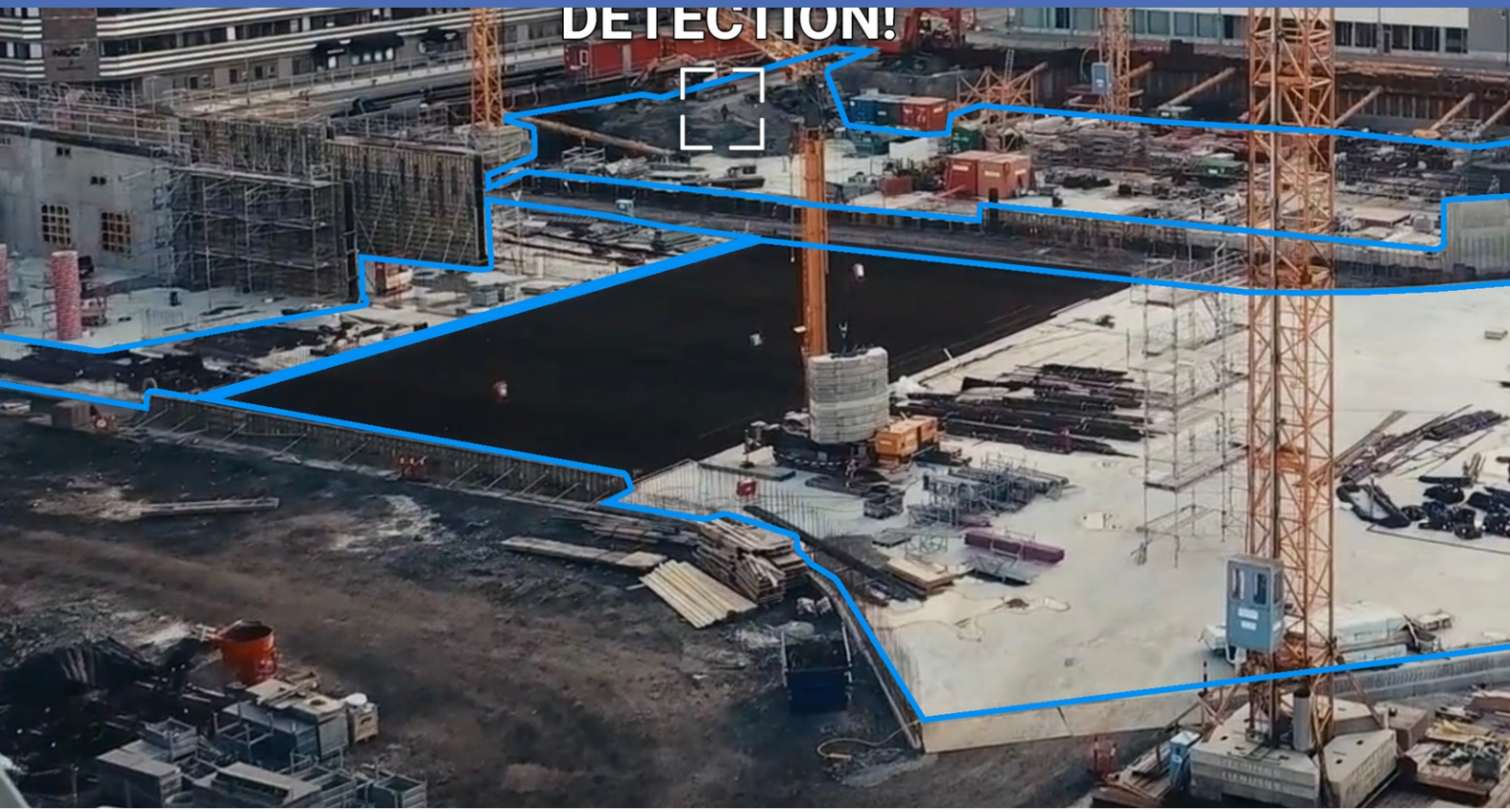
Guía

Irisity IRIS AI Analytics - Intrusion Detection



BeyondHumanVision

MOBOTIX

V1.09_16/03/2023, Código de pedido: Mx-APP-IRIS-C-INT

Índice

1

Antes de empezar

Soporte

Si necesita soporte técnico, póngase en contacto con su distribuidor MOBOTIX. Si su distribuidor no puede ayudarle, se pondrá en contacto con el canal de soporte para obtener una respuesta lo antes posible.

Si dispone de acceso a Internet, puede abrir el servicio de soporte técnico de MOBOTIX para buscar información adicional y actualizaciones de software. Visite:

www.mobotix.com > Support > Help Desk (www.mobotix.es > Soporte > Servicio de asistencia)

Notas de seguridad

- Este producto no debe utilizarse en lugares expuestos a riesgos de explosión.
- No utilice el producto en un lugar donde haya mucho polvo.
- Proteja el producto contra la entrada de humedad o agua en la carcasa.
- Instale este producto tal como se describe en este documento. Una instalación defectuosa puede dañar el producto.
- Este equipo no es adecuado para su uso en lugares donde es probable que haya niños presentes.
- Si utiliza un adaptador de Clase I, el cable de alimentación debe conectarse a una toma de corriente con una conexión a tierra adecuada.
- Para cumplir los requisitos de EN 50130-4 relativos al funcionamiento ininterrumpido de las fuentes de alimentación de los sistemas de alarma, se recomienda utilizar un sistema de alimentación ininterrumpida (SAI) para apoyar el suministro de alimentación del producto.
- Este equipo solo se debe conectar a redes PoE que no direccionen a otras redes.

Notas legales

Aspectos legales de la grabación de vídeo y sonido

Debe cumplir todas las normativas de protección de datos para el control de vídeo y sonido cuando utilice productos MOBOTIX AG. Según la legislación nacional y la ubicación de instalación de las cámaras, la grabación de datos de vídeo y sonido puede estar sujeta a documentación especial o puede estar prohibida. Por lo tanto, todos los usuarios de productos MOBOTIX deben familiarizarse con todas las normativas aplicables y cumplir estas leyes. MOBOTIX AG no se hace responsable del uso ilegal de sus productos.

Declaración de conformidad

Los productos de MOBOTIX AG están certificados de acuerdo con las normativas aplicables de la CE y de otros países. Puede encontrar las declaraciones de conformidad para los productos de MOBOTIX AG en www.-mobotix.com en **Support > Download Center > Marketing & Documentation > Certificates & Declarations of Conformity** (Soporte > Centro de descargas > Marketing y documentación > Certificados y declaraciones de conformidad).

Declaración de RoHS

Los productos de MOBOTIX AG cumplen plenamente con las restricciones de la Unión Europea sobre el uso de determinadas sustancias peligrosas en aparatos eléctricos y electrónicos (Directiva 2011/65/UE) (RoHS) en cuanto a su sujeción a estas normativas (para obtener la declaración de RoHS de MOBOTIX, consulte www.-mobotix.com, **Support > Download Center > Marketing & Documentation > Brochures & Guides > Certificates** [Soporte > Centro de descargas > Marketing y documentación > Folletos y guías > Certificados]).

Eliminación

Los productos eléctricos y electrónicos contienen numerosos materiales valiosos. Por este motivo, le recomendamos que deseche los productos de MOBOTIX al final de su vida útil de acuerdo con todos los requisitos legales y normativas (o depósitelos en un centro de recogida municipal). Los productos de MOBOTIX no deben desecharse en la basura doméstica. Si el producto contiene alguna batería, deséchela por separado (los manuales del producto correspondientes contienen instrucciones específicas cuando el producto contiene alguna batería).

Descargo de responsabilidad

MOBOTIX AG no asume ninguna responsabilidad por daños que sean a consecuencia de un uso inadecuado o de un incumplimiento de los manuales o de las normas y reglamentos aplicables. Se aplican nuestros términos y condiciones generales. Puede descargar la versión actual de los **Términos y condiciones generales** de nuestro sitio web en www.mobotix.com, haciendo clic en el enlace correspondiente en la parte inferior de cada página.

Acerca de Irisity IRIS AI Analytics - Intrusion Detection

Detectar actividad humana en zonas armadas

Irisity IRIS AI Analytics - Intrusion Detection activa alarmas cuando se entra sin autorización en zonas restringidas. El algoritmo ofrece detecciones precisas de actividad humana a largas distancias y en áreas extensas. La aplicación tiene una precisión de hasta el 99 %. La aplicación se puede probar de forma gratuita durante 30 días y se puede activar durante un periodo de tiempo ilimitado. Las detecciones de presencia humana también incluyen vehículos como bicicletas, coches y camiones, incluso en condiciones climáticas adversas y con mala iluminación.

- Detecta la intrusión de objetos de interés en zonas/áreas de detección definidas por el usuario
- Diseñado para la detección fiable de personas y vehículos que cubren solo pequeñas partes del campo de visión
- Reducción de falsas alarmas al mínimo mediante el filtrado de movimiento no crítico (por ejemplo, árboles, nubes, etc.)
- Detección simultánea en uno o más sensores de imagen
- Eventos de MOBOTIX a través de MxMessageSystem
- Búsqueda consolidada de eventos mediante la interfaz MxManagementCenter Smart Data y MOBOTIX HUB

ATENCIÓN! Esta aplicación no admite módulos de sensores térmicos ECO.

Interfaz de Smart Data para MxManagementCenter

Esta aplicación cuenta con una interfaz de Smart Data para MxManagementCenter.

Con el sistema MOBOTIX Smart Data, los datos de transacciones se pueden vincular a las grabaciones de vídeo realizadas en el momento de las transacciones. Las fuentes de Smart Data pueden ser, por ejemplo, las aplicaciones MOBOTIX certificadas (no se requiere licencia) o fuentes de Smart Data generales (se requiere licencia), como sistemas TPV o sistemas de reconocimiento de matrículas.

El sistema Smart Data de MxManagementCenter permite buscar y revisar rápidamente cualquier actividad sospechosa. La barra Smart Data y la vista Smart Data están disponibles para buscar y analizar transacciones. La barra Smart Data proporciona una visión general directa de las transacciones más recientes (de las últimas 24 horas) y, por este motivo, resulta conveniente utilizarla para revisiones y búsquedas.

AVISO! Para obtener información sobre cómo usar el sistema Smart Data, consulte la ayuda online correspondiente del software de la cámara y MxManagementCenter.

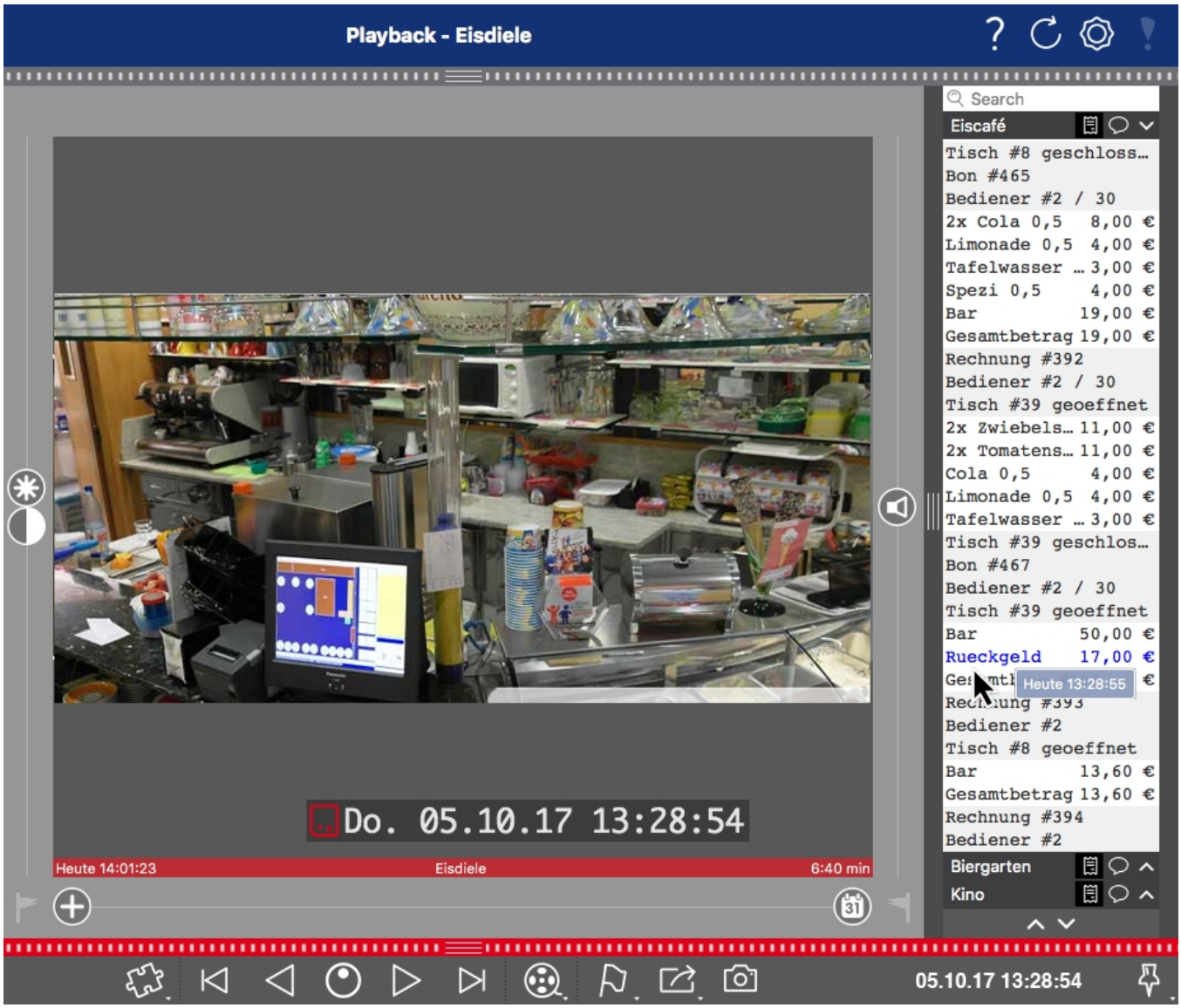


Fig. 1: : Barra Smart Data en MxManagementCenter (ejemplo: sistema TPV)

