AXIS Optimizer

AXIS Optimizer para XProtect®
AXIS Optimizer for Siemens Siveillance™

Manual del usuario

Índice

AXIS Optimizer 7
Uso previsto de AXIS Optimizer 7
Requisitos del sistema 7
Compatibilidad con sistemas federados 7
Compatibilidad con sistemas interconectados 7
Notas de la versión 7
Instalar o actualizar AXIS Optimizer 8
Instalación de AXIS Optimizer 8
¿Qué versiones están instaladas en mi sistema? 8
Opciones avanzadas de instalación 8
Migración de VMS 9
Comprobar la integridad de la instalación 9
Actualizar AXIS Optimizer 9
Actualización manual 10
Actualizar sistema automáticamente 10
Activar actualización automática 10
Desactivar la actualización automática 11
Descubrir más 11
Desinstalar AXIS Optimizer 11
Factory default (Predeterminado de fábrica): 11
Desinstalación segura 11
Privilegios de usuario 12
Acceder a los ajustes de los dispositivos 13
Asistente de dispositivo 13
Configurar un dispositivo Axis 13
Instalación de aplicaciones en un dispositivo Axis 13
Configuración de aplicaciones en un dispositivo Axis 13
Actualizar aplicaciones en un dispositivo Axis 13
Reiniciar un dispositivo Axis 14
Copiar la dirección IP de un dispositivo Axis 14
Realizar automatización 15
Creación de acciones para dispositivos Axis 15
Complemento del servidor de eventos 15
Instalación del complemento del servidor de eventos 15
Seque varias cámaras con un solo clic 15
Activación del enfoque automático para varias cámaras con un solo clic 16
Activar varias sirenas estroboscópicas con un solo clic 17
Apagado automático de las máscaras de privacidad en varias cámaras 18
Activación de una sirena estroboscópica si una cámara detecta movimiento 20
Reproduce los clips de audio en altavoces o en una zona de altavoz cuando una cámara detecta movimiento 22
Solución de problemas de una regla 23
Gestión centralizada de listas de matrículas 24
Crear una lista 24
Configurar permisos de las listas 24
Edición de una lista 24
Importación de una lista 25
Exportación de una lista 26
Más información sobre las listas 26
Responder a eventos en directo 27
Usar los controles de dispositivo 27
Controles del operador 27
Acceso a los controles de operador 27

Guarde un área de enfoque para una cámara PTZ 27
Enfoque automático de la cámara 28
Activación de Speed Dry o de las escobillas de limpieza 28
Medir la temperatura de un punto 29
Amplía y sigue automáticamente un objeto en movimiento 29
Crear controles de operador personalizados 30
Configuración del acceso a los controles del operador 30
Interactúe a través de los altavoces 30
Gestor de altavoces 30
Modos 31
Modo de AXIS Audio Manager Pro 31
Modo de AXIS Audio Manager Edge 33
Modo clásico 34
Reproducir audio en altavoces 35
Reproducir audio en altavoces en la vista de la cámara 35
Reproducir audio en los altavoces de las alarmas 36
Ajustar el comportamiento visual para la interacción con el altavoz 36
Marcadores de clips de audio en la vista de la cámara o alarmas 36
Gestión de visitantes 37
Complemento de intercomunicación 37
Configuración de un intercomunicador 37
Configuración de permisos para intercomunicador 38
Realizar una llamada de prueba 39
Evitar eco durante las llamadas 39
Control del intercomunicador desde la visualización en directo 40
Responder a una llamada desde la visualización en directo 42
Mostrar varias cámaras en la ventana de llamada 43
Acciones de la ventana de llamada 44
Mostrar una página en la ventana de llamada 44
Filtrar por extensión de llamada 45
Ver el historial de llamadas 46
Desactivación del micrófono cuando no hay una llamada activa 46
Recepción de una alarma si se fuerza la apertura de una puerta 47
Recibir una alarma si una puerta permanece abierta demasiado tiempo 47
Impedir que un cliente reciba llamadas 47
Visualización de audio 47
Vista de micrófono 47
Configurar VMS para la vista de micrófono 48
Agregar la vista de micrófono a Smart Client 48
Usar vista de micrófono 48
Escuchar varios micrófonos al mismo tiempo 49
Detectar incidentes con audio 49
Investigar incidentes después de que sucedieron 49
Búsqueda forense 50
Búsqueda forense 50
Antes de empezar 50
Configurar la búsqueda forense 50
Realizar una búsqueda 51
Afinar una búsqueda 52
Limitaciones 52
Búsqueda de vehículos 53
Configurar la búsqueda de vehículos 55
Búsqueda de un vehículo 55
Afinar una búsqueda 55
Optimizar la velocidad de búsqueda 56
Búsqueda de velocidad de zona 56

Configurar búsqueda de velocidad de zona 56
Buscar por eventos de velocidad de zona 57
Afinar una búsqueda 57
Búsqueda de contenedores 58
Configuración de búsqueda de contenedores 58
Búsqueda de un contenedor 58
Afinar una búsqueda 59
Crear un informe en PDF de alta calidad 59
Matrículas de Axis 59
Antes de empezar 60
Configurar matrículas de Axis 60
Buscar una matrícula 60
Buscar una matrícula en directo 60
Afinar una búsqueda 61
Optimizar la velocidad de búsqueda 61
Exportar una búsqueda de matrícula como informe en PDF 61
Exportar una búsqueda de matrícula como informe en CSV 62
Información de Axis 62
Acceso a Axis Insights 62
Crear un nuevo panel de control 63
Configuración de la lista desplegable del panel de control 63
Mostrar información detallada de una vista de cámara concreta 63
Configurar la información de Axis 63
Solución de problemas en Axis Insights 64
Dewarping del vídeo 65
Crear una vista con corrección esférica 65
Crear una vista con corrección esférica para cámaras panorámicas multisensor 66
Gran angular 67
Definir una posición de inicio 67
Permitir a los operadores controlar y editar vistas con corrección esférica 68
Rendimiento y solución de problemas 68
Integración para uso en el cuerpo 70
Descubrir más 70
Control de acceso 71
Configuración de control de acceso 71
Añadir un controlador de puerta de red Axis a su sistema 71
Activar licencias de puerta 72
Configure el control de acceso 72
Integración del control de acceso 73
Puertas y zonas 73
Ejemplo de puertas y zonas 74
Agregar una puerta 75
Ajustes de puerta 76
Nivel de seguridad de puerta 77
Opciones de hora 78
Agregar un monitor de puerta 79
Agregar una puerta de supervisión 79
Agregar un lector 80
Agregar un dispositivo REX 81
Agregar una zona 82
Nivel de seguridad de zona 82
Entradas con supervisión 83
Acciones manuales 84
Formatos de tarjeta y PIN 85
Configuración del formato de tarjeta 86
Perfiles de identificación 88

Comunicación cifrada 89
Canal seguro OSDP 89
BETA de varios servidores 89
Flujo de trabajo 90
Generar el archivo de configuración desde el servidor secundario 90
Importar el archivo de configuración al servidor principal 90
Revocar un servidor secundario 90
Eliminar un servidor secundario 90
Gestión de acceso 91
Flujo de trabajo de gestión de acceso 91
Agregar un titular de tarjeta 91
Agregar credenciales 92
Agregar un grupo 95
Agregar una regla de acceso 95
Desbloquear puertas y zonas manualmente 95
Exportar informes de configuración del sistema 96
Crear informes de actividad de titulares de tarjeta 96
Configuración de gestión de acceso 97
Importación y exportación 97
Copia de seguridad y restauración 99
Gestión de acceso en Smart Client 99
Configuración de roles de AXIS Secure Entry 99
Gestión de sistemas y controles de seguridad 101
Personalizar el acceso a características de los operadores 101
Ajustes de función 101
Configuración de los ajustes de función 101
Gestión de dispositivos 102
AXIS Device Manager Extend 102
Instalar el host en el extremo 102
Reclamar el host en el extremo y sincronizar dispositivos 103
Utilizar AXIS Device Manager Extend para configurar dispositivos 104
Solución de problemas para agregar dispositivos al host en el extremo 104
Importar AXIS Site Designer 104
Importar un proyecto de diseño 104
Ajustes importados 105
Limitaciones 105
Administración de cuentas 106
Conéctese a dispositivos con cuenta de servicio XProtect 106
Eventos de Axis 106
Configurar un evento para varios dispositivos 107
Información de eventos 107
Metadata and search 107
Configurar los ajustes de metadatos 107
Configurar categorías de búsqueda de Axis 108
Ciberseguridad 109
Gestión de las vulnerabilidades 109
Notificaciones de seguridad 109
Ciclo de vida seguro del producto 109
Guía de seguridad 109
¿Necesita más ayuda? 110
Preguntas frecuentes 110
Localización de problemas 110
Contactar con la asistencia técnica 110
Sugerencias y consejos 111
Agregar una página web en una vista Smart Client 111
Exportar vídeos con funciones de búsqueda integradas 111

Exportar vídeos en formato XProtect 111
Desbloquear exportaciones en ordenadores receptores 111
Reproducción de la vista de corrección de distorsión esférica de Axis exportada 111

AXIS Optimizer

AXIS Optimizer proporciona las funciones de Axis directamente en XProtect o Siemens Siveillance Video. La aplicación optimiza el rendimiento de los dispositivos Axis en estos sistemas de gestión de vídeo, lo que le permite ahorrar tiempo y esfuerzo al configurar sistemas o durante su funcionamiento diario. La aplicación es gratuita.

Uso previsto de AXIS Optimizer

Este producto está dirigido al uso por profesionales con amplios conocimientos en el manejo de un Sistema de gestión de vídeo (VMS).

Requisitos del sistema

AXIS Optimizer es totalmente compatible con las siguientes plataformas:

- XProtect Essential+
- XProtect Express+
- XProtect Professional+
- XProtect Expert
- XProtect Corporate
- Siemens Siveillance Video Pro
- Siemens Siveillance Video Advanced
- Siemens Siveillance Video Core Plus
- Siemens Siveillance Video Core

Recomendamos utilizar las últimas versiones de Management Client y Smart Client. La última versión de AXIS Optimizer está siempre verificada y es compatible con la versión más reciente del VMS. Para obtener más información, le las *Notas de la versión, on page 7*.

Nota

Plataforma compatible mínima

- Versión 2019 R3 del VMS.

Cuando se hace referencia a Smart Client en la ayuda, nos referimos tanto a XProtect Smart Client como a Video Client en un sistema Siemens.

Compatibilidad con sistemas federados

AXIS Optimizer es totalmente compatible con los sistemas federados.

Compatibilidad con sistemas interconectados

AXIS Optimizer es totalmente compatible con los sistemas interconectados.

Nota

Requisitos

- Version 2022 R3 o posterior de VMS.

Notas de la versión

Para ver las notas de la versión más reciente, vaya a *axis.com/ftp/pub_soft/cam_srv/optimizer_milestone/latest/relnote.txt*.

Instalar o actualizar AXIS Optimizer

Instalación de AXIS Optimizer



Nota

Para actualizar AXIS Optimizer, debe tener derechos de administrador.

1. Asegúrese de que cuenta con la versión cliente correcta del VMS.
2. Inicie sesión en su cuenta MyAxis.
3. Desde *axis.com/products/axis-optimizer-for-milestone-xprotect*, descargue AXIS Optimizer en cada dispositivo en el que se ejecute el cliente de gestión o Smart Client.
4. Ejecute el archivo descargado y siga las instrucciones de la guía paso a paso.

¿Qué versiones están instaladas en mi sistema?

En **System overview (Descripción del sistema)** puede ver qué versiones de AXIS Optimizer y AXIS Optimizer Body Worn Extension están instaladas en los diferentes servidores y clientes de su sistema.

Nota

Para ver los clientes o servidores en **System overview (Información general del sistema)**, estos deben contar con la versión 3.7.17.0 de AXIS Optimizer y la versión 1.1.11.0 o posterior de AXIS Optimizer Body Worn Extension.

Para ver servidores y clientes activos:

1. En Cliente de gestión, vaya a **Site Navigation > AXIS Optimizer > System overview (Navegación del sitio > AXIS Optimizer > Información general del sistema)**.

Para actualizar un servidor o cliente determinado:

1. Vaya a ese servidor o cliente y actualícelo localmente.

Opciones avanzadas de instalación

Para instalar AXIS Optimizer en varios dispositivos a la vez y sin interacción del usuario:

1. Haga clic con el botón derecho en el menú **Start (Inicio)**.
2. Haga clic en **Ejecutar**.
3. Busque el archivo de instalación descargado y haga clic en **Open (Abrir)**.
4. Agregue parámetros al final de la ruta.

Parámetro	Descripción
`/SILENT`	Durante una instalación silenciosa, no aparecen ni la guía paso a paso ni la ventana de fondo. Sin embargo, sí se muestra la ventana de progreso de la instalación.
`/VERYSILENT`	Durante una instalación muy silenciosa, no aparecen ni la guía paso a paso ni la ventana de fondo ni la ventana de progreso de la instalación.

/FULL	Instale todos los componentes, por ejemplo, el complemento de servidor de eventos opcional y el complemento Secure Entry. Resulta útil combinado con /VERYSILENT.
/SUPPRESSMSGBOXES	Suprimir todos los cuadros de mensaje. Se suele combinar con /VERYSILENT.
/log=<filename>	Crea un archivo de registro.
/NORESTART	Impide que el equipo se reinicie durante la instalación.
/EVENTSERVERPLUGIN	Instale el complemento del servidor de eventos si el equipo de destino es el servidor de eventos.
/SECUREENTRY	Instale el servicio de control de acceso Secure Entry si el equipo de destino es el servidor de eventos.

5. Presione **Enter (Intro)**.

Ejemplo:
Instalación verysilent, que se registra en output.txt, sin reiniciar el ordenador

```
.\AxisOptimizerXProtectSetup.exe /VERYSILENT /log=output.txt /NORESTART
```

Migración de VMS

AXIS Optimizer almacena la mayor parte de los datos en la base de datos del VMS y, por ello, la información se conserva al migrar el VMS a otro servidor.

Para migrar su VMS a otro servidor, consulte *How to move an XProtect VMS installation/version from old servers to new servers (Cómo trasladar una instalación/versión de XProtect VMS de servidores antiguos a servidores nuevos)*.

Comprobar la integridad de la instalación

Para comprobar la integridad del instalador AXIS Optimizer:

1. Haga clic con el botón derecho del ratón en el archivo de instalación y seleccione **Properties (Propiedades)**.
2. Vaya a **Digital Signatures (Firmas digitales)** y haga clic en **Details (Detalles)**.
3. Compruebe los siguientes aspectos:
   - En la sección **Digital Signature Information (Información sobre la firma digital)** aparece el mensaje: This digital signature is OK (Esta firma digital es válida).
   - En **Signer information (Información del firmante)** > **Name (Nombre)** aparece Axis Communications AB.

Actualizar AXIS Optimizer

Actualizamos periódicamente AXIS Optimizer con funciones nuevas, mejoras y actualizaciones de seguridad. AXIS Optimizer solo ofrece una única versión (la más reciente y mejorada) y solo esta última versión está disponible para su descarga en axis.com. Recomendamos utilizar siempre la última versión de AXIS Optimizer.

AXIS Optimizer también incluye una función que permite actualizar todos los clientes de su VMS. Para obtener más información, consulte la sección *Upgrade system automatically (Actualizar el sistema automáticamente)*.

Nota

Para actualizar AXIS Optimizer, debe tener derechos de administrador.

Notificaciones de actualización

AXIS Optimizer comprueba periódicamente si hay nuevas versiones y notifica cuando hay actualizaciones. Si tiene conexión a la red, va a recibir notificaciones de actualización en Smart Client.

Para modificar el tipo de notificaciones que recibe:

1. En Smart Client, vaya a **Settings (Ajustes)** > **Axis general options (Opciones generales de Axis)** > **Notification preference (Preferencias de notificación)**.
2. Seleccione **All (Todas)**, **Major (Principales)** o **None (Ninguna)**.

Para configurar estas notificaciones para todos los clientes de su VMS:

1. Vaya a **Management Client (Gestión de clientes)** > **Site Navigation (Navegación de instalaciones)** > **AXIS Optimizer** > **System overview (Resumen del sistema)**.
2. Haga clic en **System upgrade settings (Configuración de actualización del sistema)**.
3. Activar o desactivar **Show upgrade notifications on all clients (Mostrar notificaciones de actualización en todos los clientes)**.

Actualización manual

Puede actualizar manualmente AXIS Optimizer desde Management Client y Smart Client.

Nota

Para actualizar AXIS Optimizer, debe tener derechos de administrador.

En Management Client

1. Vaya a **Site Navigation > Basics > AXIS Optimizer (Navegación del sitio > Aspectos básicos > AXIS Optimizer)**.
2. Haga clic en **Update (Actualizar)**.

En Smart Client

1. Vaya a **Settings > Axis general options (Configuración > Opciones generales de Axis)**.
2. Haga clic en **Update (Actualizar)**.

Actualizar sistema automáticamente

Desde el servidor de gestión VMS, puede publicar una versión local de AXIS Optimizer en el sistema. Cuando lo haga, AXIS Optimizer se actualizará automáticamente en todos los equipos cliente. La actualización automática nunca interrumpe el trabajo del operador. Las instalaciones de los equipos se realizan mientras el equipo o el cliente VMS se reinician. La actualización automática también es compatible cuando el cliente no está conectado a Internet.

Nota

La actualización automática es compatible con los clientes que ejecutan AXIS Optimizer 4.4 o una versión superior.

Activar actualización automática



Nota

Requisitos

- Un sistema donde Management Client se ejecuta en la misma máquina que el servidor de administración VMS.
- Derechos de administrador de PC en el servidor de administración de VMS.

Para activar la actualización automática, debe publicar una versión específica de AXIS Optimizer en el sistema:

1. En el servidor de gestión VMS, instale la versión de AXIS Optimizer que desea publicar en todo el sistema.
2. En la máquina del servidor de administración de VMS, abra Management Client.
3. Vaya a **Site Navigation > AXIS Optimizer > System overview (Navegación de instalaciones) > AXIS Optimizer > Información general del sistema)**.
4. Haga clic en **System upgrade settings (Configuración de actualización del sistema)**.
5. Asegúrese de que la **Local version (Versión local)** es correcta y haga clic en **Publish (Publicar)**.
   Si ya existe otra versión de AXIS Optimizer publicada, se sustituye por la nueva versión.

Nota

Los equipos cliente con una versión anterior de AXIS Optimizer 4.4 deben actualizarse manualmente.

Desactivar la actualización automática

Para desactivar la actualización automática, debe restablecer la versión publicada:

1. En la máquina del servidor de administración de VMS, abra Management Client.
2. Vaya a **Site Navigation > AXIS Optimizer > System overview (Navegación de instalaciones) > AXIS Optimizer > Información general del sistema)**.
3. Haga clic **en configuración de actualización > restablecer la versión publicada** .

Descubrir más

- Los Smart Clients sin AXIS Optimizer pueden acceder al archivo de instalación publicado en la página web del servidor de gestión (*http:///[serveradress]/instalación/*) aunque no estén conectados a Internet.
- El paquete de instalación de AXIS Optimizer está disponible y es configurable en gestor de descargas del VMS.
- En sistemas federados o interconectados, debe publicar AXIS Optimizer en cada servidor de administración.
- Después de publicar una nueva versión de AXIS Optimizer, puede supervisar qué clientes se han actualizado a la versión publicada. Los equipos de la **página Información general del** sistema mostrarán un símbolo de comprobación verde cuando estén ejecutando la versión publicada.
- La actualización automática está desactivada en los equipos que ejecutan un servidor de gestión VMS.

Desinstalar AXIS Optimizer

Factory default (Predeterminado de fábrica):

Para restablecer AXIS Optimizer a su configuración predeterminada, desinstálelo del VMS y vuelva a instalarlo.

Desinstalación segura

Para eliminar por completo AXIS Optimizer y los datos almacenados del VMS, debe seguir primero los siguientes pasos, cuando proceda, antes de eliminarlo de su ordenador local.

1. Para eliminar las listas de matrículas:
   - Abra Management Client y vaya a **AXIS Optimizer** > **License plate lists (Listas de matrículas)**.
   - Elimine todas las instalaciones de la lista.
2. Para desconectar el servidor de AXIS Audio Manager Pro:

- Abra Management Client y vaya a **AXIS Optimizer** > **Speaker manager (Gestor de altavoces)**.
- Haga clic en **Disconnect (Desconectar)**.

Para eliminar AXIS Optimizer y los datos almacenados localmente en el ordenador:

1. Haga clic en el **Start menu (menú Inicio) > Settings (Ajustes)** > **Apps (Aplicaciones)** > **Installed apps (Aplicaciones instaladas)**.
2. Vaya a **AXIS Optimizer**.
3. Haga clic en p,255mm,sfx)=″graphics:graphic018FACAAED177A53B1E07E58CECD82C6″ y seleccione **Uninstall (Desinstalar)**.

Nota

Una vez desinstalado AXIS Optimizer, es posible que deba reiniciar algunos servicios de VMS.

Privilegios de usuario

AXIS Optimizer incluye una función de usuario específica de Axis Optimizer. El objetivo es facilitarle la tarea de asignar a los usuarios los privilegios Smart Client necesarios para utilizar las funciones y capacidades de AXIS Optimizer.

Si ejecuta XProtect 2018 R3 o una versión anterior, esta función solo está disponible en XProtect Corporate.

Si ejecuta XProtect 2019 R1 o posterior, esta función va a esta disponible para las siguientes ediciones de XProtect:

- Corporativo
- Experto
- Professional+
- Essential+
- Express+

Si prefiere configurar los privilegios manualmente, utilice esta configuración para que un operador de Smart Client pueda usar todas las funcionalidades incluidas en AXIS Optimizer:

- Hardware: comandos del controlador
- Cámaras: Comandos AUX

Nota

Para una gestión más avanzada de las funciones de los usuarios, consulte *Personalizar el acceso a características de los operadores, on page 101*.

Acceder a los ajustes de los dispositivos

Asistente de dispositivo

Utilice el Asistente de dispositivos para acceder fácilmente a todos los ajustes de los dispositivos de Axis directamente en VMS Management Client. Puede encontrar y acceder fácilmente al sitio web de su dispositivo Axis en el VMS a fin de modificar los diferentes ajustes del mismo. También puede configurar las aplicaciones instaladas en sus diferentes dispositivos.

Importante

- Para que se pueda utilizar el asistente del dispositivo, el equipo Axis debe estar conectado a la misma red que el cliente de gestión.
- El Asistente de dispositivos no es compatible con redes IPv6.

Configurar un dispositivo Axis

1. En Management Client (Cliente de gestión), vaya a **Site Navigation > AXIS Optimizer > Device Assistant (Navegación del sitio > Optimizador AXIS > Asistente del dispositivo)**.
2. Seleccione un dispositivo y vaya a **Device settings (Configuración del dispositivo)**. Se abrirá la página web del dispositivo
3. Configure los ajustes que desee.

Instalación de aplicaciones en un dispositivo Axis

1. En Management Client (Cliente de gestión), vaya a **Site Navigation > AXIS Optimizer > Device Assistant (Navegación del sitio > Optimizador AXIS > Asistente del dispositivo)**.
2. Seleccione un dispositivo y vaya a **Device settings (Configuración del dispositivo)**. Se abrirá la página web del dispositivo
3. Vaya a **Apps (Aplicaciones)**. La ubicación de la función **Apps (Aplicaciones)** depende de la versión de software del dispositivo. Para más información, consulte la ayuda de su dispositivo.
4. Instale las aplicaciones que desee.

Configuración de aplicaciones en un dispositivo Axis

1. En Management Client (Cliente de gestión), vaya a **Site Navigation > AXIS Optimizer > Device Assistant (Navegación del sitio > Optimizador AXIS > Asistente del dispositivo)**.
2. Seleccione un dispositivo y vaya a **Applications (Aplicaciones)**. Si hay aplicaciones instaladas en el dispositivo, las ve aquí.
3. Vaya a la aplicación correspondiente, por ejemplo, AXIS Object Analytics.
4. Configure la aplicación para que se adapte a sus necesidades.

Actualizar aplicaciones en un dispositivo Axis

1. En Management Client (Cliente de gestión), vaya a **Site Navigation > AXIS Optimizer > Device Assistant (Navegación del sitio > Optimizador AXIS > Asistente del dispositivo)**.
2. Haga clic con el botón derecho en un dispositivo y seleccione **Show updates (Mostrar actualizaciones)**. Si se puede actualizar alguna aplicación, va a ver una lista de las actualizaciones disponibles.
3. Descargue el archivo de actualización.
4. Haga clic en **How to update (Cómo actualizar)** y siga las instrucciones.

Reiniciar un dispositivo Axis

1. En Management Client (Cliente de gestión), vaya a **Site Navigation > AXIS Optimizer > Device Assistant (Navegación del sitio > Optimizador AXIS > Asistente del dispositivo)**.
2. Haga clic con el botón derecho en un dispositivo y seleccione **Restart device (Reiniciar dispositivo)**.

Copiar la dirección IP de un dispositivo Axis

1. En Management Client (Cliente de gestión), vaya a **Site Navigation > AXIS Optimizer > Device Assistant (Navegación del sitio > Optimizador AXIS > Asistente del dispositivo)**.
2. Haga clic con el botón derecho en un dispositivo y seleccione **Copy device address (Copiar dirección del dispositivo)**.

Realizar automatización

Creación de acciones para dispositivos Axis

Complemento del servidor de eventos

El complemento del servidor de eventos de AXIS Optimizer le permite crear acciones personalizadas para dispositivos Axis. Cuando utiliza el motor de reglas XProtect y el complemento del servidor de eventos, puede, por ejemplo:

- Realizar una acción personalizada cuando el operador haga clic en un botón de Smart Client. Para ver un ejemplo de configuración, consulte *Seque varias cámaras con un solo clic, on page 15*.
- Realice acciones sin interacción humana (automatización). Para ver un ejemplo de configuración, consulte *Apagado automático de las máscaras de privacidad en varias cámaras, on page 18*.

El complemento del servidor de eventos consta de dos partes:

- Un complemento independiente que se ejecuta en el servidor de eventos. Este rellena el motor de reglas con nuevas actions (acciones).
- Una página denominada **Axis actions (Acciones Axis)** en el servidor de gestión, donde se pueden crear nuevas action presets (Preconfiguraciones de acción).

Las acciones personalizadas para los dispositivos de Axis son: Ejecución del control del operador, encendido/apagado del radar, inicio de una llamada en el intercomunicador y el secado de la cámara (SpeedDry/escobilla de limpieza).

El plugin del servidor de eventos está incluido en AXIS Optimizer. En un sistema con varios ordenadores, debe instalar AXIS Optimizer tanto en el equipo del Cliente de administración como en el equipo del servidor de eventos.

Instalación del complemento del servidor de eventos

El complemento del servidor de eventos es un componente opcional que se incluye en el instalador de AXIS Optimizer. Solo se puede instalar en un servidor de eventos del sistema de gestión de vídeo (VMS). Si se cumplen los requisitos, se le presenta la opción de instalar el complemento del servidor de eventos cuando ejecute el instalador de AXIS Optimizer.

Nota

El servidor de eventos VMS requiere un breve reinicio durante la instalación y, a veces, durante la actualización de AXIS Optimizer. En ese caso, recibirá una notificación.

Seque varias cámaras con un solo clic

Con el complemento del servidor de eventos se pueden establecer reglas personalizadas que faciliten el trabajo de los operadores. En este ejemplo vamos a mostrar cómo secar todas las cámaras de un área específica haciendo clic en un botón de superposición.



Nota

Requisitos

- AXIS Optimizer versión 4.0 o posterior en el servidor de eventos y con Management Client
- Una o varias cámaras compatibles con SpeedDry o con las escobillas de limpieza; por ejemplo, las series AXIS Q86, Q87 o Q61.

1. Agregar un evento definido por el usuario:
   1.1. Vaya a **Site Navigation > Rules and Events (Navegación de instalaciones > Reglas y eventos)** y haga clic derecho en **User-defined Event (Evento definido por el usuario)**.
   1.2. Seleccione **Add User-defined Event (Agregar evento definido por el usuario)** e introduzca un nombre, en este ejemplo: "Secar todas las cámaras".
2. Crear una nueva regla:
   2.1. Vaya a **Site Navigation > Rules and Events (Navegación del sitio > Reglas y eventos)** y haga clic con el botón derecho en **Rules (Reglas)**.
   2.2. Seleccione **Add Rule (Agregar regla)** e introduzca un nombre, en este ejemplo: "Regla de secado de todas las cámaras".
   2.3. Seleccione **Perform an action on <event> (Realizar una acción al <evento>)**.
   2.4. En el campo **Edit the rule description (Editar la descripción de la regla)**, haga clic en **event (evento)**.
   2.5. Vaya a **Events > External Events > User-defined Events (Eventos > Eventos externos > Eventos definidos por el usuario)** y seleccione **Dry all cameras (Secar todas las cámaras)**.
   2.6. Haga clic en **Next (Siguiente)** hasta llegar a **Step 3: Actions (Paso 3: Acciones)**.
   2.7. Seleccione la acción: **Axis: Dry <camera> (Axis: Secar <cámara>)**.
   2.8. En el campo **Edit the rule description (Editar la descripción de la regla)**, haga clic en **Axis: Dry camera (Axis: Secar cámara)**.
   2.9. En la ventana **Select Triggering Devices (Seleccionar dispositivos de activación)**, elija **Select devices (Seleccionar dispositivos)** y haga clic en **OK (Aceptar)**.
   2.10. Seleccione en qué dispositivos desea activar la acción y haga clic en **OK (Aceptar)**) y, a continuación, en **Finish (Finalizar)**.
3. En Smart Client, añada el evento definido por el usuario como botón superpuesto en la vista de mapa o de vídeo.
4. Haga clic en el botón de superposición y asegúrese de que la regla funciona como desea.

Activación del enfoque automático para varias cámaras con un solo clic

Con el complemento del servidor de eventos se pueden establecer reglas personalizadas que faciliten el trabajo de los operadores. En este ejemplo mostramos cómo activar el enfoque automático para todas las cámaras con un solo clic.

Nota

Requisitos

- AXIS Optimizer versión 4.1 o posterior en el servidor de eventos y con Management Client
- Una o varias cámaras compatibles con el enfoque automático

1. Agregar un evento definido por el usuario:
   1.1. Vaya a **Site Navigation > Rules and Events (Navegación de instalaciones > Reglas y eventos)** y haga clic derecho en **User-defined Event (Evento definido por el usuario)**.
   1.2. Seleccione **Add User-defined Event (Agregar evento definido por el usuario)** e introduzca un nombre, en este ejemplo, "Enfoque automático".
2. Crear una nueva regla:
   2.1. Vaya a **Site Navigation > Rules and Events (Navegación del sitio > Reglas y eventos)** y haga clic con el botón derecho en **Rules (Reglas)**.

2.2. Seleccione **Add Rule (Agregar regla)** e introduzca un nombre, en este ejemplo "Realizar enfoque automático".

2.3. Seleccione **Perform an action on <event> (Realizar una acción al <evento>)**.

2.4. En el campo **Edit the rule description (Editar la descripción de la regla)**, haga clic en **event (evento)**.

2.5. Vaya a **Events > External Events > User-defined Events (Eventos > Eventos externos > Eventos definidos por el usuario)** y seleccione **Autofocus (Enfoque automático)**. Haga clic en **OK**.

2.6. Haga clic en **Next (Siguiente)** hasta llegar a **Step 3: Actions (Paso 3: Acciones)**.

2.7. Seleccione la acción **Axis: Run autofocus on <camera> (Axis: Ejecutar enfoque automático en <cámara>)**.

2.8. En el campo **Edit the rule description (Editar la descripción de la regla)**, haga clic en **Axis: Run autofocus on camera (Axis: Ejecutar enfoque automático en cámara)**.

2.9. En la ventana **Select Triggering Devices (Seleccionar dispositivos de activación)**, elija **Select devices (Seleccionar dispositivos)** y haga clic en **OK (Aceptar)**.

2.10. Seleccione en qué dispositivos desea activar la acción y haga clic en **OK (Aceptar)**) y, a continuación, en **Finish (Finalizar)**.

3. En Smart Client, añada el evento definido por el usuario "enfoque automático" como botón superpuesto en la vista de mapa o de vídeo.
4. Haga clic en el botón de superposición y asegúrese de que la regla funciona como desea.

Activar varias sirenas estroboscópicas con un solo clic

Con el complemento del servidor de eventos se pueden establecer reglas personalizadas que faciliten el trabajo de los operadores. En este ejemplo se indica cómo activar varias sirenas estroboscópicas con un solo clic en Smart Client.

Nota

Requisitos

- AXIS Optimizer versión 4.4 o posterior en el servidor de eventos y con Management Client
- Una o varias sirenas estroboscópicas de Axis
- Salida 1 de la sirena estroboscópica de Axis habilitada y agregada a los dispositivos de salida en Management Client

1. Cree un evento definido por el usuario:
   1.1. Vaya a **Site Navigation > Rules and Events (Navegación de instalaciones > Reglas y eventos)** y haga clic derecho en **User-defined Event (Evento definido por el usuario)**.
   1.2. Seleccione **Add User-defined Event (Agregar evento definido por el usuario)** y escriba un nombre, por ejemplo "Activar todas las sirenas estroboscópicas".
2. En el asistente de dispositivos, cree perfiles de sirena estroboscópica:
   2.1. Vaya a **Site Navigation > AXIS Optimizer > Device assistant (Navegación de instalaciones > AXIS Optimizer > Asistente de dispositivos)**.
   2.2. Seleccione una sirena estroboscópica. Se abre la página web de la sirena.
   2.3. Vaya a **Profiles (Perfiles)** y haga clic en **Add profile (Agregar perfil)**.
   2.4. Configure las acciones que debe realizar la sirena estroboscópica cuando el operador active las sirenas estroboscópicas en Smart Client.
   2.5. Cree los mismos perfiles en las demás sirenas estroboscópicas. Debe utilizar el mismo nombre de perfil en todos los dispositivos
3. En acciones de Axis, cree una acción predefinida:

3.1. Vaya a **Site Navigation > Rules and Events > Axis actions (Navegación de instalaciones > Reglas y eventos > Acciones de Axis)**.

3.2. Haga clic en **Add new preset (Añadir nueva posición predefinida)**.

3.3. Vaya a **Select strobe siren (Seleccionar una sirena estroboscópica)** y haga clic en **Strobe siren (Sirena estroboscópica)**.

3.4. Seleccione las sirenas estroboscópicas que quiera utilizar y haga clic en **OK (Aceptar)**.
Verá una lista con los perfiles de sirenas estroboscópicas

3.5. Seleccione el perfil de sirena estroboscópica que ha creado en el paso anterior. La acción predefinida se guarda automáticamente

3.6. Pulse F5 para actualizar la configuración del servidor. Ya puede empezar a usar la nueva acción predefinida de acción que ha creado.

4. Crear una regla:

4.1. Vaya a **Site Navigation > Rules and Events (Navegación del sitio > Reglas y eventos)** y haga clic con el botón derecho en **Rules (Reglas)**.

