiento integrada esté desactivada.
La velocidad de fotogramas de vídeo mostrada es muy baja.	Cuando hay demasiadas visualizaciones de transmisiones de vídeo, la velocidad de fotogramas puede bajar de los 8 fps, el ajuste predeterminado.	No visualice transmisiones de la cámara innecesariamente: cada una aumenta la carga de la CPU.
Un objetivo entra en la zona estéril y activa varias alertas.	La alarma dura demasiado poco.	Ajuste la duración de la alarma. Vaya a AXIS Perimeter Defender Setup > **Outputs (Configuración > Salidas)**.
Un objetivo potencial entra en la zona estéril, pero no genera una alerta, por lo que no se detecta.	Falta contraste entre el objeto y el fondo.	Asegúrese de que se cumplen los requisitos de montaje. Vea *Montar la cámara, on page 13*.
	La iluminación de la escena es inadecuada o el rendimiento de la cámara con poca luz no es suficiente.	Asegúrese de que se cumplen los requisitos de montaje. Vea *Montar la cámara, on page 13*.
	AXIS Perimeter Defender tiene la sensibilidad establecida demasiado baja.	Aumente la sensibilidad en los parámetros globales del escenario.
	La cámara se ha movido y ahora la calibración es incorrecta.	Vuelva a realizar la calibración.
	La calibración no es lo suficientemente precisa.	Verifique la calibración de la cámara. Vaya a la instalación de AXIS Perimeter Defender.
	Aunque el objetivo está en la escena, no cumple con los requisitos de un escenario condicional. Por ejemplo, en el escenario de traspaso de zona, el objeto no va de una zona a otra.	Asegúrese de que el escenario se ha especificado correctamente, incluidas las condiciones.

Problema	Posible razón	Solución
El objetivo se detecta, pero se clasifica incorrectamente (persona como vehículo o vehículo como persona).	La altura, el posicionamiento o la orientación de la cámara son incorrectos.	Asegúrese de que se cumplen los requisitos de montaje. Vea *Montar la cámara, on page 13*.
	La cámara está demasiado lejos de la zona.	Asegúrese de que se cumplen los requisitos de montaje. Vea *Montar la cámara, on page 13*.
	La calibración no es lo suficientemente precisa.	Verifique la calibración de la cámara. Vaya a la instalación de AXIS Perimeter Defender.
AXIS Perimeter Defender genera una alarma cuando no hay una intrusión en la zona estéril.	La sensibilidad del análisis es demasiado alta.	Disminuya la sensibilidad. Vaya a la instalación de AXIS Perimeter Defender.
	La calibración no es lo suficientemente precisa.	Verifique la calibración de la cámara. Vaya a la instalación de AXIS Perimeter Defender.
	La cámara se ha movido y ahora la calibración es incorrecta.	Vuelva a realizar la calibración.
	La altura, posicionamiento u orientación de la cámara son incorrectos.	Asegúrese de que se cumplen los requisitos de montaje. Vea *Montar la cámara, on page 13*.
	La cámara se mueve, se balancea o vibra.	Tome medidas para que la instalación de la cámara sea más estable.
	Hay vegetación, banderas u otros objetos en movimiento cerca de la cámara.	Retire del campo de visión de la cámara los elementos que interfieren. AXIS Perimeter Defender ignora los objetos que están constantemente en la escena pero no cerca de la cámara.
	Hay insectos sobre el objetivo de la cámara o cerca.	Tome medidas para evitar que los insectos penetren en el objetivo de la cámara o se acerquen a él.

Sobre este manual

Este manual está destinado a administradores y usuarios de AXIS Perimeter Defender. Incluye instrucciones para usar y administrar el producto en su red. Experiencia previa de redes de uso al utilizar este producto.

Reconocimiento de marcas comerciales

T10068952_es

2026-03 (M17.3)