Especificaciones técnicas

Información del producto

Nombre del producto	Irisity IRIS AI Analytics - Intrusion Detection
Código de pedido	Mx-APP-IRIS-C-INT
Compatibles Cámaras MOBOTIX	Mx-M73A, Mx-S74A
Versión de firmware mínima de la cámara	V7.3.0.x
MxManagementCenter Integración de	■ mín. MxMC v2.5.3 ■ Configuración: Se requiere una licencia de configuración avanzada ■ Investigar: Licencia de interfaz de Smart Data incluida

Características del producto

Funciones de la aplicación	■ Detecta la intrusión de objetos de interés en zonas/áreas de detección definidas por el usuario ■ Diseñado para la detección fiable de personas y vehículos que cubren solo pequeñas partes del campo de visión ■ Reducción de falsas alarmas al mínimo mediante el filtrado de movimiento no crítico (por ejemplo, árboles, nubes, etc.) ■ Detección simultánea en uno o más sensores de imagen ■ Eventos de MOBOTIX a través de MxMessageSystem ■ Búsqueda consolidada de eventos mediante la interfaz MxManagementCenter Smart Data y MOBOTIX HUB
Número máximo de zonas de reconocimiento	20
Formatos de metadatos/estadísticas	JSON
Licencia de prueba	Licencia de prueba de 30 días preinstalada
MxMessageSystem admitidos	Sí

Eventos MOBOTIX	Sí
Eventos de ONVIF	Sí (evento de mensaje genérico)

Requisitos de escena

Altura mínima de los objetos	20 px/~6 % de la altura de la imagen (análisis bloqueado actualmente a una resolución de 640 x 360)
Altura de montaje de la cámara	mín. 2 m (teniendo en cuenta los requisitos de la escena, entre 5 y 20 m suele ser óptima)
Ángulo vertical máximo	180°
Ángulo horizontal máximo	180°
Ángulo de inclinación máximo	Solo inclinación hacia abajo: sin límite

Especificaciones técnicas de la aplicación

Aplicación sincrónica/asincrónica	Asincrónica
Precisión	> 99 % (en función de los requisitos de la escena)
Número de procesamiento de fotogramas por segundo	Típ. 10 fps
Tiempo de detección	~2 seg.

Licencias de aplicaciones certificadas

Las siguientes licencias están disponibles para la Irisity IRIS AI Analytics - Intrusion Detection:

- **Licencia de prueba de 30 días** preinstalada
- **licencia comercial permanente**

El periodo de uso comienza con la activación de la interfaz de la aplicación (consulte)

AVISO! Para comprar o renovar una licencia, póngase en contacto con su socio de MOBOTIX.

AVISO! Las aplicaciones generalmente vienen preinstaladas con el firmware. En ocasiones poco frecuentes, es necesario descargar las aplicaciones desde el sitio web e instalarlas. En ese caso, consulte **www.-mobotix.com/es > Support > Download Center > Marketing & Documentation (Soporte > Centro de descargas > Marketing y Documentación)**, descargue e instale la aplicación.

Activación de licencia de las aplicaciones certificadas en MxManagementCenter

Tras el periodo de prueba, se deben activar las licencias comerciales para su uso con una clave de licencia válida.

Activación online

Cuando reciba los ID de activación, actívelos en MxMC de la siguiente manera:

1. Seleccione en el menú **Window > Camera App Licenses** (Ventana > Licencias de aplicaciones de cámara).
2. Seleccione la cámara para la que desea utilizar la licencia y haga clic en **Select** (Seleccionar).

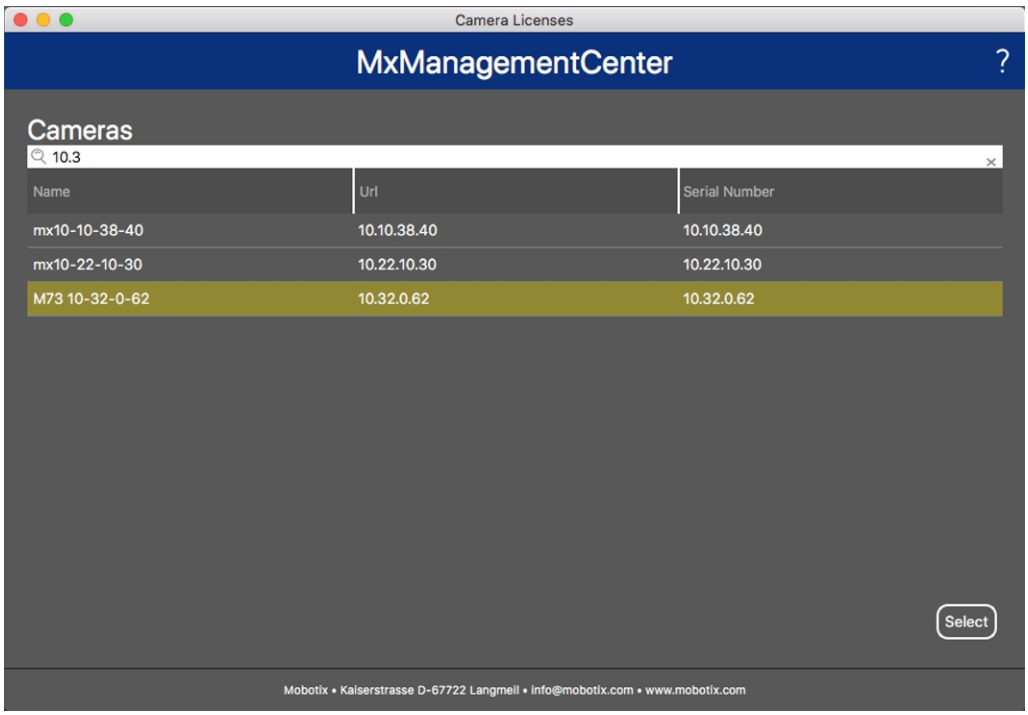


Fig. 2: Vista general de las licencias de aplicaciones de cámara en MxManagementCenter

AVISO! Si es necesario, corrija el tiempo establecido en la cámara.

1. Es posible que se muestre una vista general de las licencias instaladas en la cámara. Haga clic en **Activate License** (Activar licencia).

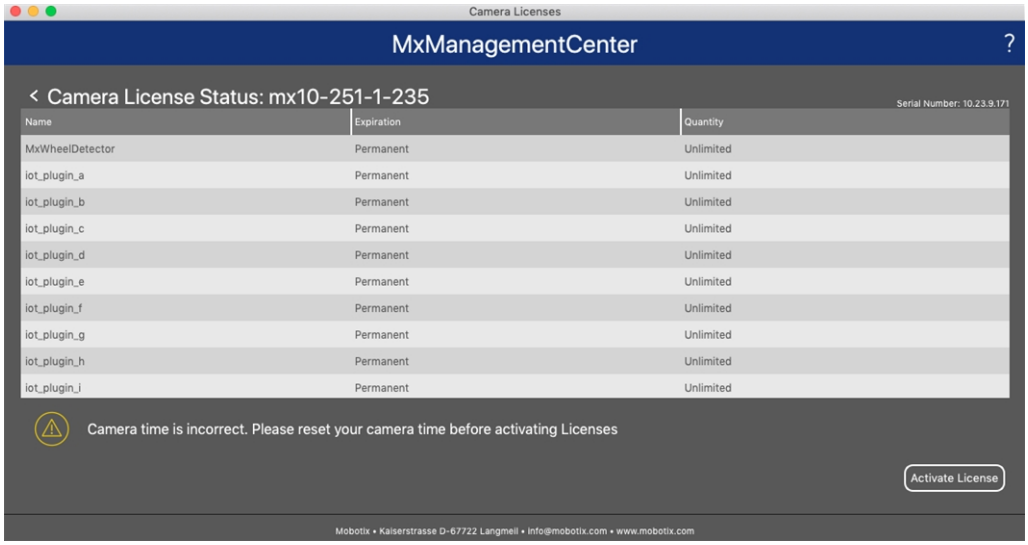


Fig. 3: Vista general de las licencias instaladas en la cámara

AVISO! Si es necesario, corrija el tiempo establecido en la cámara.

2. Introduzca un ID de activación válido y especifique el número de licencias que se instalarán en el equipo.
3. Si desea obtener una licencia para otro producto, haga clic en . En la nueva fila, introduzca el ID de activación correspondiente y el número de licencias que desee.

4. Para eliminar una línea, haga clic en .
5. Una vez introducidos todos los ID de activación, haga clic en **Activate License Online** (Activar licencia online). Durante la activación, **MxMC** se conecta al servidor de licencias. Para ello, se requiere una conexión a Internet.

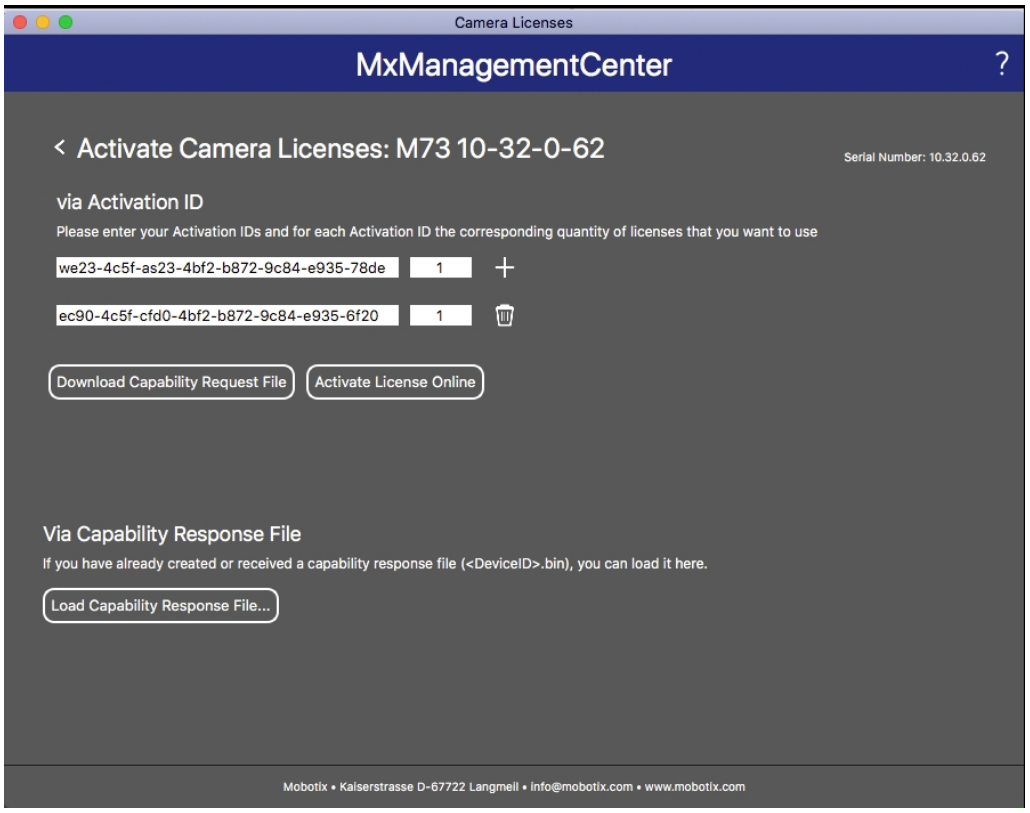


Fig. 4: Cómo añadir licencias

Activación correcta

Tras la activación, es necesario volver a iniciar sesión para que se apliquen los cambios. También puede volver al área de gestión de licencias.