4.2. Seleccione **Add Rule (Agregar regla)** y escriba un nombre, por ejemplo "Regla de activación de todas las sirenas estroboscópicas".

4.3. Seleccione **Perform an action on <event> (Realizar una acción al <evento>)**.

4.4. En el campo **Edit the rule description (Editar la descripción de la regla)**, haga clic en **event (evento)**.

4.5. Vaya a **Events > External Events > User-defined Events (Eventos > Eventos externos > Eventos definidos por el usuario)** y seleccione **Trigger all strobe sirens (Activar todas las sirenas estroboscópicas)**.

4.6. Haga clic en **Next (Siguiente)** hasta llegar a **Step 3: Actions (Paso 3: Acciones)**.

4.7. Seleccione la acción **Axis: Run a profile on a strobe siren <preset> (Axis: Ejecutar un perfil al activarse una sirena estroboscópica <posición predefinida>)**.

4.8. En el campo **Edit the rule description (Editar la descripción de la regla)**, haga clic en **preset (preajustar)**.

4.9. Seleccione la acción predefinida que quiera usar.

4.10. Haga clic en **Next (Siguiente)** y, a continuación, en **Finish (Finalizar)**.

5. En Smart Client, añada el evento definido por el usuario como botón superpuesto en la vista de mapa o de vídeo.

6. Haga clic en el botón de superposición y asegúrese de que la regla funciona como desea.

Apagado automático de las máscaras de privacidad en varias cámaras

Con el complemento del servidor de eventos puede automatizar ciertas acciones. En este ejemplo se muestra cómo desactivar automáticamente las máscaras de privacidad en varias cámaras cuando se produce un evento de análisis. El evento del ejemplo consiste en que las personas o los vehículos entren en una zona en la que no deberían estar normalmente. Por lo tanto, queremos desactivar automáticamente las máscaras de privacidad para obtener una mejor visión de lo que está sucediendo.



El flujo de trabajo está:

1. *Configurar un escenario de analítica, on page 19*en AXIS Object Analytics (u otra aplicación de análisis de su elección)
2. *Añadir controles de operador a las cámaras pertinentes, on page 19*
3. *Crear acciones predefinidas, on page 19*
4. *Crear una regla para desactivar las máscaras de privacidad cuando se produce un evento de análisis, on page 19*
5. *Crear una regla para volver a activar las máscaras de privacidad, on page 20*
6. *Comprobación de la regla, on page 20* y asegúrese de que todo funciona como usted quiere.

Nota

Requisitos

- AXIS Optimizer versión 4.0 o posterior en el servidor de eventos y con Management Client
- Cámaras con AXIS OS 7.40 o posterior
- Cámaras que puedan generar eventos, en este caso una cámara con AXIS Object Analytics

Configurar un escenario de analítica

1. Vaya a **Site Navigation > AXIS Optimizer > Device assistant (Navegación del sitio > AXIS Optimizer > Asistente del dispositivo** y encuentre el dispositivo con las analíticas que desea utilizar.
2. Haga clic en **Applications (Aplicaciones)** y cree un escenario de analíticas que activen la acción.
3. Vaya a **Devices > Cameras (Dispositivos > Cámaras)** y encuentre la cámara en la que ha creado el escenario de analíticas.
4. En la ventana **Properties (Propiedades)**, haga clic en **Events > Add (Eventos > Agregar)**.
5. Seleccione un evento del controlador; en este ejemplo, "Analíticas de objetos: prueba de evento de subida" y haga clic en **OK (Aceptar)**.
6. Haga clic en **Add (Agregar)** y seleccione el evento de controlador "Analítica de objetos: prueba de evento de bajada". A continuación, haga clic en **OK (Aceptar)**.
7. Haga clic en **Save (Guardar)**.

Añadir controles de operador a las cámaras pertinentes

1. Vaya a **AXIS Optimizer > Operator controls (AXIS Optimizer > Controles del operador)** y abra la biblioteca de controles.
2. En la ventana **Configuration (Configuración)**, seleccione la carpeta correspondiente y active tanto **Turn off privacy mask (Activar máscara de privacidad)** como **Turn on privacy mask (Desactivar máscara de privacidad)**.

Crear acciones predefinidas

1. Vaya a **Rules and Events > Axis actions (Reglas y eventos > acciones de Axis)** y haga clic en **Add new preset (Agregar nuevo preajuste)**.
2. Haga clic en **Cameras (Cámaras)** y seleccione las cámaras pertinentes. En este ejemplo: AXIS P1375 y AXIS Q6075-E. A continuación, seleccione el control **Turn on privacy mask (Activar máscara de privacidad)**.
3. Haga clic en **Add new preset > Cameras (Agregar nueva configuración predefinida > Cámaras)** y seleccione las cámaras relevantes. En este ejemplo: AXIS P1375 y AXIS Q6075-E. A continuación, seleccione el control **TURN off privacy mask (Desactivar máscara de privacidad)**.

Crear una regla para desactivar las máscaras de privacidad cuando se produce un evento de análisis

1. Vaya a **Site Navigation > Rules and Events (Navegación del sitio > Reglas y eventos)** y haga clic con el botón derecho en **Rules (Reglas)**.

2. Seleccione **Add Rule (Añadir regla)** e introduzca un nombre, en este ejemplo; "Desactivar la máscara de privacidad en analíticas".
3. Seleccione **Perform an action on <event> (Realizar una acción al <evento>)**.
4. En el campo **Edit the rule description (Editar la descripción de la regla)**, haga clic en **event (evento)**. Vaya a **Devices (Dispositivos) > Configurable Events (Eventos configurables)** y seleccione **Object Analytics: Event test Rising (Analíticas de objetos: prueba de evento Elevación)**.
5. En el campo **Edit the rule description (Editar la descripción de la regla)**, seleccione un dispositivo, en este ejemplo el modelo AXIS P1375.
6. Haga clic en **Next (Siguiente)** hasta llegar a **Step 3: Actions (Paso 3: Acciones)**.
7. Seleccione la acción **Axis: Run operator control: <preset> (Axis: Ejecutar control del operador: <posición predefinida>)**.
8. En el campo **Edit the rule description (Editar la descripción de la regla)**, haga clic en **preset (preajustar)**. A continuación, añada el objetivo **Turn off privacy mask on 2 cameras (Desactivar máscara de privacidad en 2 cámaras)** y haga clic en **OK (Aceptar)**.
9. Haga clic en **Finalizar**.

Crear una regla para volver a activar las máscaras de privacidad

1. Seleccione **Add Rule (Agregar regla)** e introduzca un nombre, en este ejemplo; "Activar la máscara de privacidad en la parada analítica".
2. Seleccione **Perform an action on <event> (Realizar una acción al <evento>)**.
3. En la sección **Edit the rule description (Editar la descripción de la regla)**, haga clic en **event (evento)**. Vaya a **Devices (Dispositivos) > Configurable Events (Eventos configurables)** y seleccione **Object Analytics: Event test Failing (Analíticas de objetos: prueba de evento Caída)**.
4. En **Edit the rule description (Editar la descripción de la regla)**, seleccione un dispositivo, en este ejemplo el modelo AXIS P1375.
5. Haga clic en **Next (Siguiente)** hasta llegar a **Step 3: Actions (Paso 3: Acciones)**.
6. Seleccione la acción **Axis: Run operator control: <preset> (Axis: Ejecutar control del operador: <posición predefinida>)**.
7. En la sección **Edit the rule description (Editar la descripción de la regla)**, haga clic en **preset (predefinido)**. A continuación, añada el objetivo **Turn on privacy mask on 2 cameras (Activar máscara de privacidad en 2 cámaras)** y haga clic en **OK (Aceptar)**.
8. Haga clic en **Finalizar**.

Comprobación de la regla

1. Vaya a **AXIS Optimizer > Device Assistant (AXIS Optimizer > Asistente de dispositivos)** y encuentre el dispositivo con la analítica que ha utilizado para crear la automatización. En este ejemplo; el modelo AXIS P1375.
2. Abra el escenario correspondiente y haga clic en **Test alarm (Comprobar la alarma)**.

Activación de una sirena estroboscópica si una cámara detecta movimiento

Mediante el complemento de servidor de eventos, puede configurar reglas personalizadas para automatizar las acciones. En este ejemplo se muestra cómo activar sirenas estroboscópicas automáticamente si una cámara detecta movimiento.

Nota

Requisitos

- AXIS Optimizer versión 4.4 o posterior en el servidor de eventos y con Management Client
- Una o varias sirenas estroboscópicas de Axis
- Salida 1 de la sirena estroboscópica de Axis habilitada y agregada a los dispositivos de salida en Management Client.
- En versiones del VMS anteriores a 2022 R2, las acciones de Axis no están disponibles como acciones de detección. En las versiones anteriores es necesario crear dos reglas independientes para ejecutar y detener la sirena estroboscópica.

1. Cree perfiles de sirena estroboscópica:
   1.1. Vaya a **Site Navigation > AXIS Optimizer > Device assistant (Navegación de instalaciones > AXIS Optimizer > Asistente de dispositivos)**.
   1.2. Vaya a **Axis output devices (Dispositivos de salida Axis)** y seleccione una sirena estroboscópica. Se abre la página web de la sirena.
   1.3. Vaya a **Profiles (Perfiles)** y haga clic en **Add profile (Agregar perfil)**.
   1.4. Debe elegir el mismo nombre de perfil para todas las sirenas.
   1.5. Configure el comportamiento de la sirena estroboscópica cuando se detecte movimiento.
2. Cree acciones de inicio y detección predefinidas:
   2.1. Vaya a **Site Navigation > Rules and Events > Axis actions (Navegación de instalaciones > Reglas y eventos > Acciones de Axis)**.
   2.2. Para crear una acción de inicio predefinida, vaya a **Strobe siren (Sirena estroboscópica)** y haga clic en **Add new preset (Agregar nueva acción predefinida)**.
   2.3. Vaya a **Select strobe siren (Seleccionar una sirena estroboscópica)** y haga clic en **Strobe siren (Sirena estroboscópica)**.
   2.4. Seleccione sirenas estroboscópicas en la lista.
   2.5. Seleccione en la lista el perfil de sirena que ha creado. La acción predefinida se guarda automáticamente
   2.6. Para crear una acción de detención predefinida, haga clic en **Add new preset (Agregar nueva acción predefinida)**.
   2.7. Vaya a **Select strobe siren (Seleccionar una sirena estroboscópica)** y haga clic en **Strobe siren (Sirena estroboscópica)**.
   2.8. En la lista, seleccione las mismas sirenas estroboscópicas que seleccionó para la acción de inicio predefinida.
   2.9. Vaya a **Select action (Seleccionar acción)** y seleccione **Stop (Detener)**.
   2.10. Seleccione el perfil de sirena que creó para la acción de inicio. La acción predefinida se guarda automáticamente
   2.11. Haga clic en **click to refresh (Haga clic para actualizar)** o presione F5 para actualizar la configuración del servidor.
3. Crear una regla:
   3.1. Vaya a **Site Navigation > Rules and Events > Rules (Navegación de instalaciones > Reglas y eventos > Reglas)**.
   3.2. Haga clic con el botón derecho del ratón en **Rules (Reglas)**, seleccione **Add Rule (Añadir regla)** y escriba un nombre.
   3.3. En **Edit the rule description (Editar descripción de regla)**, haga clic en **event (evento)**.
   3.4. Vaya a **Devices > Predefined Events (Dispositivos > Eventos predefinidos)** y seleccione **Motion Started (Se inicia por movimiento)**.
   3.5. En **Edit the rule description (Editar descripción de regla)**, haga clic en **devices/recording_server/management_server**.
   3.6. Seleccione la cámara que debe activar las sirenas estroboscópicas.

3.7. Haga clic en **Next (Siguiente)** hasta llegar a **Step 3: Actions (Paso 3: Acciones)**.

3.8. Seleccione la acción **Axis: Start or stop a profile on a strobe siren: <preset> (Axis: Iniciar o detener un perfil al activarse una sirena estroboscópica: <posición predefinida>)**.

3.9. En **Edit the rule description (Editar descripción de regla)**, haga clic en **preset (posición predefinida)**.

3.10. Seleccione la opción de inicio predefinida que ha creado anteriormente.

3.11. Haga clic en **Next (Siguiente)** y active **Perform stop action on <event> (Realizar acción de detección al <evento>)**.

3.12. Haga clic en **Next (Siguiente)** y seleccione **Axis: Start or stop a profile on strobe siren: <event> (Axis: Iniciar o detener un perfil al activarse una sirena estroboscópica: <evento>)**.

3.13. En **Edit the rule description (Editar descripción de regla)**, haga clic en **preset (posición predefinida)**.

3.14. Seleccione la opción de detección predefinida que ha creado anteriormente.

3.15. Seleccione **Finish (Finalizar)**.

4. Compruebe que las sirenas estroboscópicas funcionan correctamente cuando la cámara detecta movimiento.

Reproduce los clips de audio en altavoces o en una zona de altavoz cuando una cámara detecta movimiento



Mediante el complemento de servidor de eventos, puede configurar reglas personalizadas para automatizar las acciones, los llamados preajustes de acción. En este ejemplo, le mostramos cómo puede reproducir automáticamente un clip de audio en un altavoz de audio o en una zona de altavoz, cuando una cámara detecta movimiento.

Nota

Requisitos

- AXIS Optimizer versión 4.6 o posterior en el servidor de eventos y con Management Client.
- Uno o varios altavoces Axis dedicados o dispositivos Axis con altavoces integrados.
- Para reproducir un clip de audio en una zona de altavoces, es preciso disponer de un sistema AXIS Audio Manager Edge o AXIS Audio Manager Pro con una configuración correcta. Para obtener más información sobre cómo configurar estos sistemas, consulte *Modo de configuración, on page 31*.

1. Cargar un clip de audio:
   1.1. Con el modo AXIS Audio Manager Edge o Legacy, ponga el clip de audio que desee cargar en los altavoces dentro de la carpeta predeterminada **C:\Users\Public\Documents\AXIS Optimizer for Milestone XProtect - Audio Clips**.
   Con el modo AXIS Audio Manager Pro, suba clips de audio la interfaz web de AXIS Audio Manager Pro.

   1.2. En Management Client, vaya a **Site Navigation (Navegación de la instalación)** > **AXIS Optimizer** > **Speaker manager (Gestor de altavoces)** y seleccione un altavoz, un grupo de dispositivos o una zona del altavoz de la lista.

Nota

Para obtener más información sobre cómo seleccionar un modo de gestión de altavoces, consulte los *Modo de configuración, on page 31*.

1.3. Vaya a **Audio clips (Clips de audio)** y haga clic en **+** junto al clip de audio que desea cargar.

1.4. En el modo Legacy, repita los pasos 1.2 y 1.3 para cada altavoz en el que desee reproducir el clip de audio. Asegúrese de cargar el mismo archivo de audio en cada altavoz.

2. Crear preajustes de acción para reproducir un clip de audio en un altavoz o en una zona de altavoz:

2.1. Vaya a **Site Navigation (Navegación de la instalación)** > **Rules and Events (Reglas y eventos)** > **Axis actions (Accesiones Axis)**.

2.2. Para crear una acción de inicio predefinida, vaya a **Audio clips (clips de audio)** y haga clic en **Add new preset (Añadir nueva posición predefinida)**.

2.3. En el modo AXIS Audio Manager Edge o AXIS Audio Manager Pro, vaya a **Select playback destination (Seleccionar destino de reproducción)**.
En el modo Legacy, vaya a **Select speaker (Seleccionar altavoz)**.

2.4. Seleccione un altavoz o una zona de altavoz.

2.5. En la lista, seleccione el clip de audio que haya subido en el paso 1. La acción predefinida se guarda automáticamente

2.6. En el modo AXIS Audio Manager Pro, ir a **Select visual profile (Seleccionar perfil visual)** y configure el perfil visual y el texto.

Nota

Seleccione **Default (Predeterminado)** en la lista de perfiles visuales para utilizar el comportamiento predeterminado de los perfiles visuales en el servidor AXIS Audio Manager Pro cuando se active la acción del clip de audio.

2.7. Haga clic en **refresh (Actualizar)** o presione F5 para actualizar la configuración del servidor.

3. Crear una regla:

3.1. Vaya a**Site Navigation (Navegación de la instalación)** > **Rules and Events (Reglas y eventos)** > **Rules (Reglas)**.

3.2. Haga clic con el botón derecho del ratón en **Rules (Reglas)**, seleccione **Add Rule (Añadir regla)** y escriba un nombre.

3.3. En **Edit the rule description (Editar descripción de regla)**, haga clic en **event (evento)**.

3.4. Vaya a **Devices (Dispositivos)** > **Predefined Events (Eventos predefinidos)** y seleccione **Motion Started (Se inicia por movimiento)**.

3.5. En **Edit the rule description (Editar descripción de regla)**, haga clic en **devices/recording_server/management_server**.

3.6. Seleccione la cámara que debería activar la acción predefinida o el clip de audio.

3.7. Haga clic en **Next (Siguiente)** hasta llegar a **Step 3: Actions (Paso 3: Acciones)**.

3.8. Seleccione la acción **Axis: Play audio clip: <preset> (Axis: reproducir clip de audio: <posición predefinida>)**.

3.9. En **Edit the rule description (Editar descripción de regla)**, haga clic en **preset (posición predefinida)**.

3.10. Seleccione la acción predefinida que ha creado en el paso anterior.

3.11. Seleccione **Finish (Finalizar)**.

4. Compruebe que el clip de audio se reproduce correctamente cuando la cámara detecta movimiento.

Solución de problemas de una regla

Si una regla no funciona, compruebe los mensajes del servidor de eventos para ver si el servicio de eventos está en funcionamiento.

También puede comprobar los registros de AXIS Optimizer en el servidor de eventos. Si el están disponibles Management Client y Smart Client, úselos para habilitar y guardar los registros.

Gestión centralizada de listas de matrículas

Si usa el gestor de listas AXIS Optimizer, puede administrar de forma centralizada las listas de matrículas de todas las cámaras a la vez. Puede crear y gestionar listas de permitidos y bloqueados y listas personalizadas directamente desde el VMS. El sistema admite la combinación de listas. Esto significa que puede tener una lista global que se aplique a todas las cámaras del sistema y listas locales que se apliquen a cámaras específicas.

La gestión centralizada de listas resulta útil, por ejemplo para automatizar la entrada y salida de aparcamientos o para recibir una alarma cuando el sistema registra una matrícula determinada.

Debe ser un administrador para crear y editar listas. Es posible dar derechos de lectura y edición a otros perfiles, consulte la sección *Configurar permisos de las listas, on page 24*.

Crear una lista

Nota

Requisitos

- AXIS License Plate Verifier 1.8 o posterior instalado en las cámaras
- Si quiere crear listas personalizadas, necesita AXIS License Plate Verifier 2.0 o posterior

1. En Management Client, vaya a **Site Navigation > AXIS Optimizer > License plate lists (Navegación de instalaciones > AXIS Optimizer > Listas de matrículas)**.
2. Seleccione las cámaras a las que desea enviar la lista de permitidos, la lista de bloqueados y la lista personalizada.
3. (Opcional) Añada funciones de usuario que pueden ver y editar la lista de permitidos, la lista de bloqueados y las listas personalizadas.
4. Agregue matrículas a la lista de permitidos o bloqueados y la lista personalizada.
   También puede importar las listas de matrículas existentes.
   Cuando la lista presenta el estado de **Synchronized (Sincronizada)**, se ha transmitido a las cámaras que ha seleccionado.

Configurar permisos de las listas

Puede configurar qué perfiles de usuario pueden editar las listas de permitidos y bloqueados y la lista personalizada. Esto es útil, por ejemplo, cuando el administrador ha configurado las listas pero usted quiere que el operador añada visitantes en función de las necesidades diarias.

En Management Client

Todos los permisos para ver y editar listas se pueden seleccionar individualmente para cada lista.

1. Vaya a **Security > Roles (Seguridad > Funciones)** y seleccione una función.
2. Vaya a la pestaña **AXIS Optimizer**.
3. Vaya a **Role settings (Configuración de roles)** > **AXIS Optimizer (Optimizador AXIS)** > **License plate lists (Listas de matrículas)**.
4. Seleccione **Read (Leer)** en el campo **License plate lists (Listas de matrículas) (nodo)**.
5. Seleccione una lista en **License plate lists (Listas de matrículas)** y seleccione **Edit License plates (Editar matrículas)**.
   - En versiones anteriores a XProtect 2023 R2, vaya a **MIP > AXIS Optimizer > AXIS Optimizer Security > License lists (MIP > AXIS Optimizer > Seguridad de AXIS Optimizer > Listas de matrículas)** y seleccione **Edit license plate lists (Editar listas de matrículas)**.

Edición de una lista

En Management Client

1. Vaya a **Site Navigation > AXIS Optimizer > License plates (Navegación de instalaciones > AXIS Optimizer > Matrículas)**.
2. Seleccione la instalación que quiera editar.
3. Actualice las **Cameras (cámaras)** o **License plates (matrículas)** según sea necesario.
   Cuando la lista presenta el estado **Synchronized (Sincronizada)**, los cambios se han transferido a las cámaras seleccionadas.

En Smart Client

1. Vaya a *Matrículas de Axis, on page 59* y haga clic en **Listas de matrículas**.
   Si no aparece en la pestaña, vaya a **Settings > Axis search options (Configuración > Opciones de búsqueda de Axis)** y seleccione **Show license plate search tab (Mostrar la pestaña de búsqueda de matrículas)**.
2. Seleccione la instalación que quiera editar.
3. Agregue matrículas a la lista de permitidos o bloqueados y la lista personalizada.
   También puede importar listas de matrículas existentes.
   Cuando la lista presenta el estado de **Synchronized (Sincronizada)**, se ha transmitido a las cámaras que ha seleccionado.

Importación de una lista

Puede importar listas en varios formatos de texto o CSV.

- Formatos de texto permitido: una matrícula por línea
- Formatos CSV permitidos:
  - una matrícula por línea
  - Dos campos: matrícula y fecha
  - Tres campos: matrícula, propietario y comentarios
  - Cuatro campos: matrícula, propietario, comentarios y el texto "Activo" o "Inactivo". (El mismo formato que cuando se exporta una lista).

En Management Client

1. Vaya a **Site Navigation > AXIS Optimizer > License plates (Navegación de instalaciones > AXIS Optimizer > Matrículas)**.
2. Seleccione la instalación que quiera editar.
3. Vaya a **Allowed (Permitido)**, **Blocked (Bloqueado)** o **Custom (Personalizado)**.
4. Haga clic en ⋮ y active **Import to allow list (Importar en lista de permitidos)**, **Import to block list (Importar en lista de bloqueados)** o **Import to custom list (Importar en lista personalizada)**.
5. En el cuadro de diálogo **Reset list (Restablecer lista)**:
   - Haga clic en **Yes (Sí)** para eliminar todas las matrículas existentes y agregar a la lista solo las matrículas importadas recientemente.
   - Haga clic en **No** para fusionar las nuevas matrículas importadas con las matrículas existentes en la lista.

En Smart Client

1. Vaya a *Matrículas de Axis, on page 59* y haga clic en **Listas de matrículas**.
   Si no aparece en la pestaña, vaya a **Settings > Axis search options (Configuración > Opciones de búsqueda de Axis)** y seleccione **Show license plate search tab (Mostrar la pestaña de búsqueda de matrículas)**.
2. Seleccione la instalación que quiera editar.
3. Vaya a **Allowed (Permitido)**, **Blocked (Bloqueado)** o **Custom (Personalizado)**.

4. Haga clic en ⋮ y active **Import to allow list (Importar en lista de permitidos)**, **Import to block list (Importar en lista de bloqueados)** o **Import to custom list (Importar en lista personalizada)**.
5. En el cuadro de diálogo **Reset list (Restablecer lista)**:
   - Haga clic en **Yes (Sí)** para eliminar todas las matrículas existentes y agregar a la lista solo las matrículas importadas recientemente.
   - Haga clic en **No** para fusionar las nuevas matrículas importadas con las matrículas existentes en la lista.

Exportación de una lista

Nota

Para exportar listas de matrículas, debe tener derechos de administrador.

En Management Client

1. Vaya a **Site Navigation > AXIS Optimizer > License plates (Navegación de instalaciones > AXIS Optimizer > Matrículas)**.
2. Seleccione la instalación que quiera editar.
3. Vaya a **Allowed (Permitido)**, **Blocked (Bloqueado)** o **Custom (Personalizado)**.
4. Haga clic en ⋮ y seleccione **Export allow list (Exportar lista de permitidos)**, **Export block list (Exportar lista de bloqueados** o **Export custom list (Exportar lista personalizada)**.
   La lista exportada se encuentra en formato CSV con cuatro campos: matrícula, propietario, comentarios y estado "Activo" o "Inactivo".

En Smart Client

1. Vaya a *Matrículas de Axis, on page 59* y haga clic en **Listas de matrículas**.
   Si no aparece en la pestaña, vaya a **Settings > Axis search options (Configuración > Opciones de búsqueda de Axis)** y seleccione **Show license plate search tab (Mostrar la pestaña de búsqueda de matrículas)**.
2. Seleccione la instalación que quiera editar.
3. Vaya a **Allowed (Permitido)**, **Blocked (Bloqueado)** o **Custom (Personalizado)**.
4. Haga clic en ⋮ y seleccione **Export allow list (Exportar lista de permitidos)**, **Export block list (Exportar lista de bloqueados** o **Export custom list (Exportar lista personalizada)**.
   La lista exportada se encuentra en formato CSV con cuatro campos: matrícula, propietario, comentarios y estado "Activo" o "Inactivo".

Más información sobre las listas

- Puede crear varias instalaciones.
- Cada instalación se asocia a una o varias cámaras que tienen instalado AXIS License Plate Verifier.
- Cada instalación se asocia a una o varias funciones de usuario del VMS. La función de usuario define quién tiene permiso para leer y editar las listas de matrículas.
- Todas las listas se guardan en la base de datos del VMS.
- Al agregar la cámara a una instalación, se sobrescriben las matrículas ya existentes en la cámara.
- Si la misma cámara está presente en varias instalaciones, la cámara recibirá la suma de todas las listas.
- Si la misma matrícula está en varias listas, la de bloqueados tiene la mayor prioridad, la de permitidos tiene prioridad media y personalizada la más baja.
- Para cada matrícula, puede agregar información sobre el propietario del vehículo. Sin embargo, esta información no está sincronizada con las cámaras.

Responder a eventos en directo

Usar los controles de dispositivo

Controles del operador

Los controles del operador dan acceso a las características concretas de una cámara Axis directamente desde Smart Client. Las funciones a las que tiene acceso dependen de las cámaras de su sistema y de las características que presentan. Además de los controles de operador preinstalados, es posible crear otros personalizados. También puede configurar a qué controles tiene acceso un operador.

Algunos ejemplos de los controles de operador son:

- Encendido o apagado de las escobillas de limpieza
- Encendido o apagado del calefactor
- Encendido o apagado de IR
- Recuerdo de enfoque
- Encendido o apagado de WDR
- Encendido o apagado de la estabilización electrónica de imagen (EIS)
- Encendido o apagado de las máscaras de privacidad.

Para obtener más información sobre los controles específicos del operador de su cámara, consulte la hoja de datos.

Acceso a los controles de operador

Nota

Requisitos

- Dispositivos Axis con AXIS OS 7.10, 7.40 o posterior. (Las versiones 7.20 y 7.30 no son compatibles con los controles del operador).

1. En Smart Client, haga clic en **Live (En directo)** y vaya a la cámara Axis.
2. Haga clic en y seleccione la función que desea utilizar.

Guarde un área de enfoque para una cámara PTZ

La función de recuerdo de enfoque le permite guardar áreas de enfoque a las que la cámara PTZ vuelve automáticamente cuando se desplaza hacia esa zona de la escena. Esto es especialmente útil en condiciones de poca luz, cuando la cámara puede tener problemas para encontrar el enfoque correcto.



1. En Smart Client, mueva la cámara hacia la zona que desea enfocar.

Nota

Las condiciones de luz deben ser buenas cuando se ajusta el área de enfoque.

2. Enfoque de la cámara.
3. Seleccione **Add Focus Recall Zone (Añadir área de recuerdo de enfoque)**.

Más tarde, al desplazar o inclinar la cámara y mover la vista a un área determinada, la cámara recupera automáticamente el enfoque preestablecido para dicha vista. La cámara va a mantener la misma posición de enfoque aunque se acerque o se aleje el zoom.

Si la zona no está configurada correctamente, seleccione **Remove Focus Recall Zone (Eliminar área de recuerdo de enfoque)**.

Enfoque automático de la cámara



Las cámaras con enfoque automático pueden ajustar el objetivo de forma mecánica y automática para que la imagen permanezca focalizada en el área de interés cuando cambia la vista.

Enfoque automático en cámaras PTZ

1. En Smart Client, seleccione la vista de una cámara.
2. Haga clic en y vaya a **Set Focus > AF (Ajustar enfoque > AF)**.
   Focus Control (Control de enfoque) permite acercar o alejar el punto de enfoque:
   - Para un paso grande, haga clic en la barra grande.
   - Para un paso pequeño, haga clic en la barra pequeña.

Cámaras de caja fija y domo fijo con enfoque automático

1. En Smart Client, seleccione la vista de una cámara.
2. Haga clic en y vaya a **Autofocus (Enfoque automático)**.

Activación de Speed Dry o de las escobillas de limpieza



La función Speed Dry permite que el domo vibre a alta frecuencia al mojarse. Cuando el domo vibra a alta frecuencia, la tensión superficial del agua se rompe y elimina las gotas. Esto permite que la cámara ofrezca imágenes nítidas incluso con tiempo lluvioso.

Para activar la función Speed Dry

1. En Smart Client, seleccione la vista de una cámara.
2. Haga clic en y vaya a **PTZ > Speed Dry**.

Importante

La función Speed Dry solo está disponible en las cámaras de la serie AXIS Q61.

Activación de la función de limpieza con escobillas

Las escobillas eliminan el exceso de agua y lluvia del objetivo de las cámaras de posicionamiento Axis.

1. En Smart Client, seleccione la vista de una cámara.

2. Haga clic en .

Importante

La función de limpieza mediante escobillas solo está disponible en las cámaras de la serie AXIS Q86.

Medir la temperatura de un punto



Si dispone de una cámara integrada con lectura de temperatura localizada en el sistema, puede medir la temperatura directamente en la vista de cámara. Las cámaras AXIS con lectura de temperatura localizada son la AXIS Q1961-TE, AXIS Q2101-E y AXIS Q2901-E.

1. En Smart Client, abra una vista de cámara en una cámara integrada con lectura de temperatura localizada.
2. Para medir la temperatura localizada, haga clic en y seleccione:
   - **Medición puntual de la temperatura** para AXIS Q2901-E.
   - **Enable temperature spot meter (Habilitar medidor puntual de temperatura)** para AXIS Q1961-TE y AXIS Q2101-E.
3. Haga clic en cualquier área de la vista y verá la temperatura puntual actual.
   Para Q1961-TE y AXIS Q2101-E, haga clic en **Done (Hecho)**.
4. Para AXIS Q1961-TE y AXIS Q2101-E, la temperatura puntual permanecerá en la imagen hasta que se desactive:
   - Seleccione > **Disable temperature spot meter (Desactivar el medidor de temperatura puntual)**.

Nota

Si se utiliza un zoom digital, las mediciones de temperatura pueden dar resultados incorrectos.

Amplía y sigue automáticamente un objeto en movimiento

Autotracking

Gracias al autotracking, la cámara hace zoom automáticamente en los objetos en movimiento y los sigue. Por ejemplo, puede tratarse de un vehículo o una persona. El objeto cuyo seguimiento se quiere hacer se puede seleccionar manualmente. También se pueden crear áreas de activación para que la cámara detecte los objetos en movimiento. Cuando la cámara no sigue a un objeto, vuelve a su posición de inicio después de 5 segundos.

- Configure las áreas de activación en la interfaz web de la cámara PTZ.
- En Smart Client puede ver lo siguiente:
  - Recuadro rojo: el objeto de seguimiento.
  - Zonas azules: objetos que no se rastrean, pero que pueden seguirse si acceden a una zona de activación o se hace clic con el botón derecho.

Configuración de autotracking

Nota

Requisitos

- AXIS OS 12.0
- Cámaras Axis compatibles con Autotracking 2, como la AXIS Q6075 PTZ Dome Network Camera

1. Compruebe que la cámara y los dispositivos de metadatos están habilitados.
2. Seleccione Metadatos 1 en su cámara y haga clic en **Settings (Configuración)**.
3. Vaya a **Metadata stream > Event data (Flujo de metadatos > Datos de eventos)** y seleccione **Yes (Sí)**.
4. Haga clic en **Save (Guardar)**.
5. Configure Autotracking en la interfaz web de la cámara PTZ.

Encender o apagar autotracking

1. En Smart Client, haga clic en .
2. Seleccione **Turn on autotracking (Encender autotracking)** o **Turn off autotracking (Apagar autotracking)**.

Nota

Si hay varias opciones para activar o desactivar el autotracking, utilice la última de la lista.

Iniciar autotracking manualmente

Si se pasa el ratón por encima de un objeto, se rellena la superposición. Al hacer clic con el botón derecho del ratón sobre un objeto, este se convierte en un objetivo y la cámara comienza a seguirlo. La cámara se restablece después de 5 segundos si el objeto ya no se puede seguir.

Al hacer clic con el botón derecho fuera de los cuadros azules, se detiene el autotracking.

Crear controles de operador personalizados

1. En Management Client, vaya a **Site Navigation > AXIS Optimizer > Operator controls (Navegación de instalaciones > AXIS Optimizer > Controles de operador)**.
2. Seleccione un dispositivo o un grupo de dispositivos.
3. Haga clic en **Add new control (Añadir nuevo control)**.
4. Introduzca un **Nombre** y una **Descripción**.
5. Seleccione **Administrator (Administrador)** si desea que el control del operador solo esté disponible para usuarios con derechos de administrador.
6. Agregue la URL de VAPIX para el control específico.
   Ejemplo: Para añadir un control de Defog (Desempañado) en el control del operador, introduzca esta URL: `/axis-cgi/param.cgi?action=update&imageSource.IO.Sensor.Defog=on`.
   Para obtener más información sobre las API de dispositivos de red de Axis, consulte la .
7. Vaya a Smart Client y compruebe que el control del operador funciona de la forma esperada.

Configuración del acceso a los controles del operador

Puede determinar los controles de operador a los que tiene acceso un operador en Smart Client.

1. En Management Client, vaya a **Site Navigation > AXIS Optimizer > Operator controls (Navegación de instalaciones > AXIS Optimizer > Controles de operador)**.
2. Seleccione un dispositivo o un grupo de dispositivos.
3. Seleccione los controles de operador a los que quiere que los operadores tengan acceso en Smart Client.

Interactúe a través de los altavoces

Gestor de altavoces

El gestor de altavoces integra los productos de audio de Axis en VMS para que disponga de todas las funciones de sus dispositivos Axis.

- Acceder a los altavoces vinculados a la cámara

Conectar las cámaras a altavoces y acceder a ellos desde la visualización en directo. Ya no es necesario encontrar los altavoces manualmente.

- Enviar audio a un grupo de altavoces
  Envíe audio a muchos altavoces con un solo clic.
- Gestión de fragmentos de audio
  Podrá gestionar fácilmente sus clips de audio.
- Interactuar inmediatamente con sus interlocutores
  Responda rápidamente a una alarma sin salir del gestor de alarmas.
- Sincronizar audio entre altavoces
  Si desea utilizar su sistema de audio como hilo musical, el gestor de altavoces puede ayudarle a configurar zonas para sincronizar el audio entre los altavoces (solo en los modos AXIS Audio Manager Pro y Edge).

Modos

El gestor de altavoces admite tres modos diferentes para distintos tipos de configuraciones de altavoces.

- **Pro** para los sistemas AXIS Audio Manager Pro
  Una solución de software integral diseñada para sistemas de megafonía a gran escala o avanzados. Admite hasta más de 5 000 altavoces y más de 500 zonas, y ofrece opciones flexibles de licencia e instalación. Se recomienda para sistemas de mayor tamaño o usuarios con necesidades de programación más avanzadas.
- **Edge** para los sistemas AXIS Audio Manager Edge
  Una solución de software optimizada que gestiona hasta 200 altavoces en 20 zonas. Está integrada directamente en los altavoces de red Axis y no requiere servidores ni licencias adicionales. Se recomienda para sistemas más pequeños que no requieren programación avanzada.
- **Heredado**
  El modo clásico utiliza la integración nativa de altavoces para transmitir audio a un grupo de altavoces o activar clips de audio. No admite la transmisión sincronizada. Se recomienda para sistemas con altavoces individuales y sin necesidad de transmisión sincronizada.

Modo de configuración

La primera vez que acceda a esta página se le pedirá seleccionar un modo, pero puede cambiar de modo en cualquier momento. La configuración que realice en cada modo es independiente, pero se conserva al alternar entre modos.

1. Vaya a **Site Navigation (Navegación del sitio)** > **AXIS Optimizer** > **Speaker manager (Gestor de altavoces)**.
2. En **Mode (Modo)**, haga clic en el modo actual y seleccione el modo deseado en la ventana emergente.
3. Haga clic en **Switch mode (Cambiar modo)**.

Modo de AXIS Audio Manager Pro

Para usar este modo:

- Instale el software AXIS Audio Manager Pro en un servidor, por ejemplo, un servidor de grabación.
- Adquiera la licencia y configure AXIS Audio Manager Pro con acceso a la API.
- Opcional: configure un certificado de servidor para la interfaz web; consulte *Certificates (Certificados)*.
- Si AXIS Audio Manager Pro está instalado en un servidor VMS, cambie el puerto del servidor al puerto 443.

Este modo no requiere añadir ni obtener licencias de altavoces en el VMS, pero se creará automáticamente un hardware para la conexión al servidor AXIS Audio Manager Pro (se requiere una licencia de dispositivo VMS). Para obtener más información sobre AXIS Audio Manager Pro, consulte el *AXIS Audio Manager Pro user manual (manual de usuario de AXIS Audio Manager Pro)*.

Nota

El modo AXIS Audio Manager Pro está limitado a la compatibilidad con un único sitio local. Las arquitecturas de múltiples sitios, federadas e interconectadas quedan fuera del alcance de esta integración.

Conéctese a un servidor AXIS Audio Manager Pro en modo Pro

1. En Management Client, vaya a **Site Navigation (Navegación del sitio)** > **AXIS Optimizer Speaker manager (Gestor de altavoces)**.
2. Haga clic en **Connect (Conectar)**.
3. En el cuadro de diálogo:
   - Seleccione el servidor de grabación al que desee añadir el hardware del servidor AXIS Audio Manager Pro .
   - Introduzca la dirección y el puerto HTTPS del servidor AXIS Audio Manager Pro.
   - Introduzca el nombre de usuario y la contraseña de la API (el acceso a la API debe estar habilitado en el servidor AXIS Audio Manager Pro).
   - Haga clic en **Connect (Conectar)**.

En AXIS Audio Manager Pro, puede ver todos los destinos y zonas disponibles en el lado izquierdo. Cuando haga clic en **Servidor AXIS Audio Manager Pro**, el lado derecho mostrará la interfaz web de AXIS Audio Manager Pro.

Nota

Para acceder a la interfaz web, necesita una conexión directa entre el equipo del Management Client y el servidor AXIS Audio Manager Pro.

Si cambia algo en las zonas, los destinos, los clips de audio o los perfiles visuales en la interfaz web de AXIS Audio Manager Pro:

- Vaya a **Site Navigation (Navegación del sitio)** > **AXIS Optimizer** > **Speaker manager (Gestor de altavoces)**.
- Haga clic en **Update (Actualizar)**

Vinculación de una cámara a un destino o una zona

Puede asociar una cámara a un destino o zona específicos y utilizarlas directamente en la vista de cámara de Smart Client.

1. En Management Client, vaya a **Site Navigation (Navegación del sitio)** > **AXIS Optimizer** > **Speaker manager (Gestor de altavoces)** y seleccione un destino o una zona.
2. En **Associated camera(s) (Cámara(s) asociada(s))**, haga clic en **Add cameras... (Añadir cámaras)** y seleccione las cámaras que desea asociar al destino o la zona.

Cuando una cámara está asociada a un destino o una zona, la barra de herramientas de la vista de cámara de Smart Client muestra .

Crear perfiles visuales

- En Management Client, vaya a **Site Navigation (Navegación de la instalación)** > **AXIS Optimizer Speaker manager (Gestor de altavoces)**.
- Haga clic en **el servidor Audio Manager Pro** para acceder a la interfaz web.
- Haga clic en **Visual profiles (Perfiles visuales)** para crear o editar perfiles visuales.

Para obtener más información sobre los perfiles visuales, consulte *el manual del usuario de AXIS Audio Manager Pro*.

Modo de AXIS Audio Manager Edge

AXIS Audio Manager Edge viene preinstalado en la mayoría de los altavoces Axis y se detecta automáticamente al seleccionar este modo. Es necesario añadir al VMS los líderes de las instalaciones, los dispositivos intermediarios para la fuente de megafonía y altavoces independientes para que el modo de AXIS Audio Manager Edge funcione correctamente.

Nota

En el modo AXIS Audio Manager Edge no se pueden utilizar salidas de audio integradas en cámaras ni otros dispositivos de audio que no sean compatibles.

Para obtener más información sobre AXIS Audio Manager Edge, consulte el *AXIS Audio Manager Edge user manual (manual de usuario de AXIS Audio Manager Edge)*.

Configurar altavoces y zonas en el modo de AXIS Audio Manager Edge

Para reproducir clips de audio y hablar en directo, primero debe encender la megafonía de las zonas.

1. En Management Client, vaya a **Site Navigation (Navegación del sitio)** > **Devices (Dispositivos)** > **Speakers (Altavoces)** y añada grupos de dispositivos o añada y elimine altavoces de los grupos de dispositivos.
2. Vaya a **Site Navigation (Navegación del sitio)** > **AXIS Optimizer** > **Speaker manager (Gestor de altavoces)** y asegúrese de seleccionar el modo **Edge** .
   A continuación, el gestor de altavoces buscará todos los altavoces del sistema del VMS y mostrará todas las instalaciones y zonas de AXIS Audio Manager Edge que se pueden utilizar en Smart Client.
3. En la lista de instalaciones, seleccione una zona con la megafonía desactivada.
4. Seleccione **Turn on paging for the zone (Encender megafonía para la zona)**.

Si realiza algún cambio en las zonas o en las fuentes de megafonía:

5. Vaya a **Site Navigation (Navegación del sitio)** > **AXIS Optimizer** > **Speaker manager (Gestor de altavoces)**.
6. Haga clic en **Update (Actualizar)**

Nota

Si la configuración no es correcta, compruebe la configuración de AXIS Audio Manager Edge e inténtelo de nuevo.



Vinculación de una cámara a un altavoz o a una zona

Para usar un altavoz o una zona directamente en la vista de cámara de Smart Client puede asociarlos a una cámara.

1. En Management Client, vaya a **Site Navigation (Navegación del sitio)** > **AXIS Optimizer** > **Speaker manager (Gestor de altavoces)** y seleccione un altavoz o una zona.
2. En la ventana **Associated cameras (Cámaras asociadas)**, haga clic en **+Add cameras (Añadir cámaras)** y seleccione las cámaras a las que desea asociar el altavoz o la zona.

Cuando una cámara está asociada a un altavoz, un grupo de dispositivos o una zona, la barra de herramientas de la vista de cámara de Smart Client muestra .

Cargar clips de audio en altavoces

Para reproducir clips de audio en un altavoz o zona desde Smart Client, primero debe cargar los en los altavoces en Management Client.

1. Ponga los clips de audio que desee cargar en los altavoces dentro de la carpeta predeterminada **C:\Users\Public\Documents\AXIS Optimizer for Milestone XProtect - Audio Clips**.
2. En Management Client, vaya a **Site Navigation (Navegación del sitio)** > **AXIS Optimizer** > **Speaker manager (Gestor de altavoces)** y seleccione un altavoz o una zona.
3. Vaya a **Audio clips (Clips de audio)** y haga clic en **+** junto a los clips que desea cargar en los altavoces.

Modo clásico

El modo Legacy amplía la funcionalidad nativa de sus altavoces Axis y de otros dispositivos Axis con capacidad de audio que se hayan añadido al VMS. A diferencia de los demás modos, el modo Legacy no admite la transmisión sincronizada a varios altavoces.

Configurar altavoces en modo clásico

1. En Management Client, vaya a **Site Navigation (Navegación del sitio)** > **Devices (Dispositivos)** > **Speakers (Altavoces)** y añada grupos de dispositivos o añada y elimine altavoces de los grupos de dispositivos.
2. Vaya a **Site Navigation (Navegación del sitio)** > **AXIS Optimizer** > **Speaker manager (Gestor de altavoces)** y asegúrese de seleccionar el modo clásico.
3. Haga clic en .
   3.1. En la ventana **Manage Side Panel (Panel lateral de gestión)**, seleccione los altavoces que quiera mostrar en Smart Client.
   3.2. Haga clic en **Add (Agregar)** y en **OK**.
   Los altavoces del panel **Visible (Visibles)** se muestran ahora en Smart Client para todos los usuarios que tengan acceso al altavoz.
4. Para eliminar altavoces:
   4.1. Vaya a **Site Navigation (Navegación del sitio)** > **AXIS Optimizer** > **Speaker manager (Gestor de altavoces)** y haga clic en .
   4.2. En la ventana **Manage Side Panel (Panel lateral de gestión)**, seleccione los altavoces que quiera eliminar.
   4.3. Haga clic en **Remove (Eliminar)** y en **OK (Aceptar)**.

Vinculación de una cámara a un altavoz o grupo de altavoces

Puede asociar una cámara a un destino o zona específicos y utilizarlas directamente en la vista de cámara de Smart Client.

1. En Management Client, vaya a **Site Navigation (Navegación del sitio)** > **AXIS Optimizer** > **Speaker manager (Gestor de altavoces)** y seleccione un altavoz o grupo de altavoces.
2. En **Associated camera(s) (Cámara(s) asociada(s))**, haga clic en **Add cameras... (Añadir cámaras)** y seleccione las cámaras que desea asociar al altavoz o grupo de altavoces.

Cuando una cámara está asociada a un altavoz o grupo de altavoces, la barra de herramientas de la vista de cámara de Smart Client muestra .

Cargar clips de audio en altavoces

Para reproducir clips de audio en un altavoz o zona desde Smart Client, primero debe cargar los en los altavoces en Management Client.

1. Ponga los clips de audio que desee cargar en los altavoces dentro de la carpeta predeterminada **C:\Users\Public\Documents\AXIS Optimizer for Milestone XProtect - Audio Clips**.
2. En Management Client, vaya a **Site Navigation (Navegación del sitio)** > **AXIS Optimizer** > **Speaker manager (Gestor de altavoces)** y seleccione un altavoz o grupo de altavoces.
3. Vaya a **Audio clips (Clips de audio)** y haga clic en **+** junto a los clips que desea cargar en los altavoces.



Cambiar el volumen

Para cambiar el volumen de los altavoces:

1. En Management Client, vaya a **Site Navigation (Navegación del sitio) > Speaker manager (Gestor de altavoces)** y seleccione un altavoz o grupo de altavoces.
2. Vaya a **Volume (Volumen)** y ajuste al volumen deseado.



Reproducir audio en altavoces

1. En Smart Client, vaya a **Live (En directo)** > **MIP plug-ins (Complementos de MIP)** > **Axis speaker control (Control de altavoces Axis)** y seleccione un altavoz o una zona en la lista desplegable.
2. Permita que el micrófono envíe audio al altavoz:
   2.1. Mantenga pulsado a la vez que habla.
   Compruebe que en el indicador de nivel del micrófono se indica que hay actividad de voz.
3. Reproduzca un clip de audio en el altavoz:
   3.1. Vaya a **Media clip (Fragmentos de medios)** y seleccione un fragmento de audio de la lista desplegable.
   3.2. Para comenzar a reproducir el fragmento de audio en el altavoz seleccionado, haga clic en Reproducir.

Reproducir audio en altavoces en la vista de la cámara

1. En Smart Client, vaya a una vista de cámara.
2. Si hay una asociación con un altavoz, grupo de dispositivos o zona, se ve en la barra de herramientas.
3. Haga clic en para abrir la ventana **Axis speaker control (Control de altavoz de Axis)**.
4. Permita que el micrófono envíe audio al altavoz:
   4.1. Mantenga pulsado a la vez que habla.
   Compruebe que en el indicador de nivel del micrófono se indica que hay actividad de voz.

5. Reproduzca un clip de audio en el altavoz:
   5.1. Vaya a **Media clip (Fragmentos de medios)** y seleccione un fragmento de audio de la lista desplegable.
   5.2. Para comenzar a reproducir el fragmento de audio en el altavoz seleccionado, haga clic en Reproducir.

Reproducir audio en los altavoces de las alarmas

1. En Smart Client, vaya a **Alarms (Alarmas)**.
2. Seleccione una alarma que tenga una cámara como fuente.
   Si existe una asignación a un altavoz o una zona, aparecerán los controles del altavoz.
3. Permita que el micrófono envíe audio al altavoz:
   – Mantenga pulsado a la vez que habla.
   Compruebe que en el indicador de nivel del micrófono se indica que hay actividad de voz.
4. Reproduzca un clip de audio en el altavoz:
   – Vaya a **Media clip (Fragmentos de medios)** y seleccione un fragmento de audio de la lista desplegable.
   – Para comenzar a reproducir el fragmento de audio en el altavoz seleccionado, haga clic en Reproducir.

Ajustar el comportamiento visual para la interacción con el altavoz

En Smart Client, puede configurar el comportamiento visual de su dispositivo en el control de altavoces de Axis, directamente en la vista de la cámara o en el Gestor de alarmas.

Nota

Los perfiles visuales solo son compatibles con el modo AXIS Audio Manager Pro.

- En el panel lateral **Axis speaker control (Control de altavoces Axis)**:
  – Haga clic en .
  – Seleccione un perfil visual de la lista desplegable.
  – Escriba en el cuadro de texto si desea sustituir los textos actuales asociados al perfil visual seleccionado.
- En la vista de la cámara:
  – Vaya a la vista de una cámara específica.
  – Si hay una asociación con un altavoz, grupo de dispositivos o zona, se ve en la barra de herramientas.
  – Haga clic en para abrir la ventana **Axis speaker control (Control de altavoz de Axis)**.
  – Haga clic en .
- En el **Alarm Manager (Gestor de alarmas)**:
  – Seleccione un evento, vaya a la vista de la cámara y haga clic en .

Marcadores de clips de audio en la vista de la cámara o alarmas

Cuando reproduce un clip de audio desde los controles del altavoz en una vista de cámara o en Alarms (Alarmas), se crea un marcador con información sobre quién y qué dispositivo reprodujo el clip de audio.

Para buscar marcadores de clips de audio:

1. En Smart Client, vaya a **Search (Buscar)**.

2. Seleccione un intervalo de tiempo y una o varias cámaras.
3. Haga clic en **Search for (Buscar)** > **Bookmarks (Marcadores)** > **New search (Nueva búsqueda)**.

Gestión de visitantes

Complemento de intercomunicación

Los intercomunicadores en red de Axis combinan la comunicación, la videovigilancia y el control remoto de la entrada en un solo dispositivo. AXIS Optimizer facilita la configuración y el uso de intercomunicadores Axis junto con el VMS. Por ejemplo, puede recibir llamadas y abrir puertas.

Configuración de un intercomunicador



El bloqueo de la puerta debe conectarse normalmente al primer relé del intercomunicador. AXIS Optimizer determina qué puerto de salida se debe utilizar en función de la información de **Usage (Uso)**. Se utiliza el primer puerto que tenga **Usage = Door (Uso = Puerta)** (RELAY1 de forma predeterminada).

Nota

Requisitos

- Un intercomunicador Axis
- Un micrófono instalado en el PC que recibe las llamadas
- Smart Client listo y en funcionamiento

Nota

A partir de la versión 5.0.X.X, AXIS Optimizer configura los intercomunicadores en el VMS mediante un método de configuración distinto al de versiones anteriores. El dispositivo de metadatos puede utilizarse para la detección de llamadas en lugar de utilizar la entrada 1. Seguimos admitiendo el método de configuración antiguo, pero recomendamos el nuevo método de configuración para las nuevas instalaciones.

1. Instale la versión más reciente de AXIS Optimizer en cada cliente desde el que desee recibir llamadas y controlar la puerta.
2. Inicie sesión en Management Client.
3. Agregue el intercomunicador Axis al servidor de grabación.
4. En Management Client, habilite todos los dispositivos que necesite. Para poder recibir llamadas, en Smart Client necesita:
   - Cámara 1
   - Micrófono
   - Altavoz
   - Metadatos
   - Entrada 2 (opcional si tiene un relé de seguridad conectado al intercomunicador en el puerto 2)
   - Salida conectada a la puerta. Si sabe qué salida está conectada a la puerta, selecciónela. Si no, seleccione todas las salidas.
5. Vaya a **Site Navigation > Devices > Metadata (Navegación de instalaciones > Dispositivos > Metadatos)** para seleccionar el dispositivo de metadatos para el intercomunicador que está instalando.
6. Haga clic en **Settings (Ajustes)**.

7. Configure **Event data (Datos del evento)** en **Yes (Sí)**.
8. Haga clic en **Save (Guardar)**.
9. Si ha activado la Entrada 2, también debe configurarla.
   9.1. Vaya a **Site Navigation > Devices > Input (Navegación de instalaciones > Dispositivos > Entrada)** y seleccione la entrada 2.
   9.2. Haga clic en **Events (Eventos)** y, a continuación, en **Add (Agregar)**.
   9.3. Seleccione **Input Falling event (Evento de bajada de entrada)** y añádalo a las entradas habilitadas. Repítalo para **Input Rising event (Evento de subida de entrada)**.
   9.4. Haga clic en **Save (Guardar)**.
10. Para configurar permisos para roles determinados, consulte *Configuración de permisos para intercomunicador, on page 38*.
11. *Realizar una llamada de prueba, on page 39*.

Configuración de permisos para intercomunicador

Para gestionar llamadas es necesario habilitar los permisos.

1. Vaya a **Site Navigation > Security > Roles (Navegación de instalaciones > Seguridad > Funciones)**.
2. Elija una función.
3. Vaya a **Overall Security (Seguridad general)**.
4. Asegúrese de que los permisos necesarios para cada grupo de seguridad están establecidos. Vaya a **Hardware** y seleccione **Driver commands (Comandos de controlador)**.
5. Para definir permisos en el nivel del sistema, vaya **Overall Security (Seguridad general)**.
   Para definir permisos en el nivel del dispositivo, vaya a **Device (Dispositivo)**.
6. Configuración de permisos para los grupos de seguridad:
   6.1. Vaya a **Cameras (Cámaras)**. Seleccione **Read (Leer)** y **View live (Visualización en directo)**.
   6.2. Vaya a **Microphones (Micrófonos)**. Seleccione **Read (Leer)** y **Listen (Escuchar)**.
   6.3. Para obtener información sobre la **Overall Security (Seguridad general)**, vaya a **Speakers (Altavoces)**. Seleccione **Read (Leer)** y **Speak (Hablar)**.
   En **Device (Dispositivo)**, vaya a **Speakers (Altavoces)** y seleccione **Read (Leer)**. A continuación, vaya a la pestaña **Speech (Voz)** y seleccione **Speak (Hablar)**.
   6.4. Vaya a **Metadata (Metadatos)**. Seleccione **Read (Lectura)** y **Live (Directo)**.
   6.5. Vaya a **Input (Entrada)**. Seleccione **Read (Lectura)**.
   6.6. Vaya a **Output (Salida)**. Seleccione **Read (Lectura)** y seleccione **Activate (Activar)**.

Para asignar permisos para controlar qué operadores gestionan las llamadas desde un intercomunicador determinado:

1. Seleccione el permiso **Read (Lectura)** para el dispositivo de metadatos 1 del intercomunicador concreto.
2. Borre este permiso para las demás funciones. Los usuarios que no tienen permiso no podrán recibir llamadas.

Para ver el historial de llamadas, se necesitan permisos adicionales.

1. Para definir permisos en el nivel del sistema, vaya **Overall Security (Seguridad general)**.
   Para definir permisos en el nivel del dispositivo, vaya a **Device (Dispositivo)**.
2. Seleccione estos permisos para los grupos de seguridad:
   2.1. Vaya a **Cameras (Cámaras)**. Seleccione **Playback (Reproducción)** y **Read sequences (Lectura de secuencias)**.
   2.2. Vaya a **Microphones (Micrófonos)**. Seleccione **Playback (Reproducción)** y **Read sequences (Lectura de secuencias)**.

2.3. Vaya a **Speakers (Altavoces)**. Seleccione **Listen (Escuchar)**, **Playback (Reproducir)** y **Read sequences (Lectura de secuencias)**.

Realizar una llamada de prueba

1. En Smart Client, vaya a **Settings > Axis intercom options (Configuración > Opciones de intercomunicador Axis)**.
2. Haga clic en **Test call (Llamada de prueba)**.
3. Seleccione un intercomunicador y haga clic en **Make call (Realizar llamada)**.

Evitar eco durante las llamadas

Con la función pulsar para hablar, solo se envía audio en una dirección cada vez a través del intercomunicador. Puede activar pulsar para hablar cuando haya eco en una llamada.

Para activar **Pulsar para hablar**:

- En Smart Client, vaya a **Settings (Ajustes)** > **Axis intercom options (Opciones de intercomunicador de Axis)**.
- Vaya a **Call (Llamada)** y seleccione **Push-to-talk (Pulsar para hablar)**.

Control del intercomunicador desde la visualización en directo

Para cada vista de intercomunicador, haga clic en



para controlar rápidamente el dispositivo.

¿Cómo se hace?	Instrucciones	Comentario
Abrir el bloqueo	Haga clic en  > **Access (Acceso)** o **Extended access (Acceso ampliado)**.	Cuando el bloqueo esté desbloqueado, no va a poder hacer clic en **Access (Acceso)** o en **Extended access (Acceso ampliado)**.
Saber si una puerta está bloqueada o desbloqueada	Haga clic  y lea su estado en la parte inferior del menú.	-

¿Cómo se hace?	Instrucciones	Comentario
Hablar con una persona frente al intercomunicador	Haga clic en  > **Start call (Iniciar llamada)**.	La ventana de llamada se abre e inicia la comunicación bidireccional con el intercomunicador.
Descubra quién llamó ayer	Haga clic en  > **Call history (Historial de llamadas)**.	Va a ver una lista de llamadas realizadas con el intercomunicador actual.

Responder a una llamada desde la visualización en directo

Cuando un visitante pulsa el botón de llamada en el intercomunicador, aparece una ventana de llamada en cada Smart Client que se encuentre en funcionamiento. La ventana de llamada selecciona automáticamente la vista de cámara adecuada al redimensionar la ventana, por ejemplo, vista de pasillo o panorámica.

¿Cómo se hace?	Instrucciones	Comentario
Responder a una llamada	Haga clic en **Accept (Aceptar)**	Se abre un canal de audio bidireccional entre el operador y la persona junto al intercomunicador.
Envío de la llamada a otro operador por encontrarse ocupado	Cierre la ventana haciendo clic en **X**	Cuando se rechace una llamada, un operador diferente puede atenderla en otro cliente El intercomunicador continúa sonando y parpadeando hasta que alguien responde a la llamada. Si nadie responde, la llamada pasa al estado de missed (perdida) en el historial de llamadas.
Rechazo de la llamada porque ya se ha abierto la puerta tras una confirmación visual y no es necesario hablar con la persona	Haga clic en **Decline (Rechazar)**	Cuando se rechaza una llamada, las ventanas de llamada se cierran automáticamente en los demás

¿Cómo se hace?	Instrucciones	Comentario
Rechazo de la llamada porque no se desea hablar con un visitante determinado		clientes. Ningún otro operador puede atender la llamada. El intercomunicador deja de sonar y parpadear, y la ventana de llamada se cierra. La llamada adopta el estado de answered (respondida) en el historial de llamadas.
Apertura de la puerta	Haga clic en **Access (Acceso)**	La cerradura del intercomunicador se abre durante 7 s. Para configurar el tiempo que permanece abierta la puerta: 1. En Smart Client, vaya a **Settings > Axis intercom options > Door access (Configuración > Opciones de intercomunicador Axis > Acceso a puerta)**. 2. Cambiar **Access time (Hora de acceso)**.
Detención temporal del audio del operador en el intercomunicador.	Haga clic en **Mute (Silenciar)**	-
Hable con el visitante cuando esté habilitada la función pulsar para hablar.	Haga clic en **Talk (Hablar)**	Suelte el botón de conversación para escuchar al visitante cuando hable.
Finalizar la llamada.	Haga clic en **Hang up (Colgar)**	El ajuste de cierre automático predeterminado consiste en que la ventana de llamada se cierra cuando se rechaza o cuelga una llamada. Para cambiar el comportamiento predeterminado de la ventana de llamada: 1. En Smart Client, vaya a **Settings > Axis intercom options > Call (Configuración > Opciones de intercomunicador Axis > Llamada)**. 2. Eliminar **Auto-close window (Cierre automático de ventana)**.

Mostrar varias cámaras en la ventana de llamada

Puede mostrar hasta tres cámaras al mismo tiempo en la ventana de llamada. Esto significa que puede ver el flujo de vídeo del intercomunicador y los flujos de vídeo de otras dos cámaras dentro de la misma ventana de

llamada. Esto es útil, por ejemplo, cuando se quiere ver al repartidor y el entorno de la puerta de entrega al mismo tiempo.

Para configurar varias cámaras en la ventana de llamada:

1. En Smart Client, vaya a **Settings > Axis intercom options (Configuración > Opciones de intercomunicador Axis)**. Vaya a **Call > Intercom settings (Llamada > Ajustes del intercomunicador)**.
2. Vaya a **Selected device (Dispositivo seleccionado)** y seleccione qué dispositivo desea configurar.
3. Vaya a **Multiple cameras (Varias cámaras)**. Seleccione el intercomunicador que quiere ver como **camera 1 (cámara 1)** en la ventana de llamada.
4. Determine qué cámaras asociadas quiere ver como **camera 2 (cámara 2)** y **camera 3 (cámara 3)** en la ventana de llamada al recibir llamadas del intercomunicador.
5. Cierra la ventana **Intercom settings (Ajustes del intercomunicador)**.

Acciones de la ventana de llamada

Con las acciones de la ventana de llamada, puede configurar eventos definidos por el usuario que están vinculados a reglas en el motor de reglas XProtect. Los eventos que puede configurar y utilizar dependen de su función.

Para configurar acciones de la ventana de llamada:

1. En Smart Client, vaya a **Settings > Axis intercom options (Configuración > Opciones de intercomunicador Axis)**.
2. Vaya a **Call > Intercom settings (Llamada > Ajustes del intercomunicador)**.
3. Vaya a **Selected device (Dispositivo seleccionado)** y seleccione qué dispositivo desea configurar.
4. Vaya a **Call window actions (Acciones de la ventana de llamada)** para seleccionar las acciones de la ventana de llamada que desea utilizar.

Hay dos tipos de acciones de ventana de llamada:

- **Access button action (Acción del botón de acceso)**: Cuando configura una acción del botón de acceso, anula la acción predeterminada del botón **Access (Acceso)**. Por ejemplo, puede configurar para abrir un conjunto de puertas con el botón **Access (Acceso)**.
- **Custom action (Acción personalizada)**: Cuando configura una acción personalizada, se muestra un botón en la ventana de llamada. Puede activar la acción personalizada haciendo clic en este botón. Una acción personalizada es una acción que no necesariamente se relaciona con el acceso a la puerta, por ejemplo, enviar correos electrónicos, activar alarmas o iniciar grabaciones continuas.

Mostrar una página en la ventana de llamada

Puede mostrar páginas en la ventana de llamada cuando utilice AXIS I8307-VE Network Intercom. Esto resulta útil para mostrar información, por ejemplo, un mapa o el horario de apertura, a quien se encuentre frente al intercomunicador.

En primer lugar, configure estas páginas en el interfaz web de su intercomunicador. Consulte *AXIS I8307-VE Network Intercom*.

Cuando reciba una llamada del intercomunicador:

1. Haga clic en **Show page (Mostrar página)** para ver un cuadro de diálogo con todas las páginas configuradas en su dispositivo.
2. Haga clic en **Load previews (Cargar vistas previas)** para obtener una vista previa de todas las páginas. Para consultar una vista previa de una página configurada, coloque el cursor sobre la página y haga clic en el icono de la imagen.
3. Haga clic en una página configurada para mostrarla en el intercomunicador.

Puede configurar la ventana de llamada para que muestre tanto la imagen de la cámara del intercomunicador como la página empleando distinta cámaras asociadas; es decir, la cámara 1 para la imagen y la cámara 2 para la visualización de la página. Consulte *Mostrar varias cámaras en la ventana de llamada, on page 43*.

Recuerde que la página se cerrará al finalizar la llamada. Repita los pasos anteriores para visualizar una página para una nueva llamada.

Filtrar por extensión de llamada

De forma predeterminada, todos los ordenadores conectados a un intercomunicador reciben las llamadas. Al añadir extensiones de llamada y filtrarlas en el VMS, puede configurar los intercomunicadores para redirigir las llamadas a ciertos Smart Clients en su sistema VMS. Puede configurar programaciones para el enrutamiento de llamadas y agregar contactos de reserva. También puede enrutar llamadas a contactos basados en SIP y añadirlas como contactos de reserva.

En la interfaz web del intercomunicador

1. Vaya a **Communication (Comunicación)** > **SIP**.
2. Seleccione **Enable SIP (Habilitar SIP)**.
3. Haga clic en **Save (Guardar)**.
4. Vaya a **Communication** > **VMS Calls (Llamadas VMS)**.
5. Asegúrese de que la opción **Allow calls in the video management system (VMS) (Permitir llamadas en el sistema de gestión de vídeo (VMS))** está activada.
6. Vaya a **Communication (Comunicación)** > **Contact list (Lista de contacto)**.
7. En **Recipients (Destinatarios)**, haga clic en + para agregar un nuevo contacto. Introduzca la información del nuevo contacto y haga clic en **Save (Guardar)**. Se pueden agregar varios contactos.
   - En **SIP address (Dirección SIP)**, introduzca `VMS_CALL:<extension>`. Sustituya `<extension>` por el nombre de la extensión de llamada para su contacto, por ejemplo `ReceptionA`.
   - Si desea configurar una programación para el contacto, seleccione la disponibilidad o **Availability** del contacto.
   - Puede agregar un contacto de reserva que recibirá la llamada si ninguno de los contactos originales responde, por ejemplo `ReceptionB`.
8. Vaya a **Communication (Comunicación)** > **Calls (Llamadas)**.
9. Para dispositivos con el AXIS OS anterior a la versión 11.6, desactive la opción **Make calls in the video management system (VMS) (Realizar llamadas en el sistema de gestión de vídeo (VMS))**.
10. En **Recipients (Destinatarios)**, elimine el contacto **VMS** y añada el nuevo contacto que ha creado.

En Management Client

Recomendamos configurar los intercomunicadores en el VMS para utilizar un dispositivo de metadatos para la detección de llamadas. Consulte *Configuración de un intercomunicador, on page 37*.

En Smart Client

Configure la extensión de llamada para todos los usuarios que deban recibir las llamadas. El ajuste se guarda en el nivel del usuario. Esto significa que el usuario recibirá las llamadas independientes en las que se utilice el PC.

1. Inicie sesión en Smart Client como el usuario que debe recibir las llamadas.
2. Vaya a **Settings > Axis intercom options (Configuración > Opciones de intercomunicador de Axis)**.
3. En **Call > Call extension (Llamada > Extensión de llamada)**, introduzca el nombre de la extensión de llamada del contacto, por ejemplo `ReceptionA`. Ahora, el usuario solo recibirá llamadas si la extensión de llamada coincide con el valor del filtro.
   Si desea añadir varios nombres de extensión de llamada, sepárelos con punto y coma, por ejemplo: `ReceptionA;ReceptionC`

Ver el historial de llamadas

En Call History (Historial de llamadas) se muestran las llamadas contestadas y perdidas, y si la puerta se ha desbloqueado. Puede seleccionar entre las distintas llamadas y ver el vídeo de reproducción correspondiente si está disponible.

1. En Smart Client, vaya a la vista del intercomunicador.
2. Haga clic en  > **Call history (Historial de llamadas)**.

Nota

El historial de llamadas está limitado a 39 llamadas y 1.000 registros de acceso. El número limitado de llamadas puede ser menor si se silencian las conversaciones con frecuencia.

Para registrar cuándo se ha desbloqueado una puerta, debe establecer el tiempo de retención (días) para el intercomunicador Axis:

1. En Management Cliente, vaya a **Tools > Options > Alarm and Events > Event retention (Herramientas > Opciones > Alarma y eventos > Retención de eventos)**.
2. Defina el tiempo para **Output Activated (Salida activada)** y **Output Deactivated (Salida desactivada)**.

Desactivación del micrófono cuando no hay una llamada activa

Es posible apagar el micrófono cuando no entran llamadas en intercomunicador Axis. El micrófono se enciende cuando hay una llamada activa.

Nota

- Necesita derechos de administrador para apagar el micrófono.
- Esto no es compatible con la arquitectura de gestión federada ni cuando se utilizan contactos de reserva.

1. En Smart Client, vaya a **Settings (Ajustes)** > **Axis intercom options (Opciones de intercomunicador de Axis)**.
2. Seleccione **Turn off intercom microphone when no active call (Apagar micrófono de intercomunicador cuando no hay ninguna llamada activa)**.

Recepción de una alarma si se fuerza la apertura de una puerta

Si una puerta dispone de un relé de seguridad (Entrada 2), la superposición de la puerta en la ventana de llamada Smart Client muestra cuando la puerta está abierta o cerrada. Esto significa que si alguien abre una puerta por la fuerza mientras está cerrada, usted puede recibir una alarma.

Nota

Para recibir una alarma, debe haber al menos un Smart Client en ejecución.