Error de activación (sin conexión a Internet)

Si no se puede acceder al servidor de licencias, por ejemplo, porque no hay conexión a Internet, también es posible activar las aplicaciones sin conexión (consulte Activación sin conexión, p. 12).

Activación sin conexión

Para la activación sin conexión, el socio o instalador del que adquirió las licencias puede generar un archivo de respuesta de capacidad (.bin) en el servidor de licencias para activarlas.

1. Seleccione en el menú **Window > Camera App Licenses** (Ventana > Licencias de aplicaciones de cámara).
2. Seleccione la cámara para la que desea utilizar la licencia y haga clic en **Select** (Seleccionar).

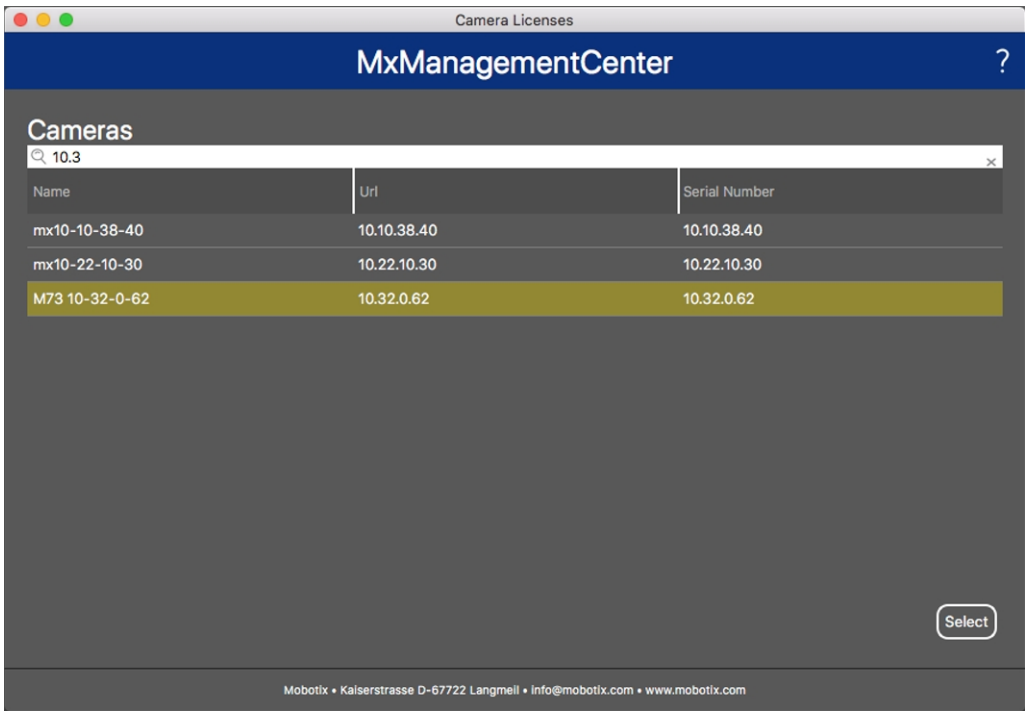


Fig. 5: Vista general de las licencias de aplicaciones de cámara en MxManagementCenter

AVISO! Si es necesario, corrija el tiempo establecido en la cámara.

3. Es posible que se muestre una vista general de las licencias instaladas en la cámara. Haga clic en **Activate License** (Activar licencia).

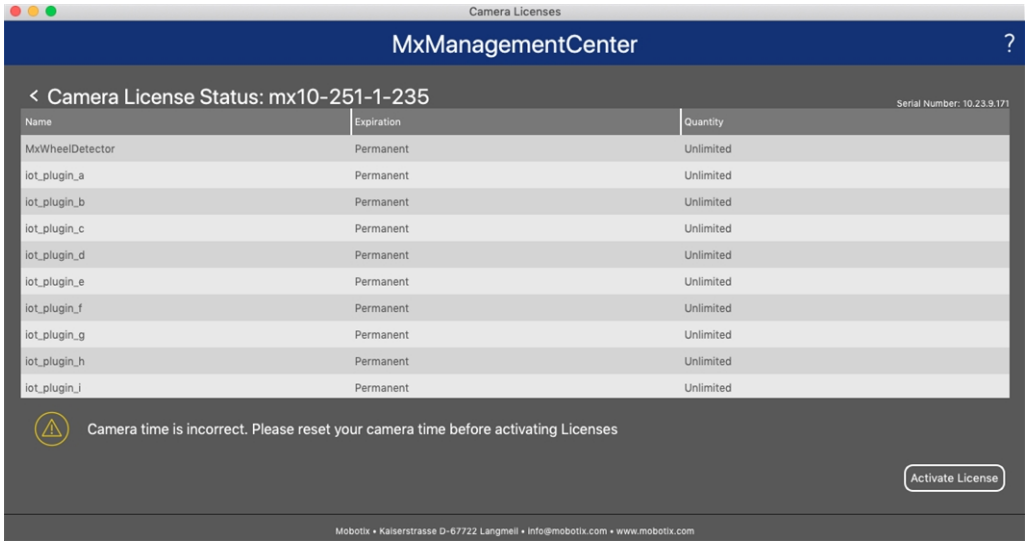


Fig. 6: Vista general de las licencias instaladas en la cámara

AVISO! Si es necesario, corrija el tiempo establecido en la cámara.

4. Introduzca un ID de activación válido y especifique el número de licencias que se instalarán en el equipo.
5. Si desea obtener una licencia para otro producto, haga clic en . En la nueva fila, introduzca el **ID de activación** correspondiente y el número de licencias que desee.
6. Si es necesario, haga clic en para eliminar una línea.
7. Una vez introducidos todos los ID de activación, haga clic en **Download Capability Request File (.lic)** (Descargar archivo de solicitud de capacidad [.lic]) y envíeselo a su socio o instalador.

AVISO! Este archivo permite al socio o instalador del que adquirió las licencias generar un archivo de respuesta de capacidad (.bin) en el servidor de licencias.

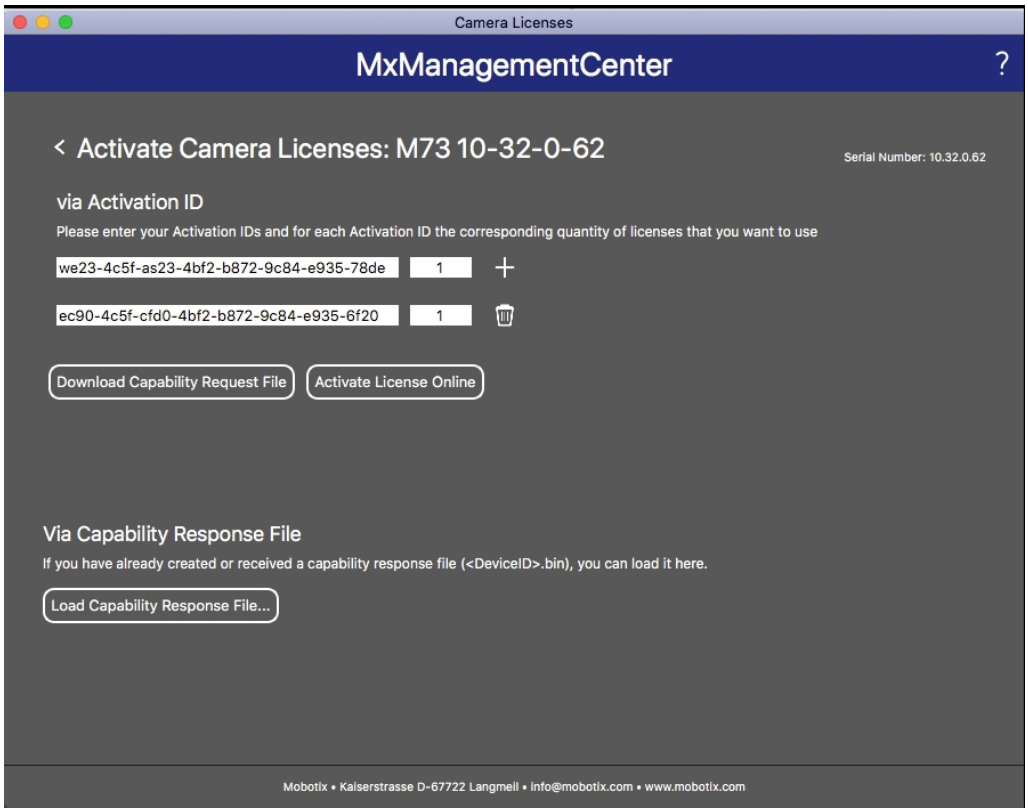


Fig. 7: Cómo añadir licencias

8. Haga clic en Load Capability Response File (Cargar archivo de respuesta de capacidad) y siga las instrucciones.

Activación correcta

Tras la activación, es necesario volver a iniciar sesión para que se apliquen los cambios. También puede volver al área de gestión de licencias.

Gestión de licencias en MxManagementCenter

En MxManagementCenter puede administrar cómodamente todas las licencias que se han activado para una cámara.

1. Seleccione en el menú **Window > Camera App Licenses** (Ventana > Licencias de aplicaciones de cámara).
2. Seleccione la cámara para la que desea utilizar la licencia y haga clic en **Select** (Seleccionar).

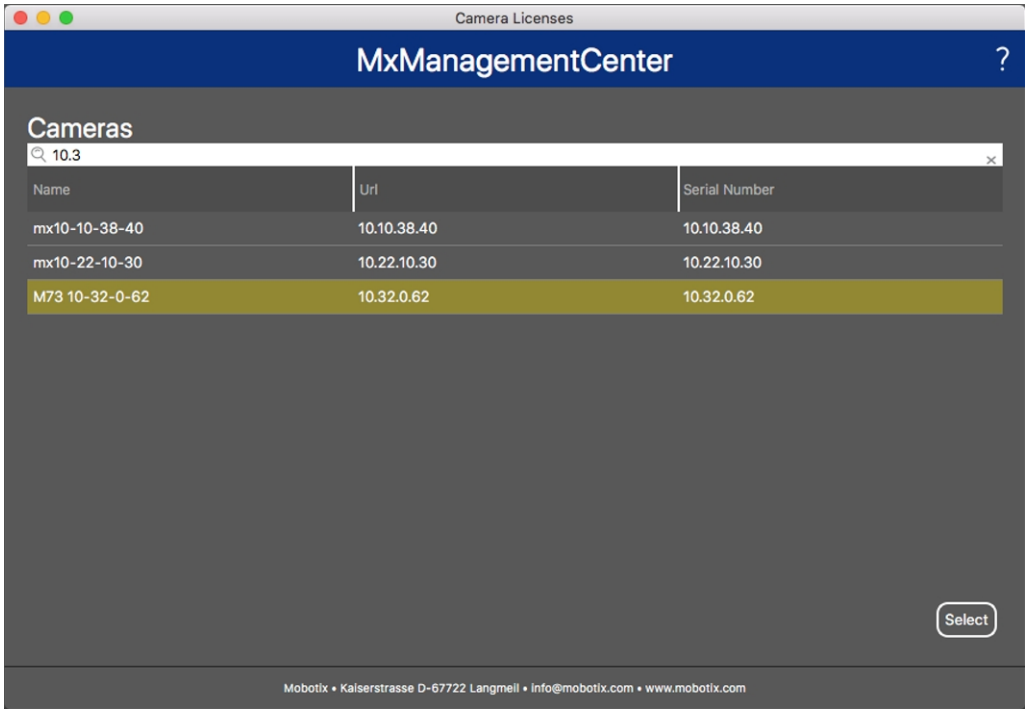


Fig. 8: Vista general de las licencias de aplicaciones de cámara en MxManagementCenter

Es posible que se muestre una vista general de las licencias instaladas en la cámara.

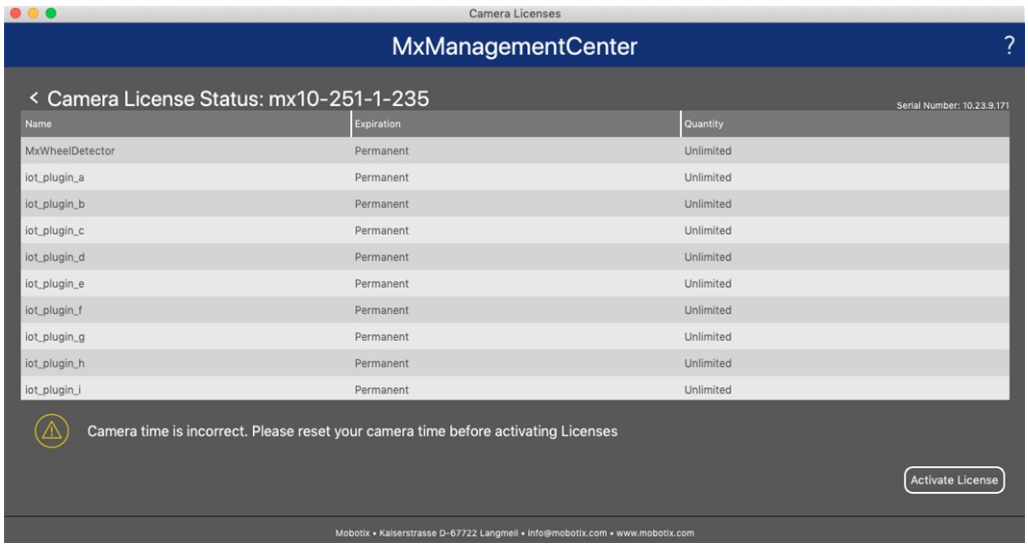


Fig. 9: Vista general de las licencias instaladas en la cámara

AVISO! Si es necesario, corrija el tiempo establecido en la cámara.

Columna	Explicación
Nombre	Nombre de la aplicación con licencia.
Caducidad	Periodo de validez de la licencia.
Cantidad	Número de licencias adquiridas para un producto.
Número de serie	Identificador único asignado por MxMC al dispositivo utilizado. Es importante tener a mano el ID del dispositivo por si surge algún problema durante el periodo de licencia.

Sincronización de licencias con el servidor

Cuando se inicia el programa, no se produce una sincronización automática de las licencias entre el equipo y el servidor de licencias. Por lo tanto, debe hacer clic en **Update** (Actualizar) para volver a cargar las licencias desde el servidor.

Actualización de licencias

Para actualizar licencias temporales, haga clic en **Activate Licenses** (Activar licencias). Se abre el cuadro de diálogo para actualizar o activar licencias.

AVISO! Se necesitan derechos de administrador para sincronizar y actualizar las licencias.

Requisitos de cámara, imagen y escena

La cámara debe configurarse de modo que la combinación de la distancia, la distancia focal del objetivo y la resolución de la cámara proporcionen una imagen que pueda ser analizada con precisión. Por lo tanto, se deben cumplir los siguientes requisitos previos para la escena:

Las posiciones de montaje más altas posibles para obtener los mejores resultados

Cuando planifique su sistema de videovigilancia, opte por las posiciones de cámara más altas posibles para cubrir la mayor área posible con cada cámara. Considere una altura de instalación de al menos 5 metros. Una altura de instalación de 10-25 metros suele ofrecer resultados significativamente mejores.

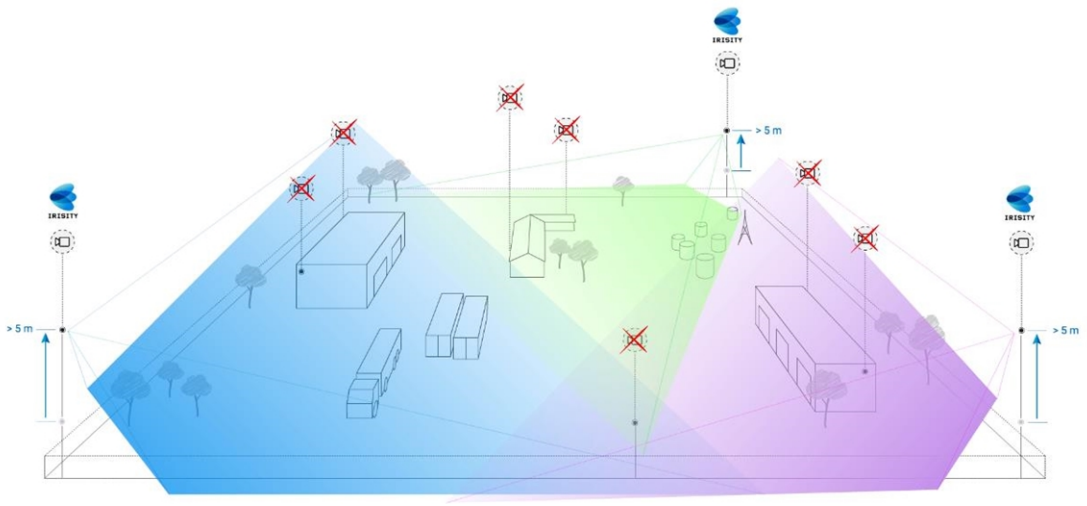


Fig. 10: Al usar posiciones de montaje altas se puede reducir el número de cámaras en una instalación CCTV clásica.

Iluminación de la escena

Con fuentes de luz óptimas (recomendamos al menos dos fuentes de luz) puede mejorar significativamente la calidad del análisis de vídeo y, por tanto, la seguridad de su sitio.

- Ilumine suficientemente el área supervisada.
- Asegure un buen contraste en el área de vigilancia.
- No sobreilumine objetos cerca de las cámaras para evitar el mezclado y el ruido.

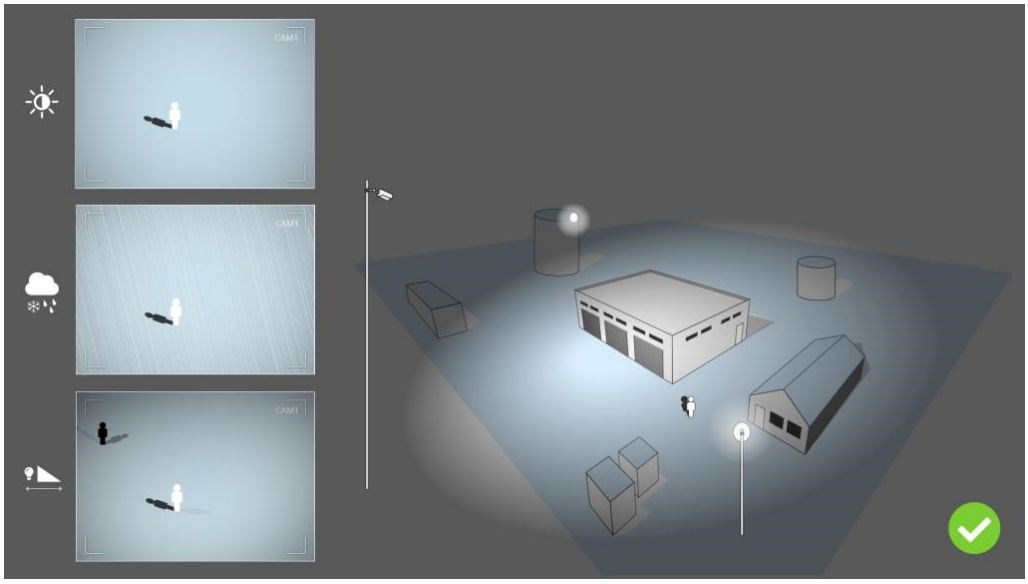


Fig. 11: La iluminación fuera del eje mejora significativamente la visibilidad, el contraste y la detección de objetos. Permite realizar detecciones precisas incluso en las condiciones meteorológicas más difíciles.

Solución de problemas

Problemas de diseño de luces

Al colocar la fuente de luz cerca de la cámara y demasiado lejos del objeto protegido, la luz emitida puede comprometer la vigilancia al crear problemas de vídeo. Los posibles problemas son:

- El contraste de la imagen de vídeo puede ser demasiado bajo (sin sombras)
- La fuente de luz puede crear ruido en la imagen acentuando las gotas de lluvia y copos de nieve
- Es posible que la intensidad de la luz no sea suficiente para iluminar el objeto protegido

Aunque la iluminación incorporada de la cámara u otra iluminación sobre eje suele resultar práctica, a menudo reduce la eficacia del sistema de vigilancia. En condiciones meteorológicas adversas, los intrusos pueden volverse casi invisibles, al quedar ocultos tras la lluvia, la nieve o la niebla

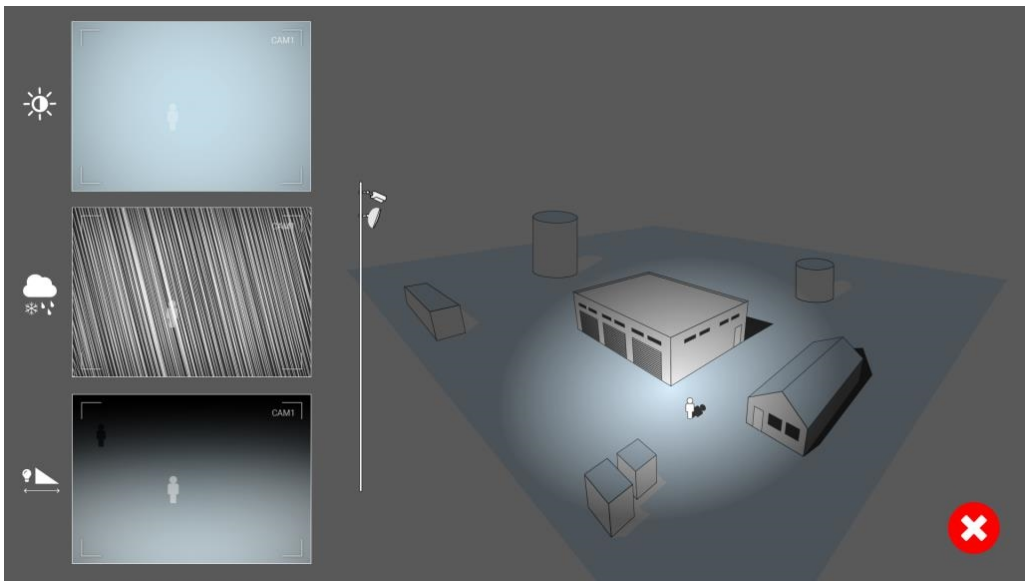


Fig. 12: En condiciones meteorológicas adversas, los intrusos pueden volverse casi invisibles, al quedar ocultos tras la lluvia, la nieve o la niebla

Activación de la interfaz de la aplicación certificada

ATENCIÓN! La Irisity IRIS AI Analytics - Intrusion Detection no tiene en cuenta las áreas oscuras definidas para la imagen en directo. Por lo tanto, no hay pixelado en áreas oscuras mientras se configura la aplicación y durante el análisis de la imagen por parte de la aplicación.

AVISO! El usuario debe tener acceso al menú de configuración (http(s)://<Dirección IP de la cámara>/control). Verifique los derechos de usuario de la cámara.

1. En la interfaz web de la cámara, abra: **Setup Menu > Certified App Settings** (Menú de configuración > Ajustes de la aplicación certificada) (http(s)://<Dirección IP de la cámara>/control/app_config).