Para configurar la alarma:

1. En Smart Client, vaya a **Settings > Axis intercom options > Administrator options (Configuración > Opciones de intercomunicador Axis > Opciones de administrador)**.
2. Seleccione **Trigger an alarm when a door has been forced open (Activar la alarma cuando se ha forzado la apertura de una puerta)**.

Recibir una alarma si una puerta permanece abierta demasiado tiempo

Si una puerta dispone de un relé de seguridad (Entrada 2), la superposición de la puerta en la ventana de llamada Smart Client muestra cuando la puerta está abierta o cerrada. Esto significa que si alguien abre la puerta y la puerta permanece abierta durante demasiado tiempo, puede recibir una alarma.

Nota

Para recibir una alarma, debe haber al menos un Smart Client en ejecución.

Para configurar la alarma:

1. En Smart Client, vaya a **Settings > Axis intercom options > Administrator options (Configuración > Opciones de intercomunicador Axis > Opciones de administrador)**.
2. Seleccionar **Trigger an alarm when a door has been open longer than (s) (Activar una alarma cuando una puerta se esté abierta durante más de [s])**.
3. Introduzca el tiempo que la puerta puede permanecer abierta antes de que salte la alarma.

Impedir que un cliente reciba llamadas

Puede configurar para que un cliente no reciba ninguna llamada. Esto significa que cuando alguien hace una llamada, no se abre ninguna ventana de llamada en el cliente especificado.

1. En Smart Client, vaya a **Settings > Axis intercom options > Call (Configuración > Opciones de intercomunicador Axis > Llamada)**.
2. Eliminar **Receive calls on this client (Recibir llamadas en este cliente)**.

Visualización de audio

Vista de micrófono

Puede visualizar audio en su sistema agregando una o varias vistas de micrófono a Smart Client. A continuación, puede supervisar el audio en la visualización en directo y en la reproducción. Puede ver cuándo los niveles de

audio superan un nivel determinado mediante la detección de audio integrada en el dispositivo Axis. Los casos que suelen usarse son:

- *Escuchar varios micrófonos al mismo tiempo, on page 49*
- *Detectar incidentes con audio, on page 49*
- *Investigar incidentes después de que sucedieron, on page 49*

Nota

Requisitos

- Versión del VMS Smart Client 2020 R2 o posterior.

Configurar VMS para la vista de micrófono

1. Defina los niveles de detección:
   1.1. En Management Client, vaya a **Navegación del sitio > AXIS Optimizer > Asistente de dispositivos** y seleccione su dispositivo.
   1.2. Abra la configuración **de detectores** . El modo de abrir estos ajustes depende de la versión de software del dispositivo.
   1.3. Vaya a Detección **de audio** y modifique el **nivel de sonido de entrada 1** para adaptarlo a sus necesidades.
2. Consultar eventos de la cámara en el VMS:
   2.1. En Management Client, vaya a **Navegación del sitio > Dispositivos > Micrófonos**.
   2.2. Haga clic en el micrófono y a continuación, en **Eventos** .
   2.3. Agregue eventos **Audio Falling** y **Audio Rising**.
3. Configure durante cuánto tiempo el sistema conserva los metadatos sobre el audio detectado:
   3.1. Vaya a **Herramientas > Opciones > Alarma y eventos > Eventos del dispositivo** .
   3.2. Encuentra **Audio Falling** y establece el tiempo de retención.
   3.3. Busque **Audio Raising** y establezca el tiempo de retención.
4. Compruebe que ha configurado la grabación de audio. Puede, por ejemplo, grabar audio continuamente o crear una regla de grabación basada en la generación de audio o la caída de audio en eventos.
5. Para cada micrófono que desee usar con la vista de micrófono, repita los pasos anteriores.
6. En Smart Client, vaya a **Configuración > Línea temporal > Datos adicionales** y seleccione **Mostrar**.

Agregar la vista de micrófono a Smart Client

1. Abra Smart Client y haga clic en **Setup (Configuración)**.
2. Vaya a **Views (Vistas)**.
3. Haga clic en **Create new view (Crear nueva vista)** y seleccione un formato.
4. Vaya a **System overview > AXIS Optimizer (Información general del sistema > AXIS Optimizer)**.
5. Haga clic en la **vista Micrófono** y arrástrelo a la vista.
6. Seleccione un micrófono.
7. Haga clic en **Setup (Configuración)**.

Usar vista de micrófono

- Vista en vivo
  - Los niveles de audio se muestran como un gráfico de barras con el nivel actual a la derecha y el historial de audio de hasta 60 s moviéndose a la izquierda.
  - Haga clic en la vista para escuchar el audio del micrófono.

  - En cada vista de micrófono hay un icono de auriculares. Haga clic en el icono para silenciar o activar el sonido de cada vista sin tener que seleccionar la vista. De este modo, podrá escuchar varios micrófonos al mismo tiempo.

- Reproducción
  - Se resaltará un icono cuando haya audio detectado disponible para el micrófono.
  - Las barras amarillas indican que el audio se ha detectado según los niveles de detección establecidos en el dispositivo.
  - Haga clic en la vista para escuchar el audio del micrófono.
  - En cada vista de micrófono hay un icono de auriculares. Haga clic en el icono para silenciar o activar el sonido de cada vista sin tener que seleccionar la vista. De este modo, podrá escuchar varios micrófonos al mismo tiempo.

Escuchar varios micrófonos al mismo tiempo

La vista del micrófono le permite escuchar varios micrófonos al mismo tiempo, tanto en vista en vivo como en reproducción.

1. *Configurar VMS para la vista de micrófono, on page 48*.
2. Abra Smart Client y haga clic en **Setup (Configuración)**.
3. Vaya a **Views (Vistas)**.
4. Haga clic en **Create new view (Crear nueva vista)** y seleccione una vista dividida.
5. Vaya a **System overview > AXIS Optimizer (Información general del sistema > AXIS Optimizer)**.
6. Para cada micrófono que desee escuchar:
   6.1. Haga clic en la **vista Micrófono** y arrástrelo a la vista.
   6.2. Seleccione un micrófono.
7. Haga clic en **Setup (Configuración)**.
8. Para cada micrófono, decida si desea silenciar o desactivarlo haciendo clic en el icono de auriculares en cada vista de micrófono. Ahora puede escuchar todos los micrófonos no silenciados al mismo tiempo.

Detectar incidentes con audio

Es posible que desee monitorear acciones desde áreas donde no se le permite instalar cámaras, por ejemplo, baños. En la vista de micrófono puede ver rápidamente cuándo se produce un incidente, es decir, cuando el nivel de sonido supera los niveles de detección.

1. *Configurar VMS para la vista de micrófono, on page 48*. Recuerde que debe establecer los niveles de detección relevantes para el dispositivo y el área que desee supervisar.
2. Agregue una vista de micrófono con el dispositivo a la visualización en directo en Smart Client, consulte *Agregar la vista de micrófono a Smart Client, on page 48*.

Investigar incidentes después de que sucedieron

Después de que ocurra un incidente, puede identificar rápidamente los períodos en la línea de tiempo de reproducción cuando sus micrófonos detectaron audio.

1. *Configurar VMS para la vista de micrófono, on page 48*.
2. Añada una o varias vistas de micrófono con los dispositivos relevantes para reproducirlo en Smart Client, consulte *Agregar la vista de micrófono a Smart Client, on page 48*.

Búsqueda forense

AXIS Optimizer ofrece cuatro categorías de búsqueda para los dispositivos Axis en la búsqueda centralizada:

- *Búsqueda forense, on page 50* (Búsqueda de objetos)
- *Búsqueda de vehículos, on page 53*
- *Búsqueda de velocidad de zona, on page 56*
- *Búsqueda de contenedores, on page 58*

También puede añadir una pestaña de búsqueda de matrículas independiente a Smart Client. Consulte *Matrículas de Axis, on page 59*.

Puede configurar estas categorías de búsqueda en un panel centralizado, consulte *Configurar categorías de búsqueda de Axis, on page 108*.

Búsqueda forense

Las cámaras AXIS OS 9.50 o posterior generan metadatos que describen todos los objetos en movimiento en el campo de visión de la cámara. El VMS puede grabar estos datos junto con el vídeo y el audio correspondientes. La función de búsqueda forense de AXIS Optimizer le permite analizar y buscar estos datos. Utilice la búsqueda forense para obtener una visión general de toda la actividad de la escena o encontrar rápidamente un objeto o evento de interés específico.

Antes de empezar

1. Asegúrese de que la cámara tiene la versión de AXIS OS más reciente.
2. Asegúrese de que el VMS tiene la versión correcta:
   - Corporate 2019 R3 o más reciente o Expert 2019 R3 o más reciente
   - Professional+ 2022 R3 o más reciente o Express+ 2022 R3 o más reciente
3. La hora de la cámara debe estar sincronizada con NTP.
4. Para filtrar por tipos de objeto **Human (Humano)**, **Vehicle (Vehículo)**, **Bike (Bicicleta)**, **Bus (Autobús)**, **Car (Coche)** o **Truck (Camión)**:
   4.1. utilice un dispositivo Axis compatible con AXIS Object Analytics. Consulte el filtro Analytics en el *Selector de producto*.
   4.2. Vaya a **System > Analytics metadata (Sistema > Metadatos de analíticas)** y habilite **Analytics Scene Description (Descripción de la escena de analíticas)** en la página web de la cámara.
5. Para filtrar por **Vehicle color (Color del vehículo)**, **Upper body clothing color (Color de la prenda superior)** o **Lower body clothing color (Color de la prenda inferior)**:
   5.1. utilice un dispositivo Axis compatible con AXIS Object Analytics. Consulte el filtro Analytics en el *Selector de producto*.
   5.2. use un dispositivo Axis con ARTPEC-8 o CV25. Consulte el filtro System-on-chip en el *Product selector (Selector de producto)*.

Configurar la búsqueda forense



1. En Management Client, asegúrese de que el dispositivo de metadatos está habilitado para las cámaras.

2. Asegúrese de que el dispositivo de metadatos esté relacionado con la cámara:
   - Vaya a **Devices (Dispositivos)** > **Camera (Cámara)** y seleccione el dispositivo.
   - Vaya a la pestaña **Client (Cliente)** y asegúrese de que el dispositivo de metadatos de la cámara está seleccionado en **Related metadata (Metadatos relacionados)**.
3. Vaya a **Site Navigation > Devices > Metadata (Navegación de instalaciones > Dispositivos > Metadatos)**.
4. Seleccione su dispositivo y haga clic en **Record (Grabar)**. Asegúrese de que **Recording (Grabación)** está activada.
   De manera predeterminada, los metadatos solo se graban cuando el VMS detecta movimiento en una escena. Por lo tanto, recomendamos ajustar el umbral de movimiento al entorno para que no se pierda el movimiento de ningún objeto.
5. Haga clic en **Settings (Ajustes)** y asegúrese de que los **Analytics data (Datos de analíticas)** están habilitados.
6. Abra la visualización en directo de Smart Client y compruebe que hay cuadros limitadores sobre los objetos y que se muestran correctamente.
   El reloj puede tardar un tiempo en adaptarse a la hora NTP.
7. Espere al menos 15 min para que el sistema grabe el vídeo y los metadatos. A continuación, puede empezar a buscar, consulte *Realizar una búsqueda, on page 51*.
8. Active **Consolidated metadata (Metadatos consolidados)** para mejorar la velocidad de búsqueda en dispositivos con AXIS OS 11.10 o superior. Consulte *Metadata and search, on page 107*.

Realizar una búsqueda



Nota

Antes de poder utilizar esta función de búsqueda, es necesario configurarla en Management Client. Para saber cómo hacerlo, consulte *Configurar la búsqueda forense, on page 50*.

1. En Smart Client, vaya a **Search (Buscar)**.
2. Seleccione un intervalo de tiempo y una o varias cámaras.
3. Haga clic en **Search for > Forensic search > New search (Buscar > Búsqueda forense > Nueva búsqueda)**. Para cada resultado de la búsqueda, va a ver el objeto y la trayectoria del objeto en la miniatura.
   - La miniatura muestra el fotograma de vídeo en el que el objeto ha sido más visible.
   - El punto verde marca la ubicación en la que la cámara ha detectado por primera vez el objeto.
   - El punto rojo marca el lugar donde la cámara ha detectado por última vez el objeto.
   - Para ver la secuencia de vídeo completa del resultado de una búsqueda, selecciónelo y haga clic en **Play forward (Reproducir hacia delante)** en el panel de vista previa.
   - Para ocultar las superposiciones gráficas, vaya a **Bounding Boxes (Cuadros limitadores)** y seleccione **Hide (Ocultar)**.

   Nota

   Las aplicaciones de análisis que se ejecutan en la cámara, por ejemplo, AXIS Object Analytics y AXIS Loitering Guard, también podrían grabar superposiciones en el vídeo. Para eliminar estas superposiciones, vaya a la página de configuración web de la aplicación.
4. Seleccione los filtros de búsqueda para reducir el número de resultados.

Para obtener más información sobre cómo utilizar los distintos filtros, consulte *Afinar una búsqueda, on page 52*.

5. Seleccione los resultados de la búsqueda que desee examinar más de cerca. Puede, por ejemplo, marcarlos como favoritos o *Crear un informe en PDF de alta calidad, on page 59*.

Afinar una búsqueda

Para limitar los resultados de una búsqueda, puede utilizar uno o varios filtros de búsqueda.

- **Region of interest (Región de interés)**
  Detecta objetos que se han movido en un área específica.
- **Dirección de objeto**
  Detecta objetos que se han movido a lo largo de una ruta concreta en una escena: a la izquierda, a la derecha, hacia abajo o hacia arriba.
- **Tipo de objeto**
  Detecta objetos de un tipo determinado: humano, vehículo, bicicleta, autobús, coche camión.

Nota

- La velocidad (km/h o mph) y matrícula solo se admiten en AXIS Q1686–DLE Radar-Video Fusion Camera.
- Debe activar las funciones de velocidad (km/h o mph) y matrícula antes de poder utilizarlas. Para ello, consulte *Configurar categorías de búsqueda de Axis, on page 108*.
- **Velocidad (km/h o mph)**
  Detectar vehículos que se mueven a una velocidad determinada.
- **Matrícula**
  Detectar vehículos que tienen una matrícula específica. También puede utilizarlo para buscar matrículas que incluyan ciertas letras o números.
- **Color del vehículo**
  Detecta vehículos de los colores elegidos.
- **Color de la prenda superior**
  Detecta ropa de los colores elegidos en la parte superior del cuerpo de una persona.
- **Color de la prenda inferior**
  Detecta ropa de los colores elegidos en la parte inferior del cuerpo de una persona.
- **Time-of-day (Hora del día)**
  Detecta objetos detectados durante una parte concreta del día. Este filtro es útil cuando se busca a lo largo de varios días, pero solo interesan los objetos identificados a una hora concreta de cada día, por ejemplo, por la tarde.
- **Tiempo mínimo en la escena (s)**
  Detecta objetos que se han detectado y rastreado durante un número mínimo de segundos. Este filtro elimina los objetos poco interesantes, por ejemplo, los que están lejos y los que son falsos (efectos de iluminación). El valor predeterminado es 1 segundo. Por lo tanto, cuando el filtro no está configurado, se excluyen los objetos con una duración inferior a 1 segundo.
- **Objetos con balanceo (% de imagen)**
  Excluye los objetos que solo se mueven en un área de restricción, por ejemplo, una bandera o un árbol que se mueve con el viento. El valor predeterminado es de 5 al 100 %. Esto significa que cuando el filtro no está configurado, excluye los objetos que no se han movido más allá del 5 % del área de la imagen.

Limitaciones

- A fin de obtener las secuencias de vídeo correctas para los resultados de la búsqueda, es importante que el reloj esté adecuadamente sincronizado.
- Los datos analizados en la búsqueda forense no tienen en cuenta la perspectiva de la escena. Esto significa que el tamaño y la velocidad de un objeto difieren en función de su proximidad a la cámara.
- Las condiciones meteorológicas, como la lluvia intensa o la nieve, pueden afectar a la precisión de la detección.

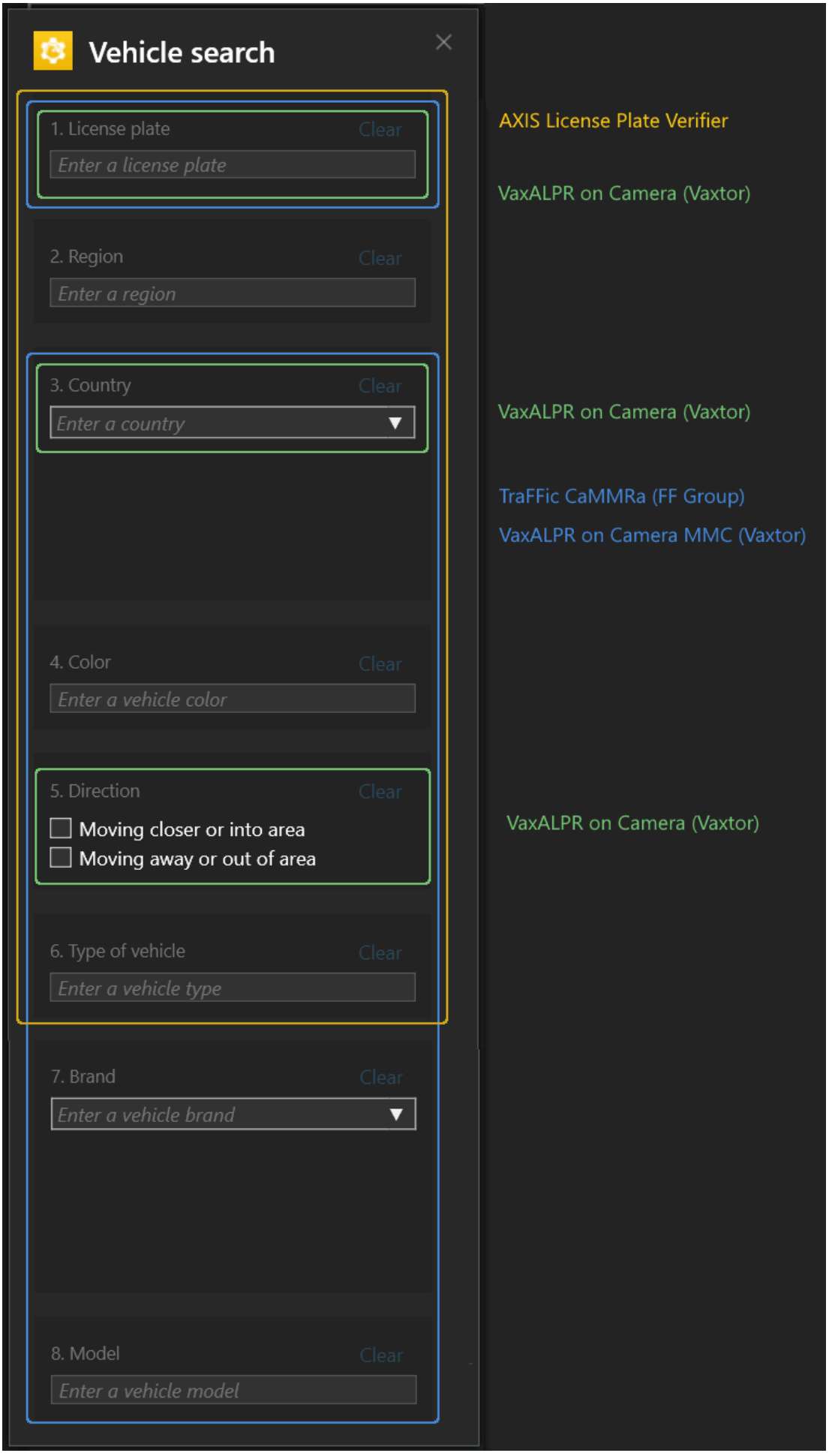
- Si hay un buen contraste con el objeto en escenas de poca luz, la analítica es más precisa.
- En ciertas circunstancias, un único objeto puede generar varios resultados. Por ejemplo, cuando se pierde el seguimiento porque un objeto queda temporalmente oculto por otro.
- Las superposiciones pueden variar en función de la versión de XProtect. Por ejemplo: las superposiciones de vista previa de vídeo requieren XProtect 2020 R3 y los colores superpuestos requieren XProtect 2020 R2.
- Para que la búsqueda forense funcione en flujos de vídeo que se han girado 180 grados, debe:
  - utilizar AXIS OS 10.6 o posterior en las cámaras, o bien
  - utilizar Device Pack 11.0 o posterior en el servidor de grabación
- La configuración del balance de blancos de la cámara debe ser precisa para conseguir una buena detección de color

Búsqueda de vehículos

Si utiliza AXIS Optimizer junto con determinadas aplicaciones instaladas en la cámara, es posible buscar, identificar y compartir datos de vídeo sobre vehículos. La búsqueda de vehículos es compatible con los datos de las matrículas de las aplicaciones siguientes:

- *AXIS License Plate Verifier* de Axis Communications
- *CAMMRA AI* de FF Group (se requiere la versión 1.3 o superior)
- *VaxALPR On Camera* de Vaxtor Recognition Technologies
- *VaxALPR On Camera MMC* de Vaxtor Recognition Technologies

Los filtros de búsqueda que puede utilizar dependen de la aplicación que ha instalado en las cámaras, consulte *Afinar una búsqueda, on page 55*


Vehicle search
1. License plate
Clear
Enter a license plate
2. Region
Clear
Enter a region
3. Country
Clear
Enter a country
4. Color
Clear
Enter a vehicle color
5. Direction
Clear
Moving closer or into area
Moving away or out of area
6. Type of vehicle
Clear
Enter a vehicle type
7. Brand
Clear
Enter a vehicle brand
8. Model
Clear
Enter a vehicle model
AXIS License Plate Verifier
VaxALPR on Camera (Vaxtor)
VaxALPR on Camera (Vaxtor)
TraFFic CaMMRa (FF Group)
VaxALPR on Camera MMC (Vaxtor)
VaxALPR on Camera (Vaxtor)

Configurar la búsqueda de vehículos

Nota

Requisitos

- Sistema de VMS
  - Corporate, Expert 2019 R3 o posterior
  - Professional+ o Express+ 2022 R3 o posterior
- La hora de la cámara está sincronizada con NTP
- Una de las aplicaciones mostradas en

1. En Management Client, agregue la cámara en la que se ejecuta la aplicación elegida.
2. Habilite todos los dispositivos que necesite. Para poder utilizar AXIS Licence Plate Verifier, es necesario tener Cámara 1 y Metadatos 1.
3. Asegúrese de que el dispositivo de metadatos esté relacionado con la cámara:
   - Vaya a **Devices (Dispositivos)** > **Camera (Cámara)** y seleccione el dispositivo.
   - Vaya a la pestaña **Client (Cliente)** y asegúrese de que el dispositivo de metadatos de la cámara está seleccionado en **Related metadata (Metadatos relacionados)**.
4. Configuración de los metadatos:
   4.1. vaya a **Site Navigation > Recording Server (Navegación del sitio > Servidor de grabación)** y encuentre el dispositivo.
   4.2. Seleccione Metadatos 1 y haga clic en **Settings (Ajustes)**.
   4.3. Vaya a **Metadata stream > Event data (Flujo de metadatos > Datos de eventos)** y seleccione **Yes (Sí)**.
5. Vaya a la pestaña **Record settings (Ajustes de grabación)** y compruebe que la grabación de los metadatos está habilitada.
6. Haga clic en **Save (Guardar)**.
7. Configure la aplicación de forma que funcione para un usuario estándar:
   7.1. Añada derechos de lectura y reproducción a la cámara y al usuario específicos.
   7.2. Añada derechos de lectura y reproducción de los metadatos a la cámara y al usuario específicos.

Búsqueda de un vehículo

1. En Smart Client, vaya a **Search (Buscar)**.
2. Seleccione un intervalo de tiempo y una o varias cámaras.
3. Haga clic en **Search for > Vehicle search > New search (Buscar > Buscar vehículo > Nueva búsqueda)**.
4. Seleccione los filtros de búsqueda para reducir el número de resultados.
   Para obtener más información sobre los distintos filtros, consulte *Afinar una búsqueda, on page 55*.
5. Seleccione los resultados de la búsqueda que desee examinar más de cerca. Puede, por ejemplo, marcarlos como favoritos o *Crear un informe en PDF de alta calidad, on page 59*.

Afinar una búsqueda

Para limitar los resultados de una búsqueda, puede utilizar uno o varios filtros de búsqueda. Las distintas aplicaciones le ofrecen diferentes opciones de filtrado.

- **Matrícula**
  Encuentre un número de matrícula específico.
  Aplicación: AXIS License Plate Verifier, VaxALPR On Camera, CAMMRA AI or VaxALPR On Camera MMC.
- **Región**
  Encuentre vehículos de una región determinada.

Aplicación: AXIS License Plate Verifier 2.9.19.

Nota

Establezca la ubicación de la cámara en los ajustes de AXIS License Plate Verifier para un reconocimiento de región óptimo.

- **País**
  Encuentra vehículos de un país determinado.
  Aplicación: Axis License Plate Verifier 2.9.19, VaxALPR On Camera, CAMMRA AI o VaxALPR On Camera MMC.
- **Color**
  Encuentre vehículos con un color específico.
  Aplicación: Axis License Plate Verifier 2.9.19, CAMMRA AI o VaxALPR On Camera MMC.
- **Dirección**
  Encuentre vehículos que se mueven en una dirección específica.
  Aplicación: Axis License Plate Verifier 2.9.19, VaxALPR On Camera, CAMMRA AI o VaxALPR On Camera MMC.
- **Tipo de vehículo**
  Encuentra un tipo de vehículo específico.
  Aplicación: Axis License Plate Verifier 2.9.19, CAMMRA AI o VaxALPR On Camera MMC.
- **Marca**
  Encuentra una marca de vehículo específica.
  Aplicación: CAMMRA AI o VaxALPR On Camera MMC.
- **Modelo**
  Encuentra un modelo de vehículo específico.
  Aplicación: CAMMRA AI o VaxALPR On Camera MMC.

Optimizar la velocidad de búsqueda

Puede mejorar la velocidad de búsqueda controlando los datos que su sistema almacena en el dispositivo de metadatos VMS.

- Desactive los datos analíticos si no los necesita.
  - Vaya a **Devices (Dispositivos)** > **Metadata (Metadatos)** y seleccione el dispositivo.
  - Haga clic en **Settings (Ajuste)** y desactive los **Analytics data (Datos de analíticas)**.
- Si necesita datos de analíticas, puede recurrir a los metadatos consolidados, si están disponibles. Consulte *Metadata and search, on page 107*.
- Desactive los eventos que no necesite de AXIS License Plate Verifier. Solo necesita el evento **Lost (Perdido)** para que AXIS Optimizer funcione. Consulte *AXIS License Plate Verifier*.
- Asegúrese de utilizar AXIS OS 12.8 o una versión posterior.

Búsqueda de velocidad de zona

En AXIS Optimizer, puede utilizar la búsqueda de velocidad de zona para buscar la velocidad de vehículos que se hayan detectado al entrar en una zona predeterminada en la vista de una cámara. La búsqueda de velocidad de zona funciona junto con la aplicación *AXIS Speed Monitor* para visualizar la velocidad de los vehículos en una zona de detección por radar en la visualización en directo de la cámara. Con la búsqueda de velocidad de zona de Axis puede configurar filtros específicos para limitar la búsqueda y exportar y compartir pruebas en vídeo durante las investigaciones.

Configurar búsqueda de velocidad de zona

Nota

Requisitos

- Sistema de VMS

  - Corporate, Expert 2019 R3 o posterior
  - Professional+ o Express+ 2022 R3 o posterior
- La hora de la cámara está sincronizada con NTP

1. En Management Client, agregue la cámara en la que se ejecuta la aplicación elegida.
2. Habilite todos los dispositivos que necesite. Para poder utilizar la búsqueda de velocidad en una zona de AXIS, es necesario tener Cámara 1 y Metadatos 1.
3. Asegúrese de que el dispositivo de metadatos esté relacionado con la cámara:
   - Vaya a **Devices (Dispositivos)** > **Camera (Cámara)** y seleccione el dispositivo.
   - Vaya a la pestaña **Client (Cliente)** y asegúrese de que el dispositivo de metadatos de la cámara está seleccionado en **Related metadata (Metadatos relacionados)**.
4. Cómo configurar los metadatos:
   4.1. vaya a **Site Navigation > Recording Server (Navegación del sitio > Servidor de grabación)** y encuentre el dispositivo.
   4.2. Seleccione Metadatos 1 y haga clic en **Settings (Ajustes)**.
   4.3. Vaya a **Metadata stream > Event data (Flujo de metadatos > Datos de eventos)** y seleccione **Yes (Sí)**.
5. Vaya a la pestaña **Record settings (Ajustes de grabación)** y compruebe que la grabación de los metadatos está habilitada.
6. Haga clic en **Save (Guardar)**.
7. Cómo configurar la aplicación de forma que funcione para un usuario estándar:
   7.1. Añada derechos de lectura y reproducción a la cámara y al usuario específicos.
   7.2. Añada derechos de lectura y reproducción de los metadatos a la cámara y al usuario específicos.

Buscar por eventos de velocidad de zona



1. En Smart Client, vaya a **Search (Buscar)**.
2. Seleccione un intervalo de tiempo y una o varias cámaras.
3. Haga clic en **Search for > Zone speed search > New search (Buscar > Buscar velocidad de zona > Nueva búsqueda)**.
4. Seleccione los filtros de búsqueda para reducir el número de resultados.
   Para obtener más información sobre los distintos filtros, consulte *Afinar una búsqueda, on page 57*.
5. Seleccione los resultados de la búsqueda que desee examinar más de cerca. Puede, por ejemplo, marcarlos como favoritos o *Crear un informe en PDF de alta calidad, on page 59*.

Afinar una búsqueda

Para limitar los resultados de la búsqueda de los eventos de exceso de velocidad, puede utilizar uno o varios filtros de búsqueda.

- **Velocidad máx.**
  Filtre la velocidad máxima de cualquier objeto en la zona durante la duración del evento. Puede definir un límite inferior y uno superior para la velocidad máxima.

- **Tipo de objeto**
  Si se selecciona **vehículo**, la búsqueda solo mostrará los eventos de exceso de velocidad en los que el objeto más rápido de la zona se haya clasificado como vehículo.
- **Nombre de zona**
  Buscar y filtrar zonas por nombre.

Búsqueda de contenedores

Si utiliza AXIS Optimizer junto con determinadas aplicaciones, podrá buscar, identificar y compartir datos de vídeo sobre contenedores. La búsqueda de contenedores admite datos de la siguiente aplicación:

- *VaxOCR Containers* de Vaxtor Recognition Technologies

Configuración de búsqueda de contenedores

Nota

Requisitos

- Sistema de VMS
  - Corporate, Expert 2019 R3 o posterior
  - Professional+ o Express+ 2022 R3 o posterior
- La hora de la cámara está sincronizada con NTP
- La aplicación aparece en

1. En Management Client, agregue la cámara en la que se ejecuta la aplicación elegida.
2. Habilite todos los dispositivos que necesite.
3. Asegúrese de que el dispositivo de metadatos esté relacionado con la cámara:
   - Vaya a **Devices (Dispositivos)** > **Camera (Cámara)** y seleccione el dispositivo.
   - Vaya a la pestaña **Client (Cliente)** y asegúrese de que el dispositivo de metadatos de la cámara está seleccionado en **Related metadata (Metadatos relacionados)**.
4. Configuración de los metadatos:
   4.1. vaya a **Site Navigation > Recording Server (Navegación del sitio > Servidor de grabación)** y encuentre el dispositivo.
   4.2. Seleccione Metadatos 1 y haga clic en **Settings (Ajustes)**.
   4.3. Vaya a **Metadata stream > Event data (Flujo de metadatos > Datos de eventos)** y seleccione **Yes (Sí)**.
5. Vaya a la pestaña **Record settings (Ajustes de grabación)** y compruebe que la grabación de los metadatos está habilitada.
6. Haga clic en **Save (Guardar)**.
7. Configure la aplicación de forma que funcione para un usuario estándar:
   7.1. Añada derechos de lectura y reproducción a la cámara y al usuario específicos.
   7.2. Añada derechos de lectura y reproducción de los metadatos a la cámara y al usuario específicos.

Búsqueda de un contenedor

1. En Smart Client, vaya a **Search (Buscar)**.
2. Seleccione un intervalo de tiempo y una o varias cámaras.
3. Haga clic en **Search for > Container search > New search (Buscar > Búsqueda de contenedor > Nueva búsqueda)**.
4. Seleccione los filtros de búsqueda para reducir el número de resultados.
   Para obtener más información sobre los distintos filtros, consulte *Afinar una búsqueda, on page 59*.

5. Seleccione los resultados de la búsqueda que desee examinar más de cerca. Puede, por ejemplo, marcarlos como favoritos o *Crear un informe en PDF de alta calidad, on page 59*.

Afinar una búsqueda

Para limitar los resultados de una búsqueda, puede utilizar uno o varios filtros de búsqueda. Todas las opciones de filtro proceden de la aplicación VaxOCR Containers.

- **Código de contenedor**
  Encuentre un código de contenedor específico.
- **Propietario**
  Encuentre los contenedores que pertenecen a un determinado propietario.
- **Código de propietario**
  Encuentre los contenedores que pertenecen a un determinado propietario.
- **Tamaño**
  Encuentre contenedores de un tamaño y tipo determinados.
- **Código de tamaño**
  Encuentre contenedores de un tamaño y tipo determinados.
- **City or country (Ciudad o país)**
  Encuentre contenedores de una ciudad o un país determinados.
- **Validación**
  Encuentre contenedores que se hayan validado mediante su código de propietario o dígito de control.

Crear un informe en PDF de alta calidad



Cree un informe en función de los resultados de búsqueda. Puede utilizar esta función para incluir imágenes de alta resolución en el resultado.

1. En Smart Client, haga una búsqueda.
2. Seleccione los resultados de la búsqueda que desee incluir en el informe.
3. Haga clic en p,255mm,sfx)=″graphics:graphic018FACAAED177A53B1E07E58CECD82C6″ > **Create high quality PDF report (Crear informe en PDF de alta calidad)**.
4. (Opcional) Introduzca el **Report name (Nombre del informe)**, el **Report destination (Destino del informe)** y las **Notes (Notas)**.
5. Para cada resultado de búsqueda, seleccione el fotograma que desee incluir en el informe. Para ampliar una imagen, haga doble clic.
6. Haga clic en **Create (Crear)**. Cuando el informe esté listo, se le envía una notificación.

Matrículas de Axis

Puede añadir una pestaña independiente para la búsqueda y gestión de matrículas en Smart Client. En esta pestaña se centralizan todas las tareas del operador relacionadas con la gestión, la búsqueda y la exportación de matrículas en función de la información proporcionada por las cámaras Axis habilitadas para LPR.



Antes de empezar

- Asegúrese de que tiene la versión VMS 2018 R3 o posterior
- Asegúrese de que tiene VMS Pack 10.1 o más posterior
- La hora de la cámara debe estar sincronizada con NTP
- Use una de las aplicaciones mostradas en

Configurar matrículas de Axis

1. En Management Client, agregue la cámara en la que se ejecuta la aplicación elegida.
2. Habilite todos los dispositivos que necesite. Para poder utilizar AXIS Licence Plate Verifier, es necesario tener Cámara 1 y Metadatos 1.
3. Asegúrese de que el dispositivo de metadatos esté relacionado con la cámara:
   - Vaya a **Devices (Dispositivos)** > **Camera (Cámara)** y seleccione el dispositivo.
   - Vaya a la pestaña **Client (Cliente)** y asegúrese de que el dispositivo de metadatos de la cámara está seleccionado en **Related metadata (Metadatos relacionados)**.
4. Configuración de los metadatos:
   4.1. vaya a **Site Navigation > Recording Server (Navegación del sitio > Servidor de grabación)** y encuentre el dispositivo.
   4.2. Seleccione Metadatos 1 y haga clic en **Settings (Ajustes)**.
   4.3. Vaya a **Metadata stream > Event data (Flujo de metadatos > Datos de eventos)** y seleccione **Yes (Sí)**.
5. Vaya a la pestaña **Record settings (Ajustes de grabación)** y compruebe que la grabación de los metadatos está habilitada.
6. Haga clic en **Save (Guardar)**.

Buscar una matrícula

1. En Smart Client, vaya a **Axis license plates (Matrículas de Axis)**.
   Si no aparece en la pestaña, vaya a **Settings > Axis search options (Configuración > Opciones de búsqueda de Axis)** y seleccione **Show license plate search tab (Mostrar la pestaña de búsqueda de matrículas)**.
2. Haga clic en **Add camera... (Agregar cámara...)**, seleccione las cámaras que corresponda y haga clic en **Close (Cerrar)**.
   Para agregar cámaras al sistema debe tener funciones de administrador. Cuando la cámara detecta matrículas, estas aparecen en directo en la lista, incluyendo imágenes recortadas de las matrículas tomadas por la cámara. El resultado de la búsqueda no mostrará más de 5000 resultados.
3. Introduzca una matrícula y un **intervalo de tiempo** para filtrar los resultados de la búsqueda.
   - Introduzca un **intervalo de tiempo** personalizado entre las dos fechas elegidas para filtrar el resultado de la búsqueda.

Buscar una matrícula en directo

1. En Smart Client, vaya a **Axis license plates (Matrículas de Axis)**.

Si no aparece en la pestaña, vaya a **Settings > Axis search options (Configuración > Opciones de búsqueda de Axis)** y seleccione **Show license plate search tab (Mostrar la pestaña de búsqueda de matrículas)**.

2. Haga clic en **Add camera... (Agregar cámara...)**, seleccione las cámaras que corresponda y haga clic en **Close (Cerrar)**.
   Para agregar cámaras al sistema debe tener funciones de administrador. Cuando la cámara detecta matrículas, estas aparecen en directo en la lista, incluyendo imágenes recortadas de las matrículas tomadas por la cámara. El resultado de la búsqueda no mostrará más de 5000 resultados.
3. Introduzca una matrícula y seleccione **Time interval (Intervalo de tiempo)** > **Live (Directo)** para filtrar el resultado de la búsqueda.

Afinar una búsqueda

Para limitar los resultados de una búsqueda, puede utilizar uno o varios filtros de búsqueda.

- **Intervalo de tiempo**
  Los resultados de la búsqueda se limitan un periodo de tiempo.
- **Matrícula**
  Los resultados se filtran por el texto de la matrícula, parcial o completo.
- **Cámaras**
  Los resultados de la búsqueda se limitan a los detectados por cámaras concretas.
- **Dirección**
  Los resultados se limitan a los vehículos que se mueven en una dirección determinada.
- **Listas**
  Los resultados de la búsqueda se limitan a determinadas instalaciones y por listas de permitidos, bloqueados y listas personalizadas. Para obtener más información sobre la creación de listas, consulte *Gestión centralizada de listas de matrículas, on page 24*.

Optimizar la velocidad de búsqueda

Puede mejorar la velocidad de búsqueda controlando los datos que su sistema almacena en el dispositivo de metadatos VMS.

- Desactive los datos analíticos si no los necesita.
  - Vaya a **Devices (Dispositivos)** > **Metadata (Metadatos)** y seleccione el dispositivo.
  - Haga clic en **Settings (Ajuste)** y desactive los **Analytics data (Datos de analíticas)**.
- Si necesita datos de analíticas, puede recurrir a los metadatos consolidados, si están disponibles. Consulte *Metadata and search, on page 107*.
- Desactive los eventos que no necesite de AXIS License Plate Verifier. Solo necesita el evento **Lost (Perdido)** para que AXIS Optimizer funcione. Consulte *AXIS License Plate Verifier*.
- Asegúrese de utilizar AXIS OS 12.8 o una versión posterior.

Exportar una búsqueda de matrícula como informe en PDF

Utilice esta función para recopilar los resultados de búsqueda que le interesen como un informe en PDF con imágenes de alta calidad.

1. Haga clic en **Export... (Exportar...)**.
2. Seleccione **PDF...**.
3. (Opcional) Introduzca el **Report name (Nombre del informe)**, el **Report destination (Destino del informe)** y las **Notes (Notas)**.
4. Para cada resultado de búsqueda, seleccione el fotograma que desee incluir en el informe. Para ampliar una imagen, haga doble clic en ella.

5. Haga clic en **Create (Crear)**. Cuando el informe esté listo, se le envía una notificación.

Exportar una búsqueda de matrícula como informe en CSV

Utilice esta función para recopilar un gran número de resultados de búsqueda como un informe en formato CSV.

1. Haga clic en **Export... (Exportar...)**.
2. Seleccione **CSV...**.
3. Elija un destino al que desea exportar el archivo.

Información de Axis

La información de Axis proporciona información general de los datos de los dispositivos mediante gráficos y paneles. De esta forma, se visualizan los metadatos de todos los dispositivos. Se pueden consultar datos sobre objetos detectados, vehículos identificados y alarmas. También puede crear nuevos paneles y compartirlos con otros usuarios.

La Información de Axis está disponible en las vistas predeterminadas de administrador y operador. La vista de administrador predeterminada en Axis Insights solo está disponible para usuarios con derechos de administrador, mientras que la vista de operador predeterminada está disponible para todos los operadores con los permisos correspondientes. Consulte *Configuración de los ajustes de función, on page 101*. La vista de operador facilita datos específicos de las vistas de cámara seleccionadas que haya configurado, mientras que la vista de administrador ofrece una visión general de todo el sistema.

Acceso a Axis Insights

- Vaya a **Smart Client** y haga clic en **Axis Insights**.
- **Dashboard (Panel de control)**: Seleccione un panel de control de la lista desplegable.
- **Vista de cámara**: Seleccione una vista de cámara específica para obtener una visión general de los datos.
- **Intervalo de tiempo**: Seleccione un intervalo de tiempo específico.
- **Auto update (Actualización automática)**: activar para actualizar los datos automáticamente.

••• El menú contextual contiene:

- **Edit dashboard (Editar panel)**: Editar, compartir o eliminar el panel de control.
- **Add chart (Añadir gráfico)**: Cree un nuevo gráfico en el panel de control.
- **About Axis Insights (Acerca de Axis Insights)**: Más datos sobre Axis Insights.

••• El menú contextual de cada gráfico contiene:

- **Maximize chart (Maximizar el gráfico)**: Haga clic para ampliar el gráfico.
- **Copy as image (Copiar como imagen)**: Haga clic para copiar el gráfico en el portapapeles.
- **Exportar**: Haga clic para exportar el gráfico como PNG o CSV.
- **Edit chart (Editar gráfico)**: Haga clic para editar el gráfico.
- **Remove chart (Retirar el gráfico)**: Haga clic para retirar el gráfico.

Nota

- Puede hacer clic en la cifra de algunos gráficos para obtener más información.
- : Muestra las selecciones específicas que se aplican a cada gráfico de su panel.

Crear un nuevo panel de control

1. **Dashboard (Panel de control)**: Seleccione **Add dashboard (Añadir panel de control)** en la lista desplegable.
2. Haga clic en **Empty (Vacío)** para crear un nuevo panel de control, o haga clic en **From existing dashboard (Desde panel de control existente)** para crear un panel de control similar a uno de los disponibles en el sistema.
3. **Name (Nombre)**: Introduzca un nombre para su panel de control.
4. **Allow other users to view this dashboard (Permitir a otros usuarios ver este panel de control)**: Haga clic para compartir su panel con otros usuarios en modo de solo lectura.
5. Haga clic en **Aplicar**.
6. **Add chart (Añadir gráfico)**: Haga clic para añadir un nuevo gráfico.
   - **Select chart type (Seleccionar tipo de gráfico)**: Seleccione el tipo de gráfico que desee y haga clic en **Next (Siguiente)**. Puede buscar un tipo de gráfico mediante etiquetas o títulos, como análisis de vídeo, vehículos, gráficos de líneas, etc.
   - **Modify data selections (Modificar selecciones de datos)**: Seleccionar filtros aplicables en cada categoría.
   - **Adjust appearance (Ajustar aspecto)**: Edite los y seleccione el tamaño del gráfico.

Configuración de la lista desplegable del panel de control

Nota

- Por defecto, solo puede ver los paneles que haya creado.

Para ver paneles compartidos por otros usuarios en la lista desplegable **Dashboard (Panel)**:

1. Vaya a **Shared dashboards (Paneles compartidos)**.
2. Active la selección de cada panel compartido que desee añadir a la lista desplegable.

Mostrar información detallada de una vista de cámara concreta

Al visualizar vídeo en directo y en reproducción en la vista de cámara, puede abrir Axis Insights con la vista de cámara activa preseleccionada.

Para abrir la información de Axis para la vista de una cámara concreta:

1. Vaya a **Smart Client** y abra una vista.
2. Haga clic **Show insights (Mostrar información)**.

Configurar la información de Axis

1. Compruebe si la cámara es compatible con Axis Object Analytics. Consulte las analíticas en el *selector de productos de Axis*.
2. Compruebe que la fecha y hora de la cámara están configuradas correctamente.
3. Asegúrese de que el dispositivo de metadatos está habilitado para las cámaras en el cliente de gestión.
4. Asegúrese de que el dispositivo de metadatos esté relacionado con la cámara:
   - Vaya a **Devices (Dispositivos)** > **Camera (Cámara)** y seleccione el dispositivo.
   - Vaya a la pestaña **Client (Cliente)** y asegúrese de que el dispositivo de metadatos de la cámara está seleccionado en **Related metadata (Metadatos relacionados)**.
5. Para ver consultar los datos disponibles en Axis Insights, habilite el análisis de escenas en su cámara a través de *AXIS Scene Metadata*:
   5.1. Vaya a **Devices (Dispositivos)** > **Metadata (Metadatos)** y seleccione el dispositivo.
      - Haga clic en **Record (Grabar)** y asegúrese de que **Recording (Grabación)** está habilitado.

- Haga clic en **Settings (Ajustes)** y asegúrese de que los **Analytics data (Datos de analíticas)** están habilitados.

5.1. Si está disponible, active **Consolidated metadata (Metadatos consolidados)** para que la carga más rápida. Consulte *Metadata and search, on page 107*.

6. Para habilitar los datos para tipos de gráficos utilizando *AXIS Object Analytics*, *AXIS Image Health Analytics* o *Environmental sensors (Sensores ambientales)*:
   - Vaya a **Devices (Dispositivos)** > **Metadata (Metadatos)** y seleccione el dispositivo.
   - Haga clic en **Record (Grabar)** y asegúrese de que **Recording (Grabación)** está habilitado.
   - Haga clic en **Settings (Ajustes)** y asegúrese de que los **Event data (Datos de eventos)** estén habilitados.
   - Le recomendamos crear una regla en el VMS para grabar siempre metadatos de este dispositivo.
7. Configuración de permisos para los grupos de seguridad:
   7.1. Vaya a **Site Navigation (Navegación de instalaciones)** > **Security (Seguridad)** > **Roles (Funciones)**.
   7.2. Seleccionar una función.
   7.3. Vaya a **Cameras (Cámaras)**. Seleccione **Read (Lectura)**.
   7.4. Vaya a **Metadata (Metadatos)**. Seleccione **Read (Lectura)**, **Live (Directo)** y **Playback (Reproducción)**.
8. Para agregar metadatos de matrículas a la información de Axis, consulte *Configurar matrículas de Axis, on page 60*

Solución de problemas en Axis Insights

Problema	Solución
Los gráficos se muestran "sin datos".	Debe configurar la información de Axis. Consulte *Configurar la información de Axis, on page 63*.
La vista del operador tarda mucho en cargarse.	• Reduzca el intervalo de tiempo. • Cree y utilice una vista de cámara con menos cámaras de análisis de escena. • Active los metadatos consolidados. Consulte *Metadata and search, on page 107*.

Dewarping del vídeo

La corrección esférica corrige la perspectiva de una imagen distorsionada geométricamente cuando se usa un objetivo gran angular u ojo de pez. La corrección esférica de Axis en el sistema de gestión de vídeo (VMS) se puede utilizar con cualquier cámara panorámica Axis de 360°. La corrección esférica se lleva a cabo directamente en la cámara o en Smart Client.

Más detalles sobre la corrección esférica:

- Cuando se utiliza la corrección esférica de cliente, se obtiene una corrección suave tanto en los vídeos en directo como durante las grabaciones.
- Cuando regresa a una vista, va automáticamente a la última ubicación con corrección esférica.
- La corrección esférica se incluye al exportar vídeos.
- Puede guardar una posición de inicio, consulte *Definir una posición de inicio, on page 67*.
- Es posible la configuración si los operadores tienen permiso para controlar y editar las vistas con corrección esférica, consulte *Permitir a los operadores controlar y editar vistas con corrección esférica, on page 68*.

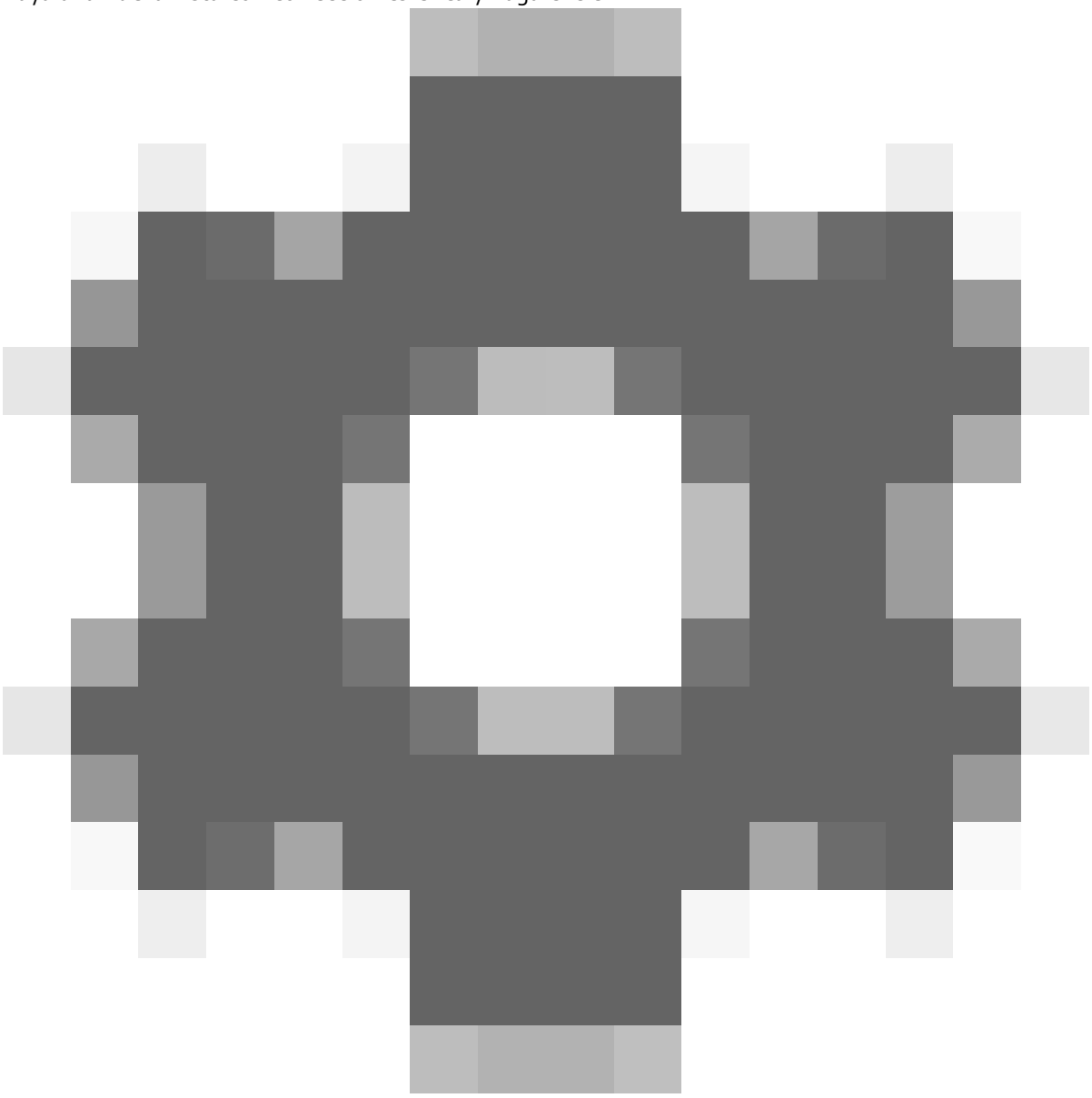
Crear una vista con corrección esférica



Nota

Para optimizar la corrección esférica en el flujo, seleccione la resolución máxima disponible para **Video stream 1 (Flujo de vídeo 1)** de la **Camera 1 (Cámara 1)** en Management Client (Management Client). Para obtener más información, consulte *Rendimiento y solución de problemas, on page 68*.

1. Abra Smart Client y haga clic en **Setup (Configuración)**.
2. Vaya a **Views (Vistas)**.
3. Haga clic en **Create new view (Crear nueva vista)** y seleccione un formato.
4. Vaya a **System overview > AXIS Optimizer (Información general del sistema > AXIS Optimizer)**.
5. Haga clic en **Dewarping view (Vista con corrección esférica)** y arrástrela a la vista.
6. Seleccione una cámara y su posición de montaje actual.
7. Haga clic en **Setup (Configuración)**.

8. Vaya a la nueva vista con corrección esférica y haga clic en .
9. Haga clic en **Set view type (Establecer tipo de vista)** y seleccione una opción. En función de cómo se monte la cámara, puede seleccionar entre **Quad**, **Normal**, **Normal with overview (Normal con vista general)** o **Panorama (Panorámica)**.

Nota

Recomendamos utilizar el 100 % de DPI. Si la resolución es distinta del 100 %, es posible que la corrección esférica Axis no sea del todo visible en el segundo monitor.

Si utiliza otra configuración de DPI, es posible que las ventanas con corrección esférica solo sean visibles parcialmente. Siga las instrucciones de estos artículos externos para solucionar el problema:

- *Problemas con XProtect en monitores de alta resolución (4K y superiores)*
- *Escalado de la interfaz gráfica de usuario en monitores con alta densidad de DPI*

Crear una vista con corrección esférica para cámaras panorámicas multisensor

Puede utilizar vistas con corrección esférica con cámaras panorámicas multisensor, por ejemplo, con cámaras AXIS P3807-PVE Network Camera y AXIS Q3819-PVE Panoramic Camera.

- Puntos de unión de cliente. Si la cámara está configurada en modo de captura client dewarp (corrección esférica de cliente), AXIS Optimizer realiza la unión de las cuatro imágenes en una única panorámica sin cortes (solo AXIS P3807-PVE).
- Ajuste del horizonte. Es posible ajustar el horizonte de la panorámica. Esto puede ser aconsejable si la cámara está inclinada hacia el suelo y el horizonte terrestre está curvado. La acción también permite que el control virtual PTZ sea más intuitivo.
- Control PTZ. Permite hacer zoom y desplazarse por la imagen como si fuera una cámara PTZ.



Nota

Requisitos

- Usuarios con alguno de los siguientes derechos de usuario:
  - Función de optimización
  - Hardware > Driver commands = Allow (Hardware > Comandos del controlador = Permitir)
- Una cámara panorámica multisensor Axis

1. Si procede, configure el modo de captura **Client Dewarp (Corrección esférica de cliente)** durante la configuración inicial del dispositivo.
2. Abra Smart Client y haga clic en **Setup (Configuración)**.
3. Vaya a **Views (Vistas)**.
4. Haga clic en **Create new view (Crear nueva vista)** y seleccione un formato.
5. Vaya a **System overview > AXIS Optimizer (Información general del sistema > AXIS Optimizer)**.
6. Haga clic en **Dewarping view (Vista con corrección esférica)** y arrástrela a la vista.
7. Seleccione una cámara panorámica multisensor.
   La primera vez que añada la cámara panorámica multisensor a una vista con corrección esférica, va a aparecer una ventana de calibración del horizonte sobre la vista.
8. Haga clic en las flechas para que la línea roja se alinee con el horizonte terrestre.
9. Haga clic en **Done (Hecho)** para guardar los ajustes y salir del modo de calibración.

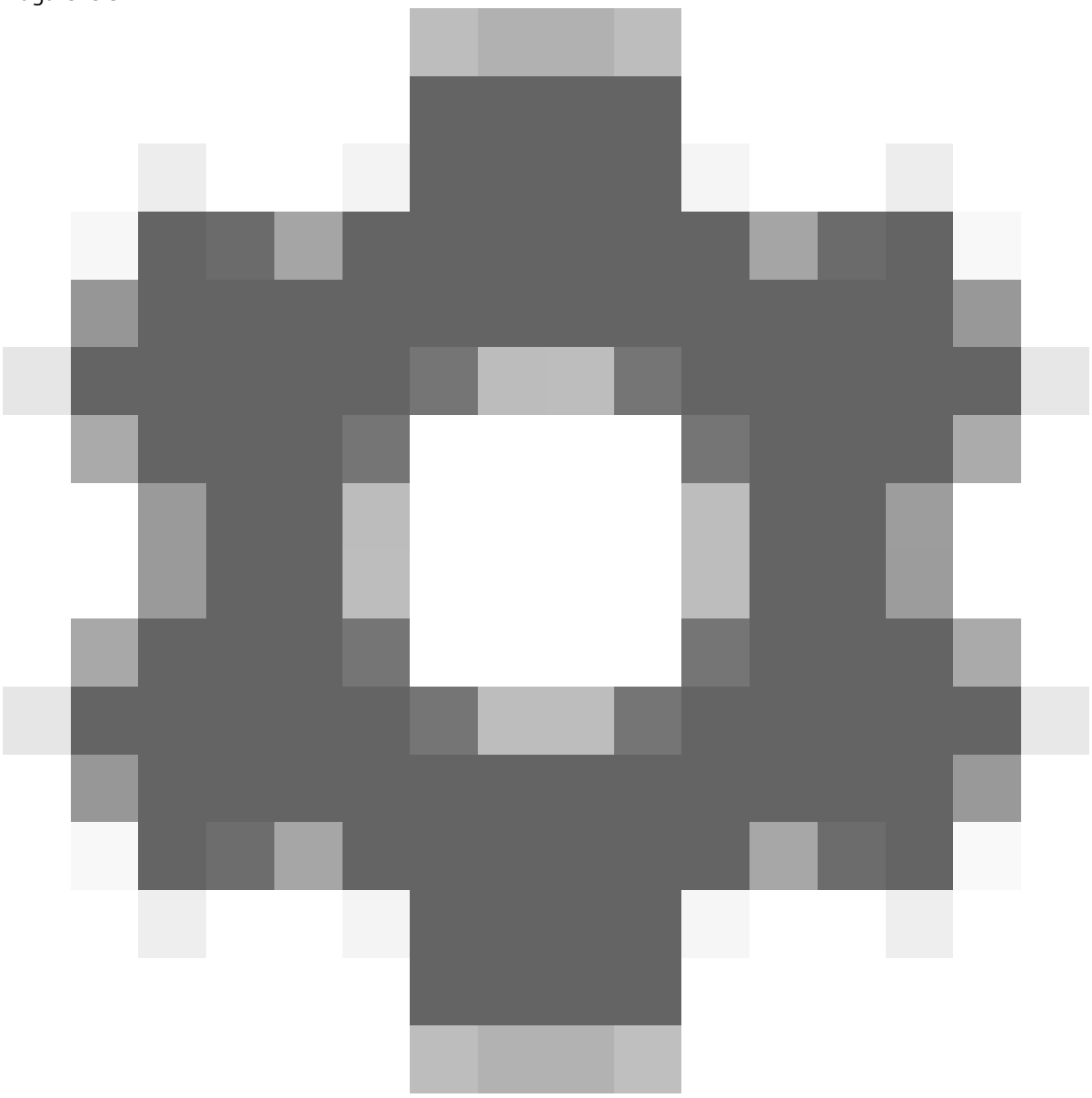
Gran angular

La vista gran angular es un tipo de vista para cámaras panorámicas multisensor. Active **wide view (gran angular)** si el campo de visión normal de 120° no es suficiente. Con gran angular, la imagen siempre tendrá corrección de distorsión. Apagie**wide view (gran angular)** para obtener una transición a la vista normal cuando se aleja por completo.

Definir una posición de inicio

1. En Smart Client, abra una vista con corrección esférica.
2. Vaya a la posición que desee guardar como posición de inicio.

3. Haga clic en



y, a continuación, en **Set home position (Establecer posición de inicio)**.

Permitir a los operadores controlar y editar vistas con corrección esférica

Es posible la configuración si los operadores pueden tener permiso para controlar y editar las vistas con corrección esférica, consulte *Personalizar el acceso a características de los operadores, on page 101*.

Rendimiento y solución de problemas

Consideraciones sobre el rendimiento

- La corrección esférica de vídeo de Axis se lleva a cabo en la GPU, cuando es posible, pero también supone una importante carga para la CPU.
- Para evitar que la velocidad de los fotogramas caiga en el caso de imágenes amplias que demanden mucha corrección esférica, tenga en cuenta lo siguiente:
  - resolución de la cámara. Una cámara con una alta resolución, por ejemplo de 2880 x 2880, demanda una gran cantidad de recursos por parte del ordenador en comparación con, por ejemplo, una resolución de 1920 x 1920.
  - Velocidad de fotogramas de la cámara. Si no necesita una velocidad de fotogramas alta, cambiar a una velocidad más baja puede evitar tirones en la vista de corrección esférica y en otras.

– Supervisión de la resolución. Los monitores de alta resolución, por ejemplo 4K, demandan muchos recursos al reproducir vídeos. Si no es necesaria la resolución más alta, una resolución de monitor más baja permite ejecutar un mayor número de vistas con corrección esférica sin sufrir tirones.

Resolución dinámica

- El flujo de vídeo se reduce automáticamente, cuando es posible, sin disminución de la calidad de vídeo. Esto puede mejorar el rendimiento de las vistas con corrección esférica.
- Si experimenta parpadeos al hacer zoom desde la vista general, puede ayudar el hecho que se desactive la resolución dinámica.
- Para activar o desactivar la resolución dinámica: en Smart Client, vaya a **Settings (Ajustes) > Axis dewarping options (Opciones de corrección esférica de Axis) > Rendering options (Opciones de renderizado)** y seleccione o borre **Dynamic resolution (Resolución dinámica)**.
- **La resolución dinámica** está activada de forma predeterminada.

Renderizado de compatibilidad

- Si hay algún error visual en la vista con corrección esférica, por ejemplo, imagen negra, o el rendimiento parece peor de lo esperado, active el renderizado de compatibilidad. Tenga en cuenta que un efecto negativo del renderizado de compatibilidad es que las transiciones entre las vistas y el desplazamiento durante la reproducción pueden parpadear.
- Para activar o desactivar el renderizado de compatibilidad: abra Smart Client y vaya a **Settings (Ajustes) > Axis dewarping options (Opciones de corrección esférica de Axis) > Rendering options (Opciones de renderizado)** y seleccione o borre **Use compatibility rendering (Usar renderizado de compatibilidad)**.
- **Usar renderizado de compatibilidad** está desactivado de forma predeterminada.

Qué esperar

En un sistema de referencia equipado con un procesador Intel i7 8700, una tarjeta NVIDIA Gefore 1050 GTX y tres monitores de 1920x1080 puede esperar:

- la ejecución de 7 vistas con corrección esférica a una resolución de 1920 x 1920 y 25 imágenes por segundo, sin caída de fotogramas, o
- 4 vistas con corrección esférica a una resolución de 2880 x 2880 y 25 imágenes por segundo

Si uno de los tres monitores se ejecuta en resolución 4K en lugar de 1920 x 1080, puede esperar:

- la ejecución de 5 vistas con corrección esférica, a una resolución de 1920 x 1920 y 25 imágenes por segundo sin caída de fotogramas, o
- 3 vistas con corrección esférica, a una resolución de 2880 x 2880 y 25 imágenes por segundo. Una vista con corrección esférica en cada monitor.

Las escalas de velocidad de fotogramas y de resolución son lineales. Un ordenador que puede ejecutar 5 vistas con corrección esférica a 30 imágenes por segundo, puede ejecutar 10 vistas si se reduce la velocidad de fotogramas a 15 imágenes por segundo.

Integración para uso en el cuerpo

AXIS Optimizer Body Worn Extension permite a los usuarios de cámaras de campo grabar, etiquetar y compartir vídeos con los investigadores de las oficinas, quienes pueden buscar y gestionar las pruebas de vídeo utilizando el VMS. El servicio permite la conexión y la transferencia segura entre el sistema Axis Body Worn y el VMS. AXIS Body Worn Extension es un servicio gratuito e independiente que debe instalarse en el servidor de grabación.

Nota

Las versiones compatibles son:

- Versión del VMS 2020 R1 Corporate o versiones posteriores
- Versión del VMS 2020 R1 Professional+ o versiones posteriores
- Versión del VMS 2020 R1 Expert o versiones posteriores

Utilice siempre las últimas revisiones del VMS y los instaladores de parches acumulativos.

Descubrir más

- Para descargar el servicio o leer la guía de implementación y la nota informativa, vaya a *axis.com*.
- Para consultar el manual del usuario, vaya a *axis.help.com*.

Control de acceso

El control de acceso es una solución que combina el control de acceso físico con la videovigilancia. Esta integración permite configurar un sistema de control de acceso Axis directamente desde Management Client. El sistema se integra perfectamente con XProtect, permitiendo a los operadores supervisar el acceso y realizar acciones de control de acceso en Smart Client.

Nota

Requisitos

- Versión de VMS 2024 R1 o posterior.
- Licencias de acceso a XProtect; consulte *access licenses (licencias de acceso)*.
- Instale AXIS Optimizer en el servidor de eventos y en Management Client.

Los puertos 53459 y 53461 se abrirán al tráfico entrante (TCP) durante la instalación de AXIS Optimizer a través de AXIS Secure Entry.

Para utilizar puertas en AXIS Secure Entry, necesita obtener una licencia por puerta; consulte *Activar licencias de puerta, on page 72*.

Configuración de control de acceso

Nota

Antes de empezar, haga lo siguiente:

- Actualice el software del controlador de puerta. Consulte en la siguiente tabla la versión mínima y recomendada de AXIS OS para su versión de VMS.
- Asegúrese de que la fecha y la hora sean correctas.

Versión de AXIS Optimizer	Versión mínima de AXIS OS	Versión recomendada de AXIS OS
6.0	12.6.94.1	12.10.73.4
5.8	12.6.94.1	12.8.55.1
5.6	12.6.94.1	12.6.94.1

Añadir un controlador de puerta de red Axis a su sistema

1. Vaya a **Site Navigation (Navegación del sitio)** > **AXIS Optimizer** > **Access control (Control de acceso)**.
2. En **Configuration (Configuración)**, seleccione **Devices (Dispositivos)**.
3. Seleccione **Discovered devices (Dispositivos detectados)** para consultar la lista de unidades que puede añadir al sistema.
4. Seleccione las unidades que desee añadir.
5. Haga clic en **+ Add (+ Añadir)** en la ventana emergente y facilite las credenciales del controlador.

Nota

- Debería ver los controladores añadidos en la pestaña **Management (Gestión)**.
- Para añadir manualmente un controlador al sistema, haga clic en **+ Add (+Añadir)** en la pestaña **Management (Gestión)**.
- Para integrar la actualización en el VMS al añadir, eliminar o editar el nombre de un controlador de puerta:
  - Vaya a **Site Navigation (Navegación de instalaciones)** > **Access control (Control de acceso)** y haga clic en la integración del Control de acceso.
  - Haga clic en **Refresh Configuration (Actualizar configuración)** en la pestaña **General settings (Ajustes generales)**

Activar licencias de puerta

Antes de poder añadir puertas, debe activar las licencias que tiene en su sistema.

1. En **Site Navigation (Navegación por la instalación)**, vaya a **License Information (Información sobre licencias)**.
2. Haga clic en **Activate License Manually (Activar licencia manualmente)** y seleccione **Online** u **Offline**.
3. Para activar las licencias de puerta online:
   – Introduzca su nombre de usuario y contraseña.
4. Para activar licencias de puerta offline, consulte *activate licenses offline (activar licencias offline)*.

Si necesita ajustar el número de licencias de puerta que se activarán:

1. Vaya a **AXIS Optimizer** > **Access control (Control de acceso)**.
2. En **Configuration (Configuración)**, seleccione **Devices (Dispositivos)**.
3. Vaya a **Allocated door licenses (Licencias de puerta asignadas)** > **Custom license allocation (Asignación de licencias personalizadas)** e introduzca el número de licencias de puerta que desea utilizar.
4. Haga clic en **Aplicar**.
5. Vaya a Go to **License Information (Información sobre licencias)** y reactive sus licencias.

Configure el control de acceso

1. Vaya a **Site Navigation (Navegación del sitio)** > **AXIS Optimizer** > **Access control (Control de acceso)**.
2. Para editar los perfiles de identificación predefinidos o crear un nuevo perfil de identificación, consulte *Perfiles de identificación, on page 88*.
3. Para utilizar una configuración personalizada para los formatos de tarjeta y la longitud del PIN, consulte *Formatos de tarjeta y PIN, on page 85*.
4. Agregue una puerta y aplique un perfil de identificación a la puerta. Consulte *Agregar una puerta, on page 75*.
5. Agregue una zona y agregue puertas a la zona. Consulte *Agregar una zona, on page 82*.

Compatibilidad de software de dispositivos para controladores de puerta

Importante

Tenga en cuenta lo siguiente cuando actualice el sistema operativo AXIS OS en su controlador de puerta:

- **Supported AXIS OS versions (Versiones del AXIS OS compatibles):** las versiones indicadas solo se aplican cuando se actualiza desde su versión original recomendada de VMS y cuando el sistema tiene una puerta. Si el sistema no reúne estas condiciones, debe actualizarse a la versión de AXIS OS recomendada para la versión específica de VMS.
- **Minimum supported AXIS OS version (Versión mínima del AXIS OS compatible):** la versión de AXIS OS más antigua instalada en el sistema determina la versión del AXIS OS mínima compatible, con un límite de dos versiones anteriores. Supongamos que está utilizando AXIS Optimizer versión 6.0 y actualiza todos los dispositivos a la versión recomendada del AXIS OS, la 12.10.73.4. A partir de ahora, la versión 12.6.94.1 del AXIS OS será la versión mínima compatible con tu sistema.
- **Upgrading beyond recommended AXIS OS version (Actualización a una versión del AXIS OS superior a la recomendada):** supongamos que se actualiza a una versión del AXIS OS superior a la recomendada para una versión concreta de VMS. Después, siempre puede regresar a la versión de AXIS OS recomendada sin ningún problema, siempre y cuando esté dentro de los límites de soporte técnico establecidos para la versión de VMS.
- **Future AXIS OS recommendations (Recomendaciones futuras del AXIS OS):** siga siempre la versión del AXIS OS recomendada para la versión correspondiente de VMS para garantizar la estabilidad del sistema y una compatibilidad total.