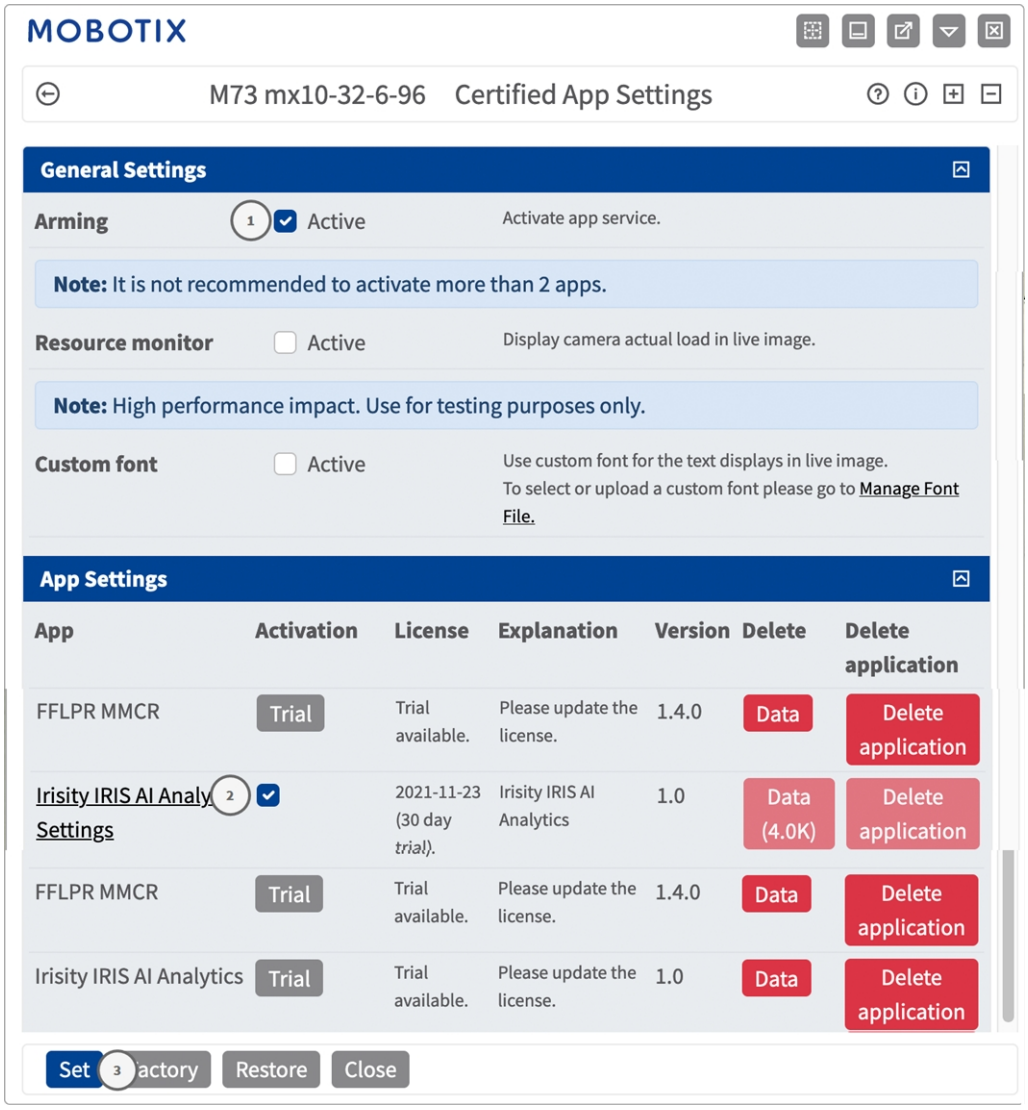


Fig. 13: Aplicación certificada: Configuración de

2. En **Ajustes generales**, active la opción **Armado** del servicio de la aplicación MOBOTIX ① .
3. Haga clic en Establecer ③ . Aparece una lista de aplicaciones instaladas.
4. En **App Settings** (Configuración de la aplicación), marque la opción **Active** (Activa) de la aplicación correspondiente.
5. Haga clic en el nombre de la aplicación ② que desee configurar para abrir su interfaz de usuario.
6. Para obtener información sobre la configuración de la aplicación, consulte Configuración de la Irisity IRIS AI Analytics - Intrusion Detection, p. 22

Configuración de la Irisity IRIS AI Analytics - Intrusion Detection

ATENCIÓN! El usuario debe tener acceso al menú de configuración (http(s)://<Dirección IP de la cámara>/control). Verifique los derechos de usuario de la cámara.

1. En la interfaz web de la cámara, abra: **Setup Menu > Certified App Settings** (Menú de configuración > Ajustes de la aplicación certificada) (http(s)://<Dirección IP de la cámara>/control/app_config).
2. Haga clic en el nombre de la **Irisity IRIS AI Analytics - Intrusion Detection**.

La ventana de configuración de la aplicación aparece con las siguientes opciones:

Detección de intrusiones IRIS

Se deben tener en cuenta las siguientes configuraciones:

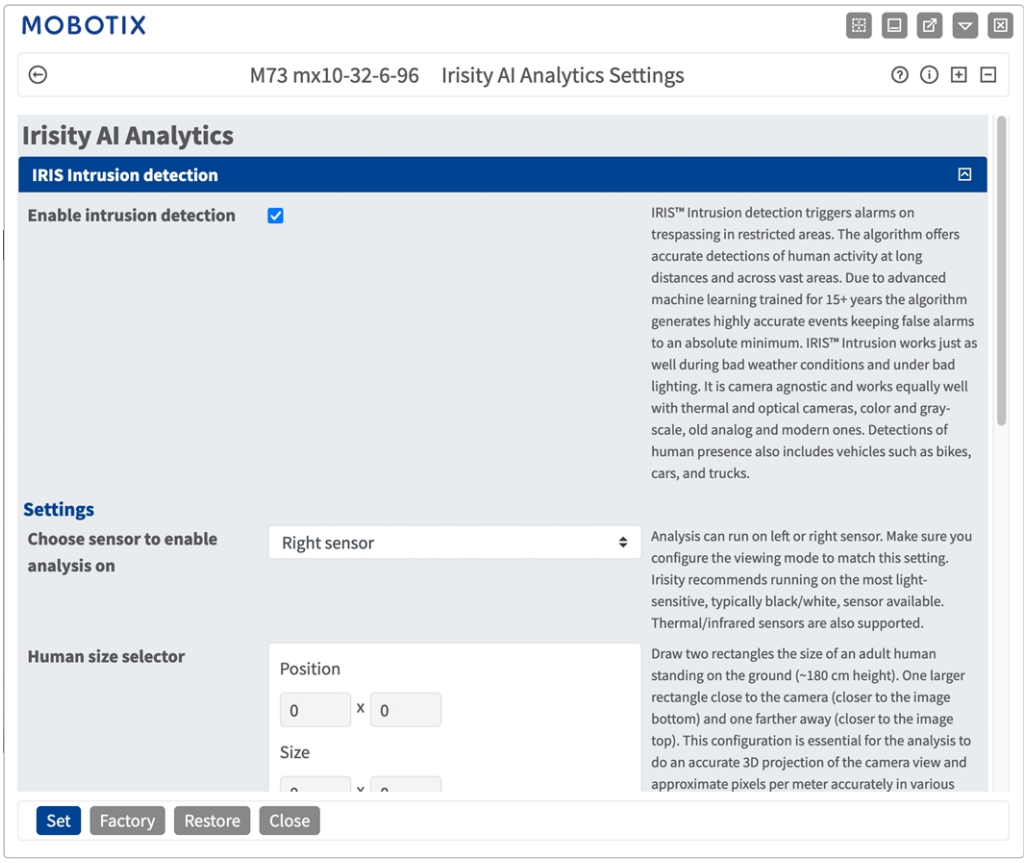


Fig. 14: Modo de funcionamiento predeterminado: Detección de intrusiones IRIS

Enable intrusion detection (Habilitar detección de intrusos): Marcar opción para activar el algoritmo

Configuración de

- **Choose sensor to enable analysis on (Elegir el sensor en el que desea habilitar el análisis):** Seleccione el sensor que se va a utilizar para el análisis de imagen.
- **Selector de talla humana:** Esta configuración es esencial para que el análisis realice una proyección en 3D exacta de la vista de la cámara y unos píxeles por metro con precisión en varias partes de la imagen (consulte Detección de manipulación IRIS, p. 23).
- **Alarm zones (Zonas de alarma):** Es necesario definir al menos una zona de alarma (área de detección) en la imagen en tiempo real (consulte Zonas de alarma, p. 24).
- **Detectar tipo de objeto:** Seleccione un filtro para activación únicamente con personas o vehículos. Entre las detecciones predeterminadas se encuentran todos los movimientos provocados humanos, como peatones, bicicletas, turismos y camiones.

Advanced Settings (Ajustes avanzados)

- **Enfriamiento de zona de alarma:** Número de segundos que se desactivará una zona de alarma después de que se active una alarma.
- **Enfriamiento de evento:** Número de segundos que una alarma desactivará las detecciones posteriores del mismo objeto de alarma, incluidos los objetos cercanos.
- **Sensibilidad:** Nivel de sensibilidad para los objetos a clasificar como actividad humana. Se recomienda la opción intermedia para la mayoría de los casos.

Detección de manipulación IRIS

Aquí puede configurar las funciones de detección de manipulación.

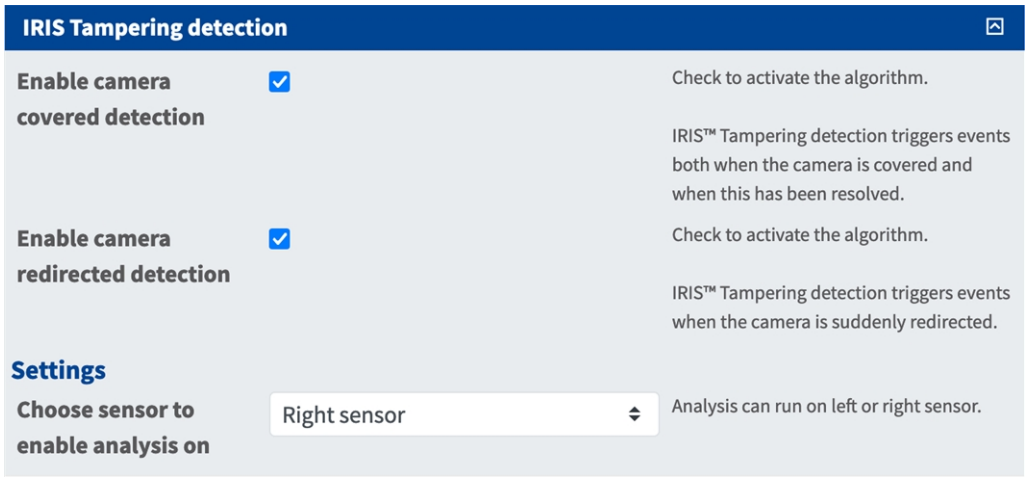


Fig. 15: Detección de manipulación IRIS

Activar la detección cubierta por cámara: Active esta opción para activar el algoritmo.

AVISO! La detección de manipulación IRIS™ activa eventos tanto cuando la cámara está cubierta como cuando se ha resuelto.

Activar la detección redirigida por cámara: Active la detección redirigida de la cámara.

AVISO! La detección de manipulación de IRIS™ activa eventos cuando la cámara se redirige repentinamente.

Choose sensor to enable analysis on (Elegir el sensor en el que desea habilitar el análisis): Seleccione el sensor en el que se debe ejecutar el análisis.

Dibujo de un selector de talla humana

1. En la vista en directo, simplemente haga clic y arrastre un área de reconocimiento rectangular.
2. Arrastre los puntos de las esquinas para ajustar el área de reconocimiento.
3. En la esquina superior derecha de la vista activa, haga clic en **Enviar** para adoptar las coordenadas del rectángulo.

Zonas de alarma

Opcionalmente, puede establecer una o más Zonas de alarma (áreas de detección). Si se deja en blanco, se utilizará toda la imagen para las detecciones.

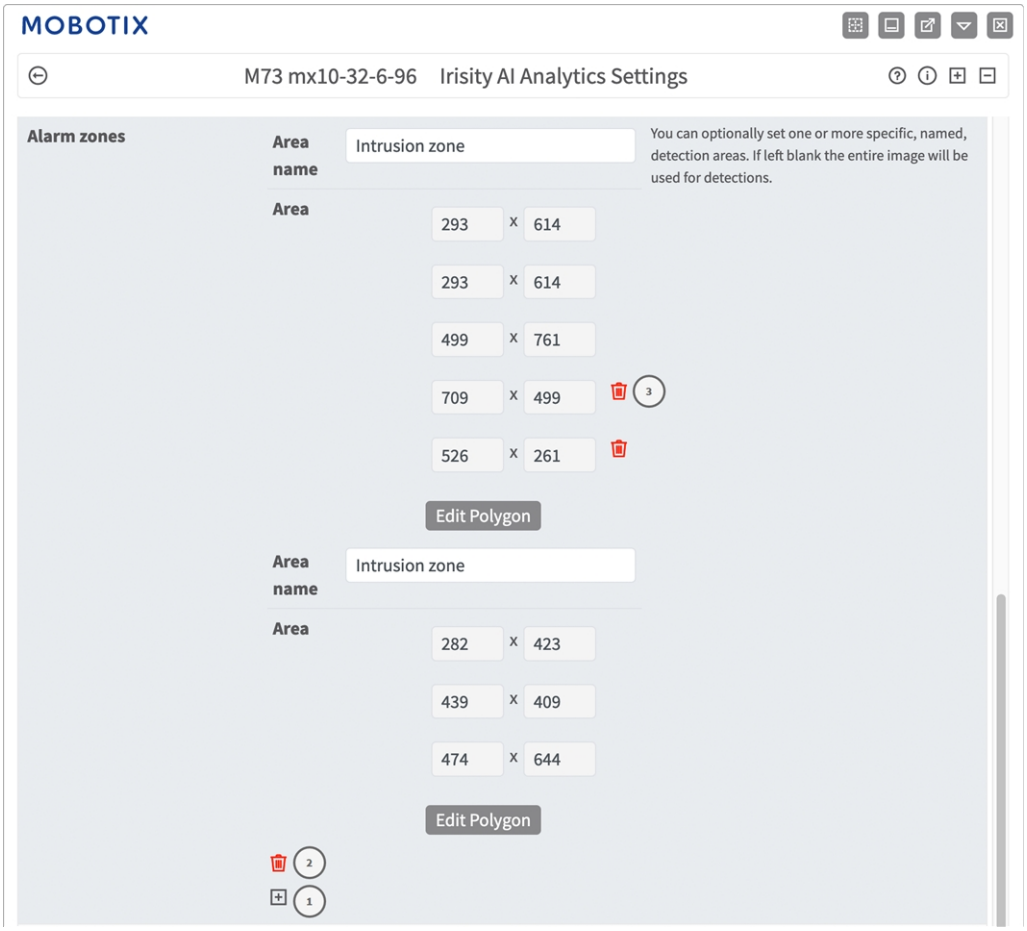


Fig. 16: Zonas de alarma

Nombre de área: introduzca un nombre único para identificar la zona de alarma

Área: Los puntos de las esquinas definidas de la zona de alarma. Haga clic en **Editar polígono** ① para dibujar el área de detección en la vista en tiempo real (consulte Dibujar un área de polígono en la vista en tiempo real, p. 26

Agregar una zona de alarma: Haga clic en el icono **más** ② para definir una nueva Zona de alarma.