Integración del control de acceso

Para integrar el control de acceso en el VMS:

1. Vaya a **Site Navigation (Navegación de instalaciones)** > **Access control (Control de acceso)**.
2. Haga clic con el botón derecho en **Access control (Control de acceso)** y haga clic en **Create new... (Crear nuevo...)**.
3. En el cuadro de diálogo **Create Access Control System Integration (Crear integración de sistemas de control de acceso)**:
   - Introduzca un nombre para la integración.
   - Seleccione **AXIS Secure Entry** en el menú desplegable de **Integration plug-in (Complemento de integración)**.
   - Haga clic en **Next (Siguiente)** hasta que observe el cuadro de diálogo **Associate cameras (Asociar cámaras)**.
     Para asociar cámaras a puntos de acceso de puertas:
     - Haga clic en **Cameras (Cámaras)** en su dispositivo para consultar la lista de cámaras configuradas en el sistema XProtect.
     - Seleccionar y arrastrar una cámara al punto de acceso al que desea asociarla.
     - Haga clic en **Close (Cerrar)** para cerrar el cuadro de diálogo.

Nota

- Para obtener más información sobre la integración del control de acceso en XProtect, consulte *Using access control in XProtect Smart Client (Usar el control de acceso en XProtect Smart Client)*.
- Para obtener más información sobre las propiedades de control de acceso, como la configuración general, las puertas y las cámaras asociadas, los eventos de control de acceso, etc., consulte *Access control properties (Propiedades del control de acceso)*.

Puertas y zonas

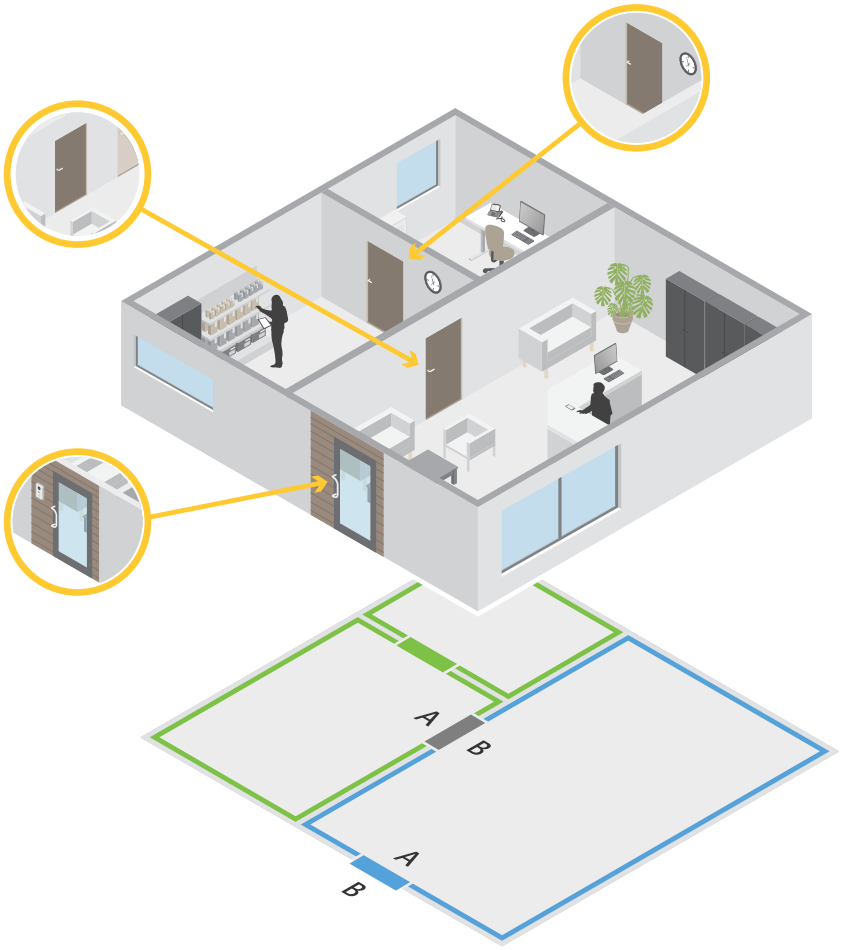
Vaya a **Site Navigation (Navegación del sitio)** > **AXIS Optimizer** > **Access control (Control de acceso)** > **Doors and zones (Puertas y zonas)** para obtener una visión general y configurar puertas y zonas.

Gráfico de PIN	Ver el gráfico de pines del controlador asociado a una puerta. Si desea imprimir el gráfico de pines, haga clic en **Print (Imprimir)**.
Perfil de identificación	Cambie el perfil de identificación en las puertas.
Canal seguro	Active o desactive OSDP Secure Channel para un lector específico.

Puertas	
Nombre	El nombre de la puerta.
Controlador de puerta	El controlador de puerta conectado a la puerta.
Lado A	La zona en la que está el lado A de la puerta.
Cara B	La zona en la que está el lado B de la puerta.
Perfil de identificación	Perfil de identificación aplicado a la puerta.
Formatos de tarjeta y PIN	Muestra el tipo de formatos de tarjeta o la longitud del PIN.
Estado	Estado de la puerta.

	• **Online (En línea):** La puerta está en línea y funciona correctamente. • **Reader offline (Lector sin conexión):** El lector de la configuración de puerta no tiene conexión. • **Reader error (Error del lector):** El lector de la configuración de puerta no admite canal seguro o el canal seguro no está activado para el lector.
Zonas	
Nombre	Nombre de la zona.
Número de puertas	El número de puertas incluidas en la zona.

Ejemplo de puertas y zonas



- Existen dos zonas: zona verde y zona azul.
- Hay tres puertas: puerta verde, puerta azul y puerta marrón.
- La puerta verde es una puerta interna de la zona verde.
- La puerta azul es una puerta perimetral solo para la zona azul.
- La puerta azul es una puerta perimetral para la zona verde y la zona azul.

Agregar una puerta

Nota

- Puede configurar un controlador de puerta con una puerta que tenga dos cerraduras o dos puertas que tengan una cerradura cada una.
- Si un controlador de puerta no tiene puertas y está utilizando una nueva versión de Axis Optimizer con un software más antiguo en el controlador de la puerta, el sistema le impedirá añadir una puerta. Sin embargo, el sistema admite puertas nuevas en los controladores del sistema con software anterior si ya hay una puerta existente.

Cree una nueva configuración de puerta para agregar una puerta:

1. Vaya a **Site Navigation (Navegación de instalaciones)** > **AXIS Optimizer** > **Access control (Control de acceso)** > **Doors and zones (Puertas y zonas)**.
2. Haga clic en **Add door (Agregar puerta)**.
3. Escriba un nombre de puerta.
4. En el menú desplegable **Controller (Controlador)**, seleccione un controlador de puerta. El controlador aparece en gris cuando no se puede agregar otra puerta, cuando está sin conexión o si HTTPS no está activo.
5. En el menú desplegable **Door type (Tipo de puerta)**, seleccione el tipo de puerta que desee crear.
6. Haga clic en **Next (Siguiente)** para ir a la página de configuración de la puerta.
7. En el menú desplegable **Primary lock (Cerradura principal)**, seleccione un puerto de relé.
8. Para configurar dos cerraduras en la puerta, seleccione un puerto de relé del menú desplegable **Secondary lock (Cerradura secundaria)**.
9. Seleccione un perfil de identificación. Consulte *Perfiles de identificación, on page 88*.
10. Configure los ajustes de puerta. Consulte *Ajustes de puerta, on page 76*.
11. Configure una puerta de supervisión. Consulte *Agregar una puerta de supervisión, on page 79*.
12. Haga clic en **Save (Guardar)**.

Copie una configuración de puerta existente para agregar una puerta:

1. Vaya a **Site Navigation (Navegación de instalaciones)** > **AXIS Optimizer** > **Access control (Control de acceso)** > **Doors and zones (Puertas y zonas)**.
2. Haga clic en **Add door (Agregar puerta)**.
3. Escriba un nombre de puerta.
4. En el menú desplegable **Controller (Controlador)**, seleccione un controlador de puerta.
5. Haga clic en **Next (Siguiente)**.
6. En el menú desplegable **Copy configuration (Copiar configuración)**, seleccione una configuración de puerta existente. Muestra las puertas conectadas y el controlador aparece en gris si se ha configurado con dos puertas o una puerta con dos cerraduras.
7. Cambie los ajustes si lo desea.
8. Haga clic en **Save (Guardar)**.

Para editar una puerta:

1. Vaya a **Site Navigation (Navegación del sitio)** > **AXIS Optimizer**> **Access control (Control de acceso)** > **Doors and zones (Puertas y zonas)** > **Doors (Puertas)**.
2. Seleccione una puerta en la lista.
3. Haga clic en **Edit (Modificar)**.

4. Cambie los ajustes y haga clic en **Save (Guardar)**.

Para eliminar una puerta:

1. Vaya a **Site Navigation (Navegación del sitio)** > **AXIS Optimizer**> **Access control (Control de acceso)** > **Doors and zones (Puertas y zonas)** > **Doors (Puertas)**.
2. Seleccione una puerta en la lista.
3. Haga clic en **Remove (Eliminar)**.
4. Haga clic en **Yes (Sí)**.

Para integrar la actualización en el VMS al añadir, eliminar o editar el nombre de una puerta:

1. Vaya a **Site Navigation (Navegación de instalaciones)** > **Access control (Control de acceso)** y haga clic en la integración del Control de acceso.
2. Haga clic en **Refresh Configuration (Actualizar configuración)** en la pestaña **General settings (Ajustes generales)**

Ajustes de puerta

1. Vaya a **Site Navigation (Navegación de instalaciones)** > **AXIS Optimizer** > **Access control (Control de acceso)** > **Doors and zones (Puertas y zonas)**.
2. Seleccione la puerta que desea editar.
3. Haga clic en **Edit (Modificar)**.

Tiempo de acceso (s)	Establece el número de segundos que la puerta permanece desbloqueada una vez se concedió permiso de acceso. La puerta permanece desbloqueada hasta que la puerta se abra o hasta que termine el tiempo establecido. La puerta se bloquea cuando se cierra aunque haya tiempo de acceso.
Open-too-long time (sec) [Tiempo de apertura demasiado largo (s)]	Solo es válido si ha configurado un monitor de puerta. Defina el número de segundos que permanece abierta la puerta. Si la puerta está abierta cuando termina el tiempo establecido, activa la alarma de puerta abierta durante demasiado tiempo. Configure una regla de acción para determinar qué acción activa el evento de puerta abierta durante demasiado tiempo.
Tiempo de acceso largo (seg)	Establece el número de segundos que la puerta permanece desbloqueada una vez se concedió permiso de acceso. El tiempo de acceso largo anula el tiempo de acceso para los titulares de tarjeta que tienen estos ajustes activados.
Long open-too-long time (sec) [Tiempo largo de apertura demasiado larga (s)]	Solo es válido si ha configurado un monitor de puerta. Defina el número de segundos que permanece abierta la puerta. Si la puerta está abierta cuando termina el tiempo establecido, activa el evento de puerta abierta durante demasiado tiempo. El tiempo de apertura demasiado largo sobrescribe el tiempo de apertura demasiado largo ya establecido para los titulares de tarjeta si activa los ajustes de **Tiempo de acceso largo**.

Tiempo antes de nuevo bloqueo (ms)	Defina el tiempo, en milisegundos, durante el que la puerta debe permanecer desbloqueada después de abrirse o cerrarse.
Volver a bloquear	• **After opening (Tras la apertura):** solo es válido si ha añadido un monitor de puerta. • **After closing (Tras el cierre):** solo es válido si ha añadido un monitor de puerta.

Nivel de seguridad de puerta

Puede agregar las siguientes características de seguridad a la puerta:

Regla de dos personas – La regla de dos personas requiere que dos personas utilicen una credencial válida para acceder.

Doble deslizamiento – El doble deslizamiento permite que un titular de tarjeta invalide el estado actual de una puerta. Por ejemplo, pueden utilizarla para bloquear o desbloquear una puerta fuera de la programación habitual, lo que es más cómodo que entrar en el sistema para desbloquear la puerta. El barrido doble no afecta a una programación ya existente. Por ejemplo, si una puerta se va a bloquear a la hora de cierre y los empleados se van a un receso para el almuerzo, la puerta se seguirá bloqueando según la programación.

Puede configurar el nivel de seguridad mientras agrega una zona puerta o puede hacerlo en una puerta existente.

Para agregar **una regla de dos personas** a una puerta existente:

1. Vaya a **Site Navigation (Navegación de instalaciones)** > **AXIS Optimizer** > **Access control (Control de acceso)** > **Doors and zones (Puertas y zonas)**.
2. Seleccione la puerta para la que desea configurar un nivel de seguridad.
3. Haga clic en **Edit (Modificar)**.
4. Haga clic en **Security level (Nivel de seguridad)**.
5. Active la **regla de dos personas**.
6. Haga clic en **Aplicar**.

Regla de dos personas	
Lateral A y **Lateral B**	Seleccione los lados de la puerta en los que utilizar la regla.
Horarios	Seleccione cuándo está activa la regla.
Tiempo de espera (segundos)	El tiempo de espera es el tiempo máximo permitido entre los barridos de tarjeta u otro tipo de credencial válida.

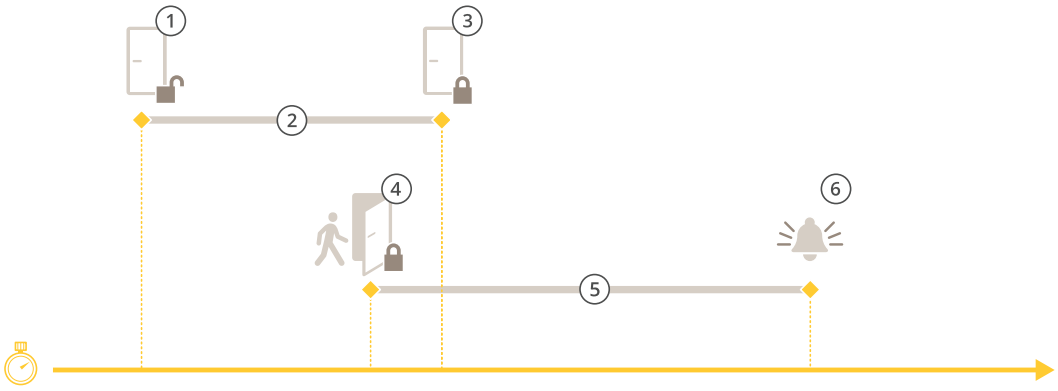
Para añadir un **doble deslizamiento** a una puerta existente:

1. Vaya a **Site Navigation (Navegación de instalaciones)** > **AXIS Optimizer** > **Access control (Control de acceso)** > **Doors and zones (Puertas y zonas)**.
2. Seleccione la puerta para la que desea configurar un nivel de seguridad.
3. Haga clic en **Edit (Modificar)**.
4. Haga clic en **Security level (Nivel de seguridad)**.
5. Active el **barrido doble**.
6. Haga clic en **Aplicar**.

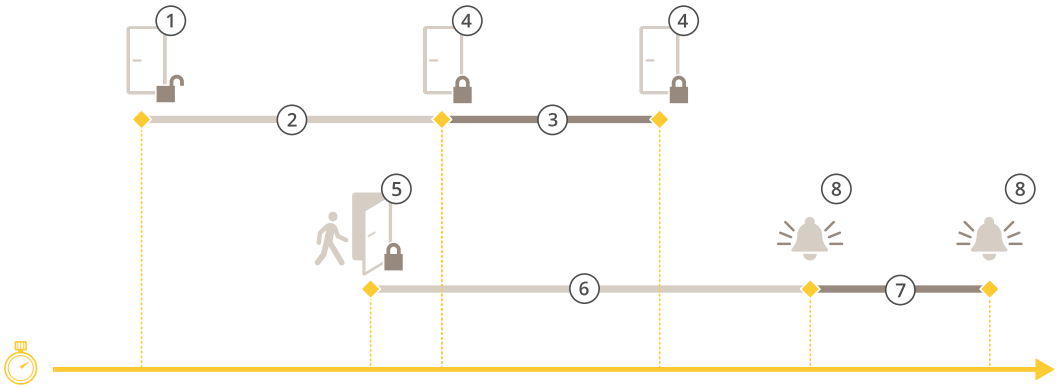
7. Aplique un **barrido doble** al titular de la tarjeta.
   7.1. Vaya a **Cardholder management (Gestión de titulares de tarjeta)**.
   7.2. Seleccione el titular de tarjeta que desea editar y haga clic en **Edit (Editar)**.
   7.3. Haga clic en **Avanzado**.
   7.4. Seleccione **Allow double-swipe (Permitir doble barrido)**.
   7.5. Haga clic en **Save (Guardar)**.

Doble deslizamiento	
Tiempo de espera (segundos)	El tiempo de espera es el tiempo máximo permitido entre los barridos de tarjeta u otro tipo de credencial válida.

Opciones de hora



1 Acceso concedido: desbloquea las cerraduras
2 Tiempo de acceso
3 Ninguna acción realizada: bloquea las cerraduras
4 Acción realizada (puerta abierta): bloquea las cerraduras o las mantiene desbloqueadas hasta que se cierre la puerta
5 Tiempo de apertura demasiado largo
6 La alarma de tiempo de apertura demasiado largo se desactiva



1 Acceso concedido: desbloquea las cerraduras
2 Tiempo de acceso
3 2+3: Tiempo de acceso largo
4 Ninguna acción realizada: bloquea las cerraduras

5 Acción realizada (puerta abierta): bloquea las cerraduras o las mantiene desbloqueadas hasta que se cierre la puerta
6 Tiempo de apertura demasiado largo
7 6+7: Tiempo de apertura demasiado largo
8 La alarma de tiempo de apertura demasiado largo se desactiva

Agregar un monitor de puerta

Un monitor de puerta es un interruptor de posición de puerta que supervisa el estado físico de una puerta. Puede agregar un monitor de puerta a la puerta y configurar cómo conectar el monitor de puerta.

1. Vaya a la página de configuración de la puerta. Consulte *Agregar una puerta, on page 75*
2. En **Sensors (Sensores)**, haga clic en **Add (Agregar)**.
3. Seleccione el **Door position sensor (Sensor de posición de puerta)**.
4. Seleccione el puerto de E/S al que desea conectar el monitor de puerta.
5. En **Door open if (Abrir puerta si)**, seleccione cómo están conectados los circuitos del monitor de puerta.
6. Para ignorar los cambios de estado antes de entrar en un nuevo estado estable, establezca un **Debounce time (Tiempo antirrebote)**.
7. Para activar un evento cuando se produce una interrupción en la conexión entre el controlador de puerta y el monitor de puerta, active **Supervised input (Entrada supervisada)**. Consulte *Entradas con supervisión, on page 83*.

Puerta abierta si	
Circuito abierto	El circuito de monitor de puerta está normalmente cerrado. El monitor de puerta envía la señal de una puerta abierta cuando el circuito está abierto. El monitor de puerta envía la señal de una puerta cerrada cuando el circuito está cerrado.
Circuito cerrado	El circuito de monitor de puerta está normalmente abierto. El monitor de puerta envía la señal de una puerta abierta cuando el circuito está cerrado. El monitor de puerta envía la señal de una puerta cerrada cuando el circuito está abierto.

Agregar una puerta de supervisión

Una puerta de supervisión es un tipo de puerta que muestra si está abierto o cerrado. Por ejemplo, puede utilizar esta opción en una puerta de seguridad contra incendios que no requiere un bloqueo pero en la que debe saber si la puerta está abierta.

Una puerta de supervisión es distinta de una puerta regular con un monitor de puerta. Una puerta regular con un monitor de puerta admite bloqueos y lectores, pero requiere un controlador de puerta. Una puerta de supervisión admite un sensor de posición de puerta pero solo requiere un módulo de relé de E/S de red conectado a un controlador de puerta. Puede conectar hasta cinco sensores de posición de puerta a un módulo de relé de E/S de red.

Nota

Una puerta de supervisión requiere un AXIS A9210 Network I/O Relay Module con el software más reciente como la aplicación de la ACAP de la puerta de supervisión de AXIS.

Para configurar una puerta de supervisión:

1. Instale AXIS A9210 y actualícelo con la versión más reciente de AXIS OS.
2. Instale los sensores de posición de puerta.

3. En el VMS, vaya a **Site Navigation (Navegación de instalaciones)** > **AXIS Optimizer** > **Access control (Control de acceso)** > **Doors and zones (Puertas y zonas)**.
4. Haga clic en **Add door (Agregar puerta)**.
5. Introduzca un nombre.
6. En **Type (Tipo)**, seleccione **Monitoring door (Puerta de supervisión)**.
7. En **Device (Dispositivo)**, seleccione el módulo de relé de E/S de red.
8. Haga clic en **Next (Siguiente)**.
9. En **Sensors (Sensores)**, haga clic en **+ Add (+ Agregar)** y seleccione **Door position sensor (Sensor de posición de puerta)**.
10. Seleccione la E/S que está conectada al sensor de posición de puerta.
11. Haga clic en **Add (Añadir)**.

Agregar un lector

Puede configurar un controlador de puerta para utilizar dos lectores cableados. Seleccione agregar un lector a un lado o a ambos lados de una puerta.

Si aplica una configuración personalizada de formatos de tarjeta o longitud de PIN a un lector, puede verlo en **Card formats (Formatos de tarjeta)** en **Configuration > Access control > Doors and zones (Configuración > Control de acceso > Puertas y zonas)**. Consulte *Puertas y zonas, on page 73*.

1. Vaya a la página de configuración de la puerta. Consulte *Agregar una puerta, on page 75*.
2. En un lado de la puerta, haga clic en **Add (Agregar)**.
3. Seleccione **Card reader (Lector de tarjetas)**.
4. Seleccione el **Reader type (Tipo de lector)**.
5. Para utilizar una configuración de longitud de PIN personalizada para este lector.
   5.1. Haga clic en **Avanzado**.
   5.2. Active **Custom PIN length (Longitud de PIN personalizada)**.
   5.3. Establezca **Min PIN length (Longitud mínima de PIN)**, **Max PIN length (Longitud máxima de PIN)** y **End of PIN character (Carácter final de PIN)**.
6. Para utilizar un formato de tarjeta personalizado para este lector.
   6.1. Haga clic en **Avanzado**.
   6.2. Active **Custom card formats (Formatos de tarjeta personalizados)**.
   6.3. Seleccione los formatos de tarjeta que desee utilizar para el lector. Si ya se está utilizando un formato de tarjeta con la misma longitud de bits, debe desactivarlo primero. Un icono de advertencia se muestra en el cliente cuando la configuración del formato de tarjeta es distinta de la configuración del sistema configurada.
7. Haga clic en **Add (Añadir)**.
8. Para agregar un lector al otro lado de la puerta, vuelva a realizar este procedimiento.

Tipo de lector	
OSDP RS485 half-duplex	Para lectores RS485, seleccione **OSDP RS485 half duplex (OSDP RS485 half-duplex)** y un puerto de lector.
Wiegand	Para lectores que utilizan protocolos Wiegand, seleccione **Wiegand (Wiegand)** y un puerto de lector.

Wiegand	
Control de LED	Seleccione **Single wire (Cable simple)** o **Cable dual (R/G)**. Los lectores con control de led dual utilizan diferentes cables para los LED rojo y verde.
Alerta de manipulación	Seleccione si la entrada de manipulación del lector está activa. • **Open circuit (Circuito abierto)**: El lector envía la señal de manipulación de puerta cuando el circuito está abierto. • **Circuito cerrado**: El lector envía la señal de manipulación de puerta cuando el circuito está cerrado.
Tiempo de rebote de manipulación	Para ignorar los cambios de estado de la entrada de manipulación del lector antes de que entre en un nuevo estado estable, defina un **Tamper debounce time (Tiempo antirrebote en manipulación)**.
Entrada supervisada	Active para desencadenar un evento cuando se interrumpe la conexión entre el controlador de puerta y el lector. Consulte *Entradas con supervisión, on page 83*.

Agregar un dispositivo REX

Puede seleccionar agregar una solicitud al dispositivo de solicitud de salida (REX) en un lado o a ambos lados de la puerta. Un dispositivo REX puede ser un sensor PIR, un botón REX o una barra pulsadora.

1. Vaya a la página de configuración de la puerta. Consulte *Agregar una puerta, on page 75*.
2. En un lado de la puerta, haga clic en **Add (Agregar)**.
3. Seleccione **dispositivo de solicitud de salida (REX)**.
4. Seleccione el puerto de E/S en el que desea conectar el dispositivo REX. Si solo hay un puerto disponible, se seleccionará automáticamente.
5. Seleccione qué **Action (Acción)** activar cuando la puerta recibe la señal REX.
6. En **REX active (REX activo)**, seleccione la conexión de circuito de monitor de puerta.
7. Para ignorar los cambios de estado antes de entrar en un nuevo estado estable, establezca un **Debounce time (ms) [Tiempo antirrebote (ms)]**.
8. Para activar un evento cuando se produce una interrupción en la conexión entre el controlador de puerta y el dispositivo de solicitud de salida (REX), active **Supervised input (Entrada supervisada)**. Consulte *Entradas con supervisión, on page 83*.

Acción	
Abrir puerta	Seleccione para desbloquear la puerta cuando recibe la señal REX.
Ninguno	Seleccione si no desea activar ninguna acción cuando la puerta recibe la señal REX.

REX activo:	
Circuito abierto	Seleccione si el circuito REX está normalmente cerrado. El dispositivo de solicitud de salida (REX) envía la señal cuando el circuito esté abierto.
Circuito cerrado	Seleccione si el circuito REX está normalmente abierto. El dispositivo de solicitud de salida (REX) envía la señal cuando el circuito se cierra.

Agregar una zona

Una zona es un área física específica con un grupo de puertas. Puede crear zonas y agregar puertas a las zonas. Existen dos tipos de puertas:

- **Perimeter door (Puerta del perímetro):** los titulares de tarjeta entran o salen de la zona por esta puerta.
- **Internal door (Puerta interna):** una puerta interna dentro de la zona.

Nota

Una puerta perimetral puede pertenecer a dos zonas. Una puerta interna solo puede pertenecer a una zona.

1. Vaya a **Site Navigation (Navegación de instalaciones)** > **AXIS Optimizer** > **Access control (Control de acceso)** > **Doors and zones (Puertas y zonas)** > **Zones (Zonas)**.
2. Haga clic en **Add zone (Agregar zona)**.
3. Escriba un nombre de zona.
4. Haga clic en **Add door (Agregar puerta)**.
5. Seleccione las puertas que desee agregar a la zona y haga clic en **Add (Agregar)**.
6. De forma predeterminada, la puerta se establece como puerta perimetral. Para cambiarlo, seleccione **Internal door (Puerta interna)** en el menú desplegable.
7. De forma predeterminada, una puerta perimetral utiliza el lado A de la puerta como entrada a la zona. Para cambiarlo, seleccione **Leave (Abandonar)** en el menú desplegable.
8. Para eliminar una puerta de la zona, selecciónela y haga clic en **Remove (Eliminar)**.
9. Haga clic en **Save (Guardar)**.

Para editar una zona:

1. Vaya a **Site Navigation (Navegación de instalaciones)** > **AXIS Optimizer** > **Access control (Control de acceso)** > **Doors and zones (Puertas y zonas)** > **Zones (Zonas)**.
2. Seleccione una zona en la lista.
3. Haga clic en **Edit (Modificar)**.
4. Cambie los ajustes y haga clic en **Save (Guardar)**.

Para eliminar una zona:

1. Vaya a **Site Navigation (Navegación de instalaciones)** > **AXIS Optimizer** > **Access control (Control de acceso)** > **Doors and zones (Puertas y zonas)** > **Zones (Zonas)**.
2. Seleccione una zona en la lista.
3. Haga clic en **Remove (Eliminar)**.
4. Haga clic en **Yes (Sí)**.

Nivel de seguridad de zona

Puede agregar la siguiente característica de seguridad a una zona:

Protección contra dobles entradas – Impide que los usuarios utilicen las mismas credenciales que otra persona que ha entrado en una zona antes. Es obligatorio que una persona salga de la zona antes de sus credenciales se puedan volver a usar.

Nota

- Con antipassback, recomendamos el uso de sensores de posición de puerta en todas las puertas de la zona para asegurarse de el sistema pueda registrar que un usuario la ha abierto tras haber pasado la tarjeta.
- Si un controlador de puerta no tiene conexión, anti passback funciona siempre que todas las puertas de la zona pertenezcan al mismo controlador de puerta. No obstante, si las puertas de la zona pertenecen a distintos controladores de puerta sin conexión, anti passback deja de funcionar.

Puede configurar el nivel de seguridad mientras agrega una zona nueva o puede hacerlo en una zona existente. Para agregar un nivel de seguridad a una zona existente:

1. Vaya a **Site Navigation (Navegación de instalaciones)** > **AXIS Optimizer** > **Access control (Control de acceso)** > **Doors and zones (Puertas y zonas)**.
2. Seleccione la zona para la que desea configurar el nivel de seguridad.
3. Haga clic en **Edit (Modificar)**.
4. Haga clic en **Security level (Nivel de seguridad)**.
5. Active las características de seguridad que desee agregar a la puerta.
6. Haga clic en **Aplicar**.

Protección contra dobles entradas	
Solo registro de infracciones (suave)	Utilice esta opción si desea permitir que una segunda persona entre por la puerta con las mismas credenciales que la primera persona. Esta opción solo genera una alarma del sistema.
Denegar acceso (exigente)	Utilice esta opción si desea evitar que el segundo usuario entre por la puerta si utiliza las mismas credenciales que la primera persona. Esta opción también genera una alarma del sistema.
Tiempo de espera (segundos)	El tiempo que se debe esperar hasta que el sistema permita la entrada de nuevo de un usuario. Introduzca **0** si no desea que se agote el tiempo de espera, lo que significa que la zona tiene antipassback hasta que el usuario sale de la zona. Utilice solo **0** tiempo de espera con **Denegar acceso (exigente)** si todas las puertas de la zona tienen lectores en ambos lados.

Entradas con supervisión

Las entradas supervisadas pueden activar un evento cuando se interrumpe la conexión con un controlador de puerta.

- Conexión entre el controlador de puerta y el monitor de puerta. Consulte *Agregar un monitor de puerta, on page 79*.
- Conexión entre el controlador de puerta y el lector que utiliza protocolos Wiegand. Consulte *Agregar un lector, on page 80*.
- Conexión entre el controlador de puerta y el dispositivo REX. Consulte *Agregar un dispositivo REX, on page 81*.

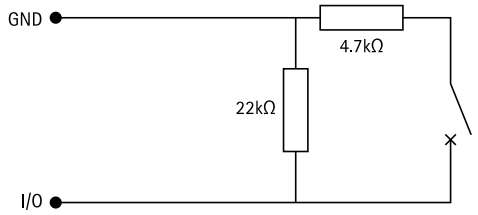
Para utilizar entradas supervisadas:

1. Instale las resistencias de final de línea lo más cerca posible del dispositivo periférico según el diagrama de conexión.
2. Vaya a la página de configuración de un lector, un monitor de puerta o un dispositivo de solicitud de salida (REX), active **Supervised input (Entrada supervisada)**.
3. Si ha seguido el diagrama de primera conexión en paralelo, seleccione **Parallel first connection with a 22 KΩ parallel resistor and a 4.7 KΩ serial resistor (Primera conexión en paralelo con una resistencia de 22 KΩ en paralelo y una resistencia de 4,7 KΩ en serie)**.
4. Si ha seguido el diagrama de primera conexión en serie, seleccione **Serial first connection (Primera conexión en serie)** y seleccione los valores de la resistencia en el menú desplegable **Resistor values (Valores de resistencia)**.

Diagramas de conexión

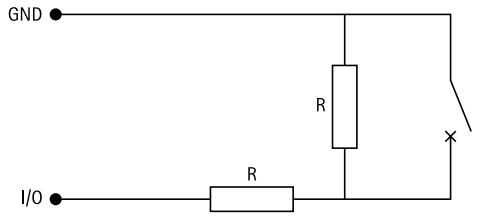
Primera conexión en paralelo

Los valores de la resistencia deben ser de 4,7 KΩ y 22 KΩ.



Primera conexión en serie

Los valores de las resistencias deben ser iguales y situarse en el rango 1-10 KΩ.



Acciones manuales

Puede realizar las siguientes acciones manuales en puertas y zonas:

Reiniciar – Regresa a las reglas del sistema configuradas.

Autorizar acceso – Desbloquea una puerta o zona durante 7 segundos y vuelve a bloquearla.

Desbloquear – Mantiene la puerta desbloqueada hasta que el usuario la reinicia.

Bloquear – Mantiene la puerta bloqueada hasta que el sistema concede acceso a un titular de tarjeta.

Bloqueo – Nadie entra o sale hasta que el usuario reinicia o desbloquea.

Para realizar una acción manual:

1. Vaya a **Site Navigation (Navegación de instalaciones)** > **AXIS Optimizer** > **Access control (Control de acceso)** > **Doors and zones (Puertas y zonas)**.
2. Seleccione la puerta o zona en la que desea realizar una acción manual.
3. Haga clic en cualquiera de las acciones manuales.

Nota

La puerta permanecerá en estado de funcionamiento manual, también conocido como modo de control manual, hasta que se vuelva a configurar según su programación habitual.

Formatos de tarjeta y PIN

Un formato de tarjeta define cómo una tarjeta almacena datos. Es una tabla de traducción entre los datos entrantes y los datos validados en el sistema. Cada formato de tarjeta incluye un conjunto de reglas diferentes para cómo organizar la información almacenada. Al definir un formato de tarjeta, se indica al sistema cómo se debe interpretar la información que el controlador recibe del lector de tarjeta.

Hay formatos de tarjeta de uso común predefinidos disponibles para que los utilice tal como están o los edite según sea necesario. También se pueden crear formatos de tarjeta personalizados.

Vaya a **Site Navigation (Navegación de instalaciones)** > **AXIS Optimizer** > **Access control (Control de acceso)** > **Card formats and PIN (Formatos de tarjeta y PIN)** para crear, editar o activar formatos de tarjeta. También puede configurar el PIN.

Los formatos de tarjeta personalizados pueden contener los siguientes campos de datos utilizados para la validación de credenciales.

Número de tarjeta – Un subconjunto de los datos binarios de credenciales codificados como números decimales o hexadecimales. Use el número de tarjeta para identificar una tarjeta o titular de tarjeta específico.

Código de instalación – Un subconjunto de los datos binarios de credenciales codificados como números decimales o hexadecimales. Use el código de instalación para identificar a un cliente final o instalación específicos.

Para crear un formato de tarjeta:

1. Vaya a **Site Navigation (Navegación de instalaciones)** > **AXIS Optimizer** > **Access control (Control de acceso)** > **Card formats and PIN (Formatos de tarjeta y PIN)**.
2. Haga clic en **Add card format (Añadir formato de tarjeta)**.
3. Introduzca un nombre de formato de tarjeta.
4. En el campo de **Bit length (Longitud de bits)**, escriba una longitud de bits entre 1 y 256.
5. Seleccione **Invert bit order (Invertir orden de bits)** si desea invertir el orden de bits de los datos recibidos desde el lector de tarjetas.
6. Seleccione **Invert byte order (Invertir orden de bytes)** si desea invertir el orden de bytes de los datos recibidos del lector de tarjetas. Esta opción solo está disponible si se especifica una longitud de bits que pueda dividir por ocho.
7. Seleccione y configure los campos de datos para que se activen en el formato de tarjeta. El **Card number (Número de tarjeta)** o el **Facility code (Código de instalación)** deben estar activos en el formato de tarjeta.
8. Haga clic en **OK**.
9. Para activar el formato de tarjeta, seleccione la casilla delante del nombre del formato de tarjeta.

Nota

- No pueden estar activos simultáneamente dos formatos de tarjeta con la misma longitud de bits. Por ejemplo, si ha definido dos formatos de tarjeta de 32 bits, solo podrá activar uno de ellos. Desactive el formato de tarjeta para activar el otro.
- Solo se pueden activar y desactivar formatos de tarjeta si el controlador de puerta se ha configurado con al menos un lector.

ⓘ	Haga clic en ⓘ para ver un ejemplo de la salida después de invertir el orden de bits.
Gama	Defina el rango de bits de los datos para el campo de datos. El intervalo debe estar dentro de lo especificado para **Bit length (Longitud de bits)**.

Formato de salida	Seleccione el formato de salida de los datos para el campo de datos. **Decimal**: También conocido como sistema numeral posicional base 10, consta de los números 0-9. **Hexadecimal**: también conocido como sistema numeral de posición base 16, consta de 16 símbolos únicos: los números 0-9 y las letras a-f.
Orden de bits del subrango	Seleccione el orden de bits. **Little endian**: El primer bit es el más pequeño (el menos significativo). **Big endian**: El primer bit es el más grande (el más significativo).

Para editar un formato de tarjeta:

1. Vaya a **Site Navigation (Navegación de instalaciones)** > **AXIS Optimizer** > **Access control (Control de acceso)** > **Card formats and PIN (Formatos de tarjeta y PIN)**.
2. Seleccione un formato de tarjeta y haga clic en .
3. Si edita un formato de tarjeta predefinido, solo puede editar **Invert bit order (Invertir orden de bits)** e **Invert byte order (Invertir orden de bytes)**.
4. Haga clic en **OK**.

Solo puede eliminar los formatos de tarjeta personalizados. Para eliminar un formato de tarjeta personalizado:

1. Vaya a **Site Navigation (Navegación de instalaciones)** > **AXIS Optimizer** > **Access control (Control de acceso)** > **Card formats and PIN (Formatos de tarjeta y PIN)**.
2. Seleccione un formato de tarjeta personalizado, haga clic en y en **Yes (Sí)**.

Para restablecer un formato de tarjeta predefinido:

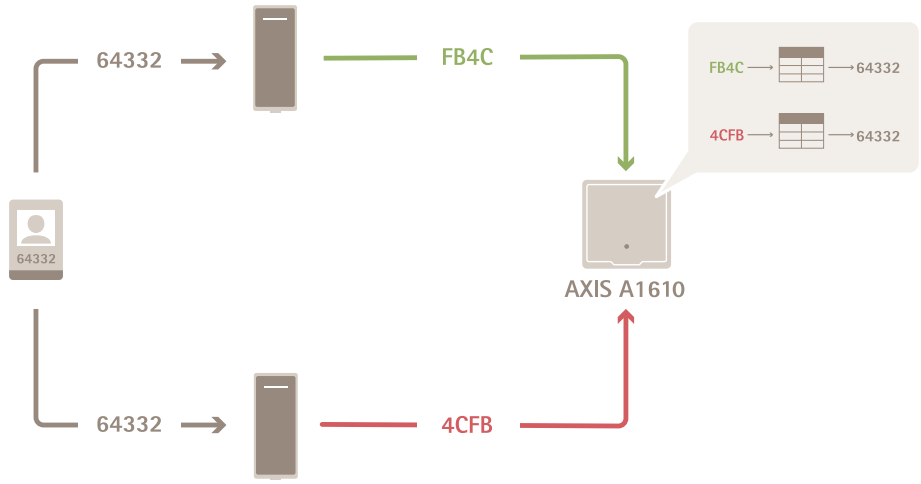
1. Vaya a **Site Navigation (Navegación de instalaciones)** > **AXIS Optimizer** > **Access control (Control de acceso)** > **Card formats and PIN (Formatos de tarjeta y PIN)**.
2. Haga clic en para restablecer un formato de tarjeta al mapa de campos predeterminado.

Para configurar la longitud de PIN:

1. Vaya a **Site Navigation (Navegación de instalaciones)** > **AXIS Optimizer** > **Access control (Control de acceso)** > **Card formats and PIN (Formatos de tarjeta y PIN)**.
2. En **PIN configuration (Configuración de PIN)**, haga clic en .
3. Especifique **Min PIN length (Longitud mínima de PIN)**, **Max PIN length (Longitud máxima de PIN)** y **End of PIN character (Carácter final de PIN)**.
4. Haga clic en **OK**.

Configuración del formato de tarjeta

Descripción general



- El número de tarjeta en decimal es `64332`.
- Un lector transfiere el número de tarjeta al número hexadecimal `FB4C`. El otro lector lo transfiere al número hexadecimal `4CFB`.
- AXIS A1610 Network Door Controller recibe `FB4C` y lo transfiere al número decimal `64332` de acuerdo con los ajustes de formato de tarjeta en el lector.
- AXIS A1610 Network Door Controller recibe `4CFB`, lo convierte en `FB4C` invirtiendo el orden de bytes y lo transfiere al número decimal `64332` de acuerdo con los ajustes de formato de tarjeta en el lector.

Invertir orden de bits

Después de invertir el orden de bits, los datos de la tarjeta que recibe el lector se leen de derecha a izquierda, bit a bit.



Invertir orden de bytes

Un grupo de ocho bits es un byte. Después de invertir el orden de bytes, los datos de la tarjeta que recibe el lector se leen de derecha a izquierda, byte a byte.



Formato de tarjeta Wiegand estándar de 26 bits



1 *Paridad líder*
2 *Código de instalación*
3 *Número de tarjeta*

4 *Paridad de cola*

Perfiles de identificación

Un perfil de identificación es una combinación de tipos de identificación y programaciones. Puede aplicar un perfil de identificación a una o más puertas para definir cómo y cuándo puede acceder un titular de tarjeta a una puerta.

Los tipos de identificación son portadores de la información de la credencial necesaria para acceder a una puerta. Los tipos de identificación comunes son tokens, números de identificación personal (PIN), huellas, mapas faciales y dispositivos de solicitud de salida (REX). Un tipo de identificación puede tener uno o más tipos de información.

Las programaciones, también conocidas como **Time profiles (Perfiles de tiempo)**, se crean en Management Client. Para configurar perfiles de tiempo, consulte *Time profiles (explained) (Perfiles de tiempo (explicación))*.

Tipos de identificación compatibles: Tarjeta, PIN y REX.

Vaya a **Site Navigation (Navegación de instalaciones)** > **AXIS Optimizer** >**Access control (Control de acceso)** > **Identification profiles (Perfiles de identificación)**.

Hay cinco perfiles de identificación predeterminados disponibles para su uso tal y como están o editar según sea necesario.

Tarjeta – Los titulares de tarjeta deben pasar la tarjeta para acceder a la puerta.

Tarjeta y PIN – Los titulares de tarjeta deben pasar la tarjeta e introducir el PIN para acceder a la puerta.

PIN – Los titulares de tarjeta deben introducir el PIN para acceder a la puerta.

Tarjeta o PIN – Los titulares de tarjeta deben pasar la tarjeta o introducir el PIN para acceder a la puerta.

Matrícula – Los titulares de tarjeta deben conducir hacia la cámara en un vehículo con una matrícula aprobada.

Para crear perfil de identificación:

1. Vaya a **Site Navigation (Navegación de instalaciones)** > **AXIS Optimizer** >**Access control (Control de acceso)** > **Identification profiles (Perfiles de identificación)**.
2. Haga clic en **Create identification profile (Crear perfil de identificación)**.
3. Introduzca un nombre de perfil de identificación.
4. Seleccione **Include facility code for card validation (Incluir código de instalación para la validación de la tarjeta)** para usar el código de instalación como uno de los campos de validación de credenciales. Este campo solo está disponible si ha activado **Facility code (Código de instalación)** en **Access management > Settings (Gestión de acceso > Ajustes)**.
5. Configure el perfil de identificación para un lado de la puerta.
6. En el otro lado de la puerta, realice de nuevo los pasos anteriores.
7. Haga clic en **OK**.

Para editar un perfil de identificación:

1. Vaya a **Site Navigation (Navegación de instalaciones)** > **AXIS Optimizer** >**Access control (Control de acceso)** > **Identification profiles (Perfiles de identificación)**.
2. Seleccione un perfil de identificación y haga clic en .
3. Para cambiar el nombre del perfil de identificación, introduzca un nuevo nombre.
4. Realice los cambios en el lateral de la puerta.
5. Para editar el perfil de identificación en el otro lado de la puerta, realice de nuevo los pasos anteriores.
6. Haga clic en **OK**.

Para eliminar un perfil de identificación:

1. Vaya a **Site Navigation (Navegación de instalaciones)** > **AXIS Optimizer** >**Access control (Control de acceso)** > **Identification profiles (Perfiles de identificación)**.
2. Seleccione un perfil de identificación y haga clic en .
3. Si se ha usado el perfil de identificación en una puerta, seleccione otro perfil de identificación para la puerta.
4. Haga clic en **OK**.

Editar perfil de identificación	
×	Para eliminar un tipo de identificación y la correspondiente programación.
Tipo de identificación	Para cambiar un tipo de identificación, seleccione uno o varios tipos en el menú desplegable **Identification type (Tipo de identificación)**.
Horario	Para cambiar una programación, seleccione una o varias programaciones en el menú desplegable **Schedule (Programación)**.
+ **Agregar**	Agregue un tipo de identificación y la correspondiente programación, haga clic en **Add (Agregar)** y establezca los tipos de identificación y las programaciones.

Comunicación cifrada

Canal seguro OSDP

Secure Entry admite el canal seguro OSDP (Protocolo abierto de dispositivos supervisados) para activar el cifrado de la línea entre el controlador y los lectores de Axis.

Para activar OSDP Secure Channel en todo un sistema:

1. Vaya a **Site Navigation (Navegación de instalaciones)** > **AXIS Optimizer** >**Access control (Control de acceso)** > **Encrypted communication (Comunicación cifrada)**.
2. Introduzca la clave de cifrado principal y haga clic en **OK (Aceptar)**.
3. Active **OSDP Secure Channel (Canal seguro OSDP)**. Esta opción solo está disponible una vez que haya introducido la clave de cifrado principal.
4. De forma predeterminada, la clave de cifrado principal genera una clave de canal seguro OSDP. Para configurar manualmente la clave de canal seguro OSDP:
   4.1. En **OSDP Secure Channel (Canal seguro OSDP)**, haga clic en .
   4.2. Elimine **Use main encryption key to generate OSDP Secure Channel key (Utilice la clave de cifrado principal para generar la clave de canal seguro OSDP)**.
   4.3. Introduzca la clave de canal seguro OSDP y haga clic en **OK (Aceptar)**.

Para encender o apagar el canal seguro OSDP para un lector específico, consulte *Doors and zones (Puertas y zonas)*.

BETA de varios servidores

Los servidores secundarios conectados pueden, con varios servidores, usar los titulares de tarjeta globales y grupos de titulares de tarjeta del servidor principal.

Nota

- Un sistema puede admitir hasta 64 subservidores.
- Requiere que el servidor principal y los servidores secundarios estén en la misma red.
- En los servidores principales y servidores secundarios, asegúrese de configurar el Firewall de Windows para permitir las conexiones TCP entrantes en el puerto Secure Entry. El puerto predeterminado es 53461.

Flujo de trabajo

1. Configure un servidor como un servidor secundario y genere el archivo de configuración. Consulte *Generar el archivo de configuración desde el servidor secundario, on page 90*.
2. Configure un servidor como servidor principal e importe el archivo de configuración de los servidores secundarios. Consulte *Importar el archivo de configuración al servidor principal, on page 90*.
3. Configure los grupos de titulares de tarjeta y de titulares globales en el servidor principal. Consulte *Agregar un titular de tarjeta, on page 91* y *Agregar un grupo, on page 95*.
4. Consulte y supervise los titulares de tarjeta y los grupos de titulares de tarjeta globales desde el servidor secundario. Consulte *Gestión de acceso, on page 91*.

Generar el archivo de configuración desde el servidor secundario

1. Desde el servidor secundario, vaya a **AXIS Optimizer** > **Access control (Control de acceso)** > **Multi server (Multiservidor)**.
2. Haga clic en **Sub server (servidor secundario)**.
3. Haga clic en **Generate (generar)**. Se genera un archivo de configuración en formato .json.
4. Haga clic en **Download (Descargar)** y elija una ubicación para guardar el archivo.

Importar el archivo de configuración al servidor principal

1. Desde el servidor principal, vaya a **AXIS Optimizer** > **Access control (Control de acceso)** > **Multi server (Multiservidor)**.
2. Haga clic en **Main server (Servidor principal)**.
3. Haga clic en + **Add (Agregar)** y vaya al archivo de configuración generado del servidor secundario.
4. Introduzca el nombre del servidor, la dirección IP y el número de puerto del servidor secundario.
5. Haga clic en **Import (Importar)** para agregar el servidor secundario.
6. El estado del servidor secundario es `Connected`.

Revocar un servidor secundario

Solo puede revocar un servidor secundario antes de importar su archivo de configuración a un servidor principal.

1. Desde el servidor principal, vaya a **AXIS Optimizer** > **Access control (Control de acceso)** > **Multi server (Multiservidor)**.
2. Haga clic en **Sub server (servidor secundario)** y haga clic en **Revoke server (Revocar servidor)**. Ahora puede configurar este servidor como servidor principal o servidor secundario.

Eliminar un servidor secundario

Después de importar el archivo de configuración de un servidor secundario, se conecta el servidor secundario al servidor principal.

Para eliminar un servidor secundario:

1. Desde el servidor principal:

1.1. Vaya a **Access management (Gestión de acceso)** > **Dashboard (Panel de control)**.

1.2. Cambie los titulares de tarjeta y los grupos globales por los titulares de tarjeta y los grupos locales.

1.3. Vaya a **AXIS Optimizer** > **Access control (Control de acceso)** > **Multi server (Multiservidor)**.

1.4. Haga clic en **Main server (Servidor principal)** para mostrar la lista de servidores secundarios.

1.5. Seleccione el servidor secundario y haga clic en **Delete (Eliminar)**.

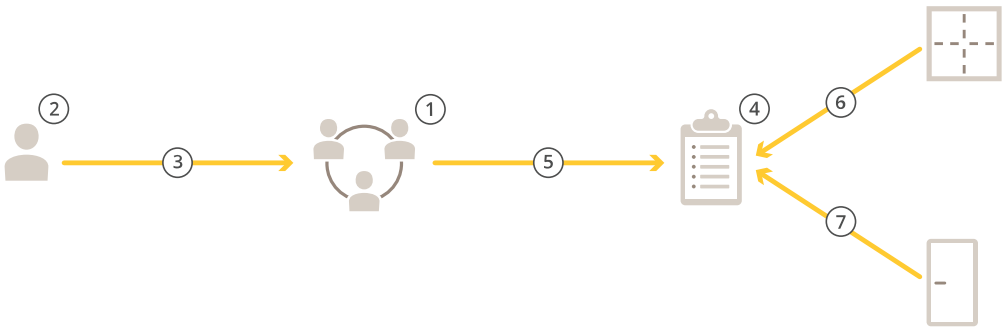
2. Desde el servidor secundario:
   - Vaya a **AXIS Optimizer** > **Access control (Control de acceso)** > **Multi server (Multiservidor)**.
   - Haga clic en **Sub server (Servidor secundario)** y **Revoke server (Revocar servidor)**.

Gestión de acceso

La pestaña de gestión de acceso permite configurar y gestionar los titulares de tarjeta, grupos y reglas de acceso del sistema.

Flujo de trabajo de gestión de acceso

La estructura de gestión de accesos es flexible, esto permite desarrollar un flujo de trabajo que se adapte a sus necesidades. El siguiente es un ejemplo de flujo de trabajo:



1. Agregar grupos. Consulte *Agregar un grupo, on page 95*.
2. Agregar titulares de tarjeta. Consulte *Agregar un titular de tarjeta, on page 91*.
3. Agregar titulares de tarjeta a grupos.
4. Agregar reglas de acceso. Consulte *Agregar una regla de acceso, on page 95*.
5. Aplicar grupos a reglas de acceso.
6. Aplicar zonas a las reglas de acceso.
7. Aplicar puertas a reglas de acceso.

Agregar un titular de tarjeta

Un titular de tarjeta es una persona con un identificador único registrado en el sistema. Configure un titular de tarjeta con credenciales que identifica a la persona y cuándo y cómo conceder acceso a las puertas.

1. Vaya a **Site Navigation (Navegación de instalaciones)** > **AXIS Optimizer** >**Access control (Control de acceso)** > **Cardholder management (Gestión de titulares de tarjeta)**.
2. Vaya a **Cardholders (Titulares)** y haga clic en **+ Add (+ Añadir)**.
3. Introduzca el nombre y apellidos del titular de tarjeta y haga clic en **Next (Siguiente)**.
4. Si lo desea, haga clic en **Advanced (Avanzado)** y seleccione las opciones que desee.

5. Agregar una credencial al titular de tarjeta. Consulte *Agregar credenciales, on page 92*
6. Haga clic en **Save (Guardar)**.
7. Agregar el titular de tarjeta a un grupo.
   7.1. En **Groups (Grupos)**, seleccione el grupo al que desea agregar el titular de tarjeta y haga clic en **Edit (Editar)**.
   7.2. Haga clic en **+ Add (Añadir)** y seleccione el titular de tarjeta que desea agregar al grupo. Puede seleccionar varios titulares de tarjeta.
   7.3. Haga clic en **Add (Añadir)**.
   7.4. Haga clic en **Save (Guardar)**.

Avanzada	
Tiempo de acceso largo	Seleccione esta opción para permitir que el titular de la tarjeta tenga un tiempo de acceso largo y un tiempo de apertura demasiado largo cuando haya un monitor de puerta instalado.
Suspender titular	Seleccione esta opción para suspender el titular de la tarjeta.
Allow double-swipe (Permitir doble barrido)	Seleccione esta opción para permitir que un titular de tarjeta anule el estado actual de una puerta. Por ejemplo, pueden usarla para desbloquear una puerta fuera de la programación normal.
Exento de bloqueo	Seleccione esta opción para permitir el acceso al titular de tarjeta durante el bloqueo.
Exento de antipassback	Seleccione para proporcionar a un titular de tarjeta una exención de una regla antipassback. La función antipassback impide que los usuarios utilicen las mismas credenciales que otra persona que ha entrado en una zona antes. Primero debe salir de la zona la primera persona antes de poder volver a utilizar las credenciales.
Titular de tarjeta global	Seleccione para poder ver y supervisar al titular de tarjeta en los servidores secundarios. Esta opción solo está disponible para los titulares de tarjeta creados en el servidor principal. Consulte .

Agregar credenciales

Puede agregar los siguientes tipos de credenciales a un titular de tarjeta:

- PIN
- Tarjeta
- Matrícula
- Teléfono móvil

Para agregar una matrícula a un titular de tarjeta:

1. En **Credentials (Credenciales)**, haga clic en **+ Add (Agregar)** y seleccione **License plate (Matrícula)**.
2. Introduzca un nombre de credencial que describa el vehículo.
3. Introduzca el número de matrícula del vehículo.
4. Establezca la fecha de inicio y fin para la credencial.

5. Haga clic en **Add (Añadir)**.

Consulte el ejemplo en *Utilizar el número de matrícula como credencial, on page 94*.

Para agregar una credencial de PIN a un titular de tarjeta:

1. En **Credentials (Credenciales)**, haga clic en **+ Add (Agregar)** y seleccione **PIN**.
2. Introduzca un PIN.
3. Para utilizar un PIN de coacción que active una alarma silenciosa, active **Duress PIN (PIN de coacción)** e introduzca un PIN de coacción.
4. Haga clic en **Add (Añadir)**.

Una credencial de PIN siempre es válida. También puede configurar un PIN de coacción que abre la puerta y activa una alarma silenciosa en el sistema.

Para agregar una credencial de tarjeta a un titular de tarjeta:

1. En **Credentials (Credenciales)**, haga clic en **+ Add (Agregar)** y seleccione **Card (Tarjeta)**.
2. Para introducir manualmente los datos de la tarjeta, introduzca el nombre de la tarjeta, el número de tarjeta y la longitud de bits.

Nota

La longitud de bits solo es configurable cuando se crea un formato de tarjeta con una longitud de bits específica que no está en el sistema.

3. Para obtener automáticamente los datos de la tarjeta de la última tarjeta que se ha pasado:
   3.1. Seleccione una puerta en el menú desplegable **Select reader (Seleccionar lector)**.
   3.2. Pase la tarjeta por el lector conectado a esa puerta.
   3.3. Haga clic en **Get last swiped card data from the selected reader (Obtener datos de la última tarjeta que se ha pasado desde los lectores de la puerta)**.
4. Introduzca un código de instalación. Este campo solo está disponible si ha habilitado **Facility code (Código de instalación)** en **Access management > Settings (Gestión de acceso > Ajustes)**.
5. Establezca la fecha de inicio y fin para la credencial.
6. Haga clic en **Add (Añadir)**.

Fecha de caducidad	
Válido desde	Establezca una fecha y hora para el momento en que la credencial debe ser válida.
Válido hasta	Seleccione una opción en el menú desplegable.

Válido hasta	
Sin fecha de finalización	La credencial nunca caduca.
Fecha	Establezca una fecha y hora en la que caduca la credencial.
Desde el primer uso	Seleccione cuándo caduca la credencial después del primer uso. Seleccione días, meses, años or número de veces después del primer uso.
Desde el último uso	Seleccione cuándo caduca la credencial después del último uso. Seleccione días, meses o años después del último uso.

Utilizar el número de matrícula como credencial

En este ejemplo se muestra cómo usar un controlador de puerta, una cámara con AXIS License Plate Verifier y el número de matrícula de un vehículo como credenciales para conceder acceso.

1. Agregue el controlador de puerta y la cámara a AXIS Optimizer.
2. Defina la fecha y la hora para los nuevos dispositivos con **Synchronize with server computer time (Sincronizar con hora del equipo del servidor)**.
3. Actualice el software de los dispositivos nuevos a la versión más reciente disponible.
4. Agregue una puerta nueva conectada al controlador de puerta. Consulte *Agregar una puerta, on page 75*.
   4.1. Añada un lector en **Side A (Lado A)**. Consulte *Agregar un lector, on page 80*.
   4.2. En **Door settings (Ajustes de puerta)**, seleccione **AXIS License Plate Verifier** como **Reader type (Tipo de lector)** e introduzca un nombre para el lector.
   4.3. Si lo desea, puede agregar un lector o dispositivo de solicitud de salida (REX) al **Lado B**.
   4.4. Haga clic en **Ok (Aceptar)**.
5. Instale y active AXIS License Plate Verifier en la cámara. Consulte el manual del usuario de *AXIS License Plate Verifier*.
6. Iniciar AXIS License Plate Verifier.
7. Configurar AXIS License Plate Verifier.
   7.1. Vaya a **Configuration > Access control > Encrypted communication (Configuración > Control de acceso > Comunicación cifrada)**.
   7.2. En **External Peripheral Authentication Key (Clave de autenticación periférica externa)**, haga clic en **Show authentication key (Mostrar clave de autenticación)** y **Copy key (Copiar clave)**.
   7.3. Abra AXIS License Plate Verifier desde la interfaz web de la cámara.
   7.4. No realice la configuración.
   7.5. Vaya a **Settings (Ajustes)**.
   7.6. En **Access control (Control de acceso)**, seleccione **Secure Entry (Entrada segura)** como **Type (Tipo)**.
   7.7. En **IP address (Dirección IP)**, introduzca la dirección IP para el controlador de puerta.
   7.8. En **Authentication key (Clave de autenticación)**, pegue la clave de autenticación que copió anteriormente.
   7.9. Haga clic en **Connect (Conectar)**.
   7.10. En **Door controller name (Nombre del controlador de puerta)**, seleccione el controlador de puerta.
   7.11. En **Reader name (Nombre del lector)**, seleccione el lector que agregó anteriormente.
   7.12. Active la integración.
8. Agregue el titular de tarjeta al que desee acceder. Consulte *Agregar un titular de tarjeta, on page 91*.
9. Agregue las credenciales de la matrícula al nuevo titular de la tarjeta. Consulte *Agregar credenciales, on page 92*.
10. Agregar una regla de acceso. Consulte *Agregar una regla de acceso, on page 95*.
    10.1. Agregue una programación.
    10.2. Agregue el titular de la tarjeta al que desee conceder acceso a la matrícula.
    10.3. Agregue la puerta con el lector AXIS License Plate Verifier.

Agregar un grupo

Los grupos le permiten gestionar de forma colectiva y eficiente los titulares de tarjeta y sus reglas de acceso.

1. Vaya a **Site Navigation (Navegación de instalaciones)** > **AXIS Optimizer** >**Access control (Control de acceso)** > **Cardholder management (Gestión de titulares de tarjeta)**.
2. Vaya a **Groups (Grupos)** y haga clic en **+ Add (+ Añadir)**.
3. Introduzca un nombre y, si lo desea, las iniciales del grupo.
4. Seleccione **Global group (Grupo global)** para poder visualizar y supervisar en los servidores secundarios. Esta opción solo está disponible para los titulares de tarjeta creados en el servidor principal. Consulte *BETA de varios servidores, on page 89*.
5. Agregar titulares de tarjeta al grupo:
   5.1. Haga clic en **+ Agregar**.
   5.2. Seleccione los titulares de tarjeta que desee añadir y haga clic en **Add (Agregar)**.
6. Haga clic en **Save (Guardar)**.

Agregar una regla de acceso

Una regla de acceso define las condiciones que deben cumplirse para conceder acceso.

Una regla de acceso consta de:

Titulares de tarjeta y grupos de titulares – a quién conceder acceso.

Puertas y zonas – dónde se aplica el acceso.

Horarios – cuándo conceder acceso.

Para agregar una regla de acceso:

1. Vaya a **Access control (Control de acceso)** > **Cardholder management (Gestión de titulares de tarjeta)**.
2. En **Access rules (Reglas de acceso)**, haga clic en **+ Add (Agregar)**.
3. Introduzca un nombre para la regla de acceso y haga clic en **Next (Siguiente)**.
4. Configure los titulares de tarjeta y los grupos:
   4.1. En **Cardholders (Titulares de tarjeta)** o **Groups (Grupos)**, haga clic en **+ Add (Agregar)**.
   4.2. Seleccione los titulares de tarjeta o grupos y haga clic en **Add (Agregar)**.
5. Configure las puertas y zonas:
   5.1. En **Doors (Puertas)** o **Zones (Zonas)**, haga clic en **+ Add (Agregar)**.
   5.2. Seleccione las puertas o zonas y haga clic en **Add (Agregar)**.
6. Configure las programaciones:
   6.1. En **Schedules (Programaciones)**, haga clic en **+ Add (Agregar)**.
   6.2. Seleccione una o más programaciones y haga clic en **Add (Agregar)**.
7. Haga clic en **Save (Guardar)**.

Una regla de acceso en la que le falten uno o más de los componentes descritos anteriormente está incompleta. Puede ver todas las reglas de acceso incompletas en la pestaña **Incomplete (Incompletas)**.

Desbloquear puertas y zonas manualmente

Para obtener información sobre acciones manuales, como desbloquear manualmente una puerta, consulte *Acciones manuales, on page 84*.

Para obtener información sobre acciones manuales, como desbloquear manualmente una zona, consulte *Acciones manuales, on page 84*.

Exportar informes de configuración del sistema

Puede exportar informes que contengan diferentes tipos de información acerca del sistema. AXIS Optimizer exporta el informe como un archivo de valores separados por comas (CSV) y lo guarda en la carpeta de descargas predeterminada. Para exportar un informe:

1. Vaya a **Reports (Informes)** > **System configuration (Configuración del sistema)**.
2. Seleccione los informes que desea exportar y haga clic en **Download (Descargar)**.

Datos del titular de tarjeta	Incluye información sobre los titulares de tarjetas, credenciales, validación de tarjetas y última operación.
Acceso para titulares de tarjeta	Incluye información sobre titulares de tarjetas y sobre grupos de titulares de tarjetas, reglas de acceso, puertas y zonas con las que está relacionado el titular de tarjeta.
Acceso de grupo de titulares de tarjeta	Incluye el nombre del grupo de titulares de tarjetas e información sobre titulares de tarjetas, reglas de acceso, puertas y zonas con las que está relacionado el grupo de titulares de tarjetas.
Regla de acceso	Incluye el nombre de la regla de acceso e información sobre titulares de tarjetas, grupos de titulares de tarjetas, puertas y zonas con las que está relacionada la regla de acceso.
Acceso a puerta	Incluye el nombre de la puerta e información sobre titulares de tarjetas, grupos de titulares de tarjetas, reglas de acceso y zonas con las que está relacionada la puerta.
Acceso de zona	Incluye el nombre de la zona e información sobre titulares de tarjetas, grupos de titulares de tarjetas, reglas de acceso y puertas con las que está relacionada la zona.

Crear informes de actividad de titulares de tarjeta

En un informe de pase de lista se enumeran los titulares de tarjeta dentro de una zona específica, lo que ayuda a identificar quién está presente en un momento dado.

En un informe de agrupamiento se enumera a los titulares de tarjeta dentro de una zona específica, lo que ayuda a identificar quién está a salvo y quién ha desaparecido en una situación de emergencia. Ayuda a los gestores de edificios a localizar al personal y a los visitantes después de una evacuación. Un punto de agrupamiento es un lector designado donde el personal se presenta durante las emergencias, y se genera un informe de personas dentro y fuera de las instalaciones. El sistema marca a los titulares de tarjeta como desaparecidos hasta que se registran en un punto de agrupamiento o hasta que alguien los marca manualmente como fuera de peligro.

Tanto los informes de pase de lista como los de agrupamiento requieren zonas para el seguimiento de los titulares de tarjeta.

Para crear y ejecutar un informe de pase de lista o agrupamiento:

1. Vaya a **Reports (Informes)** > **Cardholder activity (Actividad de los titulares de tarjeta)**.
2. Haga clic en **+ Add (Agregar)** y seleccione **Roll call / Mustering (Pase de lista / Agrupamiento)**.
3. Introduzca un nombre para el informe.

4. Seleccione las zonas que desee incluir en el informe.
5. Seleccione los grupos que desee incluir en el informe.
6. Si desea obtener un informe de agrupamiento, seleccione **Mustering point (Punto de agrupamiento)** y un lector para el punto de agrupamiento.
7. Seleccione un marco temporal para el informe.
8. Haga clic en **Save (Guardar)**.
9. Seleccione el informe y haga clic en **Run (Ejecutar)**.

Estado del informe de pase de lista	Descripción
Presente	El titular de tarjeta accedió a la zona especificada y no salió antes de que usted ejecutara el informe.
Ausente	El titular de tarjeta salió de la zona especificada y no volvió a entrar antes de que usted ejecutara el informe.

Estado del informe de agrupamiento	Descripción
A salvo	El titular de tarjeta pasó esta última en el punto de agrupamiento.
Ausente	El titular de tarjeta no pasó esta última en el punto de agrupamiento.

Configuración de gestión de acceso

Para personalizar los campos de titular de tarjeta utilizados en el panel de gestión de acceso:

1. En la pestaña **Access management (Gestión de acceso)**, haga clic en **Settings (Ajustes)** > **Custom cardholder fields (Campos personalizados del titular de tarjeta)**.
2. Haga clic en **+ Add (Agregar)** e introduzca un nombre. Puede añadir hasta 6 campos personalizados.
3. Haga clic en **Add (Añadir)**.

Para usar el código de la instalación para verificar el sistema de control de acceso:

1. En la pestaña **Access management (Gestión de acceso)**, haga clic en **Settings (Ajustes)** > **Facility code (Código de la instalación)**.
2. Seleccione **Facility code on (Código de instalación activado)**.

Nota

También debe seleccionar **Include facility code for card validation (Incluir código de instalación para validación de la tarjeta)** al configurar perfiles de identificación. Consulte .

Importación y exportación

Importar titulares de tarjetas

Esta opción importa titulares de tarjeta, grupos de titulares de tarjetas, credenciales y fotografías de titulares de tarjeta desde un archivo CSV. Para importar las fotos del titular de la tarjeta, asegúrese de que el servidor dispone de acceso a las fotos.

Al importar titulares de tarjeta, el sistema de gestión de acceso guarda automáticamente la configuración del sistema, incluida toda la configuración de hardware y elimina cualquiera guardada anteriormente.

Importar opciones	
Nuevo	Esta opción elimina los titulares de las tarjetas existentes y añade nuevos titulares.
Actualizar	Esta opción actualiza los titulares de las tarjetas existentes y agrega nuevos titulares de tarjeta.
Agregar	Esta opción mantiene a los titulares de las tarjetas existentes y añade nuevos titulares. Los números de tarjeta y los identificadores de titular de tarjeta son exclusivos y solo pueden utilizarse una vez.

1. En la pestaña **Access management (Gestión de acceso)**, haga clic en **Import and export (Importar y exportar)**.
2. Haga clic en **Import cardholders (Importar titulares de tarjeta)**.
3. Seleccione **New (Nuevo)**, **Update (Actualizar)** o **Add (Agregar)**.
4. Haga clic en **Next (Siguiente)**.
5. Haga clic en **Choose a file (Seleccionar un archivo)** y vaya al archivo CSV. Haga clic en **Abrir**.
6. Introduzca un delimitador de columna, seleccione un identificador único y haga clic en **Next (Siguiente)**.
7. Asigne un encabezado a cada columna.
8. Haga clic en **Import (Importar)**.

Importar ajustes	
La primera fila es un encabezado	Seleccione si el archivo CSV contiene un encabezado de columna.
Delimitador de columnas	Introduzca un formato de delimitador de columnas para el archivo CSV.
Identificador único	El sistema utiliza un **ID de titular de tarjeta** para identificar a un titular de forma predeterminada. También puede utilizar el nombre y el apellido o la dirección de correo electrónico. El identificador único impide la importación de registros de personal duplicados.
Formato de número de tarjeta	Se ha seleccionado **Allow both hexadecimal and number (Permitir hexadecimal y número)** de forma predeterminada.