Eliminar un área: Haga clic en el icono de **papelera** ② para eliminar el área de reconocimiento.

Superposiciones visuales

Aquí puede seleccionar objetos y datos de la detección de intrusiones IRIS para que se muestren en la imagen en tiempo real.

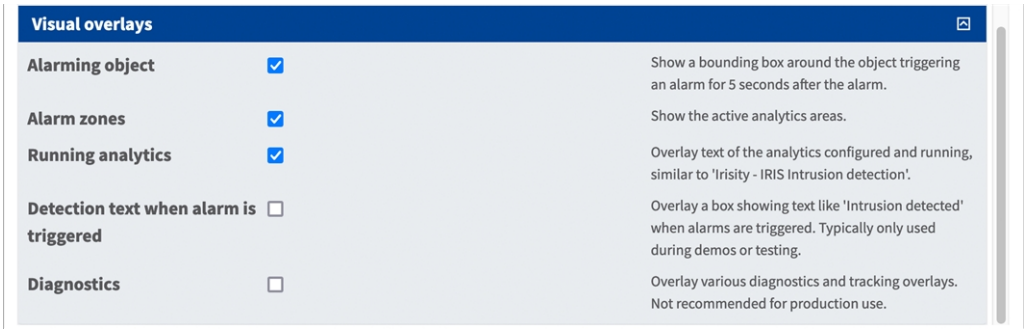


Fig. 17: Superposiciones visuales

Alarming object (Objeto de alarma): Active esta casilla para mostrar un cuadro delimitador alrededor del objeto que activa una alarma durante 5 segundos después de la alarma.

Alarm zones (Zonas de alarma): Active esta casilla para mostrar las áreas de análisis activas.

Running analytics (Análisis en ejecución): Marque para superponer texto de los análisis configurados y en ejecución, p. ej. "Irisity - Detección de intrusiones IRIS".

Detection text when alarm is triggered (Texto de detección cuando se activa la alarma): Superponer un cuadro que muestre texto como "Intrusión detectada" cuando se activen las alarmas.

Diagnostics (Diagnóstico): Marque para superponer varias superposiciones de diagnóstico y seguimiento, p. ej., para la depuración.

Dibujar un área de polígono en la vista en tiempo real

En la vista en tiempo real, puede dibujar áreas basadas en polígonos en función de la aplicación correspondiente. Estas áreas son, por ejemplo, áreas de detección, áreas excluidas, áreas de referencia, etc.

1. En la vista en tiempo real, simplemente haga clic en un área rectangular y arrástrela.
2. Arrastre los puntos de esquina a la posición deseada.
3. Para agregar otro punto de esquina, arrastre un punto más pequeño entre dos puntos de esquina en el contorno del área.
4. En la esquina superior derecha de la vista activa, haga clic en **Enviar** para adoptar las coordenadas del polígono.
5. De manera opcional, haga clic en el icono de **papelera** para eliminar el área de reconocimiento.

Superposiciones visuales

Aquí puede seleccionar objetos y datos de la detección de intrusiones IRIS para que se muestren en la imagen en tiempo real.

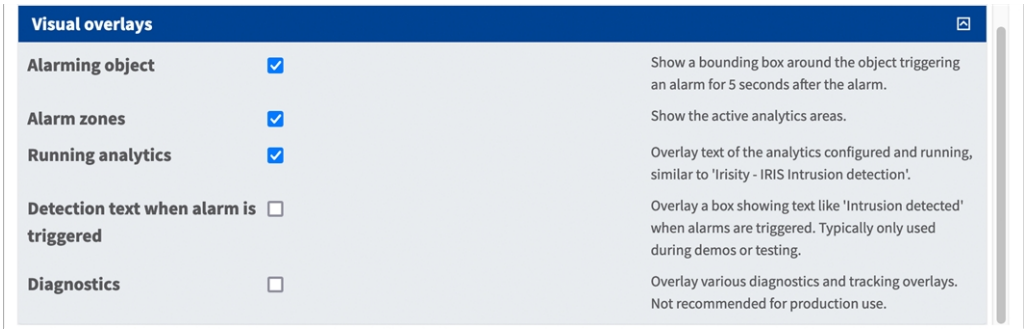


Fig. 18: Superposiciones visuales

Alarming object (Objeto de alarma): Active esta casilla para mostrar un cuadro delimitador alrededor del objeto que activa una alarma durante 5 segundos después de la alarma.

Alarm zones (Zonas de alarma): Active esta casilla para mostrar las áreas de análisis activas.

Running analytics (Análisis en ejecución): Marque para superponer texto de los análisis configurados y en ejecución, p. ej. "Irisity - Detección de intrusiones IRIS".

Texto de detección: Superponer un cuadro que muestre texto como "Intrusión detectada" cuando se activen las alarmas.

Diagnostics (Diagnóstico): Marque para superponer varias superposiciones de diagnóstico y seguimiento, p. ej., para la depuración.

Almacenamiento de la configuración

Para almacenar la configuración, tiene las siguientes opciones:

Fig. 19: Almacenamiento de la configuración

- Haga clic en el botón **Set** (Establecer) para activar sus ajustes y guardarlos hasta el próximo reinicio de la cámara.
- Haga clic en el botón **Factory** (Fábrica) para cargar los valores predeterminados de fábrica para este cuadro de diálogo (es posible que este botón no esté presente en todos los cuadros de diálogo).
- Haga clic en el botón **Restore** (Restaurar) para deshacer los cambios más recientes que no se han almacenado permanentemente en la cámara.
- Haga clic en el botón **Close** (Cerrar) para cerrar el cuadro de diálogo. Durante el cierre del cuadro de diálogo, el sistema verifica toda la configuración para ver si hay cambios. Si se detectan cambios, se le preguntará si desea almacenar la configuración completa de manera permanente.

Después de guardar correctamente la configuración, el evento y los metadatos se envían automáticamente a la cámara en caso de un evento.

MxMessageSystem

Qué es MxMessageSystem

MxMessageSystem es un sistema de comunicación basado en mensajes orientados al nombre. Esto significa que un mensaje debe tener un nombre único con una longitud máxima de 32 bytes.

Cada participante puede enviar y recibir mensajes. Las cámaras MOBOTIX también pueden reenviar mensajes dentro de la red local. De esta manera, los mensajes MxMessages se pueden distribuir a través de toda la red local (consulte Message Area: Global [Área de mensaje: global]).

Por ejemplo, una cámara MOBOTIX de la serie 7 puede intercambiar un mensaje MxMessage generado por una aplicación de cámara con una cámara MX6 no compatible con aplicaciones de MOBOTIX certificadas.

Hechos acerca de los mensajes MxMessage

- El cifrado de 128 bits garantiza la privacidad y la seguridad del contenido del mensaje.
- Los mensajes MxMessage se pueden distribuir desde cualquier cámara de las series MX6 y 7.
- El rango del mensaje se puede definir individualmente para cada MxMessage.
  - **Local:** la cámara espera un MxMessage dentro de su propio sistema (por ejemplo, a través de una aplicación certificada).
  - **Global:** la cámara espera un MxMessage que otro dispositivo MxMessage distribuye en la red local (por ejemplo, otra cámara de la serie 7 equipada con una aplicación MOBOTIX certificada).
- Las acciones que los destinatarios deben realizar se configuran individualmente para cada participante de MxMessageSystem.

MxMessageSystem: procesamiento de los eventos de aplicaciones generados automáticamente

Consulta de eventos de aplicaciones generados automáticamente

AVISO! Después de activar correctamente la aplicación (consulte Activación de la interfaz de la aplicación certificada, p. 20), se generará automáticamente un evento de mensaje genérico para esa aplicación específica en la cámara.

1. Vaya a **Setup Menu > Event Control > Event Overview** (Menú de configuración > Control de eventos > Descripción general del evento). En la sección **Message Events** (Eventos de mensaje), al evento de mensaje generado automáticamente se le asigna un nombre en función de la aplicación (por ejemplo, IRIS).

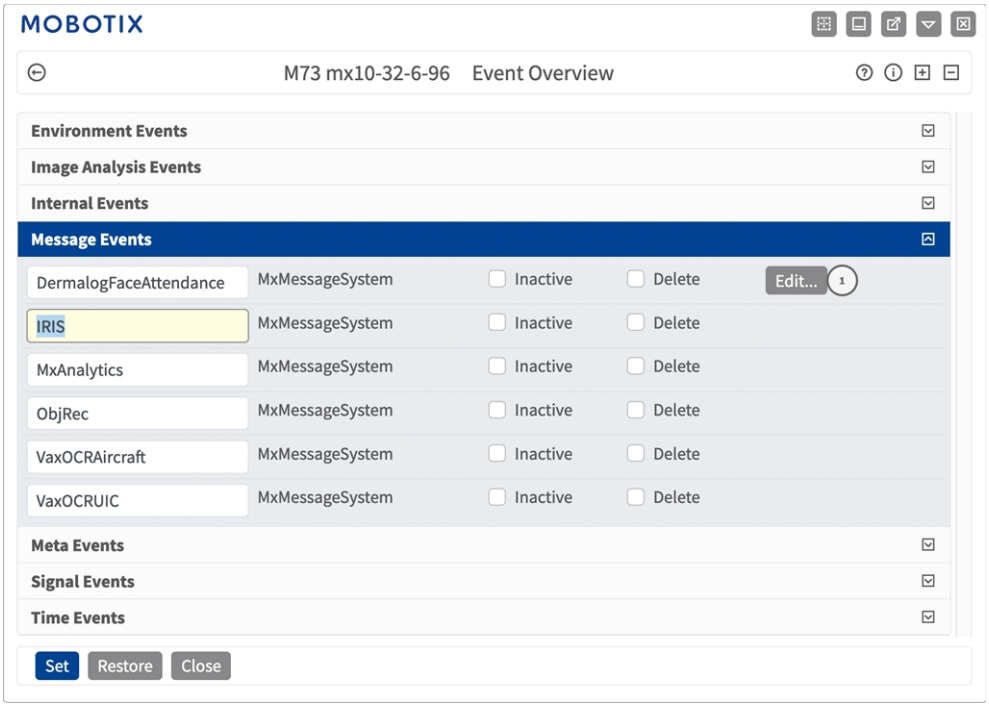


Fig. 20: Ejemplo: evento de mensaje genérico de la Irisity IRIS AI Analytics - Intrusion Detection

2. Haga clic en **Edit** (Editar)① para visualizar una selección de todos los eventos de mensajes configurados.

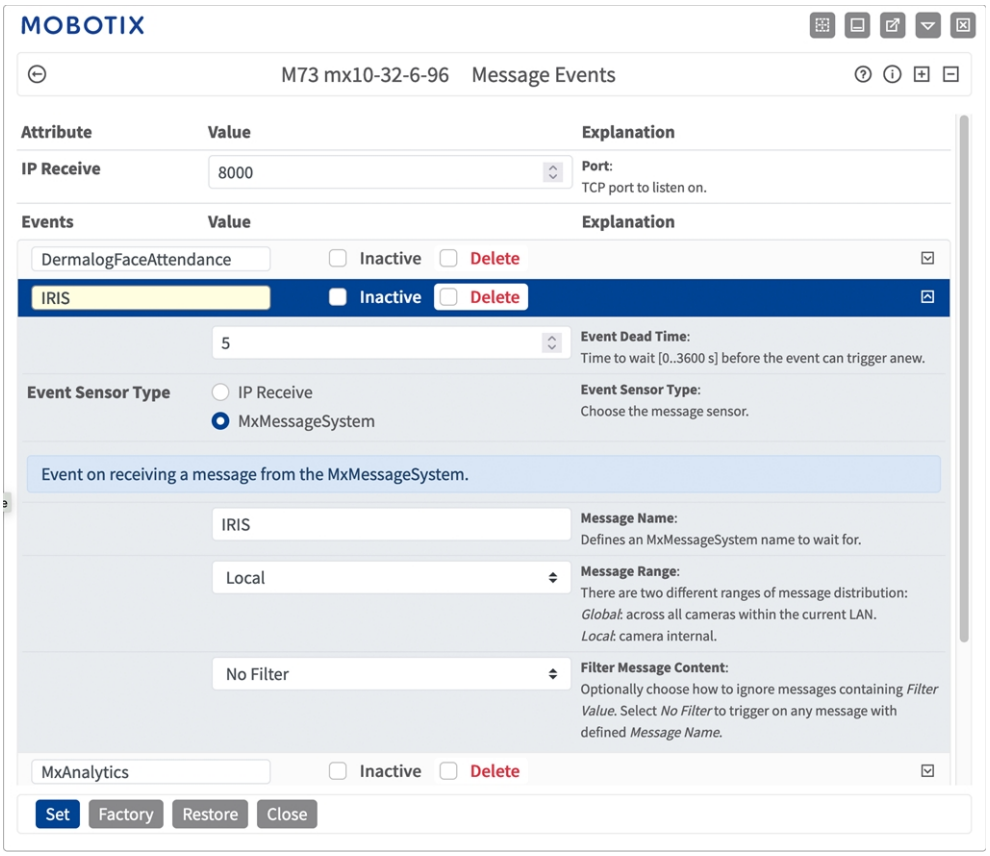


Fig. 21: Ejemplo: Detalles de evento de mensaje genérico: sin filtro

Gestión de acciones: configuración de un grupo de acciones

ATENCIÓN! Para utilizar eventos, activar grupos de acciones o grabar imágenes, es necesario activar la opción de armado de los ajustes generales de la cámara (http(s)/<Dirección IP de la cámara>/control/settings)

Un grupo de acciones define las acciones que activa el evento de la Irisity IRIS AI Analytics - Intrusion Detection.