Exportar titulares de tarjetas

Esta opción exporta los datos de titulares de tarjeta del sistema a un archivo CSV.

1. En la pestaña **Access management (Gestión de acceso)**, haga clic en **Import and export (Importar y exportar)**.
2. Haga clic en **Export cardholders (Exportar titulares de tarjeta)**.
3. Elija una ubicación de descarga y haga clic en **Save (Guardar)**.

AXIS Optimizer actualiza las fotos de los titulares de tarjetas en `C:\ProgramData\Axis Communications\AXIS Camera Station\Components\AXIS Secure Entry\Cardholder photos` cada vez que cambia la configuración.

Undo import (Deshacer importación)

El sistema guarda automáticamente su configuración al importar titulares de tarjeta. La opción **Undo import (Deshacer importación)** restablece los datos de titular de tarjeta y toda la configuración de hardware al estado en que se encontraron antes de la última importación de titulares de tarjeta.

1. En la pestaña **Access management (Gestión de acceso)**, haga clic en **Import and export (Importar y exportar)**.
2. Haga clic en **Undo import (Deshacer importación)**.
3. Haga clic en **Yes (Sí)**.

Copia de seguridad y restauración

Todas las noches se realizan copias de seguridad automáticas. Los tres archivos de copia de seguridad más recientes se almacenan en C:\ProgramData\Axis Communications\AXIS Optimizer Secure Entry\backup. Para restaurar estos archivos:

1. Traslade el archivo de copia de seguridad a C:\ProgramData\Axis Communications\AXIS Optimizer Secure Entry\restore.
2. Reinicie AXIS Secure Entry empleando uno de estos métodos:
   - Inicie el programa MSC (servicios), busque 'AXIS Optimizer Secure Entry Service' y reinicie.
   - Reinicie el ordenador.
3. Vuelva a ejecutar el instalador de AXIS Optimizer en el servidor de eventos.

Gestión de acceso en Smart Client

Mediante Smart Client, los operadores pueden realizar operaciones relacionadas con su sistema de control de acceso. La mayoría de las funciones de control de acceso, como el control manual de puertas, están disponibles en Smart Client. Para obtener más información sobre estas funciones, consulte *Using access control in Smart Client (Uso del control de acceso en Smart Client)*.

También puede gestionar el acceso directamente en Smart Client. Las siguientes funciones que se encuentran en Management Client también están disponibles en Smart Client:

- Gestión de titulares de tarjeta
- Configuración general
- Campos de titular de tarjetas personalizados
- Código de instalación
- Plantillas de correo electrónico
- Plantillas de insignias BETA

Para mostrar la pestaña de administración de acceso de Axis en Smart Client:

1. Instale AXIS Optimizer en el equipo con Smart Client.
2. Active una licencia de puerta, si no se ha activado ninguna. Para activar una licencia de puerta, consulte *Activar licencias de puerta, on page 72*.
3. Asegúrese de que el usuario que ha iniciado sesión tenga permisos de administración de acceso, consulte *Configuración de roles de AXIS Secure Entry, on page 99*.

Configuración de roles de AXIS Secure Entry

1. En Management Client, vaya a **Site Navigation** > **Security** > **Roles (Navegación de instalaciones > Seguridad > Funciones)**.
2. Seleccione un rol concreto en el sistema.
3. Seleccione **AXIS Optimizer**.

4. Despliegue la lista y haga clic en **Access control (Control de acceso)**.
5. Seleccione **Read (Leer)** para conocer los ajustes de seguridad del control de acceso.
6. Haga clic en la función para la que el rol debe tener permiso y seleccione **Grant (Permitir)**.
   - **Access control configuration (Configuración del control de acceso):** concede al operador permisos para acceder a todas las funciones de la pestaña Configuración.
   - **Access management (Gestión de acceso):** concede al operador permisos para acceder a todas las funciones de la pestaña Gestión de acceso.

Gestión de sistemas y controles de seguridad

Personalizar el acceso a características de los operadores

Ajustes de función

De forma predeterminada, los operadores tienen acceso a todas las características de AXIS Optimizer en Smart Client si también pueden acceder al dispositivo en el VMS. Sin embargo, en Management Client, se pueden configurar las características a las que un operador tiene acceso mediante los Role settings (Ajustes de funciones).

Configuración de los ajustes de función

Activar **Role settings (Ajustes de función)**:

1. En Management Client, vaya a **Site Navigation > Security > AXIS Optimizer Security (Navegación de instalaciones > Seguridad > AXIS Optimizer Security)**.

Nota

Una vez activada, no podrá desactivar los ajustes de función. La configuración es permanente.

2. Seleccione **Turn on role settings (Activar ajustes de función)**.
3. Reinicie Management Client.

Configuración de los **Role settings (Ajustes de función)**:

1. En Management Client, vaya a **Site Navigation > Security > Roles (Navegación de instalaciones > Seguridad > Funciones)**.
2. Seleccione una función y vaya a **Overall security (Seguridad general)**.
3. Haga clic en **AXIS Optimizer Security**.
4. Seleccione las características a las que la función debe tener acceso o no.
   - **Full control (Control total)**Proporciona al operador acceso completo a todas las funciones de AXIS Optimizer.
   - **Editar (no aplicable)**Se trata de una función del VMS que no se aplica a los ajustes de función de AXIS Optimizer.
   - **Acceder a AXIS Optimizer en el cliente de gestión**Los operadores pueden usar todas las funciones de administración de AXIS Optimizer en Management Client.
   - **Gestionar la seguridad de AXIS Optimizer**Los operadores pueden modificar los ajustes desde **Site Navigation > Security > AXIS Optimizer Security**.
   - **Controles de operador de cámaras dinámicas**Los operadores tienen acceso a todas las funciones preinstaladas que el sistema encuentra en un dispositivo.
   - **Control del operador de enfoque remoto**Los operadores pueden ajustar el enfoque remoto en cámaras domo fijas.
   - **Controles del operador de PTZ**El operador tiene acceso a controles PTZ específicos: control de enfoque, preajustes PTZ, controles para Autotracking 2, acceso al botón SpeedDry/escobillas de limpieza.
   - **Temperature spot measurement control.**El operador puede medir la temperatura puntual con el modelo AXIS Q2901-E.
   - **Control del operador de altavoz**Los operadores tienen acceso a todas las funciones de gestión de altavoces en Smart Client.
   - **Acceder a la gestión de visitantes**El operador tiene acceso a todo lo relacionado con la gestión de visitantes, por ejemplo, respuesta a las llamadas y a la apertura de puertas en directo.

- **Acceder al historial de llamadas**El operador puede acceder al historial de llamadas de un intercomunicador. Debe permitir que **Access visitor management (Gestión de acceso de visitantes)** pueda utilizar esta configuración.
- **Funciones de búsqueda ampliadas**Si selecciona **Deny**, la pestaña AXIS License Plate Verifier queda oculta en Smart Client. Además, no se puede utilizar la búsqueda de vehículos y contenedores dentro de la búsqueda centralizada.
- **Controlar la vista de corrección de la aberración esférica**Los operadores pueden moverse por las vistas con corrección esférica.
- **Editar la posición de inicio de una vista con corrección de la aberración esférica**Los operadores pueden editar la posición de inicio de una cámara.
- **Página Web**Los operadores pueden crear una vista con un navegador web.
- **Panel de información de datos de Axis**
  La función de operador se acceso al panel de información de Axis.

5. Haga clic en **Save (Guardar)**.
6. Reinicie todos los Smart Clients que se estén ejecutando en su sistema.

Gestión de dispositivos

AXIS Device Manager Extend

En AXIS Optimizer, puede utilizar AXIS Device Manager Extend para gestionar dispositivos de varias instalaciones. Al configurar hosts en el extremo la instalación en servidores de grabación, AXIS Device Manager Extend se conecta a los dispositivos en el VMS. Facilita la revisión de la información de la garantía y la realización de actualizaciones de software en varios dispositivos e instalaciones desde una única interfaz de usuario.

Para obtener más información sobre AXIS Device Manager Extend, consulte el *manual del usuario*.

Nota

Requisitos

- Inicie sesión en una *cuenta MyAxis*.
- Los servidores de grabación deben tener acceso a Internet.
- Solo es compatible con dispositivos en los que se ejecuta AXIS OS 6.50. Para saber qué dispositivos son compatibles, consulte las *FAQ (preguntas frecuentes)*.

Instalar el host en el extremo

El host en el extremo es un servicio de gestión local que permite a AXIS Device Manager Extend comunicarse con los dispositivos locales en el VMS.

El host en el extremo y el cliente de escritorio se tienen que instalar para utilizar AXIS Device Manager Extend en el VMS. El host en el extremo y el cliente de escritorio se incluyen en el instalador de AXIS Device Manager Extend.

1. Descargue el *instalador* de AXIS Device Manager Extend.
   El host en el extremo se debe instalar en los servidores de grabación del VMS.
2. Ejecute el instalador en el servidor de grabación y seleccione instalar solo el host en el extremo.

Consulte el *Axis Device Manager Extend user manual (manual del usuario de Axis Device Manager Extend)* para obtener más información sobre puertos de red abiertos y otros requisitos.

Reclamar el host en el extremo y sincronizar dispositivos



1. Abra Management Client.
2. Vaya a **Site Navigation > AXIS Optimizer > System overview (Navegación de instalaciones) > AXIS Optimizer > Información general del sistema)**.
3. Seleccione e inicie sesión en MyAxis.
4. Haga clic en un mosaico del servidor de grabación con un host en el extremo instalado listo para que lo reclamen.
5. En la barra lateral, cree una nueva organización o seleccione una organización creada anteriormente.
6. Haga clic y reclame el host en el extremo.
7. Espere hasta que la página se haya vuelto a cargar y haga clic en **Synchronize (Sincronizar)**.
   Todos los dispositivos Axis del servidor de grabación se agregarán al host en el extremo y pertenecerán a la organización que haya seleccionado

Nota

AXIS Device Manager Extend debe poder acceder al hardware de Axis en el VMS. Para obtener más información sobre los dispositivos compatibles, consulte *Solución de problemas para agregar dispositivos al host en el extremo, on page 104*.

8. Si agrega nuevos dispositivos a un servidor de grabación o cambia la información de un dispositivo, deberá realizar el paso 7 de nuevo para sincronizar los cambios con el sistema AXIS Device Manager Extend.
9. Repita los pasos 4 a 7 para todos los servidores de grabación con los dispositivos que desea agregar a AXIS Device Manager Extend.

Estado del host en el extremo

En cada servidor de grabación de **System overview (Información general del sistema)**, puede ver si el host del extremo se ha instalado o si ya se ha reclamado. Puede activar **Show machines that need edge host action (Mostrar las máquinas que necesiten una acción de host en el extremo)** para filtrar la vista.

- – No se ha detectado ningún host en el extremo en el servidor de grabación.
  - Si no se ha instalado ningún host en el extremo, descargue e instale el host en el extremo en el servidor de grabación. Consulte *Instalar el host en el extremo, on page 102*.
  - Si se instala el host en el extremo, significa que debe iniciar sesión en la cuenta MyAxis para poder detectar dicho host.
- – El host en el extremo se ha instalado pero no se ha reclamado. Reclame el host en el extremo creando una nueva organización o seleccione una organización creada anteriormente. Consulte *Reclamar el host en el extremo y sincronizar dispositivos, on page 103*.
- – El host en el extremo se ha instalado y reclamado pero no se puede comunicar con él. Compruebe si el servidor de grabación dispone de acceso a Internet.
- – El host en el extremo está sincronizado.

-  – El host en el extremo necesita sincronización. Pueden ser dispositivos nuevos del VMS que se pueden agregar al host local o información actualizada del dispositivo que hay que sincronizar.

Utilizar AXIS Device Manager Extend para configurar dispositivos

Una vez que los dispositivos se han sincronizado con el host en el extremo, puede configurar los dispositivos en AXIS Device Manager Extend. Puede hacerlo desde cualquier PC conectado a Internet.

Nota

Si también desea gestionar dispositivos a través de una conexión remota, deberá encender el *Remote access on each edge host (Acceso remoto en cada host en el extremo)*.

1. Instale y abra la *aplicación de escritorio AXIS Device Manager Extend*.
2. Seleccione la organización utilizada para reclamar el host en el extremo.
3. Los dispositivos sincronizados se pueden encontrar en una instalación con el mismo nombre que el servidor de grabación del VMS.

Solución de problemas para agregar dispositivos al host en el extremo

Si tiene problemas para agregar dispositivos al host en el extremo, asegúrese de hacer lo siguiente:

- AXIS Optimizer solo agregará el hardware habilitado desde el VMS.
- Compruebe que la conexión con el hardware no está rota en el VMS.
- Asegúrese de que el dispositivo tiene la versión AXIS OS 6.50 o superior.
- Asegúrese de que el dispositivo está configurado para autenticación Digest. De forma predeterminada, AXIS Device Management no admite autenticación básica.
- Intente agregar dispositivos directamente desde la aplicación de AXIS Device Manager Extend.
- Recopile registros de AXIS Device Manager Extend y póngase en contacto con el servicio de asistencia técnica de Axis.
  1. En la aplicación de AXIS Device Manager Extend, vaya a la instalación específica, en el servidor de grabación, donde está instalada la cámara.
  2. Vaya a **Settings (Configuración)** y haga clic en **Download sitelog (Descargar registro de la instalación)**.

Importar AXIS Site Designer

En AXIS Optimizer, puede importar el proyecto de diseño de AXIS Site Designer y aplicar la configuración a VMS en un proceso de importación sencillo. Utilice *AXIS Site Designer* para diseñar y configurar el sistema. Una vez finalizado el proyecto, puede importar los ajustes de todas las cámaras y otros dispositivos desde AXIS Site Designer a Management Client mediante AXIS Optimizer.

Para obtener más información sobre AXIS Site Designer, consulte el *manual del usuario*.

Nota

Requisitos

- Version 2020 R2 o posterior de VMS

Importar un proyecto de diseño



En AXIS Site Designer

1. Cree un proyecto y configure los dispositivos.
2. Cuando haya finalizado el proyecto, genere un código o descargue el archivo de ajustes.

Nota

Si realiza actualizaciones en el proyecto de diseño, deberá generar un código nuevo o descargar un archivo de ajustes nuevo.

En Management Client

1. Asegúrese de que se agregan los dispositivos relevantes a VMS.
2. Vaya a **Site Navigation > AXIS Optimizer > Import design project (Navegación por el sitio > AXIS Optimizer > Importar proyecto de diseño)**.
3. Se abre una guía paso a paso. Seleccione el proyecto que desee importar introduciendo el código de acceso o seleccionando el archivo de ajustes del proyecto. Haga clic en **Next (Siguiente)**.
4. En **Project overview (Información general del proyecto)** puede ver información sobre cuántos dispositivos se encuentran en el proyecto de AXIS Site Designer y cuántos en VMS. Haga clic en **Next (Siguiente)**.
5. En el siguiente paso, los dispositivos de VMS coincidirán con los del proyecto de diseño de AXIS Site Designer. Los dispositivos que solo tienen una coincidencia posible se seleccionan automáticamente. Solo se importarán los dispositivos que coincidan. Cuando haya finalizado la coincidencia, haga clic en **Next (Siguiente)**.
6. Los ajustes de todos los dispositivos compatibles se importarán y aplicarán a VMS. Este proceso puede tardar varios minutos, en función del tamaño del proyecto de diseño. Haga clic en **Next (Siguiente)**.
7. En **Results of import (Resultados de la importación)** puede encontrar detalles sobre los distintos pasos del proceso de importación. Si no se han podido importar algunos ajustes, arregle los problemas y vuelva a ejecutar la importación. Haga clic en **Export... (Exportar...)** si desea guardar la lista de resultados como un archivo. Haga clic en **Done (Listo)** para cerrar la guía paso a paso.

Ajustes importados

Solo forman parte de la importación dispositivos coincidentes entre VMS y el proyecto de diseño. Los siguientes ajustes se importarán y aplicarán a VMS para todos los tipos de dispositivo:

- Nombre del dispositivo utilizado en el proyecto de diseño
- Descripción del dispositivo utilizado en el proyecto de diseño
- Ajustes de geolocalización, si el dispositivo está colocado en un mapa

Si el dispositivo está habilitado para vídeo, también se aplicarán los siguientes ajustes:

- Uno o dos flujos de vídeo configurados en VMS (resolución, velocidad de fotogramas, códec, compresión y ajustes de Zipstream)
  - El flujo de vídeo 1 está configurado para la visualización en directo y la grabación.
  - El flujo de vídeo 2 está configurada para la grabación, si los ajustes de transmisión del proyecto de diseño difieren entre la visualización en directo y la grabación.
- Las reglas para la detección de movimiento o la grabación continua se configuran según el proyecto de diseño. Se utiliza la detección de movimiento integrada del VMS, se crean perfiles de tiempo para las reglas y se crean perfiles de almacenamiento para distintos tiempos de retención en los servidores de grabación.
- El micrófono está encendido o apagado según los ajustes de audio del proyecto de diseño.

Limitaciones

Existen limitaciones en el VMS al importar proyectos de diseño de AXIS Site Designer.

- La regla de grabación de movimiento predeterminada de VMS puede invalidar las reglas de grabación creadas mediante la importación. Desactive las reglas conflictivas o excluya los dispositivos afectados de las reglas.
- Las estimaciones de grabación pueden ser imprecisas para las grabaciones desencadenadas por movimiento del VMS.
- Los planos de planta no son compatibles con la versión actual.
- Si tanto las grabaciones desencadenadas por movimiento como las continuas se configuran simultáneamente en el proyecto de diseño, solo se utilizarán los ajustes de flujo de los ajustes de grabación desencadenados por movimiento.
- No puede configurar la velocidad de fotogramas mínima para Zipstream en el VMS.

Administración de cuentas

La gestión de cuentas le ayuda a administrar las cuentas y contraseñas en todos los dispositivos Axis utilizados por XProtect.

Según las pautas de Axis, no debe utilizar una cuenta raíz para conectarse a dispositivos. Con Gestión de cuentas puede crear una cuenta de servicio XProtect. Se crean contraseñas únicas de 16 caracteres para cada dispositivo. Los dispositivos que ya tienen la cuenta XProtect obtienen nuevas contraseñas.

Conéctese a dispositivos con cuenta de servicio XProtect

1. Vaya a**Site Navigation > AXIS Optimizer > Account management (Navegación del sitio > AXIS Optimizer > Gestión de cuentas)**.
   El gráfico muestra cuántos dispositivos están en línea, cuántos de estos tienen la cuenta de servicio XProtect y cuántos no tienen la cuenta de servicio XProtect.
2. Haga clic en **Show device details (Mostrar detalles del dispositivo)** para ver más información sobre los dispositivos. Los dispositivos que están en línea se muestran en la parte superior de la lista. Puede seleccionar dispositivos específicos para generar contraseñas. Si no se selecciona ninguno, todos los dispositivos que estén en línea obtendrán nuevas contraseñas. Haga clic en **OK**.

Nota

Si selecciona HTTP en la configuración del hardware, las contraseñas se enviarán en texto sin formato entre el servidor de grabación y el dispositivo Axis. Le recomendamos que configure HTTPS para asegurar la comunicación entre el VMS y su dispositivo.

3. Haga clicen **Generate passwords (Generar contraseñas)**. La contraseña generada incluye un texto aleatorio de 16 caracteres ASCII que varían de 32 a 126.
   Haga clic en **Show device details (Mostrar detalles del dispositivo)** para ver actualizaciones de estado en directo del proceso. Durante el proceso, verá una breve interrupción de las visualizaciones en directo activas y de las grabaciones pendientes.
4. Los dispositivos que están en línea obtienen la cuenta del servicio XProtect y nuevas contraseñas. Los dispositivos que están en línea y ya tenían la cuenta del servicio XProtect solo obtienen contraseñas nuevas.

Eventos de Axis

La función de eventos de Axis proporciona información general sobre los eventos disponibles para los dispositivos Axis en el VMS. Puede probar eventos en un dispositivo específico, ver los detalles sobre los eventos y agregar eventos a varios dispositivos.

En **Site Navigation (Navegación de instalaciones)**, vaya a **Rules and Events > Axis events (Reglas y eventos > Eventos de Axis)**. En la ventana **Configuration (Configuration)** se muestra una lista de todos los eventos disponibles. Puede ver qué eventos están activos en el sistema y qué eventos no están activos.

Para cada evento, puede ver el nombre de dispositivo de los dispositivos a los que se agrega el evento. También puede ver el nombre para mostrar del evento, el estado del evento y la última vez que se activó.

Nota

Requisitos

- Version 2023 R2 o posterior de VMS.

Configurar un evento para varios dispositivos

1. Vaya a **Configuration (Configuración)** y seleccione un evento.
2. Haga clic en **Add devices** .
3. La ventana **Add devices (Agregar dispositivos)** muestra una lista de dispositivos a los que se puede agregar el evento. Seleccione uno o más dispositivos y haga clic en **Add devices (Agregar dispositivos)**.

Para eliminar un evento de un dispositivo, haga clic en **Remove (Eliminar)**.

Información de eventos

En los eventos de Axis, puede ver la última aparición, el estado de los eventos y las actualizaciones en tiempo real conocidas en la interfaz de usuario. Para ello, debe establecer el tiempo de retención en el cliente de gestión.

1. Vaya a **Tools > Options > Alarm and Events > Event retention (Herramientas > Opciones > Alarma y eventos > Retención de eventos)**.
2. Defina el tiempo de retención de todo el grupo de eventos del dispositivo o de los eventos específicos del grupo.

Metadata and search

Metadatos y búsqueda ofrece un información general de todos los dispositivos que ha añadido en su VMS, sus capacidades de metadatos y las categorías de búsqueda Axis visibles para sus operadores.

Metadatos y búsqueda le permiten activar características específicas para estos dispositivos, es decir, puede activar datos de eventos, datos de analíticas y datos consolidados para varios dispositivos, así como ver las características de analíticas compatibles con sus dispositivos. Con las categorías de búsqueda de Axis, puede controlar las opciones de búsqueda de todos los operadores para reflejar las características de analíticas existentes en su VMS. La compatibilidad con las categorías de búsqueda y los filtros varía con los modelos de cámara y las aplicaciones de analíticas instaladas.

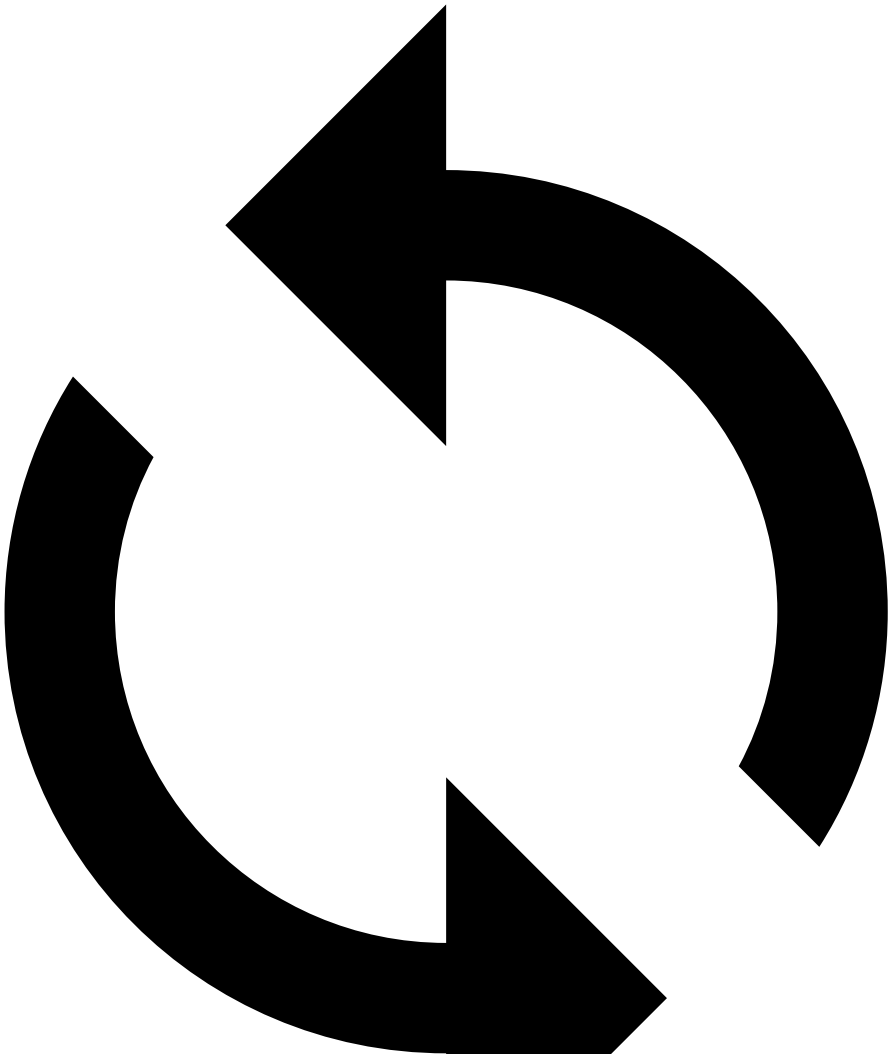
Configurar los ajustes de metadatos

1. Vaya a **Management Client (Cliente de gestión)** > **Site Navigation (Navegación de instalaciones)** > **AXIS Optimizer** > **Metadata and search (Metadatos y búsqueda)**.
   - **Datos de eventos**: Active el VMS para recuperar los datos de eventos del dispositivo. Necesita esto para varias características de AXIS Optimizer.
   - **Analytics data (Datos de analíticas)**: Active esta opción para utilizar la función de búsqueda forense y mostrar los cuadros limitadores en la reproducción y la visualización en directo.
   - **Características de analíticas**: Vea las características de analíticas de vídeo que admite actualmente el dispositivo, como el tipo de objeto (humanos, coches) y el color del objeto. Una actualización del software del dispositivo puede proporcionar más funciones de analíticas.
   - **Metadatos consolidados**: Actívelos para una búsqueda forense más rápida y un tiempo de carga menor en investigaciones de Axis.

   Nota

   Requisitos de metadatos contrastados
   - Dispositivos Axis con AXIS OS 11.10 o versiones posteriores.

   Limitaciones de metadatos consolidadas
   - Los cuadros limitadores de la visualización en directo y la grabación, y las opciones de búsqueda integradas en VMS no están disponibles.

– 
: Haga clic para volver a cargar después de realizar cambios en la configuración de su dispositivo.

Configurar categorías de búsqueda de Axis

1. Vaya a **Management Client (Cliente de gestión)** > **Site Navigation (Navegación de instalaciones)** > **AXIS Optimizer** > **Metadata and search (Metadatos y búsqueda)**.
2. Active las categorías de búsqueda que desee utilizar en el cuadro de diálogo **Axis search categories** (Categorías de búsqueda de Axis):
   - Búsqueda forense
   - Búsqueda de vehículos
   - Búsqueda de velocidad de zona
   - Búsqueda de contenedores
3. Seleccionar filtros aplicables en cada categoría de búsqueda.

Nota

Requisitos de categorías de búsqueda de Axis

- AXIS Optimizer versión 5.3 o posterior en Smart Client.

Ciberseguridad

La ciberseguridad contribuye a un ciclo de vida satisfactorio del producto con riesgos minimizados. Puede encontrar información detallada y documentación sobre nuestro enfoque en materia de ciberseguridad en *about our cybersecurity approach at axis.com/about-axis/cybersecurity*. Siga las directrices de ciberseguridad que se indican a continuación para recibir notificaciones de seguridad de Axis sobre el producto y para realizar la configuración de su producto de modo que garantice un ciclo de vida y una desinstalación seguros.

En *Axis Trust Center*, puede encontrar información sobre la implementación que hace Axis de las medidas de cumplimiento de seguridad, transparencia, protección de datos y privacidad.

Gestión de las vulnerabilidades

Axis es una *Common Vulnerability and Exposures (CVE) Numbering Authority (CNA) (autoridad numeradora de vulnerabilidades y exposiciones comunes (CVE) (CNA))*. Para minimizar su riesgo de exposición, satisfacemos las normas del sector a la hora de identificar y resolver vulnerabilidades en nuestros dispositivos, software y servicios. Consulte más información sobre nuestra política de gestión de vulnerabilidades o notifique una vulnerabilidad en *axis.com/vulnerability-management*.

Notificaciones de seguridad

Suscríbase a los correos electrónicos de notificaciones de seguridad de Axis en *axis.com/security-notification-service*. Le enviaremos información sobre vulnerabilidades, los avisos de seguridad correspondientes y otros asuntos relacionados con la seguridad de su producto Axis.

Ciclo de vida seguro del producto

Axis minimiza los riesgos a lo largo de la vida útil de nuestros productos mediante una gestión segura del ciclo de vida. Utilice nuestras guías de refuerzo en *help.axis.com* para configurar y operar sus productos Axis del modo más seguro y para encontrar información sobre:

Primer uso seguro – Los productos Axis vienen preconfigurados con un alto nivel de protección por defecto para permitir una inicialización segura y una comunicación cifrada desde el primer momento.

Uso previsto y errores de configuración comunes – Nuestras guías facilitan información sobre el uso previsto de los productos Axis, incluidos errores de uso comunes relacionados con la seguridad y errores de configuración que deben evitarse.

Gestión de vulnerabilidades y transparencia en la cadena de suministro – Con cada lanzamiento de software se publica una lista de materiales de software (SBOM) en *axis.com y* con el fin de revelar vulnerabilidades y mejorar la transparencia de la cadena de suministro.

Desinstalación y borrado seguro de datos – Para desinstalar un producto de forma segura cuando alcanza el término de su ciclo de vida, restablézcalo a los valores predeterminados de fábrica. Esto eliminará sus configuraciones, datos almacenados e información confidencial.

Guía de seguridad

Como parte integral de su infraestructura VMS, AXIS Optimizer requiere configuraciones específicas para garantizar un entorno seguro. Es fundamental seguir estos ajustes recomendados para proteger las contraseñas de los dispositivos, salvaguardar la información privada y evitar el acceso no autorizado a su sistema.

- Utilice HTTPS cuando añada dispositivos Axis al VMS.
- Active el cifrado entre los clientes y los servidores de VMS.
- Activa el almacenamiento cifrado de datos en el VMS.
- Revise todos los roles del VMS y asegúrese de que no tengan más permisos de los necesarios.

¿Necesita más ayuda?

Preguntas frecuentes

Pregunta	Respuesta
¿Cómo puedo actualizar AXIS Optimizer cuando el PC cliente no tiene acceso a Internet?	Publicación de la nueva versión en el servidor de gestión VMS, consulte *Actualizar sistema automáticamente, on page 10*.
¿Debo realizar una copia de seguridad de los ajustes antes de actualizar a una versión más reciente de AXIS Optimizer?	No, no necesita hacer una copia de seguridad. Nada va a cambiar al actualizar a la versión más reciente.
Si tengo más de 30 ordenadores clientes con AXIS Optimizer, ¿tengo que actualizarlos uno por uno?	Puede actualizar las clientes individualmente. También puede impulsar la actualización automáticamente publicando una versión local de AXIS Optimizer en su sistema, consulte *Actualizar sistema automáticamente, on page 10*.
¿Puedo activar o desactivar cada complemento dentro de AXIS Optimizer por separado?	No, pero no consumen recursos si no se utilizan activamente.
¿Qué puertos utiliza AXIS Optimizer?	Los puertos 80 y 443 son necesarios para comunicarse con axis.com a fin de que su sistema pueda obtener información sobre nuevas versiones y descargar actualizaciones. Los puertos 53459 y 53461 se abren al tráfico entrante (TCP) durante la instalación de AXIS Optimizer a través de AXIS Secure Entry.

Localización de problemas

Si surgen problemas técnicos, active el registro de depuración, copie el problema y comparta los registros con el servicio de asistencia técnica de Axis. Puede activar el registro de depuración en Management Client o Smart Client.

En Management Client:

1. Vaya a **Site Navigation (Navegación del sitio)** > **Basics (Ajustes básicos)** > **AXIS Optimizer**.
2. Seleccione **Turn on debug logging (Activar registro de depuración)**.
3. Haz clic en **Save report (Guardar informe)** para guardar los registros en su dispositivo.

En Smart Client:

1. Vaya a **Settings (Ajustes)** > **Axis general options (Opciones generales de Axis)**.
2. Seleccione **Turn on debug logging (Activar registro de depuración)**.
3. Haz clic en **Save report (Guardar informe)** para guardar los registros en su dispositivo.

Contactar con la asistencia técnica

Si necesita más ayuda, vaya a *axis.com/support*.

Sugerencias y consejos

Agregar una página web en una vista Smart Client

AXIS Optimizer puede mostrar casi todas las páginas web directamente en Smart Client, no solo las páginas html. Este modo de vista web funciona con un moderno motor de navegación y es compatible con la mayoría de las páginas web. Esto es útil, por ejemplo, cuando desea acceder a AXIS Body Worn Manager desde Smart Client o mostrar un tablero de AXIS Store Reporter junto a sus vistas en vivo.

1. En Smart Client, haga clic en **Setup (Configuración)**.
2. Vaya a **Views (Vistas)**.
3. Cree una nueva vista o seleccione una existente.
4. Vaya a **System overview > AXIS Optimizer (Información general del sistema > AXIS Optimizer)**.
5. Haga clic en **Web view (Vista Web)** y arrástrela a la vista.
6. Introduzca una dirección y haga clic en **OK (Aceptar)**.
7. Haga clic en **Setup (Configuración)**.

Exportar vídeos con funciones de búsqueda integradas

Exportar vídeos en formato XProtect

Para ver vídeos con funciones de búsqueda integradas de AXIS Optimizer y/o corrección de distorsión esférica de Axis, asegúrese de exportar vídeos en formato XProtect. Esto puede resultar útil, por ejemplo, para fines de demostración.

Nota

Comience desde el paso 3 para AXIS Optimizer versión 5.3 o posteriores.

1. En Smart Client, vaya a **Settings (Ajustes)** > **Axis search options (Opciones de búsqueda de Axis)**.
2. Active **Include search plugins in exports (Incluir complementos de búsqueda en exportaciones)**.
3. Seleccione **XProtect format (Formato XProtect)** al crear la exportación en Smart Client.

Desbloquear exportaciones en ordenadores receptores

Para utilizar correctamente la exportación en otro ordenador, asegúrese de desbloquear el archivo de exportación.

1. En el ordenador receptor, haga clic con el botón derecho en el archivo de exportación (zip) y seleccione **Properties (Propiedades)**.
2. En **General (General)**, haga clic en **Unblock (Desbloquear)** > **OK (Aceptar)**.
3. Extraiga la exportación y abra el archivo "SmartClient-Player.exe".

Reproducción de la vista de corrección de distorsión esférica de Axis exportada

1. Abrir el proyecto exportado.
2. Seleccionar la vista que incluye la vista de corrección de distorsión esférica de Axis.

T10134385_es

2026-09 (M61.2)

© 2021 – 2026 Axis Communications AB