1. En la interfaz web de la cámara, abra: **Setup Menu > Action Group Overview** (Menú de configuración > Vista general de grupo de acciones) (http(s)://<Dirección IP de la cámara>/control/actions).

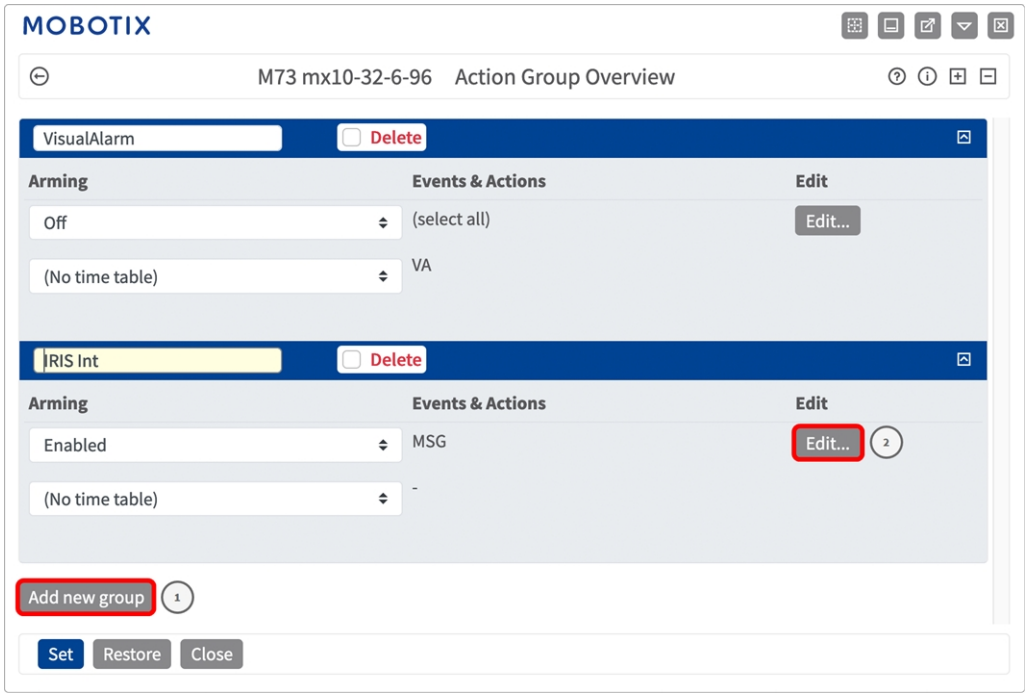


Fig. 22: Definición de grupos de acciones

2. Haga clic en **Add new group** (Agregar nuevo grupo)① y asigne un nombre significativo.
3. Haga clic en **Edit** (Editar)② para configurar el grupo.

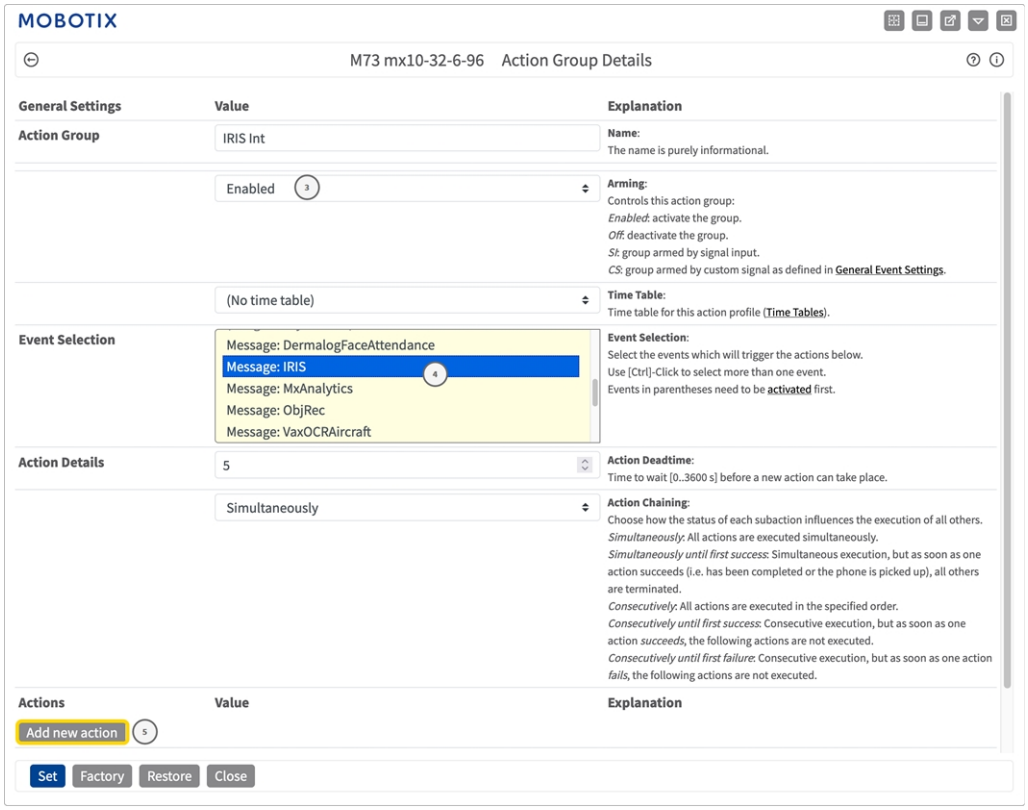


Fig. 23: Configuración de un grupo de acciones

4. Active **Arming** (Armado)③ en el grupo de acciones.
5. Seleccione su evento de mensaje en la lista **Event selection** (Selección de eventos) ④ . Para seleccionar varios eventos, mantenga pulsada la tecla Mayús.
6. Haga clic en **Add new Action** (Agregar nueva acción)⑤ .
7. Seleccione una acción apropiada en la lista **Action Type and Profile** (Tipo de acción y perfil)⑥ .

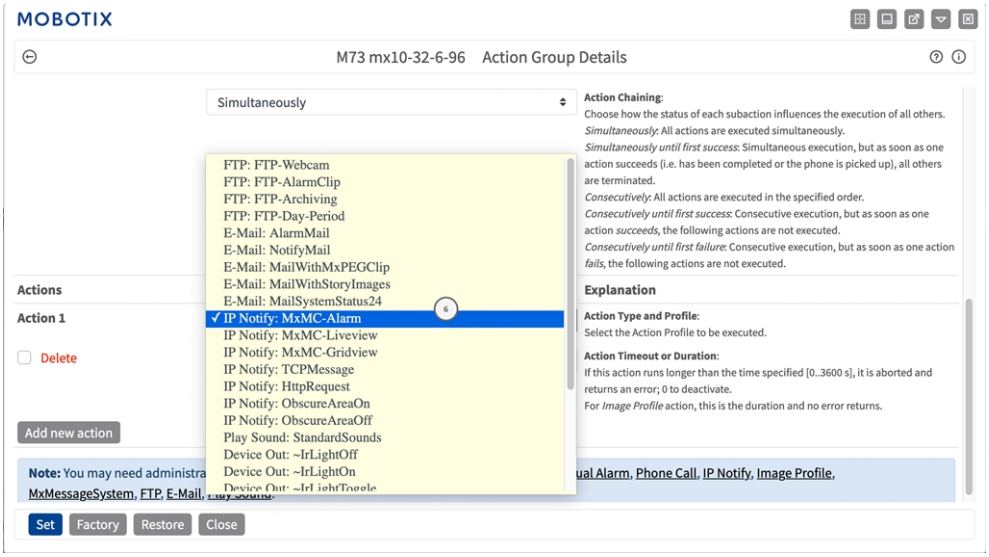


Fig. 24: Selección de tipo de acción y perfil

AVISO! Si el perfil de acción necesario aún no está disponible, puede crear un nuevo perfil en las secciones del menú de administración "MxMessageSystem", "Transfer Profiles" (Perfiles de transferencia) y "Audio and VoIP Telephony" (Audio y telefonía VoIP).

Si es necesario, puede agregar más acciones haciendo clic en el botón de nuevo. En ese caso, asegúrese de que la "cadena de acciones" esté configurada correctamente (es decir, al mismo tiempo).

8. Haga clic en el botón **Set** (Establecer) al final del cuadro de diálogo para confirmar la configuración.

Ajustes de acciones: configuración de las grabaciones de la cámara

1. En la interfaz web de la cámara, abra: **Setup Menu > Event Control > Recording** (Menú de configuración > Control de eventos > Grabación) (http(s)/<Dirección IP de la cámara>/control/recording).

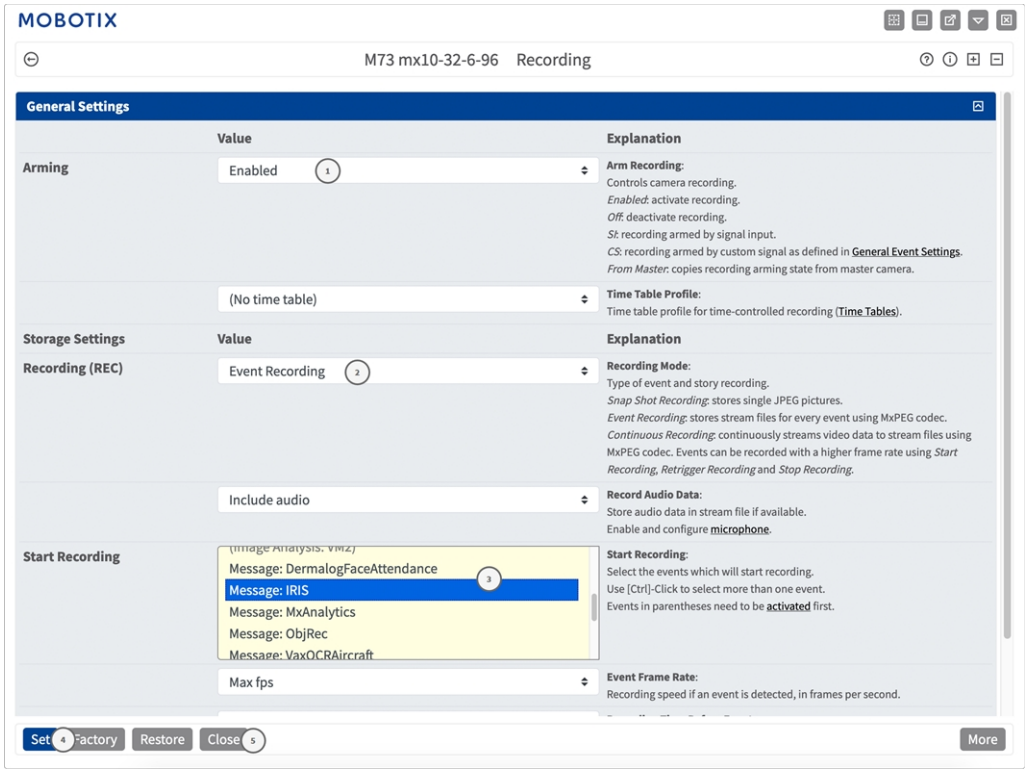


Fig. 25: Configuración de los ajustes de grabación de la cámara

2. Active **Arm Recording** (Armar grabación) ① .
3. En **Storage Settings**/**Recording (REC)** (Ajustes de almacenamiento/Grabación [REC]), seleccione un **Recording mode** (Modo de grabación)② . Están disponibles los siguientes modos:
   - Grabación de instantánea
   - Grabación de eventos
   - Grabación continua
4. En la lista **Start recording** (Iniciar grabación) ③ , seleccione el evento de mensaje que acaba de crear.
5. Haga clic en el botón **Set** (Establecer) ④ al final del cuadro de diálogo para confirmar los ajustes.
6. Haga clic en **Close** (Cerrar) ⑤ para guardar los ajustes de manera permanente.

AVISO! Como alternativa, puede guardar la configuración en el menú Admin en Configuración / Guardar configuración actual en la memoria permanente.

MxMessageSystem: procesamiento de los metadatos transmitidos por las aplicaciones

Metadatos transferidos dentro de MxMessageSystem

Para cada evento, la aplicación también transfiere metadatos a la cámara. Estos datos se envían en forma de un esquema JSON en un MxMessage.

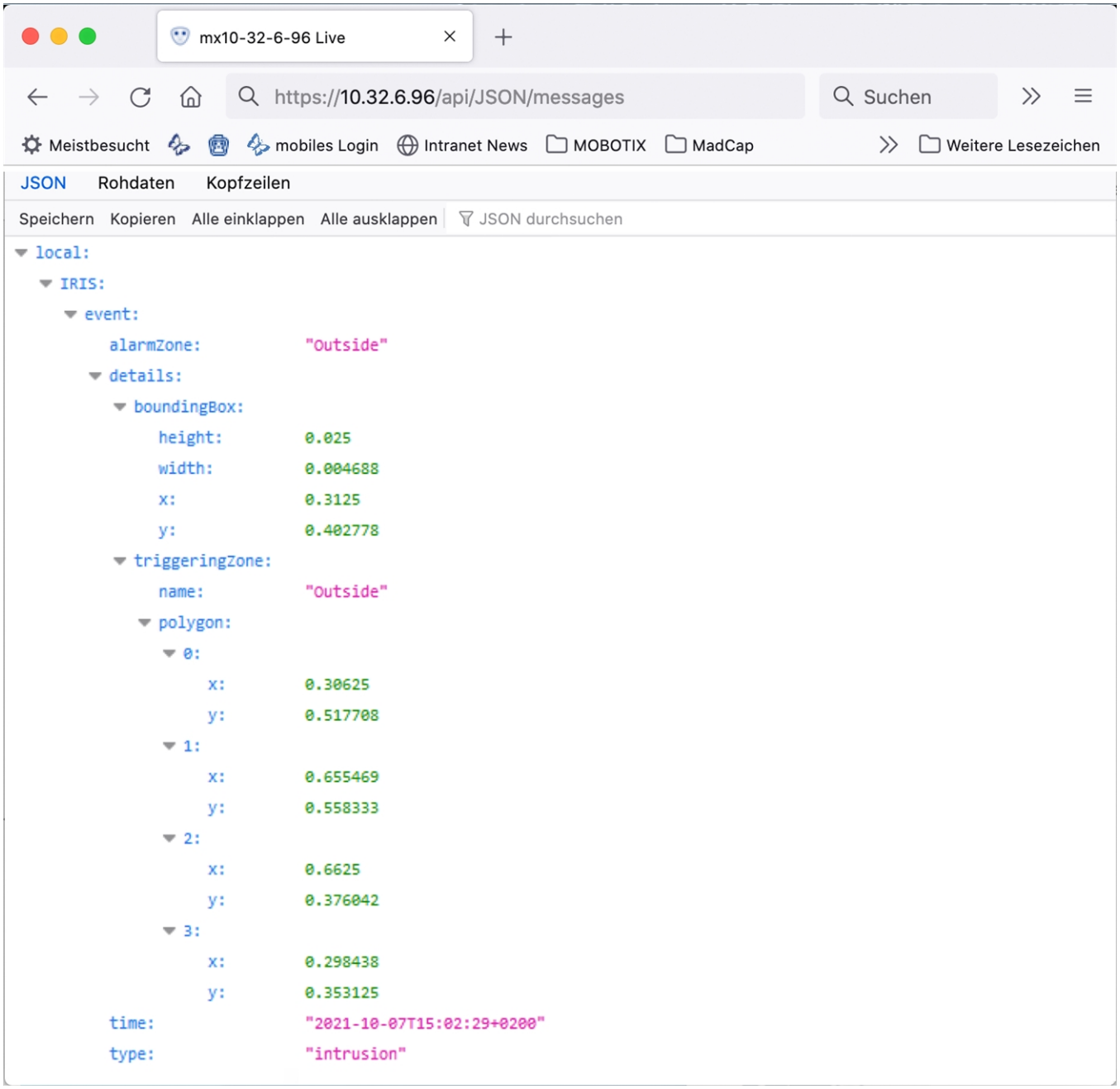


Fig. 26: Ejemplo: Metadatos transmitidos dentro de un MxMessage de Irisity IRIS AI Analytics - Intrusion Detection

AVISO! Para ver la estructura de metadatos del último evento de la aplicación, introduzca la siguiente URL en la barra de direcciones del navegador: http(s)/direcciónIPdelacámara/api/json/messages

Creación de un evento de mensaje personalizado

1. Vaya a **Setup Menu > Event Control > Event Overview** (Menú de configuración > Control de eventos > Descripción general del evento). En la sección **Message Events** (Eventos de mensaje), al evento de mensaje generado automáticamente se le asigna un nombre en función de la aplicación (por ejemplo, IRIS).

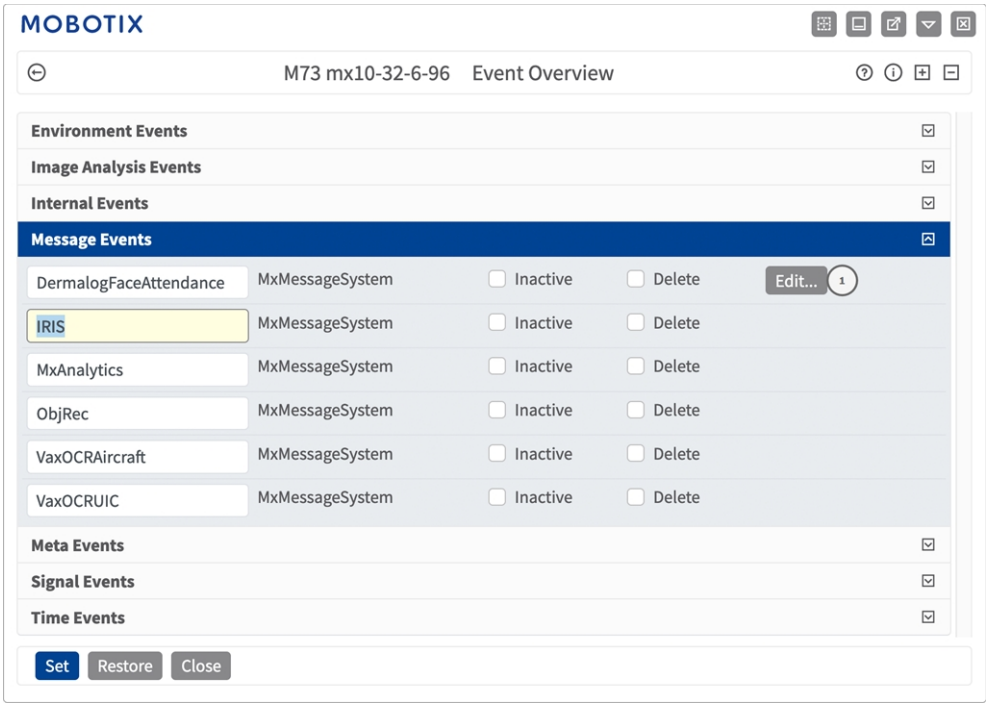


Fig. 27: Ejemplo: Evento de mensaje genérico de la Irisity IRIS AI Analytics - Intrusion Detection

2. Haga clic en **Edit** (Editar)① para visualizar una selección de todos los eventos de mensajes configurados.

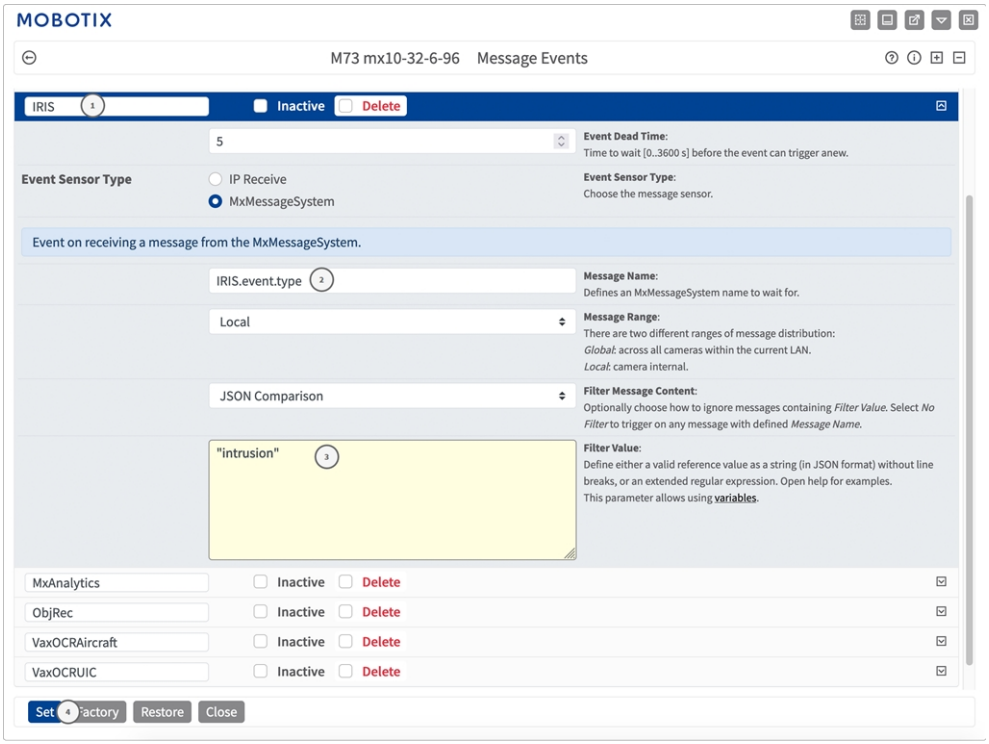


Fig. 28: Ejemplo: Evento de mensaje de intrusión

3. Haga clic en el evento (por ejemplo, IRIS) ① para abrir la configuración del evento.
4. Configure los parámetros del perfil del evento de la siguiente manera:

- **Message Name (Nombre del mensaje):** Introduzca el nombre del mensaje ② de acuerdo con la documentación del evento de la aplicación correspondiente (consulte Ejemplos de nombres de mensajes y valores de filtro de la Irisity IRIS AI Analytics - Intrusion Detection, p. 38)
- **Message Range (Rango del mensaje):**
  - **Local:** ajustes predeterminados para la Irisity IRIS AI Analytics - Intrusion Detection
  - **Global:** MxMessage se reenvía desde otra cámara MOBOTIX en la red local.
- **Filter Message Content (Filtrar contenido del mensaje):**
  - **Evento genérico:** "No Filter" (Sin filtro)
  - **Evento filtrado:** "Comparación JSON"
- **Filter Value (Valor de filtro):** ③ consulte Ejemplos de nombres de mensajes y valores de filtro de la Irisity IRIS AI Analytics - Intrusion Detection, p. 38.

ATENCIÓN! La opción de valor de filtro se utiliza para diferenciar los mensajes MxMessages de una aplicación o paquete. Utilice esta entrada para aprovechar los tipos de eventos individuales de las aplicaciones (si están disponibles).

Seleccione la opción "No Filter" (Sin filtro) si desea utilizar todos los MxMessages entrantes como evento genérico de la aplicación relacionada.

2. Haga clic en el botón **Set** (Establecer) ④ al final del cuadro de diálogo para confirmar los ajustes.

Ejemplos de nombres de mensajes y valores de filtro de la Irisity IRIS AI Analytics - Intrusion Detection

Detección de intrusiones IRIS	Nombre del MxMessage	Valor de filtro
Evento genérico	IRIS	
Evento de zona de alarma	IRIS.event.alarmZone	Nombre de la zona de alarma, p. ej.: "Zona de intrusión 2"
Tipo de evento	IRIS.event.type	"intrusión"

MOBOTIX

BeyondHumanVision

ES_03/23

MOBOTIX AG • Kaiserstrasse • D-67722 Langmeil • Tel.: +49 6302 9816-103 • sales@mobotix.com • www.mobotix.com